

SIAS

2012

7^E CONFÉRENCE
INTERNATIONALE SUR
LA SÉCURITÉ DES SYSTÈMES
INDUSTRIELS AUTOMATISÉS

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



11-12 OCTOBRE 2012 MONTRÉAL, CANADA OCTOBER 11-12, 2012

Actes de la 7^e conférence internationale
sur la sécurité des systèmes industriels automatisés

*Proceedings of the 7th International Conference
on the Safety of Industrial Automated Systems*



THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS

CONFERENCE SCIENTIFIC COMMITTEE

Philippe Charpentier, INRS, France
Yuvn Chinniah, École Polytechnique, Canada
Marek Dzwiarek, CIOP-PIB, Poland
Elie Fadier, INRS, France
Jeff Fryman, RIA, USA
Toshihiro Fujita, NECA, Japan
Timo Malm, VTT, Finland
Hiroyasu Ikeda, JNIOH, Japan
Michael Schaefer, IFA, Germany
Steve Shaw, HSE, UK

Legal Deposit

Bibliothèque et Archives nationales du Québec
2012
ISBN : 978-2-89631-635-9 (PDF)
ISSN : 0820-8409

IRSST – Communications and Knowledge
Transfer Division
505 De Maisonneuve Blvd. West
Montréal, Québec
H3A 3C2
Phone: 514 288-1551
Fax: 514 288-7636
publications@irsst.qc.ca
www.irsst.qc.ca
© Institut de recherche Robert-Sauvé
en santé et en sécurité du travail,
October 2012

THURSDAY, OCTOBER 11, 2012

8:00 – 8:50	Registration and coffee
8:50 – 9:00	Welcome speech
9:00 – 9:45	<p>PLENARY SESSION Chair: Yuvin Chinniah, Canada</p> <p>Risk Assessment: Advances and Challenges <i>Bruce Main, design safety engineering, inc.</i></p>
9:45 – 10:25	<p>SESSION 1 – RISK ASSESSMENT Chair: Yuvin Chinniah, Canada</p>
9:45	
10:05	<p>The RAPEX - Risk Assessment method for European market surveillance authorities <i>Hans-Joerg Windberg, Fed. Inst. for Occ. Safety & Health</i></p>
10:25 – 10:45	Coffee break
10:45 – 11:45	<p>SESSION 2 – SAFETY OF MACHINERY; ERGONOMIC AND HUMAN FACTORS AND CONCEPTION Chair: Michael Schaefer, Germany</p>
10:45	<p>The contribution of standards to risk control in machinery design: the role of ergonomics <i>Elie Fadier, Jean-Louis Pomian, INRS</i></p>
11:05	<p>Implementation of ergonomic principles in the design of machinery <i>Georg Kraemer, VBG</i></p>
11:25	<p>Prevention through design in OSH by risk assessment of virtual river locks <i>Peter Nickel, Andy Lungfiel, Michael Huelke, IFA, Eugen Pröger, WSV-FVT, Rolf Kergel, UK Bund</i></p>
11:45 – 13:00	Lunch
13:00 – 14:20	<p>SESSION 3 – PROTECTIVE DEVICES AND SYSTEMS Chair: Philippe Charpentier, France</p>
13:00	<p>Pedestrian Detection for Industrial Vehicles based on morphological recognition: first feed-back after 18 months of operation <i>Franck Gayraud, Arcure, Laurent Lucat, CEA</i></p>
13:20	<p>Application of RADAR Technology to Mobile Machine-Pedestrian <i>David Tihay, INRS</i></p>
13:40	<p>Systematic failures & functional safety (a challenge for the selection and application of protective devices) <i>Otto Görnemann, SICK AG</i></p>
14:00	<p>Spectral Light Curtains - A Novel Near-Infrared Sensor System for Production Machines <i>Norbert Jung, Bonn-Rhein-Sieg University of Applied Sciences</i></p>

14:20 – 15:40**POSTER SESSION**

(Coffee will be served during the poster session.)

15:40 – 16:40**SESSION 4 – FUNCTIONAL SAFETY AND CONTROL SYSTEM****Chair: Timo Malm, Finland****15:40**

Validation of machines under consideration of the new EN ISO 13849-2

*Klaus-Dieter Becker, Validation of control systems***16:00**

Evaluating performance levels of machine control functions

*Marita Hietikko, VTT***16:20**

An a posteriori estimation of the performance level for a safety function using NF EN ISO 13849-1:2008

*Sabrina Jocelyn, IRSST***19:30**Banquet – Le Place d'Armes Hôtel & Suites (www.hotelplacedarmes.com/en/)**FRIDAY, OCTOBER 12, 2012****9:00 – 10:00****SESSION 5 – ROBOTS SAFETY****Chair: Jeff Fryman, USA****9:00**

Industrial Robotic: Accident analysis and Human - Robot Coactivity

*Philippe Charpentier, Adel Sghaier, INRS***9:20**

Risk assessment and investigation of change from pressure feeling to pain

*Matthias Umbreit, Berufsgenossenschaft Holz und Metall***9:40**

Evaluation of Injury Level and Probability for Risk Assessment of Mobile Robots

*Tatsuo Fujikawa, Masami Kubota, Yoji Yamada, Hiroyasu Ikeda, Japan Automobile Research Institute***10:00 – 10:20**

Coffee break

10:20 – 11:40**SESSION 5 – ROBOTS SAFETY (CONTINUED)****Chair: Jeff Fryman, USA****10:20**

Collaborative Robotics: Measuring Blunt Force Impacts on Humans

*Joe Falco, Jeremy Marvel, Rick Norcross, NIST***10:40**

Development of Safety Technology for Outdoor-use Person Carrier Robots that Achieve the Optimal Safety and Usability in the Ageing Society with a Declining Birthrate

Kazuya Okada, Tatsuyoshi Kuriyama, Osugi Norifumi, Dohi Masao, Toshihiro Fujita, IDEC Corporation

11:00	Safety of Industrial Robots: From Conventional to Collaborative Applications <i>Bjoern Matthias, ABB AG Corporate Research Jeff Fryman, Robotic Industries Association</i>
11:20	How to approve Collaborative Robots: a Force Pressure Measurement System <i>Michael Huelke, Jürgen Ottersbach, IFA</i>
11:40 – 13:00	Lunch
13:00 – 14:40	SESSION 6 – MACHINE SAFETY; PRACTICAL APPLICATIONS AND KNOWLEDGE DISSEMINATION Chair: Hiroyasu Ikeda, Japan
13:00	New Focus on safety at machinery work places <i>Michael Schaefer, IFA</i>
13:20	Safety functions of automated mobile working machines <i>Timo Malm, Marita Hietikko, Risto Tiusanen, VTT, Ari Ronkainen, MTT</i>
13:40	Design of fault-tree-based software to improve the safety of printing press operators <i>Laurent Giraud, Sabrina Jocelyn, IRSST</i>
14:00	The Improvement of Industrial Safety achieved by the Introduction of Safety Assessor / Safety Basic Assessor Qualification System and its International Operations <i>Masahiro Tochio, Japan Certification Corporation</i>
14:20	Design and build machines really safe: how to pass from myth to reality ? <i>Patrik Doucet, Université de Sherbrooke, Alain Brassard, Roche ltd, Consulting Group</i>
14:40 – 15:00	Coffee break
15:00 – 16:00	SESSION 7 – MACHINE SAFETY; MAINTENANCE AND OTHER ASPECTS Chair: Joseph-Jean Paques, Canada
15:00	Preliminary results of the lockout/tagout application and observations in the sawmills industries in Québec <i>Pascal Poisson, Yuvin Chinniah, École Polytechnique de Montréal</i>
15:20	Integration of maintenance at design stage. The «machinery» directive lays down objectives <i>Blaise Jean-Christophe, INRS</i>
15:40	
16:00 – 16:15	WRAP-UP

POSTER SESSION**RISK ASSESSMENT**

The Application of Risk Assessment to Facilities Planning: A Synthesis of Risk Assessment Methods and Layout Design Models

Afrooz Moatari Kazerouni, École Polytechnique de Montréal

Quantitative Analysis Of The Risks Associated With An Industrial Machine: The Case Of A Compression Moulding Press

Tony Venditti, ASFETM et École de Technologie Supérieure

SAFETY OF MACHINERY, ERGONOMICS, HUMAN FACTORS AND CONCEPTION

Virtual Reality in OSH for Product Safety and Usability

Peter Nickel, Andy Lungfiel, Birgit Naber, Michael Hauke, Michael Huelke, IFA

Safety Service Engineering - An additional concept for safety of machinery

Takashi Kabe, NPO Safety Engineering Laboratory

PROTECTIVE DEVICES AND SYSTEMS

The Accident prevention of Mobility scooter by automatic slowdown with laser range finder

Hiroto Inoi, Shinya Hashimoto, Tatuoyoshi Kuriyama Toshihiro Fujita and Kazuya okada, Osaka University

Consideration on RFID Devices Applying to Safety of Integrated Manufacturing Systems

Takabumi Fukuda, Nagaoka University of Technology

Development of Interlock Switch with Lock Function for theimproved Safety in the Event of Breakage

Takeo Yasui, Norifumi Obata, Takao Fukui, Atsushi Matsumoto, Toshihiro Fujita, IDEC Corporation

Safety Control for Collaboration Work of Press Machine and Person Based on Safety Level Defined by Position and Velocity Vector

Yukio Hata, Komatsu Industries Corp., Yuji Hirao, Nagaoka University of Technology

A Study of Risk Reduction Strategy using Supporting Protective Device

S. Shimizu, S.Umezki , JNIOOSH

Study on Evaluation of Position Detectors for an Interlocking Guard in Consideration of Safety and Hygiene Aspect

Hiroyuki Omura, The Japan Food Machinery Manufacturer's Association, Takabumi Fukuda, Nagaoka University of Technology, Noboru Sugimoto, Meiji University

FUNCTIONAL SAFETY AND CONTROL SYSTEM

Automatic Generation of Diverse Software Channels for Fail-safe Industrial PC

Frank Schiller, Beckhoff Automation

Reliability Databases used by the ISO 13849 tool SISTEMA

Michael Huelke, Andy Lungfiel, IFA

An Improvement in Applying Safety Standard "ISO 13849" using Fuzzy Logic

Mohammad Sohani, Mohamed-Salah Ouali, Yuvin Chinniah, École Polytechnique de Montreal

The use of ISO 13849-1 to design "basic" safety functions

Philippe Charpentier, James Baudoin, Jean-Paul Bello, INRS

Architectural Views of Safety Systems

Timo Vepsäläinen, Seppo Kuikka, Tampere University of Technology

Consideration on the structure for risk reduction of fire from electric heating devices

Akira Matsuura, Takabumi Fukuda, Nagaoka University of Technology

ROBOTS SAFETY

Development of a Self-Check Sheet for Safety Design of Human-Collaborative Robots

Hiroyasu Ikeda, Kuniyuki Niwa, Yuichiro Shimizu, JNIOOSH

Serial Kinematics based Motion Simulator - Passenger safety

Karan Sharma, Sami Haddadin, Tobias Bellmann, Sven Parusel, Tim Rokahr, Johann Heindl, Gerd Hirzinger, Institute of Robotics and Mechatronics, German Aerospace Center (DLR)

Study on Law and Social Systems for the Safety of Social-care Robots

Masahiro Kato, Manufacturing Science and Technology Center

Empirical Approach to Assessing Foot Injury Level Resulting from being Run Over by a Mobile Robot

Masami Kubota, Tatsuo Fujikawa, Japan Automobile Research Institute

MACHINE SAFETY; PRACTICAL APPLICATIONS AND KNOWLEDGE DISSEMINATION

Analysis of the contribution of equipment reliability problems in the chain of causality of industrial incidents and accidents in a pulp and paper plant

François Gauthier, Dominic Bourassa, Université du Québec à Trois-Rivières

Adaptive safety concepts for automated mobile machine systems

Risto Tiusanen, T. Malm, Ronkainen, VTT

MACHINE SAFETY; MAINTENANCE AND OTHER ASPECTS

Intervention on Machines - Operating Modes with "disabled safeguarding

Blaise Jean-Christophe, Guy Welitz, INRS

Development of knowledge about the practice and the specificities of lockout in the municipalities in Québec

Damien Burllet-Vienney, IRSST

A study on nullification of safeguards for industrial machinery in Japan

Kohei Okabe, Hiroyasu Ikeda, Shigeo Umezaki, JNIOOSH

SIAS
2012

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



SESSION 1

RISK ASSESSMENT

The RAPEX- Risk Assessment method for European market surveillance authorities

Hans-Joerg Windberg, Fed. Inst. For Occ. Safety and Health, Dortmund, Germany

When finding a dangerous (technical) product on a local european market which keeps a serious risk for the health and the safety of persons, all market inspectors are obliged to use the european rapid exchange information system (RAPEX)to inform their colleagues in the other member states quickly.

Since a couple of years the European Commission takes efforts in developping a harmonized system of assessing a risk to avoid uncoordinated and oversized actions of the market- or labour- inspection bodies.

After a short period of testing a first version meanwhile an optimized risk assessment method is on the market and published in the "RAPEX-Guidelines" of the EU.

It is foreseen to use these harmonized method in all member countries and by every market inspector to assess a risk of a product more thoroughly than it was done in the past.

The filled out risk assessment form shall be attached to any future official RAPEX- notification which informs on a serious risk.

The author who is head of the German RAPEX- focal point will introduce the method in comparison with the ISO- 14121/ISO 12100- methods and show on example(s) of common consumer products how it works.

The Application of Risk Assessment to Facilities Planning: A Synthesis of Risk Assessment Methods and Layout Design Models

A. Moatari Kazerouni, B. Agard, Y. Chinniah

Department of Mathematical and Industrial Engineering, École Polytechnique de Montréal - Canada

(afrooz.moatari-kazerouni@polymtl.ca; bruno.agard@polymtl.ca; yuv.chinniah@polymtl.ca)

KEY WORDS: occupational health and safety (OH&S), facilities planning models, risk assessment methods

ABSTRACT

The layout planning of facilities constitutes an important issue to be faced by a company. While the main concern with the facilities layout planning is to reduce the cost of material handling, the layout of a facility plays a major role in the safety and productivity of operations. Many approaches have been presented for planning facilities layouts; however, OH&S issues were often ignored in most previous studies. This is despite the need for preventing or minimizing accidents through proper facilities layout planning.

Moreover, methods of identifying hazard and assessing risks, which may exist in a company, can take many forms. Each method offers a different perspective and with it differing strengths and weaknesses. Depending on the system design of the company and the user interactions with it, one or more methods can be used to assess risks. Therefore, which particular method best suits for risk assessment, would depend on the application.

Due to the diversity of the tools for facilities planning and risk assessment, this paper surveys the facilities layout planning models and risk assessment methods. Different methods, used by companies as the risk assessment tools, are presented. Most of the conventional algorithms and techniques for solving facilities layout problems are also reviewed and their characteristics are commented. This survey will pave the way to the integration of these two types of tools, i.e. having a facility planning tool which incorporates OH&S. General remarks and tendencies are reported for merging these two research fields.

1 INTRODUCTION

Safety management and risk assessment receive growing attention as companies seek to implement methods in order to maximize the use of safety and optimize the use of financial resources. The risk assessment process is flexible and scalable as exposed in real world applications. However, it is likely that the diversity of risk estimation tools, which are available to carry out the risk assessment, be attributed to the needs of companies. Therefore, a risk assessment method which successfully used in one company does not necessarily meet the requirements of the other [1].

Likewise, facilities layout planning, as an important research topic in physical system design, has recently received much attention from production engineers. This is partly due to the increased global competition in manufacturing and the efforts to reduce manufacturing costs [2]. The majority of previous research in facilities layout planning has focused on optimizing movement costs, site costs, and qualitative preferences; the relationship between facilities layout and safety concerns has not been considered extensively in developing the methods and models. This paper attempts to present a state-of-the-art review of risk assessment methods, models of facilities layout planning, and characteristics of each of these tools. This is the first step in integrating facility planning and risk assessment.

2 FACILITIES PLANNING MODELS

Where to locate facilities and the efficient design of those facilities are important and fundamental strategic issues facing any manufacturing industry [3]. Traditionally, planning a layout starts by making a layout diagram for the facilities, which consists of different activities connected to each other. The design proceeds by trial and error until a compromise is reached, which more or less satisfies all the known factors and restrictions [4]. Therefore, a layout is traditionally developed using relationships among the various facilities, based on the judgement of experts who decide the importance and strength of relationships between each pair of facilities. However, the decision of experts is vague and usually based on many quantitative or qualitative considerations pertaining to the desired closeness or relationships among the facilities; e.g. flow of materials between facilities or ease of supervision of employees [5].

Moreover, the main objective of the facilities layout problem is to minimize the materials handling cost, which is a quantitative factor. However, qualitative factors such as plant safety, flexibility of layout for future design changes, noise and aesthetics need to be considered as well [6].

2.1 Formulations of Facilities Layout Problem

The facility layout problem considers the assignment of facilities to locations so that the quantitative or qualitative objective of the problem is optimized [7]. The quantitative objective is to minimize the material handling cost, while the qualitative objective is to maximize the subjective closeness rating by considering vital factors such as safety, flexibility, noise, etc. [8] The facility layout problem is one of the best-studied problems in the field of combinatorial optimization, where more particularly it has been modelled as a: (1) quadratic assignment problem (QAP), (2) quadratic set-covering problem (QSP), (3) linear integer programming problem, (4) mixed integer programming problem (MIP), and (5) graph-theoretic problem.

Although these approaches hold much promise, they have drawbacks. Even a powerful computer cannot handle a large instance of the QAP problems. The disadvantage of the QSP approaches is that the problem size increases as the total area occupied by all the facilities is divided into smaller blocks. Computational experiences for linear integer programming models indicated that they are not suitable for problems with more than nine facilities. For MIP, only facilities layout problems of size six or less are optimally solvable. Similar to QAP approaches, unequal area problems of even small size cannot be solved optimally for graph-theoretic problems [7, 9].

2.2 Analytical Solution Methods

Since the late 1950s a number of algorithms have been developed to solve the facility layout problem, classified as:

1. Optimal algorithms: these algorithms, which were developed to solve QAP, fall into two classes: branch and bound algorithms and cutting plane algorithms. The common disadvantages of the optimal algorithms are the high memory and computer time requirements, while the largest problem solved optimally is a problem with 15 facilities. This has encouraged researchers to use sub-optimal algorithms.
2. Sub-optimal algorithms: many researchers developed sub-optimal algorithms to also deal with QAP. These algorithms are classified as: construction algorithm (where a solution is constructed from scratch), improvement algorithm (where an initial solution is improved), hybrid algorithm (combination of two optimal or sub-optimal algorithms), and the graph theoretic algorithm [7].

The major drawbacks of the aforementioned approaches lie in the fact that the search for the best layout is not very efficient and the multi-objective nature of the facilities layout problems are not considered [10]. Many studies focussed on new and recent developments rather than conventional approaches to overcome these drawbacks. Intelligent techniques are presented as new advancements to tackle the problem.

3. Meta-heuristics algorithms: the most well-known of these systems are neural networks, genetic algorithm, simulated annealing, tabu-search, and ant colony optimization;
4. Expert systems;
5. Fuzzy systems; and
6. Intelligent hybrid systems.

Table 1 illustrates some of the analytical solution methods used for facilities layout problems.

Table 1. Survey of analytical solution methods for facilities layout problems

Model	Technique	Objective	Comments
PLANET [11]	Construction	Flow cost	Starts at centre, 2 facilities located at once
FATE [12]	Construction	Flow cost Closeness	Extension to MAT, two criteria to rank facility pairs
MAT [13]	Construction	Flow cost	Allows user to assign facilities to any desired location
ALDEP [14]	Construction	Closeness	Randomly selects a facility, starts at upper left corner
SHAPE [15]	Construction	Flow cost	Based on generalized assignment problem
FLAT [16]	Construction	Flow cost	Facilities of unequal areas, low compute time, good quality results
CORELAP [17]	Construction	Closeness	Selects first facility depending on total closeness value
FLAG [18]	Construction	Flow cost	Interactive, considers various shapes, realistic distances between facilities, the user can modify the layout as desired
RMA [19]	Construction	Closeness	Similar to CORELAP, start at centre
Linear Placement [20]	Construction	Flow cost Closeness	Only for facilities of equal areas, single and multi-storey buildings
HC66 [21]	Construction	Flow cost	Uses criteria of Vogels' approximation in TP
INLAYT [22]	Construction	Flow cost	User can modify the output by using a light-pen
LSP [23]	Construction	Closeness	High computational efforts, similar to ALDEP, flexibility
CRAFT [24]	Improvement	Flow cost	Up to 40 facilities, does not perform well for facilities of unequal areas, uses 2- and 3-way exchanges for smoothing irregular shapes
TSP [25]	Improvement	Flow cost	Similar to CRAFT, executes selective pairwise exchanges, reduces compute time
FRAT [26]	Improvement	Flow cost	Only for facilities of equal area, good quality results, uses principles from e.g. HC63-66, CRAFT, COL
H63 [21]	Improvement	Flow cost	Only pairwise exchanges between adjacent facilities, only for facilities of equal areas, based on a move desirability table
HC 63-66 [21]	Improvement	Flow cost	Limits the exchanges only to facilities which lie on a horizontal, vertical or diagonal line, only for facilities of equal areas, a modification of H63, allows exchange of non-adjacent facilities.
Revised Hillier [27]	Improvement	Flow cost	Uses H63, considering 4-way perturbations, produces solutions at least as good as H63, more computation time than H63
COFAD-F [28]	Improvement	Flow cost	Considerable amount of compute time, flexibility, uses COFAD
COFAD [29, 30]	Improvement	Flow cost	MHS selection, uses CRAFT, jointly considers layout and material handling system, more realistic layouts
COL [31]	Improvement	Flow cost	Good quality solutions, twice as fast as HC66, less memory storage
MICROLAY [32]	Hybrid	Flow cost	Manual adjustments for e.g. aisle space, interactive, a combination of construction and improvement
DISCON [33]	Hybrid	Closeness	Dispersion phase provides good starting points, difficult to justify the outcome, uses a two-phase algorithm of dispersion-concentration
KTM [34]	Hybrid	Flow cost	Uses 2- and 3-way exchanges, a combination of construction and improvement, very good results within very little computer time
FLAC [35]	Hybrid	Flow cost Closeness	Has three stages, a combination of construction and improvement
Wheel Expansion [36]	Graph Theoretic	Adjacency	Similar to Deltahedron
Branch and Bound [37]	Graph Theoretic	Adjacency	Obtain optimal solution, a require maximal planar graph
Deltahedron [37]	Graph Theoretic	Adjacency	Avoid the testing of planarity
FADES [38]	Expert System	Flow cost Closeness, Materials handling cost	Knowledge-based approach, for solving general facility design problems, selecting equipment that meets the required technology level and performing economic analysis, written in PROLOG
IFLAPS [39]	Expert System	Adjacency	In FORTRAN, does not involve paired comparisons between departments or the overall, relationship between various facilities
KBML [40]	Expert System		For machine layout in automated manufacturing systems, a forward-chaining inference strategy is utilized
[41]	Neural Network		Near-optimum parallel algorithm, for an N-facility layout problem, BEING capable of generating better solutions over the existing algorithms for some of the most widely used benchmark problems

[42]	Genetic Algorithm		Pharmaceutical industry, allows the user to select the most important objectives in each particular layout design, outperforms all existing computer layout algorithms such as CRAFT, CORELAP and BLOCPAN as well as human designers in maximizing the throughput rate and minimizing the traveling time/trip
HOPE [43]	Genetic Algorithm		For solving single-floor facility layout problem, considered departments of both equal and unequal sizes, results indicated that GA might provide a better alternative in a realistic environment where the objective is to find a number of reasonably good layouts
MULTI-HOPE [44]	Genetic Algorithm		Multiple-floor layout problems, extends HOPE algorithm, averagely gives a better solution than existing multi-floor layout algorithm
[45]	Fuzzy System	Flow cost Closeness	AHP is used to find the weights of qualitative and quantitative factors affecting the closeness rating between departments, a modified version of CORELAP (FZYCRLP) is used
[46]	Fuzzy System	Flow cost Closeness	Considers organizational links optimisation. A linguistic pattern approach for multiple criteria facility layout problems.
FLEXEPRET [47]	Intelligent Hybrid System		A fuzzy-integrated expert system, generates the best layout that satisfies the qualitative as well as the quantitative constraints on the layout problem, VP-Expert is used
[48]	Intelligent Hybrid System		A neural expert system, creates effective multi-bi-directional generalization behavior, goal-driven layout design experience

3 RISK ASSESSMENT METHODS

Risk assessment methods are proposed by organizations that are involved in the safety of industrial machines (e.g. standardization bodies, OH&S associations) while some companies have established their own methods and tools of analysis [1]. The large number of tools proposed and used indicates that there is no single universal approach for risk assessment [49]. Although risk assessment methods have existed in various forms for many years, interests have recently been increased because of factors such as time, cost, competition, international influences, capturing knowledge, product liability, lack of standards, schedule control, and customer requirements [50]. Despite the fact that there are different tools and methods for assessing risk, it may not be an easy task to choose the tool that best adapted to the needs of each company. Table 2 addresses the common families or types of risk assessment methods.

Table 2. Risk assessment methods for facilities layout problems

Types	Description	Comments
Risk Matrix [51]	A multidimensional table for combination of any class of severity of harm with any class of probability of occurrence of that harm.	Tools can have 2 or more parameters (e.g. severity of harm and probability of harm).
Risk Graph [52]	A tree structure that enables risk to be determined for each safety function.	Usually four parameters are used: consequence of hazardous event, frequency of presence in hazardous zone and potential exposure time or occupancy, probability of avoiding hazardous event, probability of unwanted occurrence.
Numerical Scoring [53]	Numerical scoring tools have 2-4 parameters that are broken down into a number of classes in much the same way as risk matrices and risk graphs.	Parameters are: severity, probability of exposure, avoidability and degree of exposure, numerical values ranging 1-20 are used instead of qualitative terms.
Quantified Risk Assessment (QRA) [54]	It is a top-down approach that answers three questions: (1) what can go wrong, (2) how likely is it, and (3) what are the consequences.	Risk is expressed as annual frequency of death of individuals, can be subjective and prone to mistakes. The use of small numbers to express risk make believe of high precision whereas there can be considerable uncertainty in the data used to calculate the risk.
Preliminary Hazard Analysis (PHA) [55]	It is primarily an analysis of hazard detection and the most important examination of the state of safety of the system.	Best conducted early in design process, traditionally used to identify hazards although often extended to assess risks and reduce them.
Event Tree Analysis (ETA) [56]	ETA starts with an event such as malfunctioning of a system, process, or construction. The predictable accidental results, sequentially propagated from initiating event, are presented graphically.	Representing system safety based on the safeties of sub-events, consists of an initiating event, probable subsequent events and final results caused by the sequence of events.

Fault tree analysis (FTA) [55]	A top down symbolic logic technique that models failure pathways within the system, tracing them from a predetermined, undesirable condition or event to the failure or fault that may induce it.	Best applies to cases with: large perceived threats of loss, complex or multi-element systems or processes, already-identified undesirable events and indiscernible mishap causes. Depicts functions that lead undesired outcomes, provides both qualitative and quantitative analysis, provides insight into the system behaviour.
Cause Consequence Analysis (CCA) [57]	It is a blend of fault tree and event tree analysis that combines cause analysis (from fault trees) and consequence analysis (from event trees).	Identifies chains of events causing undesirable consequences.
Management Oversight Risk Tree (MORT) [58]	A comprehensive analytical procedure that provides a disciplined method for determining systematic causes and contributing factors of accidents in an existing system.	Similar to fault tree analysis, used as a non-quantitative safety tool.
Failure Mode and Effects Analysis (FMEA) [55]	Identifies potential failure modes that could lead to incidents. It breaks down designs into components and subcomponents, and systematically evaluates the potential for and effects of individual failures by focusing on how they can lead to hazards or negative consequences.	Most familiar for design engineers, widely used in automotive and medical devices industries to evaluate system failure, well suited to situations where engineers are unsure what problems might occur or how small problems could lead to larger ones, useful in determining which of several potential problems should receive priority attention.
Failure Mode, Effects and Criticality Analysis (FMECA) [59]	An analysis method wherein criticality analysis for a quantitative assessment is performed taking the effect of the failure mode on the system as the failure grade in addition to the FMEA.	The two methods to analyse critically are quantitative analysis and qualitative analysis.
Structured What-If Technique (SWIFT) [55]	A structured approach to identify potential hazards and evaluating their consequences.	Considers deviations from the design, construction, modification, or operating intent of a process or facility.
Hazardous operations (HAZOP) [55]	A formal procedure to identify how a process might fail and how such failures can be avoided. Conducted at the end of the design process.	Not strong or necessarily effective in prioritizing effects of the failures, does not study the relative effectiveness of proposed corrective actions.

4 CONCLUSION

Methods of analysing risks as well as the models for solving facility layout problems can take many forms. Some of the most frequently used tools were exposed in this paper. Each method offers a different perspective and with its differing strengths and weaknesses. While, a new trend in designing plant layouts consists of extending the layout formulations with safety issues, the cited models for solving the layout problems do not directly include safety issues. Though, with the mixed integer linear programming models that have been proposed to reduce financial costs, e.g. [60-63], modelling safety issues unavoidably end up in these models. Moreover, artificial intelligent techniques (particularly genetic algorithm and expert system) have been proposed which consider both quantitative and qualitative factors, including safety and ergonomics; e.g. [64-66].

Further research would aim to propose a methodology by which facility planning models and risk analysis tools can be integrated together in order to better meet the safety requirements of companies. In this concern, a facility layout problem can be formulated as a mathematical model while considering OH&S issues as the constraints of the model. The OH&S issues can be taken out from the quantitative and qualitative parameter of one or more of the risk assessment methods. The developed mathematical model will thereafter be solved through using an analytical solution method. By this means, safety issues would be considered as an important factor as cost, closeness, material flow, flexibility, or material handling system concerns, in the facility layout problems.

The research can be expanded by an actual study of considering OH&S issues while planning the layout of an industrial facility. The practical tools that are already used by these facility planners as well as the safety factors that they consider would support the aforementioned developed model. Furthermore, collaborations with industrial partners will permit improving their actual methods in two ways; by include safety aspects in facilities planning methods as well as considering machines positioning in security evaluations. The long term objective is to improve the health and safety of the workforces, while recuperating the efficiency of the industrial facility.

5 REFERENCES

1. Chinniah, Y., et al., *Experimental Analysis of Tools Used for Estimating Risk Associated with Industrial Machines*, 2011, IRSST: Montreal.
2. Foulds, L.R., *LayoutManager: A Microcomputer-Based Decision Support System for Facilities Layout*. Decision Support Systems, 1997. **20**(3): p. 199-213.
3. Singh, S.P. and R.R.K. Sharma, *A Review of Different Approaches to the Facility Layout Problems*. International Journal of Advanced Manufacturing Technology, 2006. **30**(5): p. 425-433.
4. Whitehead, B. and M.Z. Eldars, *The Planning of Single-Storey Layouts*. Building Science, 1965. **1**(2): p. 127-139.
5. Karray, F., et al., *Tools of Soft Computing as Applied to the Problem of Facilities Layout planning*. IEEE Transactions on Fuzzy Systems, 2000. **8**(4): p. 367-379.
6. Francis, R.L., J.A. White, and L.F. MacGinnis, *Facility Layout and Location: An Analytical Approach*. Vol. 31. 1974: Prentice-Hall Englewood Cliffs, New Jersey.
7. Shouman, M.A., et al. *Facility Layout Problem (FLP) and Intelligent Techniques: A Survey*. in *Proceedings of 7th International Conference on Production Engineering, Design and Control*. 2001. Alexandria, Egypt.
8. Malakooti, B. and A. Tsurushima, *An Expert System Using Priorities for Solving Multiple-Criteria Facility Layout Problems*. International Journal of Production Research, 1989. **27**(5): p. 793-808.
9. Meller, R.D. and K.Y. Gau, *The Facility Layout Problem: Recent and Emerging Trends and Perspectives*. Journal of Manufacturing Systems, 1996. **15**(5): p. 351-366.
10. Hillier, F.S. and M.M. Connors, *Quadratic Assignment Problem Algorithms and the Location of Indivisible Facilities*. Management Science, 1966. **13**: p. 42-57.
11. Apple, J.M. and M.P. Deisenroth. *A Computerized Plant Layout Analysis and Evaluation Technique (PLANET)*. in *Annual AIIE conference*. 1972. Norcross, Georgia: J.A. Tompkins and J.M. Moor (ed.), American Institute of Industrial Engineers Inc.
12. Block, T.E., *FATE: A New Construction Algorithm for Facilities Layout*. Journal of Engineering Production, 1978. **2**: p. 111-120.
13. Edwards, H.K., B.E. Gillett, and M.E. Hale, *Modular Allocation Technique (MAT)*. Management Science, 1970. **17**(3): p. 161-169.
14. Hales, H.L., *Computer-aided facilities planning*. Vol. 9. 1984, New York: Marcel Dekker Inc.
15. Hassan, M.M.D., L. Gary, and R.S. Donal, *SHAPE: a Construction Algorithm for Area Placement Evaluation*. International Journal of Production Research, 1986. **24**(5): p. 1283-1295.
16. Heragu, S. and A. Kusiak, *A construction algorithm for the facility layout problem*, in *Working paper #14/861986*, Department of Mechanical and Industrial Engineering, University of Manitoba: Winnipeg, Manitoba, Canada.
17. Lee, R.C. and J.M. Moore, *CORELAP: Computerized Relationship Layout Planning*. Journal of Industrial Engineering, 1967. **18**(3): p. 195-200.
18. Ketcham, R.L. and E.M. Malstrom. *Computer Assisted Facilities Layout Algorithm Using Graphics*. in *Industrial Engineering Conference, Integrating People and Technology*. 1984. Atlanta, GA, USA.
19. Muther, R. and K. McPherson, *Four Approaches to Computerized Layout Planning*. Industrial Engineering, 1970. **21**: p. 39-42.
20. Neghabat, F., *An Efficient Equipment-Layout Algorithm*. Operations Research, 1974. **22**: p. 622-628.
21. Nugent, C.E., T.E. Vollmann, and J. Ruml, *An Experimental Comparison of Techniques for the Assignment of Facilities to Locations*. Operations Research, 1968. **16**: p. 150-173.
22. O'brien, C. and S.E.Z.A. Barr, *An Interactive Approach to Computer Aided Facility Layout*. International Journal of Production Research, 1980. **18**(2): p. 201-211.
23. Zoller, K. and K. Adendorff, *Layout Planning by Computer Simulation*. AIIE Transactions, 1972. **4**(2): p. 116-125.
24. Buffa, E.S., G.C. Armour, and T.E. Vollmann, *Allocating Facilities with CRAFT1964*: Harvard University.
25. Hitchings, G.G. and M. Cottam, *An Efficient Heuristic Procedure for Solving the Layout Design Problem*. Omega, 1976. **4**(2): p. 205-214.
26. Khalil, T.M., *Facilities Relative Allocation Technique (FRAT)*. International Journal of Production Research, 1973. **11**(2): p. 183-194.
27. Picone, C.J. and W.E. Wilhelm, *A Perturbation Scheme to Improve Hillier's Solution to the Facilities Layout Problem*. Management Science, 1984. **30**(10): p. 1238-1249.
28. Shore, R.H. and J. Tompkins, *Flexible Facilities Design*. AIIE Transactions, 1980. **12**(2): p. 200-205.
29. James, A.T. and R. Ruddell Jr, *An Applied Model for the Facilities Design Problem*. International Journal of Production Research, 1976. **14**(5): p. 583-595.
30. Tompkins, J.A. and R. Reed Jr, *Computerized Facilities Design*. Technical Papers, 1973: p. 75-87.
31. Vollmann, T.E. and E.S. Buffa, *The Facilities Layout Problem in Perspective*. Management Science, 1966. **12**(10): p. 450-468.
32. Chamoni, P., *MICROLAY: An Interactive Computer Program for Factory Layout Planning on Microcomputers*. European Journal of Operational Research, 1987. **31**(2): p. 185-193.
33. Drezner, Z., *DISCON: A New Method for the Layout Problem*. Operations Research, 1980. **25**(6): p. 1375-1384.

34. Kaku, B.K., G.L. Thompson, and T.E. Morton, *A Hybrid Heuristic for the Facilities Layout Problem*. Computers & Operations Research, 1991. **18**(3): p. 241-253.
35. Scriabin, M. and R.C. Vergin, *A Cluster-Analytic Approach to Facility Layout*. Management Science, 1985. **31**(1): p. 33-49.
36. Eades, P., L. Foulds, and J. Giffin, *An Efficient Heuristic for Identifying a Maximum Weight Planar Subgraph*, in *Combinatorial Mathematics IX*1982, Springer: Berlin. p. 239-251.
37. Foulds, L.R. and D.F. Robinson, *Graph Theoretic Heuristics for the Plant Layout Problem*. International Journal of Production Research, 1978. **16**(1): p. 27-37.
38. Fisher, E.L. and S.Y. Nof. *FADES: Knowledge-Based Facility Design*. in *Proceedings of International Industrial Engineering Conference*. 1984. Chicago.
39. Kumara, S.R.T., R. Kashyap, and C.L. MOODIE, *Application of Expert Systems and Pattern Recognition Methodologies to Facilities Layout Planning*. International Journal of Production Research, 1988. **26**(5): p. 905-930.
40. Sunderesh, S.H. and A. Kusiak, *Machine Layout: An Optimization and Knowledge-Based Approach*. The International Journal of Production Research, 1990. **28**(4): p. 615-635.
41. Tsuchiya, K., S. Bharitkar, and Y. Takefuji, *A Neural Network Approach to Facility Layout Problems*. European Journal of Operational Research, 1996. **89**(3): p. 556-563.
42. Hamamoto, S., *Development and Validation of Genetic Algorithm-Based Facility Layout: A Case Study in the Pharmaceutical Industry*. International Journal of Production Research 1999. **37**(4): p. 749-768.
43. Kochhar, J.S., B.T. Foster, and S.S. Heragu, *HOPE: A Genetic Algorithm for the Unequal Area Facility Layout Problem*. Computers & Operations Research, 1998. **25**(7-8): p. 583-594.
44. Kochhar, J.S., *MULTI- HOPE : A Tool for Multiple Floor Layout Problems*. International Journal of Production Research 1998. **36**(12): p. 3421-3435.
45. Dweiri, F. and F. Meier, *Application of Fuzzy Decision-Making in Facilities Layout Planning*. International Journal of Production Research, 1996. **34**(11): p. 3207-3225.
46. Raoot, A.D. and A. Rakshit, *A 'Linguistic Pattern' Approach for Multiple Criteria Facility Layout Problems*. International Journal of Production Research 1993. **31**(1): p. 203-222.
47. Adedeji, B.B. and A. Arif, *FLEXPERT: Facility Layout Expert System Using Fuzzy Linguistic Relationship Codes*. IIE Transactions, 1996. **28**(4): p. 295-308.
48. Chung, Y.K., *Application of a Cascade BAM Neural Expert System to Conceptual Design for Facility Layout*. Computers & Mathematics with Applications, 1999. **37**(1): p. 95-110.
49. Paques, J.J., F. Gauthier, and A. Perez, *Analysis and Classification of the Tools for Assessing the Risks Associated with Industrial Machines*. International Journal of Occupational Safety and Ergonomics, 2007. **13**(2): p. 173-187.
50. Main, B.W., *Risk Assessment in the Real World*2004, Ann Arbor, Michigan: Design Safety Engineering Inc. .
51. Garvey, P.F. and Z.F. Lansdowne, *Risk Matrix: An Approach for Identifying, Assessing, and Ranking Program Risks*. Air Force Journal of Logistics, 2002. **22**(1): p. 18-21.
52. Baybutt, P., *An Improved Risk Graph Approach for Determination of Safety Integrity Levels (SILs)*. Process Safety Progress, 2007. **26**(1): p. 66-76.
53. Etherton, J.R., *Industrial Machine Systems Risk Assessment: A Critical Review of Concepts and Methods*. Risk Analysis, 2007. **27**(1): p. 71-82.
54. Apostolakis, G.E., *How Useful is Quantitative Risk Assessment?* Risk Analysis, 2004. **24**(3): p. 515-520.
55. Main, B.W., *Risk Assessment*. Professional Safety, 2004. **49**(12): p. 37-47.
56. Hong, E.S., et al., *Quantitative Risk Evaluation Based on Event Tree Analysis Technique: Application to the Design of Shield TBM*. Tunnelling and Underground Space Technology, 2009. **24**(3): p. 269-277.
57. Keong, T.H. *Risk Analysis Methodologies*. 1997 [cited 2012 17 April].
58. Anderson, W.E., *Risk Analysis Methodology Applied to Industrial Machine Development*. Industry Applications, IEEE Transactions on, 2005. **41**(1): p. 180-187.
59. Kyokai, N.K., *Risk Assessment Guideline: Estimation and Assessment of Risks Leading to Identify Hazards*, 2009, ClassNK.
60. Penteado, F.D. and A.R. Ciric, *An MINLP Approach for Safe Process Plant Layout*. Industrial & Engineering Chemistry Research, 1996. **35**(4): p. 1354-1361.
61. Papageorgiou, L.G. and G.E. Rotstein, *Continuous-Domain Mathematical Models for Optimal Process Plant Layout*. Industrial & Engineering Chemistry Research, 1998. **37**(9): p. 3631-3639.
62. Patsiatzis, D.I. and L.G. Papageorgiou, *Optimal Multi-Floor Process Plant Layout*. Computers & Chemical Engineering, 2002. **26**(4-5): p. 575-583.
63. Patsiatzis, D., G. Knight, and L. Papageorgiou, *An MILP Approach to Safe Process Plant Layout*. Chemical Engineering Research and Design, 2004. **82**(5): p. 579-586.
64. Pham, D.T. and H.H. Onder. *An Expert System for Ergonomic Workplace Design Using a Genetic Algorithm*. in *Applications of Artificial Intelligence in Engineering*. 1991. Oxford, UK.
65. Carnahan, B.J. and M.S. Redfern, *Application of Genetic Algorithms to the Design of Lifting Tasks*. International Journal of Industrial Ergonomics, 1998. **21**(2): p. 145-158.
66. Pham, D.T. and H.H. Onder, *Knowledge-Based System for Optimizing Workplace Layouts Using a Genetic Algorithm*. Ergonomics, 1992. **35**(12): p. 1479-1487.

System Safety Analysis of an Industrial Process Using Fuzzy Methodology

Tony Venditti, Nguyen Duy Phuong Tran, Anh Dung Ngô
École de Technologie Supérieure
1100, rue Notre-Dame Ouest
Montréal, Québec, Canada H3C 1K3

Key words : Risk, fuzzy fault trees, optimization

Abstract

In this paper, a research is presented which proposes a design-for-safety methodology based on risk analysis. The analysis includes two types of calculations. First, calculation of probabilities of occurrence of machine failures and worker accidents. Second, minimization of cost of safety improvements so as to reach a given safety target (an accident or failure rate) including the savings, in time, resulting from less accidents occurring. However, such an analysis presents problems. In particular, data on failure and accident rates are sparse and uncertain. In particular, human factors which may lead to accidents are difficult to quantify properly. Also, accident scenarios may depend not only on the occurrence of contributing factors, but on their sequence of appearance in time. To address this time dependency issue, the proposed methodology uses fuzzy fault trees and Markov diagrams. Human reliability data will be gathered experimentally for a given industrial work situation. The problem of minimizing the cost of required safety (with due account taken of savings resulting from improved safety) is modeled as a mathematical optimization equation under constraints. Fuzzy probability of occurrence of accidents and optimized cost functions will be evaluated. Finally, an experimental validation of the analysis model will be undertaken.

1. Introduction

The operation of industrial machines involves various risks, particularly for the operators. In order to analyze these risks and better protect the operators, a methodology is needed. As well, for employers, safety regulations and internal standards must be respected. It would be desirable to be able to reach these targets at minimal cost.

Firstly, in order to analyze risks, many methods have been developed, among them fault tree analysis. Fault tree analysis attempts to identify the various events that lead to an accident. The probability of occurrence of such an accident can then also be evaluated. This probability depends on the probability of occurrence of the contributing events. But often, uncertainty surrounds these data. To deal with this problem, probabilities can be expressed, not as crisp values, but, rather, as fuzzy numbers which reflect a range of values. In addition, accidents often occur if certain factors occur in a certain order. For instance, if a safety device on a given industrial machine fails before the entry of a worker in the danger zone, an accident can then occur. But, if the device failure occurs after the entry, the accident may not happen. To handle this time dependency, dynamic fault trees and Markov chains can be used. From these concepts, the required probabilities can then be determined.

Secondly, failure and accident rates can unfortunately never be zero but can be set to very low levels often by regulations and standards. As just seen, accidents and failures are the results of contributing factors. An interesting question is then, what optimal combination of contributing factors occurrence probabilities lead to the prescribed safe probability of system failure or accident so as to minimize the cost of safety measures. The employer can then assign resources on the relevant factors in the best possible way.

Moreover, probabilities related to human factors present additional challenges. In particular, data on human errors occurring during the operation of many industrial systems are difficult to find. To remedy this situation, it is proposed to experimentally simulate the work situation under study and observe human error rates.

2. Concepts used for risk analysis and estimation

2.1 Fuzzy numbers

In risk analysis we often do not know the precise values of the probabilities of occurrence or of failure of the systems or of its components. So one way to deal with this problem is to consider that the variables of interest follow a normal probability distribution with a mean value and a standard deviation. However, another approach to the problem is to use fuzzy triangular number.

A fuzzy number is represented by three numbers $\langle a_1, a_2, a_3 \rangle$. This representation is interpreted as a membership function such as illustrated in Figure 1:

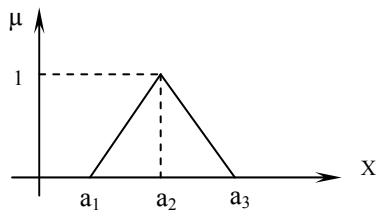


Fig.1 A fuzzy triangular number

In this representation, a_2 corresponds to a membership value of 1 meaning that we think that the most probable value of the variable under consideration is a_2 . a_1 and a_3 are the lower and upper bounds, respectively, of the distribution.

In order to perform calculations on fuzzy fault trees, arithmetic operations on fuzzy numbers have to be introduced.

2.1.2 Fuzzy operations

The four basic arithmetical operations that can be performed on fuzzy triangular numbers

However, a problem with triangular fuzzy numbers is that addition and subtraction as well as multiplication and division are not reciprocal operations [1,2]. To overcome this difficulty, subtraction and division operations definitions have to be modified.

2.2 Fault tree analysis (FTA)

2.2.1 Static fault tree analysis

Fault tree analysis attempts to identify the various events that lead to an accident , [3]. The probability of occurrence of such an accident can then also be evaluated using fault tree analysis. A simple example of fault tree is shown in Figure 2.

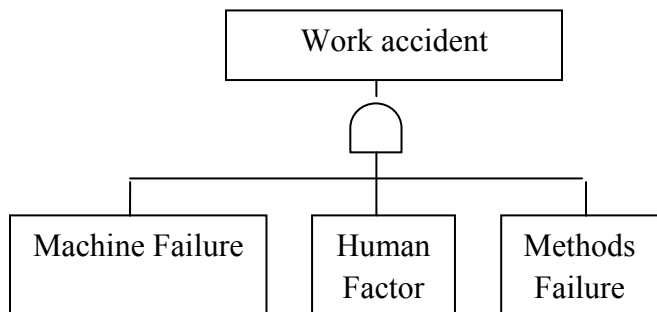


Fig.2 A simplified fault tree

Fuzzy FTA works on the same principle but the assessment of the effects is done in terms of fuzzy numbers as to account for the uncertainty of the available data, [4].

2.2.2 Dynamic fault tree analysis

These methods take a static view of the system; that is, the sequence of events leading to the undesirable event which can depend on one another is taken into account. To remedy this deficiency, the dynamic fault tree method has been developed. In this

method, dynamic gates are introduced which capture the dynamic features of the system. For instance, instead of using static AND gates as in a traditional static fault tree, a dynamic fault tree uses a PAND gate whose output changes to a failure state only if all of its inputs have failed in a predetermined order.

2.3 Markov Analysis

From a dynamic fault tree, a so-called Markov diagram can be drawn. This enables one to write a first-order differential state equation which can then be solved.

Markov analysis is a technique used for modelling system state transitions and calculating the probability of reaching various system states from the model, [4].

The analysis takes the form of a diagram where the nodes represent states of the systems and the arcs, transitions, such as seen in Figure 3. In this example, component 1 fails before component 2. The opposite transition, component 2 failing before 1 is not allowed.

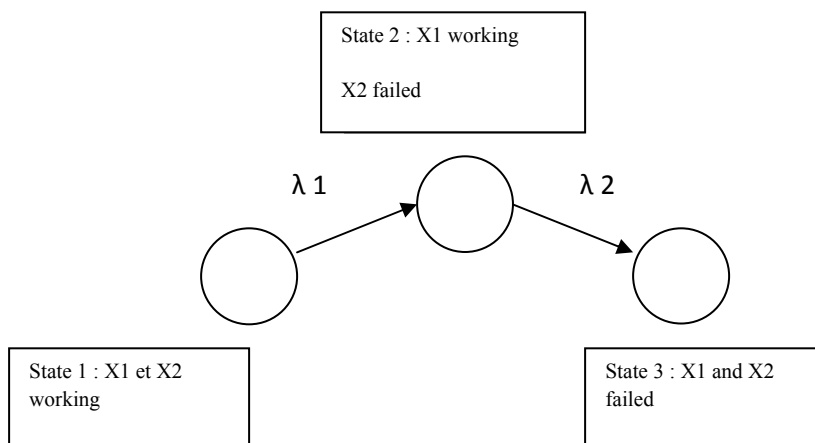


Fig.3 A simplified Markov Diagram

2.4 Fuzzy optimization of a safety cost function

The problem of minimizing a safety cost function, given that work accidents (the top event in a fault tree) must respect a maximum acceptable rate set by regulation can be solved using the Lagrange multipliers method which can be expressed as,[2]:

$$\begin{cases} \nabla f(\mu_X) + \sum_{i=1}^P \lambda_i \nabla h_i(\mu_X) = 0 \\ \lambda_i h_i(\mu_X) = 0 \\ h_i(\mu_X) < 0 \\ \lambda_i \geq 0 \end{cases}$$

where f is the cost function which depends on the (fuzzy) contributing events probabilities, μ_X , h_i are the constraints (written from the fault tree) and the λ_i are Lagrange multipliers, all of which are also fuzzy numbers.

3. Methodology

This research is comprised of the following parts:

3.1 Industrial machine system with no time dependency

3.1.1 The fuzzy probability of occurrence of a worker accident will be calculated from the corresponding fuzzy fault tree.

3.1.2 The cost function fuzzy optimization will be solved.

3.2 Industrial machine system with no time dependency

3.2.1 The equations of state will be written from the dynamic fault tree and Markov diagram of the system. These equations will yield the probability of occurrence of the work accident event under consideration

3.2.2 The cost function fuzzy optimization will be solved.

3.3 Experimental study

To validate this mathematical modeling, an experimental setup will be designed consisting of a simple machine with components having approximately known failure rates. Simple tasks simulating the operation of the machine will be performed by subjects. A sensor will detect entry by the subject into a defined danger zone. This will allow calculation of the human error rate associated with the operation of the machine. The results will be compared against the calculations of the model.

4. Conclusion

In this paper we presented a research aiming at developing a methodology for risk analysis of an industrial systems based on fuzzy numbers. Two types of systems were considered: static, time-independent and dynamic, time-dependent. The analysis comprises two types of calculations: Fuzzy accident probability occurrence and fuzzy cost function optimization. An experimental validation of the analysis method was described.

5. References

- [1] Gani, A.N. (2012), *A new operation on triangular fuzzy number for solving fuzzy linear programming problem*, Applied Mathematical Sciences, vol. 6. No.11 pp. 525-532.
- [2] Rogers, F., Younbae, J. (2009), *Fuzzy nonlinear optimization for the linear fuzzy real number system*. International Mathematical Forum, vol. 4 No.12 pp. 587-596.
- [3] Rajiv Kumar Sharma, Pooja Sharma (2010), *System failure behavior and maintenance decision making using, RCA, FMEA and FM*, Journal of Quality in Maintenance Engineering, vol. 16 (1) pp.64-88.
- [4] Rong Wu, Xin, Deng (2010), *Application of fuzzy fault tree analysis on burning and blasting of LPG tank*, Logistics Systems and Intelligent Management, vol. 2 pp. 1093-1096.

SIAS
2012

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



SESSION 2

SAFETY OF MACHINERY; ERGONOMIC, HUMAN FACTORS AND CONCEPTION

The contribution of standards to risk control in machinery design: the role of ergonomics

Elie Fadier

Institut National de recherche et de Sécurité
Département Expertise et Conseil Technique
Approche Globale des Situations de Travail
Tel : 03 83 50 2193
fadier@inrs.fr

Jean Louis Pomian

Institut National de recherche et de Sécurité
Département Expertise et Conseil Technique
Approche Globale des Situations de Travail
Tel : 01 40 44 30 23
pomian@inrs.fr

Abstract:

The evolution of European legislation on occupational risk prevention emphasises the obligation of results in terms of the prevention of occupational accidents and diseases. A real opportunity exists for ergonomics, one which has not yet really been seized, to develop normative reference documents describing the methodologies to be applied to achieve this end. Reference to ergonomics is certainly made in Annex 1.1.6. of Machinery Directive 2006/42/EC and in many technical standards termed “harmonised”, but only in a secondary and simplistic way, notably without providing users with the methods, means and tools to ensure efficient application and use of the principles on which they are founded. It will be on this basis that we shall firstly cover some reference points concerning the activity of designers before moving on to the possibility of changing the paradigm concerning the integration of OSH into the process of designing work equipment. Lastly, we shall present the structure of a method based on the analysis of real work. Three examples of applications will be briefly presented and discussed.

In conclusion, this presentation highlights that an ergonomic approach centred on the analysis of work activities allows the construction of an effective designer-ergonomist dialogue.

Key words: ergonomic approach, work activity, machinery design, Machinery Directive, harmonised standards, EN ISO 12100, EN 614-1

Introduction

The law of 31 December 1991 relative to occupational risk prevention places the emphasis on an obligation of results in terms of preventing occupational accidents and diseases. A genuine opportunity exists for ergonomics to draw up normative reference documents describing the methodologies to be applied to achieve this aim. Reference to ergonomics has certainly been made in Annex 1.1.6. of Machinery Directive 2006/42/EC and in many technical standards termed “harmonised”, but only in a secondary and simplistic way, without providing the users with methods, means and tools allowing them effective application and use of the principles underpinning it. While many facets of risk control have been explored in the normative technical documentation, it has become clear that there is an absence of interdisciplinary vision and effective communication between engineering and ergonomics. While it is well accepted that interdisciplinarity has not become compulsory and that it will take time for it to penetrate into culture and practices, the change is not going to come about on its own and kickstarting “the miracle” must come from ergonomists themselves. Nevertheless, the situation needs to be analysed – in coherence with our practices – to allow for a better understanding of the point of view of the activity of designers and the reasons for insufficient integration of Occupational Safety and Health (OSH) in the design process, in particular in the process of designing work equipment, namely machinery. It will be on this basis that we shall firstly cover a number of reference points concerning the activity of designers before going on to look at the possibility of changing the paradigm regarding the integration of OSH into the work equipment design process. Lastly, the structure of a method founded on the analysis of “real work” will be presented. Three examples of applying this method are briefly presented and discussed.

1. Reference points concerning the activity of designers and the integration of OSH

1.1. The construction of technological certainty

Current knowledge of the activities of designers and of the activity of designing work equipment allows us to establish a knowledge base capable of opening up ways forward to improve risk control (Rumelhart et al., 1978, Falzon, 1994 and 2008; Vicente, 1999; Fadier et al. 2003a; Fadier et al., 2006; Nachreiner, 2007).

Generally, the process of design is primarily founded on essentially technical requirements based, in the majority of cases, on the presumed efficiency of the technical choices (Fadier, E., De la Garza, C. & Didelot, A., 2003a). Technological certainty sought through the reliability and stability of the process, notably, is founded on the conviction that all the work and the operating modes of an industrial system are predictable and that, as a result, appropriate technical solutions exist that can be employed without too many risks.

In contrast, studies have highlighted a series of inadequacies in terms of design (Falzon, 1994; De la Garza, 2005) consisting in: considering the design as the resolution of well defined problems; proposing a conceptually logical but restrictive solution regarding the real needs of workers; reasoning primarily on the basis of a nominal operation; not taking into consideration knowledge of the operational needs of operators in real situations by proposing solutions termed innovatory (from the “blank state” theory); limiting the assessment to normative data alone.

To these generalisations, which are not a comprehensive list, have been added even more precise observations that appear just as problematic (Vicente, 1999; Falzon, 2008): Each designer has a different representation of the need; A frequent reasoning in terms of design results in simultaneously examining the problem and its solution, the variety of future utilisation conditions and more generally the real uses that could be made of the machine to be designed not being taken into account; The regulatory or normative constraints to be integrated resulting generally in a reduction in the scope for creation and encouraging recourse to old solutions; The participation of the personnel concerned by the design project is, rather than being recognised as legitimate and rich, more often than not undervalued and even shunned.

The presumed efficiency of the technical solutions underpinning the said technological certainty is in opposition to a series of observations made in the wake of an industrial system in real operation showing that the operators, exposed to new risks on account of system operation conditions more often than not less than optimal, must endlessly anticipate, adapt and regulate. Worthy of note is that the difference between the expected operation and the real operation (integrating vagaries) is one of the most important sources of "risk taking", as for the operator/user it means dealing with a situation not planned for during the design phase.

Thus, a design based on technical know-how alone can only constitute a partial response to the requirements of the real work.

1.2. OSH requirement

The OSH requirement stems from a regulatory requirement to be taken into account when drawing up technical specifications for the design of an item of work equipment and when drawing up technical specifications. There is a great deal of room for manoeuvre in its application that depends on many factors, in particular the involvement of the designer and the standards taken as reference.

1.2.1. The regulatory reference system

The regulatory reference system stems primarily from European directives, notably Health and Safety Directive 89/391/EC and Machinery Directive 2006/42/EC. Directive 89/391/EC requires coupling the risk analysis with the work analysis without setting out a methodology for analysing the work. In addition, Machinery Directive 2006/42/EC, its application guide, Standards EN ISO 12100 and EN 614-1 mention taking ergonomic principles into account when designing machines and emphasise the need to base the “design” on knowledge of the work and the requirements of the tasks and work activities. On the whole, these references do not set out sufficiently precise and comprehensive “guidelines” allowing designers to implement the ergonomic approach, and from this, comprehend the interest and advantages.

1.2.2. Taking OSH into account in technical specifications

The design process is a complex activity which sets out from and is founded on an initial requirement expressed to the designer in a technical specification (Hatchuel et al. 1992, Falzon, 1995).

During a design process, the safety and health requirement depends on the quality (form, legibility, relevance, etc.) of the data laid down in the technical specification.

Translating the compulsory character of the requirement can be done, (De la Garza, 2005), either on the basis of knowledge stemming from the experience of the designer (the “indirect route”) or by way of the standards (the “direct route”).

It has also been observed that the regulatory OSH requirement:

- is often input by an expert who is not always considered as a design participant.

- is in opposition to production (it “stops the system”).
- is sometimes considered as a constraint both by the designer and the user:

It should be noted that when there are less requirements in the technical specification, there is a greater risk of their being ignored in the development of the solution (Lebahar, 1993). OSH is, in the best case scenario, considered as a “weak” and even inexistent requirement in technical specifications. Recourse to standards is then often the sole means at the disposal of the designer to “make the best of it”. The standards termed “harmonised” with the Machinery Directive indeed make reference to ergonomics and, a priori, could offer an assurance of the possibility of OSH integration. However, it is not the real activity that these standards consider, but the task to be executed.

1.2.3. The reduction made by the “machine safety” standards

In keeping with certain standards, such as the ISO 13407 standard for interactive systems, work equipment designers are encouraged to integrate health and safety criteria at the needs expression phase. The tools proposed to achieve this are not, however, adapted to the methodological requirements demanded.

An example is given with the NF EN 12100 standard, harmonised with Machinery Directive 2006/42/EC. It proposes an a priori risk reduction methodology which covers the essentials but does not guarantee any result concerning operator health and safety. In particular, a set of good practices likely to be integrated into the design of equipment is proposed, but without giving the means of verifying coherence. Moreover, we note that: 1) One of the major occupational risk prevention principles, namely adapting work to people, is not investigated. 2) The concept of “reasonably foreseeable misuse” is highlighted in the standard. This concept should be treated with caution. 3) Lastly, when putting the standard into practice, prevention specialists do not have the relevant criteria at their disposal allowing them to know when to conclude their risk appraisal should they wish to go beyond “normal operation” alone. They can reduce the need to go further or vice versa pursue the iterations beyond that which is necessary.

1.2.4. Ergonomic standards: a techno-task centred vision

Generally, the ergonomic model in the existing standards is part of the ergonomics of the task. Every task and all the work are considered as predictable. In this sense, the activity is contained in the task in such a way that the extent of the activity is limited to the scope of the predicted task. Thus, any reasonably predictable deviation of the activity from the predicted task is considered as a “reasonably foreseeable misuse”.

However, observation of day-to-day work shows a significant difference between the work stipulated (task) and the work carried out (activity), which encourages examining the meaning and the content of the real work in order to identify, if it does differ, how it can be divergent from the work stipulated. What are the effects on the system (namely, does it benefit the performance of the system or not)? Will it be a new resource? And if the answer is positive we find ourselves in an area of activity not encompassed in the task stipulated.

Moreover, the work of Rasmussen (1997) has underlined that every system undergoes transformations, adaptations and drifts from its design until it is first used. It is therefore important to identify these evolutions and their impacts on the performance of the system designed (productivity, health and safety). Moreover, Fadier et al. (2003b) added an additional dimension, the life cycle of the installation, by putting forward the hypothesis that these limits, defined (partly) in a certain manner at the design stage, will drift (vary, evolve) as soon as the shift from design to installation is made, then from installation to use, under the influence of various factors.

Not taking this vision into account (migration and drift from solutions) leads designers to consider each deviation from the recommended model as an error, whereas this divergence is often necessary.

The observation is thus made that the logic of designing work equipment can be founded on data which, like normative data, gives the assurance of objectivity whereas in fact they dissuade from going further in taking into account the real needs of operators/users. While the data stemming from standards, prior measurements, and even immediate experience feedback are objective, the conceptual decisions relying on them are necessarily subjective. Subsequently, by reducing the area of possible solutions that might open up the possibility of a little more wellbeing and safety at work, the logic of design is deprived of part of the efficiency that ought to have been given to it by taking into account the wealth of know-how built up over the long term by each operator.

2. A paradigm change or reorganisation?

The brief review of the preceding questions situates the standards as a resource used for risk prevention in design. However, this resource appears insufficient to ensure risk control. As a result, it would seem to be important to examine the existing possibilities of enhancing efficiency to be in a better position to enrich the design process itself.

Giving greater consideration to the fundamentals of the ergonomic approach would, on this basis, lead to the proposal to make the NF EN 12100 and EN 614 standards more coherent.

2.1. A functional logic enriched by the logic of use

The prognosis concerning the situation to be designed is established on the basis of a functional design logic which frames the process of drawing up the specifications – themselves termed “functional” – and lead to “technological certainty” (see §1.1.). After having underlined the inadequacies of this approach, it should be considered vital to envisage that there is a real complementarity between the prognosis (P) of the future operation and the diagnosis (D) stemming from a prior analysis of similar existing situations. Only such a diagnosis could allow updating of the logic of use and, therefore, the real needs of the end users. Certain authors have, moreover, proposed bringing these two concepts of prognosis and diagnosis into dynamic interaction (De la Garza and Fadier, 2006) so as to organise experience feedback fed by the different points of view (engineering, ergonomics, prevention, those on the ground, etc.). While enriching “prognosis” by “diagnosis” requires collaboration between designers and end users, it should be noted that the means of mediation (models, scenario construction, prototypes, CAD, etc.) can make this collaboration even more effective. With this in mind, risk control at the design stage lies as much in the ability of the prevention professional (ergonomist) to articulate his or her knowledge and to translate it in the form of proposals adapted to a particular project, as it does in the aptitude of designers to grasp and employ this knowledge. This observation strengthens the need to (Béguin, 2007; 2008): 1) develop experience feedback so that the rich resources stemming from the experience of operators of similar systems are put to good use in orientating the decisions by becoming in this respect a source of the activity of designers. 2) enrich the work of designers so that the result of the design process orients and is a source of the activity of operators. 3) Organise and facilitate dialogue between the activity of designers and the activity of operators during the design process.

2.2. The fundamentals of an ergonomic approach

The analytical approach developed by ergonomics allows the establishment of a diagnosis, notably by demonstrating that there is a gap between the work stipulated and the real work and that this gap must be translated by compensatory measures or by ease of use during the design. This gap, which depends on the context and unforeseen events (production vagaries, operational constraints, process variability, etc.) cannot be determined in advance. To anticipate and better understand the sources of variability, it is crucial to analyse the real activity of the operators working on existing equipment or similar equipment. The aim of this is to extract the main characteristics, to measure and assess the constraints of the activity, and to identify the real needs of these activities in order to better integrate them into the design specifications. The behaviour of a system is necessarily indeterminate, the reason for this being that its components constantly evolve. This applies for example to technical components (wear, malfunctions, evolution of product ranges, changing equipment, etc.), organisation (procedures, workforce, etc.) and people themselves (age, disabilities, apprenticeship, etc.). Ergonomics recognises this and emphasises that it is vital to allow operators the ability to anticipate and to retain their “power to act” (i.e. the legitimate feeling of having the power to act). The importance of the contribution of activity regulations as a possibility in giving the system the ability to function is stressed in particular. The analysis of real activity shows the need for these regulations while allowing an assessment of the risks accompanying their being employed. In particular, it shows that these regulations are justified by the context and that they must not be considered as being “misuse” of the equipment, even though they go against the procedures. The role of ergonomics is not merely to apply measurement and assessment standards, but to develop methods to analyse the real work allowing effective anticipation of the risks linked to using the machine. Even though this is founded at the outset on subjective hypotheses, the ergonomic approach thus objectifies the solutions to be employed for the design of the equipment and facilitates the appropriation process of the personnel concerned.

Thus, logic guided by the timely taking into account of the various work situations likely to be encountered and the real needs of operators allows a better adaptation of work to people that is coherent with general prevention principles. By seeking to reduce risks and protect operator health and safety while strengthening the decisional autonomy of the operators, ergonomics “makes the difference”. It would appear to be genuinely interesting for designers, industrial decision makers and prevention specialists alike to describe in a standard the elements structuring this “difference”. **An ergonomic approach based on analysing work activity is a multi-criterion, iterative and structured approach.**

Figure 1 below shows its structure and especially the important role of personnel in charge of the activity. Indeed, it implies the real participation of operators who primarily have the skills and knowledge linked to the work to be

done. In this approach, the analysis of the initial demand allows a better understanding, positioning and identification of the needs of the enterprise. This step is generally followed by a comprehensive analysis of the situation that enables the ergonomic analyst to set the context and build his or her knowledge on the data and the characteristics of the system. Lastly, the analysis of the work activity (collecting elements, observations, interviews, etc.) allows the formulation of hypotheses concerning the needs, requirements and the difficulties encountered in carrying out the work.

All in all, the aim of an ergonomic approach tool by methods scientifically validated by the profession is:

- to ensure the validity of the solutions proposed at each step of the design process,
- to yield elements concerning the constraints, the requirements and the characteristics of the activities,
- to appraise the coherence of the organisational measures proposed as well as the usefulness and the effectiveness of the protective systems with respect to the requirements of the real work,
- to verify that the solutions proposed guarantee a real adaptation of the work to people.

This being so, “the activity analysis is a powerful mediation tool as it offers the framework necessary for opening a multidisciplinary debate on work tensions and thus sets the players in motion, i.e. in a position to socially develop a thought” (Brahim, 2011).

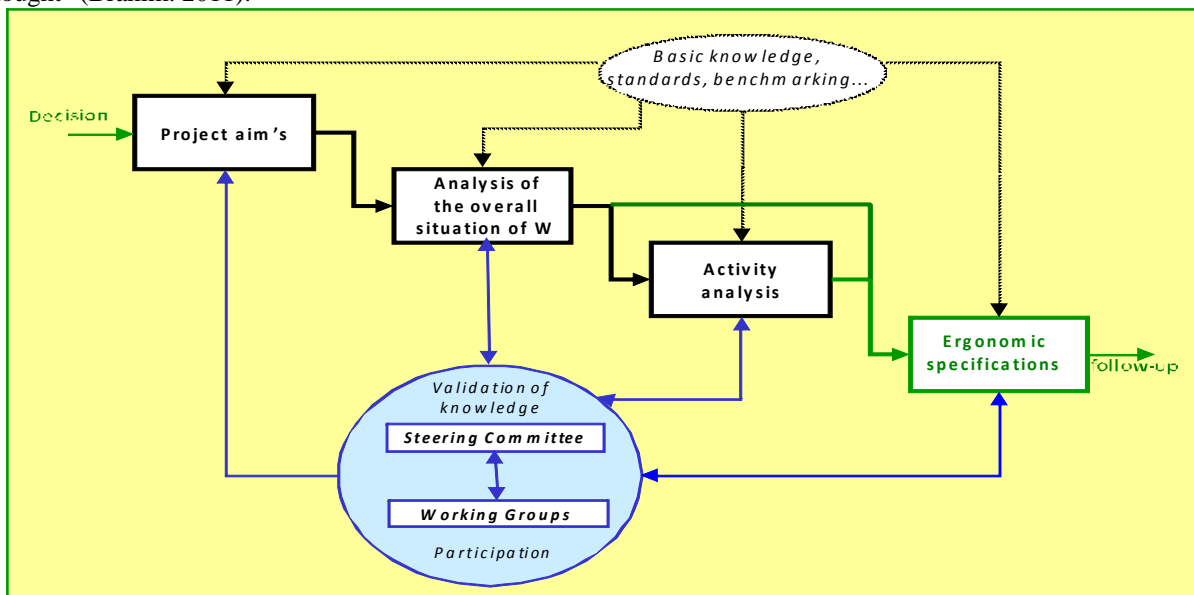


Figure 1: structure of the ergonomic approach

3. Some examples illustrating the contribution of the ergonomic analysis of work activity to design

The design projects presented below refer to three very different types of systems: an offset printing line, an industrial wireless remote control (IWRC) and a control joystick for the arm of a verge mower.

- An offset printing line: complex system comprising a series of machines arranged in a line (between 70 and 90 m long depending on the type and model). The assembly is termed “rotary”. It is intended for printing coloured magazines, catalogues, advertising material, etc. (Fadier et al. 2007)
- A small portable system “the industrial wireless remote control (IWRC)” whose basic structure includes a mobile control desk that transmits the operator’s instructions to a remote control system. Transmission is either by radio or infrared link, each type of wireless link has its unique characteristics and requires a number of precautions concerning use (Fanchini et al. 2008).
- A joystick intended to control the articulated arm system of a verge mower. This part is integrated into a structure (tractor) designed for general farming work.

In all three cases, there is a new design involved whose stated objective is an improvement in performance through better integration of the health and safety of users.

The ergonomic analysis of the activities of operators/users/workers in similar systems provided the designers with data explaining not only the difficulties encountered by operators in using the existing solutions, but also all the resources introduced (in the form of palliative activities) allowing the maintenance of an acceptable efficiency and

satisfaction of the production requirements. These activities, considered as vital resources stemming from operators' expertise and safety know-how, are, in many cases, accompanied by risk taking compromising their safety and health. All the data and the information gleaned from the activity analysis have allowed the designers to propose solutions that take into account the difficulties, reduce risk taking and leave enough room for manoeuvre to the operators for them to contribute to the efficiency of the system. In oral presentation, we describe and comment the main information stemming from these three cases.

Conclusion

In conclusion, it can be emphasised that employing an ergonomic approach centred the analysis of work activities shows the possibility of constructing an efficient designer-ergonomist dialogue. In this respect, this means:

- organising feedback so that the wealth of resources of operator activity developed in similar systems feed into and orient the activity of designers;
- accompanying the work of designers so that the result of the design work focuses on « future possible activity areas » rather than on the design of artefacts;
- facilitating dialogue between designers and operators during the design process, resulting in their having a genuine understanding of both the requirements linked to the activity and the technological constraints.

4. Bibliography

- BEGUIN, P., (2007) - Prendre en compte l'activité de travail pour concevoir. *Activités*, 4 (2), pp. 107-114, <http://www.activites.org/v4n2/v4n2.pdf>
- BEGUIN, P., (2008) – Design et santé : quelques remarques sur le statut de l'activité de travail dans la design des systems de production. *Psychologie du travail et des organisations*, 14, 4, p369-384.
- BRAHIM M-B., « La pluridisciplinarité en SST », journée du 11 février 2011, CNAAM, Paris
- DARSES F., (sous la direction de) (2002). *Activités coopératives de design*. Editorial du numéro spécial, *Le travail Humain*, 2002, tome 65, n° 4, 289-292.
- DE LA GARZA C., (2005). The integration of safety from the design stage of machines posing risks to operators: comparison of the different logics of design. *Pistes*, <http://petnt/pistes/v7n1/articles/v7n1a2.htm>.
- Machinery Directive 2006/42/EC of 17 May 2006
- Health and Safety Directive 89/391/CEE
- EN 614-1, 1995. European standard, safety of machinery, Ergonomic design principles – Part 1: terminology and general principles, European committee for standardisation, Brussels.
- EN ISO12100. Safety of machinery - general principles for design - Risk assessment and risk reduction (12100:2010)
- FADIER E.,(2008) Special Issue on Design process and human factors integration, CTW Volume 10 number 1 2008, Edited by E. Fadier.
- FADIER E., DE LA GARZA C., (2006). Safety design: Towards a new philosophy. *Safety Science*, 44, 2006, 55–73.
- FADIER E., DE LA GARZA C., (2007) - Towards a proactive safety approach in the design process: The case of printing machinery. *Safety Science* 45 (2007) 199–229.
- FADIER E., DE LA GARZA C., DIDELOT A., (2003a). Safe design and human activity: construction of a theoretical framework from an analysis of a printing sector. *Safety Science*, 41(9), November 2003, 759-789.
- FADIER E., NEBOIT M., CICCOTELLI J., (2003b) Intégration des conditions d'usage dans la design des systems de travail pour la prevention des risks professionnels. Bilan de la thématique 1998 –2002. Note Scientifique et Technique, NS 237, INRS, p.39
- FALZON, P., (1994) Les activités méta-fonctionnelles et leur assistance. *Le Travail Humain*, 57 (1), 1-23.
- FALZON, P., (2008) Enabling safety: issues in design and continuous design. In *Cogn Tech Work Special issue on “Design process and human factors integration”*; Guest Editor Elie Fadier. (2008) 10:7–14.
- FANCHINI H., FADIER E., (2008) - De la design d'un system technique à la conceptualisation d'un system de travail : le cas de la TCISF. Actes du 43ème congrès de la Société d'Ergonomie de Langue Française. Ajaccio 17-19 septembre 2008
- GARRIGOU A., THIBAUT J-F., JACKSON M., MASCIA F., (2001) Contributions et démarche de l'ergonomie dans les processus de design. *Revue électronique Pistes*, Volume 3, n°2, octobre 2001. <http://www.pistes.uqam.ca/v3n2/pdf/v3n2a6.pdf>.
- HATCHUEL A., WEIL B., (1992) *L'expert et le system*, Economica, Paris.
- HATCHUEL A., (b) (2002). Towards Design theory and expandable rationality. *Journal of Management and Governance*, 2002, 5, 3-4, 260-273.

- HATCHUEL A., (a) (2002)- Sources of Intensity in Work Organizations. In: *Creating Sustainable Work Systems. Emerging Perspectives and Practice*. P. Docherty, J. Forslin and A.B.S. Shani. (Eds.), Londres, Routledge, 2002, pp.40-51.
- LEBAHAR J.C., (1993). Aspects cognitifs du travail de designer industriel. *Design Recherche*, 1993, 3, 39-55.
- NACHREINER F., (2007) Applying ergonomics standards in the design of work systems: means for improving the safety related design quality of work systems. *HST-CND Journal* N° 205.
- RASMUSSEN J., (1997). Risk Management in a dynamic society: a modeling problem. *Safety Science*, 1997, 27(2-3), 183-213.
- RUMELHART D.E, NORMAN D.A., (1978) Accretion, tuning and restructuring: three modes of learning. In J.W Cotton & KLATZKY R.L., (Eds.), *Semantic factors in cognition*. Hillsdale, N.J., Lawrence Erlbaum..
- VINCENTE K., (1999) *Cognitive work analysis. Toward safe, production and healthy computer-based work*. Lawrence Erlbaum, London.
- VISSER W., (2004) *Dynamic aspects of design cognition*. INRIA Report RR-5144, March 2004. Rocquencourt, France: INRIA.

Implementation of ergonomics principles in the design of machinery

Georg Krämer

Chairman of ISO/TC 159 "Ergonomics"
Isaac-Fulda-Allee 3
55124 Mainz – Germany
georg.kraemer@vbg.de

KEYWORDS: Standardization, Ergonomics, Safety of machinery, ErgoMach,
Bridging document

Abstract

The manufacturer of machinery is under obligation to carry out a risk assessment procedure to identify all relevant hazards and to estimate and to evaluate all risks which apply to his machine. Among them, hazards and risks generated by neglecting ergonomic principles should be considered. The risk assessment can be done as described in ISO 12100. Inadequate adaptation of the machines to the capacities and skills of the intended user population can lead to hazards as mentioned in ISO 12100:2010, chapter 6.2.

To this end, an iterative process to reduce significant risks has to be carried out to cover all residual risks. ISO 12100 describes how this process can be managed. Suitable procedures which can be used to verify the actual implementation of the described ergonomic measures have to be defined and user information especially concerning the residual risks has to be provided.

This presentation describes the main ergonomic factors influencing the safety of machinery and gives a framework for incorporating them into the design process by integration of important ergonomic principles in industrial design of machines, such as:

- operators variability,
- posture and movement space,
- work rate and pattern,
- human error,
- human/machine interface,
- workplace environment.

The approach is based on ISO Guide 78 and ISO 12100 with its iterative process to reduce significant risks and also covers the ergonomic requirements given in Annex I, 1.1.6 of the European Machinery Directive 2006/42/EC.

Each step of this iterative process has been adapted to include ergonomics principles and practical guidance is given to apply horizontal standards.

1. Introduction

Ergonomics as defined by the International Ergonomics Association is the scientific discipline concerned with the understanding of the interactions among human and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance.

ISO/TC 159, through standardization and co-ordination of related activities, promotes the creation of working and living conditions which fit the anatomical, physiological and psychological characteristics of human beings taking into account the physical, social and technical environment.

Ergonomics standards provide information about human characteristics and performance, and methods for specifying, designing and evaluating products, systems, services and environments.

The benefits and main objectives of standardization of ergonomics in the actual business environment are:

- to enhance health, safety and well-being of the users as well as the overall performance
- to prepare standards in the field of ergonomics, in order to meet the requirements for ergonomic and efficient products under the conditions of free trade
- to improve the usability of products

to deliver a consistent set of ergonomic requirements as a reliable basis for a world-wide machine design.

The principal deliverable of ISO is the International Standard. An International Standard embodies the essential principles of global openness and transparency, consensus and technical coherence. These are safeguarded through its development in an ISO Technical Committee (ISO/TC), representative of all interested parties, supported by a public comment phase (the ISO Technical Enquiry). ISO and its Technical Committees are also able to offer the ISO Technical Specification (ISO/TS), the ISO Public Available Specification (ISO/PAS) and the ISO Technical Report (ISO/TR) as solutions to market needs. These ISO products represent lower levels of consensus and have therefore not the same status as an International Standard.

The foremost aim of international standardization is to facilitate the exchange of goods and services through the elimination of technical barriers to trade.

2. Role of standardization

ISO/TC 159 deals with products, work systems and work equipment, which are used all over the world in a wide range of different areas.

Standardization in the field of ergonomics resulted from requirements to design machinery, work equipment, and products according to human characteristics in order to enhance the usability and thus the productivity, health, safety and well-being of the operator or user.

As a matter of fact, ISO standards, when dealing with health and safety aspects, mostly do so in order to improve products in a market oriented perspective. Nevertheless, items such as noise, vibrations, cold and heat stresses have been the subject matter of ISO standards aiming at health and safety benefits.

Ergonomic design, as represented in ergonomics standards, can enhance work life for many persons through the design of work systems and equipment. Ergonomic data and design principles are also applicable to the design of consumer products and living environments.

Standardization thus has clear implications for enhancing the overall quality of life for individuals and populations. Since ergonomic principles, data and design are not only relevant to the design of work equipment, work systems or work environments, but also to consumer products for private use, equipment for leisure activities and non-work environments, ergonomic design following ergonomics standards can at the same time be regarded as a contribution to a more general approach to human engineering for the general quality of life. Standardisation in the field of ergonomics thus has quite clear implications for the general and the work related level of quality of life.

In the European Union there already exists a set of well accepted European standards for the implementation of ergonomic knowledge into the machines already in the design phases. They could be transformed to International standards to get a reliable set of global guidelines for ergonomics, which is desirable in times of globalization. Many goods and services in Europe fall under internal market regulations. The internal Market comprises an area without internal frontiers in which free movement of goods, services, persons and capital is ensured.

Standards are documented voluntary agreements, which establish important criteria for products, services and processes. Standards, therefore, help to make sure that products and services are fit for their purpose and are comparable and compatible.

Apart from the efficient usage of ergonomically designed products and work systems the application of ISO/TC 159 standards contributes directly to the reduction of machinery accidents respectively hazards. The direct result of this work is that if the methodology is followed by the designer of machinery there will be a related reduction in machinery accidents and hence the consequential reduction in pain and suffering to the individual and overall costs to society.

It is not possible to calculate the total cost of every machinery accident in the world but recent studies have shown that for a single accident, the total cost to the individual and to the society can be up to \$ 1 million. Clearly any measure that can reduce the number of accidents will result in a saving in pain and injury to the individual and the overall costs to society.

Furthermore, when considering ergonomics positive effects occur in various areas. The hazards will be reduced e.g. in the field of work with visual display terminals or the design of control centres and the economic benefit will be achieved since e.g. the costs for workplace absence due to sickness are reduced and a higher efficiency is reached.

Information about the structure of ISO/TC 159, the scopes of any existing subcommittees and information on existing and planned standardization projects as well as publications of ISO/TC 159 and its subcommittees can be found on the public homepage of ISO/TC 159.

Structure of the ISO committee:

http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees.htm

Publications and current projects of the ISO technical committee and its subcommittees:

<http://www.iso.org/iso/search.htm>

All national standardization bodies have the right to participate in the work of technical committees and subcommittees. In total ISO/TC 159 comprises 56 members divided in 26 P-members (participating) and 30 O-members (observing).

Since memberships change in time please see the public homepage of ISO/TC 159 for details:

http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=53348

All the ISO national members are entitled to participate in the work of ISO/TC 159 as P- or O-member.

To participate in the activities of this ISO/TC, please contact the national standards organization in your country. Our P- and O-members nominate delegates for the TC and SC meetings and participate actively in meetings and ballot voting.

Except the ISO national members above, the following parties are interested in the standardization process:

Category A-Liaison has been established with:

- European Commission (EC);
- European Computer Manufacturers Association (ECMA);
- International Commission on Illumination (CIE)
- International Ergonomics Association (IEA);
- International Labour Organization (ILO);
- World Health Organization (WHO).

3. Implementation initiatives

As an initial start to emphasize the role of ergonomics in the design of machinery, the German Commission for Occupational Health and Safety and Standardization KAN organized a European conference with the title “The new Machinery Directive 2006/42/EC – The expectations of prevention experts regarding standardization” on 27 and 28 May 2008 in Munich.

One of the workshops dealt with “ergonomics requirements” in the new Machinery Directive 2006/42/EC. The fundamental result: **Ergonomics has to be an incorporated, self-evident part of construction and standardization.**

In order to reach this aim, a whole series of proposals which are beneficial and well suited were formulated.

It was decided to install a little working group in order to help the EC (European Commission) to write the ergonomic part of the “Guide to application of the Machinery Directive 2006/42/EC”.

As a consequence of the discussion, the relevant standardization committees were asked to discuss appropriate measures in order to support the implementation process.

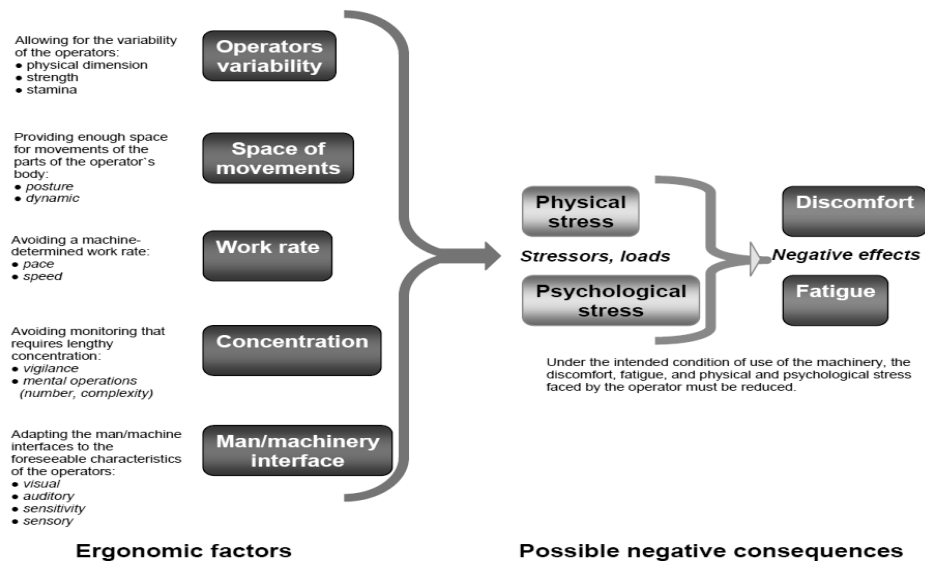
3.1 Ergonomics in the Guide to application of the Machinery Directive

The new version of the Machinery Directive (MD) attaches greater importance to ergonomics. The MD now contains ergonomic requirements formulated in annex 1.1.6. A supplement which explains the ergonomic requirement in greater detail was now added to the European Commission’s guide to application of the 2006/42/EC MD. The purpose

of the guide is to explain the requirements of the MD in sufficiently general terms to enable them to be implemented without the need of further sources.

The aspects of ergonomics addressed in Annex 1.1.6 are divided into two groups. The first group includes five ergonomic factors that have to be taken into account when designing machinery. These factors are listed in the intents of section 1.1.6 however it should be underlined that this list is not exhaustive but it is intended to draw the attention of manufacturers and designers to certain important aspects of ergonomic principles.

The second group, listed in the first sentence of section 1.1.6, includes negative effects that can be caused by these factors. Good design reduces the negative effects of these factors on persons whereas inadequate design is likely to give rise to discomfort, fatigue or physical or psychological stress. These effects may, in turn, give rise to musculoskeletal disorders, for example. They also tend to make accidents more likely.



The diagram illustrates requirements set out in section 1.1.6

In order to provide more information detailed explanations of the illustrated nine factors and effects were developed and will be integrated directly into the future (3rd) edition of the guide. The requirements are explained in terms suitable for non-ergonomists and supplemented by illustrated examples on a two- to three-page information sheet for each requirement.

3.2 Implementation of ergonomic principles in safety standards

In order to support the results of the Munich conference, relevant standardization committees were asked to discuss appropriate measures in order to support the implementation process. ISO/TC 159 "Ergonomics" and ISO/TC 199 "Safety of machinery" picked up the findings and started activities to develop a "bridging document" with the aim to make it easier for designers to consider ergonomics requirements with the necessary closeness.

It was decided in both committees to develop a bridging ISO technical report that explains the relation between the Machinery Directive, the A-standard EN ISO 12100 and the ergonomics standards of ISO/TC 159, with the intention to influence machinery design. It was recommended to develop this document in WG 6 of ISO/TC 199 as a joint working group with experts from both committees.

To convince designers to take up and use ergonomics principles in the design process, it is indispensable to elaborate the document in line with the design steps described in Guide 51 "Safety" and the iterative process given in ISO 12100.

This step by step approach is well known and accepted by designers of machinery.

The general procedure can be divided into:

Step 1: Clarifying the limits of the machine. This is important in order to determine clearly the usability of the machine with regard to operators and exposed persons.

- Step 2: Identifying the relevant ergonomic aspects by means of hazard identification. The hazards identified will be considered as relevant ergonomic hazards.
- Step 3: Complete risk estimation taking into account all the relevant ergonomic hazards which can occur during the life cycle of the machine in order to distinguish between those relevant ergonomic hazards which are in fact negligible and those which form ergonomic risks requiring further evaluation.
- Step 4: Risk evaluation of the remaining relevant risks to determine a list of significant ergonomic risks.
- Step 5: Risk reduction for the significant ergonomic risks which are dealt with in the standard. It is possible not to deal with one or more of the significant ergonomic risks, but if this is the case it must be mentioned in the scope of the standard and the risks must be listed.
- Step 6: Verification methods for the risks dealt with in the standards.
- Step 7: Information for use concerning the residual ergonomic risks that are both dealt with and not dealt with in the standard.

By applying this approach to ergonomics aspects given in ISO 12100 no new tools or new processes are necessary.

Important ergonomics aspects are related to

- postures and movements,
- ease of operation,
- noise, vibration, thermal effects
- the working rhythm
- automatic succession of cycles;
- lighting on or in the machine;
- manual controls (actuators)
- indicators, dials and visual display units.

In order to acquire a fundamental understanding of hazards caused by ergonomically inadequate design, the core piece of the document is to show the relation of ergonomics hazards and mechanical/electrical hazards. Discomfort, fatigue, musculoskeletal disorders and/or stress are significant hazards at the same level of importance like mechanical or electrical hazards with the risk of causing a physical injury. The figure below shows an example comparing hazards arising from the failure to adequately consider mechanical, electrical and ergonomics aspects in the design of machinery.

Hazards arising from the failure to adequately consider	Mechanical aspects	Electrical aspects	Ergonomics aspects
Origin of hazard	Sharp edge	Electricity	Exhausting posture
Factors influencing the risk	Surface characteristics	Electrical insulation not appropriate	Space for movement restricted
Hazard	Cutting	Electric shock	Discomfort/Fatigue
Harm	Injury/Pain/Bleeding	Injury/Pain/Death	Back pain/ Musculoskeletal disorder
Severity of harm	Slight to severe injury	Slight to fatal injury	Slight to severe health damage (reversible/chronic)

Figure: Comparison of hazards related to mechanical, electrical and ergonomics aspects

Discomfort, fatigue, musculoskeletal disorders and/or stress are comparable alarming signals, as they may lead to an occupational disease or to an accident and influences system performance and product quality. The realization and acceptance of this relationship is the key point that ergonomics became a self-evident part of construction.

In order to be similar with European regulations and requirements, the bridging document as an International document discusses similar factors as given in Annex 1.1.6 of the European Machinery Directive and explained in detail by ErgoMach.

In a first step the assessment of risks is limited to the most important factors mentioned in the Machinery Directive. Good machinery design according to basic ergonomic principles supports healthy work for all operator groups, independent of body dimensions, gender, age, cultural background and disabilities. It is necessary to consider the variability of the operators and focus in particular to physical dimension, strength and stamina.

Proper design will ensure good posture and provide sufficient movement space for all operators affected to handling the machinery (installing, operating, adjusting, maintaining, cleaning, dismantling, repairing, transporting), the equipment, raw

material and products, for the intended use and any reasonably foreseeable misuse. Sufficient space of movement for workers is essential for the workplace design, whole body access and circulation and all access openings. Size and dimension of workplace design is dependent on the anthropometrical data of the staff and their work tasks.

Work rate and pattern is a flow that describes the number of pieces per time unit and how they were handled measured at one operator's working station. When non adjustable by the operator(s), work rate and pattern imposed by the machine could cause problems. A machine determined work rate and linking the operator's working rhythm to an automatic succession of cycles must be avoided.

If the ergonomic factor human error is not taken into account by machinery designers the risk of unintended behaviour of the operator or reasonably foreseeable misuse of the machine occurs. If machinery design involves tasks requiring heavy workload, lengthy or intense concentration/sustained attention, the effect on the operator can be monotony and reduced vigilance. Both an overload and an underload affecting concentration can lead to mental fatigue, monotony and reduced vigilance. Lighting, climate, noise, odours are other factors affecting concentration. These two fatigue-like states are key contributing factors to human error and increase the risk of incidents and accidents.

Human-machine interface design primarily concerns the task interface, which defines the functions to be performed by the operator and by the machinery. The design also concerns the interaction interface, which tailors the dialogue between operators and machinery. Therefore foreseeable characteristics of the operators like visual, auditory, sensitivity and sensory need to be considered.

In order to integrate workplace environment in design adequate lighting needs to be provided. Flicker, dazzling, shadows and stroboscopic effects shall be avoided if they can cause a risk. The design of machinery shall take into account the effects of any exposure of noise and vibration but also thermal emissions produced during the operation of the machine.

In addressing the given information into the iterative design process following ISO 12100 a successful implementation of ergonomic principles in the design of machinery is possible. Ergonomics will have a good chance to become an incorporated, self evident part of construction and standardization.

References

<http://www.kan.de/de/publikationen/kanbrief.html>: KAN Brief 03/2008 and KAN Brief 02/2012.
<http://www.ergomach.eu/ergomach/index.jsp>
http://ec.europa.eu/enterprise/sectors/mechanical/files/machinery/guide_application_directive_2006-42-ec-2nd_edit_6-2010_en.pdf
http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_en.htm
<http://www.nora.kan.de/en/ergo>
<http://www.iso.org/iso/home.htm>
http://www.iso.org/iso/standards_development/technical_committees.htm
http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees.htm
<http://www.iso.org/iso/search.htm>

Prevention through Design in Occupational Safety and Health by Risk Assessment of Virtual River Locks

Peter Nickel, Andy Lungfiel, Michael Huelke

Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), Alte Heerstraße 111, D-53757 Sankt Augustin, Germany, Tel. +49 (0)2241 2312832, Fax +49 (0)2241 2312234, E-mail peter.nickel@dguv.de, <http://www.dguv.de/ifa/sutave>

Eugen Pröger

Federal Waterways and Shipping Administration, Traffic Engineering (WSV-FVT), Systems Engineering Group, Weinbergstraße 11-13, D-56070 Koblenz, Germany, Tel. +49 (0)261 9819 2100, Fax +49 (0)261 9819 2355, E-mail eugen.proeger@wsv.bund.de, <http://www.fvt.wsv.de>

Rolf Kergel

German Social Accident Insurance Institution of the Federal Government (UK Bund), OSH and Prevention - West, Cheruskerring 11, D-48147 Münster, Germany, Tel. +49 (0)251 93200 941, Fax +49 (0)251 93200 930, E-mail rolf.kergel@uk-bund.de, <http://www.uk-bund.de>

Virtual Reality, Accident prevention, Risk assessment, Machinery Safety, Prevention through Design

ABSTRACT

Prospective and preventive risk assessments refer to early design stages of machinery development. Today assessments of future machinery in the future contexts of use provide an opportunity to integrate safety and health through machinery design and to avoid resource-demanding corrections when machinery design has already been completed. A project has been initiated to investigate the suitability of virtual reality (VR) based simulations for risk assessment support. The machinery for assessment is an extension of a river lock in the planning phase. A VR based simulation model of the future river lock has been developed in 1:1 scale based on planning information available and has been envisaged for risk assessments by an interdisciplinary team of inspectors. Recent analyses resulted in an identification of work scenarios at the river lock and an agreement to focus on mechanical hazards and hazards arising from a lack of consideration of human factors and ergonomics design principles. The work scenarios provided a basis for (1) the description of the limitations of machinery as an initial step in risk assessment, (2) the implementation of flexibility and dynamics requirements in the VR simulation and (3) an initial evaluation of the suitability of VR to support risk assessments. At the current stage of the project evidence tends to suggest VR based simulations to be rather suitable for risk assessment support of the specific river lock and machinery in general. More elaborate conclusions, however, can be drawn when risk assessments of the virtual river lock have been completed.

1 INTRODUCTION

Risk assessments in the context of the Machinery Directive 2006/42/EC aim at determining essential health and safety requirements applicable to machinery, and informs about measures to be taken into account to comply with these requirements [1]. When placing machinery on the European Union market, individual parts of machinery could have already been included in different risk assessments according to the Machinery Directive. This could have happened because an assessment already referred to an individual component of the machinery, and this component now is an integrated part in the prototype of a more complex machinery to be considered for risk assessment. It could also have happened when the machinery was heavily modified at a later stage in life cycle and therefore underwent another assessment. This approach is based on the rationale that 'the whole is greater than the sum of the parts' and refers to the notion that potential hazards may also change with functionality of machinery and with information about intended contexts of use. As a consequence, risk assessments always encounter different machinery.

Effective risk assessment, however, faces a dilemma in that it should be performed at an early stage of machinery development while at the same time consider all the risks associated with the machinery within future contexts of use (EN ISO 12100:2011). Therefore, assessments referring to early stages of machinery development are often

called preventive and prospective risk assessments [2], while others addressing ready-made machinery are called amendatory or corrective risk assessments. Advantages in prospective risk assessments could be seen for at least two reasons. The sooner potential hazards can be detected, the better measures can be integrated in machinery development at early design stages to combat associated risks. The better information about the intended context of use is available, the less adaptation in form of re-design by additional safety measures may be required after machinery development. Central to this issue is the determination of the limits of the machinery in order to get a clear understanding of the machinery and its use as an initial step in risk analysis. Also in this situation it is crucial to collect and to analyse information regarding the parts, mechanisms and functions of machinery and its intended context of use, even if similar machinery is not available or the context of use reaches to the far future.

Risk assessments at early design stages of machinery in practice often benefit from functional knowledge, experience with similar machinery, mental simulation and imagination in order to compensate for incomplete predictions of future machinery in future contexts of use [3]. Increasingly, this is supported by model based simulation and animation methods for components of machinery (e.g. 3D CAD), for the whole machinery (e.g. mock-up, prototyping), and for machinery in the context of use (e.g. virtual reality (VR) simulation). The knowledge available about the suitability and effectiveness of model based simulation for machinery in the context of use to support risk assessment at early design stages, however, is rather limited [4, 5].

A project has therefore been initiated by the German Social Accident Insurance Institution of the Federal Government to investigate the suitability of VR based simulations for risk assessments and if possible, provide information about potentials for risk reduction. The extension of the River Neckar lock 'Kochendorf' has been chosen for model assessment, because (1) river locks require testing and certification according to Machinery Directive 2006/42/EC [6], (2) this river lock is the first among 26 going to be extended at river Neckar in the near future and (3) once built, river locks should be in service for several decades and modifications should be avoided due to expenses and complexity. The project is carried out by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) in close cooperation with the federal waterways and shipping administration (WSV-FVT).

2 METHOD

2.1 Simulation and task environment

In industry and services VR has grown into a simulation tool for humans to interact with virtual environments and into a methodology for applied research in human-machine system design and evaluation. VR can facilitate assessments of fully functioning machinery in realistic work scenarios, of safety concepts for future work systems, and of the usability of safety measures in the context of use without placing the operators and others in danger [7, 8]. The VR laboratory of the IFA (www.dguv.de/ifa/sutave) offers effective prevention through design in occupational safety and health (OSH) to be addressed by means of innovative technology. For risk assessments in VR work scenarios the laboratory provides a 7 m² operating space in front of a curved presentation wall of 24 m² (3 m x 8 m) [9].

River locks are treated as machinery and therefore mandate risk assessments according to regulations of the Directive 2006/42/EC [6]. Among 26 locks of the German river Neckar, that will be extended over the next two decades, the Kochendorf river lock has been chosen as it is regarded as a suitable representation for river Neckar locks and as this lock will be the first to be extended in reality. Currently, Kochendorf allows locking of river barges with a length of 110 m and a width of about 11.45 m at maximum. All river locks at river Neckar will be extended to allow locking of river barges of 135 m [10]. Results obtained from risk assessments within the given project could therefore provide information for the river lock at Kochendorf and for subsequent river locks of the river Neckar. Because risk assessments should be performed similar to reality it was seen necessary to set up a model of the river lock within specified contexts of use and to simulate the prospective design for an extension of the specific river lock in 1:1 scale. The model was based on information already available in 3D CAD (e.g. components of machinery such as electro-mechanical linear actuators), maps (e.g. landscape), photos (e.g. taken during site inspections), and drawings (e.g. water engineering); the latter being currently in the process of official approval of plans (see Figure 1). Model composition consisted of systematic import of individual components into Python (Python Software Foundation, USA) and the Vizard Virtual Reality Toolkit (WorldViz LLC, USA), the application of kinetical and environmental models (e.g. gravity, water, sky), the animation of moving parts of machinery (e.g. lock gates, elec-

tro-mechanical linear actuators, water level) and inclusion of components necessary for contexts of use under investigation (e.g. river barges, measurement devices).

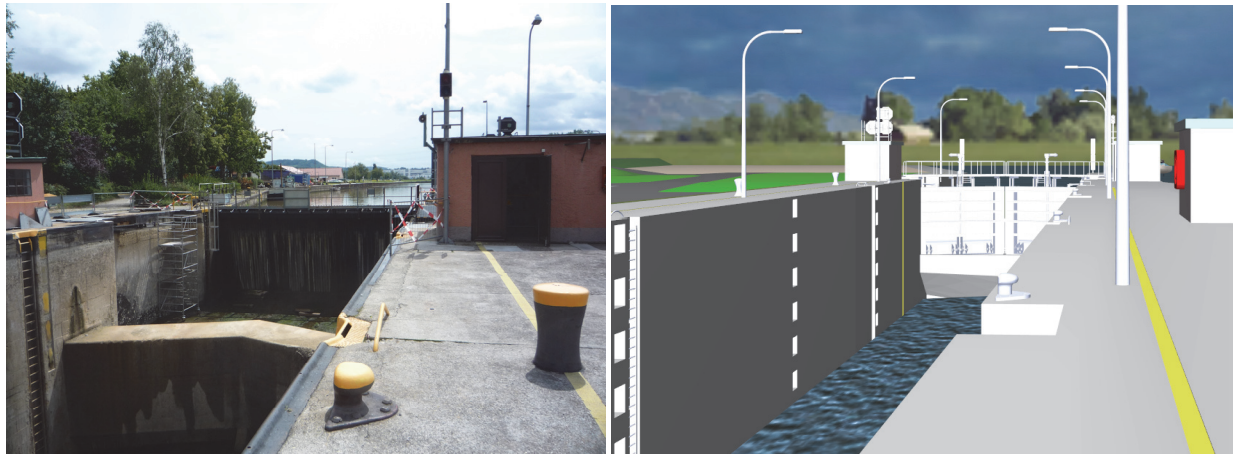


Figure 1. River lock in reality at current state (left) and future river lock in virtual reality (right)
 (Pictures: © IFA Nickel, © IFA Lungfiel/ WSV).

2.2 Risk assessment

A three step procedure for risk reduction is recommended in EN ISO 12100:2011 starting with risk analysis, followed by risk evaluation and resulting in risk reduction [11, 12, 13]. While risk analysis includes determination of the limits of the machinery, hazard identification, and risk estimation, this taken together with risk evaluation forms the risk assessment (see Figure 2). Risk assessments as iterative processes can be performed at different

- stages of the machine life cycle (i.e. during development and modification of machinery),
- levels of maturity of machinery (i.e. mock-up and prototype), and
- degrees of detail (e.g. referring to individual components and whole machinery).

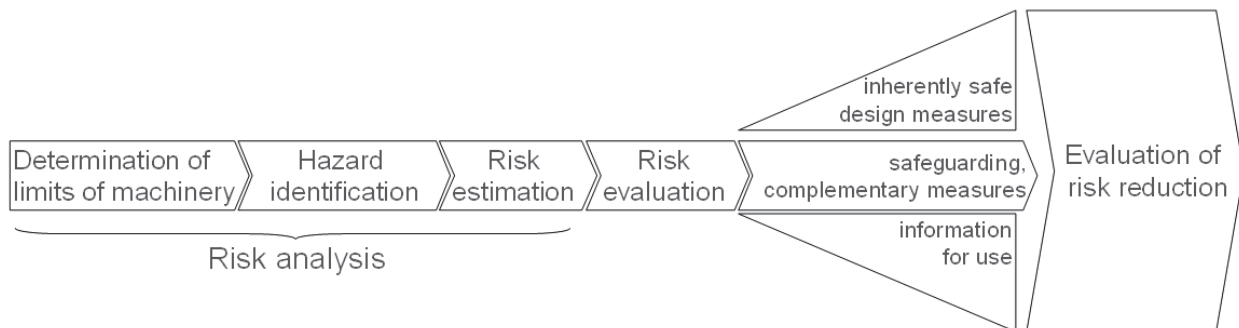


Figure 2. Process of risk assessment according to EN ISO 12100:2011.

Experts of the Federal Waterways and Shipping Administration and those involved in the given project on risk assessment of river locks have agreed to focus on mechanical hazards and hazards arising from a lack of consideration of human factors and ergonomics design principles. Risk assessments should refer to a selection of scenarios to facilitate different demands. First, scenarios should allow investigating potential risks of the future river lock within future contexts of use [14] to meet health and safety requirements according to the Machinery Directive. Next, scenario development in VR is closely linked to the development of the VR simulation model and variations in scenario requirements may increase the complexity of the simulation model to provide a suitable basis. Finally, the scenarios should also serve to draw conclusions on potential advantages and disadvantages of VR for risk assessments of river locks. Qualitative assessments and comparisons of risk assessment with and without VR are assumed to provide valuable information. Scenario selection therefore intended to take advantage of VR as a dynamic simulation tool, in

that main components of the machinery (e.g. signals, lock gates, water level) and the context of use (e.g. river barge, weather) interacted and collaborated within work scenarios (e.g. locking of ships) and in that repeated play and control of dynamic scenarios within specifically designed contexts of use was available (e.g. passing of ships). Apart from risk assessments for selected scenarios, overarching issues were the identification of potential constructional or model shortcomings of the river lock (e.g. bollard anchorages show in underground cable pipe). In addition, a set of tools was integrated in the scenarios for risk assessment to allow selecting focal points, taking virtual measurements and accessing caverns for machinery. For risk assessments in the VR laboratory an interdisciplinary team of inspectors (e.g. health and safety professionals, operating company, manufacturers) was envisaged.

3 PRELIMINARY RESULTS

3.1 Risk assessment of virtual scenarios

Documentation of limits of the machinery is the initial step in risk assessment. Information about parts, mechanisms and functions of machinery should be analysed for potential human-machine interactions in order to get a clear understanding of the machine and its usage. The limits of machinery also refer to different stages during the machine life cycle including installation, commissioning, maintenance, decommissioning, correct use and operation as well as the consequences of reasonably foreseeable misuse or malfunction (EN ISO 12100:2011). It has been possible to gather information on the limits of the river lock in one document, while specifics for individual scenarios were documented with the scenario. Determination of the limits of the river lock has also been served by documentations on ongoing activities for extensions of the River Neckar locks and on risk assessments of river locks in general [15, 14]. The VR simulation model has been improved to fit all requirements of scenarios for risk assessment (e.g. built-in functionality for movements of parts of the machinery and of barges). Several tools have been developed in VR for the selection of settings for colours, for the setting of appropriate points of view for different scenarios, for triggering predefined movements of various moving parts of the river lock within a context of use, for triggering procedures according to storyboards, for taking pictures for documentation, and for using various measures while being able to virtually walk on top of the river lock Kochendorf.

In order to allow for a clear understanding of the machine and its usage, documentation of limits of machinery also includes descriptions of scenarios for risk assessments under investigation. Five categories for scenarios on the virtual river lock have been short-listed.

(1) Passage of river barges in harbour area.

This scenario should allow investigating potential hazards with regard to the spatial situation of the redesigned harbour area and with a river barge mooring at the harbour close to the river lock. The scenario was subdivided according to directions a river barge of 135 m passes the harbour area. In subsection 1 a barge travels from the lock chamber in direction to the harbour and further downstream, whereas in subsection 2 a barge travels upstream in direction to the harbour and further into the lock chamber.

(2) Locking of river barges of 135 m.

This scenario refers to the river lock in terms of machinery as a whole part. It includes the dynamic simulation of changes and movements of signals, ships, water levels, electro-mechanical linear actuators, and lock gates. The scenario is subdivided according to processes of upstream and downstream locking.

(3) Maintenance work.

This scenario should address potential hazards during on-site maintenance and procedures required at the river lock for off-site maintenance. The scenario is subdivided according to its focus on maintenance of electro-mechanical linear actuators and maintenance of lock gates.

(4) Positioning of the superstructure of the lock.

This scenario should allow investigating potential hazards for different locations for the house for machinery and different locations for masts, i.e. for video systems and illumination.

(5) Lock safeguarding.

This scenario should provide information about the suitability and dimensioning of guardrails, safety markings, and safety distances available and/or required.

The scenarios selected support risk assessments (a) of the whole machinery within contexts of use (e.g. lock with harbour), (b) of parts of the machinery only (e.g. gate maintenance), (c) during dynamic operation and while interaction of various moving parts of the machinery (e.g. locking of ships), (d) under different operating conditions (e.g. normal operation and maintenance), (e) including all superstructure of the lock and fittings (e.g. dimensioning of walkways alongside machine houses, masts, sign posts and holder for life vests), (f) with regard to risk comparison of alternative design options (e.g. positioning of superstructure), and (g) with regard to risk evaluation for given options for risk reduction in the context of use (e.g. lock safeguarding).

3.2 Suitability of VR for risk assessment

The development of the VR based simulation model and initial work on risk assessments in VR also yielded benefits and limitations of the use of VR for risk assessments of machinery. A compilation of information on the suitability of VR in the present context assumes to use a VR based simulation model and the VR laboratory facilities as add on to common tools and procedures to support assessments [14]. The use of VR should neither replace risk assessments in reality nor should it replace well-known and established support for risk assessment, but should at least serve as an acceptable extension. In general, because VR can be characterised as a simulation tool several benefits and limitations are similar to those of simulation tools per se [16, 8]. However, also VR per se has specific benefits and limitations with its relevance depending on the context of use (e.g. handing over material between real and virtual environments; [7]). Examples collected as benefits and limitations refer to comparisons of risk assessments with and without use of VR.

In general, it seems reasonable to assume that VR supports human information processing of inspectors during risk assessment by triggering imagination, mental simulation, reasoning and visible experience with regard to parts, mechanisms and functions of machinery and its intended future context of use. Quite different to commonly available models of machinery (e.g. drawings, diagrams, listings) during product development, a VR based model of the river lock in its context of use may serve a vivid model easy to comprehend, to use and to imagine for all members of interdisciplinary teams. The VR model therefore provides common ground for risk assessments, reviews and evaluations of design issues.

The following issues may be in favour of the use of VR in risk assessment, because a VR based simulation model

- provides fully functioning future machinery (e.g. river lock) within a future context of use in 1:1 scale,
- may be seen as an integration of fragmented planning information (e.g. drawings, maps, photos, listings, machinery components),
- is visible, accessible, walkable, assessable,
- allows for dynamic simulations, i.e. dynamic demonstrations of movements of different parts of machinery (e.g. procedure of locking if ships),
- enables views from different perspectives and locations (e.g. quay walls, barge, control centre),
- enables also views and access of the inside model structure (e.g. caverns for machinery, water saving basins),
- supports identification of undetected hazards (e.g. by dynamics of moving parts of whole machinery),
- supports identification of testing modes and logic reasoning for dimensioning functional safety,
- supports the selection of provisions and measures,
- enables multiple repetitions of the same scenario (e.g. scenario play, pause, stop),
- serves assessments of various modes of operation (e.g. normal operation, maintenance, accidents), and
- helps evaluation of dimensioning of future caverns, of cable pipes, of walkways, of future lock superstructure for unobstructed views for barge crew and control centre operator.

The following issues may speak against risk assessment in VR, because it

- is available only with presentation tools (e.g. panel, wall, head mounted display),
- requires an additional planning model,
- may lead as an add on or additional tool to conflicting results,
- cannot cover all issues (e.g. safety of control software),
- requires a high level of fidelity and precision of the model to satisfy requirements for risk assessment,
- may exceed resources available and may go beyond cost-benefit limits, and

- can only refer to common knowledge (e.g. no simulation of unknown situations or effects) as regards the VR based simulation model.

4 DISCUSSION

The project aims at investigating the suitability of VR to support risk assessments of machinery. Before it actually will be possible to conduct the risk assessments, a considerable amount of preliminary work has been required. This mainly referred to the development of the VR simulation model in 1:1 scale based on information available. However, because the VR model is among the key elements, it has already been possible to learn some lessons and to gather information for an assessment of the suitability of VR. Towards the end of the project the suitability of VR for risk assessments will undergo a final assessment. This should address the development of the VR simulation model, the stages of risk assessment and the consequences for the design of the River Neckar lock at Kochendorf.

Although the project aims to inform about potential OSH issues at a specific river lock, results should be beneficial for the remaining river locks at River Neckar. In addition, it could be assumed that several benefits and limitations identified in the current project on river locks as machinery will also hold for other machinery and work systems (e.g. risk assessment of machinery in industrial production, of process control centres, of automated or autonomous systems). This provides a sound basis for guiding similar projects along the lessons learned and experiences gained in the current project.

5 REFERENCES

1. Fraser I., *Guide to application of the machinery directive 2006/42/EC (2nd edition)*, Brussels, European commission, enterprise and industry, 2010.
2. Merdian J., *Risikobeurteilung in Arbeitssystemen*, Die BG, 10, 1995, 518-524.
3. Wickens C.D., Hollands J.G., *Engineering psychology and human performance*, Upper Saddle River, Prentice Hall, 2000.
4. Williams M.J., *Application of virtual reality for risk assessment and training in the mineral industry (Doctoral thesis)*, Nottingham, University of Nottingham, 2000.
5. Harrison G.W., Haruvy E., Rutström E.E., *Remarks on virtual world and virtual reality experiments*, Southern Economic Journal, 78 (1), 2011, 87-94.
6. Schneider W., *Leitfaden zur Maschinensicherheit an Anlagen der WSV*, Koblenz, WSV-FVT, 2010.
7. Stanney K.M., Cohn J.V., *Virtual environments*, In Salvendy, G. (ed.), *Handbook of human factors and ergonomics*, Wiley, Hoboken, 2012, pp. 1031-1056.
8. Nickel P., Lungfiel A., Naber B., Hauke M., Huelke M., *Virtual Reality in Occupational Safety and Health for Product Safety and Usability*, Proc. of the 7th Int. Conf. on Safety of Industrial Automated Systems (SIAS), Montréal, 2012, in this volume.
9. Huelke M., Nickel P., Lungfiel A., Nischalke-Fehn G., Schaefer M., *Cave automatic virtual environments for research into occupational safety and health – practical recommendations and solutions for the construction*, Proc. of the 6th Int. Conf. on Safety of Industrial Automated Systems (SIAS), Tampere, 2010, F6044, pp. 1-4.
10. Lenz, E.-U., *Die Planungen zur Verlängerung der Schleusen am Neckar*, WSV Informationsschrift, 2007, 13-17.
11. BGIA, *BG/BGIA risk assessment recommendations according to machinery directive. Design of workplaces with collaborative robots (revision)*, Sankt Augustin, DGUV, 2011.
12. Etherton J., Main B., Cloutier D., Christensen W., *Reducing Risk on Machinery: A Field Evaluation Pilot Study of Risk Assessment*, Risk Analysis, 28, 2008, 711–721.
13. Paques J.-J., Gauthier F., Perez A., *Analysis and Classification of the Tools for Assessing the Risks Associated With Industrial Machines*, International Journal of Occupational Safety and Ergonomics, 13 (2), 2007, 173-187.
14. Schneider W., *Musterrisikobeurteilung an einer Schleuse*, Koblenz, WSV-FVT, 2010.
15. ARGE CGGH, *Grundinstandsetzung und Verlängerung der rechten Schleusenammer der Schleuse Kochendorf. Ausbau der Liegestelle im Unterwasser, Neubau einer Bootschleppe, Neckar-km 103,888. Erläuterungsbericht Teil I*, Heidelberg, Amt für Neckarausbau (ANH) der WSV, 2011.
16. Meister D., *Simulation and modelling*, In J.R. Wilson, E.N. Corlett (eds.), *Evaluation of human work. A practical ergonomics methodology*, London, Taylor & Francis, 1999, pp. 202-228.

Virtual Reality in Occupational Safety and Health for Product Safety and Usability

Peter Nickel, Andy Lungfiel, Birgit Naber, Michael Hauke, Michael Huelke

Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA),
Alte Heerstraße 111, D-53757 Sankt Augustin, Germany, Tel. +49 (0)2241 2832, Fax +49 (0)2241 2234,
E-mail peter.nickel@dguv.de, <http://www.dguv.de/ifa/sutave>

Virtual Reality, Accident prevention, Product Safety, Human-System Interaction, Usability

ABSTRACT

Simulation techniques such as virtual reality (VR) have increasingly being used in industry and services. VR has grown into a simulation tool for humans to interact with dynamic, three-dimensional virtual environments and into a methodology for applied research in human-machine system design and evaluation. Safety and Usability through Applications in Virtual Environments (SUTAVE) facilitates effective prevention through design in occupational safety and health (OSH) to be addressed by means of innovative technology. In the SUTAVE laboratory of the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) projects are being conducted in cooperation with OSH partners, companies and research institutes. Currently, there are VR projects concerning the development of safety concepts for future workplaces with collaborative robots, i.e. robots working directly alongside human beings. Another project addresses the usability of an innovative safety control for mobile elevating work platforms by evaluations in virtual working and accident scenarios. VR is also used in a project to conduct risk assessments for work scenarios at a 1:1 scale river lock. Another project refers to human factors issues in dimensioning and indication of three-dimensional detection zones by electro-sensitive protective equipment. Among others, these projects enable analysis, design and evaluation of products and processes that do not yet exist or that could present a hazard – but without placing the operator or others in danger. All social accident insurance institutions may benefit from the expertise gathered in the SUTAVE laboratory of the IFA.

1 INTRODUCTION AND CONCLUSION

Accidents and hazards at the workplace can be attributed, among others, to inadequate usability of products and processes and other human factors issues [1]. Mal-operation during monitoring and control of machinery as well as defeating safeguards [2, 3] could be avoided or at least reduced by adapting products and processes to human behaviour and their tasks within work systems (see EN ISO 6385:2004). The human abilities to perceive, process and act upon information must be taken into account in the design of human-machine interfaces. Although human factors and ergonomics literature on work systems design is available and more intensively addresses human behaviour and information processing issues in product design and safety [4], it is not always possible, to easily transfer and adapt given recommendations directly to current occupational safety and health (OSH) problems in practice. This may be due to the rather generic nature of recommendations and guidelines (e.g. ISO 9241-11:1998; ISO 10075-2:2000), facing a broad range of specific problems in practice. Another reason could be seen in the variety of tasks, specific activities, workplaces and specific working conditions to be considered for the design of different products and contexts of product use. It could also be based on the fact that OSH considerations for human factors issues should not only aim at safety improvements for products already available, but also at safety for future products in future contexts of use.

Over the past decades simulation techniques have cleared their way for applied use in industry and services [5, 6], however, not necessarily to substitute more traditional techniques for analysis, design, and evaluation in laboratories or in the field, but to bridging the gap between them [7]. According to [8] simulation may be seen a representation of reality or an imitation of real processes in the past, present or future. But it may also go beyond [1, 4] and simulate scenarios not desirable or too dangerous to face in reality (e.g. accident scenarios), or simulate machinery not yet available (e.g. human-robot collaboration as future work scenarios). Simulation opened up new and effective methods to face some problems in work systems analysis, design and evaluation, in that it allows for systems investiga-

tion across the life cycle from construction and development, over application in the context of use, up to modification and recycling [5, 8]. There is a long tradition also in OSH to use simulation techniques. Applications may refer to (a) procedures agreed on and established for testing product safety (e.g. laboratory heat stress testing for hydraulic pipes simulates product use), (b) role plays in OSH trainings intending to simulate safety behaviour at the workplace, (c) retro-perspective accident analysis (e.g. cause effect and if what/when reasoning and analyses), and (d) investigations of unavailable, undesirable or future work scenarios (e.g. safety concepts development in virtual reality simulation for human-robot collaboration).

Among simulation techniques available, virtual reality (VR) has grown into a simulation tool for humans to interact with dynamic, three-dimensional virtual environments and into a methodology for applied research in human-machine system design and evaluation as well as for training, for demonstration, and for visualisation purposes [9, 10]. Improvements in technology and success stories from industrial applications attracted VR also to OSH. Applications often refer to rehabilitation [11] and to qualification and training [12], with the latter placing an emphasis e.g. on safe behaviour at work or risk assessments [13, 14, 15]. In OSH organisations VR is increasingly being used in studies on analysis, design and evaluation of human-machine interfaces of machinery with regard to improvements in ergonomics and safety [16, 17, 18, 19, 20, 21]. Among these organisations, the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) established the concept 'Safety and Usability Through Applications in Virtual Environments' (SUTAVE) to facilitate effective prevention through design in OSH to be addressed by means of innovative technology. Information about current activities in the VR laboratory in general and technical information is given elsewhere (www.dguv.de/ifa/sutave; [22]).

Within the scope of accident prevention and product safety the IFA identified four general principles to concentrate SUTAVE activities and to focus on in projects in cooperation with OSH partners, companies and research institutes.

2 HUMAN FACTORS FOR RELIABLE HUMAN-SYSTEM INTERACTION

The topic *systematic and empirical research into human factors for reliable human-system interaction* is currently covered by VR projects on human-robot interaction. For future industrial workplaces it is envisaged to permit human-robot-collaboration (HRC), i.e. spatio-temporal cooperation in a joint movement area, if requirements of OSH concerning the design and specification of such work systems are implemented [23]. Whereas some design-related requirements, i.e. for the prevention of bio-mechanical hazards, are already being agreed on internationally in a technical specification on guidelines for the safe operation of collaborative robots (ISO TS 15066:2011), human factors and ergonomics requirements are pending. The latter would call for an inclusion of principles of human information processing in the design of HRC and should serve prevention of accidents and reduction of hazards. Within the EsIMiP joint research project of the Bavarian Research Foundation a VR simulation study has therefore been conducted to investigate the impact of trajectorial speed and separation distance on operator safety, performance and well-being [19]. In an industrial HRC virtual work environment operators performed a manufacturing component task on a notebook facing the robot (see Figure 1, left). In parallel, operators performed a quality control task in direct interaction with the industrial robot. According to preliminary analyses, operator task performance tended to improve for a lower level of robot distance but for a higher level of speed. More clearly high robot speed at close distance was perceived more hazardous than low robot speed at far distance [19]. Although the empirical basis is still rather small to draw general conclusions and detailed data analyses is pending, the results provide some evidence for human factors and ergonomics requirements with regard to robot speed and distance for safe HRC applications.

In addition, studies on the validity of research into human-system interaction in the SUTAVE laboratory have been conducted. Human information processing demands (e.g. perception of space, size, depth, colours and gray-scales) have empirically been compared in a robot cell in reality with its simulation in VR. While for most factors no differences were found between reality and virtual reality, for other factors discrimination of more subtle shading (e.g. 10 % gray, mixed colours) was adversely affected in VR. As a result, modifications of the VR equipment were arranged to improve information processing support. Potential limitations could also be taken into account for VR scenario design of upcoming research projects [24, 25]. In another study effects of intensity levels of human-robot interaction on human information processing have been investigated by means of task performance measures, psychophysiology and questionnaires in a VR simulated robot cell. The experience of immersion and presence increased with

more intensive human-robot interaction in VR. Increases in human information processing demands were accompanied by shifts in human performance accordingly. It could be concluded, that measures taken during VR scenarios were suitable to tap close to reality human-system interaction behaviour and that an assessment of human information processing demands is feasible in the VR laboratory of the IFA [26].

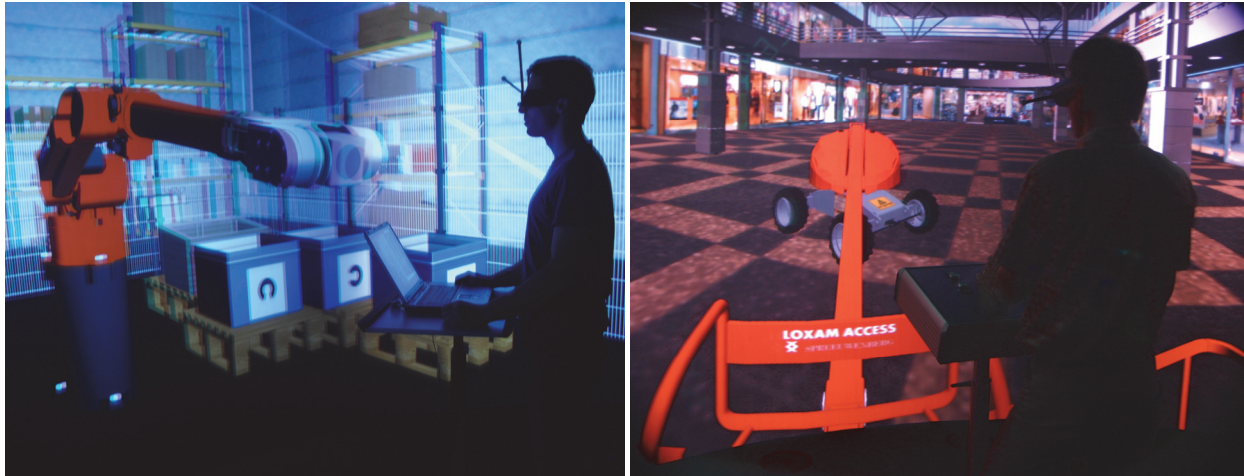


Figure 1. Human-robot collaboration scenario in VR study (left) and Mobile elevating work platform in work scenario in VR (right) (Pictures: © IFA Nickel, © IFA Lungfiel).

3 SAFETY AND USABILITY ASSESSMENTS

SUTAVE activities also focus on *safety and usability assessments of safety concepts for machinery in virtual context of use*. The project allotted to this topic aims to evaluate the usability of a safety related measure for a mobile elevating work platform (MEWP; EN 280:2010) in an industrial work environment, simulated in VR. Although MEWP manufacturers, rental companies, users, and occupational safety and health organisations have made continuous efforts to improve MEWP safety, the number of injuries and fatalities with MEWPs involved seemed to increase or at least maintain at a relatively high level [27, 28]. Countermeasures and intervention strategies for accident prevention often take long to become effective and potential solutions under development cannot be tested in the context of use (e.g. accident situations) to avoid the risk placing operators or others in danger. The German DGUV expert-committee 'Trade and Logistics', sub-committee 'Goods Handling, Storage, and Logistics' in cooperation with the German Social Accident Insurance Institution for trade and distribution industry have initiated a research project to address this issue. The usability of a prototype supplementary MEWP safety measure, intending to avoid crushing accidents [29], should be evaluated in VR while the safety measure is still in the development phase and before detailed recommendations will be given to manufacturers or users.

Virtual work and accident scenarios have been developed to allow operators to use real control panels with built-in safety functions in a virtual MEWP in the SUTAVE laboratory. A pilot study has been conducted and informed the suitability of virtual work scenarios and of methods for usability assessments. In order to investigate the usability of the MEWP safety measure it was required to perform close to reality inspection and driving tasks in the work scenario (see Figure 1, right). A mixed reality set up should support operators to behave similar as in real work environments and experience dangerous or hazardous situations, without being placed in danger. This allowed testing the safety functions in the context of use facing demands of realistic work scenarios. The usability evaluation in these situations referred to whether, to what extent, when and how operators were being able to take advantage of the safety functions. While operator task performance measures served an effectiveness assessment of usability, workload and effort measures were taken to assess the efficiency and the satisfaction of the use of the safety device in work scenarios.

Preliminary results suggest the prototype safety measure being suitable in terms of not disturbing normal MEWP operations [20]. The usability in accident scenarios, however, requires further investigation. OSH may take advantage of VR as future implementation of prevention measures can be accelerated early on. At the current state of the project it can be concluded that the use of the safety control in virtual environments as close to practice can be evaluated whilst it is still at the development phase.

4 RISK ASSESSMENT DURING PRODUCT DEVELOPMENT

The topic *risk assessment during development of products and processes* is covered by a project on risk assessment in the context of the Machinery Directive 2006/42/EC. This directive aims at determining essential health and safety requirements applicable to the machinery and informs about measures to be taken into account to comply with these requirements. Effective risk assessment, however, faces a dilemma in that it should be performed at an early stage of machinery development while at the same time consider all risks associated with the machinery within future contexts of use (EN ISO 12100:2011). A project has therefore been initiated by the German Social Accident Insurance Institution of the Federal Government to investigate the suitability of VR based simulations for risk assessments of machinery at early design stages. The extension of the River Neckar lock 'Kochendorf' has been chosen for model assessment because among others river locks require testing and certification according to the machinery directive [21]. The project is carried out by the IFA in close cooperation with the Federal Waterways and Shipping Administration (WSV-FVT).

Risk assessments will be performed for a selection of work scenarios of the Kochendorf lock in 1:1 scale in the VR laboratory by an interdisciplinary team of inspectors (e.g. health and safety professionals, operating company, manufacturers). It has been agreed to focus on mechanical hazards and hazards arising from a lack of consideration of human factors and ergonomics design principles. The focus during preparations for risk assessment was on VR simulation model development. The model was based on information already available in 3D CAD (e.g. electro-mechanical linear actuators), photos (e.g. from site inspections), and drawings (e.g. water engineering); the latter being currently in the process of official approval of plans (see Figure 2). In addition, it was necessary to integrate functionality into the VR model to enable dynamic scenarios (e.g. simulate a barge of 135 m during upstream locking) and to provide tools required (e.g. a measure for the height of guardrails) for risk assessment.

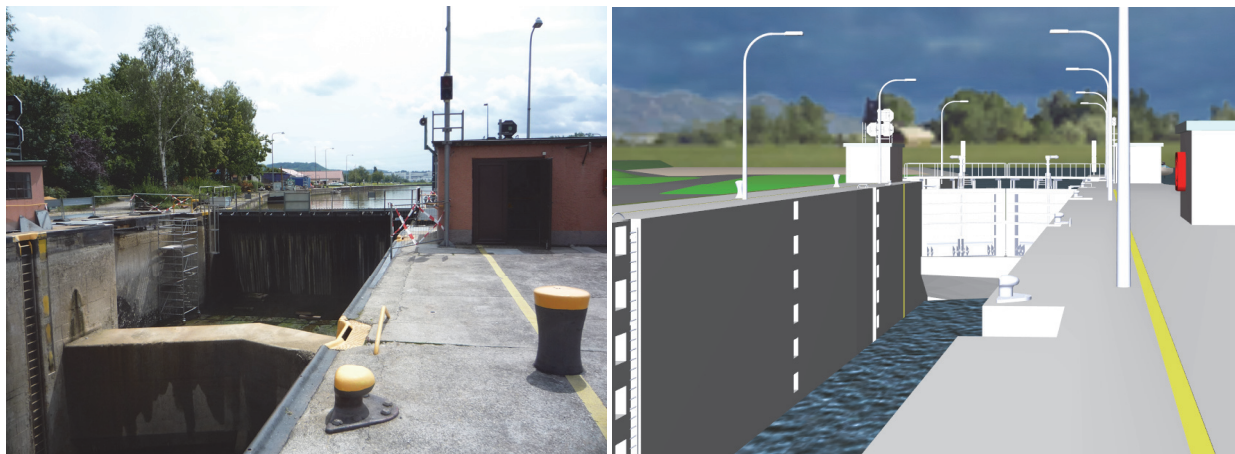


Figure 2. River lock in reality at current state (left) and future river lock in virtual reality (right)
(Pictures: © IFA Nickel, © IFA Lungfiel/ WSV).

Preliminary results of the project [21] refer to a documentation of limits of the machinery with regard to individual scenarios. Five categories of scenarios have been shortlisted (e.g. locking of river barges of 135 m, maintenance work). The VR simulation model of the river lock has been developed and provides all functionalities required to perform the risk assessments. Apart from benefits and limitations for simulation models and for VR in general [5, 9], it has also been possible to identify some benefits and limitations relevant for the suitability of VR for risk assess-

ments of machinery. Risk assessment benefits from a VR model presenting a visible, accessible, walkable and assessable fully functioning future machinery and providing scenarios within specified contexts of use. The limits of VR models could be seen in its availability on panels, presentation walls or head mounted displays only and that it can only refer to common knowledge, i.e. no simulation of unknown situations or effects. Further assessments of the suitability of VR for risk assessments should refer to the development of the VR simulation model, the stages of risk assessment and the consequences for the design of the river locks at River Neckar.

5 ANALYSIS, DESIGN AND EVALUATION OF HUMAN-SYSTEM INTERACTION

The topic on *analysis, design and evaluation of human-system interaction across the product life cycle* currently refers to a VR project investigating effects of geometry and identification marks for 3D detection zones of electro-sensitive protective equipment (ESPE). The project has been initiated by the German DGUV expert-committee 'Woodworking and Metalworking', sub-committee 'Machinery, Plants, Automation and Design of Manufacturing Systems' in cooperation with the German Social Accident Insurance Institution for the woodworking and metal industry. The project aims at information and recommendations for setting up 3D safeguarding detection zones in manufacturing, potentially in contrast to 2D detection zones of protective equipment. ESPE can safeguard hazards of machinery by detection of approaching obstacles or humans and as a consequence may trip the machinery. For safety reasons it is required to install the ESPE at a distance to the hazard area that machinery trips before human being is capable to cross the safety distance (EN ISO 13855:2010). Geometry and identification marks of the detection zone are among potential key differences in ESPE with 3D and 2D detection zones. In VR a manufacturing task scenario for human-robot interaction has been developed and variations in geometry and identification marks of 3D detection zones of a virtual ESPE have been tested on effect of human performance and safety. According to a preliminary pilot study [30], analyses of human-robot interactions during the manufacturing task scenario tend to be in favour of geometries matching the shape of the hazard area. Potential effects for both factors (geometry and identification marks) are currently under investigation. Results may also inform setting up 3D detection zones relative to the worker and to the hazard area (EN ISO 13855:2010).

6 REFERENCES

1. Wickens C.D., Lee J.D., Liu Y., Gordon Becker S.E., *An introduction to human factors engineering*, Upper Saddle River, Pearson, 2004.
2. Apfeld R., 2010, *Stop Defeating the Safeguards of Machines*. Proc. of the 6th Int. Conf. on Safety of Industrial Automated Systems (SIAS), Tampere, 2010, F6001, pp. 1-6.
3. Schaefer M., Lüken K., *Reasons for the manipulation (tampering of protective devices)*. Proc of the 4th Int. Conf. on Safety of Industrial Automated Systems (SIAS), Chicago, 2005, S 8, pp. 1-7.
4. Wickens C.D., Hollands J.G., *Engineering psychology and human performance*, Upper Saddle River, Prentice Hall, 2000.
5. Meister D., *Simulation and modelling*, In J.R. Wilson, E.N. Corlett (eds.), *Evaluation of human work. A practical ergonomics methodology*, London, Taylor & Francis, 1999, pp. 202-228.
6. Miller C., Nickel P., Di Nocera F., Mulder B., Neerinx M., Parasuraman R., Whiteley I., *Human-Machine Interface*, In G.R.J. Hockey (ed.), *THESEUS Cluster 2: Psychology and Human-Machine Systems – Report*, Strasbourg: Indigo, 2012, pp. 22-38.
7. Chapanis A., van Cott H. P., *Human engineering tests and evaluations*. In H.P. van Cott, R.G. Kinkade (eds.), *Human engineering guide to equipment design*. Washington: AIR, 1972, pp. 701-728.
8. Stanton N., *Simulators: A review of research and practice*, In N. Stanton (ed.), *Human Factors in Nuclear Safety*, London: Taylor & Francis, 1996, pp. 117-141.
9. Stanney K.M., Cohn J.V., *Virtual environments*, In Salvendy, G. (ed.), *Handbook of human factors and ergonomics*, Wiley, Hoboken, 2012, pp. 1031-1056.
10. Stanney K.M. (ed.), *Handbook of virtual environments*, Mahwah, LEA, 2002.
11. Friedman F., Regenbrecht H.T., Schubert T.W., *Measuring the Sense of Presence and its Relation to Fear of Heights in Virtual Environments*, *Int. Journal of Human-Computer Interaction*, 10(3), 1998, pp. 233-249.

12. Cobb S., Neale H., Crosier J., Wilson J.R., *Development and evaluation of virtual environments for education*, In K.M. Stanney (ed.), *Handbook of virtual environments*, Mahwah, LEA, 2002, pp. 922-936.
13. BG Chemie, *Mensch-Sicherheit-Technik. Gestern, Heute, Morgen* [Human-Safety-Technology. Yesterday, Today, Tomorrow (ACHEMA 2003 brochure)], BG Chemie, Heidelberg, 2003.
14. Leskinen T., *Improving safety by interactive design and simulation in immersive virtual work space*, CIOP-PIB Virtsafe Workshop Presentation, Warsaw, 2005.
15. Saulewicz A., Myrcha K., Skoniecki A., Kalwasiński D., *VR fork lift simulator – challenges and limitations*, CIOP-PIB Virtsafe Workshop Presentation, Warsaw, 2005.
16. Helin K., Evilä T., Viitaniemi J. et al., *HumanICT. New Human-Centred Design Method and Virtual Environments in the Design of Vehicular Working Machine Interfaces*, Tampere, VTT, 2007.
17. Määttä T.J., *Virtual environments in machinery safety analysis and participatory ergonomics*, *Human Factors and Ergonomics in Manufacturing* 17(5), 2007, 435-443.
18. Marc J., Belkacem N., Marsot J., *Virtual reality: A design tool for enhanced consideration of usability 'validation elements'*, *Safety Science* 45, 2007, 589-601.
19. Naber B., Nickel P., Huelke M., Lungfiel A., *An investigation in virtual reality on human factors requirements for human-robot-collaboration*, Proc. of the 6th Int. Working on Safety Conf. 'Towards Safety through Advanced Solutions', Sopot, 2012.
20. Nickel P., Lungfiel A., Nischalke-Fehn G., Huelke M., Trabold R.-J., *A virtual reality pilot study towards elevating work platform safety and usability in accident prevention*. Proc. of the 6th Int. Working on Safety Conf. 'Towards Safety through Advanced Solutions', Sopot, 2012.
21. Nickel P., Lungfiel A., Huelke M., Pröger E., Kergel R., *Prevention through Design in Occupational Safety and Health by Risk Assessment of Virtual River Locks*. Proc. of the 7th Int. Conf. on Safety of Industrial Automated Systems (SIAS), Montréal, 2012, see this volume.
22. Huelke M., Nickel P., Lungfiel A., Nischalke-Fehn G., Schaefer M., *Cave automatic virtual environments for research into occupational safety and health – practical recommendations and solutions for the construction*. Proc. of the 6th Int. Conf. on Safety of Industrial Automated Systems (SIAS), Tampere, 2010, F6044, pp. 1-4.
23. Ottersbach H.J., Huelke M., *Requirements for hazard analyses referring to mechanical exposure in workplace applications with collaborative robots*, Proc. of the 6th Int. Conf. on Safety of Industrial Automated Systems (SIAS), Tampere, 2010, F 6045, pp. 1-5.
24. Nickel P., Lungfiel A., Huelke M., Schaefer, M., *Evaluationsstudien zur Tiefenwahrnehmung in realer und virtueller Roboterzelle*, In Gesellschaft für Arbeitswissenschaft (ed.), *Gestaltung nachhaltiger Arbeitssysteme - Wege zur gesunden, effizienten und sicheren Arbeit*, Dortmund: GfA-Press, 2012, pp. 243-247.
25. Nickel P., Lungfiel A., Huelke M., Schaefer, M., *Prozesse menschlicher Informationsverarbeitung in realer und virtueller Roboterzelle*, In G. Athanassiou, S., Schreiber-Costa, O. Sträter (ed.), *Sichere und gesunde Arbeit erfolgreich gestalten - Forschung und Umsetzung in der Praxis*, Kröning: Asanger, 2012, pp. 177-180.
26. Nickel P., Lungfiel A., Nischalke-Fehn G., Pappachan P., Huelke M., Schaefer M., *Evaluation of Virtual Reality for Usability Studies in Occupational Safety and Health*, Proc. of the 6th Int. Conf. on Safety of Industrial Automated Systems (SIAS), Tampere, 2010, F6043, pp. 1-6.
27. BGI 720, *Sicherer Umgang mit Hubarbeitsbühnen* (written by L. Dippel, R. Jäkel, K. Stocker, O. Petzsch, C. Zepp, A. Deuchert) [Safe use of elevating work platforms], Düsseldorf, BG HM, 2011.
28. NIOSH, *NIOSH Researchers Partner with Equipment Manufacturers and Standards Committees to Protect Workers from Falls*, Washington, National Institute of Occupational Safety and Health, 2009.
29. Nischalke-Fehn G., Bömer T., *Use of a modified joystick for the avoidance of crushing accidents on elevating work platforms*, Focus on IFA's work 0332, 2011, pp. 1-2.
30. Hoyer G., Hauke M., Lungfiel A., Nickel P., Huelke M., Bömer, T., *Gestaltungsempfehlungen für dreidimensionale Schutzfelder für Fertigungszellen mit Mensch-Roboter-Interaktion – Eine experimentelle Untersuchung in virtueller Realität*, In G. Athanassiou, S., Schreiber-Costa, O. Sträter (ed.), *Sichere und gesunde Arbeit erfolgreich gestalten - Forschung und Umsetzung in der Praxis*, Kröning: Asanger, 2012, pp. 169-172.

Safety Service Engineering

-An additional concept for safety of machinery

Takashi Kabe

NPO The Safety Engineering Laboratory, 3-39-8 Shoan, Suginami-ku, Tokyo 167-0054, Japan, kabe@safetylabo.com

Abstract:

The well examined CE-Marking System has been carried out almost since 20 years in EU and became nowadays a model to achieve the safety of machinery worldwide together with A-B-C standard-structure. The basic philosophy of the CE-Marking System is a) to cover the dangerous machine to avoid human approach and b) shut off the energy, which leads to dangerous movement of machinery. The responsibility for safety lies clearly on manufacturers of machines. In many cases the manufacturers will not always be informed, what happen with machines after the distribution. Therefore it would be helpful to consider the life cycle of machine to optimize the requirement of machine users in design phase. The problem of defeating machine, which cause severe accidents was researched by IFA (BGIA) several years ago and certain changes were required in European machine directive and also relevant standards to optimize these problems. This problem is so called undefined factors, which will be led because of different interests between manufacturer and users of machine. In this case, further development of safety devices and advocating certain rules between machine manufacturer and user are necessary to enable human-machine-interaction in certain phases of machine operation. Therefore the new way of thinking to increase customer's satisfaction will be proposed as Safety Service Engineering on the base of PEST-analysis.

Keywords: safety of machinery, Safety Service Engineering ,machine lifecycle, productivity

1. Introduction

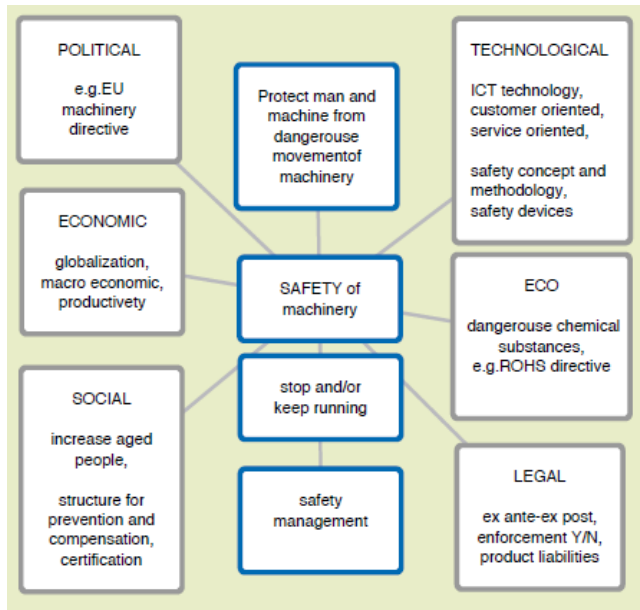
Systems engineering seeks a safe and balanced design in the face of opposing interests and multiple, sometimes conflicting constraints. Optimize the overall design, including safety as a essential part of design methodology, now a days in a "Risk Society", where a social evolution is going on because of rapidly technological changes. Systems Engineering is an interdisciplinary process that ensures that the customer's need are satisfied throughout a system's entire life cycle. The purpose of systems engineering is to produce systems that satisfy the customers' needs, increase the probability of system success, reduce risk and life-cycle cost.

Systems engineering is a methodical, disciplined approach for the design, realization, technical management, operations, and retirement of a system. A system is a construct or collection of different elements that together produce results not obtainable by the elements alone.

Systems Theory is a response to limitations of the classic analysis techniques in coping with the increasingly complex system being built and means the change of the worldview of "decomposition", or analytic reduction and linear way of thinking and approach. N.Werner applied the approach of systems theory to control and communications engineering and L.v.Berantalanffy developed ideas for biology, that the emerging ideas could be combined into a general theory of system. The systems engineering in consideration with whole system and whole life time of equipment and machines became also a base of MIL-STD-882 series.

The New Machinery Directive 2006/42/EC applied since December 2009 provides the regulatory basis for the harmonization of the essential health and safety requirements for machinery at EU level. This is nowadays a ideal model to achieve safety of machinery also in consideration of increasing Human Machine Interaction (HMI). ISO 12100:2010 specifies basic terminology, principles and a methodology for achieving safety in the design of machinery, which is essential and well tried systematic design method of prevention,

but the user's matter is out of scope, whereas machines are used and operated by machine users. The effectiveness and efficiency of the prevention is well known^{1,2)}.



2. PESTEL-Analysis for safety

Safety is an emergent property of systems and can only be determined by the relationship between the components and the system. While safety and safe life have social factors, it is necessary to look around, which factor influence safety. A rough observation of this issue, based on PESTEL-Analysis³⁾ is summarized in Figure 1.

Safety is a matter of technique originally, but has to do with economic factor, especially Cost Benefit Analysis(CBA) during the lifecycle of machine.

Would the existing safety technology and social system overcome also the problem of rapid aging populations, which is expected worldwide? Here lots of social factors should be considered.

3. Safety Service Engineering(SSE)

To discuss the possibility and limitation of existing technology and social system, a working group "Safety Service Engineering (SSE)" was formed in the Division of Industrial, Chemical Machinery and Safety of Japan Society of Mechanical Engineering in April 2010.

Service Science or Service Engineering^{5,6,7)} from the viewpoint of customer are also new scientific trend, especially since about 10 years. Also the basic concept of Human-centered design processes for interactive systems – ISO13407 was considered in the working group.

Concerning the lifecycle process we refer ISO/IEC 15288:2008 – Systems and software engineering – System life cycle processes, which describe lifecycle of systems created by human. The life cycle processes are based on Agreement-Organizational-Project-Technical and system life cycle⁴⁾ is composed of Concept-Development-Production-Use/Support-Disposal. Because of increasing of aged people, it is sufficient to take also consideration on Gerontology. The defined processes can be applied at any level in the hierarchy of a system's structure, and can be applied throughout the life cycle for managing and performing the stages of a system's life cycle. This is accomplished through the involvement of all interested parties, with the ultimate goal of achieving customer satisfaction, which is defined also in ISO 9004.

Nowadays almost 70% or more people are engaging in service factor, while around 20% are engaging in the manufacturing sector for instance in case of Japan. Therefore it is essential to take consideration on customer's satisfaction through qualitative services.

The project management, for instance defined in ISO21500 is also an essential methodology for the successful implementation of systems engineering.

The main stakeholder of safety of machinery and it's legal base or standard is clearly manufacturer of machine, it means from the view point of provider, whereas machines are used and operated from machine customers. SSE invited special speakers especially in the field of Safety of Machinery, Process Safety, New Clear Power Plant, Service Engineering, Gerontology, Engineering Ethics, Automobile and Electric Industry, Certification Bodies etc. and discussed with members of SSE, which consist out of

representatives of academic and industrial sectors in Japan. After 2 years works we have achieved certain conclusions, especially from the viewpoint of machine-users are shown in Figure 2.

- Systems thinking is effective
- To overcome the trade-off problems between manufacturer and user is welcome

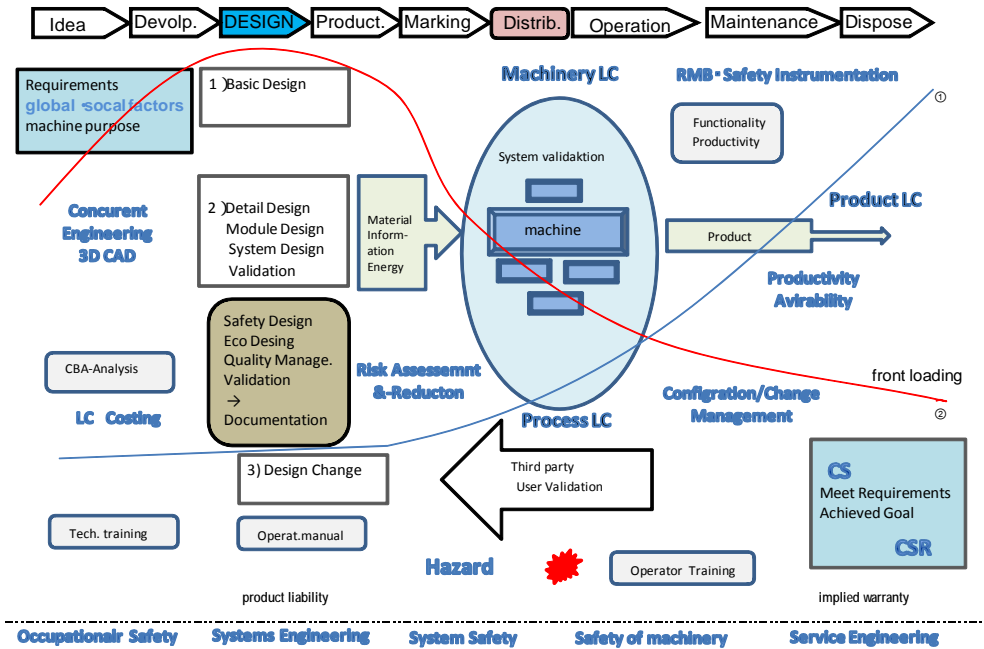


Figure 2. Concept of Safety Service Engineering(SSE)

- Frontloading of design is a key factor to optimize the efficiency during the whole lifecycle
- The design knowledge can be combined in CAD-system for utilization
- Configuration- or change management should be carry out to enable efficient management
- Comply with international standards is effective
-

4. Discussion

Back to the technical issue of safety of machinery, it is obvious, that the New Approach of EU was originally based on two principles, namely 1) cover the machine, which cause dangerous movement and/or 2) stop the machine in case of dangerous movement of machine. The machine user try not to stop the machine during the operation because of productivity obviously. The report of BGIA on defeat safety devices in 2006 showed clearly, that lots of safe machines are manipulated to enable or continue production. To overcome this realistic problem, some changes were put in legal or standard basis, as shown in Figure 3.

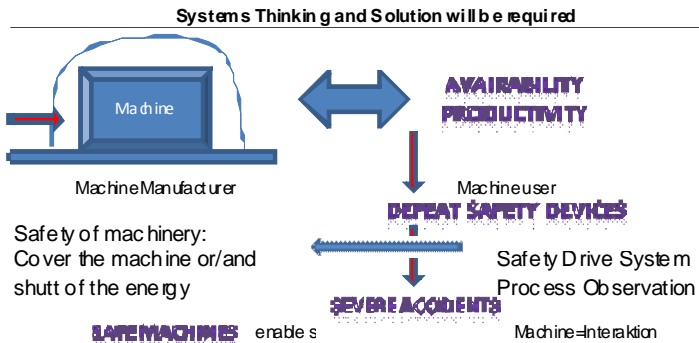


Figure 3. Basic methodology to achieve safety of machinery

The EU-directive 2006/42/EC, Cl.a.2.5 allows certain HMI as "Process Observation". The standard on interlocking devices EN1088 requires machines with safety guard with less possibilities of defeating.

The traditional way of safe guarding of machine based actually on treating I/O-signals to shut of the machine.

The ISO13849-1: Safety-related parts of Figure 3. Basic methodology to

achieve safety control systems describes requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS). The safety drive system according to IEC61800-5-2, based on the functional safety IEC 61508, defines the possibility to realize HMI by controlling the drive system e.g. Safety Limited Speed, Safely Monitored Direction, Safely Limited Position, Safe Braking And Holding System etc.

In case of HMI, additionally to keep machine safe, the approaching of human being to dangerous machine should also be observed and detected, ideally by 3D-camera system, which is still not yet

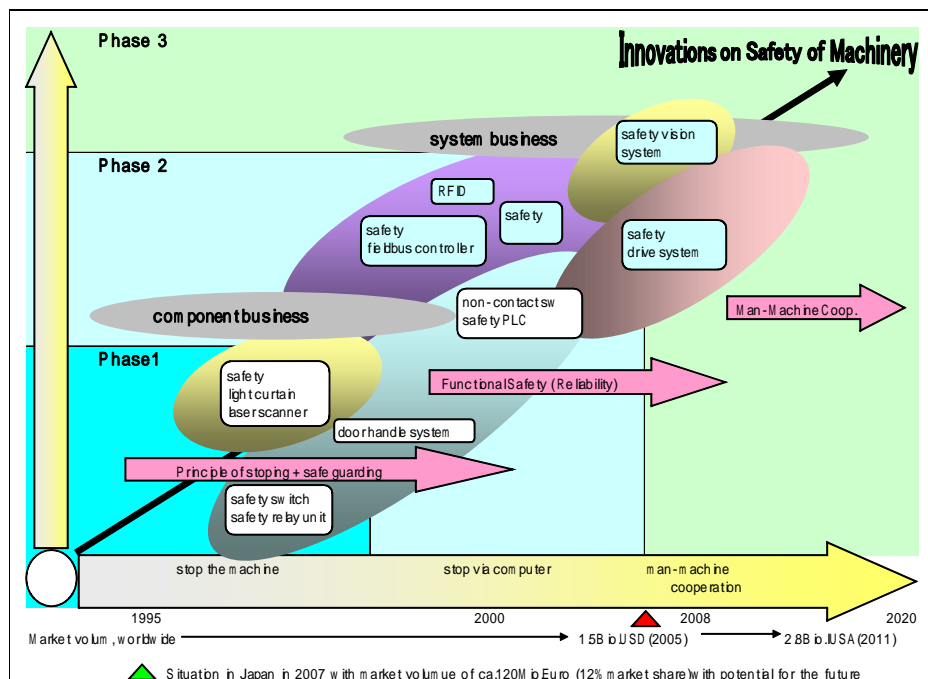


Figure 4. Development of safety devices

provided for factory automation with high dynamic movement. The development of safety devices with

influence of functional safety is shown in Figure 4. Technical specification providing the guidelines for the safe operation of collaborative robots, including safety devices are right now in discussion in the working group of ISO TS 15066.

5. Conclusion

The Article 28-2 of Japanese Industrial Safety and Health Law requires carry out of risk assessment and risk reduction to machine users, but this has no punishment, it means no enforcement. Therefore it is necessary to make more consideration in case of Japan, how the in EU or America implemented risk-based-approach could be implemented in domestic machinery market. The PESTE+-Analysis is therefore necessary.

Even the Europe's machinery directive requires cover the machine or stop the machine, which cause more costs for machine and disturb in certain process the productivity or availability of machine, this could be well balanced, when the concept of SSE will be adopted, even in Japan. Take a balance means, the systems thinking will be required for the optimization of machine system.

Because of continuously and rapidly developing technology it is necessary, that safety devices and social system to imply safety make changes also in future also from the viewpoint of SSE..

References:

- 1) PESTEL analysis of the macro-environment, Oxford University Press. 2007. Retrieved 2009-01-27.
- 2) Final Report : Quality in Prevention-Effectiveness and Efficiency of the Prevention Services of the Social Accident Insurance in Germany, BGAG,2009
- 3) Forschung zur Wirksamkeit von Praeventionsmassnahmen am Arbeitsplatz, Kolloquium der IVSS-Sektion Forschung ISSA, 2009
- 4) Service Engineering und Praevention, O.Cernavin, B.Ebert, S.Keller, BC GmbH Forschungs- und Beratungsgesellschaft, 2007
- 5) Service in Automation, ZVEI, 2004
- 6) K. Watanabe, K. Kimita and Y. Shimomura: Requirement Negotiation Process for the Design of Cooperative Services. In CIPR Journal of Manufacturing Science & Technology, Special issue on: sustainable manufacturing, CIRP, Vol. 2, No. 2, pp. 192-197, 2010.
- 7) Yuji Naka, Strategic Process Safety Management based on Life-Cycle Engineering, Journal of Japan Society for Safety Engineering , Volume 49 No.1, 2010

SIAS
2012

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



SESSION 3

PROTECTIVE DEVICES AND SYSTEMS

**PEDESTRIAN DETECTION FOR INDUSTRIAL VEHICLES BASED ON MORPHOLOGICAL
RECOGNITION:
FIRST FEEDBACK AFTER 18 MONTHS OF OPERATION**

F. Gayraud¹, N. Allezard², L. Lucat², P. Mansuy¹

¹Arcure S.A : 170, rue Raymond Losserand, 75014 PARIS - FRANCE. contact@arcure.net

²Institut CEA LIST DIASI / Vision and Content Engineering Laboratory
Bât. 864 – PC 173 – F 91191 Gif-sur-Yvette Cedex - FRANCE. laurent.lucat@cea.fr

Keywords: Pedestrian detection, morphological recognition, work-site, off-road

ABSTRACT

In order to help preventing collisions between vehicles and pedestrians working around, many technical approaches like rear camera, various kinds of radars or RFID tag detection equipment, have been developed and tested on the field. All these approaches suffer major limitations, impairing their efficiency and their reliability in operational conditions. Thanks to major improvements of hardware and algorithms, a new promising technology based on video real time processing implementing namely stereoscopic vision together with morphological recognition is now emerging. Based on an approach initially developed for automotive applications, algorithms and hardware have been drastically redesigned in order to comply with the industrial constraints, in particular with the huge variability of operational conditions in terms of context, but also in terms of image quality (poor illumination, dazzle, dust, smoke, etc.) and of pedestrian posture, gesture and clothing. The growth of embedded processing unit power combined with a software and algorithmic optimization made possible the implementation of this new approach within small form factor equipment able to cope with vehicles' electrical and mechanical constraints.

1 INTRODUCTION

Collisions between pedestrians and off-road vehicles on the work place are a major cause of severe injuries. In order to help preventing these accidents, several detection technologies were tested with a limited success, due to serious limitations. Morphological recognition is a very performing approach overcoming the defaults of these other classical detection technologies.

Video-based protection has been paid increasing attention over the last decade. As a significant example, pedestrian detection systems have emerged as new key safety equipment for high-end cars. Nevertheless, due to the very specific constraints to be faced on the work place, detection for cars is not directly applicable for industrial or earth-moving machineries.

Blaxtair, which feedback analysis is presented here, is the first equipment which has been developed specifically for these very demanding applications and which is operational. It is the result of a fruitful collaboration between ARCURE, French privately held company and CEA LIST, a public Research and Technology Center. CEA LIST provided a software library of key computer vision algorithms, which have been integrated in an ARCURE industrial application. ARCURE also designed, developed, manufactured and intensively tested the product in operational conditions.

This article will first provide insights on computer vision technologies involved in pedestrian detection, with a focus on particularities linked to the context of off-road industrial vehicles. Then, it gives some details on BLAXTAIR, and a first feedback after 18 months in operations.

2 PEDESTRIAN DETECTION USING COMPUTER VISION: STATE OF THE ART

Thanks to improvements in pattern recognition together with the increase of processing unit capabilities, the topic of pedestrian detection benefited from significant improvements over the last decade.

A survey of existing pedestrian detection methods has been proposed in [1], in the context of driver assistance. According to the authors, the data processing chain can be decomposed in 5 steps. Existing solutions encompass some, but not necessary all, of these steps:

- Pre-processing: despite not specific to the task of pedestrian detection, image enhancement such as local dynamic range control is of great interest and impacts the overall system performances.

- Foreground segmentation: the aim is to extract regions of interest (ROIs) which will have to be analyzed, thus avoiding exhaustive scanning. This ROIs extraction can be performed through monocular image analysis (color, intensity, gradient orientation...), stereo analysis (including selection of boxes only located on the floor), or through motion analysis (e.g. based on optical flow)
- Object classification: this can be considered as the core unit of the detection. Despite some authors proposed a silhouette matching, the literature is largely focused on appearance. Classifiers are trained during an off-line learning phase, thanks to a list of positive patterns (pedestrians) and negative ones (all what is not a pedestrian). Design of the classifier involves selecting low-level images features, and a learning algorithm.
- Verification / refinement: this can be seen as a post-processing, the goal of which is either to confirm a pedestrian using other criteria or to increase precision of the pedestrian location in order to get a confident distance to the camera or to help for the tracking.
- Tracking: it aims to exploit temporal correlation between consecutive frame detections; this allows to filter sporadic errors (false detection or detection miss) as well as to predict the next location of the silhouette inside the image, thus helping the foreground segmentation module.

Two extra-modules are also presented:

- Sensor fusion: camera processing output can be mixed with other signals coming e.g. from thermal infrared (TIR) camera or a radar device.
- Application layer: this includes high-level decisions as well as man-machine interface.

More specifically on classification algorithms, an overview has been proposed in 2009 by Dollar et al. [2]. Methods were compared in terms of classification rates on the same evaluation corpus. The considered use case was related to on-road and mostly urban pedestrian detection in a car, resulting in dedicated video content as well as acquisition configuration (frontal view). This review has been extended in [3]. According to the authors, despite significant improvements over the last decade, performances remain under expectations, almost at low resolution and with partially occluded pedestrians. Furthermore, it is quite complicated to compare the classification algorithms since detectors were trained with different training sets and relative results depend on the test corpus parts (small vs. large scale, no or large occlusions...). Despite a methodology was proposed in order to globally rank the methods, the difference between the 6 best-performing methods is statistically not significant. However, not surprisingly, the oldest algorithms like Viola & Jones [4] are the less-performing ones, while more recent ones such as MULTIFTR+MOTION [5], CHNFTRS [6] or FPDW [7] appear to be more performing.

3 DETECTING PEDESTRIANS IN OFF-ROAD CONTEXT

As mentioned, the large part of the literature, if not the whole, is devoted to the context of car navigation, on roads and mainly in urban areas.

Due to the characteristics of the off-road contexts, these methods cannot be used straightforward.

Limitations of classical approaches in off-road contexts

First, image content is significantly different as for car navigation. Considering the case of warehouses, there is a large variety of vertical structures within the region of interest, having various appearances, some of which are highly similar to pedestrians, such as illustrated in Figure 1.

Large variety of appearances also concerns the positive examples, i.e. pedestrians. If in on-road context, people are standing, the posture can be varying a lot for people working on a worksite, ranging from crouching to standing. Arms are not necessary along the body since workers may give indications with their hand or often handle tools. The later ones may also generate large occlusions of the body.

For these reasons, discrimination of people vs. insignificant patterns is more complex in the considered domain of industrial vehicles.

Appearance fluctuation is also extended due to the variability of the camera positioning. On the contrary to car configuration, where the camera is always mounted with a (roughly) horizontal orientation and a height not exceeding 1.5m, positioning of the camera on industrial vehicles may range from 1 to 3 meters, with angle ranging from 10 to 30 degrees due to technical constraints. As a consequence, perspective effect in the image may be large. Applying angular correction to the image generates distortion, which penalizes the detection process.

In the on-road case, the floor is considered as a plane, sometimes even an horizontal plane. Obviously, this assumption fails in the case of off-road navigation, thus increasing the complexity of foreground segmentation. Regarding the tracking phase, some assumptions can be made for urban navigation. First the trajectory of the pedestrians is quite linear: people don't change their walking direction each fraction of second. Secondly, people walking on a pedestrian crossing have a perpendicular and linear trajectory. These assumptions also clearly fail on a worksite, where people do some steps in order to take a tool, and then come back and so on. Thus, a simple tracking module would be inefficient in our case.

Furthermore, the precision of the pedestrian localization is not a critical point for on-road navigation, since there is no unambiguous rule to determine whether or not a person is considered being in a dangerous area, involving to launch an alarm to the driver. Contrarily, a fine localization precision is required for industrial vehicles, since in the surrounding area, some workers are located closed to the vehicle but are not considered being in a dangerous situation, such as illustrated in Figure 2. According to the type of vehicle and associated function, a precise danger zone shall be defined, and alarm shall be raised if detected people are outside.



Figure 1: Pattern of the background having an appearance close to the one of a profile pedestrian.



Figure 2: People localized around the vehicle. In this case, no alarm should be launched.

Finally, ADAS systems only based on TIR cameras are devoted to night operation mode, due to required high thermal contrast. Obviously, our system must be operational at day time, as well as in presence of hot materials such as asphalt.

Proposed solution

Considering the specificities of the off-road context mentioned above, a dedicated algorithmic solution has been developed. It is characterized by the following features:

- Foreground segmentation module: a stereoscopic acquisition is performed in order to extract pedestrian candidates. First, a ground area is computed in order to locate ROIs. This involves computing disparity map from stereo data. From this disparity, an extraction of 3D patterns is done.
- Candidate classification: the classifier is trained using dedicated video sets. For enhanced performance, video were acquired in real operational conditions. AdaBoost [8] algorithm has been used, based on optimized image gradient features.
- Tracking: all targets are tracked, no matter their nature, pedestrian or not. Algorithm is based on a Kalman filter, operating on the 3D position of the targets. Estimated location of the target is a tradeoff between prediction from the last position and observation in the considered frame.

Algorithms evaluation and validation

Algorithms have been unitary evaluated on defined tests sequences. The later ones are a combination of CEA and ARCURE proprietary sequences or isolated patterns, whose content is likely to be difficult for algorithms.

Finally, on the field assessment has been carried out thoroughly and feedback analysis is provided here under.

4 Our approach with regard to safety improvement around industrial vehicles

Our goal is to significantly reduce the occurrence of pedestrian-vehicles collisions on the work place. A total elimination of these collisions is unforeseeable for many reasons among which the unreasonable behavior of some drivers or pedestrians. Our approach is to assess the risk around each type of vehicle depending on its kinematics and on accident or near-miss accidents statistics around this specific vehicle.

Why near-miss accidents statistics are helpful in assessing risk around the vehicle? Studies by Frank E. Bird Jr. in 1969 and H. W. Heinrich in 1931 showed the linear relation between the rate of accident and the rate of near-miss accident (The accident pyramid model : ANNEX 1). The ratio near-miss accidents/serious accidents was measured between 60 and 100 depending on the configuration of the vehicle and the work place.

Our risk assessment considered the following vehicles: Large Excavators, Compact excavators, Medium to small loaders, Load and Hoal, Tandem rollers, Earth rollers, Graders, Dumpers, Bull dozers. For each vehicle, a danger zone was determined depending on the risk assessment. The danger zone is the area around the vehicle in which the presence of a pedestrian triggers an alert for the driver. The risk assessment around these vehicles showed that the accidents happen in the close vicinity of the vehicle and almost always just after a motion direction change. Consequently, the danger zone scarcely exceeds 6 to 7 meters from the vehicle. Having larger danger zones is practically counter-productive and finally gives the driver a misleading feeling of safety and confidence for the following reasons:

- large number of useless alarms, which diverts the driver's attention from real danger with lethal consequences on his behavior;
- wrong belief of the driver that considering the range of detection, he will have time to react in case of a presence of a pedestrian. As a consequence, the driver will tend to drive faster without controlling that the way is clear enough.

5 System composition and functions

BLAXTAIR is made of a Stereoscopic Sensor Head (120° HFOV), a Processing Unit, a screen, a Visual Alarm and the wiring (see Figure 4). A danger zone is defined in front of the Sensor Head with a pedestrian detection area and an obstacle detection area (Figure 3). The screen displays the image captured from the sensor head. When an obstacle enters the obstacle area or a pedestrian enters the pedestrian area, the visual alarm becomes red and the bell rings. Otherwise, there is no sound and the visual alarm is green. Any obstacle is localized with a precision of about 15cm in order to know whether or not it is inside the danger zone. Lying pedestrians or squatting pedestrians without reflecting vest are not detected. In case of default (hardware failure or poor visibility conditions preventing an optimal detection), the visual alarm becomes flashing purple and a diagnosis message is displayed on the screen.



Figure 3: Illustration of the danger zone.

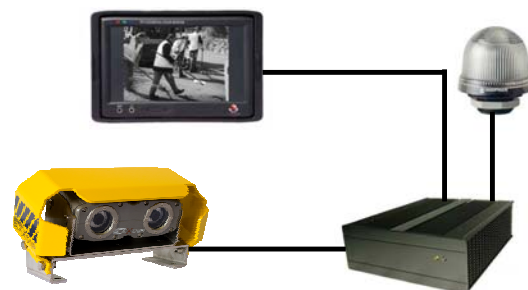


Figure 4: BLAXTAIR system composed of: a stereoscopic sensor head, a processing unit, a screen, a visual alarm and the wiring.

6 Achievements after 18 months in operation

More than 100 BLAXTAIRs were installed on various vehicles (Large Excavators, Compact excavators, Medium to small loaders, Load and Hoal, Tandem rollers, Earth rollers, Graders, Dumpers, Bull dozers, small, medium and large forklifts, guided machines, transship) and in various operational conditions (on public engineering and road construction sites, in factories and storage facilities, in quarries and underground mines). More than 100.000 hours were cumulated in operation. Almost all BLAXTAIRs were equipped with a data recorder enabling ARCURE to monitor BLAXTAIR's behavior and measure performance. These features were crucial when trying to assess performances of Hardware and Software as well as analyzing drivers' experience. Together with drivers feedback (through interviews), they were the sound bases on which functional and ergonomic improvements were defined and validated. Our performance statistics are based on these recordings.

Pictures of Figure 5 illustrate the type of environment Blaxtair is operated in, and show some vehicles equipped with Blaxtair.



Figure 5: Examples of working sites

Performances measured operationally are:

- Each time a standing pedestrian has entered the danger zone and a risk of collision occurred (vehicle not moving or moving toward the pedestrian), an alarm was raised to the driver.
- False alarm rate (alarm raised although no pedestrian is present in the danger area) is between 0.14 and 1 per hour depending on the environment.

Regarding the overall performance, the qualitative conclusions are:

- The driver's experience was significantly improved thanks to BLAXTAIR (less anxiety, focus on productive tasks). Among the more than drivers, no one rejected the system.
- The rate of near-miss accidents drastically fell, especially in close coactivity pedestrians/vehicle conditions (almost no near-miss accident).

Interviews put in evidence that Blaxtair is perceived by drivers and Safety and Health managers as equipment improving safety of pedestrians around dangerous large vehicles while improving productivity. The precise localization of the pedestrian is also highly appreciated and is considered as an advantage with respect to all other detection devices : even after months of usage, the driver reacts strongly to any alarm raised by the Blaxtair, since these alarms are scarce and the driver knows by experience it is reliable : alarm means 'danger'.

7 Conclusion and next steps

From computer vision algorithm perspectives, it was emphasized that algorithms originally designed for on-road car navigation have to be drastically reworked in order to efficiently address the context of off-road operation with industrial vehicles. Un-flat grounds, various human postures, distorted diagonally viewpoints, unpredictable pedestrian trajectories and required high localization precision are significant examples of specific constraints, the algorithms have to deal with.

From an applicative point of view, a relevant pedestrian detection should be based only on real accidents data and not on hypothetical risks that are not measured on the operational field.

BLAXTAIR is the first system of morphological recognition able to bring relevant information to the driver without disturbing him with useless alerts. Its robustness was proven under severe conditions (underground, night, dust, rain, etc.)

ARCURE is working on several fields of improvement:

Color: Exploitation of the color information for better discrimination in very cluttered environment (forest, waste recycling).

New fields of use: We are enlarging the scope of use of our image processing technology to additional fields of use: pedestrian and vulnerable road users 'detection in the vicinity of buses circulating in city centers, very accurate obstacle detection.

Increased integration and larger HFOV: The goal is to ease integration of Blaxtair, even in smaller vehicles. In some vehicles, it may also be interesting to enlarge the Horizontal Field Of View of the Sensor Head. The next Hardware generation should use larger field optics with adapted image processing algorithms.

8 REFERENCES

1. Geronimo D., Lopez A.M., Sappa A.D. and Graf T., *Survey of Pedestrian Detection for Advanced Driver Assistance Systems*, in IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.32, No. 7, July 2010, pp. 1239-1258.
2. Dollar P., Wojek C., Schiele B. and Perona P., *Pedestrian detection: a benchmark*, in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) , 2009, pp. 304-310.
3. Dollar P., Wojek C., Schiele B. and Perona P., *Pedestrian Detection: an Evaluation of the State of the Art*, in IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.34, No. 4, April 2012, pp. 743-761.
4. Viola P.A. and Jones M.J., *Robust Real-Time Face Detection*, International Journal on Computer Vision, Vol. 57, No. 2, 2004, pp. 137-154.
5. Walk S., Majer N., Schindler K. and Schiele B., *New Features and Insights for Pedestrian Detection*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2010.
6. Dollar P., Tu Z., Perona P. and Belongie S., *Integral Channel Features*, Proceedings of the British Machine Vision Conf., 2009.
7. Dollar P., Belongie S. and Perona P., *The Fastest Pedestrian Detector in the West*, Proceedings of the British Machine Vision Conf., 2010.
8. Freund Y. and Schapire R., *A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting*, Journal of Computer and System Sciences, Vol. 55, No. 1, 1997, pp. 119-139.
9. Bégard J., Allezard N. and Sayd P., *Real-time Human Detection in Urban Scenes : Local Descriptors and Classifiers Selection with AdaBoost-like Algorithms*, in Proceedings of the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), Workshop on Object Tracking and Classification Beyond the Visible Spectrum, 2008.

Application of RADAR technology to mobile machine-pedestrian collision prevention

David TIHAY
Institut National de Recherche et de Sécurité (INRS)
1 rue du Morvan – CS 60027
F-54519 VANDOEUVRE cedex
david.tihay@inrs.fr

Keywords: detection, mobile machine-pedestrian collision, radar

ABSTRACT

Prevention of mobile machine-pedestrian collisions is a problem involving many sectors of activity including manufacturing, building and civil engineering, handling of goods, waste collection or transport/logistics. Implementation of organisational measures and those aimed at improving driver visibility can prove insufficient for guaranteeing personal safety in certain work situations. Resorting to additional technical measures, such as installation of devices aimed at alerting the driver of the presence of a person near his machine, is therefore possible. These driver alerting devices can only be considered warning devices since they claim no safety component status. Several technologies (radar, ultrasound, radio-electric marker and vision systems) can be considered among available warning devices. The purpose of this paper is to present the results of INRS-conducted research into RADAR detection of persons. These reveal the advantages and limits of the technology, whether they are intrinsic to it or associated with the constraints inherent to the intended application. Subsequent experiments allowed us to illustrate radar technology's limitations, show the impact of certain environmental factors on device performance and identify their possible effects in relation to detection of persons. The results of these analyses allowed us to draw up a list of strong and weak points for these personal detection devices implementing RADAR technology. Based on these conclusions, this paper informs potential device users and prevention specialists of the functionalities offered by this technology. It provides a summary of RADAR technology-based personal detection device characteristics, enabling potential users to check whether these effectively correspond to their needs and are compatible with specific application constraints. Finally, the paper provides information on precautions applicable to implementation and usage, which are necessary to nominal operation of this type of warning system.

1 INTRODUCTION

Prevention of mobile machine-pedestrian collisions is a problem involving many sectors of activity in relation to which Institut National de Recherche et de Sécurité (INRS) assistance has been regularly sought for a number of years. Despite the equipment-related technical advances achieved, measures aimed at improving visibility at the driving station, organisational measures and training schemes implemented, the number of accidents involving the running over of persons working near mobile machinery remains high; over 200 such accidents were recorded in France during the period 2000-2010, of which more than half were fatal [1]. Today, new prevention actions have therefore been initiated not only by machinery manufacturers, but also by operators and prevention specialists. Their objective is to promote additional technical measures, such as proximity detection devices that warn the driver in case of the presence of a person near the machine. Different technologies now permit contactless detection of a person using either active or passive detectors, depending on whether energy is entirely supplied by the physical phenomenon or whether they supply themselves the energy required for measurement. Detection technologies envisaged within the scope of mobile machine-pedestrian collision prevention include laser, ultrasound, radio-electrical marker, vision and radar. This paper describes the work undertaken by INRS on radar technology and on possible application of this technology to preventing mobile machine-pedestrian collisions.

2 RADAR TECHNOLOGY

A radar is a sensor, which emits an electromagnetic wave into a portion of space and receives return waves reflected by targets present in the monitored space. Radar operation is mainly based on the echo principle and radio wave propagation characteristics. Radar technology's area of application is extremely wide. Use of radars in activity sectors as varied as medicine, aeronautics or the automotive engineering has prompted development of different types of radar. These can be classified according to various criteria, such as the type of observed target, the position of the emitter and the receiver, the frequency range or the type of signal. If the latter criterion is retained, three types of radar that are currently used as personal detection devices can be identified.

- Pulsed radars emit hyper-frequency signal pulses often at high power. Each pulse is followed by a period of silence required to observe an echo signal representing possible target presence. Measurement of the pulse time of flight allows the distance to the target to be deduced.
- Fixed frequency continuous wave radars, in which evaluation of the frequency difference between the emitted signal and the echo signal allows the target relative displacement velocity to be determined, but not the distance. These so-call "Doppler" radars are named as a tribute to the physicist C. Doppler, who discovered that a phase difference exists between the emitted wave and the received wave when the target is moving.
- Frequency-modulated continuous wave radars, in which continuous emission of the wave is associated with frequency modulation, usually based on a triangular function. When a moving target is present, the echo signal displays not only a phase difference, but also a time difference. These differences allow the relative displacement velocity and the radar-target distance to be respectively estimated.

Whatever the radar type and intended application, we should recall the regulatory framework, within which any usage of this type of system falls. In principle, when there is emission of hyper-frequency signals, as in the case of radars, these signals can only be emitted in compliance with ITU¹ recommendations. The ITU allocates frequency bands to "services" defined by category and by region. Each country must then implement this regulation by defining applications relating to each service and, in particular, its authorised maximum emission powers. Any prevention specialist or user wishing to implement a radar system must first ensure system compliance with current regulations.

3 RADAR APPLICATION TO PERSONAL DETECTION

3.1 System functional suitability

Prior to considering any selection criterion for such a system, quick analysis of the technical characteristics of selected radars indicates that their suitability for the function is only partial; radars are obstacle detection devices. They do not allow us to distinguish a person from the obstacles. Research has been conducted in this direction [4, 5], but the major problem encountered is the difficulty of identifying a marker that is representative of a human being. Identification methods used in aviation to identify an aeroplane, for example, turn out to be difficult to apply. R.C.S.² used to characterise a target's reflection capacity proves difficult to implement in cases in which the target is a pedestrian. In this technology, detection is based only on the presence of an echo signal, whose power is considered high enough to be representative of an obstacle, and not on the pedestrian presence.

The power received by a radar can be calculated using the following equation:

$$P_R = \frac{P_T \times G^2 \times \lambda^2 \times \sigma}{(4\pi)^3 \times R^4 \times L}$$

P_R = received power
 P_T = emitted power
 G = antenna gain
 λ = wavelength
 σ = RCS - Radar Cross Section
 R = radar – target distance
 L = loss coefficient

¹ ITU = International Telecommunication Union

² R.C.S. = Radar Cross Section

Quick analysis of this equation shows that many factors condition the received power:

- Some are intrinsic to technical options retained at design stage. The emitted power, antenna reception and emission gains and wavelength are technical characteristics, which are imposed during design by the intended application and need to be considered when calculating the received power.
- Others are related to the environment, in which the radar is used. In practice, wave propagation is affected by many energy losses caused mainly by atmospheric absorption phenomena. A weighting factor L was therefore introduced to take into account these phenomena. These energy losses become larger and larger as the radar – target distance increases.
- The last factor to be considered is the radar cross section (R.C.S.). For a given frequency, the radar cross section depends on the target size, geometry and composition material(s).

In the case of mobile machine-pedestrian collision prevention, the R.C.S. to be considered is that of the pedestrian. The radar cross section of a shape as complex as the human body cannot be modelled, so it is difficult to evaluate theoretically the impact of R.C.S. variation on the detection suitability of commercially available radars.

3.2 Devices tested

A number of suppliers offer warning devices based on radar technology, but few of these meet the regulatory requirements currently applicable in France. The experiments conducted at INRS were based on two systems identified as A and B. It should be noted that system B is unauthorised in France.

System A

The first identified system is a pulsed-type radar operating at a 5.8 GHz frequency. This comprises an antenna and a module remotely installed in the driver's cab, which uses a visual and acoustic alarm to inform the driver of target presence. This system claims to detect fixed and moving targets throughout the detection area.

System B

Unlike the system described above, system B is a frequency-modulated continuous wave radar. This also comprises an antenna operating at 10.525 GHz and a warning module to be located near the driver. This system detects neither fixed targets nor those moving away from the radar.

3.3 Strong points of radar technology

The main advantage of radar technology is its robustness in difficult environments. Unlike detection systems implementing optical technology, radar detection is possible in very poor lighting and visibility conditions. A radar can detect an obstacle as well in darkness as in front of a very strong light source. Tests [2, 3] show that radar detection is also possible in an outdoor environment subjected to bad weather featuring rain, fog or snow. Presence of dust and even mud on the detector does not prompt false alarms.

It should also be noted that the tested systems are relatively easy to install. Compliance with fairly unrestrictive supplier precautions is all that is required. Such systems require neither adjustment nor calibration, which greatly reduces their installation time and the risks of mistakes during commissioning.

3.4 Highlighting of limitations

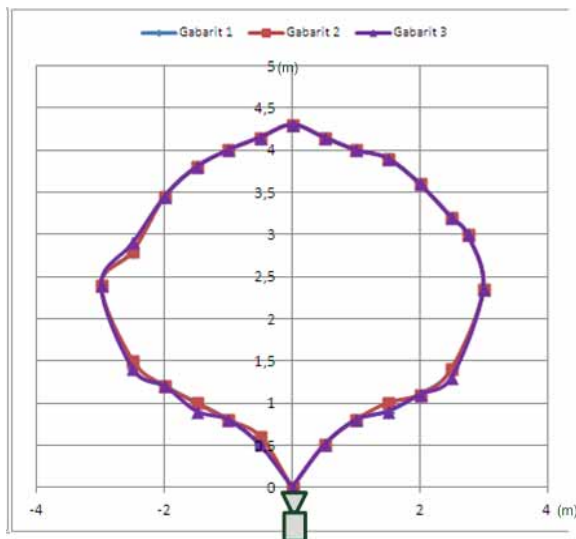
When applied to personal detection, variation in target R.C.S. is reflected by the variety of pedestrian sizes, postures, attitudes and positions in the detection area as well as movements. Test target selection, initially oriented towards using a manikin, rather than the trihedral corner or sphere-shaped targets conventionally used for radar characterisation, quickly revealed its limits.



Figure 1. Choice of target type

As Figure 1 effectively illustrates, presence only of a manikin wearing work clothing triggers no alarm, while presence of a pedestrian of the same height prompts detection. Impact of the type of material composing the target on functional suitability is therefore significant. A human body, essentially composed of water, has better reflective qualities than those of a manikin essentially composed of plastic.

As Figure 2 shows, tests were conducted on pedestrians with different morphologies without any notable difference in the detection area dimensions being observed.



All tests were conducted on a 171 cm tall pedestrian weighing 67 kg, based on the installed radar configuration (1 m high) and the insignificant influence of the target corpulence on system performance.

Figure 2. Impact of pedestrian size on detection area

Note. This first experiment highlighted the difficulties involving test target selection, when using radars.

Target complexity, such as a pedestrian, does not depend only on its type of clothing materials, but also on the many possible postures within the scope of a work activity. Various postures were envisaged, in particular those for which the emitted wave is found to be minimised. Several postures enabled us to reveal faults with both radar systems, such as squatting or side-on positions. Figure 3 illustrates an instance of no detection, when a pedestrian is standing in the theoretical detection area.



Figure 3. No detection in target presence

This phenomenon is due to the fact that the potential reflecting area is small and that wave reflection is more diffuse on the shoulders and legs than on the torso. In this case, the energy received is insufficient to ensure detection (Figure 4).

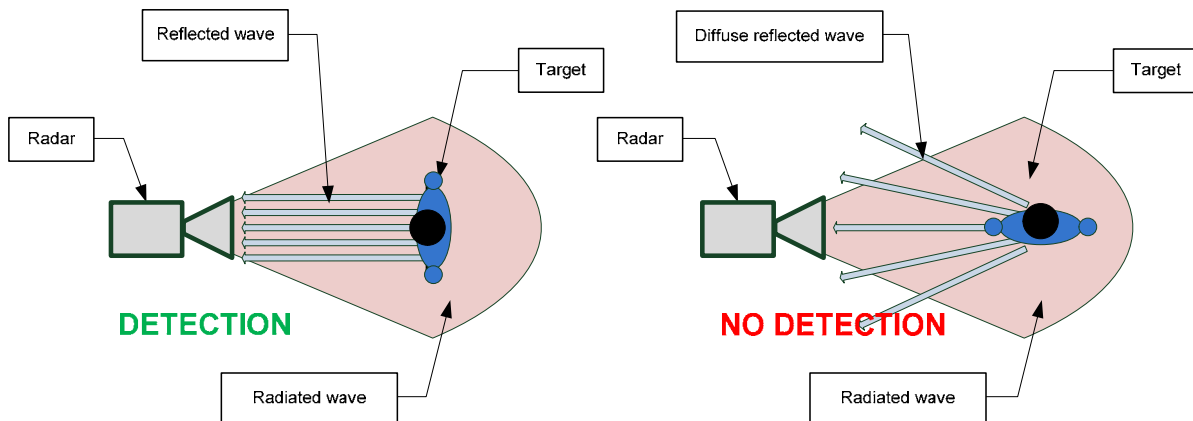


Figure 4. Impact of target area on detection

This phenomenon was observed for both radar systems and several targets and it therefore causes systematic “non-detection”, which can be reproduced throughout the theoretical detection area. Diffuse reflections caused by a pedestrian standing side-on also prevents detection and may lead to masking effects. In Figure 5, not only is target 1 (positioning side-on at approximately 1 metre from the radar) not detected, but it creates a shadow represented by a shaded area in the figure, in which target 2 is positioned and not detected either.

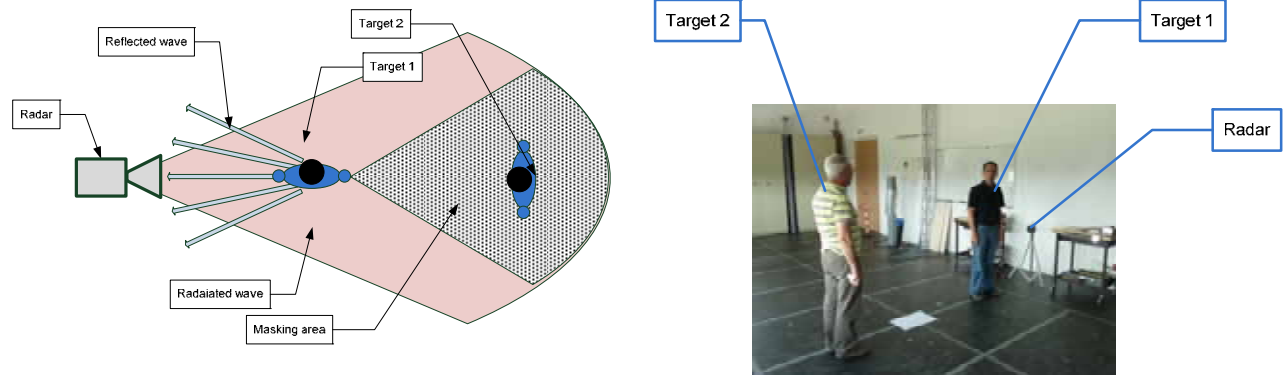


Figure 5. Masking phenomenon

We were able to observe other situations causing instances of pedestrian “non-detection”. Unlike the previous envisaged case, in which reflection was diffuse and the target area too small, the following situation involves specular reflection and a target area corresponding to a pedestrian face-on. The pedestrian is performing a handling operation, in which he has to handle a 1m² steel plate. Plate orientation is found to cause a wave deviation phenomenon and this leads to no detection (Figure 6).

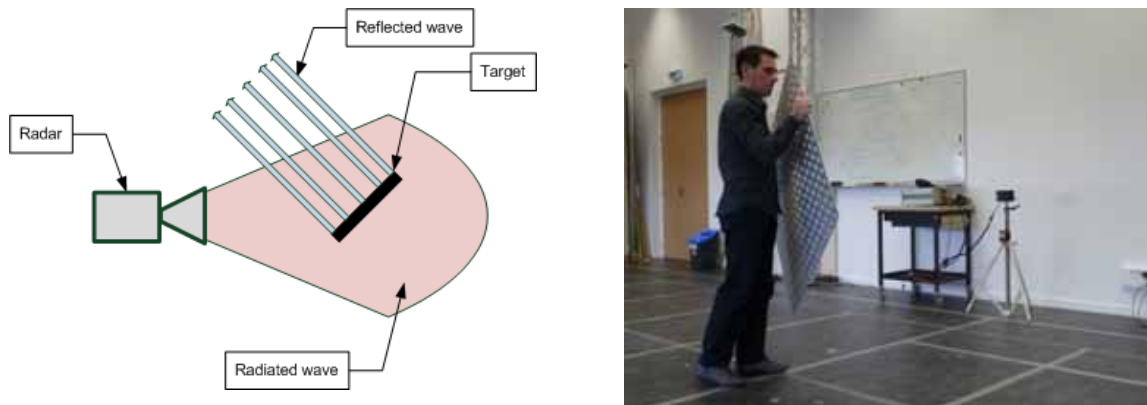


Figure 6. Deviation phenomenon

3.5 Usage precautions

Given the limitations observed during the experiments, it appears that user training is essential for implementing and using this type of system within a mobile machine-pedestrian collision prevention framework. These systems are only warning devices and their use in no way exempts one from complying with safety regulations. They must be installed in compliance with the manufacturer’s recommendations, taking care to ensure that their chosen positioning on the mobile machine does not curtail driver visibility or expose the system to risks of damage, such as crushing during a reversing movement, for example. Periodic inspection and checking is essential to ensure proper radar system operation.

4 CONCLUSIONS

Analysing the technical characteristics of existing radar systems reveals that their contribution to the “personal detection” function is only partial since they are, in fact, only obstacle detection systems. Obstacle presence in a mobile machine environment will cause unwanted detection and will discredit the system in the long term.

Functional losses have been observed and there is no reliable detection area, in which a pedestrian can be systematically detected irrespective of his/her attitude, position or activity. The experiments conducted reveal systematic non-detection in two different type (pulsed and Doppler) radar systems, reducing the theoretical detection area to nothing. We therefore need to recall that resorting to radar detection systems can only be envisaged as complementary to implementing organisational measures and those aimed at improving mobile machine driver visibility.

Radar systems are not safety components and their behaviour, when confronted by a possible failure, is not guaranteed. They must therefore be considered warning devices and special precautions must be adopted in relation to both selection and usage of this type of device. First and foremost, adequacy between a need and an envisaged product must be checked, users must be informed of the limitations of these systems, a systematic inspection procedure for detection function availability must be drawn up and regular cleaning of the device must be ensured, when it is used in a severe environment.

5 REFERENCES

1. Marsot J., Charpentier P., Tissot C., *Collisions engins-piétons : Analyse des récits d'accidents de la base EPICEA*, Hygiène et Sécurité du Travail, ND 2318, 4^{ème} trimestre 2009, 217, pp. 23-32.
2. Yamauchi B, *Fusing ultra-wideband radar and lidar for small UGV navigation in all-weather conditions*, Proc. SPIE 7692, 2010.
3. Ruff M. Todd, *Evaluation of devices to prevent construction equipment backing incidents*, national institute for Occupational Safety and Health, 2004.
4. Naoyuiki Yamada, *Radar cross section for pedestrian in 76 GHz band*, R&D Review of Toyota CRDL, Vol. 39, N°4.
5. Yarovoy A.G., Lighthart L.P., Matuzaz J., Levitas B., *UWB radar for human being detection*, IEEE A&E systems magazine, 2006.

Systematic failures & functional safety

(a challenge for the selection and application of protective devices)

Otto Görnemann
SICK AG, Industrial Safety Systems, Erwin Sick Straße 1,
D-79183 Waldkirch, Germany
Tel. +49 (0) 7681 202-5420, Fax +49 (0) 7681 202-3628, E-mail Otto.Goernemann@sick.de

Keywords : Functional Safety, systematic failure, safeguard selection, risk reduction contribution

Systematic failures & functional safety
(a challenge for the selection and application of protective devices)

Abstract

The standardization of the application of functional safety machinery has not only changed the approach in the design of safety related parts of control systems. It also has created a new challenge for the adequate selection and integration of protective devices. The most critical effect appears when the application of ISO 13849-1 is reduced to the mere use of numbers and calculations ignoring proper consideration of systematic failures. This becomes reflected more and more not only in inadequate referencing and application of functional safety in standards, especially in C Type standardization groups but also in unrealistic demands of large machinery users. The application of sensors to detect the approach or the presence of a person in a hazardous area in order to trigger a protective function is a typical example of this problem.

The contribution presents the above mentioned problems, showing typical examples of neglecting a “systematic approach”. Based on the guidance of well proven B-type Standards the contribution presents an example for a method for the selection of protective devices which takes into account this systematic approach. Additionally the contribution presents a standards relationship chart to support C-Type standardization writers on considering the right standards and requirements for protective devices.

Selection of protective devices

The revision of the old ISO 13849-1 (~EN 954-1) in 2006 takes into account the probability of failure of the components, the measures for fault detection and fault resistance, the avoidance of common cause and systematic failures, the quality of the related software and the overall functional safety management. For the selection and proper integration of adequate protective device the consideration of the systematic approach is a critical part. While ISO 13849-1 emphasizes in the effects of supply voltage variations and program errors and defect sequences, the physical effect of the environment on a device and the physical ability of the device to perform the intended function under this parameters is not properly considered.

Either if it is a pressure sensitive sensor like a safety mat or a safety edge, or it is an optoelectronic sensor like a safety light curtain or a laser scanner, the effect of the physical and environmental parameters (e.g. aggressive atmospheres, strong extraneous light sources, dust, vibration, falling objects) needs to be carefully considered in order to ensure the intended function, in this case a reliable detection of an endangered person. For this reason the B-2 Type Standards, provide specific requirements intended to cover potential risks related to systematic failures. The question arises if systematic failures are properly addressed in these standards

Consideration of systematic failures in Standardization.

Example: requirements for ESPE in IEC 61496

Unlike simple control systems, such as electronic safety switches, additional criteria need to be taken into account for electro sensitive protective equipment. These include the required detection capability that results from the optical active principles and that is specified in the series of standards, IEC 61496.

Part 1 of the IEC Series 61496 contains the general requirements for ESPE, while the other parts state or will state in the future the generic requirements and verification procedures for AOPD's (Active Optoelectronic Protective Devices) AOPDDR's (Active Optoelectronic Protective Devices using Difuse Reflection) and VBPD's (Vision Based Protective Devices). Part 1 states that ESPE shall not only comply with functional requirements but also with requirements for design and environmental aspects, While the design requirements are intended to reduce the influence of common cause, the environmental requirements are mostly aimed to avoid the influence of systematic failures. In addition the standard also states the relationship between the different types of ESPE and the maximum PL or SIL which can be reached by functions applying these devices. The significant functional safety requirements for ESPE stated in subclause 4.1.3 describe the required structures, which in fact are identical to those of ISO 13849-1. In addition subclause 4.1.3 refers to sub clauses 4.2.2.3 to 4.2.2.5 for the requirements of fault detection and corresponding reactions depending of the different ESPE types.



Figure 1 - Person intrusion detected

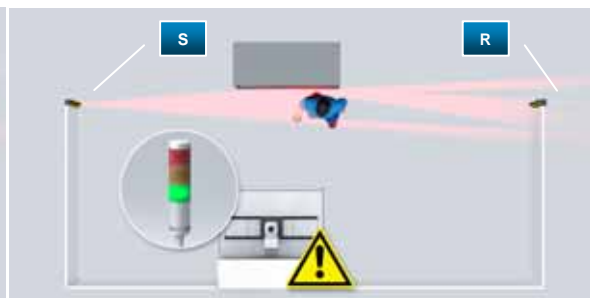
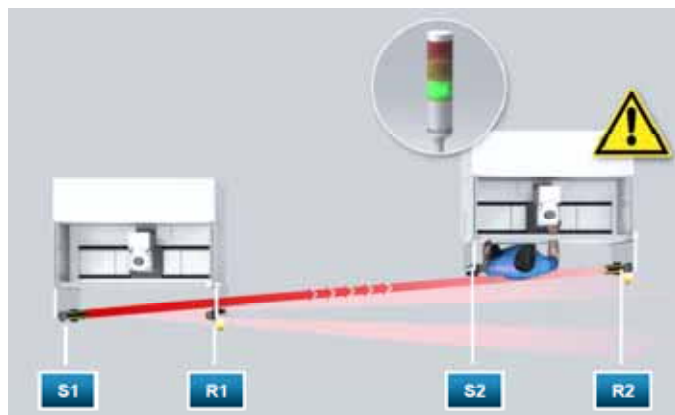


Figure 2 – Person intrusion not detected

Figures 1 and 2 show that large EAA may lead to a detection failure. While in figure 1 the person entering the hazardous area interrupts the AOPD beam, in figure 2 while the center of the beam is interrupted the side lobes are not, and their reflection at the surface of the container placed nearby reaches the receiver, this avoiding the proper detection and rendering the protective function inoperative.

Figure 3 shows similar a similar problem which may occur if several AOPD's are operated in close proximity to each other, the sender beams from the system (S1) can reach the receiver of the other system (R2). A person in the hazardous area may interrupt the beam of the first Sender (S1) but the corresponding



receiver may be alighted by the second Sender thus leading to the loss of the protective function

Figure 3 - Dangerous interference

Part 2 of the IEC Series 61496 contains the generic requirements for AOPD's. Subclause 4.1.2.2 deals with the optical performance corresponding to the detection reliability. AOPD shall be designed and constructed to :

- limit the possibility of failure to danger resulting from external reflections
- limit the misalignment for normal operation
- limit the possibility of malfunction during exposure to extraneous light in a specific frequency range
- Control the size of the emitter beam in order to minimize any negative effects on other equipment.

These requirements can be achieved by ensuring that the effective aperture angle (EAA) of each emitting and each receiving element does not exceed certain values given in the standard or other technical alternative means for the restriction of the EAA leading to an equivalent performance. The restriction of the maximum aperture angle of the optics of type 4 devices to 5° reduces the probability of the non-detection of objects due to reflection effects (optical bypassing) and thus also the probability of a potentially dangerous failure. For the avoidance of interferences which may lead to the loss of the protective function. Subclause 4.3.5 of Part 2 states requirements to prevent interferences caused by light.

The ESPE shall continue in normal operation when subjected to

- incandescent light;
- flashing beacons;
- fluorescent light operated with high-frequency electronic power supply.

The ESPE shall not fail to danger when subjected to

- incandescent light (simulated daylight using a quartz lamp);
- stroboscopic light;
- fluorescent light operated with high-frequency electronic power supply;
- for a type 4 ESPE, radiation from an emitting element of identical design.
- Misalignment (mainly related to nearby reflective surfaces)

In addition to these optical requirements the standard also states other requirements. Nevertheless users of such devices or members of C-Type standardization committees cannot assume that devices according to these standards provide enough consideration of the systematic failures in a particular application, since the standards define different types with different requirements. As a result, users have to compare the requirements of the different types with the foreseeable characteristics of the machine and the machine environment to select the right device. This does not seem very realistic, due that the standard is mainly aimed to the manufacturers of such protective devices.

Consideration of systematic failures in future standardization.

Example: evaluation of DC in series connections of potential free contacts

In Safety functions according to Category 2, 3 and 4 of ISO 13849-1, a single fault on SRP/CS should be detected by the logic unit (e. g. logic controller, safety relay unit, integral diagnostic function). If guard interlocking devices using position switches with potential free contacts are

connected in series in a redundant SRP/CS, a single fault will not lead to the loss of the safety function and will be detected. However it is foreseeable that more than one movable guard will be opened e. g. due to subsequent fault finding procedure.

Due to the serial connection, the operation of other switches can reset the detected fault in the logic unit, masking the initial fault, thus allowing the interlocking circuit to be reset. As a result the operation of the machine is possible while a single fault is present in the interlocking circuit. Certain assumptions can be considered as realistic. This allows the evaluation of the ratio between detected dangerous failures and the total dangerous failures. Based on this consideration a TR – Technical Report is being drafted to support the designer of SRPCS during the design.

Figure 4 shows the development of a single fault masking due to the operation of other movable guards which have their switch contacts connected in series.

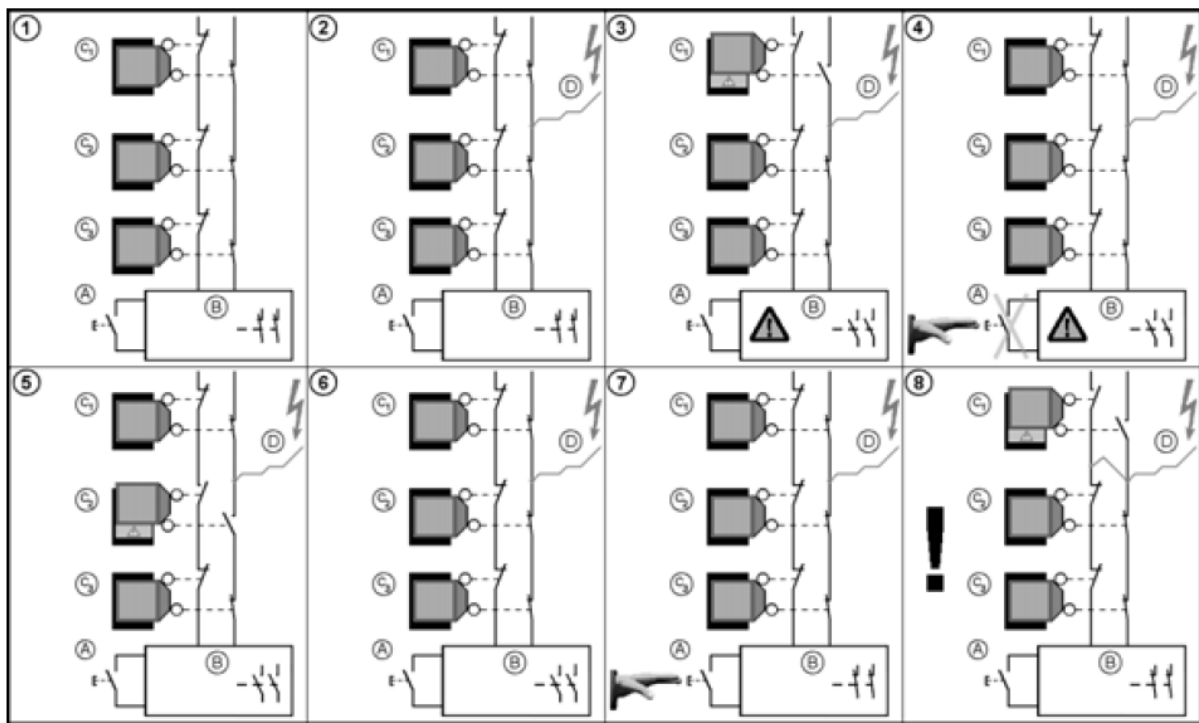


Figure 4 – mechanism of fault masking in a series connection of potential free position switches

Key

- | | | | |
|------------|--|---|------------|
| A | Reset device | B | Logic unit |
| C1, C2, C3 | Interlocking devices with potential free contacts position switches | | |
| D | Initial fault (Due to a cable fault, the cross-circuit to an external voltage renders the second contact of the first switch inoperative.) | | |

- | | |
|---|--------------------------------|
| (1) Normal situation | (2) Initial fault occurs |
| (3) Actuation of the first guard | (4) Fault detection & Lock-out |
| (5) Actuation of the second guard while fault-finding | |
| (6) Actuation & closing of the second guard originates a correct signal therefore masking the initial fault | |
| (7) Reset of the logic unit allows the machine operation even while a single fault is present | |
| (8) A following fault (further damage of the cable) leads to the loss of the safety function. | |

The actual draft of the intended TR evaluates the impact of these series connections taking into account the main elements; redundant signal evaluation, cabling structure and likelihood of the masking event.

On redundant channel circuits, different designs may be used to detect certain faults. In designs of channels with the same polarity the SRP/CS (logic unit) evaluates redundant signals which have the same (control) voltage. These designs do not allow the detection of short circuits to the control voltage or cross circuits between the channels, while short circuits to ground do not lead to a dangerous fault. Designs of channels in which the SRP/CS (logic unit) evaluates redundant signals with inverse polarity can be used to detect cross circuits between the channels, but they can not detect short circuits of a channel signal to their corresponding voltage, which can lead to a dangerous fault. Some SRP/CS (logic units) evaluate redundant signals from contacts fed with dynamic signals (test pulses). This design allows detecting short circuits of a channel signal to the control or ground voltage. If different dynamic signals (test pulses) are used the SRP/CS (logic units) are also able to detect cross circuits between the channels.

The cabling structure is another key factor which affects fault avoidance. Star cabling is a cabling structure where every interlocking device position switch is wired with a single cable to the electric cabinet or enclosure in which the SRP/CS (logic unit) which evaluates the redundant signals of interlocking guards is installed. Branch (trunk) cabling is a cabling structure where a single cable from the electric cabinet is wired to the first position switch and from this position switch to the next, and so on, until the last position switch and the resulting signals are wired the same way back to the electric cabinet. In star and branch (trunk) cabling, short circuits to the control voltage and cross circuits of contacts are possible if the cables are not protected from external damage. Loop cabling is a cabling structure where a single cable from the electric cabinet is wired to the first position switch and from this position switch to the next, and so on, until the last position switch while the signals return to the electric cabinet in a separate cable. Loop cabling avoids cross circuits of contacts and the most short circuits.

Cabling can be considered as protected if it is permanently connected (fixed) and protected against external damage, e. g. by cable ducting, armouring, or within an electrical enclosure according IEC 60204-1 (See ISO 13849-2:2003 Annex D4). In addition, if the cables used to wire the position switches include wires with additional voltage intended for the supply of other elements, (e.g. pilot lamps) the possible short circuits to the interlocking signal wires need to be considered.

The probability of masking faults is dependant on several parameters that should be considered including:

- Number of interlocking devices wired in series;
- Actuation frequency of each movable guard;
- Distance between the movable guards;
- Accessibility of the movable guards;
- Number of operators.

While distance and accessibility are difficult to quantify or qualify, the intended opening frequency and the number of connected interlocking devices can be used to assume a certain probability of fault masking.

Number of frequently used movable guards ^a		Number of additional movable guards	Fault masking probability
0	+	2 to 4	low
		5 to 30	medium
		> 30	high
1	+	1	low
		2 to 4	medium
		5 to 30	high
		> 30	high
> 1	+	>= 0	high

^a If the frequency is higher than once per hour.

Table 1 shows the fault masking probability and the maximum achievable DC. The number of additional movable guards can be reduced by one line for each of the following conditions are met

- when the minimum distance between any guard is more than 5m
- when all additional movable guards are only non directly reachable

It is surprising that the relevant standard IEC 60204-1 does not give guidance on this issue. Nevertheless the masking likelihood depends mainly on application parameters. The draft of the intended TR considers the above mentioned factors and their combination. The example table 2 shows the maximum achievable DC for cabling using multicore cables with wires carrying additional U+ voltage.

Unprotected multicore cables with wire(s) carrying additional +U voltage											
Switch arrangement	cabling	Redundant channel signal type									
		same polarity			inverse polarity			Dynamic signals			
single switch (two contacts)	Branch	none	low	mid	none	low	mid	low	mid	mid	Resulting Maximum DC
	Loop	none	low	mid	none	low	mid	mid	mid	mid	
double switch (single contact)	Branch	none	low	mid	none	low	mid	low	mid	mid	
	Loop	none	low	mid	none	low	mid	mid	mid	mid	
		high	mid	low	high	mid	low	high	mid	low	
Fault masking probability											

The draft of the intended TR also for cabling using multicore cables without wires carrying additional U+ voltage and for protected cabling. With the method presented in the draft of the intended TR the designer of an SRPCS gets not only the guidance to evaluate the impact of masking in safety related control circuits but also enough guidance to improve his design.

Approach for the consideration and evaluation of systematic failures.

As described before, the selection and integration of protective devices shall be done with utmost care and consideration of systematic failures. However, the designer of a machine which integrates a protective device or the expert in a C-Type standardization group has to be aware that applicable B-Type standards not always contain complete guidance for this task, although many of these standards are subject of cyclic revisions.

When safety functions have to be designed and validated a practical method according to the following flowchart, can be used to evaluate possible systematic failures.

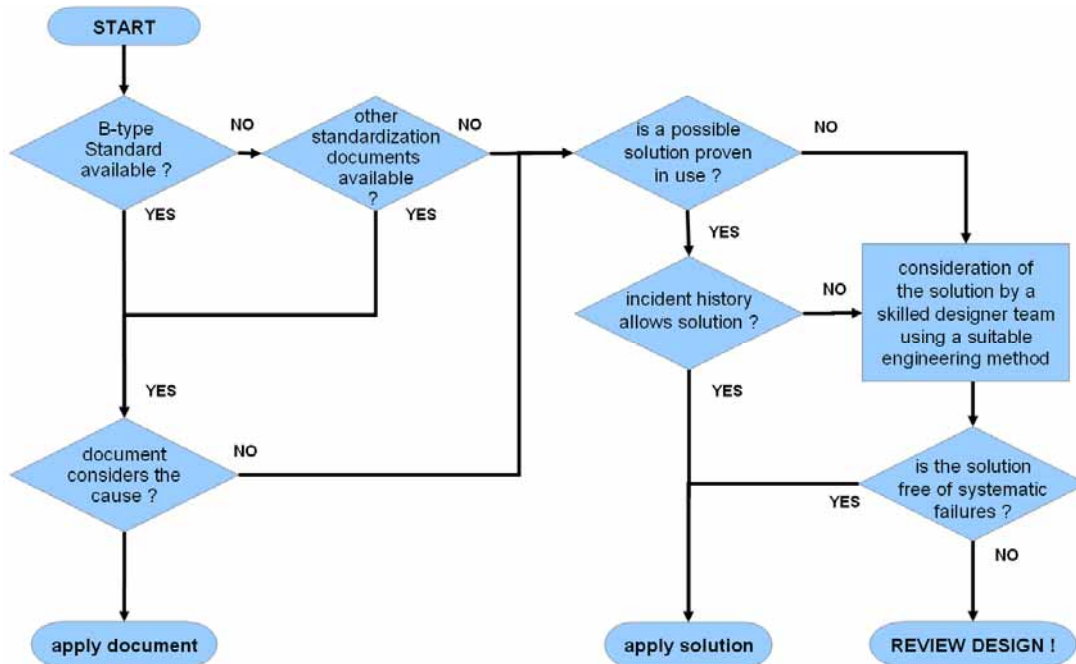
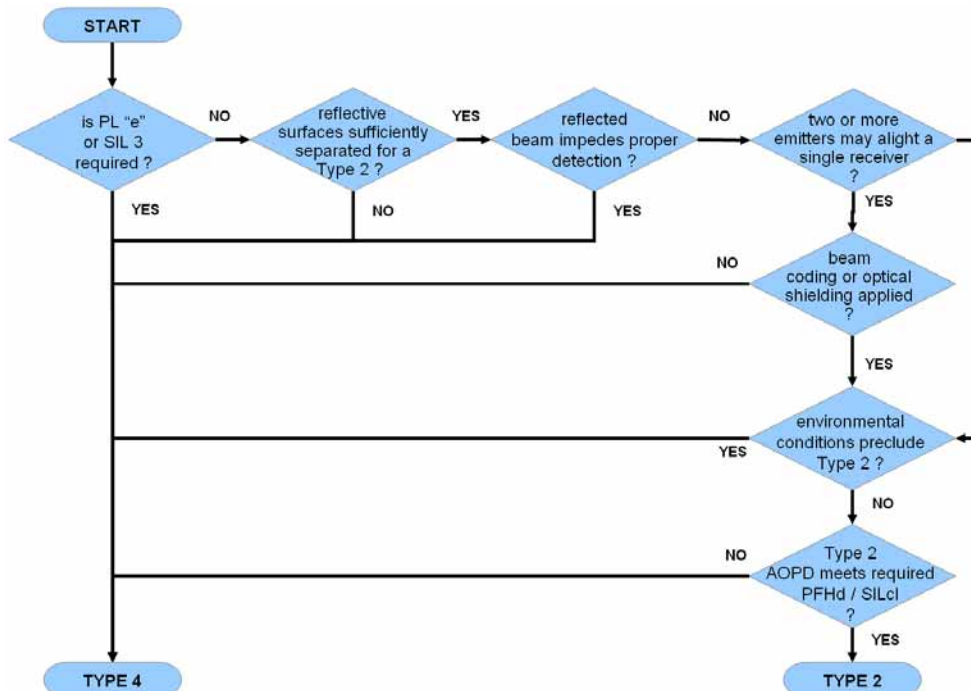


Figure 5 – Flowchart for the generic consideration of systematic failures

It may be necessary to develop single evaluation or selection methods for any particular kind of protective device or for other sensors used in safety related functions (e.g. muting sensors, operations mode sensors etc.). The next figure shows, as an example, a flowchart which can be used to select the suitable AOPD for a certain application taking into account systematic failures.

Figure 6 – Flowchart for the selection of an AOPD Type considering the application and systematic failures



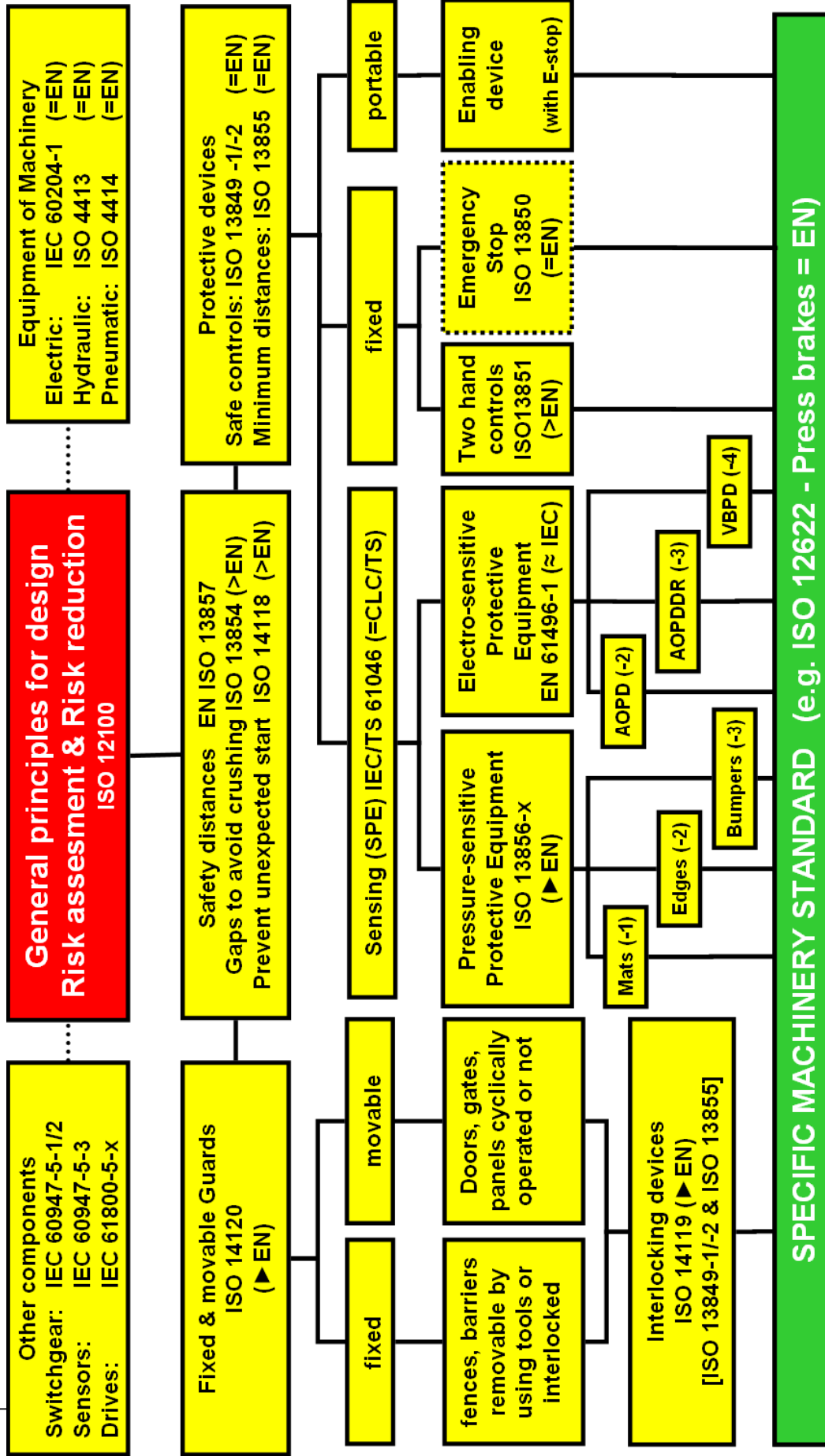
Similar tools as those used for risk assessment (graphs, matrices or numerical methods) can be used to evaluate some conditions or parameters, thus allowing a consistent consideration of systematic failures during the engineering process. Nevertheless, a team approach is indispensable during the assessment of solutions which are not covered by standards, other documents or have not been proven in use.

Conclusion

During the selection of protective devices or other sensors used for safety functions, the consideration of possible systematic faults shall be done carefully. The user shall be aware that even in the case of existing International standards these may not offer sufficient guidance or consideration. In addition, these standards do not always answer the question how much an SRPCS (or a device) contributes to the risk reduction required by the application. This may sometimes lead to the determination that a required Performance Level cannot be reached with a particular component or technology. In order to deal with this situation the user needs to apply basic physics knowledge to ensure that systematic failures do not lead to a failure of the intended safety function. A team approach and the use of adequate methods is helpful, while a basic knowledge of the mentioned Standards (see Figure 7) is imperative.

Otto Görnemann
SICK AG
Waldkirch / Germany

Figure 6



Spectral Light Curtains - Novel Near-Infrared Sensor System for Production Machines

Holger Steiner, E-mail: holger.steiner@h-brs.de

Oliver Schwaneberg, Email: oliver.schwaneberg@h-brs.de

Sebastian Sporrer, Email: sebastian.sporrer@h-brs.de

Jannis Konrad, E-mail: jannis.konrad@h-brs.de

Norbert Jung, E-mail: norbert.jung@h-brs.de

Institute for Safety and Security Research, Bonn-Rhine-Sieg University of Applied Sciences, Sankt Augustin,
Germany www.isf.h-brs.de

KEY WORDS optical safeguard sensor, skin detection, light curtains

Abstract:

At previous SIAS conferences, we presented a novel opto-electronic safety sensor system for skin detection at circular saws jointly developed with the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA). This work now presents the development results of our consecutive research on a prototype of a sensor system for more general production machine applications including robot workplaces. The system uses off-the-shelf LEDs and photodiodes in combination with dedicated optics and a microcontroller system to implement a so-called spectral light curtain. The idea is to extend the established safety light curtain functionality by adding a reliable surface material classification of objects intersecting with the light beam. This allows to distinguish workpieces or tools from the hand of an operator, for example. Whereas the feeding or unloading of workpieces and tools to or from a machine without engaging the safety sensor can be very useful for a flexible operation of the machine, the intrusion of a hand in a hazard area of the machine must be detected. State of the art safeguarding equipment uses a technique known as muting to realize this functionality. However, typical muting implementations require a well defined model for the machine operation, including exact parameters about timing, position, orientation, shape and size of the fed workpieces and tools. These limitations can be minimized or even abandoned by means of the proposed novel sensor system. In addition to the surface material classification, the distance between the surface and the sensor is estimated by triangulation. Besides an improved reliability of the classification, this allows for further flexibility for the safety function. Moreover the system can be trained to suit different applications by machine learning techniques. First tests of the safety sensor system in practical applications were already successful.

1. Introduction

Manually-fed machines are often equipped with potentially dangerous moving parts that are difficult to shield off from the limbs of the user. Therefore, contactless, fast and reliable detection of human limbs at manually-fed machines is a desirable feature for safety applications. For many years light curtains (also referred to as light grids) have been used as hand-protection- or access-control-systems in production and manufacturing environments – including automatic placement machines, palletizing systems, mechanical presses or textile machines. They span a two-dimensional safety surface in front of the danger zone. Breaching the safety surface leads to a warning signal or an immediate machine stop. In these cases productivity and safety might conflict with each other: Safeguards have to respond with sufficient reliability, but should not affect productivity by unnecessary machine stops. Movements of workpieces or tools into the safety zone should be allowed, but the operation has to be interrupted immediately if extremities – even wearing protective clothes – penetrate the zone. On the one hand, high safety standards may lead to frequent false alarms and increased machine down times. On the other hand, high productivity can compromise safety. A reliable and quick distinction between safety zone violations caused by human limbs from those caused by workpieces or tools will be a major improvement. This paper offers an alternative and presents an active multispectral scanning sensor capable of contactless classification of an object's surface material in order to distinguish between different kinds of materials and human skin.

2. Operation principle

Already in 1955, one of the first investigations on the NIR spectrum of human skin was published by Jacquez et al. [1]. They present a comparison of very different skin tones and state that: ‘...the reflectance of human skin above 1.2 μm is primarily the reflectance of a scattering component mixed with water. The reflectance is dominated by the absorption bands of water’. In more recent work it has also been suggested that the NIR spectrum is of special interest for human skin detection. The domination of the absorption bands of water in the reflectance spectrum of human skin is the key feature in this context, while variations related to different skin tones are comparably small. This renders the NIR spectrum very interesting for the reliable detection of any human skin.

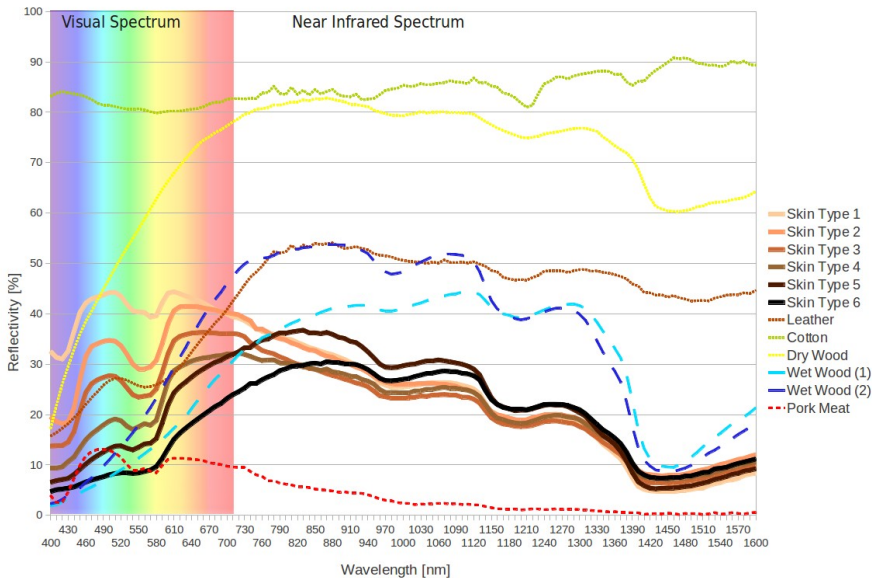


Figure 1: Remission spectra of different materials compared to human skin

As example for the skin properties figure 1 presents remission spectra of 6 samples, ordered from very light (1) to very dark (6) skin tone according to the categories proposed by Fitzpatrick [2], compared to different materials relevant here. Within the near infra-red (NIR) spectrum, the shape of the curves for human skin are identical for all skin types, but differs significantly from those of other materials. Even typical workpieces or tool materials can also be discriminated from each other by their respective shape within the NIR spectrum. By using spectroscopy in the NIR spectrum, these characteristic features could be easily measured. However, spectroscopy in its normal application is not suited for the use in safeguarding equipment on machines. Beside the high cost for the instrument the measurement procedure is too slow and very susceptible to interfering light.

Stating the mentioned basis the problem that has to be solved in a technical safeguarding system is how to measure the spectral signature in the actual application on the machine reliably over a larger distance facing extraneous light. To overcome these problems, Institute for Safety and Security Research of the Bonn-Rhine-Sieg University of Applied Sciences (BRS-U) ran several research projects jointly with the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) on the problem of human limb detection for safeguarding equipment [4,8,9,10]. The extraction of the so-called "spectral signatures" from the characteristic shape of the remission spectra like a "fingerprint" solves the problem. The spectral signatures have to be measured with an active optical sensor system and consist of a small number of remission intensities at different narrow wavebands, which represent the most important features to distinguish the given materials. Only three well-chosen wavebands are already sufficient to reliably distinguish skin from wood, for example. An extension to more wavebands is easily possible to enhance the performance further.

On previous SIAS conferences we have presented the first implementations of the sensor system for bench saws and a push-button sensors [3,5,6]. The next goal are sensors for more demanding applications with higher distances and also allowing the use of gloves by the workers. We call these sensors Spectral Light Curtains (SLC). For the spectral light curtains the combination of active NIR-sensors and an optimized optical setup supplemented by an intelligent data processing system allows the safe distinction of materials over a distance of about $L=1\text{m}$ with a resolution of about $S=30\text{ mm}$ between adjacent beams. This is considered as "approximately finger-safe". The light curtain is realized by means of a light barrier based on a two-way transmission measurement with sensor units containing both

transmitter and receiver modules on each side. It works similar to common light curtains while the beams are not intersected by an object. As soon as a beam intersection is detected, the proposed spectral light curtain performs immediately a remission measurement at the (one dimensional) position of the object from both sides and classifies the object's surface material. Depending on the application, specified actions can be performed if a specific material is detected, for example a safety function can be triggered if human skin is detected. The principle of the SLC system is illustrated in figure 4.

Using a network of such sensors, large danger zones can be monitored. If the safety zone is violated by human extremities or illegitimate materials, a warning signal is issued or the machine is stopped immediately. An electronic control unit based on a microcontroller with a reliable interface provides automatic calibration, self diagnosis and error correction for the whole system. Efficient classification algorithms and machine learning techniques guarantee a flexible adaptation to different applications and a fast reaction time of below 5ms.

3. Sensor Design

An ideal multispectral point scanning sensor should emit a light beam with a smaller diameter than the minimal width of the objects that must be detected reliably, e.g. the width of a human finger. Applicable standards specify the width of the smallest finger as $DF=11\text{mm}$, therefore the diameter of the received beam must not exceed a diameter of $DB < 11\text{ mm}$ at any point within the specified range of operation to allow a complete coverage of the beam by a single finger. The beam should be generated from a single point source with switchable wavebands that is positioned exactly at the focal point of a lens. As shown in figure 2, its receiver should be positioned side by side to the transmitter. The separation of the transmitter's and receiver's optical paths results in a variable angle of incidence of the reflected light to the receiver. This variance can be used for distance estimation based on the well known triangulation principle, if the receiver is able to measure the incidence angle with sufficient accuracy.

An ideal sensor should have a sufficient signal-to-noise ratio by design and measurement artifacts must be minimized. To achieve this, the system has to create a narrow and sharply contoured beam with a divergence of ideally 0° .

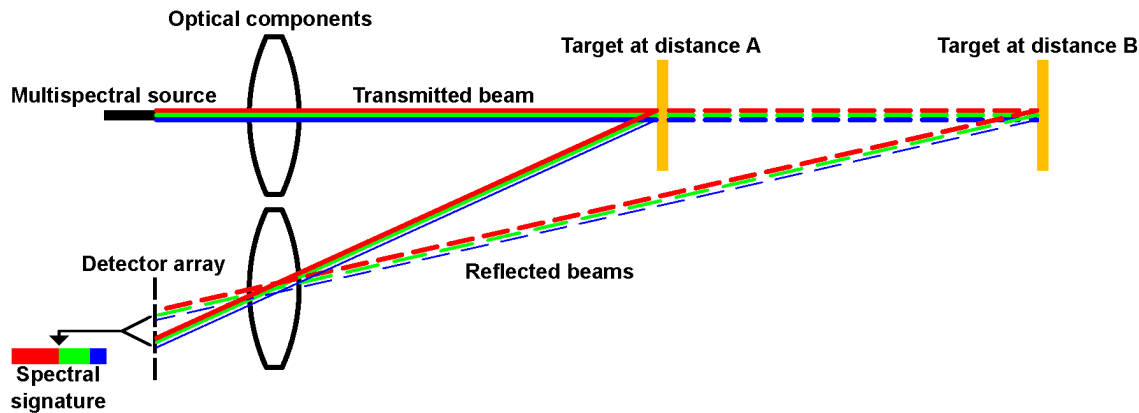


Figure 2: Optical setup of SLC-Sensor

In contrast to an ideal sensor, an actual LED-based sensor has to deal with the problem that real LED chips have a fixed peak wavelength for each type and emit radiation with a spectral Full-Width at Half-Maximum (FWHM) of typically $\Delta\lambda \approx 100\text{ nm}$. Moreover, different LED chips have to be placed close to each other and the optical paths differ the more an LED is placed away from the focal point of the lens. Therefore, the number and selection of wavebands is limited and choosing a well-suited combination is crucial for the sensor's performance. [10]

In order to find the best possible combination of up to four LEDs that still delivers a good performance, spectrometer measurements of about 1000 skin samples from more than 300 persons, 75 samples of wood at different moisture levels, and about 200 further samples of different materials (e.g., plastics, rubber, cloth, and metal) were gathered and analyzed using a software tool developed specifically for this purpose. The tool tries to separate all samples of one class (e.g. skin) from the other classes by applying a classification algorithm on all possible combinations of wavebands in a bruteforce search to find the best suited combination. The result showed that four LEDs with peak wavelengths at $\lambda_0 \approx 830\text{ nm}$, $\lambda_1 \approx 1060\text{ nm}$, $\lambda_2 \approx 1300\text{ nm}$, and $\lambda_3 \approx 1550\text{ nm}$ are sufficient to reliably distinguish between skin and typical workpieces.

For the considered prototype, a relevant operation range is specified as $100 \text{ mm} \leq L \leq 1000 \text{ mm}$. The beams of the different wavebands should be aligned to be coextensive over the entire optical path. Furthermore, a homogeneous distribution of each waveband inside the beam showed to be crucial. Otherwise, a partial intersection of the beam and an object would result in a different remission intensity for each waveband compared to a complete intersection of the beam and the same object. This would introduce errors to the measured intensities at different wavebands.

Different possible optical setups were simulated with a commercial software for optical engineering and ray tracing called FRED (Photon Engineering, LLC). It could be shown that the best results can be achieved by using a single lens for the transmitter and mixing the emitted radiation from the different LEDs as homogeneously as possible. For this purpose, all LEDs are located underneath an optical fiber. The other end of the fiber is located at the focal point of the lens to create a beam with minimized divergence. This setup has the disadvantage that the majority of the LED's radiation cannot be coupled into the fiber, as the radiation emitted at the edges of the chips gets absorbed internally. On the receiver's side, a line of four photodiodes was necessary in order to receive a signal for all distances within the specified working range. The optoelectronic components were coupled with driver and amplifier electronics directly adjacent to them, as well as a microcontroller which controls the measurement process, classifies the measured data and provides communication interfaces. An augmented-reality image of the sensor module is shown in figure 3, combining a side view of the simulated optics and the actual hardware.

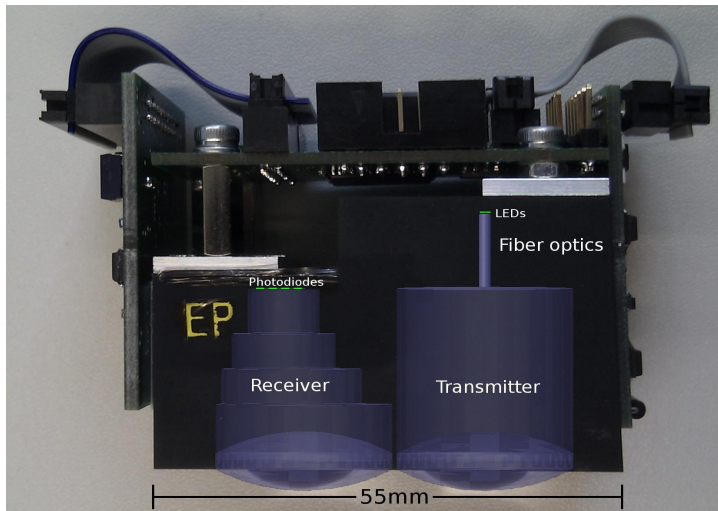


Figure 3: Design of the sensor modules

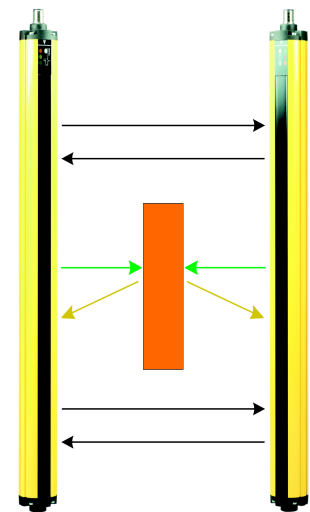


Figure 4: Working principle of the SLC system

In order to build up a demonstrator that would be suitable for field tests, two of these sensor modules each were combined in an aluminium casing. The casings of the prototype are slightly larger than those of typical light curtain products available on the market, but the size could easily be reduced in an industrialization process. Both units are connected with an external control module, which also provides power supply for the sensor modules.

4. Material classification

As the classification of different types of material based on their spectral signature, which has to be measured under the influence of varying distances and angles, is a very complex task, state of the art machine learning algorithms have been applied to solve this problem. For this purpose, a large amount of training data had to be collected by using a computer-controlled industrial positioning system, which allowed to take many measurements of objects in a wide range of exactly specified distances in a short time. Based on this data, each sensor module can be individually calibrated and a distance estimation algorithm could be implemented. Based on the measurement distance, a correction of the measured (and distance-depending) spectral signature can be performed.

The resulting extended spectral signatures have been analyzed in great detail by using advanced classification and machine learning algorithms. The use of Support Vector Machines (SVM) showed the best classification results on the recorded data. With this technique, even minor differences in the signatures can be used to differentiate materials. However, the use of SVMs requires more computational power as the previously used thresholding-based

approach. To maintain fast reaction times, the use of more powerful microcontrollers was investigated and a new prototype of the sensor system is currently in development.

5. Safety assessment

The hardware development has been guided by safety and reliability aspects like reliable components, functional redundancy, functional tests during start-up and operation to allow a later certification of following safety products according to relevant safety standards (e.g. DIN EN ISO 13849). A V-Model based development process for both the embedded software and the hardware modules was applied. It covers well-defined change management and test cases as well as the implementation of a safety framework with initial and periodical self-tests and methods to test the peripheral units. In this context the applied programming guidelines provide a safer application of the ANSI-C standard and increase the quality of the source-code with respect to readability and maintainability. Together with the use of well-proven development tools, these measures should have a supportive effect on a certification process.

The implemented peripheral tests of the sensor system cover supervision of the supply voltages as well as tests of the transmitter and receiver modules by both measuring the voltage drop over the LEDs and comparing the photodiode readout value with expectancy values. This way, even the occurrence of dirt on the lenses can be detected by the sensor. Self-tests of the microcontroller include the correct operation of any used CPU command, CPU register, SRAM-, EEPROM and ROM-memory tests as well as program flow and stack size tests. To maintain fast reaction times of the system, these tests were embedded into the safety framework of the software in form of inline-assembler code to keep the runtime of the tests acceptable.

According to a preliminary reliability assessment performed using the SISTEMA software tool provided by the IFA, the system could achieve a performance level of “c” to “d” (if build up with one channel and an additional test channel with a high diagnostic coverage) or even “e” (if build up as a two channel system). The safety assessment of a basic version of the proposed sensor system has been published and presented on the 9th International Symposium of the TÜV Rheinland Group [7]. A certification as additional safeguarding equipment, which would not replace passive safeguarding equipment such as a guard or protective housing, should be possible, according to a first guess from IFA. However, if the sensor system was meant to replace such passive safeguarding equipment, an intensive study proving the underlying principles would be necessary for the certification.

6. Results and Conclusion

For evaluation, a motorized positioning system was used to measure a set of samples from distances of 75 mm to 1.000 mm with a step size of 1 mm. This equals a total of 926 positions of measurement. At least 20 measurements were acquired per position. In total, a set of 10^6 individual measurements were acquired from dozens of samples.

This comprehensive data set was used as the basis of the evaluation. The data was split up to create ten distinct selections, where 90% of the available data were randomly selected as training data for material classifiers and the remaining 10% were used for testing. In this way, ten different classifiers were trained for each of the tasks 'Skin vs. Wood', 'Skin vs. Meat' and 'Rubber glove vs. Meat'. The results of the individual classifiers for a distinct task were merged to form a median confusion matrix. A confusion matrix shows the number of *true positive*, *false positive*, *false negative* and *false positive* classifications, whereby a *false negative* classification would be a dangerous failure in terms of functional safety. Certain statistics can be derived from a confusion matrix:

- The *Accuracy (ACC)* is defined as the ratio of correct classifications (true negative/positive) to all classifications (false negative/positive + true negative/positive).
- The *True Positive Rate (TPR)* is defined as the ratio of *true positive* classifications to the sum of *true positive* and *false negative* classifications, which equals the sum of all positive samples in the ground truth table.
- The *False Positive Rate (FPR)* denotes the ratio of *falsely positive* classified negative samples to the sum of *false positive* and *true negative* classifications, which equals all negative samples in the ground truth table.
- The *Precision (PREC)* denotes the ratio of *true positives* to the sum of *true positives* and *false positives*. So, the *Precision* is an indicator for the classifiers rate of false alarms.

Table 1 presents the results of the performed experiments. It shows a perfect results for the tasks of differentiating skin from wood as well as rubber gloves from meat, which is relevant for meat processing. Differentiating skin from meat is a very challenging task, as both materials are of very similar nature. Thus, the results are quite well, but do not satisfy the demanding requirements for safeguarding equipment yet, especially with respect to productivity.

	ACC	TPR	FPR	PREC
Skin vs. Wood	1.00	1.00	0.00	1.00
Skin vs. Meat	0.97	1.00	0.08	0.96
Rubber glove vs. Meat	1.00	1.00	0.00	1.00

Table 1: Results of the classification algorithm on different data sets

In conclusion, the proposed system setup implements an optoelectronic safety device with highly reliable distinction between workpieces, protective clothes and human skin. It provides safe operation over distances of more than one meter, which is truly awesome. Even larger distances of several meters might be possible with further optimization of the beamforming optics. Furthermore, a coverage of large danger zones can be achieved if multiple sensor modules are meshed to form a large curtain. Due to the spatial resolution of about 30 mm (limited by the beam spacing), such a curtain is approximately finger-safe. Again, the spatial resolution can be increased with further optimization of the optics. The fast reaction time of $T < 5$ ms is sufficiently fast already for most applications, whereby the performance of the low cost 8 bit microcontroller currently used is the major limiting factor. In addition, the sensor modules implement fault detection methods that are also capable of detecting dirt, which allows the use in rough environments.

7. Outlook

The realized system is optimized for skin detection. If gloves have to be taken into account too, an application specific improvement of the sensor performance is easily possible by means of a new optimization run for the wave bands to be used on base of the spectral measurements of the relevant materials involved in the application, as well as a new training process of the classification algorithm.

Beam broadening currently is one of the limits for the maximum distance between sensor and receiver. Another optimization would be the optical design with multi-lens systems. This would allow larger distances. Very large distances will only be possible using laser diodes, which in turn would also optimize the selectivity of the material classification as experiments show. However, the use of lasers is expensive and may cause other safety problems.

8. Acknowledgements

The Authors would like to thank the K.A. Schmiersal GmbH & Co. KG, the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) and the European Fonds for Regional Development, Ziel 2 NRW (Ministry of Innovation, Science and Research) for the support of this project.

9. References

- /1/ Jacquez, J.A. et al.: Spectral Reflectance of Human Skin in the Region 0.7-2.6 μ m, Journal of Applied Physiology, 8(3):297, 1955.
- /2/ Fitzpatrick, T.B.: The validity and practicality of sun-reactive skin types I through VI. Archives of Dermatology, 124(6):869, 1988.
- /3/ Reinert, D., Schwaneberg, O., Jung, N. et al.: Hand and Finger Protection for Circular Saws. SIAS-2007 Conference, Tokyo, 2007.
- /4/ Reinert, D., Jung, N., Schwaneberg, O. et al.: Finger and hand protection on circular table and panel saws; Elsevier, SAFETY Vol. 47 Issue 8, 2009.
- /5/ Schwaneberg, O., Jung, N., Steiner, H. et al.: "Push-buttons with Material Classification based on Spectral Signatures"; SIAS-2010 Conference, Tampere, Finland.
- /6/ Jung, N., Schwaneberg, O., Steiner, H. et al.: "Field Study Results of a skin detecting Safety Sensor on Circular Saws", SIAS-2010 Conference, Tampere, Finland.
- /7/ Steiner, H., Asteroth, A., Jung, N. et al.: "Safety Assessment of a Material Classifying Safety Sensor using ISO 13849-1 supplemented by Model Checking", 9th International TÜV-Symposium "Functional Safety in Industrial Application", Köln, 2010.
- /8/ Schwaneberg, O., Köckemann, U., Steiner, H., Jung, N.: A Near-Infrared LED-based Material Classification Sensor System, in Optical Sensors, OSA Technical Digest (CD), Optical Society of America, 2011.
- /9/ Steiner, H., Schwaneberg, O., Jung, N.: "Advances in Active Near-Infrared Sensor Systems for Material Classification," in Imaging Systems and Applications, OSA Technical Digest (Optical Society of America, Washington, DC, 2012), ITu2C.2. ISBN: 1-55752-947-7
- /10/ Schwaneberg, O., Steiner, H., Bolivar, P., Jung, N.: 2012. Design of an LED-based sensor system to distinguish human skin from workpieces in safety applications. Appl. Opt. 51, 1865-1871, 2012.
- /11/ Huelke, M., Hauke, M., Pilger, J., 2008. SISTEMA: a tool for the easy application of the control standard EN ISO 13849-1. White paper, http://www.dguv.de/ifa/en/prasoftwa/sistema/paper_e.pdf.

The Accident prevention of Mobility scooter by automatic slowdown with laser range finder

Hiroto INOI,Shinya HASHIMOTO, Tatuyoshi KURIYAMA Toshihiro FUJITA and Kazuya OKADA

KEY WORDS: Transportation engineering, Maneuverability, Comfortability

ABSTRACT

In this paper, the mobility scooter was considered as a service robot. The number of accidents of the mobility scooter is increasing. The laser range finder was used and the mechanism of decelerating the speed of a mobility scooter was developed. When the laser range finder notices barriers on direction of travel, slowdown is made automatically. The main purpose of this paper is to examine the improvement of maneuverability of mobility scooter by automatic slowdown.

The experiment was conducted using three types of courses; right-turn, a left-turn course and a straight course with an obstacle. 8 ladies and gentlemen selected as examinees. They are over 65 ages and have not ever to drive mobility scooter. All examinees were requested to drive mobility scooter 3 times for each type of courses.

Effect of automatic slowdown is drawn from 2 way. One is comparison of indicators between mobility scooters run with and without automatic slowdown. The number of contact to the wall of a test course was the index shows improvement in maneuverability. The length of time to pass through a test course was the index shows improvement in convenience. The other is subjective opinion from hearing.

The length of time is decrease. And in some cases there is statistical significance. It shows that automatic slowdown does not lead to the depression of convenience. From hearing survey, automatic slowdown gives margin to concentrate drive's mind on steering. It shows that automatic slowdown gives improvement in driving performance.

As the result automatic slowdown can be improved driving performance without worsening convenience. That shows the automatic slowdown can improve the safety and the operativity of a mobility scooter, and can support driving.

When considering safety of AGV or transport machines for passenger, these research findings are valuable.

1 INTRODUCTION

(1)Wider use of Mobility Scooter and the problems

With aging of society, it is expected more people will have difficulty in mobility because of their bad physical conditions, thus the transportation for those with difficulty in mobility will be necessary. As one of these methods, Mobility Scooter is used. However, with increasing use of Mobility Scooter, the number of the related accidents also has increased. According to National Institute of Technology and Evaluation in Japan (NITE), 67 cases of one-car accidents were reported in 5 years from 2005 to 2009. 20 of these accidents resulted in death and 16 resulted in serious injury. Or with the serious accidents with clear causes, about 75 % of them were caused by the mal operation or negligence by the drivers. The measures have to be taken immediately to prevent accidents and to enable the users to operate them.

Specification of mobility scooter was defined in Japan Industrial Standard (JIS) T 9208 established in 2009. This safety function and additional design work for risk management were provided in JIS T9208. This is mainly on the standard for the product itself, it is hard to expect that this leads to the prevention of accidents caused by the errors in operation or judgment by the users. So, new measures are required.

(2)Goal of this study

In this study, automatic deceleration of Mobility Scooter in the case the scooter comes too near to the danger of collision is examined as a way to improve operation. To achieve automatic deceleration, Laser Ranger Finder (LRF) is used. Irrespective of the operation ability of the driver, automatic deceleration is activate to prevent accidents or serious damage. Because this system supports the operation by the driver in terms of the part of cognitive activity to find the obstacles and the part of operation, the driver can concentrate on the control of the steering wheel, with smaller burden, thus the better operation can be achieved. As a disadvantage of this system, the automatic deceleration or the machine's overriding the operator's control may deprive the drivers of their freedom in driving the scooter and damage convenience. So, the following are the goals of this study.

-To Verify the change in operation and convenience brought by the automatic deceleration system.

-To verify the situation where the automatic deceleration is effective.

As an objective guideline to verify the change in operation, the number of collision is measured. As an objective guideline to verify the change in convenience, the operation time is adopted. In addition, hearing and questionnaires are conducted.

In order to let the unskilled drivers of Mobility Scooter operate without accidents, the subjects of this study are the unskilled users. Through the study of these, it will be verified whether the automatic deceleration can improve the operation without damaging convenience. Especially the study of the situation where automatic deceleration is most effective is to be conducted to study where the system is useful for accidents prevention or better operation in the limited space.

2 MOBILITY SCOOTER FOR THE EXPERIMENT

(1) LRF

In order to achieve automatic deceleration of Mobility Scooter, LRF is applied in this study. The specification of LRF (SE1L-H02LP Trial products, IDEC) for this study is shown in Table 1. LRF is set at the height of 540mm (this height stand for the height of the irradiation point of the laser.) from the floor on the central line going through the front of Mobility Scooter. With LRF, time required for the laser to be irradiated, hit the object, reflected and come back is measured to calculate the distance to the obstacle, which enables LRF to detect the obstacle within its set detection range. Detection range can be set for 3 levers, but in this study, 1 range is used.

Table 1. Specification of LRF

item	Specification
Type	Se1L-H02LP Trial Product
Protection Area	Max.3.5 m
Warning Area	Max. 10 n
Detection Angle	190degree
Scan Cycle	30 ms
Response Time	Off 60 ms - 510 ms On 210 ms - 510 ms
Outer size	90mm (L), 90mm (W), 9.5mm(H)
Weight	Less than 1.0kg
Light source wavelength	905nm

(2) Automatic deceleration

LRF installed on the front of Mobility Scooter detects the obstacles in front of it. Since LRF is installed on the steering wheel, the direction of the steering wheel and LRF are always the same, thus always the obstacles ahead of the scooter can be detected. In this way, obstacles in the set detection range can be detected. When LRF detects an obstacle in the range, Mobility Scooter automatically decelerates. Without obstacles, the maximum speed of the scooter is 6km/h as with the scooter without LRF, but with obstacles in the range, the maximum speed is 2km/h. After detecting an obstacle, the speed of the vehicle is slowed down to the one-third of the ordinary times. The Mobility Scooter used for this study proceeds for another 1 m till completion of deceleration after detecting an obstacle when it was running at the speed of 6km/h.

(3) Setting of detection range

Before commencement of experiments using LRF, it is necessary to think about the setting of detection range of LRF. In this study, an experiment is conducted beforehand, to study how the range should be set. As a result of this pre experiment, it is found that it is necessary to set the detection range in a way deceleration takes place before controlling the steering wheel and detection is only for the front of the scooter. Also it is necessary to make clear notification of the information about automatic deceleration in conducting experiment. More precisely, information about the distance required for deceleration to start and complete or detection range should be provided before actually experiencing them. With these settings, the experiment is conducted.

3 METHODOLOGY

(1) Outline of the experiment

Date: December 9th (15:00-17:30), December 13th (9:30-12:00 and 15:00-17:30), December 16th (15:00-17:30)

Venue: Osaka University, Photonics Center IDEC laboratory (Indoor)

The number of subjects:8 (Male 4, Female 4)

The subjects were novice for driving Mobility Scooter and are 65 years or older.

2 types of experiment courses are set with certain control of steering wheel assumed. Referring to the preceding researches, the difficulty of the courses is set at the level which requires a certain level of driving skill. (Ishibashi et al.(2010)) These conditions recreate a situation where improved operation is required in using Mobility Scooter in daily life. As the guidelines for evaluation related to operation and convenience, operation time and the number of collision are counted as objective guidelines, while questionnaires and hearings are conducted as objective guidelines. Through study and analysis of the changes in these guidelines with or without automatic deceleration, the goals of this study can be achieved. From now on, the case with the automatic deceleration is described as “with automatic deceleration” and the one without as “with an existing situation”. Following are the outline of the experiment courses.

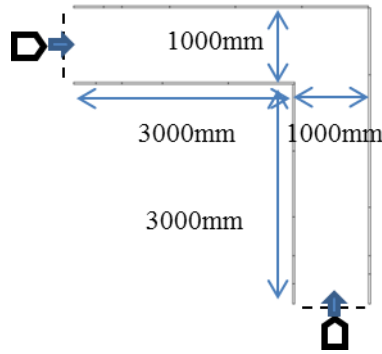


Figure 1, Outline of the course with a right angle corner

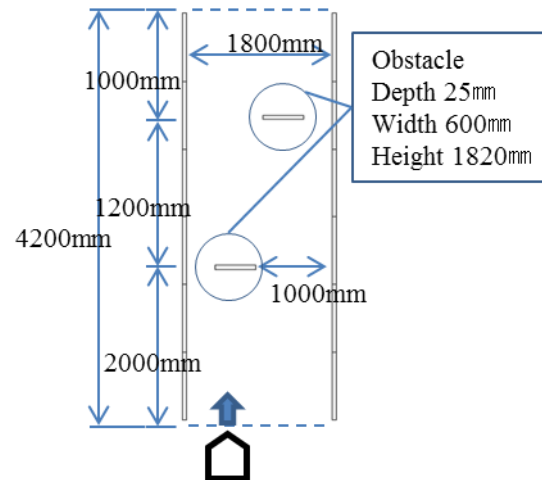


Figure 2, Outline of the course with obstacles

(2) Procedure of experiment

Before the experiment, to make the subjects got used to the operation of Mobility Scooter, the subjects were required to drive for about 10 to 20 minutes after having explanation about how to operate the vehicle.

Following is the procedure of the experiment.

1. The subject waits at the start point to confirm the conditions for driving.
2. The course and the driving condition (with or without automatic deceleration) vary each time.
3. With a signal, the subject starts Mobility Scooter and drives it to the goal.
4. A staff runs after the subject to record the operation time and the number of collision. Another staff shoots a crane shot video of the operation.
5. After reaching the goal, the subjects answers the questionnaires by category.

The procedure from 1 to 5 is conducted for both cases of “with automatic deceleration” and “with an existing situation”. After completing 1 set of procedure, questionnaire for comparison is given. After completing 3 sets, questionnaires with free answer are given. 2 subjects participate in 1 set of experiment.

(3) Verification method

In order to verify the effect of automatic deceleration, various guidelines are measured to compare the effects between with or without the automatic deceleration. The change in the number of collision is related to operation and the change in the operation time is related to convenience. Therefore, as the objective guidelines, the number of collisions and operation time are evaluated. The questionnaires and hearing upon completion of driving can show the subjective ideas of the drivers for verification. It is expected that automatic deceleration influences judgment and operation by the driver, so the questionnaire includes the items about these points.

4 RESULT

(1) The result of operation time measurement

The average operation time in both “with the existing situation” and “with the automatic deceleration” for each course and the results of measurement are shown in Table 2.

Table 2, The average operation time for each course and the results of measurement.

Course	Average operation time(s)		Significant probability (central figure)	Significant difference (5% standard)
	Existing situation	Automatic deceleration		
With the right angle corner (left turn)	13.43	12.38	0.026	Yes
With the right angle corner (right turn)	16.67	14.43	0.161	None
With obstacles	14.36	14.67	0.449	None

Wilcoxon signed-rank test is applied.

As the result of the experiment, no significant change was observed in operation time with the automatic deceleration, which means automatic deceleration worked as well as the speed control by the driver. Thus no degradation of convenience was observed in terms of operation time in this experiment. It can be said that automatic deceleration has small possibility of causing inconvenience for the drivers.

(2)The result of measurement of the number of collision

The average number of collision in both “with the existing situation” and “with the automatic deceleration” and the results of measurement are shown in Table 3.

Table 3, The average number of collision and the results of measurement

Course	Average operation time(s)		Significant probability (central figure)	Significant difference (5% standard)
	Existing situation	Automatic deceleration		
With the right angle corner (left turn)	0.13	0.08	0.655	None
With the right angle corner (right turn)	0.13	0.13	1.00	None
With obstacles	0.38	0.08	0.068	None

Wilcoxon signed-rank test is applied.

As the result of the experiment, no decrease was observed in the number of collisions “with the automatic deceleration”. This was because the number of collisions in the “existing situation” and the number of samples were small and hard to make difference. However decrease was observed in the average with the automatic deceleration. Therefore it is expected with the larger number of samples, the clearer effect of the automatic deceleration can be observed.

(3) The result of questionnaires

Two kinds of questionnaires were given upon completion of driving each course and after driving both “the existing situation” and “with the automatic deceleration”. The former was about various difficulties the driver found during operation and the latter was about the comparison between with or without the automatic deceleration.

Following questions were asked in the questionnaire about difficulty in 7 grades.

- The difficulty of the course
- Timing to control the steering wheel in turning the corner
- Control of the steering wheel
- Drive as you expect

Table 4 shows the result of the questionnaire. The higher the grade is, the more positive the answers are, which means easy or comfortable to operate, while the lower the grade is, the more negative the answers are, which means difficult or hard to operate.

As a result of these questionnaires, it is found that automatic deceleration makes it easier for the driver to judge the timing to make a turn, to control the steering wheel and to drive without getting nervous. In the hearing, drivers mentioned the benefit of automatic deceleration even with a delay in cognition, feeling of safety for being able to avoid serious damage even in collision due to limited speed near obstacles, and concentration on judging the timing to make a turn or controlling the steering wheel due to easier speed control with automatic deceleration.

Table 4, The result of the questionnaires about various difficulties

course	item	Existing situation	Automatic deceleration	Significant Probability
With the right angle corner (left turn)	Difficulty of the course	1.25	1.75	0.003**
	Judging timing to turn the corner	1.08	2.13	0.000**
	Steering Wheel control	1.00	1.46	0.040*
	Operation as imagined	1.21	2.00	0.003**
With the right angle corner (right turn)	Difficulty of the course	1.08	1.74	0.002**
	Judging timing to turn the corner	1.21	1.93	0.001**
	Steering Wheel control	1.04	1.48	0.007**
	Operation as imagined	1.30	1.51	0.185
With obstacles	Difficulty of the course	0.67	1.42	0.016*
	Judging timing to turn the corner	0.71	1.92	0.002**
	Steering Wheel control	0.42	1.38	0.001**
	Operation as imagined	0.79	1.67	0.002**

** Wilcoxon signed-rank test is applied by 1% significance, *5% significance

5 DISCUSSION

(1) Verification of the situation where automatic deceleration is effective

It was found through Chapter4, that automatic deceleration made it easier for the drivers to operate Mobility Scooter. Here to find out the situation where automatic deceleration is effective, differences by conditions are studied.

(2) Verification of differences by conditions

Here the differences in the effect of automatic deceleration by conditions are studied, using Chi-square test based on the results of the questionnaires conducted after driving to find about the differences in the effect of automatic deceleration by conditions. As a result of the test, no difference was found in the effect of automatic deceleration by courses or the number of driving. On the other hand, difference in the effect of automatic deceleration was observed according to the different difficulty level of driving felt “with the existing situation”, Table 5 shows the summary of difficulty drivers felt when they drove “with the existing situation. It was found that the more difficult the drivers found driving “with the existing situation”, the greater improvement in overall operation was found “with automatic deceleration”,

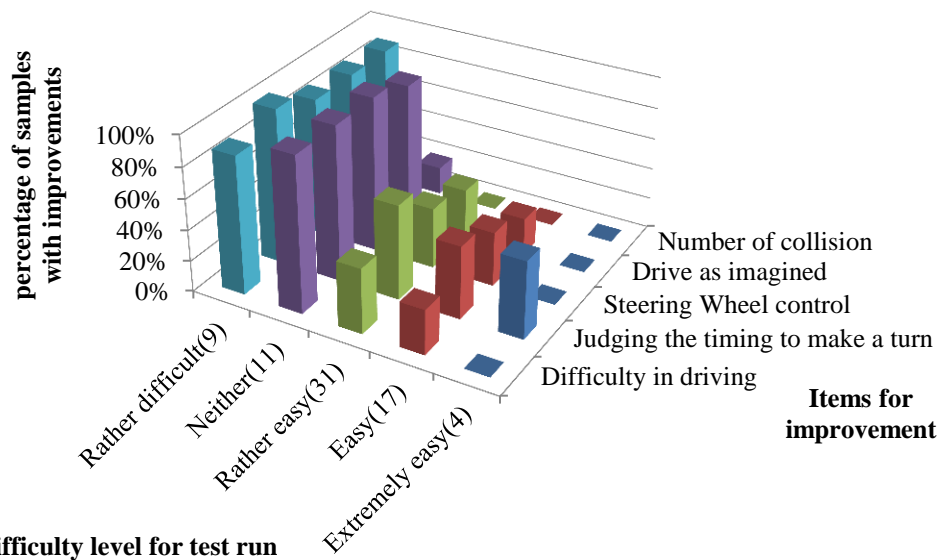


Figure 4, Rate of improvements by driving difficulty “with existing situation”

(3) Summary of analysis

It was found that difference in effect of automatic deceleration was generated by the difference of difficulty level in driving. Because the drivers feeling greater difficulty in driving “with the existing situation” tend to feel more difficult about judging the timing to make a turn or controlling the steering wheel than the other drivers, these drivers can expect positive effect of automatic deceleration on these activities. Furthermore, as a result of improved judgment of timing or control of steering wheel, it became possible for them to drive easily or as they imagine. Thus, the group which felt driving “with the existing situation” more difficult could observe greater improvement in overall operation.

The difficulty felt by the drivers differs from driver to driver. In this study, all the drivers operate Mobility Scooter for the first time with same practice time. So this difference in difficulty can be attributed to the skill level of the drivers. Therefore it can be said that the less skilled driver can have greater effect.

6 CONCLUSION

It was found that automatic deceleration can improve operation without damaging convenience from subjective view point. In this study, improvements could not be observed from the objective guidelines. However the better results can be expected with more samples.

As the specific effects seen in questionnaires and hearing, easier control of speed and driving without fear were raised as ways to allow the better judgment of timing to turn a corner or better operation of steering wheel.

The study of situation where automatic deceleration is effective found the effect differs based on the difficulty the driver felt about the course. It was found that the more difficult the drivers felt about the course, the greater improvement they found with the overall operation, because these drivers also felt judging the timing to turn a corner or control of steering wheel very difficult. It was found the drivers with these difficulties could have greater improvement.

REFERENCES

Tatsuo ISHIBASHI, Moto NISHIOKA, Hiroto INOI, Naoko KIMURA (2010) A Study on the Usability of Mobility Scooter, Proceedings of the 12th International Conference on Mobility and Transport for Elderly and Disabled People, A085

Consideration on RFID Devices Applying to Safety of Integrated Manufacturing Systems

Takabumi FUKUDA

Department of System Safety, Nagaoka University of Technology, 940-2188, JAPAN,
t-fukuda@vos.nagaokaut.ac.jp

KEYWORDS : Integrated manufacturing System, PFID device, Risk reduction, Supporting protective device

Abstract

This paper concerns the application of RFID (radio frequency identification) devices to safety measure of integrated manufacturing systems (IMS), such as shown in ISO 11161. In the IMS, even if all machines are completed enough safe measures, the new hazards are generated by combining some machines. For example, when a machine in the IMS is maintained by a skilled maintenance person, “tag out” is useful countermeasure for preventing unsafe restart by another operator in usual situation. But this measure is not effective (1) when the maintenance person has forgotten the procedure of tag-out, (2) when the other persons are in the hazardous areas without tag, (3) when a operator takes unpermitted work, and so on, mainly caused by human error. These situations are risky. For improving these situations and reducing risk in such a condition, to indentify the worker including his/her skill and access control by the area gate is requested. Adding to this, it is preferable to detect his/her position. The author and related group members are testing to use RFID devices for IMS safety. As in our experience, there are few problems to identify the worker, in this paper the author forces on the application to judge in which zone a worker is. For this purpose, principle of triangulation is applicable. One of the issues to apply RFID devices to this purpose is the accuracy of the measured distances between RFID tag and readers. The other issue is how the metal blocks, like machine tool is influence on the estimated distances. The author carries out the simple model experiment, and makes clear: (1) The signal intensity is change by sway of RFID, and as the result, the estimated distance is widely change. It makes difficult to locate the person’s position. (2) It is recommended not to put reader extremely near the metal block. Otherwise, the signal intensity is stable.

1. Introduction

In this paper, the author reports the experimental result taken as one part of research activities “Risk Reduction Strategy using Supporting Protective Device” organized by Japan Machinery Federation (See related paper submitted to SIAS 2012: A Study of Risk Reduction Strategy using Supporting Protective Device by S. Shimizu, and S. Umezaki, JNIOOSH. and reference¹⁾ and formerly by Nippon Electric Control Equipment Industries Association (NRCA)). The topic of this paper is forced on specifying the position of each worker among the other topics, *e.g.* workers identification.

In the experimental results, the radio signal strength received by RF reader (RF receiver) is not shown in the physical parameters such as [V/m], but RSSI (Received Signal Strength Indication) value, which is relative index. Adding to this, as well known, the results depends on the radio frequency of the device. The experiment is carried out by using RFID devices for 426MHz. The results would be changed if the experiment was carried out for 1.2GHz. However, the fundamentals of discussion may be almost same or similar.

2. Experimental Study Parameter and Specification of RFID Device

(1) Study parameter:

In this paper, the characteristic is evaluated when RFID devices are used for worker’s location as one of the functions which are expected to accomplish by using the supporting protective system. The main interests are (1) the effect of the handling position and posture of the device and (2) the effect of the metal bodies near the RFID device.

(2) RFID devices used in this study:

The specification is shown in *Table 1*.

Table 1 Specification of RFID devices

Standard	ARIB STD-T67
Frequency band	426MHz band
Communication procedure	Single way
Modification	FSK
Transmitting power	1mW (+20%, -50%)
Reader antenna	Whip antenna

(3) Experimental details:

Parameters in the experiment are follows:

1. The handling position and posture of RFID tag:

The effect of position and posture of RF tag on the RSSI value is investigated (*Table 2*).

2. The effect of metal body around the RF tag:

The effect of metal body (e.g. press machine, turning machine) on the RSSI value is investigated.

Table 2 Experimental conditions

Position and Posture	(a) In hand at front of his body and his face is toward the RF reader. (Standard Condition). <Human body -- RF tag in hand ----- RF reader>
	(b) In hand at front of his body and his back is toward the RF reader. < RF tag in hand – Human body ----- RF reader>
	(c) In front pocket of jacket and his face is toward the RF reader. <Human body -- RF tag in pocket ----- RF reader>
	(d) In back pocket of trousers and his face is toward the RF reader. <RF tag in packet -- Human body ----- RF reader>

3. Experimental Results

In feasibility study, it is cleared that the difference among the individual RFID tags and readers is not negligible. However, this difference is adjustable by test in normal condition (e.g. by the difference of RSSI value in free space). Therefore, the following experiment is carried out by using one pair of RF tag and RF reader.

1. The effect of position and posture of RF tag on the RSSI value

The results are shown in *Fig. 1*.

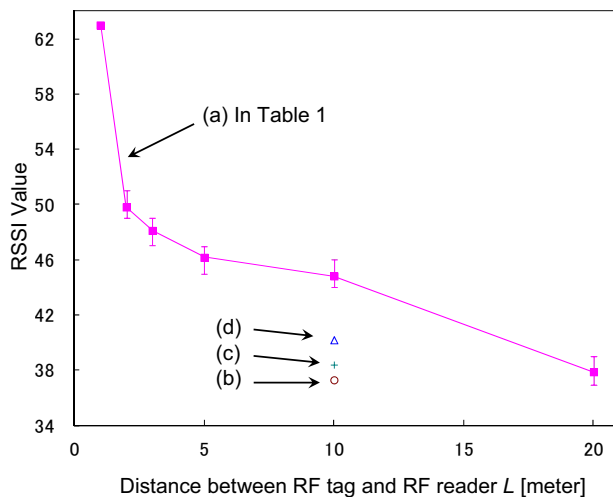


Fig. 1 The effect of tag handling position and posture

compared with (a). However, the RSSI value is the minimum among the conditions (b) – (d). Therefore, the dominate factor (whether the absorption by near body or cloth and the absorption by passing through the body) is not clarified through these experiments.

2. The effect of metal body around the RF tag

The purpose of this experiment is to understand the effect of machine tool etc. on RSSI value. In this experiment, a metal locker for dress-changing is placed as shown *Fig. 2*. It is not clear whether the effect by a locker which is made of thin metal plates is equivalent to the effect by machine which is made of metal block. However, in this experiment carried out with a locker, the effect is observed, it is certain that some effect on RSSI value is expected when the system is applied to actual workplace.

The locker is placed on points shown in Fig. 2: The distance from the RF reader is 0 (sticking to the RF reader), 1, 2 meters. The RF tag is put on 15 point whose directions are a, b, c, d and e, and the distance

- 1) The RSSI value monotonously decreases according to the distance between the RF tag (tag holder) and RF reader.
- 2) The dependency of RSSI value on distance is strong when the distance is less than 5 meters. The dependency is small when the distance is greater than 5 meters.
- 3) The RSSI values in conditions (c) and (d) at 10 meters correspond to 20 meters in condition (a). This result is considered that the signal is weakened by body which is very near in conditions (c) and (d) and clothes. The dominate factor (whether body or cloth) is not clear.
- 4) The RSSI values in condition (b) at 10 meters also correspond to 20 meters in condition (a). This result means that the signal is weakened by body. No effect by cloth is considered when the result is

between RF tag and RF reader is 1, 3, 5 meters. The RSSI value is measured for each position.

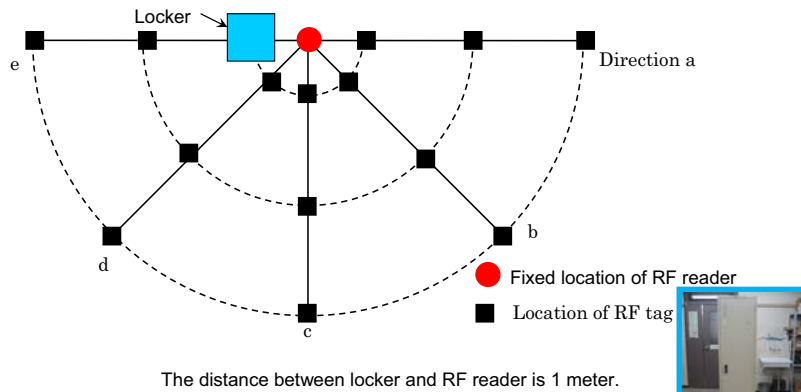


Fig. 2 Location of RF tag and Locker

The results are shown in **Fig. 3**. Under the condition that the locker sticks to RF reader, the RSSI value is dropped in condition when the locker is located on the line between RF tag and RF reader. However, even the locker is put between the RF tag and RF reader, no clear effect is observed when the distance between the locker and RF reader is greater than 1 meter.

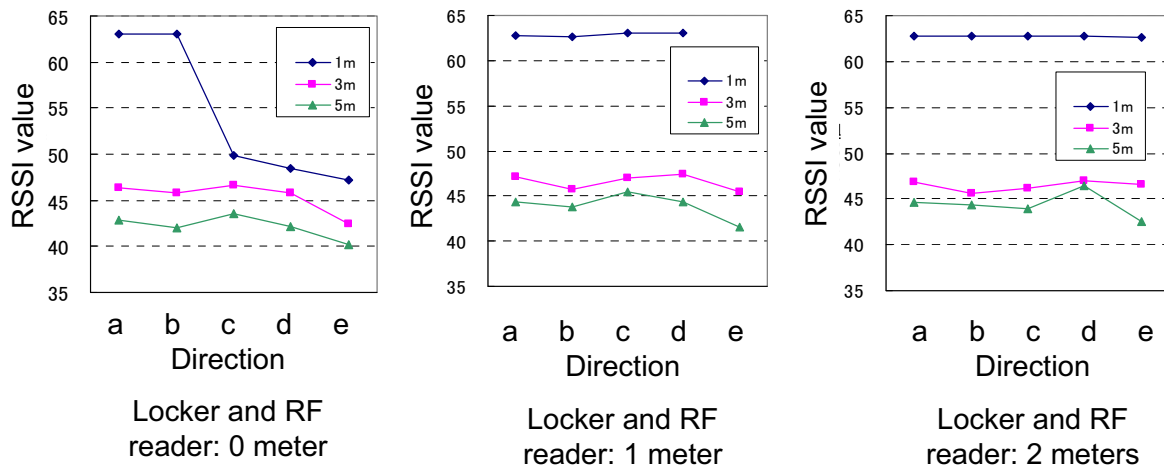


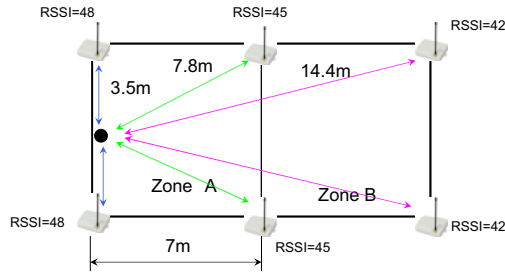
Fig. 3 Experimental result – RSSI value

4. Specification of the location of the tag holder

From Fig. 1, The RSSI value depends on distance clearly within 5 meters and the distance is measured by accuracy of 1 meter from RSSI value. Within the range 5 meter and 10 meter, the dependency is weak and the accuracy is several meters. More than 10 meters, it is considered impossible to measure the distance. The maximum square whose diagonal line is less than 10 meter is 7 meter around. **Figure 4** shows 3 typical cases. It is sever but possible to identify from the rank of RSSI value received by each RF reader, in which zone the worker (RF tag holder) is.

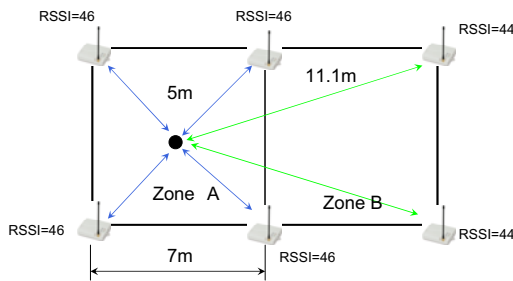
5. Risk reduction by supporting protecting device

The proposed system in this study is to activate an alarm when the system catches the dangerous situation, e.g. (1) number of workers detected in the IMS²) area by the supporting system is not the same as counted workers by entrance-exit gate management system, (2) when inappropriate worker is near the machine when a special task (die-change, maintenance, troubleshooting etc.) is performed. Therefore, this system is not “safety condition confirming and work permission” type. However, even if a machine is perfectly designed and implemented safety measures (inherently safe design measure, safeguarding and complementary protective measure and information for use), there is some tasks whose safety depends on workers’ skill and his/her awareness and attentiveness. In these tasks, workers are near machine and machine is supplied energy and in



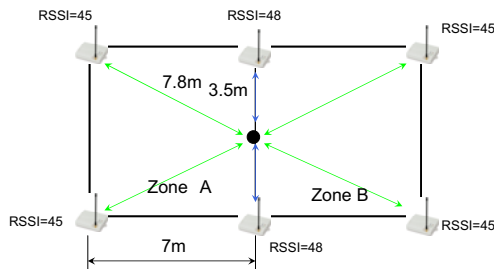
Clearly recognized a RF tag holder is not in Zone B, but Zone A

Case a: A holder is the opposite side of Zone B



Not recognized a RF tag holder is in Zone A because RSSI value 46 and 44 is in the range of deviation.

Case b: A holder is in the center of Zone B



Case c: A holder is near the border of Zone A and Zone B

Fig. 4 Position monitoring of RF tag holder by RSSI value

4 RF reader are located in 4 corner (6 RF readers in zone A and B), and no metal block near RF readers, possibility to monitor the worker's position by identifying zone is supported.

- 3) However, these constrains are strict for actual work place. Therefore, it is more suitable to use RFID device as an identifier.
- 4) Task and purpose of "supporting protective device" are different from "safeguarding" for machinery denoted in ISO 12100. However this supporting system is available for enhancement of safety by adding on the management measure. And as the result, risk is expected to be reduced in such a situation.

References

- 1) Shimizu, S., *et. al.*: Study of Ensuring Worksite Safety for Multiple Workers, Proceeding of SIAS 2010, Session 3.2, 2010
- 2) ISO 11161:2007 Safety of machinery – Integrated manufacturing systems – Basic requirements

some situation, machine actually moves. Especially in order to ensure safety for IMS (Integrated manufacturing System), cases in which neighboring machine are operated independently with the target machine. "Blind spot" is hazardous area. Management measures, workers roll call, lock-out, tag-out *etc.*, are applied for ensuring safety. But, it is also true that safety is partially depends on not hardware measure but software measure, *i.e.* task management. The proposed "supporting protective device" is applicable for these situations. It is useful to avoid human error not to lead to accidents. Therefore, the author considers the proposed supporting device is effective to reduce risk in maintenance and so on.

6. Concluding Remarks

In this paper, the application of RFID devices to supporting protective device, especially for workers' positioning, is investigated experimentally. The summary is shown below:

- 1) To measure the distance from RF tag holder (worker) and RF reader with accuracy of several meters is impossible. The main reason is the effect of posture of tag and metric bodies around the work places. Even if these parameters are controlled, the available range is less than 10 meters.
- 2) As the result of 1), if neighboring squared zones, A and B are 7 meter around and

Development of Interlock Switch with Lock Function for the improved Safety in Consideration of Failure

Takeo Yasui¹, Norifumi Obata¹, Takao Fukui¹, Atsushi matsumoto¹, Toshihiro Fujita¹

¹ IDEC CORPORATION

7-31, Nishimiyahara 1-chome, Yodogawa-ku Osaka 532-8550, Japan

KEY WORDS: interlock switch, internal energy, reverse energy structure,

Abstract

Safeguarding is a protective measure that assures operator's safety in HMI environment where humans and machines interact. Providing a safeguard is the most typical method of safeguarding, and the safeguard has a door equipped with an interlock switch that enables the hazard source (machine) to start only when the door is closed, and prevents startup when the door is open, so that operators can work safely inside the safeguarded area for maintenance and other purposes.

International standards specify various requirements of interlock switch function and structure to ensure operators' safety, but there has been no reference to the foreseeable failures that occur when excessive force than expected is applied on the interlock switch. Nor have sufficient measures been taken against failures in such event. In this paper, we report on the safety concept to counter the issue and also the next-generation interlock switch that assures safety even when the switch has failed.

1. Introduction

Within the various technological fields that make use of industrial robots, such as FA (factory automation), it is necessary to design machines and equipment which ensure the safety of people working in HMI (human machine interface) environments, where operators and machines are both present in the same place at the same time.^[1,4,5] In addition, risk assessment in the workplace is now virtually a requisite under ISO12100.^[4]

Risk assessment is the process used to identify the sources of risk associated with machinery and equipment, to estimate and evaluate the risk, and to try to reduce it to an acceptable level. This process has to be conducted during the design phase for each machine, during operation, and whenever a machine is being repaired.

Reduction of risk is carried out using a 3-step method which proceeds in order of inherently safe design measures, safeguarding or complementary protective measures, and information for use.

There are many risks which cannot be adequately eliminated by inherent safe design measures, alone. In such cases, the safety of the operator should be ensured by reducing the risk using safeguarding measures. Figure 1 shows an example of safeguarding measures associated with a robotic system. The robot is enclosed by a safety fence to prevent the operator from coming too close to the hazard. However, in some cases it is necessary for the operators to enter inside the safety fence in order to carry out maintenance or repairs. Therefore, it is necessary to design



Fig. 1 Safeguarding measures

the system so that the robot cannot be activated when the door of the safety fence is opened by the operator. A safety interlock switch can detect any opening or closing of the door on the safety fence. It acts as a safeguarding device to prevent the activation of the hazard while the door is open and serves to isolate the operators from the hazard when the door is closed. If the type of hazard involved requires the door to be locked, an interlock switch with solenoid lock should be used.

In this study, interlock switch damage due to excessive stress on an interlock switch with solenoid lock is investigated and reported.

2. Safety status of the interlock switch at the time of failure

2.1 Usage of an interlock switch with solenoid lock

As mentioned above, in order to reduce risk to an acceptable level it is necessary to take safeguarding measures against those types of risk which cannot be eliminated by inherently safe design measures alone.^[1] Safeguarding measures are based on the concept that safety is ensured as long as the operator and the machine do not share the same space at the same time, and the operator does not touch the active parts of the machine. In other words, safety is ensured by enforcing separation of the operator and the machine both in space (the principle of separation) and in time (the principle of stoppage). More precisely, this can be realized through the combination of a safety fence and a door interlock system (safeguarding device), as shown in Figure 2. This measure is very effective in reducing risk with automatic machines which do not need the operator to be present in the immediate vicinity.

ISO12100 defines interlocks as “mechanical, electrical or other type of device, the purpose of which is to prevent the operation of hazardous machine functions under specified conditions”. The type of interlock described in this paper can control machines and equipment using safety confirmation information generated by the safety devices themselves. Thus, a door interlock system can allow a particular machine to be activated when the door is closed because this means that the hazardous area is isolated and there is no risk. Conversely, when the door is open, the system does not allow the machine to be activated because the hazardous area is now accessible.^[1,2] The door interlock system controls the opening and closing of the door by inserting an actuator into the interlock switch fixed to the door.

This type of interlock switch, along with an emergency stop switch, meets all the important requirements for use as a safety device - keeping operators away from hazardous machines when they are in operation. One of the requirements to achieve this level of safety is the presence of a “direct opening action” (based on Annex K in the international standard IEC 60947-5-1). This function acts as an emergency stop switch - breaking the circuit by ensuring the separation of contact points when the door is opened. A further key requirement is the “defeat prevention” (based on ISO14119, 5.7.1). This makes it impossible to activate the machine by any means other than the special actuator fixed to the door. Items such as readily available screws, needles, metal wafers, keys, coins or general tools cannot be used to activate the machine. In keeping with this requirement, the order for the machine to stop operation is maintained in place, without fail, as long as the door is open.^[3,5]

Machine tools such as lathes or other machining equipment have rotating parts which do not always stop moving immediately after the power is cut, because of inertia. In those cases where moving parts do not stop completely or have not slowed down to a safe level by the time the operator reaches the machine, even after cutting power by opening the door and using the interlock switch, the door has to be kept locked until it is safe for the operator to approach. An

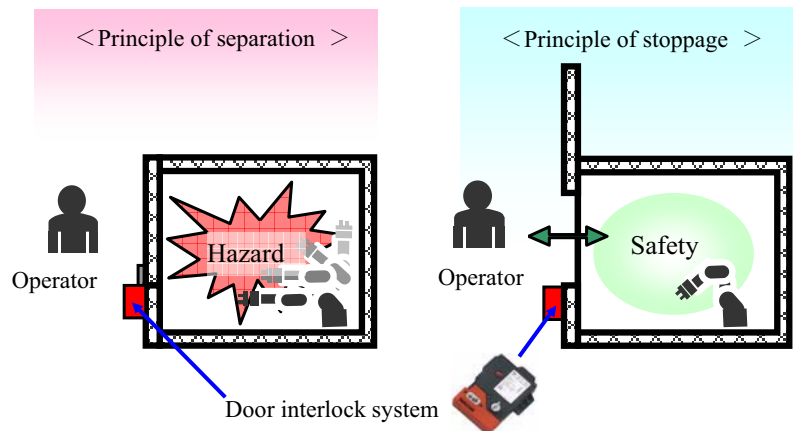


Fig. 2 Basic principles for safeguarding measures

interlock switch with solenoid lock is, therefore, required.

More precisely, if the time it takes the operator to reach the hazard is shorter than the amount of time needed for the hazard to be rendered safe (for example, the response time for the safety system + the time needed for the machine to stop moving), it is necessary to choose an interlock switch with solenoid lock, as shown in Figure 3.

2.2 Structure of an interlock switch with solenoid lock

The interlock switch generates an output signal regarding the open or closed condition of the door by means of movable contact points (rotating a cam inside the interlock switch with a special actuator). The interlock switch with solenoid lock stops the rotation of the cam altogether so that the actuator will not disengage when the door is locked. This means that, in order to open the door, the signal to cancel the lock must be given to the interlock switch, releasing the lock on the cam and opening the door by pulling out the actuator.

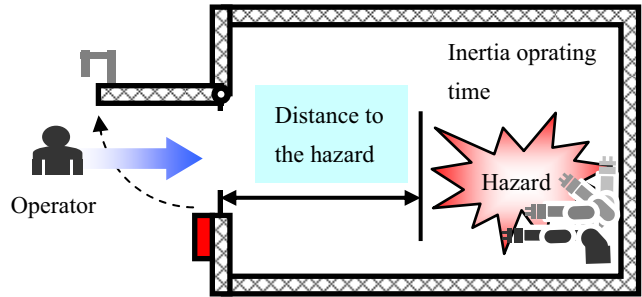


Fig. 3 Countermeasures against hazards caused by inertia and moving parts

Figure 4 shows the operation process involved in opening the door and the structure of the lock portion of the interlock switch.

- 1) The actuator is inserted and locked. The notch on the cam is caught by the lock so that the cam cannot rotate. In this situation, the actuator cannot be pulled out. The cam is not exerting pressure on the rod, so the contact point on the side of the safety circuit is turned ON, due to the force of the spring.
- 2) In order to open the door, the signal to cancel the lock is sent to the interlock switch. The lock part then moves in the direction shown by the arrow, which allows the lock to be released from the notch on the cam. This makes it possible for the cam to rotate.
- 3) The actuator is pulled out and the cam rotates. The rotating cam pushes the rod and the contact point on the side of the safety circuit to the OFF position.

When the door is locked, as shown in 1), even if the operator tries to open the door it will not respond and so the operator will be separated from the hazard and kept safe. However, if enough physical pressure is exerted on the door, exceeding the strength of the internal safety devices, the interlock switch and the lock may break.

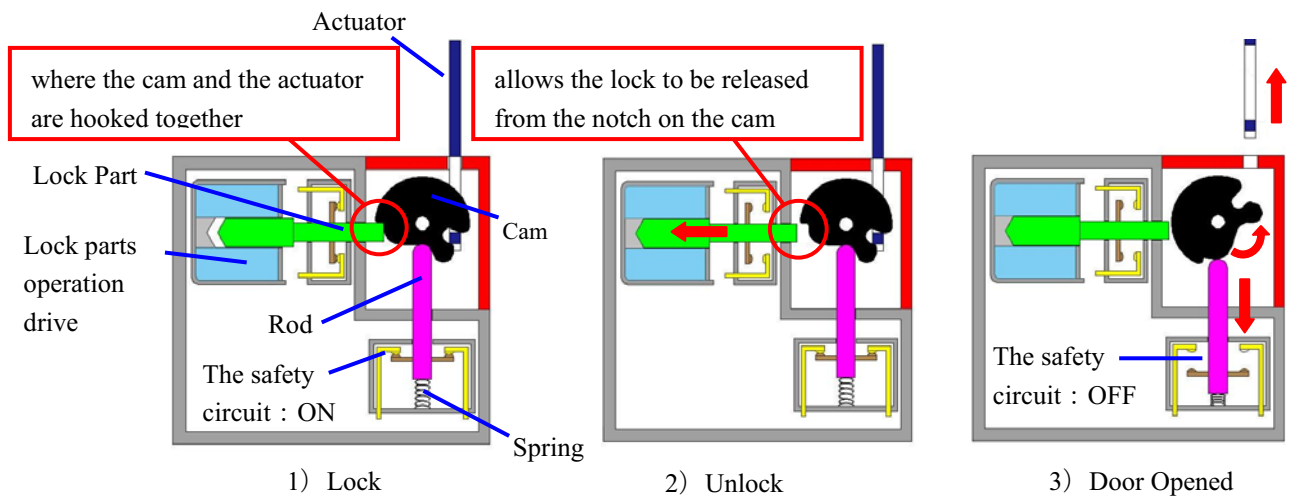


Fig. 4 Interlock switch with solenoid lock and structure, showing the usual operation procedure

2.3 Safety structure needed to deal with the failure of an interlock switch with solenoid lock

When the operator tries to open the locked door using force, there is a risk of structural and component failure if the installed interlock and the lock itself are not strong enough for a heavy door, or if excessive pressure is applied repeatedly to an inadequate door design. Therefore, we examined the various possible ways in which an interlock

switch with solenoid lock could fail.

As mentioned earlier, the contact point on the side of the safety circuit is turned on and off by the rod and the spring controlled by the cam. The spring maintains pressure on the cam and the rod keeps them in contact. Our examination focused on the strength of this spring and the internal energy it provides.

The interlock switch has two operating states, one with the spring under pressure (internal energy is high) when the contact point on the device is turned off (due to the function of the cam and the contact point on the side of the safety circuit) and the other with the spring under pressure (internal energy is high) when the device is turned off. With the former, the internal energy always keeps the contact point on the side of the safety circuit turned ON, while the latter keeps the contact point turned OFF. Therefore, we can refer to the latter condition as “reverse energy structure”.^[6]

Next we examine what can happen when excessive pressure (exceeding the device’s tolerance) is applied to an interlock switch with solenoid lock.

When the actuator is pulled out with excessive force, any of the cam, rod or lock components inside the interlock switch can break and the actuator will disengage. If the contact point on the side of the safety circuit can be switched from ON to OFF before this occurs it is possible to stop the machine, but if the actuator disengages with the contact point on the side of the safety circuit still turned ON, the machine will not stop even if the door is opened and the operator will be exposed to danger.

Therefore, it is important to examine where the failure takes place and the subsequent function of the contact point on the side of the safety circuit. The structure of an interlock switch with solenoid lock can be classified in terms of “3 generations” of technological development, as shown in Table 1. This table summarizes the basic structures and the modes of expected failures.

With a first-generation interlock switch, it is not always possible to predict where a failure will take place when too much pressure is applied. In addition, the internal energy of the device always works in favor of maintaining it in a potentially hazardous state.

Because of this first-generation structure, it is expected that failures could occur at any of the following 4 locations: (1) where the cam and the actuator are hooked together, (2) where there is a gap on the cam shaft when it moves in the direction that pulls out the actuator, (3) where there is a deformation or failure at the point of contact between the cam slope and the rod and (4) when the notch in the cam fails to stop the rod. However, of these 4 cases, it is only in (4) that the contact point on the side of the safety circuit is turned OFF when the failure takes place. In cases (1) to (3), the failure takes place with the contact point on the side of the safety circuit still turned ON.

The second-generation interlock switch with solenoid lock also has the internal energy working in favor of maintaining the device in a potentially hazardous state, but incorporates the concept of controlling potential failures by turning the contact point OFF.

Because of this second-generation structure, it is expected that failures could occur at any of the following 3 locations: (1) where the cam and the actuator are hooked together, (2) where there is a gap on the cam shaft when it moves in the direction that pulls out the actuator, and (3) when the notch fails to stop the cam. If the amount of strength applied to (1) and (3) is intentionally manipulated so that the notch fails to stop the cam or if (3) takes place first, this will still cause a failure, but the device will remain safe with the contact point turned OFF. However, if the type of failure described in (2) takes place, the device could still be left in a hazardous state, as described above for first-generation systems.

With a third-generation interlock switch with solenoid lock, the expected failure locations are the same as the second-generation examples noted above. However, the different structural design ensures that the internal energy (reverse energy structure) now always works in favor of maintaining the device in a safe state.

Because of the way in which the contact point on the side of the safety circuit is kept in the OFF position by the internal energy, the third-generation interlock switch stays OFF even if the gap on the cam shaft moves in the direction that pulls out the actuator.

Based on these examples and considerations, we can conclude that a third-generation interlock switch with solenoid lock has the highest probability of maintaining safety even if a switch failure does occur.

Table 1. Comparison of interlock switch characteristics

	1st generation		2nd generation		3rd generation	
Direct Opening	Welded contact point on the side of the safety circuit is surely torn off by pushing in with the cam	Very Good	Welded contact point on the side of the safety circuit is surely torn off by pushing in with the cam	Very Good	Welded contact point on the side of the safety circuit is surely torn off by pushing in with the cam	Very Good
Prevention of operation by the tools other than the special actuator	only with the special actuator	Very Good	only with the special actuator	Very Good	only with the special actuator	Very Good
Energy on the contact point on the side of the safety circuit	<p>Close : Low ⇔ Open : High</p> <p>The internal energy always keeps the contact point on the side of the safety circuit turned ON.</p> <p>Circuit: ON (yellow) / Circuit: OFF (blue)</p> <p>inserted actuator stroke pulled out</p>	No Good	<p>Close : Low ⇔ Open : High</p> <p>The internal energy always keeps the contact point on the side of the safety circuit turned ON.</p> <p>Circuit: ON (yellow) / Circuit: OFF (blue)</p> <p>inserted actuator stroke pulled out</p>	No Good	<p>Close : High ⇔ Open : Low</p> <p>The internal energy always keeps the contact point on the side of the safety circuit turned OFF.</p> <p>Circuit: ON (yellow) / Circuit: OFF (blue)</p> <p>inserted actuator stroke pulled out</p>	Very Good
Basic Structure	<p>It is not always possible to predict where a failure will take place when too much pressure is applied. In addition, the internal energy of the device always works in favor of maintaining it in a potentially hazardous state</p> <p>【Foreseeable Failure Mode】</p> <p>(1) where the cam and the actuator are hooked together</p> <p>(2) where there is a gap on the cam shaft when it moves in the direction that pulls out the actuator</p> <p>(3) where there is a deformation or failure at the point of contact between the cam slope and the rod</p> <p>(4) when the notch in the cam fails to stop the rod</p> <p>【Failure Example】</p> <p>The shaft deforms, causing the cam to be displaced, but the contact does not turn off.</p> <p>Pull off with force</p> <p>LOCK The safety circuit: ON</p>	No Good	<p>The internal energy working in favor of maintaining the device in a potentially hazardous state, but incorporates the concept of controlling potential failures by turning the contact point OFF.</p> <p>【Foreseeable Failure Mode】</p> <p>(1) where the cam and the actuator are hooked together</p> <p>(2) where there is a gap on the cam shaft when it moves in the direction that pulls out the actuator</p> <p>(3) where there is a deformation or failure at the point of contact between the cam slope and the rod</p> <p>(4) when the notch in the cam fails to stop the rod</p> <p>【Failure Example】</p> <p>(1) is designed to have more strength than (3), so that the contact turns off when the notch is damaged. But the contact does not turn off when there is a gap on the cam shaft when it moves in the direction that pulls out the actuator.</p> <p>Pull off with force</p> <p>LOCK The safety circuit: OFF</p>	No Good	<p>the expected failure locations are the same as the second-generation examples noted above. However, the different structural design ensures that the internal energy (safety potential) now always works in favor of maintaining the device in a safe state.</p> <p>【Foreseeable Failure Mode】</p> <p>(1) where the cam and the actuator are hooked together</p> <p>(2) where there is a gap on the cam shaft when it moves in the direction that pulls out the actuator</p> <p>(3) when the notch fails to stop the cam</p> <p>【Failure Example】</p> <p>The cam shaft deforms, causing the cam to be displaced. Contact turns off.</p> <p>Pull off with force</p> <p>LOCK The safety circuit: OFF</p>	Good
Assessment of safety in the case actuator is pulled out stronger than the specified lock strength value						Very Good

3. Conclusion

This paper discusses the reliability of “third-generation interlock switches with solenoid lock” in terms of their ability to ensure safety in the event of a switch failure. An interlock switch of this type, with solenoid, can be used as a safeguarding measure - physically separating the operator and the hazard.

In principle, it is desirable to only use an interlock switch with solenoid lock within the range specified for the product in question and in the appropriate working environment. For example, when the switch is properly installed and the pressure exerted on the interlock switch throughout its lifetime does not exceed its design parameters and strength tolerances, even a first- or second-generation interlock switch will function correctly and not break. However, in actual use, unexpected pressure can be applied or an unexpected failure can occur in the working environment in which such a switch is installed. We therefore assessed various operating systems in conditions where “the interlock switch with solenoid lock may break”. In such cases, there was a great deal of difference in the ability of first- and third-generation switches to maintain safety, and our assessment concluded that a new concept of operator safety should be adopted, extending the existing definition to include safety even in the event of a switch failure. Our results also showed that the type of switch selected to achieve this should incorporate third-generation design and technology.

We have developed a HSIL interlock switch, as shown in Figure 5, which complies with all existing conventional international standards and incorporates the principles of third-generation design into its basic structure. Figure 6 compares the internal structure of the HSIL interlock switch with solenoid lock to one of the third-generation interlock switches shown in Figure 1. When excessive force is applied, the cam shaft deforms and shifts the cam itself. As a result, the internal energy of the device ensures that the contact point on the side of the safety circuit is turned OFF. This ensures operator safety even in the event of switch failure.

Some way of decreasing the number of workplace accidents is needed urgently. We will continue to further improve the safety of the internal switch described above by all possible means, incorporating any new ideas and concepts as they arise and making use of all available technology. In conclusion, we would also like to express our deep appreciation to the members of IDEC for providing us with much advice when preparing this paper.



Fig. 5 HSIL interlock switch

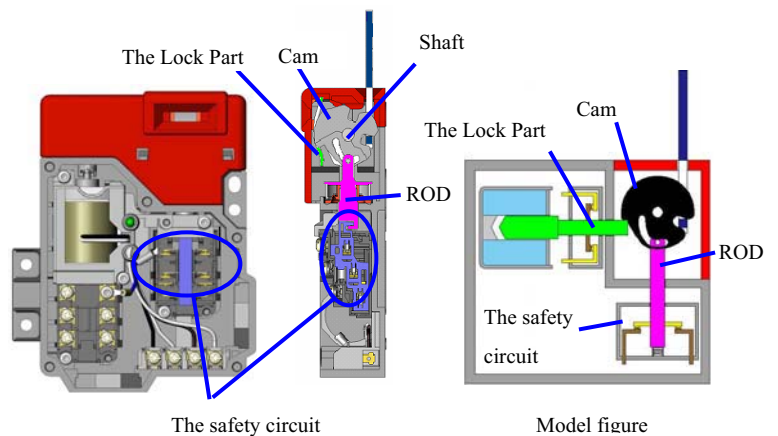


Fig. 6 Internal structure of HSIL interlock switch

Acknowledgements

The authors would like to thank all the people of IDEC Corporation who offered kind guidance and advice to the completion of this paper.

Reference

- [1] ISO12100 ; (2010), Safety of machinery -- General principles for design -- Risk assessment and risk reduction -
- [2] IEC60947-5-1 ; (Ed.3.1 2009/ Ed.3.0 Amd 1:2009), Low-voltage switchgear and controlgear. Part5-1: Control circuit devices and switching elements - Electromechanical control circuit devices
- [3] ISO14119: (1998/Amd 1:2007), Safety of machinery -- Interlocking devices associated with guards -- Principles for design and selection
- [4] M. Mukaidono, Machine System Safety Technology in the Age of Globalization, edited by the Society of Safety Technology and Application, The Nikkan Kogyo Shimbun, Ltd. 2000
- [5] Y. Kamino, et al., « Coexistence of Human and machine from the Standpoint of Safety », presented to the Human Interface Symposium 1999, pp. 801-806
- [6] Takayuki Sakai , Takashi Iwami , Masashi Fujimoto , Shigetoshi Fujitani , Atsushi Matsumoto , Toshihiro Fujita , Lanny Schuberg ; «DEVELOPMENT OF A NEW EMERGENCY STOP SWITCH TO ASSURE AN OPERATOR’S SAFETY AGAINST FORESEEABLE FAILURE» ; presented to the Human Interface Symposium 2003, Human Interface Society, Japan, 2003

Safety Control for Collaboration Work of Press Machine and Person Based on Safety Level Defined by Position and Velocity Vector

Yukio Hata, Yuji Hirao

Komatsu Ltd. / Nagaoka University of Technology

1603-1, Kamitomioka, Nagaoka, Niigata 940-2188, Japan

E-mail uhh03796@nifty.com, yukio_hata@komatsu.co.jp, hirao@vos.nagaokaut.ac.jp,

KEY WORDS: press machine, Safety distance, position, velocity, vector

ABSTRACT

In international standards of protection against mechanical hazards, for collaboration of machine and person, in which inherent safety measures are not possible, measures to ensure safety based on isolation or stop are required. However, in hand-in-die work, i.e. work by a worker's hand within the press machine operation area, simultaneous operation by machine and person is accepted during the machine's upward process to the stop at TDP, top dead center. This paper, aiming at the hand-in-die-work which is common in small-scale press machines, proposes a new safety control for collaboration work of press machine and person based on a safety level defined by the position and velocity vector, a control which is based on the consideration that safety/risk levels vary depending on the relative position and velocity of machine and person. Concretely, safety levels are determined by dynamic safety distance, which is obtained by monitoring the movements of the press machine and the person continuously, i.e. the position and velocity vectors, and press machines are controlled appropriately to ensure safety for the collaboration work depending on the safety levels. This new safety control is specifically effective in muting work of press machines, which is one of the most acute problems, and it is applicable not only to press machines but also to a wide variety of machines at work. It also substantially contributes to the enhancement of productivity as well as safety.

1 INTRODUCTION

The press machine is known as one of the most dangerous machines. The injury by the hand in die work which takes material and a product in and out of a dangerous area manually has occurred mostly. This paper focuses on the hand in die work which is the collaboration work of press machine, and person, and shows the outline of the control system from the viewpoint of the safety of the collaboration work of machine and a person. First, the issues of the safety control system of the collaboration work of machine and person during muting of the protective device in the tool area and so on are picked up. Next, we define the dangerous and safety conditions and consider how these conditions are applied to the safety control system for the collaboration work of machine and a person. And we evaluate the effects of this system for the safety for the collaboration work of machine and person, and the improvements of the productivity. We think that this system will lead to good contribution to the safety collaboration work of machine and person and the improvements of the productivity.

2 Present issues of the press machine

Muting of the protective device of press machine is defined as "temporary automatic suspension of a safety function(s) by safety related parts of the control system during otherwise safe conditions in the operation of a

machine"[1]. And Muting is allowed during the opening stroke (upward process) or allowed when the dangerous phase of the closing stroke (downward process) is passed and there is no risk of injury at the tools. Actual application of the muting area is set by cams and/or the information of the encoder that detect the crank angle and are applied only for the single mode that will stop at TDP(top position of the press stroke).

The some of the present issues of the collaboration work of press machine and person are followings. .

- 1) Muting is allowed only for single stroke. And the tool setting is operated by inch mode without using the protective device. Then the inch mode is used under the limited moving stroke length or speed. Its operability and safety are not good for operators.
- 2) The setting area of the Muting (and other safety related settings such as braking monitor and TDP stop and so on) shall be considered all ranges of the machine speeds and the stroke lengths (see fig.1). And therefore the present setting of the safety related part of the press control system is limited by the machine speed. These limitations make the setting of safety related control and the operability of press machine difficult. And sometimes, these difficulties depending on the operator may cause the human error and accident, and the limitation by the machine speed reduces the productivity of the machine.
- 3) The present brake monitor is detected only when the "overrun" occurs. Recently in the press machine field, Servo driven press machines without clutch systems spread in the market. Therefore the "overrun" needs to be detected before the "overrun" failure occurs.

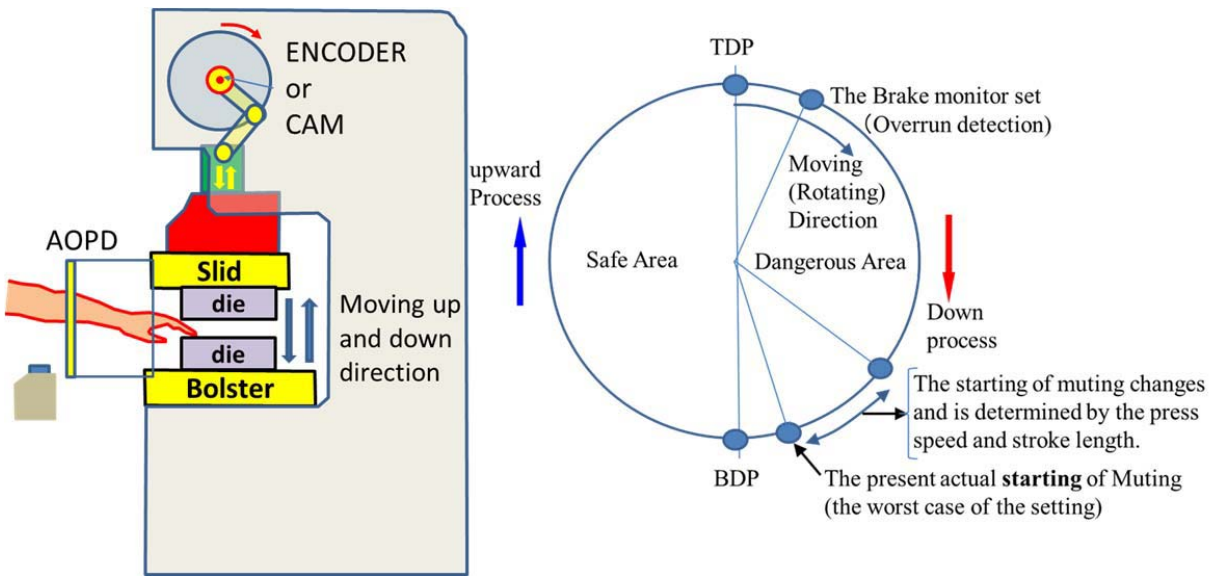


Fig.1 Single stroke of the press machine

3 Technical approach to the present issues

First, the safe conditions in the downward and upward processes of a press machine are defined by a model of the press machine which uses single AOPD shown with Fig. 1. The collaboration work of machine and person is fundamentally regarded as the hazard to all the area during downward process of press machine and regarded as the safe area during upward process of press machine. However, safe conditions may be satisfied with the case that a part of body cannot reach at a Hazard zone certainly during the downward process of a press machine or it can

escape from a Hazard zone. The model which determines the safe conditions on the downward and upward processes of the Press machine is shown with Fig. 2. The AOPD is installed according to the Safety distance(Ds) that is calculated by ISO13855 [2]. The safe condition during the downward process is that the slide position has already been in the upward stroke when a part of human body reaches to the hazard zone. Then the safe condition during the downward process is shown with the relations (1). And the starting position of muting during the downward stroke is shown with the relations (2) that is converted from the relation(1).

$$(DS/Vh(t)) \times Vm(t)+Pm(t) > 180(\text{deg.}=\text{degrees}) \quad -(1)$$

$$Pm(t) = 180(\text{deg.})-Vm(t) \times (Ds/Vh(t)) \quad -(2)$$

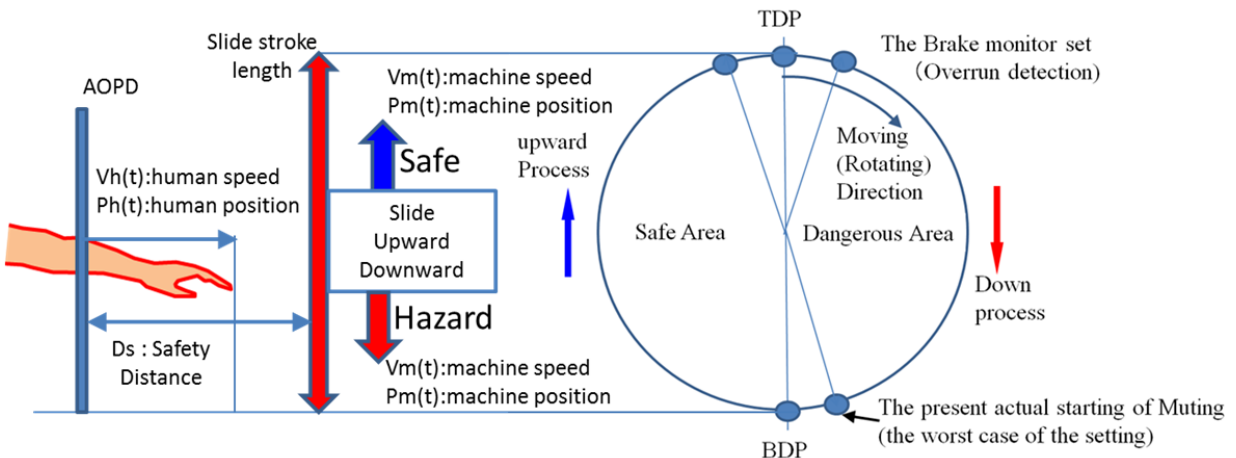


Fig.2 Model for the determination of the safe and hazard condition of upward and downward process

Next, in the collaboration work of machine and person, it can be fundamentally regarded as the safety during all upward process of the press machine. But if a part of human body cannot escape from the hazardous zone until the slide moves from upward stroke to downward stroke, it may lead to a serious injury of person. Then the safe condition during a collaboration of machine and person on the upward process is calculated by checking the dynamic travel distance obtained from the slide position, and slide speed and moving direction, If the dynamic travel distance plus present position is less than TDP position, the condition of a collaboration of machine and person is safe.

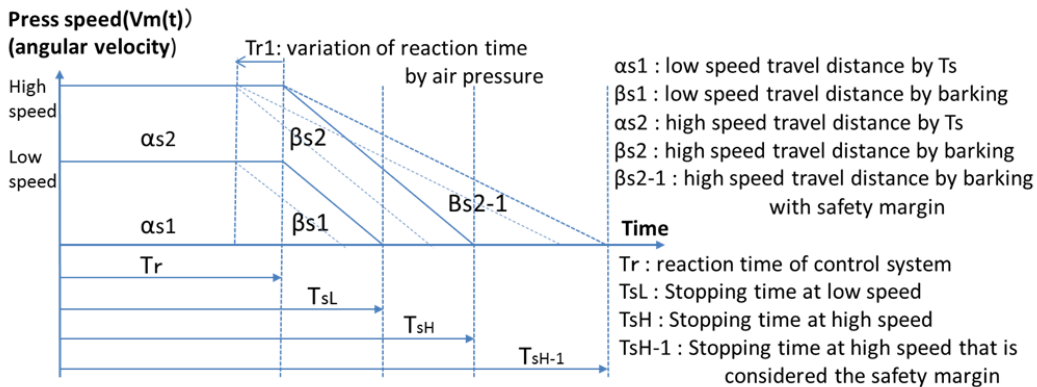


Fig.3 Angular velocity variation during stopping and total travel distance

Then the safe condition during the upward process is shown with the relations (3).

$$\int_t^{t+T_{stotal}} V_m(t) dt + P_m(t) > 360(\text{deg.}) - (3)$$

As shown in Fig.3 , "Tstotal" is a parameter that consists of the reaction time(Tr) of the braking system and the braking time . "Tstotal" must be considered the worst case. The braking time is usually proportional to the speed of the press machine. But the reaction time(Tr) of the braking system is variable by the air pressure of the mechanical brake release. The worst case of "Tstotal" is usually obtained by the measured stopping characteristics at highest air pressure of the mechanical brake release.

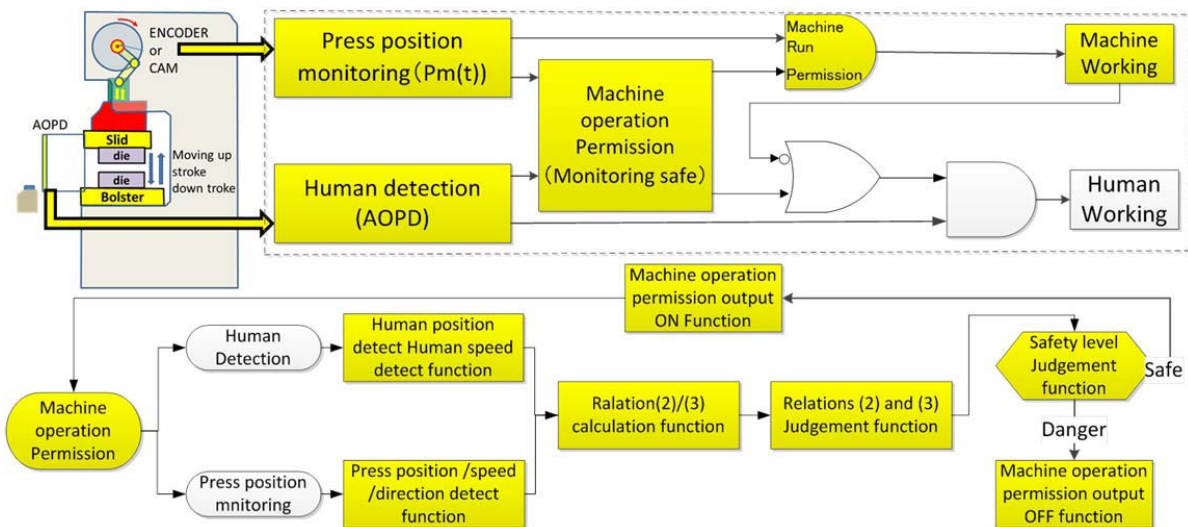


Fig.4 Function block of the Press safety monitoring system

Fig.4 is the Function block diagram of the Press safety monitoring system that we considered to achieve the safety collaboration work of a machine and a human. Safety category of each function in Fig.4 needs SIL3 IEC62061 [3] . Because the collaboration work of the Press machine. Safety category of each function in Fig.4 needs SIL3 IEC62061, because severity of harm from the hazard in the tool area of the Press machine leads to a serious injury.

4 Effect and Evaluation of the concept of the Press Safety Control

If this safety control for collaboration work of press machine and person based on safety level defined by position and velocity vector is applied to the press machine, the improvements can be anticipated not only in the safety but also in the productivity are expected. The followings are the improvements on the present press machine.

- 1) The safety condition will be kept with all press operation mode if the control system shown with Fig.4 is always applied to all the press modes and situations.
- 2) Especially, the press machine can reduce the risk of the "overrun" , because the ability to stop at TDP is monitored at all the time during the collaborating operation.
- 3) The muting position automatically changes by detecting the dynamic safety distance, and moreover by utilizing this control system the productivity will improve at higher speed because of the increase

of the operable time.

We have compared the working time (and working area for human) with the machine speed of 1 stroke as a comparative example between the present and the new proposal to see the improvement of the productivity. The selected machine specification is that the speed is 100spm (strokes per minute), maximum stopping time is 150ms, and the distance between hazard zone to AOPD is 300mm. The reaction time is usually 10-20% of all stopping time, but Fig.5 is calculated on the condition that as the reaction time is approximately zero. A working time ratio becomes large in the high speed area in which a production rate improves. And human working area also expands wider proportional to the higher machine speed. As a result of this system, the proposed control based on position and velocity vector will contribute to both the human safety and the productive efficiency.

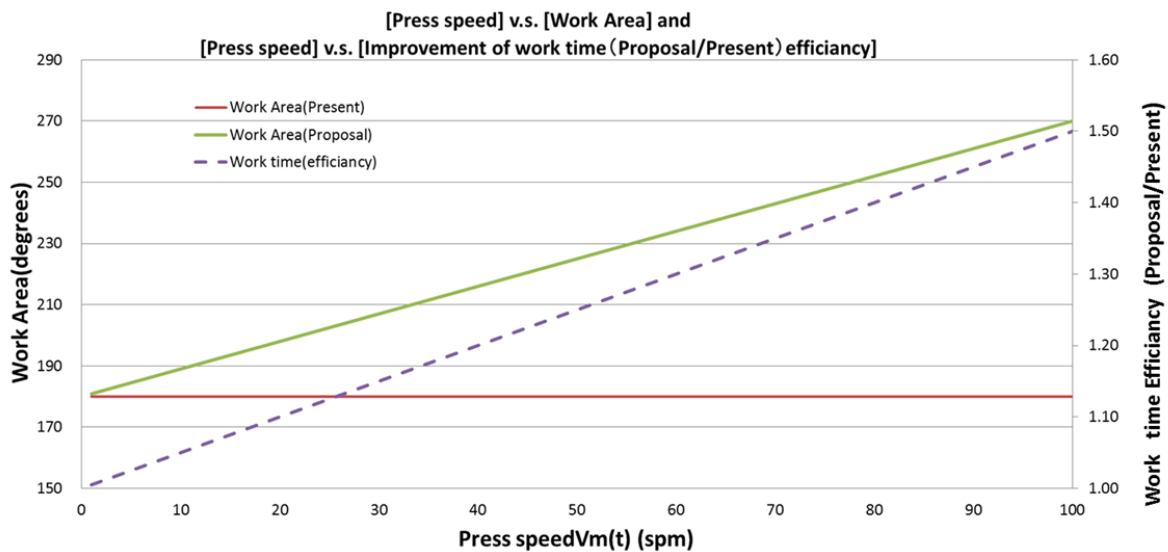


Fig.5 Improvement of Working efficiency

5 Conclusion and future study

The proposal of the safer and more productive control system of press machine for the collaboration work of press machine and person by definition of the safety level by position and velocity vector was shown in this paper.

In near future, servo driven press machines without clutch system spread in the market, and the press safety monitoring system by the definition of the safety level by position and velocity vector will be necessary in this market. Our next step is to apply this to the actual press machine and to study the efficiency and put it to practical use.

6 REFERENCES

1. EN692- Machine tools - Mechanical presses – Safety, 2005+A1:2009, 9p.
2. ISO13855-Safety of machinery — Positioning of protective equipment with respect to the approach speeds of parts of the human body,2010, 7p
3. IEC62061-Safety of machinery— Functional safety of safety-related electrical, electronic and programmable electronic control systems, 2005, Annex.A
4. Yukio Hata, Yuji Hirao, Safety Control for Collaboration Work of Machine and Person ,IEICE,Tokyo,28 July 2012, 3-4p

A Study of Risk Reduction Strategy using Supporting Protective Device

Shoken Shimizu, Shigeo Umezaki

National Institute of Occupational Safety and Health, Japan (JNIOSH), 1-4-6, Umezono, Kiyose, Tokyo, Japan
E-mail shimizu@s.jniosh.go.jp

KEY WORDS: Supporting protective device, Risk reduction ,RFID, Stereo camera

ABSTRACT

There are some operations in which workers need to approach the hazardous areas near s machine for trouble-shooting, maintenance, etc., while the machine is in motion, which is called as “hazardous point nearby operations.” Many risks exist when multiple workers operate in an extensive area, such as a large-scale manufacturing line, where work space often overlaps with the space held by movable mechanical equipment. In a worksite, even when a worker has entered a hazardous area, a third person may start mechanical equipment and an occupational accident may occur due to improper management or a dead angle arising from layout of the equipment. In order to prevent such accidents, workers’ qualifications and a task’s conditions must be confirmed, and workers’ locations must be appropriately monitored. The aim of this study is to propose risk reduction measures using supporting protective device, in which radio frequency identification (RFID) is used in combination with a camera. The proposed measures do not rely only on worker attentiveness. In this study, a model line was manufactured, in which a transportation system and a press machine were arranged, to evaluate the effects of the proposed risk reduction measures. Consequently, the occurrence probability of occupational accidents may be dramatically reduced.

1 INTRODUCTION

In Japan, the number of occupational accidents has gradually decreased since it peaked in 1961. In recent times, the work environment has undergone enormous changes; we have seen an increase in the variety of employment systems and the mass retirement of the Baby Boomer Generation of workers. Serious accidents caused by human error or an inadequate instruction manual have often occurred. In Japan, following the revision of international safety standards, such as the International Standardization Organization (ISO) 12100, the Guidelines for the Comprehensive Safety Standards of Machinery (published in June 2001 and revised in July 2007), and the Labor Safety and Sanitation Law (revised in November 2005), it has become obligatory for business owners to execute risk assessment and establish safety measures based on the results of that assessment. The concept of risk reduction is based on either “spatial separation” or “temporal separation” (for example, keeping workers away when the hazardous source is in motion or, alternatively, stopping the movement of the source when workers approach it). However, there are some operations in which workers need to approach the dangerous moving parts of a machine while the parts are in motion in order to facilitate checking, adjustment, processing, troubleshooting, maintenance, inspections, repairs, cleaning, or removal. We call these “hazardous point nearby operations.” There are also operations in which multiple machines are cooperatively controlled (an integrated manufacturing system (IMS)), or operated by multiple workers in a large area. In these operations, appropriate risk reduction cannot be achieved only through rigorous safety design policies or equipment-related safety measures. Therefore, risk reduction measures, such as the development of appropriate education, training, equipment management, and the use of protection devices, must be implemented at worksites. In these cases, the success of risk management is highly dependent upon human attentiveness; this introduces an element of uncertainty and, as a result, many occupational accidents have occurred. The aim of this study is to propose risk reduction measures using supporting protection equipment in which radio frequency identification (RFID) is used in combination with a camera. The proposed measures do not rely only on worker attentiveness. In this study, a model line was manufactured in which a transportation system and press machines were arranged and used to evaluate the effects of the proposed risk reduction measures. Consequently, the occurrence probability of occupational accidents may be dramatically reduced.

2 REQUIREMENTS FOR SUPPORTING PROTECTION EQUIPMENT

Machine designers and manufacturers provide users with information on how to use the equipment (including information on the protection measures that have been applied and the residual risks), whereas the machine’s users provide designers and manufacturers with the machine’s usage conditions when it is ordered and information obtained after its use (generally, information on “intentional use of the machine” provided by the machinery industry and information provided by specific users).

Basically, a system integration function is required, which takes into consideration technical information provided by the designers, the manufacturers, and the users of a machine. It also notes the distribution of workers required for the machine and its operational configuration and proposes appropriate residual risk management for the designers, manufacturers, and users. However, this function is not sufficiently applicable.

Risk reduction performed by a machine’s designers and manufacturers is based on either “spatial separation” or “temporal separation” (for example, keeping workers away when the hazardous source is in motion or, alternatively, stopping the movement of the source when workers approach it); thus, worksite safety is ensured when risk reduction is performed in this way. However, users of a machine are asked to handle almost all the hazardous points of nearby operations in which workers need to approach the dangerous moving parts of the machine while the parts are in motion and conduct infrequent operations (checking, adjustment, processing, troubleshooting, maintenance, inspections, repairs, cleaning, and removal of the machine) as residual risks.

Users of a machine make the effort to reduce these residual risks by reviewing the machine’s operation procedure, enhancing their education and training, and using protection devices. Among these residual risks, the safety level of the operations is barely maintained due to the machine’s operational configuration, based on the attentiveness of workers who, in many cases, have been appropriately educated and trained. However, risk reduction measures are highly dependent upon human attentiveness; this introduces an element of uncertainty and, as a result, many occupational accidents have occurred. Supporting protection equipment that can improve risk reduction measures with high uncertainty is defined as “equipment to support risk reduction measures with high uncertainty, which takes into consideration information for use of a machine provided by its designers and manufacturers (information of residual risks), risk reduction measures such as education, training, and management performed by its users when it is used, and human errors.”

Figure 1 shows the differences between risk reduction measures that depend solely on the machine user’s human attentiveness weighed against the residual risks and the risk reduction measures that take into consideration the application of supporting protection equipment. Since risk reduction measures that only depend upon human attentiveness have been conventionally employed, regardless of the risk level, the uncertainty of maintaining safe operation of the machine is high and constant at any risk level. Therefore, when an error occurs, the severity of an occupational accident increases as the level of residual risk increases. Risk reduction measures, which take into consideration the application of supporting protection equipment, can be classified into the following three levels, based on the level of residual risk: (1) a level, at which risk reduction measures depend only on human attentiveness; (2) a level, at which both human attentiveness and supporting protection equipment are used; and (3) a level, at which risk reassessment is proposed to the machine’s designers and manufacturers. Depending upon whether or not supporting protection equipment is applied, the uncertainty decreases at each of these three levels as risk reduction measures are implemented and the level of residual risk increases. By lowering the dangerous failure rate, the probability of occurrence of injury can be reduced.

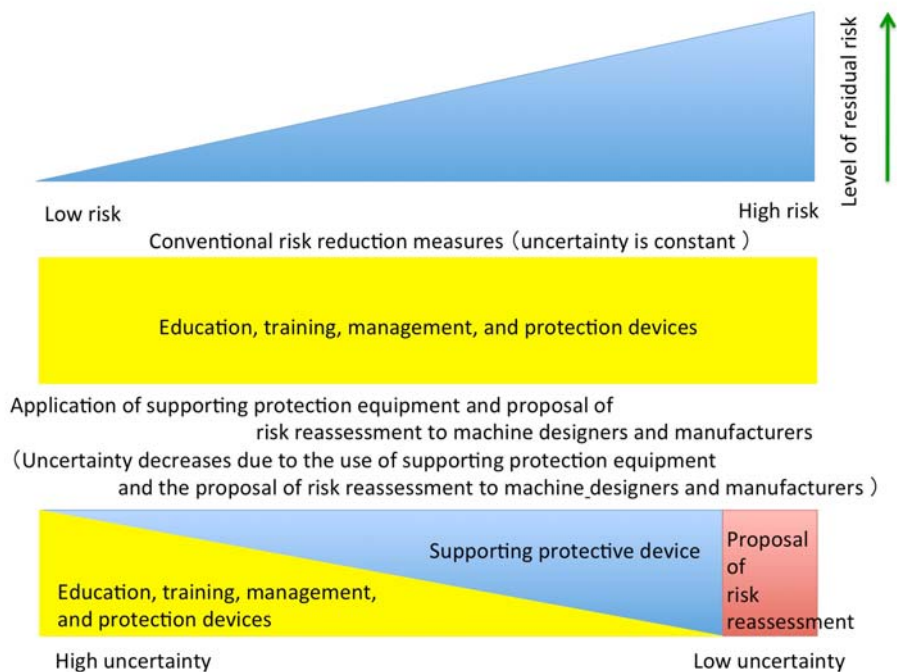


Figure 1. Risk reduction measures using supporting protection equipment.

Figure 2 shows a method to classify the requirements for supporting protection equipment. In Figure 2, the results obtained by analyzing risk elements of “severity of injury,” “frequency of accident occurrence,” and “uncertainty due to human attentiveness” are classified into five categories; additionally, the performance of human risk reduction measures at each risk level are classified into five classes. Here, human risk reduction measures that use supporting protection equipment are classified as Class B1, Class B2, or Class B3. Class A, in which the residual risks are low, corresponds to risk reduction measures that only rely on human attentiveness. Class C, in which the residual risks are high, proposes risk reassessment to the machine’s designers and manufacturers. The conditions required for applying supporting protection equipment consist of appropriate risk reduction performed by the machine’s designers and manufacturers and appropriate safety management of the residual risks performed by the machine’s users, which is based on the risk analysis proposed in international safety standards and guidelines and the priority of risk reduction measures. Therefore, as previously discussed, these conditions cannot be used as appropriate protection measures.

3 SYSTEM CONFIGURATION OF AN INTEGRATED MANUFACTURING SIMULATION MODEL FOR VERIFICATION TESTS

Photograph 1 shows a simulation model used for verification tests. The area surrounded by a safety fence was specified as the area of virtual danger and a place at the center of the model was denoted as the virtual entrance gate. Using this model, verification tests were conducted. Figure 3 shows the overall system diagram of the model. In the verification tests, four active tag readers were installed at four corners (one reader at each corner) in a virtual danger area surrounded by a wire-netting fence that was 2.4 m high. In front of the virtual entrance gate, two LF mats (a mat with a built-in antenna coil for RFID with a 125-kHz band) were placed approximately 1 m apart (this is referred to as the LF gate). In between the two LF mats, a stereo camera was installed at a height of 2.5 m (hereinafter a gate in which two LF mats are used in combination with a stereo camera is referred to as the virtual gate). The virtual gate could judge whether a worker was entering or leaving the virtual dangerous area according to which LF mat was first passed over when each worker was wearing an RF tag (in the verification tests, an RFID tag with both active and passive functions is called an RF tag). The four active tag readers installed at the corners could judge whether a worker was in the virtual dangerous area by receiving signals related to the order in which each RF tag passed over each LF mat and, thus, it would provide the latest information regarding each worker’s location.

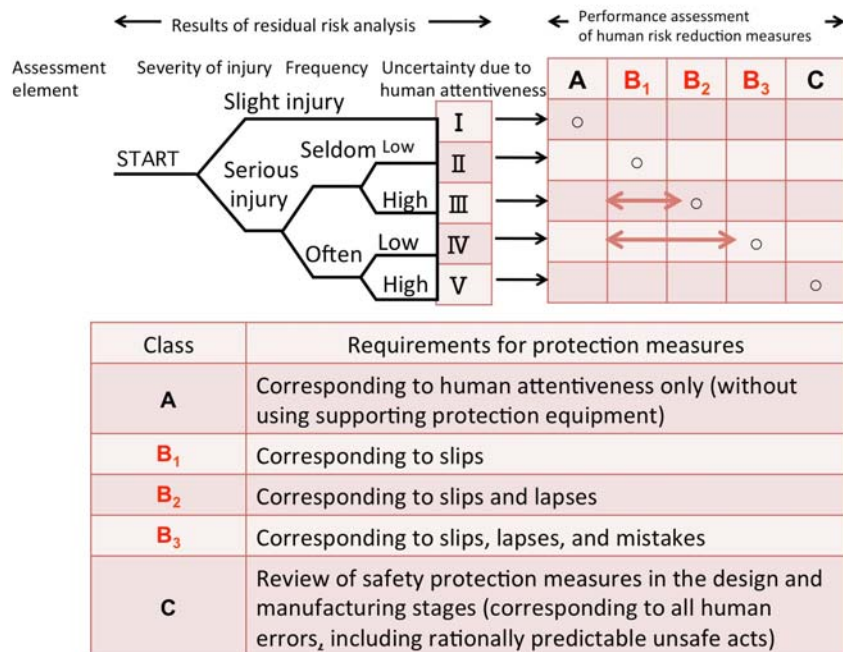


Figure 2. Method to classify the requirements for supporting protection equipment (example).

4 ITEMS AND RESULTS OF VERIFICATION TESTS

1) LF gate

We investigated the system's ability to both detect workers passing through the LF gate and to identify any workers present in the virtual dangerous area. We showed that by accurately adjusting the sensitivities of the FL mats, the RF tag's location and direction of its passage through the LF gate could be detected. The optimal conditions of this test were determined as follows: the sensitivity of the FL mat was best at 170 mm; the interval between the two FL mats should be at least 1 m; and there should be no metal objects within 1.1 m of each FL mat. In one situation, when multiple workers passed through the LF gate simultaneously, traffic signals from all the workers' RF tags could not be correctly received. However, by receiving additional signals that were transmitted after passage through the LF gate, as well as other periodical signals, it was ultimately possible to pinpoint the workers' latest locations.

2) Virtual gate

When only RF tags and active tag readers are being used and when multiple workers pass through the LF gate simultaneously, any one of whom is wearing an RF tag, a worker who is not wearing an RF tag cannot be detected. We wished to investigate whether the RF tag and reader could be used in combination with a stereo camera to cope with this kind of predictable human error and intentional unsafe act. We were able to demonstrate that the virtual gate, in which the RFID system was used in combination with a stereo camera, could correctly count the number of workers passing through the gate, with or without an RF tag.

3) Accuracy of detecting a worker's location

The active reader's optimum level for receiving signals from the RF tag varied according to a worker's carrying position. Since the performance of each RF tag differed, it was difficult to detect a worker's location in the dangerous area just by adjusting the active reader's level for receiving signals from the RF tag. To address this, RF tag-related technology must be improved and its use in combination with other technologies must be further explored.

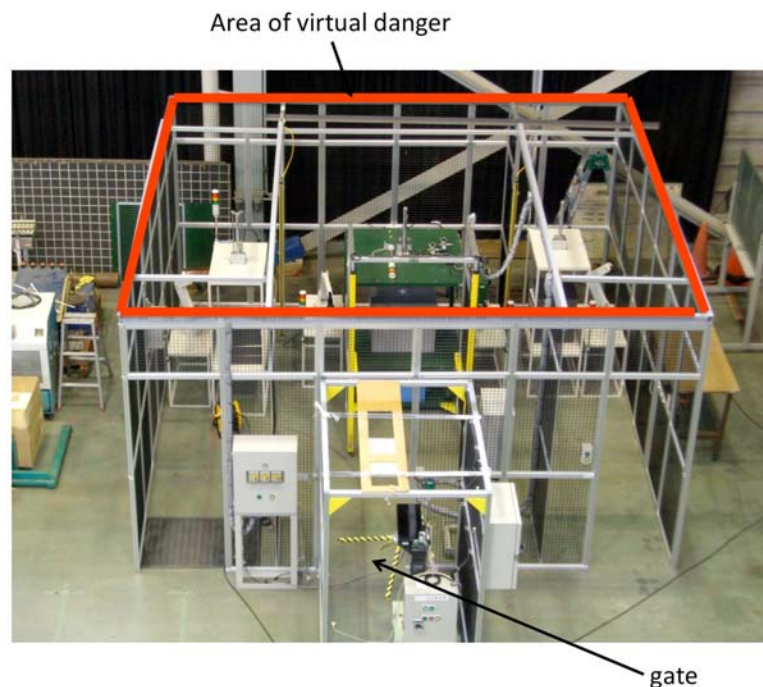


Photo1. Simulation model for verification tests

5 DISCUSSING AND FUTURE PERSPECTIVE

The present study examined “risk reduction measures taken by users” and verified the validity of a system in which RFID was used in combination with a stereo camera to propose a safety management system, based on a new concept of supporting protection equipment for hazard sources and hazardous situations, the risks of which were too high to only allow for a risk reduction system that is solely based on human attentiveness. The results obtained in the verification tests revealed that a device in which RFID was used in combination with a stereo camera could be used as supporting protection equipment, although the conditions regarding its management and installation must be determined.

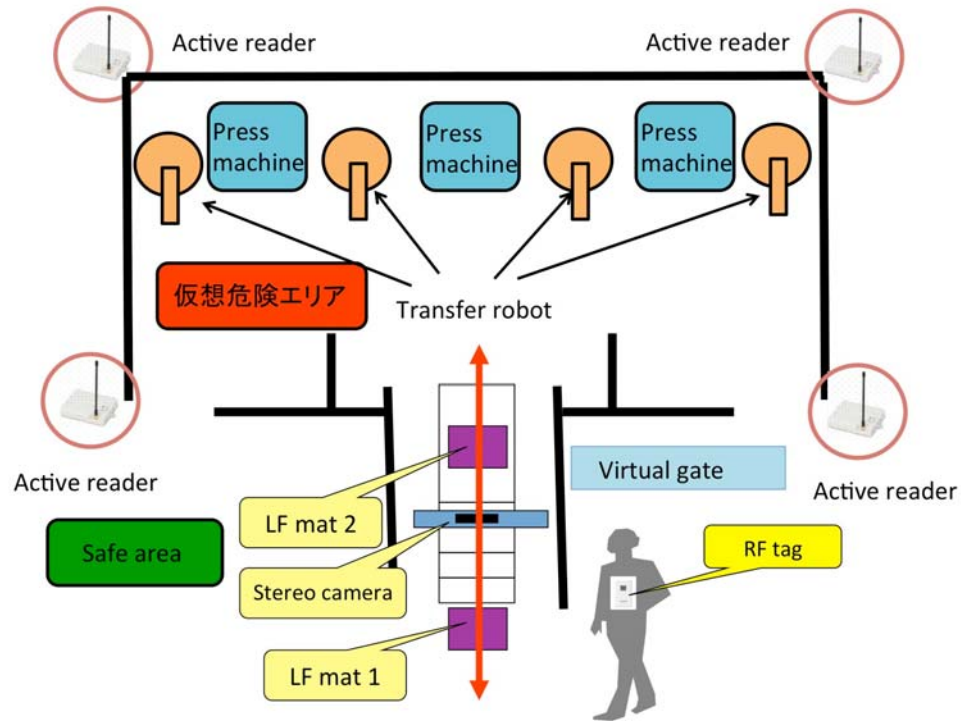


Figure 3. Diagram of the simulation model for verification tests.

Study on Evaluation of Position Detectors for an Interlocking Guard in Consideration of Safety and Hygiene Aspect

Hiroyuki OMURA¹, Takabumi FUKUDA², Noboru SUGIMOTO³

¹The Japan Food Machinery Manufacturer's Association, 108-0023, JAPAN,
ohmura@fooma.or.jp

²Department of System Safety, Nagaoka University of Technology, 940-2188, JAPAN,
t-fukuda@vos.nagaokaut.ac.jp

³Graduate School of Science and Technology, Meiji University, 214-8571, JAPAN
sugmac@meiji.ac.jp

KEY WORDS : Risk-based Design, Risk Assessment, Safety Engineering, Hygiene risks,

Abstract

Risks referred to by hygiene requirements (hygiene risks) differ from the risks of physical injuries and damage to health (safety risks) that specific machine operators suffer. And these measures for both risks sometimes conflict. The typical portion where these risks exist is the safeguard (guard) installed at the food processing part. A hygienic structure is needed for the processing part of food processing machinery. Hence, in designing the structure of the guard, which is installed to reduce risks existing in the actuator of the processing area, both safety risks and hygiene risks need to be taken into account. This paper will focus on the position detector that plays an important role in the interlocking guard used for food processing machinery, and clarify hygienic issues about the position detector which are not referred to by the relevant standard, conditions for the said detector that the designer should take into account, and considerations when selecting such detector.

1. Introduction

International standards on safety of machinery (Hereafter, "safety standards") are classified into three types, A, B, and C as shown in the introduction of ISO 12100[1].

The safety standards had been established with main focus on structural requirements to ensure operators' safety until 2002 when ISO 14159[2] ("Hygienic-B standard"), which is a type B standard that defines hygiene requirements, was created, so that hygiene requirements were introduced in a series of safety standards for the first time.

Risks targeted by hygiene requirements ("hygiene risks") are different from those of physical injury or damage to health suffered by operators of specific machines ("safety risks"). Main measures to prevent hazards caused by safety risks are generally constituted by such approaches as to stop energy sources that will cause harm, isolate workers from energy sources, etc. in principle. On the other hand, harm of hygiene risks are suffered by unspecified consumers of products processed by machines (e.g., foods, drugs, cosmetics, etc.), so that it is impossible to limit those suffer from the harm. Therefore, measures to prevent occurrence of the harm mainly consists of removing foreign body (cleansing, cleaning) and preventing retention of products, thereby minimizing proliferation of microorganisms.

However, when an energy source is stopped, which is regarded as a protective measure for safety, the product will be retained and then increase the probability of proliferation of microorganisms, while "isolation from energy sources" makes it difficult for workers to access residual foreign body for cleaning. In other words, in order to reduce hygiene risks due to those hazards, it is required to study how to minimize retention of products by preventing stop of machinery and equipment, etc. and structure that is difficult for workers to access them for

confirmation. As explained, protective measures for risk reduction on one hand may increase risks on the other hand so that designers should design carefully in view of that.

This paper focuses on a cam-operated device out of interlocking devices used for interlocking movable guards (“interlocking guards”) installed on surfaces in contact with foods (“food contact surfaces”), which are typical areas where caution is required for risk reduction involving safety risks and hygiene risks, and discusses safety issues that should be considered when a cam-operated device is adopted.

2. Requirements about hygienic structure of food processing machinery

2.1. International requirements about hygienic structure

WTO (World Trade Organization) has determined to provide international standards to protect health of humans and animals and avoid protectionist measures while recognising countries’ involvement in trade (GATT Article 20). Regarding hygiene, “Agreement on the Application of Sanitary and Phytosanitary Measures” defines harmonization to various standards created by Codex Alimentarius Commission (CAC). Regarding machinery, “Agreement on Technical Barriers to Trade ” defines harmonization to standards created by ISO/IEC.

Concept about hygienic structure of machinery is shown by “General Principles of Food Hygiene (GPFH)” in “Food hygiene – Basic texts[3]” issued by CAC. However, the requirements are mainly about performance of hygiene that should be considered in designing food processing machinery, and there are no descriptions about concrete methods, such as how to achieve the requirements. On the other hand, the Hygienic-B standard, which focuses on reduction of hygiene risks and defines concrete methods for that, does not describe relation to GPFH in particular, but as **Table 1** shows, the requirements shown by the Hygienic-B standard conforms to the performance requirements defined by GPFH.

Therefore, it is presumed that conformity to the requirements of hygienic structure of machines defined by GPFH is achieved by satisfying the structure shown by the Hygienic-B standard. Here, the Hygienic-B standard is one of the standards constituting a system of international safety standards. Therefore, when presuming conformity to GPFH using the Hygienic-B standard, it is necessary to study risk reduction measures based on the risk reduction process shown in Figure 1 of ISO12100. When implementing risk assessment in which safety risks and hygiene risks are combined, the repetition route shown by the risk reduction process becomes important [4].

Table 1 Relationship between the requirements of the hygiene principles and these of ISO 14159

Requirements of the hygiene principles	Article numbers of ISO 14159 requirements
cleanable and pasteurizable	5.2.1.1, 2.1, 2.2, 2.3, 2.5, 2.6, 2.7, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.16, 5.2.3.1, 3.3,
non-toxic	5.2.1.2, 1.3, 2.13, 3.4,
durable	5.2.1.1, 1.2, 1.3, 1.4, 1.5, 2.8, 3.3, 3.4,
accessible	5.2.2.2, 2.13, 3.1, 3.3,
controllable	—
ingress-proof	5.2.2.4, 2.15, 2.16, 3.2, 3.4,

2.2. Hygienic design and guard defined by international safety standards

According to ISO 12100, 5.5.2.1, a risk depends on “the severity of harm” and “the probability of occurrence of that harm.” When determining concrete hygienic structure based on international standards, it should be implemented based on levels of residual risks. For risk management, effective protective measures should be determined in the following sequence of “inherently safe design measures,” “safeguarding and complementary protective measures,” and “information for use.” “Inherently safe design measures” are measures to eliminate hazards or reduce risks by structural features without using a guard, etc. “Safeguarding and complementary protective measures” are measures to reduce risks using a guard, etc. “Information for use” involves measures to convey information about risks to users to avoid occurrence of harm.

Generally, a food processing part has a large opening in order to ensure “cleanable and pasteurizable” condition, one of the requirements of the hygienic structure. It is difficult to adopt the inherently safe design measures as protective measures to prevent operators from accessing to moving parts from an opening, as shown in section 1.

Therefore, it is generally studied to adopt an interlocking guard for an opening, which is one of the guards classified into “safeguarding and complementary protective measures.” However, when installing interlocking guards, unless hygienic hazards created after the installation are considered, there is a high probability of residual hygiene risks. The next section will explain outline of a cam-operated device, one of the interlocking devices used in interlocking guards.

3. Outline of cam-operated device used in interlocking guards

An interlocking device detects a safe state in which a guard is closed and generates safety information. It plays an important role in the safety of interlocking guards. ISO 12100, 6.2.11.3 prescribes that the action of start is implemented by “the passage from State 0 to State 1 if binary logic elements are considered.” Therefore, an interlocking device that gives starting conditions should be handled so that it generates state 1 energy in a safe state, i.e. a closed-guard state.

ISO 14119, 5[5] stipulates that a switch used for generating information about machine stop should operate in a positive mode, etc. A positive mode refers to a mode in which a moving mechanical component inevitably moves another component along with it by direct contact. (ISO 12100, 6.2.5).

A cam-operated device (ISO 14119, Annex A) is, for example, installed with a cam that operates in conjunction with opening and closing of a guard. It has a function to push a roller plunger when a guard is open, separate a contact forcefully, and disconnect power to a drive part. Therefore, an interlock using this switch allows power supply to a drive part only when the guard is closed (**Figure 1**). **Table 2** shows a logical mechanism of the interlock using this switch.

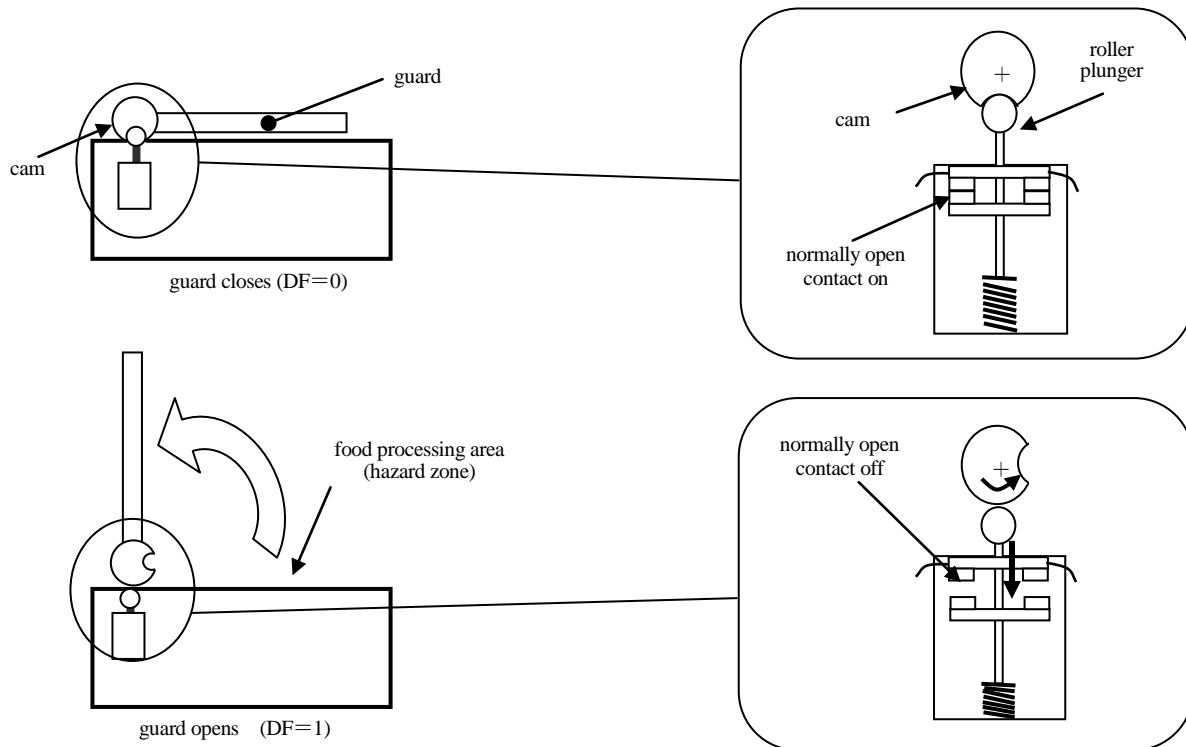


Figure 1 Example of the cam operated detector

Table 2 The combination concerned the position of the guard and the switching state of the contact

DF	Coff	Meaning of logic	Equation of logic	State of safety
0	0 (normal)	The guard is closed and the contact point is not off.	DF = Coff	Tolerable (DF ≤ Coff)
1	1 (normal)	The guard is opened and the contact point is off.		
0	1 (abnormal)	The guard is closed and the contact point is off.	DF < Coff	
1	0 (abnormal)	The guard is opened and the contact point is not off.	DF > Coff	Intolerable (DF > Coff)

3.1. Operation of positive mode

Mechanism of a positive mode is explained as follows using logical formulas. Here, open and closed states of a guard is expressed by a logical variable $DF \in \{1, 0\}$, with open being 1 and closed being 0. Additionally, a state of electric contact off is expressed by a logical variable $Coff \in \{1, 0\}$, with off being 1 and not off being 0. **Formula (1)** shows a logical relation between the guard and the electric contact point for a positive mode. However, if a tolerable failure mode, which will be explained later, is included, it can be expressed by **Formula (2)**. **Table 2** shows combination of the logical variables of these logical formulas and meaning of logical values.

$$DF = Coff \quad (1)$$

$$DF \leq Coff \quad (2)$$

A positive mode holds on the assumption that **Formula (1)** is true, but it is impossible to make a failure rate 0. There can be two types of failures. One is “closed-guard state, contact point being off (DF < Coff).” The other is “open-guard state, contact point being not off (DF > Coff).” In the state of “DF < Coff,” workers cannot access moving parts, so that this failure is called “failure on the safety side.” On the other hand, in the state of “DF > Coff,” workers can access moving parts when they are moving, so that this failure is called “failure on the hazard side.” A positive mode is defined as a mechanism that satisfies **Formula (2)**, in which failure on the safety side occurs predominantly.

4. Study on safety of cam-operated device for which safety is considered

Section 2 shows performance requirements on hygiene required for food processing machinery. Here, only the structural requirements, “cleanability and pasteurizability,” “accessibility,” and “ingression-proof” are discussed.

When a cam-operated device is properly water and dust proofed, it can be considered that it satisfies a condition of “ingress-proof.” However, a roller of a switch is less accessible. Therefore, in order to ensure not only “accessible” condition but “cleanable and pasteurizable” switch including a guard, normally, a guard of food contact surfaces is designed to be easily detached. When a guard is designed to be detachable, a serious problem arises regarding conformity to safety conditions. That is, when “a guard is not installed on purpose” or “a guard is forgotten to be installed”, “closed guard (DF=0)” information will be generated despite “open guard (DF=1)”.

Accordingly, the state of safety of this interlocking guard is evaluated as “intolerable” as shown in **Table 2**. In other words, by satisfying the “easily detachable” condition, i.e. a hygiene requirement, an intolerable guard of “DF > Coff” can be easily created.

In order to prevent a common cause failure of a positive-mode switch, ISO 14119, 5.4.1 and **Figure 4** refer to combination with a non-positive mode switch using b contact (normally closed contact) which becomes on when a plunger is pushed via a guard (**Figure 2**). In this case, as a switch element is made redundant, it helps reduce probability of failure. Also, as a non-positive mode switch directly monitors “closed” guard state, it is actually adopted in some machines as a measure to improve the drawback of generating “closed guard (DF=0)” information in an open-guard state.

Safety conditions based on a guard can be expressed by the following formula, with a state of the guard being DF (DF=1 is open guard, DF=0 is closed guard), a state of electric contact point off of a positive mode switch being Coff (Coff=1 is contact point off (open), Coff=0 is contact point not off (closed)), and a state of electric contact point on of a non-positive mode switch being Con (Con=1 is contact point on (closed), Con=0 contact point not on (open)) in a logical mechanism of this interlock system.

Additionally, “ \neg ” shows negative.

$$\neg DF = (\neg Coff \cdot Con) \quad (3)$$

In order to express DF without using a negative, the following formula holds according to De Morgan’s law.

$$DF = Coff \vee \neg Con \quad (4)$$

Table 3 shows combination of logical variables and meanings of logical values of this logical formula.

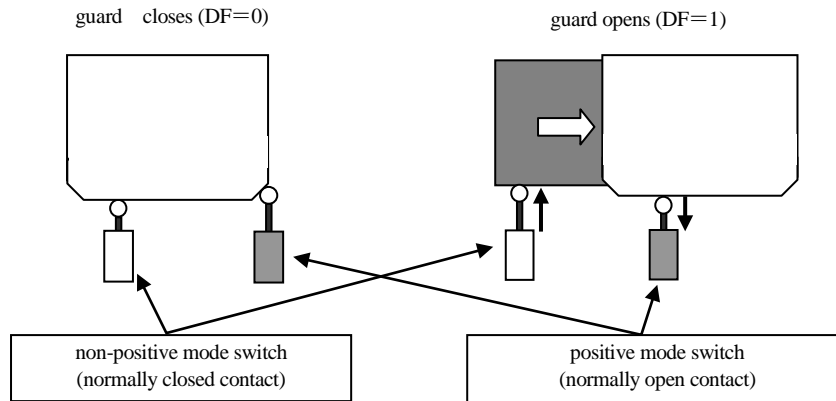


Figure .2 Interlocking with tow cam-operated switches

Table 3 Conformity and relation to the safety state shown by binary logic

DF		Coff	\neg Con	$Coff \vee \neg Con$	The state of operation	The state of safety
state	binary logic	Positive mode	Non-positive mode	combination		
Opened guard	1	1 (normal)	1 (normal)	1 (off)	normal	Tolerable $DF = (Coff \vee \neg Con)$
	1	1 (normal)	0 (abnormal)	1 (off)	abnormal	
	1	0 (abnormal)	1 (normal)	1 (off)	abnormal	
	1	0 (abnormal)	0 (abnormal)	0 (on)	abnormal	Intolerable $DF > (Coff \vee \neg Con)$
Closed guard	0	1 (abnormal)	1 (abnormal)	1 (off)	abnormal	Tolerable $DF \leq (Coff \vee \neg Con)$
	0	1 (abnormal)	0 (normal)	1 (off)	abnormal	
	0	0 (normal)	1 (abnormal)	1 (off)	abnormal	
	0	0 (normal)	0 (normal)	0 (on)	normal	

This model has a system in which dual switches are used and safety is represented by a product of two signals. Therefore, failure of either switch creates a signal of “open guard.” This state of failure on the safety side is represented by “ $DF < (Coff \vee \neg Con)$ ” or “ $\neg DF > (\neg Coff \cdot Con)$ ”, so that a tolerable state by this system can be expressed by the following formula.

$$DF \leq (Coff \vee \neg Con) \quad (5)$$

$$[\neg DF \geq (\neg Coff \cdot Con)]$$

However, even if dual switches are used, the problem of an easily detachable guard to ensure “accessible” and “cleanable and pasteurizable” conditions cannot be solved. That is because a non-positive mode switch can be easily disabled by a finger, tape, etc.

Accordingly, when adopting an interlocking guard using a cam-operated device, “a guard should not be detached easily” is an indispensable condition. Taking the fact into consideration that it is mainly operators that disable safety related guards, it is difficult to evaluate the safety risks as tolerable even if the measures that require “the use of special tools for detaching and installing guards” are taken.

5. Conclusion

The case of a cam-operated device in this paper is an example showing protective measures for reducing hygiene risks may increase safety risks. When using a cam-operated device for an interlocking guard requiring measures against not only safety risks but hygiene risks, state of safety can be evaluated as tolerable only when “accessible” and “cleanable and pasteurizable” conditions can be achieved without detaching a guard.

As explained above, it should be noted even protective measures that can be evaluated as “tolerable” for industrial machines in general can sometimes be “intolerable” when hygienic safety has to be considered.

References

1. ISO 12100: *Safety of machinery - General principles for design - Risk assessment and risk reduction*, 2010.
2. ISO 14159: *Safety of machinery - Hygiene requirements for the design of machinery*, 2002.
3. *Food hygiene -Basic texts*, Fourth edition, The codex alimentarius commission, 2009, pp. 9-10.
4. Ohmura H., Fukuda T., Futsuhara K., and Sugimoto N., *A Study of Risk Assessment Method Containing Hygiene Aspect and Safety Aspect*. Transactions of the Japan society of mechanical engineers, Series C, Vol. 77,2011, No. 784,2011,pp. 4682-4692.
5. ISO14119: *Safety of machinery - Interlocking devices associated with guards - Principles for design and selection*, 1998.

SIAS
2012

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



SESSION 4

**FUNCTIONAL SAFETY
AND CONTROL SYSTEM**

Validation of control systems

Integration of safety aspects in the Design of safety related parts in the control system in machines under consideration of the new EN ISO 13849-2 (FDIS)

Dipl.-Ing. Klaus-Dieter Becker
Professional Association
Printing and Paper Converting Industry
D-65185 Wiesbaden

Abstract

The integration of Safety and Ergonomics in the Construction and Design is fundamental important for the maintenance of industrial health and safety standards. A substantial contribution of the risk reduction results in the design of the safety related parts of the control system. From November 2006 follows with the publication of the new "EN ISO 13849-1:2006: Safety of machinery – Safety-related parts of control systems – Part 1: General principles of design" [1] as well as the retirement of the EN 954-1 in November 2011 a substantial change which influences the design of the safety related parts of the control system in the mechanical engineering. As a concluding process requires the EN ISO 13849-1 in paragraph 8 the validation of the safety functions. Verification and validation refer to quality assurance measures for avoidances of faults during the design and implementation of safety related parts of control systems which perform safety functions. In view of the new EN ISO 13849-2 [2] the following example of safety functions are emphasizing the integration in the design of the control systems with consideration of the new approach.

Introduction

In the valid standards EN ISO 13849-1 the required risk reduction of the safety related control system has to be determined as the result of the risk assessment. The necessary risk reduction will be described through the quantifiable aspects e.g. the reliability of the components, architecture of the control system, the diagnostic of the components and the consideration of the common cause failure for redundant systems. The standards EN ISO 13849-1/IEC 62061 has additional requirements for non-quantifiable aspects e.g. prevention of systematic faults. In modern control systems the application software and embedded software are more and more responsible for the necessary risk reduction. The software is not quantifiable. As the result of systematic fault in the design/modification of the software a fault can lead to loss of the safety function.

Based of the increasing automation in the mechanical engineering the safety functions are intensive linked with the function of the machines. The new standard EN ISO 13849-1 attempts to combine the complex probabilistic approach of the IEC 61508 with the generally recognized concept of categories of the EN 954-1. This is reached by that categories which are furthermore contribute an important part to the risk reduction. In addition there are new concepts e.g. the description of the reliability of parts, the description of diagnostic coverage (Diagnostic) and the description of requirements to the safety software. The requirements to the software are playing an important role, because software based computer systems taking over the tasks of the safety functions and the increasing level of automation leads to an intensive connection between the automation and the safety function.

The new EN ISO 13849-1 offers the possibility to assess the safety tasks of complex control systems with simply methods.

On machines with proper safeguarding, danger points and hazardous areas are not accessible during normal production runs. However, quite often various tasks (like plate changing, cleaning of cylinders, preventive or corrective maintenance etc.) are to be performed, for which the guards must be opened. When safety guards are opened, all drives that cause a hazardous movement must be safely stopped and an automatic (unintended) restart must be safely prevented. To stop drives on "electronic shaft" systems, the required command signals are transmitted to the individual drive elements by electronic bus systems. Consequently, also these bus systems are safety related components and the increased level of safety contributed to risk reduction by means of safety measures in control systems.

Unintended restart or speed-up of the machine with a guard open is extremely dangerous because it gives the operator very little chance to remove himself or parts of his body in time. This situation gets even worse on machines with individual drives (like web presses) because of the tremendous acceleration potential of such singular drive systems.

On the other hand, operations like cylinder cleaning or plate changing can only be carried out under

powered operational conditions. The machine however, may run only at safely reduced speed in hold-to run mode. In modern machines with singular drives, all motors are synchronised by the “electronic shaft”.

Signal processing for safety-related machine conditions such as opening of safety guards, hold-to-run mode with reduced speed, crawl speed or emergency stop, is under responsibility of the safety-related parts of the control system. As the result of realised safety functions in modern machines the complexity of the control system has increased.

So it is more and more important to describe reasonable procedure to validate the safety related functions. The new EN ISO 13849-2 will be published as FDIS (final draft international standard) and has included a machinery example describing the procedure of the validation taken to account the failure mode effect analysis (FMEA). The presentation will focus on what is required to comply with the essential requirements of the validation of the control systems and shall illustrate how the designer of the control system can validate the safety functions of the control systems taking into account the new approach of the EN ISO 13849-2.

Validation Procedure

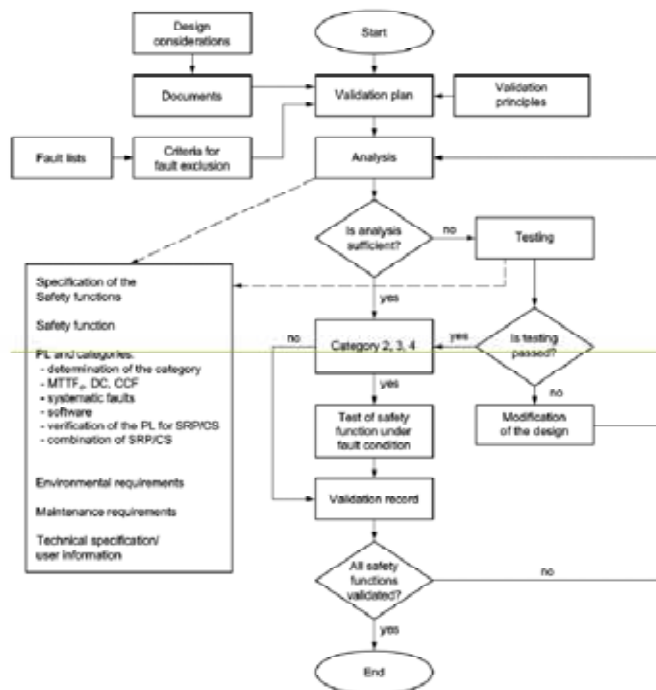


Figure1: Overview of the verification and validation procedure to EN ISO 13849-2(FDIS)

The process of assessment of safety function in its implementation by an SRP/CS is therefore a combination of verification and validation steps which deal with both the SRP/CS as a whole, and specific aspects of it. The procedure shown in Figure 1 can be employed for planning of the steps required for this purpose. In the new Standard is the first time a test with fault injection for redundant control system required.

Concept of PLC redundancy for opening of an interlocked guard and the stop function

If, for instance, in figure 2 illustrated control system, a guard is being opened, this information is processed to both PLCs. The operational PLC A initiates a stop via the current inverter (T1a). The rotation signal (cos/sin) of G1 is used for the regulation of the speed and the pulse sensor is used to read the current actual speed value into the monitoring PLC B and to compare it to the reference value. In case of a deviation exceeding a defined tolerance, the monitoring PLC B will disconnect the inverter (T1b) from power supply by means of using safe impulse blocking (via K1). This measure is required as in the event of failure in the operational PLC a, a normal operational stop or slow-down would not be possible any more. The signal of the rotation sensor G 1 and the signal of the pulse sensor G2 are fed into the operational PLC and also into the monitoring PLC b. Both PLCs can initiate safety actions.

Machine start-up with open interlocking guards must be possible only with speed reduced to safe level. The hold-to-run signal is also read into both processor systems. The functional PLC A acts on the inverter (T1a), i.e. for enabling and specification of nominal values. The rotation signal is used for control as well as for speed monitoring of the operative PLC A. Retrieval of actual values is also being read into the operative and the monitoring PLC B. In case of non acceptable speed increase due to a fault in the inverter, this fault is detected in monitoring PLC B. The monitoring PLC B can initiate the safety-directed action, i.e. initiation of safe impulse blocking. Incorrect nominal values due to a fault in the operative PLC A is also detected by the monitoring PLC B and lead, if the speed limit is exceeded, to stop by de-energising the power of relays K1. While the guard is in open position, it must be ensured that a fault in the enabling path of the operative PLC does not lead to uncontrolled start-up. This can be achieved by the monitoring PLC B disconnecting the power of K1 as soon as standstill is accomplished. Where disconnection from power supply is not feasible, removal of energy and possibly application of a brake in case of failure of the operative PLC B or the inverter can only be triggered by the standstill monitoring system of the monitoring PLC B. It must be checked that the response times of the monitoring system are appropriate so as not to present a non-tolerable hazard.

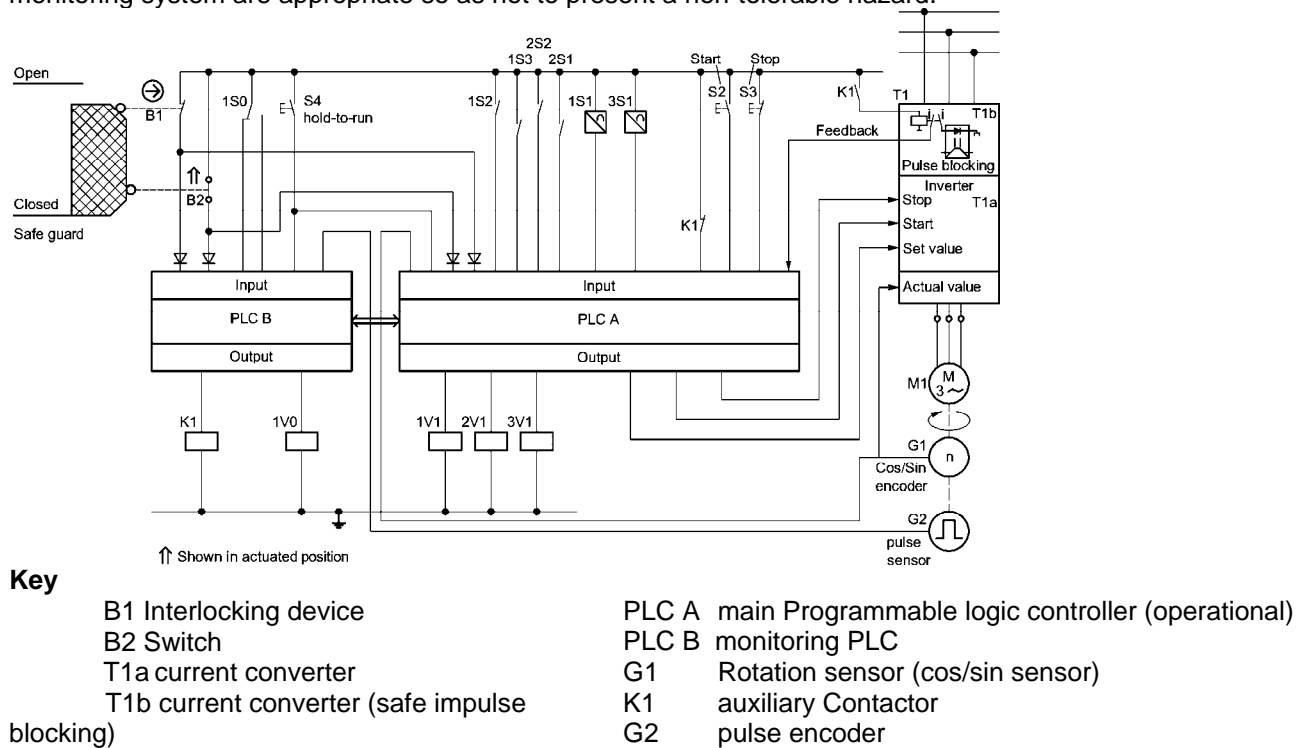


Figure 2: electrical functional diagram (above) and for the stop function in the case of opening interlocked safety guard

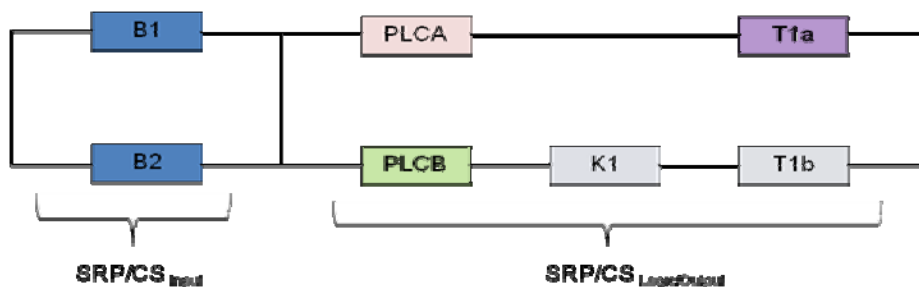


Figure 3: logical blockdiagram of the stop function

The safety-related parts of stopping function and their division into channels can be illustrated by the safety-related block diagram shown in Figure 3.

The Quantification of DC_{avg}

components	DC(%)	justification
K1	99	Due to normally open and normally closed mechanical linked contacts
S1	99	Due to normally open and normally closed mechanical linked contacts
S2	90	Due to normally open and normally linked contacts
PLCA	90	Checking the monitoring device reaction capability (e.g., watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility.
T1a	90	shut-off path with monitoring of the actuators by logic and watchdog
PLCB	90	Checking the monitoring device reaction capability (e.g., watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility.
T1b	99	Indirect monitoring (monitoring of relay K1)
G1	99	Fault detection by the process (all machine elements must run absolutely synchronously) and functional test ($\sin^2 + \cos^2 = 1$)

Table 1: calculated values of DC_{avg} related to the control system illustrated in figure 2

For an estimation of PL, an average DC value (DC_{avg}) is needed. The related DC of every tested component is illustrated in table 2 considering the simplified procedure described in table in [3] of the standard EN ISO13849-1.

Validation of sensor and PLC in consideration of FMEA for the stop function

With a failure mode and effect analysis (FMEA), the DC values that are assigned to each component SRP / CS by the implemented monitoring measures, and the failure of the system can be checked. During the FMEA of the safety function the fault consideration in both situations that means before and during the safety function (grey) is required has in the new standard EN ISO 13848-2 been taken to account. In the tables below is represented by which faults for each safety-related component (possible failure) can happen and depending on the realized measures the fault can be detected.

As a result of fault detection a safety related reaction has to be initiated. This is in the "action/ reaction" described. In the column "tests for conformation" is described how a successful validation can be run through considering fault injection.

Component/unit	Potential fault	Fault detection	Effect/reaction	Tests for confirmation
Interlocking switch B1	Contact does not open when the guard is opened (mechanical faults). ^a	Fault is recognized independently by PLC A and PLC B through signal change in B2 when the safety function is demanded (opening of the safety guard, plausibility check).	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs before the guard is opened.
	No dangerous fault while the guard is open (fault exclusion).	—	—	—
Interlocking switch B2	Contact does not open when the guard is opened (electrical or mechanical faults)	Fault is recognized independently by PLC A and PLC B through signal change in B1 when the safety function is demanded (opening of the safety guard, plausibility check).	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs before the guard is opened.
	Spontaneous contact closure while the guard is open (mechanical faults).	Fault is recognized independently and immediately by PLC A and PLC B as a result of there being no corresponding signal change in B1.	Electric motor M1 is stopped via T1a by the PLC A and via K1 and T1b by the PLC B and re-start is prevented.	Apply a static high level at the relevant input of both PLCs while the guard is open.

Table 2: FMEA and assessment of DC-values for components of Sensor B1 and B2 [5]

<p>PLC A</p>	<p>Stuck-at-fault at the input/ output cards, or stuck-at or wrong coding or no execution in the CPU, which prevents PLC A from sending a stop command to T1a before or when the guard is opened.</p>	<p>Fault is recognized by PLC B through reading of G2 to compare its time-related signal with the expected change in the number of revolutions. Some faults (e.g. output cards) are recognized by PLC A through reading of G1 at an operational stop of the electric motor M1 or when the safety function is demanded. Other faults can be detected early by the internal watchdog (WD^a) function of PLC A.</p>	<p>Electric motor M1 is stopped by PLC B via K1 and T1b after a time delay when the guard is opened, and re-start is prevented. In the case of faults detected by PLC A through reading of G1 during the operational stop, PLC A informs PLC B. As a result of reporting PLC B, the electric motor M1 is stopped and re-start is prevented by PLC B. In the case of faults detected by WD, PLC A tries to stop electric motor M1 and prevent the re-start via T1a before the safety function is demanded or before electrical motor M1 comes to an operational stop, and then to inform PLC B.</p>	<p>Apply a static high level at the stop output of PLC A before the guard is open.</p>
--------------	---	--	--	--

	<p>Stuck-at-fault at the input/ output cards, or stuck-at or wrong coding or no execution in the CPU, which removes the PLC A stop command from T1a while the guard is open.</p>	<p>Faults cannot be recognized by PLC B through reading of G2 because the motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. Some faults (e.g. output cards) are recognized by PLC A through reading of G1 on closing the guard. The above and additional faults are detected by operator through process observation on closing the guard, or by PLC B when the safety function is next demanded (opening of the guard). Other faults can be detected early by WDa function of PLC A.</p>	<p>Electric motor M1 remains stopped by PLC B via K1 and T1b while the guard is open. In the case of faults detected by PLC A through reading of G1 on closing the guard, PLC A informs PLC B. As a result of reporting PLC B, the unintended start-up of electric motor M1 is prevented by PLC B. In the case of faults detected by WD, PLC A tries to keep electric motor M1 stopped and to prevent the re-start via T1a, and to inform PLC B.</p>	<p>Transfer the start signal to the inverter while the guard is open.</p>
--	--	---	--	---

Table 3: **FMEA and assessment of DC-values for components of PLC [extract of 5]**

Conclusion:

As the result of realised safety functions in modern machines the complexity of the control system has increased. So it is more and more important to describe reasonable procedure to validate the safety related functions. The new EN ISO 13849-2 will be published as FDIS (final draft international standard) and has included a reasonable machinery example describing the procedure of the validation taken to account the failure mode effect analysis (FMEA).

References

- [1] ISO 13849-1:2006, Safety of machinery - Safety-related parts of control systems
- [2] EN ISO 13849-2(FDIS):2012, Safety of machinery - Safety-related parts of control systems, Part 2 Validation
- [3] ISO 13849-1:2006, Appendix E, Table E.1
- [4] ISO 13849-1:2006, Appendix K, Table K.1
- [5] EN ISO 13849-2(FDIS):2012, Appendix E, Table E.3 and Table E.4

Evaluating performance levels of machine control functions

Marita Hietikko, Timo Malm, Jarmo Alanen
VTT, P.O.Box 1300, FIN-33101 Tampere, Finland
Tel. +358 20 722 111, Fax +358 20 722 3499, marita.hietikko@vtt.fi, timo.malm@vtt.fi, jarmo.alanen@vtt.fi

Heikki Saha
Sandvik Mining and Construction Oy, P.O. Box 100, FIN-33311 Tampere, Finland
Tel. +358 400 346 537, heikki.saha@sandvik.com

KEY WORDS: machines, control function, safety

ABSTRACT

According to the basic machinery safety standard ISO 13849-1, the capability of a machine control system to perform a safety function is expressed using performance levels (PL). This paper brings out some challenges in the process of evaluating performance levels for safety related machine control functions. One of these examines the use of different cabling schemes in the implementation of a safety function and its effect on the PL evaluation. The challenges are highlighted using a generic example of a safety function relating to a mobile work machine where different technologies (electrical, hydraulic and pneumatic) can be utilized. A safety stop function with different structures was used as an example in PL calculations. Analogue cables in mobile work machines can cause a remarkable risk, since they are vulnerable to disturbances and failures. A part of these failures may be difficult to detect. In this study it was detected that by replacing analogue cabling with digital communications the reachable PL can be increased.

1 INTRODUCTION

According to the basic machinery safety standard ISO 13849-1, the capability of a machine control system to perform a safety function is expressed using performance levels (PL). The required performance level for a safety function is defined in a machine specific standard or it has to be defined using risk analysis. After ISO 13849-1 standard becoming effective, VTT has made several evaluations for estimating if required performance levels (PL_r) of machine safety functions are fulfilled. The purpose of evaluating performance levels for machine safety functions is to ensure the implementation of safety features in the control system of machinery.

Experiences have shown that the biggest challenges in evaluating the PL of the safety related parts of the control system (SRP/CS) are related to the formulation of the safety block diagrams for these parts and collecting source information for the PL calculations. Different evaluators may construct a safety block diagram for a safety function in various manners. This may lead to different results in the evaluation of the achievable PL. Also the input source of the failure rate data for the calculation has a huge effect on the $MTTF_d$ values. It is still difficult to get information relating to $MTTF$ values of components.

This paper brings out some challenges in the process of defining the PL of a safety function implementation. One of these examines the use of different cabling schemes of the SRP/CS and their effect on the PL evaluation. The challenges are highlighted using a generic example of a safety function relating to a mobile work machine where different technologies (electrical, hydraulic and pneumatic) can be utilized. The different principles and solutions for considering things in the evaluation of the PL are discussed in this paper.

2 PL ESTIMATION

When starting to evaluate the PL for a certain safety function it is important to clear up if the required PL (PL_r) exists for this safety function. PL_r may be expressed in the C type machinery safety standard. If the PL_r is found in the C type standard, it is applied. If the PL_r is not known, it can be estimated using a risk graph method given in ISO 13849-1. After this phase the safety function is to be designed so that the estimated PL_r is fulfilled.

After determining the PL_r for each safety function in a machine control system, a safety block diagram has to be drawn. This is done for each safety function and it consists of only those components that participate in the execution of the safety function. Usually a safety block diagram consists of input (e.g. sensors, limit switches etc.), logic and output (e.g. actuators, contactors etc.) components. The safety function can be either a single or dual channel solution. It is important to notice that the safety block diagram of a safety function may look completely different from the technical realization or, for example, from the functional block diagram. ISO 13849-1 introduces designated architectures, which show a logical representation of the system structure for each category (B, 1, 2, 3 or 4). The category of the SRP/CS should be chosen by the system architect, but in some cases, the category is pre-defined in the safety function specification along with the PL_r . The category also affects MTTF or $MTTF_d$ calculations.

When the safety block diagrams for the safety functions of the control system have been created, the MTTF or $MTTF_d$ values for the parts (components) of the safety functions should be collected. If there is no information available about MTTF or $MTTF_d$ values in the components manufacturers' data sheets (which is a typical case), the values of the ISO 13849-1 standard can be used. For components, the MTTF of which depends on the number of use cycles, the component manufacturer's data sheets may include information on the number of cycles until 10 % of the components of the same type fail dangerously (i.e. the B_{10d} values of components). In this case, $MTTF_d$ for the components can be calculated from the equations given in ISO 13849-1.

The diagnostic coverage (DC) should be estimated for the input, logic and output parts of the safety function. For estimating the DC for these parts, tables in Annex E of ISO 13849-1 are useful to go through. After this, the average DC (DC_{avg}) can be calculated for the safety function implementation and this can be done using the formula given in Annex E of ISO 13849-1. In general, structural principles can be used for avoiding, discovering or tolerate failures. In practice, measures like redundancy, diversity or monitoring can be used. In addition, the diagnostic coverage (DC) should also be at least "low" in order to reach PL d. The diagnostic coverage could also be estimated using FMEA, in which case the detection of each failure mode should be analysed. Finally, the common cause failures (CCF) for category 2, 3 and 4 structures should be estimated. In addition, software implementation and systematic failures should be assessed following the ISO 13849-1 standard. After carrying out these measures and estimating these parameters, the attainable PL for the safety function of the control system can be defined based on the graph given in ISO 13849-1.

3 ERRORS IN DISCRETE CABLING

Based on a long-term follow-up concerning mobile work machines, typical life time for an instrumentation cable varies between 1 and 3 years. The life time is mainly dependent on the operational environment, not on the signalling type. The failure rate of discrete wiring is higher than that of digital network wiring due to much larger amount of wire [3]. Single-channel discrete I/O-wiring cannot offer any confirmation about the signal validity, which is clearly required in safety related control systems by the standards [10]. An input device can only check, whether the input signal is within the specified range or not. Actual signal sources for analogue signals cannot be identified by the input-device. The actual transmitter may be the signal source, but also any wiring failure may contribute at least part of the signal value.

According to the safety standards, discrete wiring shall be analysed together with the corresponding subsystem [10]. Certain faults can be excluded only based on detailed justification given in the technical documentation [1]. It is clearly stated that a well-tried component for some applications can be inappropriate for other applications [2]. In machinery applications it means that cables need to be analysed because of relatively high cable failure rates.

4 ERRORS IN CANOPEN NETWORKS

One of the main targets of the CAN-communication has been to achieve less than one unrecognized error appearing in average life time of a vehicle [3]. The residual error rate cannot be computed directly by CRC and binomial distribution equations because of the various error detection mechanisms combined in CAN. Local errors are distributed globally, why increasing number of nodes per network decreases the residual error probability [4].

The residual error probability extrapolated from the published curves [5] is equal or less than the result of equation

1. Bit-error probability 10^{-3} [3] and 10^{-4} [5] [9] presented for CAN may be obsolete, because significantly lower values from 10^{-7} down to 10^{-11} are published later, together with the measurement arrangement [6]. Residual errors can be divided into the following categories: loss + masquerade (corrupted ID field maps to another safety critical message), loss + insertion (corrupted ID field maps to a non-safety critical message), loss (corrupted ID field maps to a not used message), and corruption (corrupted data field). Bit errors only in the CRC field are always detected. Subsequently, the CAN protocol executes a retransmission of the message that was corrupted. Retransmissions cause increase in the bus load. This shall be considered when assessing the delay errors and network scheduling.

All messages with corrupted data are potentially dangerous. Messages with a corrupted identifier are dangerous only, if the corrupted identifier corresponds to an identifier used by another valid safety critical message.

The message error probability can be either extrapolated from the curves presented in the literature [5] or computed from Equation 1:

$$P_{ME} = 1 - (1 - P_{BE})^{N_{BitsInMsg}} \quad (1)$$

Where P_{BE} is the bit error probability, P_{ME} is the message error probability and $N_{BitsInMsg}$ is the number of bits in a message. Furthermore, the residual error probability P_{RES} for CAN can be computed by Equation 2 [7]:

$$P_{RES} = P_{ME} \cdot 4.7 \cdot 10^{-11} \quad (2)$$

For simplicity, the residual error probability for both corruption and masquerade errors is assumed to be one, which is slightly pessimistic. Thus P_{Mas} equals P_{RES} . Finally, the effect of the masquerade errors can be computed based on the number of message identifiers in use – M_{InUse} – and total number of available message identifiers – 2^{IdSize} , where the use of 11-bit identifiers is assumed (see Equation 3):

$$P_{MasEff} = P_{Mas} \cdot \frac{M_{InUse} - 1}{2^{IdSize} - 1} \quad (3)$$

The most interesting result is that CAN communication can meet the SIL2 target or even SIL3 with reasonable safety measures, depending on the bit error probability specific to the application environment [7], and provided that the application messages and their protocol are carefully designed to tolerate all the communication error types (loss, insertion, unacceptable delay, unintended repetition, incorrect sequence, masquerade and addressing) besides the bit error caused corruption error (which is manifested as a masquerade, loss or insertion error if the bit error hits the CAN identifier field). The CANopen communication services and device profiles with proper application design tackle most of these error types. Heartbeat consumer and RPDO timeout monitoring are the main CANopen safeguards for signal transfers, covering deletion and timing errors. All detected errors in the CAN-layer are visible as delayed transmissions in the CANopen layer. Also insertions caused by an unspecified device or a configuration error can be detected, when a valid RPDO is received, but the heartbeat of the corresponding producer is missing. The TPDO inhibit time is the main safeguard against repetition. To follow a standardized design process is essential, because all communication is configured based on the system project information. Masquerade errors may be detected in the CANopen layer, if a corrupted message has a different number of data bytes than the corresponding valid message. Tolerance to repetition errors typically need to be verified by performance testing of RPDO-reception.

5 CASE STUDY

The safety function evaluated in the case study was a stopping function of a sub-system which is integrated on a mobile work machine. The PL for the safety related part of the control system that executes the stopping of the sub-system was estimated for three alternative structures, A, B and C. When estimating the PL the following presumptions were made: common cause failures (CCF), software implementation and systematic failures have been analysed and found to meet the requirements. The sub-system is normally stopped by releasing the joystick to the middle position. The stopping function of the sub-system can also be induced e.g. by exceeding encoder limits. In addition, the sub-system can also be stopped using emergency stop device, which cut off all power from the drives.

However, the PL calculations were executed for that case where a stop function is initiated by one of the encoders.

In the structure A, drives are located centralized as one block (Figure 1). There is a hard-wired safety cut-off device in the block. There is an individual I/O (4...20 mA for measurements), which is marked using narrow lines. The broad lines in Figure 1 denote CANopen. Scaling of measurements and control values as well as control and adjustment calculations etc. are made by PLC2. The safety block diagram for the structure A is presented in Figure 2 for the case where one of the encoders initiates the stopping function.

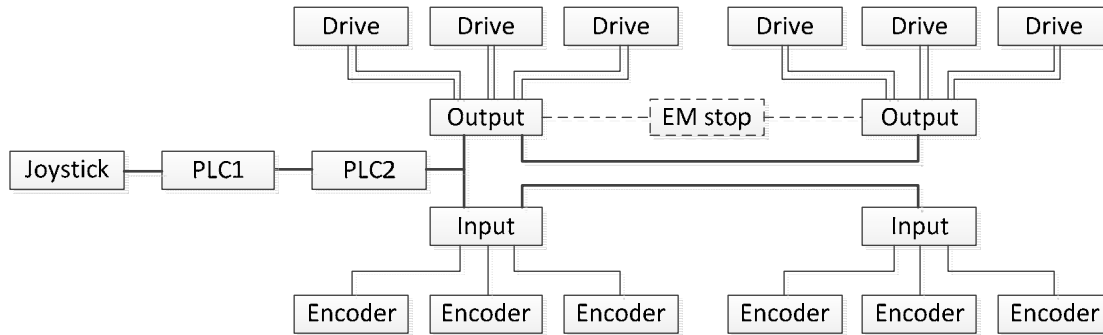


Figure 1. The functional diagram of structure A.

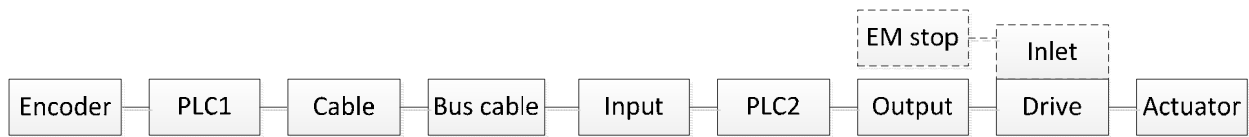


Figure 2. The safety block diagram of structure A, where one of the encoders initiates the stopping function.

The structure A is a single channel system and all parts have at least some kind of monitoring. The structure has relatively long analogue cables from the encoders to the input devices and from the output devices to the drives. These cables are sensitive to interruptions since the cables are situated outside of an enclosure and close to an actuator. The monitoring of encoders and their cables can detect a failure, which leads to values outside of the acceptable range. Sometimes water and dirt can cause a partial short circuit, which has acceptable conductance. This means that the diagnostic coverage is poor. The input part of the safety function was evaluated to fulfil the category 2 requirements.

According to a study [11], over 30 % of all failures in mobile work machines are related to cables or hoses. (Calculated from the cable failures, 66 % related to open circuits of sensor cables.) The value is 4 to 10 times higher than the value in stationary production [11]. This means that the cable failures cannot be neglected when mobile work machines are considered.

In the structure B (Figure 3), drives and encoders are like in the structure A. All components connect to the same CANopen network. The filtering and scaling of measurements and control values are realized in encoders and drives. All control and adjustment calculation is executed in PLC2. The safety block diagram for structure B is presented in Figure 4.

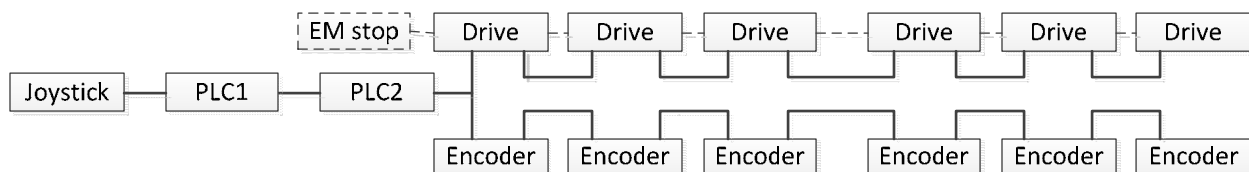


Figure 3. The functional diagram of structures B and C.

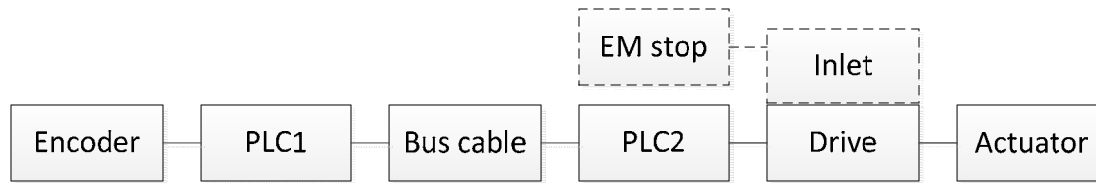


Figure 4. The safety block diagram of structure B, where one of the encoders initiates the stopping function.

The structure B is a single channel system, where all parts are monitored. The structure has no analogue cables and therefore the failures related to them do not exist.

The structure C resembles structure B but the difference is that the drives are integrated into the actuating devices. Only the safety cut-off device is located outside the actuator. CANopen network is implemented like in the structure B. Measurement filtering and scaling is implemented in encoders, and sub-system-specific adjustment is distributed into drives. Manual control is executed by deviating the target position of the sub-system. A redundant limit indication for the movement is implemented using another encoder. The safety block diagram for the structure C is quite similar to as presented for the structure B (see Figure 4). In the structure C solution, software is distributed to encoders and drives more than in the structure B solution.

When comparing the attainable PL for these structures, which represent category 2 solutions, a calculation example was done. The following $MTTF_d$ values for the components were used: 160 years for encoder, 50 years for PLC1, 24 years for input device and 4 years for analogue cables. Analogue cables with an input device were included when calculating the $MTTF_d$ for the input part of the structure A safety function. Using these values, the $MTTF_d$ of 3 years (low) for the input part of the structure A was got as a result. If the DC_{avg} is “low”, the reachable PL in this case is “a”, and it would not increase if the DC_{avg} is improved from “low” to “medium”. CAN bus cables were not included into calculations, because failures in CAN cables typically result in the situation in which there is no communication.

The corresponding calculations with the same $MTTF_d$ values for components were made to the input part of the structure B safety function, removing analogue cables and an input device from the calculations. Now, the $MTTF_d$ for the input part of the structure B safety function is 38 years (high). If the DC_{avg} is “low”, the reachable PL in this case is “c”. The reachable PL would be improved to even “d”, if the DC_{avg} could be increased from “low” to “medium”. Similar kinds of results were detected when calculating $MTTF_d$ values and PL’s for the output parts of the structures A and B. There is no difference in the PL calculations between structures B and C safety functions, if the same $MTTF_d$ values are used for the components.

6 DISCUSSION

The number of cables especially in mobile working machines has increased much. If buses like CANopen were not used, the number of cables would be still bigger. Instead of cables, wiring harnesses are installed to machines, which also increase the number of cabling in mobile work machines. If communication buses are used in the machine control systems, the number of cables is not as high as is necessary in the systems where buses are not used.

There are several challenges in the evaluation of PL’s (that may have an effect on the evaluation results):

- All cables can fail. In digital communication nearly all failures lead to the complete loss of communication, which can be easily detected. In analogue communication failures may lead either to the loss of signal or to a constant acceptable value. The constant value fault is difficult to detect.
- Cable failures are very typical in practice, but they are not usually taken into account in the $MTTF$ calculations. In mobile machines the cables are under hard stress (mechanical and environmental) and therefore they don't last as long as in an easy environment.
- Some $MTTF$ values of sensors may include also cable failures, but not all. This may bring false results in the calculations.
- Occasional disturbances are possible in all cables and are related to the environment and the quality of the connection. In the digital communication a message error is usually detected with specific checksums (e.g. CRC) and only very seldom an erroneous message can pass the check, and it would be even much rarer to

happen twice in a row. In analogue cables most of the disturbances can pass checking, but usually small changes are under control.

- Disturbances are not taken into account in the MTTF calculations, but only failures. Disturbances, which cause message errors, are calculated separately. Disturbances are more usual in bus cables than failures.
- When using digital communication, a single undetected erroneous message has not much time to produce a failure in an actuator (actuator too slow to do anything fatal). Usually the next correct message fixes the situation. If two consecutive errors occur, they are random (the same error does not usually happen again) and therefore, typically, they do not lead to a continuous dangerous state.

The performance level that is possible to be achieved can be improved, among other things, by removing analogue communication cables from the structure of the SRP/CS implementation. The use of a CANopen bus in the safety function decreases the probability of failures remarkably. The number of failing components in the safety function decreases and the remaining failures are easier to detect.

7 ACKNOWLEDGEMENT

The work is part of project FAMOUS (Future Semi-Autonomous Machines for Safe and Efficient Worksites), which is part of Fimecc's (Finnish Metals and Engineering Competence Cluster) research program EFFIMA (Energy and Life Cycle Efficient Machines). The main financier of the project is Tekes (Finnish Funding Agency for Technology and Innovation). The Finnish Work Environment Fund financed the previous project within which the tool for calculating PL's was developed.

8 REFERENCES

1. EN ISO 13849-1. 2006. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design.
2. EN ISO 13849-2. 2004. Safety of machinery – Safety-related parts of control systems – Part 2: Validation.
3. Kiencke U., Dais S., Litschel M., Unruh J., Error Handling Strategies for Automotive Networks, SAE technical paper 880587, SAE, pp. 19 – 28
4. Unruh J., Mathony H.-J., Kaiser K.-H., Error Detection Analysis of Automotive Communication Protocols, SAE technical paper 900699, SAE, 10 p. 10 p.
5. Charzinski J., Performance of the Error Detection Mechanisms in CAN, Proc. of 1st iCC, CiA, 1994, 10 p.
6. Ferreira J., Oliveira A., Fonseca P., Fonseca J., An Experiment to Assess Bit Error Rate in CAN, Proceedings of 3rd International Workshop of Real-Time Networks, 2004, pp. 15 – 18.
7. CAN Specification 2.0 Part B, Reprinted by CiA, 38 p.
8. Alanen J., Hietikko M., Malm T., Safety of Digital Communications in Machines, VTT Research Notes 2265, 2004, 93 p., ISBN 951-38-6503-7 (pdf).
9. Rufino J., Veríssimo P., Arroz G., Almeida C., Rodrigues L., Fault-tolerant broadcasts in CAN, Proceedings of the The Twenty-Eighth Annual International Symposium on Fault-Tolerant Computing, IEEE Computer Society, 1998, ISBN 0-8186-8470-4, pp. 150-174.
10. EN 62061. 2005. Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems. 26.09.2005. 201 p.
11. Hänninen S., Järvenpää J., Reunanen M., Suominen J. The failure of mechatronic components and devices. Technical Note 15/90. The Central of Finnish Metal, Machinery and Electrical Industries. 1990, ISBN 951-817-479-2 (in Finnish).

An *a posteriori* estimation of the performance level for a safety function using *NF EN ISO 13849-1:2008*

Sabrina JOCELYN¹, James BAUDOIN², Yuvin CHINNIH³, Philippe CHARPENTIER²

¹Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST)
505, boul. de Maisonneuve Ouest, Montréal (Québec), Canada H3A 3C2

²Institut National de Recherche et de Sécurité (INRS)
1 rue du Morvan - CS 60027 – F-54519 Vandœuvre-lès-Nancy cedex (France)

³Polytechnique Montréal
2500 chemin de Polytechnique, Montréal (Québec), Canada H3T 1J4

sabjoc@irsst.qc.ca
james.baudoin@inrs.fr
yuvin.chinniah@polymtl.ca
philippe.charpentier@inrs.fr

Key words: machine, control system, safety, function, performance level

ABSTRACT

In industry, machine users and people who modify or integrate equipment often have to evaluate the safety level of a circuit that they have not necessarily designed. The modifications or integrations can involve work to render an existing machine that does not comply with normative or regulatory requirements safe. A study was carried out to explore the feasibility of an *a posteriori* validation procedure for evaluating the safety level of such a circuit. Standard *NF EN ISO 13849-1:2008* is used for the procedure for the *a posteriori* (post-design) estimation of the safety level of a safety function. In the standard, the safety level is called the “performance level.” A horizontal plastic injection molding machine is used for the exercise. Several difficulties and limitations of the procedure were identified during the study. This article presents the most important ones, while discussing the results of this procedure undertaken for two different contexts of use: a laboratory context and an industrial context. The results obtained for these contexts differ. This difference is discussed while addressing the main limitations and difficulties encountered in the formulation of hypotheses, due to insufficient information from the designer.

1 INTRODUCTION

In industry, machine users and people who modify or integrate equipment often have to evaluate the safety level of a circuit that they have not necessarily designed. The modifications or integrations can consist of work to render an existing machine that is noncompliant with normative or regulatory requirements safe. For this, a study was carried out to explore the feasibility of an *a posteriori* (post-design) validation procedure that would make it possible to evaluate the safety level of such a circuit. The study also identified several difficulties and limitations of such a procedure.

As an example, this article presents the important difficulties and limitations encountered. The exercise was carried out on the circuit of a safety function of the 38-tonne horizontal plastic injection molding machine in the Machine Safety Laboratory at the IRSST. The adopted procedure and the discussion of the results are presented below.

2 The *a posteriori* validation

2.1 Procedure adopted

2.1.1 Identification and specification of the safety function, choice of standard

The procedure involves two preliminary steps: identification and specification of the safety function. These two steps are suggested by the current standards for safety-related control system design: *IEC 62061* [1] and *ISO 13849-1* [2] (more precisely: *NF EN 62061:2005* and *NF EN ISO 13849-1:2008*). The first standard applies to solely electrical, electronic and programmable electronic control systems. The second applies to electrical and non-

electrical (e.g., hydraulic) control systems. Therefore, once the safety function has been identified and specified, the applicable standard must be chosen from these two standards.

The safety function was identified as follows:

- Its safety action consists of stopping the closing movement of the movable platen (the targeted hazardous component) of the molding machine;
- The safety function is initiated by the following action: opening of the operator's gate. This is a gate ensuring the molding machine user's safety with respect to the hazards in the mold area (e.g., crushing or shearing risks from the closing movement of the movable platen (Figure 1));
- This safety function is valid during any mode of operation of the molding machine.

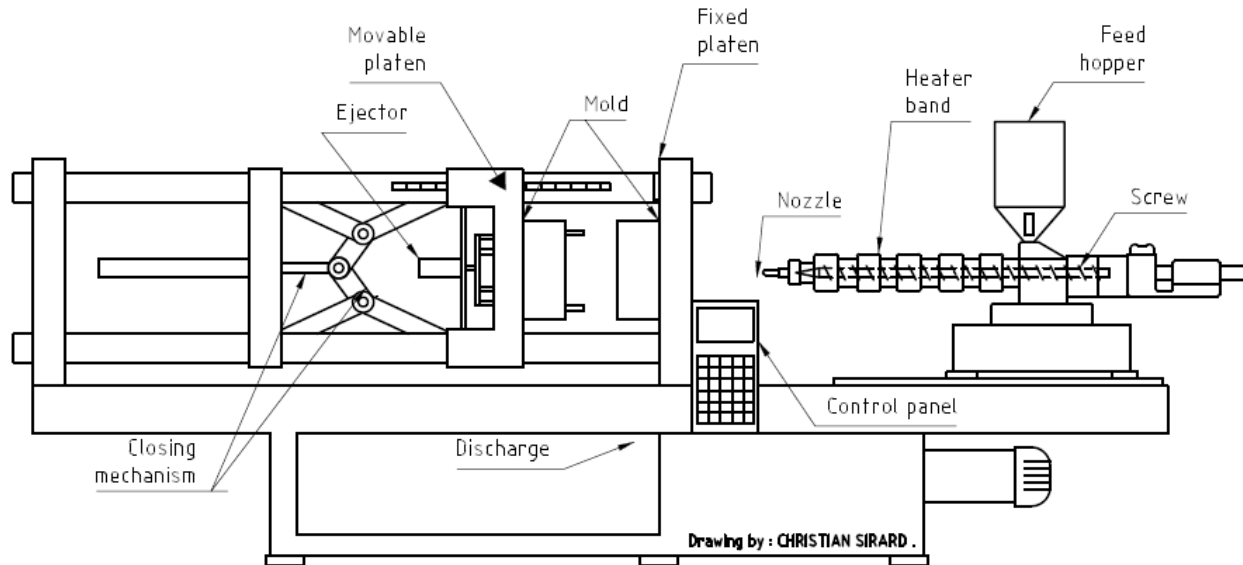


Figure 1. Location of the movable platen in relation to the other components of the molding machine [3]

After the safety function was identified, it was specified in order to establish its limits and identify its characteristics (e.g., inputs, outputs, its priority in relation to other functions).

Reading of the molding machine plans at the specification step revealed that the safety function is performed by two types of energy: electrical and hydraulic. Therefore, *ISO 13849-1* is the standard on which the *a posteriori* validation of the safety level of the safety function will be based. In this standard, the safety level is called: "Performance level (PL)." The PL is the "discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions." [2] There are 5 performance levels: a, b, c, d, e, going from the highest to the lowest PFH_d (average probability of dangerous failure per hour). Note that PL "a" corresponds to the lowest performance level.

2.1.2 Main part of the validation procedure

The next part of the procedure includes several steps aiming in the end to verify whether the PL is greater than or equal to PL_r. This is the ultimate goal of the procedure since PL_r is the PL "applied in order to achieve the required risk reduction for each safety function." [2] These are the eight steps involved:

- 1) determination of PL_r (PL_r = e for the safety function studied, according to section 5.2.1 of EN 201:2009 [4]);
- 2) determination of the designated architecture of the safety function;
- 3) estimation of MTTF_d (mean time to dangerous failure);
- 4) estimation of DC_{avg} (average diagnostic coverage);
- 5) estimation of measures against CCF (common cause failures);
- 6) verification of the requirements for the safety-related software (not applicable in our case because no software contributes to the performance of the studied safety function);
- 7) verification of measures to counter the systematic failures;

8) verification of ability to perform the safety function under foreseeable environmental conditions.

Throughout the procedure, assumptions had to be made due to insufficient information from the designer and manufacturer. In the context of the article, we will focus on the steps in which the most important assumptions influence the results: determining the designated architecture and the calculations relating to the $MTTF_d$, DC_{avg} and PL.

2.2 Determining the designated architecture

The “designated architecture” is the architecture belonging to a category of a safety function. The category is one of the criteria for judging the PL. There are 5 categories, from the weakest to the most robust: B, 1, 2, 3, 4. To satisfy $PL_r = e$, the safety function must reach a category 3 or 4, according to Figure 5 of *NF EN ISO 13849-1:2008*, a figure based on Table K.1 of the standard.

To determine the designated architecture, the material structure (here, hydraulic and electrical) performing the safety function had to be identified first, and then the components participating in this function. An analysis in the absence and then in the presence of faults (FMEA: failure modes and effects analysis) was performed. The circuit involved in the safety function was analyzed from the standpoint of several logical deductions based on the electrical and hydraulic plans of the molding machine and some information from the manufacturer. To optimize their accuracy, these deductions were carried out by different experts in safety-related control systems. First, the analysis revealed an architecture with two-channels. Using FMEA, we:

- differentiated the components contributing to the functional part of the safety function from those involved in the diagnostic part;
- verified the criteria for achieving categories 3 and 4 relating to the resistance of the safety function to faults, as well as its behavior in the presence of faults.

The FMEA mainly consisted of studying the effect of different single faults on each of the components involved in performing the safety function (Figure 2):

- switches S151A, S151B and S175 as inputs for the safety function. They are installed on the operator gate to detect its opening;
- relays K01, K02 and K03 (at the start of the FMEA, we did not know whether these relays had a functional or diagnostic role);
- controls of the hydraulic valves: Y101 and Y171 acting as outputs of the safety function.

Based on different scenarios, two types of single faults were studied: a component that remained “on” and a component that remained “off.” A component other than those mentioned above could not be studied: it was a programmable electronic card that we assumed was responsible for the diagnosis. Unfortunately, we were unable to obtain information about it, since we lacked sufficient information from the manufacturer. We therefore considered its contribution in terms of diagnosis as zero. Considering the characteristics of switches S151B and S175, as well as their installation, we felt that they benefitted from fault exclusion. In fact, information from the manufacturer indicated that these switches have direct opening action. Also, they were seen to be installed on the molding machine with positive mechanical action.

Finally, the FMEA showed that:

- the failures resulting in the single faults do not cause a loss of the safety function;
- the single faults are detected as much as reasonably achievable;
- relays K01 and K02 play a role in the functional part of the safety function, whereas relay K03 provides a diagnostic role whose diagnostic coverage (DC) was able to be quantified according to the criteria of the standard.

These conclusions of the analysis enabled us to determine the designated architecture of the safety function (Figure 2).

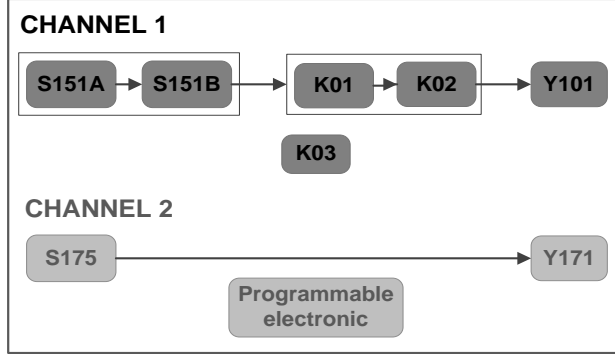


Figure 2. Architecture of the studied safety function

2.3 Calculation of the $MTTF_d$, DC_{avg} and PL

Table K.1 in the standard indicates that to obtain $PL = e$, the safety function studied must satisfy one of the two following groups of requirements:

$$\left\{ \begin{array}{l} 62 \text{ years} \leq MTTF_d \leq 100 \text{ years} \\ \text{Medium } DC_{avg}, \\ \text{therefore } 90\% \leq DC_{avg} < 99\% \\ \text{Category 3} \end{array} \right. \quad \text{OR} \quad \left\{ \begin{array}{l} 30 \text{ years} \leq MTTF_d \leq 100 \text{ years} \\ \text{High } DC_{avg} \\ \text{therefore } DC_{avg} \geq 99\% \\ \text{Category 4} \end{array} \right.$$

$MTTF_d$ (resulting $MTTF_d$) and DC_{avg} were calculated by *Excel* from formulas in the standard and applied to our case:

$$MTTF_d = \frac{2}{3} \left(MTTF_{d \text{ CHANNEL } 1} + MTTF_{d \text{ CHANNEL } 2} - \frac{1}{\frac{1}{MTTF_{d \text{ CHANNEL } 1}} + \frac{1}{MTTF_{d \text{ CHANNEL } 2}}} \right) \quad (1)$$

where:

$$MTTF_{d \text{ CHANNEL } 1} = \frac{1}{\frac{1}{MTTF_{d \text{ S151A}}} + \frac{1}{MTTF_{d \text{ K01}}} + \frac{1}{MTTF_{d \text{ K02}}} + \frac{1}{MTTF_{d \text{ Y101}}}} \quad (2)$$

$$MTTF_{d \text{ CHANNEL } 2} = \frac{1}{\frac{1}{MTTF_{d \text{ Y171}}}} \quad (3)$$

$$DC_{avg} = \frac{\frac{DC_{S151A}}{MTTF_{d \text{ S151A}}} + \frac{DC_{K01}}{MTTF_{d \text{ K01}}} + \frac{DC_{K02}}{MTTF_{d \text{ K02}}} + \frac{DC_{Y101}}{MTTF_{d \text{ Y101}}} + \frac{DC_{Y171}}{MTTF_{d \text{ Y171}}}}{\frac{1}{MTTF_{d \text{ S151A}}} + \frac{1}{MTTF_{d \text{ K01}}} + \frac{1}{MTTF_{d \text{ K02}}} + \frac{1}{MTTF_{d \text{ Y101}}} + \frac{1}{MTTF_{d \text{ Y171}}}} \quad (4)$$

The values of $MTTF_d$ and DC by component were determined from arbitrary choices related to the conditions of use of the safety function (average annual demand), information from the manufacturer, and data from *ISO 13849-1*, such as B_{10d} (the “number of cycles until 10% of the components fail dangerously”[2]). At this stage in the calculations, assumptions were also made, for example, about the fixed $MTTF_d$ of the hydraulic components. In fact, we considered that the $MTTF_d$ of the two valves to be 150 years (value from *ISO 13849-1*) since we assumed that these valves satisfied all the requirements of Annex C.3 of the standard, since information from the manufacturer was lacking.

The resulting $MTTF_d$ and the DC_{avg} were calculated for two contexts: a laboratory context (that of the IRSST laboratory with a demand rate based on its use in 2010, or 5 days/year) and an industrial context with a demand rate based on possible use in a Quebec plant, or 350 days/year. These demand rates had to be determined, in order to calculate the n_{op} (mean number of annual operations) of the safety function. Hence, the $MTTF_d$ by component

(switches and relays) that depend on the B_{10d} and the n_{op} could be calculated using the following formula from *ISO 13849-1*: $MTTF_d = B_{10d} / (0,1 \times n_{op})$.

The assumptions made throughout the procedure, but also concrete data from the manufacturer, allowed the *a posteriori* estimation of PL of the safety function for each of the two study contexts. Tables 1 and 2 present the results obtained.

Table 1. Results for the “Laboratory” context

Parameters	Value	
Category	None of the four possible categories is satisfied	} PL undetermined → PL_r not satisfied
Score to counter CCFs	65 → minimum required score satisfied	
Resulting $MTTF_d$	100 years* → High $MTTF_d$	
DC_{avg}	19,64% → DC_{avg} zero	

**Excel* calculated an $MTTF_d$ of 127 years, but the value 100 is displayed, because the standard requires limiting this parameter to 100.

Table 2. Results for the “Industrial” context

Parameters	Value	
Category	3	} PL = e = PL_r
Score to counter CCFs	65 → minimum required score satisfied	
Resulting $MTTF_d$	66,67 years → High $MTTF_d$	
DC_{avg}	98,43% → Medium DC_{avg}	

2.4 Discussion

2.4.1 Impact of the assumptions made to determine the designated architecture

The main hypothesis related to determining the designated architecture involves the role provided by certain components in performing the safety function. As mentioned in 2.2, the architecture of the circuit consists of a programmable electronic card for which we assume a diagnostic role. Due to insufficient information about this card, a zero DC had to be assumed. This assumption introduces a limitation to the *a posteriori* validation: without indications from the manufacturer or designer, it is impossible to know the functions of cards integrating programmable components. This observation suggests that circuits consisting of “elementary” electronic components can be more easily validated *a posteriori*.

Assigning a role to each component during the procedure was possible, mainly due to an exercise in reverse engineering. This exercise was not always obvious since a safety function had to be validated where the procedure and logic used during design were unknown. Therefore one has to put oneself in the place of the designer, trying to imagine what he thought. It was understood that depending on whether this procedure is accompanied or not by the designer, the available information allows us to end up with tangible facts or with deductions or assumptions that can lead to different results. If different people attempt to carry out this validation exercise alone, it will not be surprising to arrive at different interpretations at the architectural level. One way of offsetting this difficulty is to have the procedure guided by a team of experts (as was done in our study), in order to challenge different logics and to arrive at a more enlightened result. However, this practice is not always achievable in companies.

2.4.2 Impact of the assumptions made during calculation of the $MTTF_d$, DC_{avg} and PL

The main assumptions relating to the calculations of the $MTTF_d$, DC_{avg} and PL involve:

- the ability of the studied safety function to be performed under foreseeable environmental conditions;
- the lack of reliability data for certain components which were taken from the tables proposed in standard *ISO 13849-1*.

Tables 1 and 2 show that, depending on the chosen conditions of use, different results are obtained for the performance level: PL undetermined for the “Laboratory” context, PL = e for the “Industrial” context. How does one explain why in one case, the PL_r is not satisfied, in addition to the impossibility of judging the PL, while in the other case, PL_r is satisfied? This is explained by the fact that for the “Industrial” context, the assumed conditions of use

(cf. point 2.3 in this article), the calculations and analyses yielded results satisfying all the requirements for achieving the PL_r . However, for the “Laboratory” context, one of the criteria for obtaining PL_r could not be met: the category (neither 3 nor 4 was achieved) due to a zero DC_{avg} . A zero DC_{avg} was found, instead of the low or medium DC_{avg} required by category 3 and the high DC_{avg} required for category 4. Point 2.3 in this article, and particularly formula (4), make it possible to understand that with a lower mean number of annual operations, a lower DC_{avg} is obtained. Thus, the zero DC_{avg} obtained for the “Laboratory” context is explained by the mean number of annual operations of the safety function, much lower than that for the “Industrial” context. In addition to not achieving the PL_r for the “Laboratory” context, an undetermined PL is obtained. This is due to the fact that the *a posteriori* estimation procedure is based on a standard dictating a simplified method for estimating the PL:

- By considering this standard’s designated architectures, obtaining category 2 is impossible because it requires, among other things, a low DC_{avg} while the calculated one is zero; the lower categories can also not be achieved because they require a single channel, and we have two. This is why the conclusion is that the category is undetermined, which explains the undetermined PL found.
- Furthermore, one could determine the PL for the “Laboratory” context by using a calculation method other than the simplified method in the standard, which is based on “designated architectures.” Among these other calculation methods, section 4.5.1 of the standard states, for example: “Markov modeling, Generalized Stochastic Petri Nets (GSPN).” [2]

3. CONCLUSION

The imposed reverse engineering work is not easy to carry out. This *a posteriori* estimation procedure for the PL is difficult to carry out without the help of the designer. It is difficult to determine a safety level (here, the performance level) with certainty, due to the many assumptions made. In fact, in addition to the hypotheses mentioned in points 2.4.1 and 2.4.2, others had to be made in order to determine the PL. They were: 1) the conditions of use of the safety function, and 2) compliance by the designer with the requirements to control, prevent and avoid a systematic failure.

In the end, the results obtained can only be optimized by surrounding oneself with experts in safety-related control system design or by involving the designer (which is difficult to achieve). However, it seems obvious that a validation exercise of this type must be solidly documented and the assumptions clearly documented in order to know its limitations. Communication of these limitations to the users would be desirable to prevent or to better guide all modifications of a safety-related control circuit by the users.

References

1. Association Française de Normalisation, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*, Association Française de Normalisation, NF EN 62061, 2005.
2. Organisation internationale de normalisation, *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1 : Principes généraux de conception*, Comité européen de normalisation, NF EN ISO 13849-1, 2008.
3. Jocelyn S., Massé S. and Sirard C., *Presse à injection de plastique horizontale – Grilles de vérification de la sécurité*, Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST), Montréal, Québec, Canada, Guide RG-670, 2011, p. 3.
4. Association Française de Normalisation, “Machines pour les matières plastiques et le caoutchouc – Machines de moulage par injection – Prescription de sécurité,” Association Française de Normalisation, NF EN 201, 2009, p. 26.

Automatic Generation of Diverse Software Channels for Fail-safe Industrial PC

Martin Früchtl

Beckhoff Automation, Safety Products, Eiserstr. 5, D-33415 Verl, Germany
m.fruechtl@beckhoff.com

Frank Schiller

Beckhoff Automation, Scientific Safety & Security, Ostendstr. 196, D-90482 Nuremberg, Germany
f.schiller@beckhoff.com

KEY WORDS: Electronic Control Units (ECU), Coding Schemes, Error-Detecting Codes, Arithmetic Codes

ABSTRACT

In the automation industry, the importance of safety is continuously increasing. In order to fulfill functional and safety demands, normative requirements result in considerably more effort at both the hardware and the software level. Because of the hardware dependent certification process, advances of purely functional components (commercial off-the-shelf, COTS) cannot be used easily. This leads typically to a limitation of the flexibility of hardware and user application with respect to safety. Therefore, a new concept is required to master these challenges. In this paper, a new methodology that applies arithmetic codes to detect hardware errors through software measures is introduced. The achieved hardware independence prevents the limitation of the hardware design by the certification process. Furthermore, a concept is presented to provide a high-level language like C for safety user applications and to automatically incorporate the safety measures into the user application. This increases the flexibility for the application program as well.

1 INTRODUCTION

The manufacturers usually aim for certification when a safety component is developed to be used in safety loops. The certification according to common safety standards provides evidence that the component is sufficiently qualified. The standards define certain classes that have to be achieved depending on the intended application scenarios. The following specific values are determining for the eligibility of those categories: the probability of a Dangerous Failure per Hour (PFH) or the Probability of Dangerous Failure on Demand (PFD). They are based on the Residual Error Probability (REP) which is the probability that an error occurs and stays undetected. With the intention to achieve a certain REP, the component obviously needs the ability to detect errors. Measures to accomplish this are so far carried out on the hardware layer, using homogenous or heterogeneous redundancy of hardware components to recognize hardware errors at runtime (as shown in [1]) or using additional components to monitor the executing hardware (as suggested in [2]). Those hardware measures cause a hardware dependency of the certification process. Thus they prevent COTS to be used in safety loops, so that the fast development on the sector of e.g. integrated circuits cannot be exploited for safety-relevant components. Moreover, user applications for safety scenarios are typically implemented by means of fixed function blocks. The handling of huge systems on the basis of function blocks gets more time-consuming and complicated, as the complexity of modern safety applications continuously increases. For this reason, a new idea is required.

A new strategy is presented in this paper using arithmetic codes to detect hardware errors on the software layer. This constitutes a hardware independency of the certification process. Therefore, limitations in hardware design are avoided and previously purely functional components are able to serve as logic component in safety scenarios. Moreover, the possibility of using a high-level language like C to implement safety applications is established. This causes increased flexibility of the user application and allows the use of complex control structures.

In [3], an approach has been published that uses arithmetic codes to detect hardware errors on the software layer. The fundamental scheme supports the coding of data and the coding of arithmetic operations. There it is necessary to take ancillary hardware measures. The paper [4] analyses some variants of the coding scheme of [3].

Our paper is structured as follows: the limitations for hardware design and user applications when developing a component for safety-relevant scenarios according to normative requirements are described in Section 2. Furthermore, an overview of the relevant hardware errors is given. In Section 3, basic strategies were analyzed to achieve given safety goals. The final part of the section shows an idea known from coding theory that allows the detection of hardware errors through mathematical techniques. A corresponding coding scheme is deduced in Section 4, providing the capability to detect the error types of Section 2. In Section 5, the process of automatically generating diverse software channels is sketched. Section 6 shows a concrete implementation of the method. In Section 7, a conclusion and an outlook is finally given.

2 PROBLEM DEFINITION

The most important point of the paper is the logic component of a safety loop, the so-called Intelligent Safety Component (ISC). It is defined in the following way:

Definition 1. (Intelligent Safety Component). An Intelligent Safety Component is a component of a safety loop, whose task is receiving input signals from the I/O components, processing the data, and sending corresponding output signals to the I/O-components. Thereby, the processing logic is determined by the user.

As brought up in Section 1, the certification of the component for a certain safety category is typically aimed by the manufacturers of ISC. Those classes are defined in common safety standards (e.g. [5] or [6]), and the classification depends on the capability to detect errors of the hardware.

A distinction into two main categories is made in order to give a good overview of possible errors within the ISC. It is based on the implication of an error. The first type occurs if an error leads to the complete failure of the ISC. Then no measures can be taken locally to detect this error and trigger a corresponding action. This error type can only be detected at components safely connected to the ISC, e.g. at components of the safe communication that detect erroneous or missing telegrams of the failed component. The other type of error on this level leads to an erroneous processing of data and therefore to falsified output signals sent to the I/O-components. This type of error is subject of the discussion here.

The following paragraphs describe classes which differentiate errors in data processing.

Operand Error. An operand error occurs, when an operation is correctly executed with the correct operator, but at least one operand is erroneous. If, for example, the operation shown in Equation (1) is supposed to be calculated,

$$x + y = z \quad (1)$$

the operand error causes the original value x to be falsified by an error term $\Delta\epsilon$ (cf. Equation (2)). In reality, the operation in Equation (2) is calculated, causing an erroneous output value z .

$$(x + \Delta\epsilon) + y = \underbrace{(x + y)}_z + \Delta\epsilon = z + \Delta\epsilon \quad (2)$$

Operand errors are often caused by errors associated with memory operations. If a memory section is erroneous, an erroneous value is possibly read and used within a successive operation.

Operator Error. If an operation is correctly executed with the correct operands, but with a wrong operator, an operator error occurred. Similar to Equation (1), an operator error causes a falsification $\Delta\epsilon$ of the result z . In the example, instead of the required addition $x + y$, the operator error leads to the calculation of the multiplication $x \cdot y$ (shown in Equation (3)).

$$x \cdot y = z + \Delta\epsilon \quad (3)$$

An operator error can be caused by a sporadic error in the addressing or an erroneous Arithmetic Logic Unit (ALU), the main part of a processor that executes all arithmetic operations.

Operation Error. Besides the operand error and operator error, there is the possibility that an operation error occurs. An operation error is the erroneous execution of an operation with the correct operands and the correct operator. Again, these errors are usually caused by an erroneous ALU and lead again to a direct falsification of the result value z (shown in Equation (4)) for a desired addition $(x + y)$.

$$x + y = z + \Delta\epsilon \quad (4)$$

To avoid the dependence of safety proofs on the hardware of ISC is the major purpose of this paper. Thusly, the use of high-performance COTS as the logic part of a safety loop should be admitted. Hence, it is necessary to transfer the measures to detect hardware errors to the software layer.

Additionally, the flexibility of user applications has to be increased by use of a flexible high-level language like C.

3 FUNDAMENTAL STRATEGIES TO DETECT ERRORS

The ISC requires the provable capability to detect internal hardware errors in order to qualify it for a certain safety category. There exist diverse methods to reach this aim. They are described in the following.

3.1 Basics

The verification of the result is the essential idea behind the detection of hardware errors in ISC. This is usually done by a specific technique. It is called redundancy and defined in the following way.

Definition 2. (Redundancy IEC 61508). Redundancy is the existence of more operational resources in a component than actually needed to fulfill the required function.

Redundancy can be furthermore distinguished between homogeneous and heterogeneous redundancy. In homogeneous redundancy architectures, the redundant channel is comprised of exactly the same components like the original one. But there is a disadvantage related to the sensitivity of the channels to a Common Cause Failure (CCF) since they have the same specification and therefore the same vulnerabilities. Heterogeneous redundancy follows another approach. It is implemented by components realizing the same functionality as the original channel by various methods. So, a CCF is less probable in such architectures.

The safety measures were usually realized in the hardware layer. The development of safety solutions in control technology, however, shows a tendency away from hardware solutions up to software solutions. The complete change to hardware independent solutions has not happened yet, though more and more functionality is moved to the software layer. The following section introduces arithmetic codes that constitute a solution to create diversity in software.

3.2 Arithmetic Codes to Create Data Diversity

A widely spread method to achieve heterogeneous redundancy on data level are codes. There, the transformation of the used data into diverse, coded data is fundamental. With the help of these data, the verification of the results of the original channel has been enabled. Consequently, hardware errors affecting the operation results can be detected.

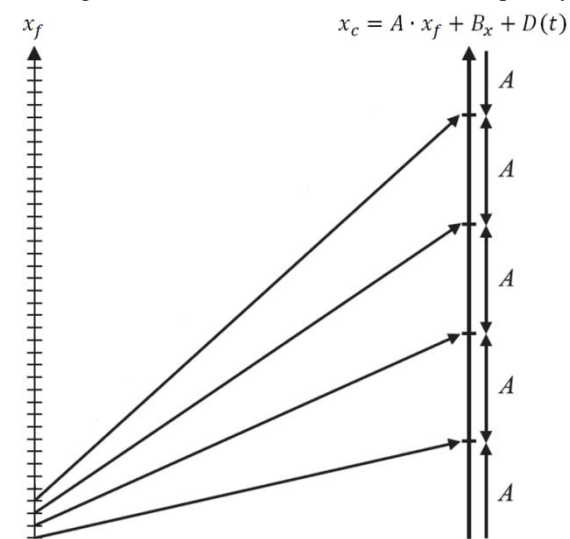


Figure 1. Effect of coding on data areas

In order to display the functionality and reasoning in the context of using coding theory for safety applications, a coding scheme is introduced in [3].

The basic coding consists of multiplying original variables x_f with a prime number A in order to construct a greater codomain and therefore creating a gap between valid coded values x_c . By means of the difference between valid values, the validity of operation results can be verified by the check, if the values are multiples of the prime number A ($x_c \text{ mod } A == 0$) as only such multiples are part of the code and are therefore valid. Based on this coding, the falsification of values can be recognized as long as the error term $\Delta\epsilon$ is not a multiple of A . In [3], a so-called static signature B_x for each used variable is additionally introduced in order to identify each value and creating the ability to recognize mix-ups of variables. Furthermore, [3] suggests a dynamic signature $D(t)$ to identify the cycle and assuring the values are used within the correct cycle. The complete coding of data is carried out according to Equation (5).

$$x_c = A \cdot x_f + B_x + D(t) \quad (5)$$

The effect of the coding mechanism on the data areas of uncoded and coded values (x_f and x_c) is illustrated in Figure 1.

The uncoded values x_f (on the left-hand side) are coded, resulting in a set of values where the difference between two adjacent values is equal to the value of A . The resulting coded values are shown on the right-hand side.

The advantage of arithmetic codes is the fact, that specific coded operations can be constructed such that the correct result is part of the code and the validity can be checked by $((x_c - Bx - D(t)) \bmod A == 0?)$. In Equation 6, the coded addition of two values x_c and y_c is developed analogously to [3].

$$\begin{aligned}
 z_f &= x_f + y_f \\
 z_c - B_z - D(t) &= x_c - B_x - D(t) + y_c - B_y - D(t) \\
 z_c &= x_c + y_c - B_x - B_y - D(t) + B_z \\
 z_c &= x_c + y_c + \underbrace{(B_z - B_x - B_y)}_{\text{constant}} - D(t)
 \end{aligned} \tag{6}$$

The pre-calculated constant summand $(B_z - B_x - B_y)$ emphasizes the advantage of the kind of coding. The constant contains information about the operators and the kind of operation to be used. So operand errors, operator errors, and operation errors can be detected with high probability.

Coded versions of the addition and multiplication of two values x_c and y_c are given in [3] and solutions for the remaining operations are brought up but are not elaborated there.

With this encoding scheme, a residual error probability of $1/A$ can be obtained (see [7]). Therefore, in order to achieve a sufficiently low REP, the value A has to be chosen as large as possible. Note, only if a uniform distribution holds, $1/A$ represents the correct REP. Uniform distribution in case of an error means, that each value is equally probable, if an error occurs. But in this context, this assumption does not completely hold. Thus, in order to select a good value A , additional deterministic criteria are to be applied. There are two main characteristic values: Hamming Distance (HD) and Arithmetic Distance (AD).

- The HD - or the minimum HD - of a code is the minimum number of bits that have to be changed in order to map one code word to another code word.
- The AD of two values x and y is the minimum number of bits at value one of the two possible arithmetic differences $(x - y)$ and $(y - x)$. The minimum AD of a code is the minimum AD of all values x and y , $x \neq y$.

When selecting the proper parameters like A of the code, both the HD and AD have to be taken into account. The value A should be as large as possible, but at the same time providing an adequate HD and AD. Apart from this fact, a third criterion already brought up in [2] should be considered, the selection of A as a prime number (as suggested in [3]). The reason for that is as follows: A series of n arithmetic additions is executed. Each addition adds a constant error term $\Delta\epsilon$. Therefore, at the end of the n operations, the overall error term is $n \cdot \Delta\epsilon$. If the result is still a multiple of A , this error cannot be detected. If A is prime, this can only be true, if either n or $\Delta\epsilon$ is divisible by A .

The coding mechanism in [3] is a complete single-channel approach (single-channel software on single channel hardware) applied in the Metro in Paris for driverless trains. Since a particular hardware has been taken to encode the data for the operations there, restrictions to the hardware architecture are imposed. Additionally, the user implemented the coded version of the software manually since the need for totally flexible programming like in automation has not been considered to be essential there. Still, the approach [3] illustrates a good foundation for the solution discussed here.

In the next sections, an advanced coding scheme is deduced in order to meet the challenges.

4 DEDUCTION OF THE CODING SCHEME

The use of several software channels significantly increases the error detection rate or decreases the residual error probability REP, respectively. Consequently, not only one, but n additional diverse software channels are applied besides the original uncoded channel. An error can only stay undetected, if a combination of $(n + 1)$ errors occur (n coded channels and the original channel), so that each error term $\Delta\epsilon_i$ (with i as the identification of a channel) results in a valid code word. Additionally, the error terms have to emerge in a certain characteristic, as the results of all channels have to form a valid combination of uncoded and coded values. A mutual test between all n channels is performed to detect errors and to initiate a safe reaction.

In order to avoid special hardware to encode input and decode output data, the coding scheme is directly connected to a safe communication protocol. Though, the error detection mechanism of the safe communication is used as a redundant check to the internal ones. In Figure 2, the whole architecture is shown.

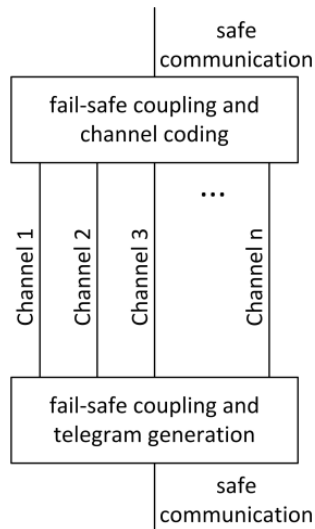


Figure 2. Overall on-line architecture

Following the process exemplarily explained in Equation (6), coded versions of operations such as addition, subtraction, multiplication, division, conjunction, disjunction, exclusive disjunction, negation, and relational operators have been derived. These operations can be used to realize a large choice of safety-relevant applications. The possible error types in Section 2 have to be considered in the deduction process of the operations, such that falsifications of operands, operators, or erroneous performance of particular operations can be detected.

The mutual consistency check between 2 coded channels can be executed by Equation (7).

$$A_2 \cdot (z_{c1} - B_{z1} - D(t)) == A_1 \cdot (z_{c2} - B_{z2} - D(t))? \quad (7)$$

Because of the possibility that the skipping of individuals code lines or even whole code blocks can still make for valid (but erroneous) results, the coding has to be further enhanced in order to ascertain the correct performance of the source code at runtime.

One of the objectives set in Section 2 was to raise flexibility for user applications by the use of high-level languages. The utilization of the established coding mechanism demands several variants of the user code, but manually embedding of those variants would considerably decrease the usability and applicability. Therefore, the necessary diverse software channels have to be generated automatically. This will be discussed in the next section.

5 AUTOMATIC GENERATION OF DIVERSE SOFTWARE

One target of automatic embedding of safety measures is to leave the user code (the uncoded channel) unchanged for e.g. documentation. Therefore, it could be executed in parallel to the coded versions.

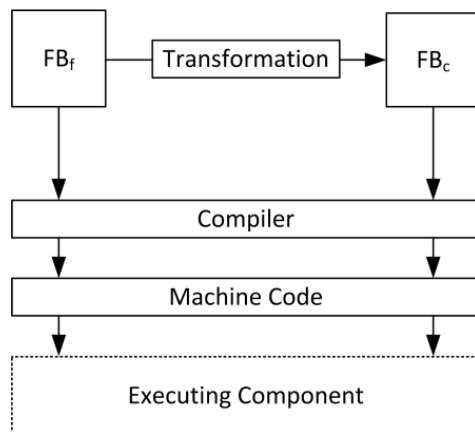


Figure 3. Overall off-line architecture

Hence, a source code block programmed by the user (named FB_f in Figure 3) is taken as input in an off-line procedure. The so called Transformation creates the diverse software channels, i.e. the coded versions of the source code. It is named FB_c in Figure 3. Both uncoded and coded versions are then compiled by the same regular compiler (without special qualification). It results in the machine code which lastly is executed within the ISC's runtime. In Figure 3, the complete procedure is exemplified.

After a successful transformation, the source code (FB_f and FB_c) is ready for compiling and for the following download to the runtime environment. Related to safety applications, the input and output values of the logic have to be moved safely to the periphery. Therefore, a particular safety runtime environment is required to treat this objective.

The cyclic safety data flow of the ISC is controlled by the runtime. In each cycle, the next steps are executed:

1. **Input:** The telegram is received from the safe communication protocol. After treatment of protocol specific activities (like controlling the Frame Check Sequence (FCS) of the package), the raw data values are coded and passed to the n coded channels (fail-safe coupling and channel coding in Figure 2).
2. **Main Logic:** In the main logic part, the uncoded channel and the n coded channels are performed, and the appropriate results are computed.
3. **Output:** Result values of the main logic are decoded and the output telegram is built. This means that both the output data and the computed FCS are passed onto the safe communication (fail-safe coupling and telegram generation in Figure 2). The determination of the FCS is based on the coded results.

The safety runtime has to ensure the execution of all source code parts, so that the skipping of single lines or even source code blocks can be detected. Additional measures apply. It is important, that the partial execution of the program (with skipped sections occurring) cannot lead to a valid output telegram and therefore to a potentially hazard as the result of an erroneous reaction of the system.

6 IMPLEMENTATION

The introduced approach has been implemented in the context of the TwinCAT Safety PLC by Beckhoff Automation. The Safety PLC enables the previously purely functional Beckhoff Industrial PC (IPC) to be used as logic component (Intelligent Safety Component, ISC) within a safety loop up to Safety Integrity Level 3 (SIL 3) according to IEC 61508 [5]. Current Microsoft Windows Embedded versions are usually used as operating system by the Beckhoff IPC product family. The additional calculation effort does not cause a measurable time delay for typical safety applications because of the high degree of efficiency of the used IPC.

Safety applications for the Safety PLC can be implemented in a high-level language called Safety C. This is a nearly unlimited derivative of Standard C. It allows the use of control structures like IF-THEN, SWITCH-CASE and data types known in Standard C for the application logic. The approach enables a previously unknown flexibility of safety user applications.

The intricacy of safety applications concerning functionality and dimension continuously increases. In consideration of this fact, the introduction of the Beckhoff IPC as flexible logic component of safety applications is an important step towards future challenges in safety technology. TÜV SÜD, an internationally operating independent authority, has already confirmed the certifiability of the approach according to [5] in a proof-of-concept document.

7 CONCLUSION AND OUTLOOK

In this paper, a new approach for the use of arithmetic codes for Intelligent Safety Components has been presented. The method enables a previously purely functional component to serve as logic device in safety scenarios. The certification process no longer depends on the hardware due to the exact mathematical base. Therefore, the approach can be applied to any hardware architecture. A modern purely functional component like the IPC can be used as safety controller in that way.

The realization for the Beckhoff IPC has demonstrated the practicability of this work. The development of this technology is further pursued to continuously extend its flexibility and functionality.

REFERENCES

1. Krebs H., Mitra S., *Hardware redundant vital computers – demonstration of safety on the basis of current standard*, Proc. of the 18th International Conference on Computer Safety, Reliability and Security, London, 1999, pp. 153-162
2. Rajabzadeh, A., Miremadi S., *A hardware approach to concurrent error detection capability enhancement in cots processors*, Proc. of the 11th Pacific Rim International Symposium on Dependable Computing, Washington, DC, 2005, pp. 83-90
3. Forin P., *Vital coded microprocessor principles and application for various transit systems*, IFAC Control, Computers, Communications, Paris, 1989, pp. 79-84
4. Schiffel U., *Hardware Error Detection using An-codes*, 2011
5. IEC 61508, *IEC 6150: Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems*, 2002
6. ISO 13849, *ISO 13849: Safety of Machinery - Safety-related Parts of Control Systems*, 2006
7. Ozello P., *The coded microprocessor certification*, International Conference on Computer Safety, Reliability and Security, 1992, pp. 185-190
8. Oh S., Mitra S., McCluskey E.J., *Ed4i: Error detection by diverse data and duplicated instructions*, IEEE Transaction on Computers, 2002, pp. 180-199

Reliability Databases used by the ISO 13849 tool SISTEMA

Michael Huelke, michael.huelke@dguv.de; Andy Lungfiel, andy.lungfiel@dguv.de;
Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA),
Alte Heerstrasse 111, 53757 Sankt Augustin, Germany

KEY WORDS: safety, machinery, ISO 13849, reliability database, SISTEMA

ABSTRACT

The ISO 13849-1 gives guidelines to develop, validate and certify in a simple way safety-related control systems in the field of machinery. The IFA supports the application of the new probabilistic methodologies by having launched the software SISTEMA in 2008. SISTEMA has become a global de facto standard tool. This is also due to the IFA approach to provide a database definition which is widely used to exchange reliability data for control devices and components – from device vendor to SISTEMA user or within a company from users to users. Most global players in safety automation provide SISTEMA libraries. For the last two years, a working group of the VDMA (German Engineering Federation) with participation of IFA has developed the VDMA standard sheet 66413 which describes a reliability database definition. This definition is the so called “universal database”, which could also be useful on an international level. The universal database serves as a common platform for information exchange of safety-relevant characteristics between equipment manufacturers, device manufacturers, notified bodies (as the IFA) and providers of computational tools (as SISTEMA) in the field of functional safety.

1 INTRODUCTION

The ISO 13849-1 “Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design” [1] gives guidelines to develop, validate and certify in a simple way safety-related control systems in the field of machinery. Deterministic and probabilistic requirements are combined in a practicable manner: The category of the control system (e.g. redundancy and testing) and its probabilistic properties (failure rates of components called MTTFd, diagnostic coverage of tests called DC, common cause failure rates) underlie the determination of the “Performance Level” (PL). The IFA supports the application of the new simple methodologies by having launched the software SISTEMA in 2008 [2], [3].

SISTEMA has become a global de facto standard tool. This is also due to the IFA approach to provide a database definition which is widely used to exchange reliability data for control devices and components – from device vendor to SISTEMA user or within a company from users to users. In the beginning of 2012 there are already over 40 companies linked to the IFA information page on available libraries. About 20 to 30 more companies have already announced to prepare libraries for their products. Most global players in safety automation provide SISTEMA libraries. The SISTEMA database definition is developed and updated by the IFA staff and is hence no open source. But it is proven effective and continuously updated. Moreover, the IFA database documentation is available on request without charges [4]. It could be used by the vendors to develop a database export into the SISTEMA library definition. But most companies use the SISTEMA editor itself in order to build relatively small libraries.

For the last two years, a working group of the VDMA (German Engineering Federation) Division Electric Automation with participation of IFA has developed the VDMA standard sheet 66413 [6] which describes a reliability database definition. This definition could also be useful on an international level. A first draft has been published in the beginning of 2012. The VDMA standard sheet 66413 gives an agreement on definitions of the electronic representation for components or parts of control systems in the field of functional safety. This definition is the so called “universal database” (see Chapter 3). The universal database serves as a common platform for information exchange of safety-relevant characteristics between equipment manufacturers, device manufacturers, notified bodies (as the IFA) and providers of computational tools (as SISTEMA) in the field of functional safety. The standardized electronic exchange format is supposed to simplify the workflow to calculate the probability of failure of safety functions in accordance with ISO 13849 and IEC 62061. In drafting the standard sheet, important requirements have been considered by the parties involved in data exchange, such as: The device characteristics will be available as a standardized, human-readable XML library; Such databases could be used in any calculation tools; Transparency of the reliability values; Minimization of the costs of providing such databases.

2 SISTEMA DATABASE

Upon request to IFA, a documentation of the SISTEMA database [4] is made available. This documentation is primarily directed at manufacturers who wish to make a parts library accessible via SISTEMA. For the understanding of this document, previous knowledge of SQL, XML, Schema and the use of SISTEMA itself are assumed. The Help file of the software (contained in Setup) - in particular the chapter on the basic elements - provides a comprehensive description of the elementary business-data objects, the so-called basic elements, which to a certain extent serve the user as building-blocks for his project.

IFA offers manufacturers of parts and components in the safety technology sector the opportunity to provide users of SISTEMA with a database of parts in the form of a SISTEMA library. The graphic user interface (GUI) of the application permits the user, in a convenient manner, to incorporate new libraries from the local file system or from a remote server, or to toggle between libraries already registered. Own libraries can also be created and administered with the aid of the GUI (see 2.3). There is also the option of protecting a library from write-access by users.

However, the limits of the integrated editor are quickly reached, when it comes to the automated generation of a library, as would be required for very large part databases. By offering access to further interfaces, we are able to overcome this limitation of the editor, and thus meet the requirements of parts manufacturers.

2.1 CONTENTS OF THE SISTEMA LIBRARY

For publication via a library three of the seven basic element types which can be administered by SISTEMA come under consideration. A detailed description of these types can be found in the SISTEMA Help file:

- The Subsystem (**SE**; rank 3 in the elements hierarchy) normally implements a so-called Designated Architecture of the standard. The EN ISO 13849 recommends for each category an architecture which stipulates the parameters for the basic structure, the number of channels and the test equipment. SISTEMA permits the user to connect several subsystems within the context of a security function in sequence.
- The Block (**BL**; rank 5) represents a function block within the framework of a logical block diagram. It divides a channel into logical function units (e.g. sensor, logic and main contactor).
- The Element (**EL**; lowest rank 6) represents the lowest hierarchy stage of the basic elements. Elements are electronic, electro-mechanical, hydraulic, mechanical or pneumatic parts of which a function block is composed.

The basic element channel (**CH**; rank 4) or test channel (**TE**; also rank 4) is simply used as a structuring component. Channels and test channels can therefore only be administered as sub-groups of a subsystem in the library; they cannot be saved or loaded individually. The following element types, in addition to channel and test channel, are also not supported by the library:

- The project (**PR**; highest rank 1) represents the project file (*.ssm) itself and normally refers to a machine or hazard point which is under observation.
- The safety function (**SF**; rank 2) is defined as a function of the observed machine, the failure of which can lead to a direct increase of the risk. It is implemented by one or more subsystems, but however does not represent any component, but rather a functionality, and therefore also cannot be administered within the library.

2.2 INTERFACES OF THE SISTEMA LIBRARY

SISTEMA offers a simple editor for the library as standard, within the context of the graphic user interface. This convenient interface is described in Chapter 2.3. This editor is the tool of choice for libraries of limited scope. However, the automatic production of contents on the basis of an existing database is not possible via this interface.

In this situation therefore, the SQL interface of the database comes under consideration. Since the complex connections between the data objects cannot all be recorded due to SQL constraints, the onus here is to some extent on the interface user, to produce valid data which can be correctly processed by SISTEMA. In the SISTEMA documentation [4], we describe the structure of the Firebird database which forms the basis for the library, and define the for-

mat for valid contents. Alternatively, it is possible (but not really recommended) to import data using the XML format. A concealed import function of the library editor makes it possible to read-in library contents via an XML file. Here too, major format faults are indeed caught by a validating formula (XML Schema Definition), but it is also very easy to create formats to which SISTEMA reacts with unexpected behaviour or a fault response. It is therefore advisable to keep to the conventions described in the documentation. We recommend the SQL interface in preference to the XML interface since, due to stronger constraints, it is less prone to fault and simplifies debugging.

SISTEMA stores libraries as files with the suffix .slb in the file system. Behind such a file is hidden a Firebird® database. This can be accessed and processed with the aid of corresponding tools via the SQL Standard (acc. to ANSI SQL-99). SQL scripts permit, via INSERT, UPDATE AND DELETE statements, the creation and modification of generic library contents. In the documentation, we will further explain the SQL interface of the database, so that you are in a position to fill a database input via SISTEMA using SQL commands.

For the sake of completeness, the scripts employed in SISTEMA for creation of a new library are included with this document. In addition, you will find an example script which illustrates the data creation via this interface. Some SQL scripting tools permit the generation of SQL command sequences from existing databank contents. Should you be uncertain how to proceed, we recommend that you first compile the desired library contents using the integrated editor (see 2.3) and then export the data to an SQL script, using such a tool.

2.3 GRAPHIC USER INTERFACE

Obviously the simplest option for the input and manipulation of libraries is offered by the integrated library editor of the graphic user interface. The limitations of this editor have already been indicated, where it is required to produce contents of larger extent. The appearance of the editor (Figure 1) is very similar to the main display of SISTEMA in its structure: There is a working area in the centre of the window, a navigation window with a directory tree view (left) an information window (bottom) a context window (bottom left) and a Help window for direct help (right). Additional control elements at the upper border of the window permit the control and configuration of the libraries themselves:

- List of libraries (left side): Contains all integrated libraries. By selecting a list entry, the corresponding library is loaded, thus making its basic elements accessible.
- List of properties of the library (right side): Permits the viewing and the configuration of the meta-information of a loaded library, as name, location, author, last alteration, SISTEMA versions and a text information.



Figure 1. Control area of the integral library editor of the user interface

It is a standard action to incorporate an existing library from the local PC file system into the list. An additional dialog enables libraries to be imported from one or more central database server. SISTEMA thus supports efficient collaboration between multiple SISTEMA users within an enterprise. Installation and use is described in [5].

2.4 STRUCTURE AND CONTENT

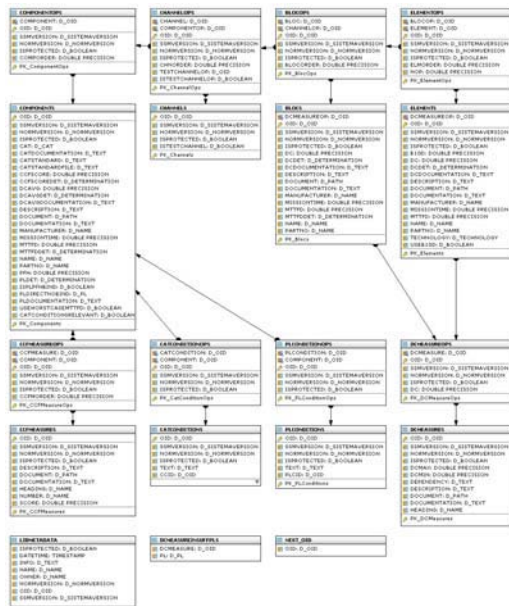


Figure 2 just serves as an illustration of the comprehensive static structure of the database tables in the form of an UML Class Diagram. The SISTEMA documentation contains detailed documentation of the table fields, data types and constraints (foreign keys and checks). Please note, however, that not all dependencies and conditions can be checked by the database.

Figure 2. Class diagram of the SISTEMA database

2.4 THE SISTEMA XML INTERFACE

The SISTEMA library editor includes a hidden interface for the import and export of files in XML format. It must however first be enabled by the setting of a registry value. This effects the activation of two additional commands in the "Edit" menu of the library. The "Import..." switch causes all contents from the XML file of the currently-loaded library to be added. Existing entries are still retained. The "Export..." switch saves the entire library to an XML file. Naturally, the contents of such an XML file can also be manually edited or created. In this context it should be ensured that the relational table structures of the SQL databank are represented via the XML structure. SISTEMA checks the validity of the XML files (.ssm projects and XML imports) on the basis of a rudimentary XML model under the filename ssm.xsd. If an error is already found at the stage of parsing the file on the basis of the model, the line and reason for the error are displayed to the user. In this case, the file will not even be loaded. However, the model only recognises gross faults in the structure of the data. For example, the exceeding of ranges of individual fields is not recognised. Such faults, which are not registered during the parsing process, are usually recognised by the programme logic during reading-in of the data.

3 UNIVERSAL DATABASE VDMA 66413

The VDMA standard sheet 66413 [6] gives an agreement on definitions of the electronic representation for components or parts of control systems in the field of functional safety. It determines terms and definitions, definitions of characteristic values and the standardised electronic format (data format).

Control devices vary in terms of technology, application, availability and use of diagnostic mechanisms and diagnostic information. As a result, different device types have been defined. Devices can generally be distinguished by the following features:

- Device that can be used directly as a SRP/CS or subsystem (subelement) in a safety function because the manufacturer has already developed the device for this specific application (*DeviceType1* and *DeviceType4*). These correspond to the SISTEMA Subsystem **SB**.
- Device that is only defined and assessed as a SRP/CS or subsystem (subelement) through the user's design process (*DeviceType2* and *DeviceType3*). Type 2 correspond to SISTEMA Block **BL**, Type 3 correspond to SISTEMA Element **EL**.

The data structure of the VDMA 66413 library (Figure 3) consists of following entities:

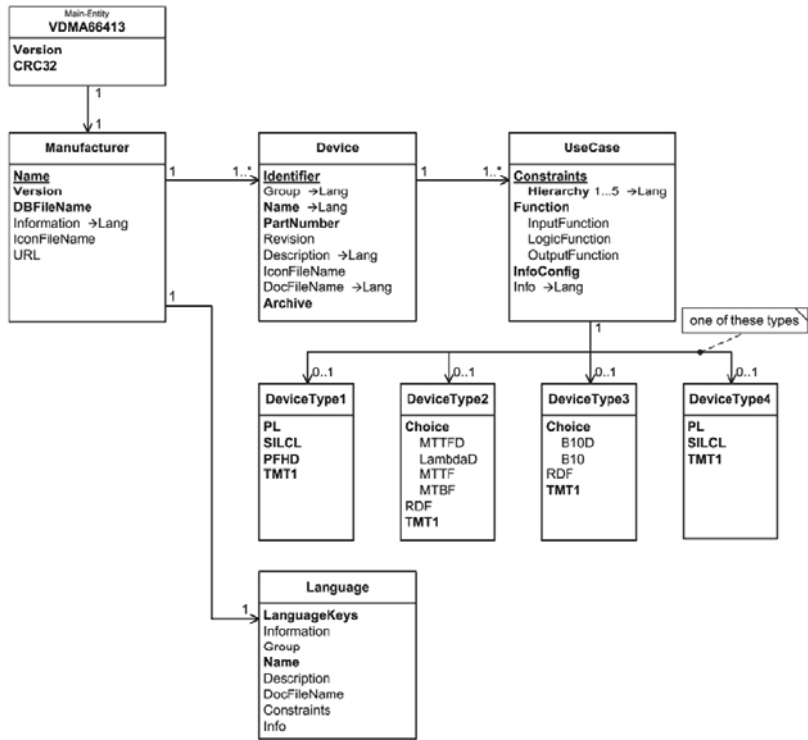


Figure 3. Data structure of the characteristic value library (from VDMA66413, Beuth Verlag Berlin)

VDMA66413: Version number of the database definition and check sum covering the whole library

Manufacturer: The device manufacturer is the person who manufactures devices and/or components and makes them available to the machine manufacturer or user. As a result, the creator of a characteristic value library can and indeed may only be the device manufacturer. This entity gives details of the device manufacturer: unique global name, Version of the library, file name of the characteristic value library...

Device: This information is used to describe a device (from the perspective of the device manufacturer) and to provide the user with further details about the device: Name, part number, revision, description ...

UseCase: Describes the use case(s) of a device, with there own characteristic value set(s). If there are several use cases of a device and different safety-related characteristic values apply for each use case, then *UseCase* is used to distinguish between these characteristic value sets.

DeviceType1..4: The value sets depend on the type of device and are at last used by the tools to determine the probability of failure of a safety function according to ISO 13849-1 or IEC 62061.

Language: The language texts are available in at least one language in the characteristic value library. Other languages may be provided in one or more separate language libraries. Each language library belongs to exactly one characteristic value library.

The data format of a VDMA 66413 library is XML (Extensible Markup Language). XML defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is defined in free open specifications. All necessary data types are provided and described in the VDMA standard sheet. The XML schema which is provided by the VDMA standard sheet, defines the formally correct structure and syntax of the characteristic value library. The schema contains some additional, necessary structural constructs which are not addressed in the VDMA standard sheet. The schema is used to check the characteristic value library for formal correctness. If a calculation tool detects any inconsistencies in the characteristic value library, the whole characteristic value library should be rejected.

4 CONCLUSION

In the context of functional safety of machinery, SISTEMA has introduced in 2008 a vendor independent library concept for exchange of reliability values of safety-relevant devices. It is free and easy to use, because SISTEMA comes with a simple library editor. Thus it became a success story with today about 50 vendors who provide SISTEMA libraries - and the number is still growing. The success factor is that the IFA as an accepted and independent organisation has been able to launch and further develop very quickly a technical platform that meets most requirements of manufacturers of control devices or machinery and companies for testing and consultancy. In the perspective of some companies, this is a drawback: SISTEMA and its database and the libraries are not open source. But the library documentation has been disclosed, it is free and available on request from the beginning in 2008.

The VDMA 66413 database, starting in 2012, promises to be the open and universal platform for all device manufacturers that in turn can be used by all calculation tools. This is a desirable goal. One difference from SISTEMA is that this database definition must be developed by many participants in the consensus. A SISTEMA library is usually created only by SISTEMA itself and is read again from the same tool. On the other hand, a VDMA 66413 library must be able to be created by several tools and be processed by many other tools. The demands on the precision of the database definition and the mutual compatibility of the tools are correspondingly high.

What are the technical differences? In a VDMA 66413 library, only equipment from one manufacturer can be saved. It is indeed a database, a kind of catalogue, for single products by this one manufacturer. But in practice there are also complete applications, that are combinations of several safety-related standard devices (including multi-vendor), which are often used in safety controls. SISTEMA is able to one-click-store and -load these applications in its data base, in addition to single devices. Therefore, the SISTEMA libraries will continue to remain useful for users (machine manufacturer) of devices and applications, who not want to miss the opportunity to create their own project-specific libraries.

One advantage of the VDMA 66413 is the concept of multilingual libraries. In SISTEMA applies: Each language has its own library file. In 66413, each device may have different use cases, each use case with its own characteristic set of values. In SISTEMA, each use case is mapped by a single basic element type (Subsystem, Block or Element). To sum it up: There are structural differences and some new data fields at the VDMA database.

How will it go with SISTEMA? For 2013 it is planned to implement an interface for importing the devices from the VDMA database. At the same time, some of these new data fields are added to the SISTEMA database. Both databases thus approach the content, even if they remain structured differently. IFA will continue to support and improve the SISTEMA libraries. The SISTEMA library manager will also be significantly optimized and new features added.

5 REFERENCES

1. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006)
2. Hauke M. et.al., *BGIA Report 2/2008e - Functional safety of machine controls - Application of EN ISO 13849*, German Social Accident Insurance, Sankt Augustin, 2009, <http://www.dguv.de/ifa/en/pub/rep/rep07/bgia0208/index.jsp>
3. Apfeld R. et.al., *SISTEMA Cookbook 1- From the schematic circuit diagram to the Performance Level – quantification of safety functions with SISTEMA*, Institute for Occupational Safety and Health of DGUV (IFA), Sankt Augustin, 2010, <http://www.dguv.de/ifa/en/pr/softwa/sistema/kochbuch/index.jsp>,
4. Pilger J., Lungfiel A., *SISTEMA Documentation Library Interfaces VI.1.2*, Institute for Occupational Safety and Health of DGUV (IFA), Sankt Augustin, 2010. Internal paper, available on request.
5. Lungfiel A., Huelke M., *SISTEMA Cookbooks 2 and 3*, Institute for Occupational Safety and Health of DGUV (IFA), Sankt Augustin, 2010, <http://www.dguv.de/ifa/en/pr/softwa/sistema/kochbuch/index.jsp>
6. VDMA 66413:2012-07, *Functional Safety - Universal Database for safety-related values of components or parts of control system* (in German), Beuth, Berlin, 2012

An Improvement in Applying Safety Standard “ISO 13849” using Fuzzy Logic

Mohammad Sohani, Yuvin Chinniah, Mohamed-Salah Ouali

KEYWORDS:

ABSTRACT

Accurate risk allocation and validation steps are essential to apply ISO 13849 standard on safety related control systems. However, failure rate data is rarely available to designers and usually not provided with components used in safety systems. Recently, manufacturers have started to perform measurements for failure rates in order to include them into their data sheets. Meanwhile, other data sources may be used which encompass uncertainty and error due to dissimilar specifications between test and implementation environment. Conventional methods used in standards based on crisp levels are not appropriate in this respect. Additionally, risk assessment method employed to define required performance level (PL_r) for the safety control system uses expert's opinion to define risk component levels. Using expert's opinion entails subjectivity problem and crisp values are not appropriate to express judgmental risk assessment. Applying fuzzy logic in the standard can solve both these problems. Fuzzy logic has been proven to deal effectively with uncertainty and subjectivity. It can improve the methodology and reduce under or overdesign possibility.

1 INTRODUCTION

The aim of performing risk reduction on an industrial machine is to satisfy requirements of safety regulations and standards and also to ensure sufficient safety. Acceptable risk for a machine is achieved by using a combination of methods including intrinsic safe design, safeguarding and training. Accordingly, functional safety can be used as an effective and useful approach in reducing associated risks linked to machine. Functional safety is “part of the safety of the machine and the machine control system which depends on the correct functioning of the SRECS, other technology safety-related systems and external risk reduction facilities” [1]. When used for industrial machine, it is realized by deploying safety related control (SRC). To design SRC, standard ISO 13849 [2] is required to guarantee required safety level. This standard uses performance levels (PLs), each associated with an interval of probability of failure per hour (PFH), to classify safety related control systems based on their resistance to faults. These levels show how much SRC system should contribute in the risk reduction process and show their safety level. The method used in ISO 13849 requires performing risk assessment and associating a performance level to the safety control system. It uses graphical method and defines the required performance level as a combination of three parameters. Each risk parameter is found based on expert's opinion. Using expert's opinion to define risk parameters, however, is imprecise and uncertain [3]. Moreover, performance level allocations are frequently conservative as a result of accumulation of assumptions to be on the safe side. Furthermore, performance levels (PLs) are defined as crisp intervals and crisp intervals are not appropriate especially when PFH is marginally in an interval. Another type of uncertainty encountered is related to the lack of knowledge about the machine and vagueness in interpretation of risk components. The designed safety control system is then validated against requirements of the associated performance level.

The quality of analyses employed to validate an SRCS is extremely important to assure safety. Such analyses are based on crisp levels where performance level (PL), mean time to dangerous failure ($MTTF_d$) and average diagnostic coverage (DC_{avg}) are calculated and defined with sharp boundaries. The variability of the failure rates to define $MTTF_d$ and DC_{avg} and also assumptions used in the standard for analytical models are based on uncertain and subjective nature of information applied. It is difficult to collect failure rate data for all components and in many cases companies do not provide such data with their components. In such cases, external sources such as MIL-HDBK-217F, IEC/TR 62380, NPRD 95 or IEC 61709 have to be used which entail imprecise information.

As a conclusion, resulting safety function may be considered inexact and the outcome could be an under or over-designed function. An under-design can be dangerous since no adequate risk reduction is obtained. An over design can also be a problem since the additional cost can be a deterrent to the implementation of such measures. Thus, it is important to look for methods that can deal with imprecision in reliability data and subjectivity of risk assessment method. An approach can be using fuzzy logic [4], [5]. Fuzzy has been recently applied successfully in reliability and safety field [6-8]. Nait-Said et al. [9] used fuzzy to solve inconsistency problem in the result of graphical risk

assessment method, caused from subjectivity and interpretation problem. They showed how linguistic values in fuzzy can improve graphical risk assessment. They also provided a calibration method to design fuzzy scales. Sandri and Dubois [3] showed how fuzzy can be used to better educe expert’s opinion. They used possibility theory to deal with imprecision in expert judgment.

The contribution of this paper is to use fuzzy logic to improve methodology of ISO 13849 and help defining requirements of the safety control function. It will be shown how the risk of under/over design, which entails expensive system, can be decreased. This paper is structured as follows. Section 2 discusses the required steps in ISO 13849 to design a SRC and existing shortcomings. Section 3 states the fuzzy approach, and Section 4 provides results from an example.

2 ISO 13849

In 1999, ISO published a new standard using probabilistic methods in addition to previous qualitative measurements in EN 954. To mitigate the pain of using probabilities and various quantifiable measurements, the standard introduced a simpler approach using graphical tools and designated structures [2]. Although using probabilistic approach is a breakthrough in designing safety systems for industrial machines, there are still shortcomings in using such methods.

After studying the machine and its limitations, required safety functions to secure the machine can be identified. Consequently, if safety function has to be implemented using a SRC system, a detailed specification has to be provided for each SRC. A required performance level is then allocated to SRC by using simplified graphical allocation method (See Figure 1).

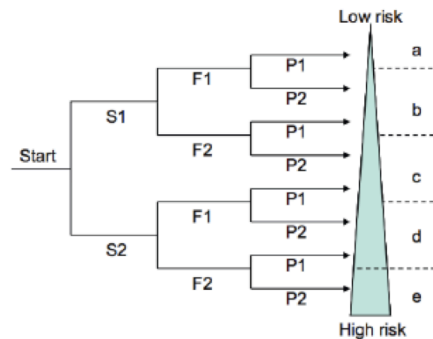


Figure 1. Determination of Performance Level (PL) based on Severity of injury (S1: reversible injury,S2: irreversible and death), Frequency and/or exposure to hazard (F1: low, F2: high), Possibility of avoiding hazard or limiting harm (P1: possible under specific conditions, P2: scarcely possible).

Three risk parameters, namely: severity of injury (S), frequency and exposure to hazard (F), and possibility of avoiding hazard or limiting harm (P) have to be determined. For each parameter two levels are defined. These parameters are then translated to PLs as illustrated in Figure 1. These are lingual values associating a situation to one of the five PLs. One or more experts are asked to give their opinion about each parameter by choosing between linguistic values. Such pooling method is prone to error due to subjectivity and having crisp levels [3].

Subsequently, each PL is associated with a design structure for input, logic and output. After the design is finished, SRC has to be assessed against various performance criteria to verify if required performance level is attained. The three quantitative measurements used in ISO 13849 are: mean time to dangerous failure ($MTTF_d$), average diagnostic coverage (DC_{avg}). Since performance levels as well as $MTTF_d$, DC_{avg} are defined as crisp intervals, for a wide range of probabilities it is probable to under/over design the safety function. Next section shows how fuzzy system is defined and can improve the result.

3 Fuzzy Logic

Fuzzy sets constitute one of the most influential notions in engineering and science. The concept of fuzzy set is intuitive and transparent as it defines how the real world is perceived and described by human. Fuzzy logic has been proven to be a powerful tool to model nonlinear, complex and ill-defined systems [10]. Unlike conventional modeling tools, it is based on human reasoning capability in complex and imprecise environment. Consequently, in

contrast to approaches that require accurate equations to model real world systems, fuzzy logic can deal with existing ambiguities in human driven measurements and judgments.

A membership value $\mu_A(x)$ is allocated to each value of x in the fuzzy set A . The membership value shows grade to which an element x belongs to the fuzzy set A . The power of fuzzy is originated from the fact that an element can simultaneously belong in degrees to two fuzzy sets. Various functions, called fuzzifiers, can be deployed as membership functions. However, trapezoid and triangular functions are the most common fuzzifiers. Choosing the type of the membership function depends on the context and generally is arbitrarily according to the user experience [11].

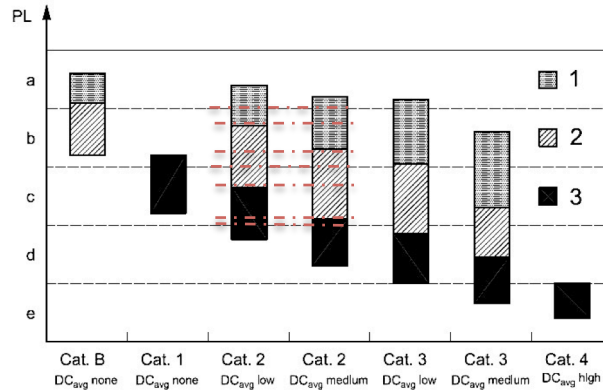


Figure 2. Simplified method to verify PL attain from using the SRC. 1: Low MTTFd, 2: Medium MTTFd, 3: High MTTFd (see Table 1 and 2).

Denotation of each channel	MTTFd
Low	$3 \text{ years} \leq \text{MTTFd} < 10 \text{ years}$
Medium	$10 \text{ years} \leq \text{MTTFd} < 30 \text{ years}$
High	$30 \text{ years} \leq \text{MTTFd} \leq 100 \text{ years}$

Table 1. Mean time to dangerous failure of each channel (MTTFd)

Notation	DC
None	$\text{DC} < 60\%$
Low	$60\% \leq \text{DC} < 90\%$
Medium	$90\% \leq \text{DC} < 99\%$
High	$99\% \leq \text{DC}$

Table 2. Performance Levels and associated probabilities of dangerous failure per hour

Inputs are mapped to output membership function by passing through fuzzy logic inference system. Two popular fuzzy inference methods are Mamadani [12] and Sugeno (TSK). In TSK (Sugeno) model, rules are extracted from the input data. Although TSK-Sugeno is more powerful in modeling a system from data sets, the generated rules have no meaning for experts. In fact, Mamdani fuzzy type is more proper for generating models based on human reasoning and existing rules. Mamdani fuzzy inference has been successfully applied to various problems. The aggregation of fuzzy rules is a way to employ T-norms or T-conorms operators to combine multiple fuzzy sets and produce a single result. Any operator that has T-norm and T-conorm properties can be used, however, min-max operators that are used in this paper have the advantage of simplicity and have extensively been used.

In some cases, the results from fuzzy inference system (FIS) are required to be transformed into crisp numbers. This is in fact, the reverse of fuzzification process. Various approaches have been introduced for distinct applications, amongst which, the most extensively used approach is centroid-defuzzification.

A. Fuzzy determination of required Performance Level (allocation)

Making use of fuzzy logic toolbox in Matlab, the risk allocation method of Figure 1 is implemented. The universe of discourse for each risk factor is $[0,1]$. Since the risk parameters constitute two levels and it is essential to implement the assessment methodology of the standard, it is not possible to add linguistic values to risk parameters. Thus, only two linguistic membership values of: ‘low’ and ‘high’ are used. If X_1 means low and X_2 means high, then X is any risk factor used in the risk allocation method from the set (S, F, P); i.e S_1 means low severity or reversible injury while S_2 means high severity or irreversible injury. By using fuzzy set theory, experts can allocate values to risk parameters between zero and one to show risk estimation between low and high. Semi-triangle functions are used for each membership function (see Figure 3). For X_1 , membership function is equal to one at zero, meaning that its membership value, $\mu_{X_1}(x)$, is equal to one at zero and it decreases toward moving to one. The same theory holds for

X_2 at one and its membership grade decreases moving toward zero. Thus, moving from X_1 toward X_2 means decreasing membership of X_1 and increasing membership for X_2 , i.e. moving from S_1 toward S_2 means increasing severity. Membership functions are defined as shown in Figure 3.

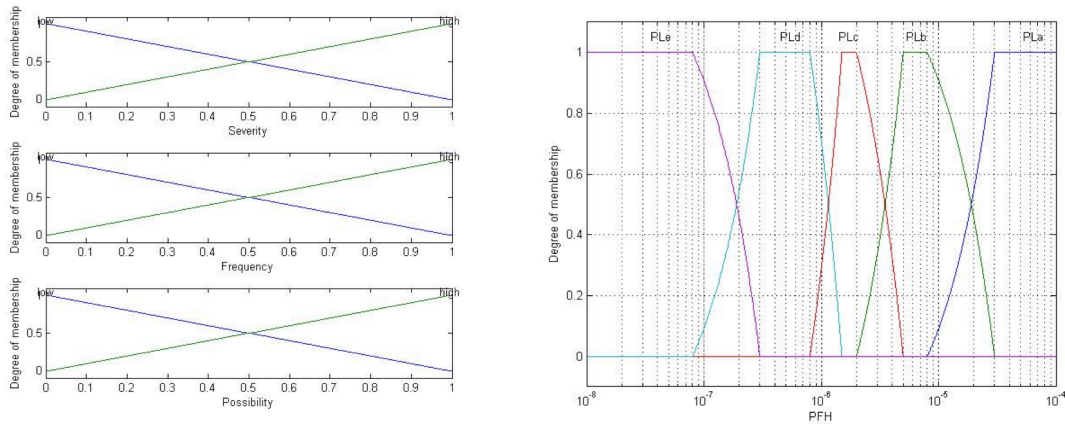


Figure 3. Fuzzification and de-fuzzification membership functions

Owing to the rules in the standard, the performance level determination method in Figure 1 is used to generate fuzzy rules. The total number of fuzzy rules is equal to eight. Table 3 shows rules generated based on risk allocation method in the standard.

	Severity		Frequency		Possibility		PL
1	S1	AND	F1	AND	P1	=>	a
2	S1	AND	F1	AND	P2	=>	b
3	S1	AND	F2	AND	P1	=>	b
4	S1	AND	F2	AND	P2	=>	c
5	S2	AND	F1	AND	P1	=>	c
6	S2	AND	F1	AND	P2	=>	d
7	S2	AND	F2	AND	P1	=>	d
8	S2	AND	F2	AND	P2	=>	e

Table 3. IF-THEN rules based on PL_r allocation rules in the standard

The result of applying fuzzy rules is a set of values (a_1, a_2, a_3, a_4, a_5) showing degrees of each output membership performance level ($PL_a, PL_b, PL_c, PL_d, PL_e$). The last step is to defuzzify the membership values. Trapezoid membership functions are appropriate to transform linguistic values to PFH as they can represent a definite value in an interval. Membership degree of one is assigned to each function for intervals where values are definite, i.e. kernel of trapezoid. The difference between kernel and support (see Figure 5) depends on degree to which engineering and management group may accept a performance level to be part of a higher or lower PL. Strict PL allocation requires kernel to be equal to support, meaning that square membership function is used instead of trapezoid. Various defuzzification methods exist in the literature. Max function may be used when safe side results are required. The disadvantage of max function is that it considers one membership value. The centroid function, however, considers all membership function in the output.

B. Fuzzy validation of the implemented performance level

Subsequent to design of a safety control system, achieved performance level (PL) has to be measured against $MTTF_d$ and DC_{avg} . These two measurements define the maximum claimable PL.

Because category is defined based on the structure of SRCS, it has to be determined in advance and cannot be included in the fuzzy approach. Therefore, distinct fuzzy systems are designed for each category and the two variables $MTTF_d$ and DC_{avg} define maximum claimable PL. The membership functions are defined based on Tables 1 and 2 using trapezoid function.



Figure 4. Steps to design fuzzy validation

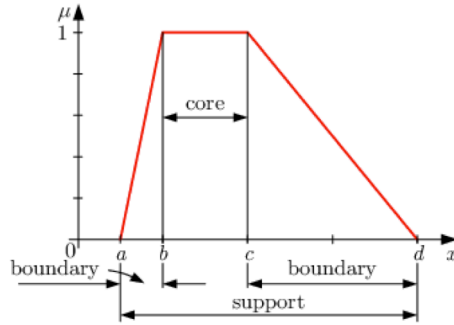


Figure 5. Trapezoidal membership function, distance between a and b = support, and distance between b and c = kernel

Minimum number of rules (n), required for each category depends on values of set $S=(PL, MTTF_d, DC_{avg})$. For each category, illustrated by squares in Figure 1, the following steps must be followed:

1. Minimum value of $MTTF_d$ in the category is chosen and n will be equal to 1.
2. Increase $MTTF_d$ and consider elements of set S.
3. If a level change occurs in any element of set S: increase n; end membership function for the element and start another membership function.
4. Go to step one and continue till end point of $MTTF_d$ in the category.

Membership functions are derived based on procedure above. Boundaries in trapezoid function give ability to a variable to be member of two neighbor sets.

4 Results and Conclusions

As explained in Section 3, as fuzzy inference system is applied, the information flows through each step in the fuzzy system. The fuzzification-inference-defuzzification process generates a defuzzified output from an expert opinion. For any combination of risk parameters, the output shows required safety level as PFH. The result could be evaluated as PL by using max function for output membership functions, before defuzzification is performed. If risk value cannot be shown as extreme values of 0 or 1, expert allocates his assessment by choosing a singleton value in between. A point in risk assessment, means expert is sure about the risk value. Figure 5 illustrates the fuzzy allocation. As it can be seen, expert is able to choose values for risk parameters (severity, frequency and possibility) between zero and one, which is not possible in crisp allocation.

Another evaluation technique is to use possibility theory to pool expert's opinion [3] and then rank each membership function by the expert judgment. Using possibility theory is not considered here.

At the evaluation step, the result is interesting. Table [4] shows the result of crisp evaluation against fuzzy evaluation technique. For values near transition points in Table 1 and 2, conventional approach is very sensitive to changes. The difference between 89.9% and 90.1% can result to a change in PL regardless of $MTTF_d$ value. This is due to the fact that transitions are crisp, and no difference is given to $MTTF_d$ and DC_{avg} unless there is a change in

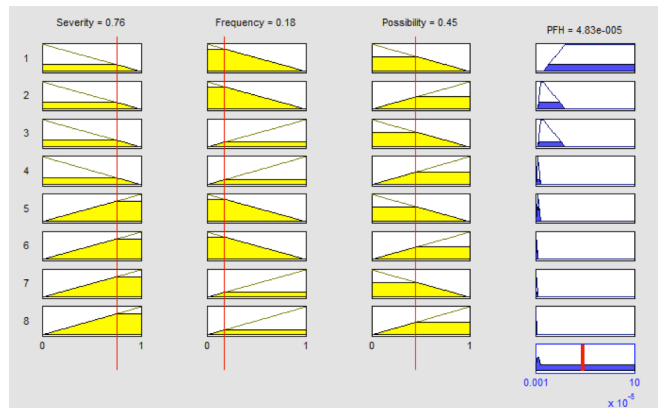


Figure 5. Fuzzy risk allocation; singleton evaluation of risk parameters

Item	MTTF _d	DC _{avg}	PL: Conventional Approach	Fuzzy Approach
1	6.8y: Low	80%	a	1.21*10 ⁻⁵
2	6.8y: Low	89%	a	9.98*10 ⁻⁶
3	6.8y: Low	91%	b	9.83*10 ⁻⁶

Table 4. Validation based on conventional and fuzzy approach

their level.

5 References

1. *IEC 62061 ed1.0, Safety of machinery – Functional safety of safety related electrical, electronic and programmable electronic control systems*, International Electrotechnical Commission, 2005.
2. *ISO 13849-1, Safety of Machinery – Safety Related Parts of Control Systems – Part I, General Principles for Design*, International Standard Organization (ISO), 1999.
3. Sandri S., Dubois D., *Elicitation, Assessment and Pooling of Expert Judgments Using Possibility Theory*, IEEE Transaction on Fuzzy Systems, Vol. 3, No. 3, August 1995, pp. 313-335.
4. Wu Y., Zhang B., Lu J., Du K. L., *Fuzzy Logic and Neuro-Fuzzy Systems: A Systematic Introduction*, International Journal of Artificial Intelligence and Expert Systems (IJAE), Vol. 2, Issue 2, 2011.
5. Nait-Said R., Zidani F., Ouzraoui N., *Fuzzy Risk Graph Model for Determining Safety Integrity Level*, International Journal of Quality, Statistics, and Reliability, Vol. 2008.
6. Bowles, J. B., Pelaez C. E., *Fuzzy Logic Prioritization of Failure in a System Failure Mode, Effect and Critically Analysis*, Reliability Engineering and System Safety, 50, 1995, pp. 203-2013.
7. Xu K., Tang L. C., Xie M., Ho S. L., Zhu M. L., *Fuzzy Assessment of FMEA for Engine Systems*, Reliability Engineering and System Safety, 75, 2002, pp. 17-29.
8. Guimaraes A. C. F., Lapa C. M. F., *Fuzzy Inference to Risk Assessment on Nuclear Engineering Systems*, applied Soft Computing, 7, 2007, pp 17-28.
9. Nait-Said R., Zidani F., Ouzraoui N., *Modified Risk Graph Method Using Fuzzy Rule-Based approach*, Journal of Hazardous Materials, Vol. 164, 2009, 651-658.
10. Wang L., Langari R., *Complex Systems Modeling via Fuzzy Logic*, Proceedings of the 33rd IEEE Conference on Decision and Control, Vol. 4, 1994, pp. 4136-4141.
11. J. Mendel. Fuzzy logic systems for engineering: a tutorial. Proceedings of the IEEE, 83(3), pp. 345–377, Mar 1995
12. Mamdani E. H., *Application of Fuzzy Algorithms for Control of a Simple Dynamic Plant*, Proc. IEEE, 12(1), 1974, pp. 1585–1588.
13. <http://www.mathworks.com/help/toolbox/fuzzy/trapmf.html>

The use of ISO 13849-1 to design "basic" safety functions

Philippe CHARPENTIER, James BAUDOIN, Jean-Paul BELLO
Institut National de Recherche et de Sécurité (INRS)
1 rue du Morvan - CS 60027
F-54519 VANDOEUVRE cedex
philippe.charpentier@inrs.fr, james.baudoin@inrs.fr, jean-paul.bello@inrs.fr

Keywords: ISO 13848-1, control system safety

ABSTRACT

Medium, small and very small enterprises, which manufacture machines only integrating one or a limited number of "basic" safety functions, such as an emergency stop initiated by a mobile protector, experience difficulties in designing control systems for their machines. An example is provided by machine manufacturers encountered in the food processing industry (e.g. vegetable cutters), in some building and civil engineering or service sectors (e.g. drilling machines). These enterprises cannot offer their personnel advanced training in integrating these functions in compliance with existing reference frames, in this case ISO 13849-1 applicable to designing safety functions for control systems combining several types of energy.

This observation has led INRS to conduct a study aimed at editing a guide for the design of these types of safety function by investigating two ways: direct application of ISO 13849-1 and usage of SISTEMA software, a tool designed for calculating, evaluating and checking the safety of control system parts based on ISO 13849-1. These two ways were implemented to design the same "basic" safety function by considering two different architectures.

This paper sets out to describe the main characteristics of the approach proposed by INRS in relation to using ISO 13849-1 to design a "basic" safety function. Additionally, it provides experience feedback on using the SISTEMA software tool for safety function design purposes.

1 "BASIC" SAFETY FUNCTION DESIGN APPROACH

1.1 Background

Design of work equipment (e.g. a machine) requires taking into account its "control system" part, which is intended to ensure the functionalities expected of the equipment. When safety functions are necessary, the control system must also process them, thereby contributing to the reduction of risks generated by the work equipment in relation to exposed operators and third parties.

Among the reference frames available for machinery design, ISO 13849-1 [1] describes the general principles for designing the Safety-related Parts of Control Systems (SRP/CS) implementing different types of energy such as electrical, hydraulic or pneumatic. This standard replaces Standard EN 954-1 [2], which was widely known by industrial companies but is no longer applicable.

ISO 13849-1 conserves the major design principles required by EN 954-1. The main new features of this standard involve introduction of the Performance Level (PL), characterised by the safety function's contribution to risk reduction ("a" to "e", "a" being the lowest PL) and quantification of a number of parameters, in particular:

- the Mean Time To dangerous Failure (MTTF_d) calculations based on reliability data and demand rate of the components implemented,
- the measures adopted to ensure component diagnostic coverage,
- the measures adopted against common cause failures.

These developments in the standard may disconcert companies required to design machines, whose control systems only integrate one or few of “basic” safety functions, e.g. a stop initiated by a mobile protector. This is specifically the case when designing safety functions for control systems combining several type of energy requiring application of ISO 13849-1.

This paper not only details the significant points in the INRS-proposed approach to designing these types of safety function, but also provides experience feedback on using the SISTEMA software tool for designing safety functions.

1.2 Selection of the best suited approach

It is important that designers direct themselves towards the approach best suited to their specific problem. To help them, INRS proposes a graphical aid to select this approach, which takes into account their usual practices, and the possibility to use existing components or modules. Several solutions can be envisaged (cf. Figure 1 at the end of this document) that will involve different actions on the part of the designer, depending on whether he is resorting to:

- Only SRP/CS of known PL, higher or equal to the required PL for the SRP, e.g. an off-the-shelf safety module, a photoelectric safety barrier, etc., these PL will have been determined by the designers of these different modules;
- A combined solution implementing SRP/CS of known PL, higher or equal to the required PL for the SRP and one or more SRP/CS designed by himself (cf. Figure 2);
- A single, specifically designed SRP/CS, e.g. an assembly of often basic components, such as position switches, proximity sensors or electromagnetic relays.

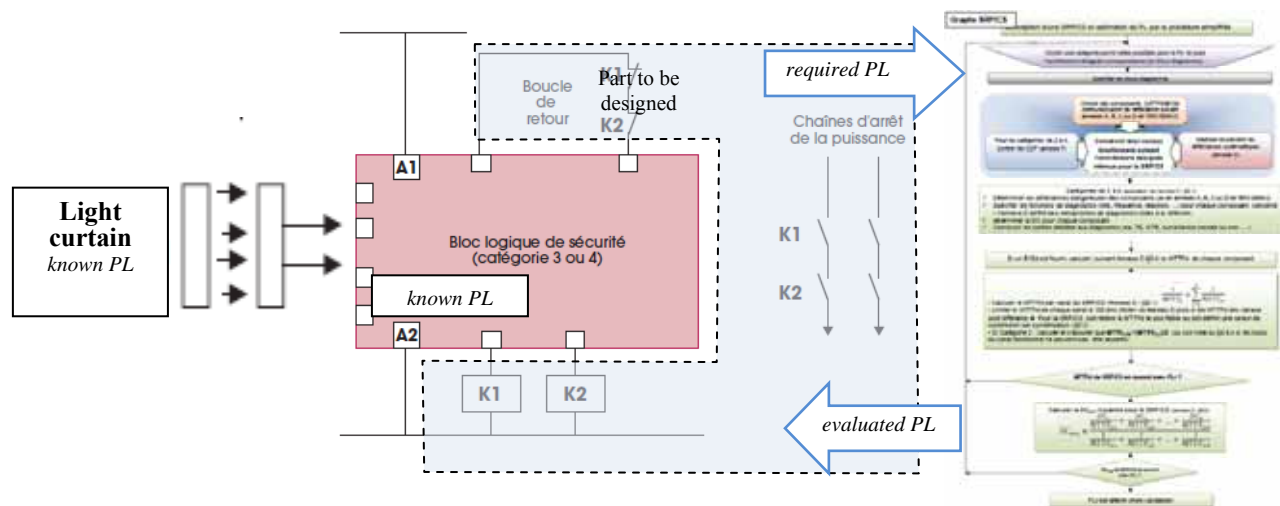


Figure 2. Combined solution

1.3 Design of a SRP/CS

In the case of approaches b) and c), the designer has to design at least one SRP/CS after specifying it. His objective will be to design the SRP/CS by implementing the necessary measures for achieving a performance level at least equal to that required for the SRP. To achieve this, the designer must consider:

- the structure,
- safety function behaviour in the event of failure,
- the capacity for executing a safety function under foreseen environmental conditions,
- Common Cause Failures (CCF),
- systematic failures,
- the MTTFd for single components,
- the Diagnostic Coverage (DC),
- the safety-related software.

The following graph (Figure 3) is intended to facilitate SRP/CS design (excluding the software part) by applying the simplified method provided by the standard, based on a previously specified, required performance level.

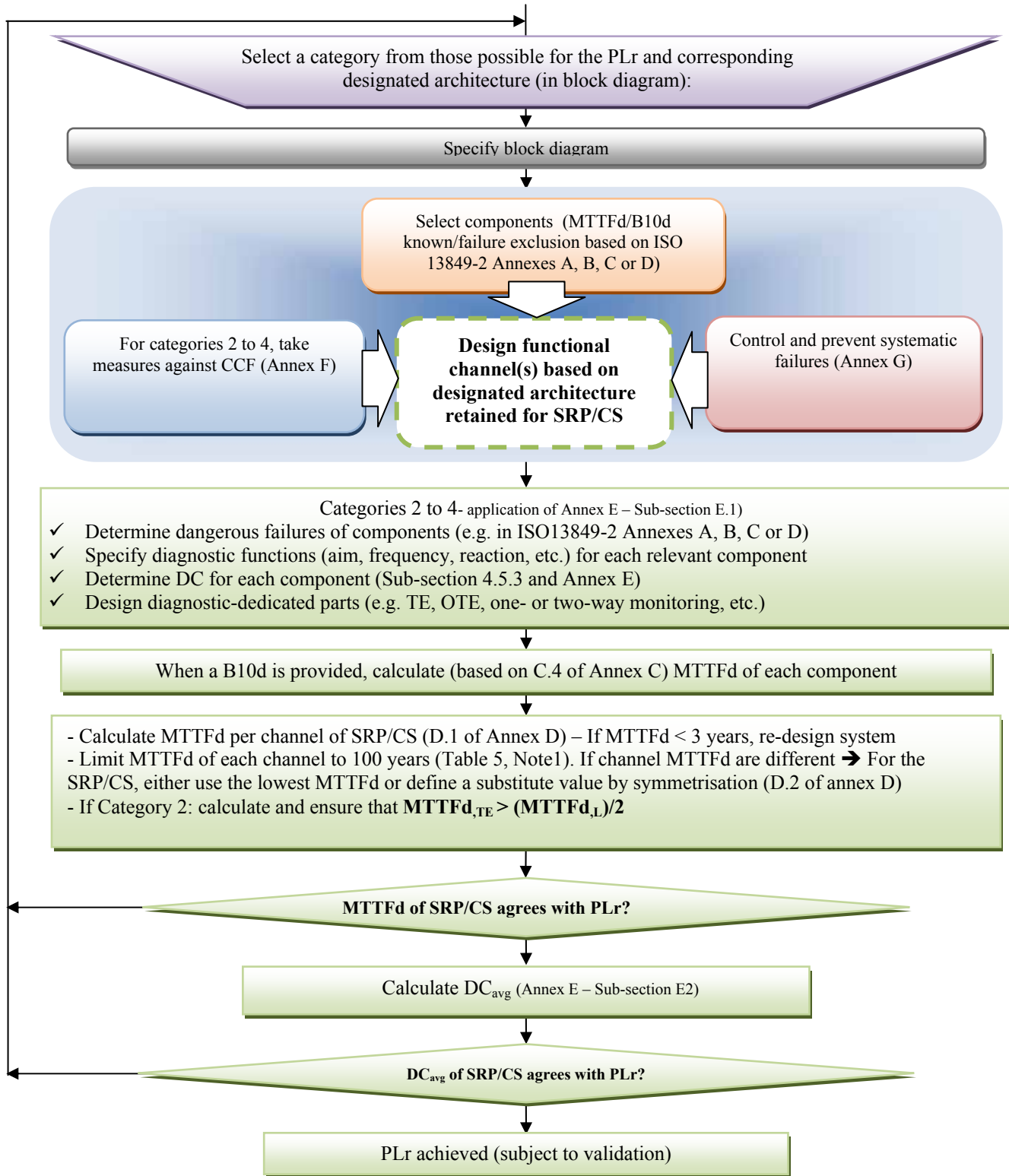


Figure 3. Graph of SRP/CS design

The simplified method given in the standard is based on a number of designated architectures, for which “pre-calculations” were performed, thereby facilitating application of its quantitative requirements. To facilitate design work, INRS proposes reformulating the Figure 5 table in the standard, in such a way that it does not disconcert designers because, for a given PL, it progresses from the idea of category in EN 954 (blue part) to then introduce the additional requirements of the new ISO 13849-1 (brown part). Table 1 provides an example of this reformulation for performance level “d”.

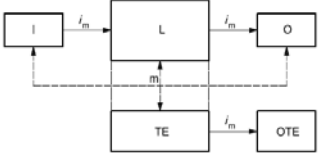
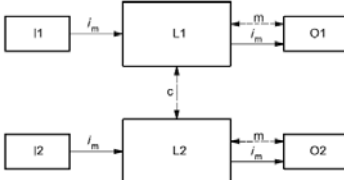
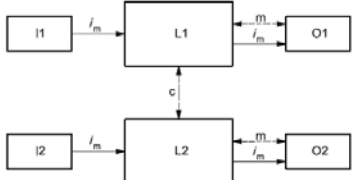
Minimum requirements for achieving PL “d” (based on Table 7 in the standard and applying the simplified procedure)			
Authorised categories	Cat 2 Sub-section 6.2.5	Cat 3 Sub-section 6.2.6	Cat 3 Sub-section 6.2.6
Other category compliance	Complies with Cat B requirements		
Specific characteristics	- Well-tries components and safety principles - MTTFd,TE to be considered	- Well-tries components and safety principles - Single fault = Safe state	- Well-tries components and safety principles - Single fault = Safe state
Checking of functions - Frequency	Machine start-up, then periodic (automatic or manual), and request rate $\leq 1/100$ test rate	If possible, at or before the next demand	If possible, at or before the next demand
Checking of functions - Reaction	If fault detected: switch to safe state (stop) OR danger warning	If fault detected: switch to safe state (stop)	If fault detected: switch to safe state (stop)
Designated architecture			
Systematic failures	Annex G of standard		
MTTFd per functional channel <i>Sub-section 4.5.2</i>	30 yrs \leq MTTFd \leq 100 yrs (thus MTTFd = “High”)	30 yrs \leq MTTFd \leq 100 yrs (thus MTTFd = “High”)	10 yrs \leq MTTFd \leq 100 yrs (thus MTTFd \geq “Average”)
Min. DCavg <i>Sub-section 4.5.3 and Annex E</i>	DCavg \geq 90% (thus DCavg \geq “Average”)	DCavg \geq 60% (thus DCavg \geq “Low”)	DCavg \geq 90% (thus DCavg \geq “Average”)
CCF Annex F	score \geq 65	score \geq 65	score \geq 65

Table 1. Minimum recommendations for a given PL – example of PL “d”

1.4 Applying the approach

The approach described above was applied to the same safety function (stop using protector of PL “d”) by resorting to two different architectures (categories 2 and 3). This process enabled us to show that the calculations to be performed remain reasonable and limited, if the safety functions are simple and involve few components or the selected components have known performance levels.

2 USE OF SISTEMA SOFTWARE

For cases involving more complex applications, a free software tool is available: SISTEMA. This enables Standard ISO 13849-1 to be applied by requiring the designer to go through the design stages recommended by the standard and by calculating the necessary data.

Note. For the examples considered, the PL results obtained using SISTEMA are the same as those obtained using the simplified method provided by the standard.

Several observations can be made following SISTEMA usage:

- ✓ It does not explicitly consider the measures to be implemented for dealing with systematic failures, obliging the designer to consider these separately by applying Annex G of the standard;
- ✓ It does not exempt the designer from possessing accurate knowledge of the standard since he remains responsible for design decisions. For example, how does he decide on the use of a safety category and a designated architecture without knowing its characteristics?
- ✓ It does not deal with the software part of safety-related control systems;
- ✓ The SISTEMA terminology is different to that of ISO 13849-1 in relation to SRP/CS, which are called “Subsystems” (SB) and it introduces the notion of elements (block “sub-parts”) which does not explicitly appear in the standard. The proposed process decomposition is close to that of IEC 62061;
- ✓ Its usage requires the same preparatory work as when the design is performed without it, for example:
 - specifying the SRP (called “SF”), the SRP/CS (called “SB”) and components (called “BL” and/or “EL”),
 - considering and selecting the foreseen designated architecture,
 - determining the component reliability data (B10d, MTTFd) or failure exclusion,
 - specifying CCF counter-measures,
 - analysing possible failures to determine parts to be taken into account,
 - specifying diagnostic functions.

Finally, with or without SISTEMA, the functional part control and diagnostic set-ups still need to be designed in strict compliance with established specifications and declared design choices.

3 CONCLUSION

The INRS-proposed method, soon to be published, allows to design “basic” safety functions without using a specific tool. Based on the simplified approach of ISO 13849-1, it provides designers with an accessible means of dealing with simple safety functions, if there are few implemented components or the components/modules involved in the design have known performance levels. The approach also enables the designer to refer easily to the detailed recommendations of the standard by systematically quoting sub-section or annex references.

When more complex functions have to be designed, SISTEMA software facilitates the design iterations and allows a final report to be drawn up; in common with all software tools, it therefore ensures project traceability and makes easier the possible future evolutions. It therefore represents a helpful tool, when used along with ISO 13849-1 as a support and application guide to the latter standard’s recommendations.

Finally, it is important to stress that, in either case, it will be compulsory for the designer to have appropriated the standard to a minimum degree before embarking on the slightest development.

4 REFERENCES

1. ISO 13849-1, *Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design*, 2006, 102 p.
2. EN 954-1: 1997, *Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design*, 44 p.

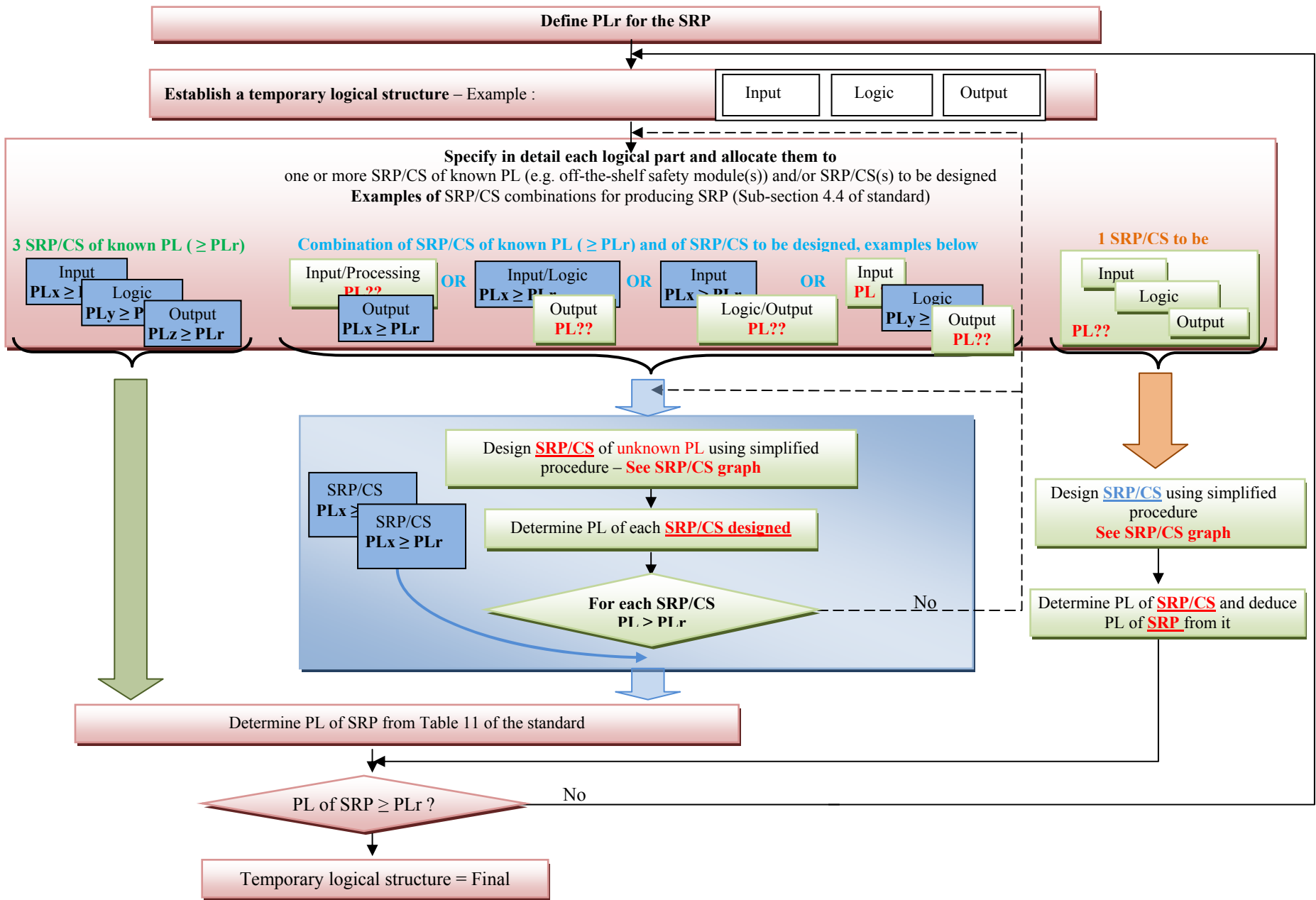


Figure 1. Graph of general design process for a safety circuit based on achieving a required PL

Architectural Views of Safety Systems

Timo Vepsäläinen, Seppo Kuikka

Tampere University of Technology, Department of Automation Science and Engineering,
P.O. Box 692, FI-33101 Tampere, Finland
Tel. +358 40 849 0062, Fax +358 (0)3 3115 2340, E-mail {timo.vepsalainen, seppo.kuikka}@tut.fi

KEY WORDS functional safety, software architecture, documentation

ABSTRACT

Traditionally, the preferred technologies for functional safety systems have included, for example, mechanical, electrical and (non-programmable) electronics. However, due to demands for flexibility, cost-efficiency and performance, also safety-related systems are nowadays increasingly implemented with software and programmable units as their essential parts. In software development, one of the most important development phases affecting the quality of the final products is architecture design. However, related to software architectures, many safety standards still focus on issues that are more important in traditional safety systems, e.g. redundancy.

In this paper, the focus is on *software architectures* of safety systems and their documentation using modern practices of software engineering. We approach the subject by extending a general purpose architecture knowledge management (AKM) database with architectural safety views and functions supporting safety system development. The views focus on efficient presentation of safety related information, traceability, consistency as well as guidance on making architectural decisions. With the resulting AKM database, which is demonstrated with an example application, we foresee it possible to facilitate both the development and certification of safety systems.

1 INTRODUCTION

Traditionally, the preferred implementation technologies for functional safety systems have included, for example, mechanical, electrical and (non-programmable) electronics. However, due to demands for flexibility, performance and cost-efficiency, also safety-related systems and their safety functions are increasingly implemented with software and programmable units as essential parts of them. Software functions are flexible and modifiable even without changes to hardware. Small programmable units may supervise numerous devices and perform numerous safety functions which may include complex logic for initiating interlocking and protective actions. However, assessing software safety and reliability differs from assessing them in traditional mechanical or electrical components which have led to different kinds of approaches in ensuring their quality. Instead of statistics and probabilities, safety standards such as IEC 61508 [1] concentrate on development techniques, measures and tools to be used during different development phases, e.g. requirement specification, detailed design and implementation.

During recent years, the consciousness over the importance of software architectures has raised in software engineering research and industry. For example, ISO/IEC 42010:2007 [2] (also known as IEEE 1471) standard as well as numerous publications have been written about developing and documenting software architectures. In the standard [2], software architecture is defined as fundamental organization of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution. Traditionally, software architecture have been documented using viewpoints and views, the most popular set of viewpoints being known as “4+1 model”, including logical, development, process and physical views as well as scenarios [3]. However, recently the focus in architecture documentations has been widened to cover also the rationale behind design, in addition to design itself. For example, Kruchten et al. [4] define architectural knowledge as a sum of architectural design and architectural decisions (rationale for the design). Moreover, architectural knowledge can be divided to application-generic (e.g. design patterns) and application-specific knowledge [5].

Also within safety systems, well-defined and justified architectures may facilitate the achievement of both safety and security goals whereas inadequate solutions are more difficult to understand, develop and maintain in a controlled manner. The importance of architectures is significant especially in safety systems if their lifespan is long and they are developed, produced and distributed in different versions over years. The most important design phase affecting the simplicity of further developing systems, adding new functionalities and reacting to changing customer

and business needs is - without a doubt - architecture design. Software architectures of safety systems not only include aspects such as fault detection and redundancy but their structural and functional organizations, decisions and rationale behind them, use of design patterns as well as practices guiding their development. However, it is our fear that not all these aspects are given adequate attention in many safety standards. Nevertheless, in order to produce certifiable safety systems, the requirements of safety standards must be fulfilled.

In this paper, our aim is to address the issue of documenting architectures of safety applications by extending the information content and views of an architectural knowledge management (AKM) database to provide more support for safety system development. As a basic functional safety standard we use IEC 61508; partly because of its wide influence and partly because it has been renewed recently (2010) and consequently should present the industrial state-of-the-art. The new architectural modelling concepts that constitute a metamodel are implemented as Sulava AKM database that we have developed during Sulava project on Polarion ALM (Application Lifecycle Management) platform and will use in this paper for demonstration purposes. A mobile elevating work platform (a) that will be used as an example throughout the paper and the functional safety requirements of (b) it are illustrated in Figure 1, the latter part thus providing an example of one of the safety views developed for the AKM system.

The rest of this paper is organized as follows. In section 2, we focus on documenting software architectures of safety systems and the additions to the AKM designed for this purpose. In section 3, we extend the scope of the Sulava AKM to guidance on architecture design. Finally, in section 4, before conclusions, we discuss and present work related to this important research topic.

- a) Safety related example system b) Safety related, functional requirements related to the system.

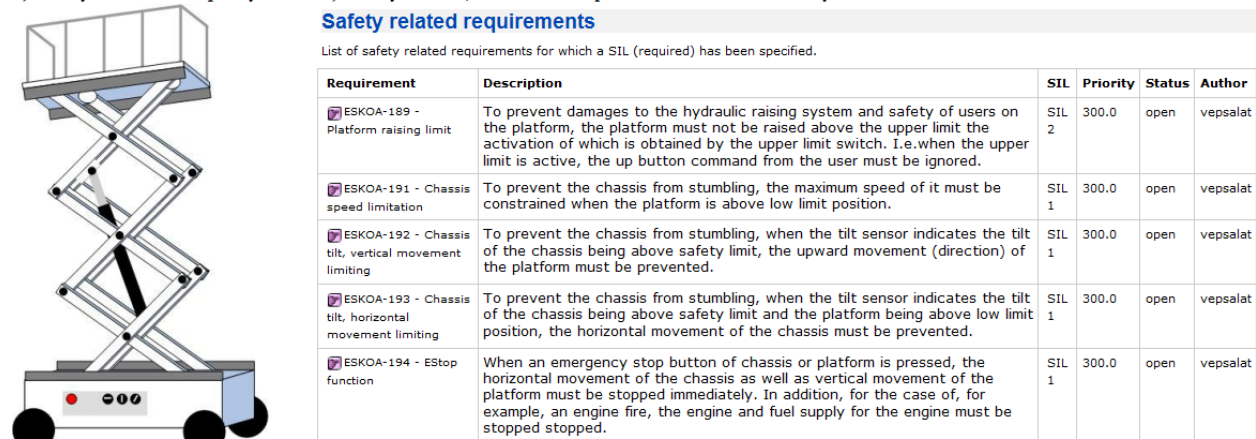


Figure 1. An example system that is used for demonstration purposes in this paper.

2 DOCUMENTING ARCHITECTURES OF SAFETY SYSTEMS

The objective of our work during Sulava project was to extend the support of the Sulava AKM database, presented in detail in [6], for documenting architectures of safety systems while maintaining its views and functionality related to general architectural work. In architecture documentations of safety systems, special attention need to be paid on documenting their safety related features and aspects that affect their certifiability. On the other hand, instead of other safety system development phases, we focus on architecture design because most essential design decisions should be made by system architects. Selection of a programming language for a project, for example, should be made by the system architect and documented as part of architecture documentation although it is in, for example, IEC 61508 related to implementation phase.

However, a challenge related to architectures of systems that may contain both safety related parts and non-safety-related parts is that artefacts of same type, e.g. requirements, can be safety-related in some cases but not in some others. In the work, solving this challenge was the first objective and approached by using general purpose architecture documentation artefacts as a basis and extending their information content in order to be able to *identify* the safety related ones and to present them in an efficient manner in safety views while maintaining the other views. Secondary objectives of the AKM database development were in supporting *traceability* and *consistency* between the artefacts - with the justification that they are objectives the achievement of which can be significantly improved by using models to store information and automating model processing. For example, models can be used for checking that all requirements are traced to implementing components and that the specified safety levels of the

components are compatible with the requirements. Another aspect, which will be discussed in section 3, is guiding architectural decision making based on recommendations of safety standards to ensure conformance to them. Of the architecture documentation concepts that are presented in detail in [6], we concentrated on *requirements*, *components*, *design patterns* and *decisions*. The importance of requirements is significant as the main purpose of safety systems can be seen in implementing their specified safety requirements, which are thus essential information for architects. Safety requirements, in general, consist of two parts including the required safety functionality and the level of safety, defined with e.g. SIL, on which the functionality must be implemented. Components are in Sulava AKM the main concept for specifying structural building blocks of systems, such as, control loops or interlocking functions. *Design patterns*, which have been wide studied in general software engineering, are general, reusable solutions to re-occurring design challenges with documented pros and cons. For safety systems, design patterns - or recommended solutions that could be presented in the form of design patterns - could be also found from safety standards. Finally, architectural *decisions* are those of architects related to the system and the development of it. Similarly to patterns, also decisions may be recommended by standards. For example, a decision could concern the use of modelling techniques that may be recommended to different safety integrity levels. Figure 2. presents a metamodel specifying the developed concepts including their information contents and relations to each other.

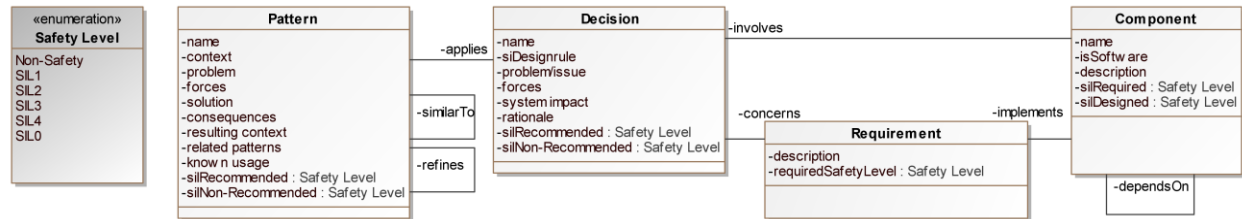


Figure 2. Central safety related concepts of the Sulava AKM database including their safety related attributes.

In models conforming to the metamodel, instances of the concepts can be identified as safety-related with use of attributes of type Safety Level. For this purpose, the metamodel defines 4 levels according to the safety integrity levels (SIL) in IEC 61508 and an additional level, SIL0, meaning safety related but below actual SILs or non-specific SIL. The purpose of specifying also safety levels, in addition to simply marking concepts as safety related e.g. with simple Boolean attributes, is to enable consistency checks between, for example, safety level specifications of requirements and components. In addition to the attributes shown, all instances of the concepts include properties such as author and status that are common to all work elements in the AKM database.

By nature, requirements are assumed to be functional and they can be identified (marked) as safety related by specifying an appropriate, required safety level. Components can be identified as safety-related by specifying the required and designed SILs – of which the designed SILs should be greater or equal to those required. Decisions and Patterns, finally, can be identified as safety related based on their SIL recommended and SIL non-recommended attributes. These attributes are intended for specifying the highest level for which a pattern or decision is recommended and the lowest level for which it is non-recommended - with the purpose of being able to automate checking that they are suitable to be used in the current design context. In addition, any pattern or decision can be specified as safety related by using the SIL0 level, literally meaning a safety related pattern or decision for which a recommendation is not available. As a whole, the properties mentioned above are the main means of the Sulava AKM database to *identify* modelling concepts that are related to safety and should be shown in safety *views*.

The views in which the concepts are shown can be divided to 2 categories based on their purposes. Views of the first category present compilations of safety related concepts and are aimed to facilitate finding and viewing safety related information from the database. Those of the second category, on the other hand, concentrate on traceability and consistency between concepts. An example view of the first category, showing tabular presentation of requirements related to the example system was shown in part b of Figure 1 in section 1. In addition to descriptions of requirements, the table in the figure shows their statuses, priorities, authors and required safety levels. Similar views are also available for components, decisions and patterns; however they are not illustrated with any figures in this paper. Related to components, the view presents both the required and designed SILs and related to patterns and decisions, both the SIL recommended and SIL non-recommended values. Additionally, the component view automates the calculation of required safety levels for components based on SIL specifications of requirements and how the components are specified to implement the requirements - either directly or by being required by other components implementing a requirement. Status and priority information, on the other hand, could be used to assess the progress of a project whereas author information, which is maintained automatically, improves the transparency of development work by storing the author and designer information of, for example, components.

The views of the second category are intended to improve *traceability* and *consistency* between the artefacts. For example, Figure 3. illustrates a view that presents the traceability between specified requirements and components that are primarily responsible for implementing the requirements. In the view, safety requirements are presented in rows and components implementing them in columns. A component implementing a requirement (traceability between them) is illustrated with a mark the colour of which is normally black but which is highlighted with red colour if the designed SIL of the component is non-compatible with the required safety level. In the figure, for example, component ESKOA-209 is designed to have safety level SIL 1 although it is supposed to implement a requirement with required safety level SIL 2. This kind of faults, that could be easily caused by, for example, raising a safety level of a requirement, are thus automatically discovered and warned by the database. Other views of the category present dependencies between components as well as traceability between components and decisions and between components and patterns. In addition, inconsistencies between designed SILs of components and between level recommendations of patterns and decisions are warned by highlighting them with red colour.

Especially with the automated warnings we have tried to remove manual work from developers allowing them to concentrate on more demanding design tasks. For example, in case of large systems, modifications to required safety levels after first iterations of development work could cause unpredictable amount of non-profitable work related to determining which components and design practices must be modified. With use of the database, however, this work is automated based on dependencies and traceability between requirements, components, patterns and decisions, resulting in both reduced amount of repeated work and increased confidence in compatibility of the architecture.

REQUIREMENTS, required SIL COMPONENTS: required SIL, designed SIL	ESKOA-206 - Speed limit interlock : SIL1, SIL1	ESKOA-207 - Tilt prevention interlock : SIL1, SIL1	ESKOA-208 - Emergency Stop interlock : SIL1, SIL1	ESKOA-209 - Platform upper limit interlock : SIL2, SIL1
ESKOA-189 - Platform raising limit , SIL2				x
ESKOA-191 - Chassis speed limitation , SIL1	x			
ESKOA-192 - Chassis tilt, vertical movement limiting , SIL1		x		
ESKOA-193 - Chassis tilt, horizontal movement limiting , SIL1		x		
ESKOA-194 - EStop function , SIL1			x	

Figure 3. An example of a traceability sub-view presenting traceability between requirements and components.

3 FROM DOCUMENTATION TO GUIDANCE

In addition to aiding documentation, software architecture design could be also facilitated by guiding architectural decision making based on safety standards and their recommendations. IEC 61508 [1], for example, in its third part explicitly recommends a number of architectural solutions as well as techniques and measures to be used in different development phases of software applications. Table A.2 of annex A [1], for instance, presents the recommended techniques and measures to be used in software architecture design. Similar tables are available for all phases of the traditional V-model, which is used as a reference in the standard, many of them containing recommendations to decisions that are usually made by architects. For example, selection of a programming language for a system is often a decision to be made by the system architect, although it is in the standard related to implementation phase. Modelling such recommendations could alone benefit architects by making the recommendations visible during design. However, it could also enable project specific decisions to be linked and compared to recommendations in order to compose and provide information on 1) what recommended decisions have been already made, 2) what recommended decisions are still to be made, and 3) would the design be compatible for other safety levels.

A simple metamodel presenting a set of concepts specified for this purpose is shown in Figure 4. In the metamodel, the Safety Profile concept is aimed for modelling of both standards and their sections related to, for example, architecture design or implementation. Required Decisions are intended to model decisions that should be made and for which there may be several alternatives. Decision Alternatives, on the other hand, are contained by Required Decisions and can be non-recommended (NR), highly-recommended (HR), recommended (R) or non-specified (NS) for different safety levels. For example, in our example project, we have created instances of the safety profile concept for IEC 61508 and for architecture design the first one being the parent of the latter one. For architecture design, we have defined 15 required decisions and for all of them at least one decision alternative similarly to recommendations of IEC 61508 in its table A.2 of annex A. A subset of them is shown in Figure 5.

The relation from Decision to Decision Alternative, finally, is aimed for marking correspondences between project specific decisions and decision alternatives that are not aimed to be project-specific. That is, safety profiles and their contents should be application-generic information and only referenced from project specific documentations and decisions with use of the instanceOfAlternative relation.

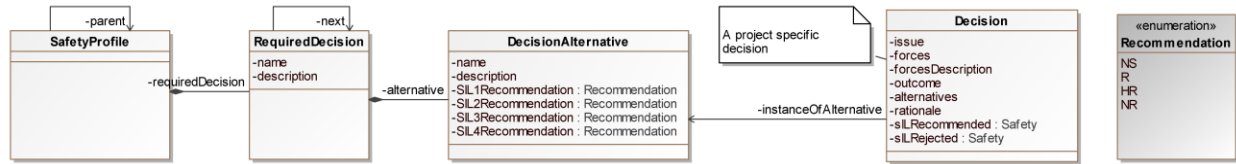


Figure 4. Concepts of the Sulava AKM database for modelling of safety standards and their recommendations.

A table view utilizing the concepts is shown in Figure 5. that have been visually modified to meet the space restrictions of SIAS publications. When constructing the view from the information contents of the database, requirements are first analysed in order to find the highest required safety level. Profiles, required decisions sand decision alternatives are presented in the rows so that the recommendation column corresponding to the highest found safety level is emphasized with grey and the decision alternatives used in the project either with light green or light red, depending on whether or not the alternative is recommended to the safety level in question. In addition, the table calculates the amount and percentage of recommended decision referenced by the project-specific decisions.

For example, according to the table, the highest required safety level in the project is SIL 2. In the project, static resource allocation and cyclic behaviour approaches have been used which are recommended or highly-recommended for SIL 2. In addition, there would be 10 (12-2) other required decisions with recommended or highly-recommended decision alternatives for SIL2, e.g. fault detection as seen in the figure.

With the view, we have aimed to facilitate both the work of the architects as well as the certification processes of the systems. Architects, firstly, may use the view when considering different kinds of techniques and approaches to organize and develop new systems. Linking project specific decisions to recommended ones enables calculation of statistics and, for example, compatibility of the decisions to other safety integrity levels could be easily tested by changing the highest safety level in the project and reloading the view to obtain new statistics. During certification, on the other hand, the view could provide the authorities an insight about how the techniques and measures used during the project are compatible with the standard. Finally, profiles and their recommendations can be modified when standards change or new standards are taken into use by modifying the work items used to model them; that is, the support of the AKM database is not limited to the current version of IEC 61508.

Profile	Required Decision	Decision alternative	SIL1	SIL2	SIL3	SIL4
IEC 61508, architecture design						
	Fault detection and diagnosis					
		Fault detection	-	R	HR	HR
		...				
	Execution timing					
		Event-driven, with guaranteed maximum response time	R	HR	HR	-
		Time-triggered architecture	R	HR	HR	HR
		Cyclic behaviour, with guarantees maximum cycle time	R	HR	HR	HR
	Resource allocation					
		Static resource allocation	-	R	HR	HR
	Access to shared resources					
		Static synchronization of access to shared resources	-	---	R	HR
Number of recommended or highly recommended decisions made between the alternatives for SIL 2:	2 / 12					
Percentage of recommended or highly recommended decisions made between the alternatives for SIL 2:	16%					
Number of non-recommended decisions made between the alternatives for SIL 2:	0					

Figure 5. An example view showing and linking project specific decisions to recommendations of standards.

4 RELATED WORK

Architectures of safety systems are addressed by practically all safety standards. For example, IEC 61508 [1] and ISO EN 13849 [7] give guidance on selecting architectural approaches related to fault detection and handling, timing as well as management of resources, among other aspects. In addition, ISO EN 13849 presents simple, general

structures for safety systems of different categories with emphasis on monitoring and redundancy aspects. Redundancy and redundancy-related design patterns are also addressed by several other publications focusing on safety system development and architectures. Douglass, for example, in [8] presents 4 patterns for safety systems including: Homogeneous Redundancy, Diverse Redundancy, Monitor-Actuator and Safety Executive patterns. However, what is missing in many standards and other safety publications is guidance on how to document architectures, decisions and traceability in an efficient and certification-friendly manner. Application lifecycle management (ALM), which can be seen as product lifecycle management for software systems, is an activity that could be used also in safety system development for the coordination of activities and management of artefacts (e.g. requirements, source code and test cases) of complex software systems. In this work, we extended Polarion ALM tool, which is a commercially available, extendable, web-based ALM solution. In addition to our work, Polarion, which can be specialized by specifying both the modelling concepts and the views utilizing the concepts, has been extended for special purposes also by others. MedPack [9], for example, has been specified to facilitate fulfilling the requirements of IEC 62304 and certifying of medical applications.

5 CONCLUSIONS

In this paper, we have presented safety-related additions to Sulava AKM database. With the work, we have tried to extend its support for safety related systems by aiding finding and efficient presentation of safety related, architectural information. In addition to finding information, the new concepts and properties to existing ones have been specified with automated model-checking and traceability in mind. The presented views implement several features that we believe to be useful in development of safety systems and their architectures. Firstly, the views enable calculation of safety levels for components based on relations between components and between components and requirements. On the other hand, traceability and consistency views link the modelling artefacts together and warn developers about mismatches between components, decisions and patterns if their recommended safety levels are appropriately specified. Finally, a view has been specified for presenting recommendations of safety standards and for enabling statistics to be generated about correspondence of project specific decisions to standards. In the paper, we have also used design pattern concept for the modelling of technique and measure recommendations of IEC 61508. Defining patterns based on standards could be beneficial also in general because of the form of patterns that has been developed to aid communicating common solutions to re-occurring design challenges.

In future research, we seek to integrate the developed concepts and tool support with our past work related to modelling and model-driven development of safety related control systems on more detailed levels of design. That is, we believe that a combination of modelling techniques and model processing support for both architecture and detailed design is required in developing future safety related control systems.

6 REFERENCES

1. International Electrotechnical Committee. IEC 61508: functional safety of electrical/electronic/programmable electronic safety-related systems. Parts 1-7. 2010.
2. International Organization for Standardization: ISO/IEC 42010:2007 systems and software engineering – recommended practice for architectural description of software-intensive systems. 2007
3. Kruchten, P. The 4 + 1 View Model for Architecture, IEEE Software, vol. 12, issue 6, November 1995.
4. Kruchten, P, Lago, P., van Vliet, H., Wolf, T. Building up and exploiting architectural knowledge. In: Proceedings of the 5th IEEE/IFIP Working Conference on Software Architecture (WICSA), pp. 291-292. IEEE Computer Society, USA (2005).
5. Lago, P., Avgeriou, P., First Workshop on Sharing and Reusing Architectural Knowledge, ACM SIGSOFT, Software engineering notes, vol. 31, issue 5, September 2006.
6. Eloranta, V.-P., Hylli, O., Vepsäläinen, T. and Koskimies, K. TopDocs: Using Software Architecture Knowledge Base for Generating Topical Documents. Joint 10th Working IEEE/IFIP Conference on Software Architecture & 6th European Conference on Software Architecture. August 20-24, Helsinki, Finland.
7. ISO EN 13849-1. 2007. Safety of machinery — Safety-related parts of control systems - Part 1: General principles for design.
8. Douglass, B. Safety-Critical Systems Design, in Embedded Systems Conference, 1998.
9. Polarion MedPack extension. <http://www.johner-institut.de/index.php?id=3093>.

CONSIDERATION ON THE STRUCTURE FOR RISK REDUCTION OF FIRE FROM ELECTRIC DEVICES

Akira MATSUURA¹, Takabumi FUKUDA²

¹ Nagaoka University of Technology, 1603-1 Kamitomioka-machi, Nagaoka, Niigata 940-2188, Japan
amatsu24@tba.t-com.ne.jp

² Nagaoka University of Technology, 1603-1 Kamitomioka-machi, Nagaoka, Niigata 940-2188, Japan
t-fukuda@vos.nagaokaut.ac.jp

Abstract

One of the basic safety measures for avoiding risk of overheating and fire, is energy elimination. By cutting off energy, some kinds of machine move toward safe state; e.g. pressurized equipment. In the pressure system, it is possible to avoid an accident by opening the safety valve when the pressure force from inside is greater than the spring force.

However, some systems cannot move toward safe state from dangerous condition for avoiding risk immediately after the energy source has been cut off. (This situation is discussed in this paper.) Rotating systems with large inertia are typical examples.

In this paper, the authors consider on the structure for instinct safety in the heating system. If hardware circuit had detected the dangerous condition and it has cut off energy source to the heater when a condition had already had met to the potential ignition condition; the heater ignites. Before such a situation, it is considered to cut off quickly enough. However, in many cases, it conflicts with the original functions for the machine to perform.

The basic structure for the pressure system's safety is established and is shown in EN764-7 as three layer strategy. In this paper, the authors compared heating system with pressure system, and proposed the safety strategy which is:

- (1) By providing a sufficient margin of protection of three phase,
- (2) When there is a failure in safety-related functions, the operation will be stopped even if the machine condition is safe
- (3) By providing diagnostic system in the temperature control unit.

The summary of our proposal is incorporating a system of two concepts (redundancy and diversity) on control unit of electric heater, before it becomes dangerous condition, and the abnormal event occurs on the control system, the power source is cut off.

It is desired to indicate a plant safety considering plant itself and the integrated safety-related system. In accordance with that performance has degraded by the aging, hard circuit shuts off power before the internal heater is high fever and high temperature above the critical value.

1. Introduction

Fire accident report ^[1] has been issued on Nov. 2011 (by NFPA: National Fire Protection Association). As shown in Figure 1.1, the number of accidents decreased from 1980 of 232,000, to 2009 of 58 900. The data is from the fire report by U S fire department.

In Fig. 1.2, the data details the situation in the last four years; i.e. the number of accidents (ignition by an electric heater for home-use equipment (Home heater lamp)) is, "quantity 600 '06, quantity 500 '07, quantity 400 '08, quantity 400 '09." That is, bottoming out state (reduction is saturated.).

Ratio of the electrical heater in fire accident was about 60%: Failure of temperature control, about 14%: Failure of electrical circuits (for example, short) 26%, Other: some (such as unknown).

Number of ignition accidents has not decreased as shown in Figure 1.2.

Figure 1.1. Home Fires Involving Heating Equipment, 1980-2009, by Year

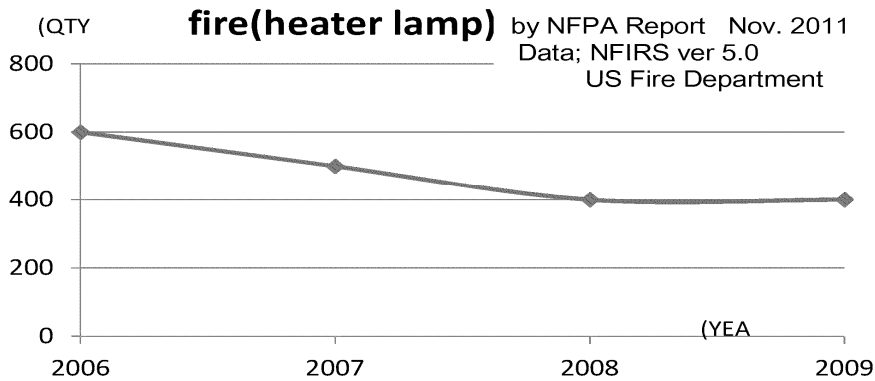
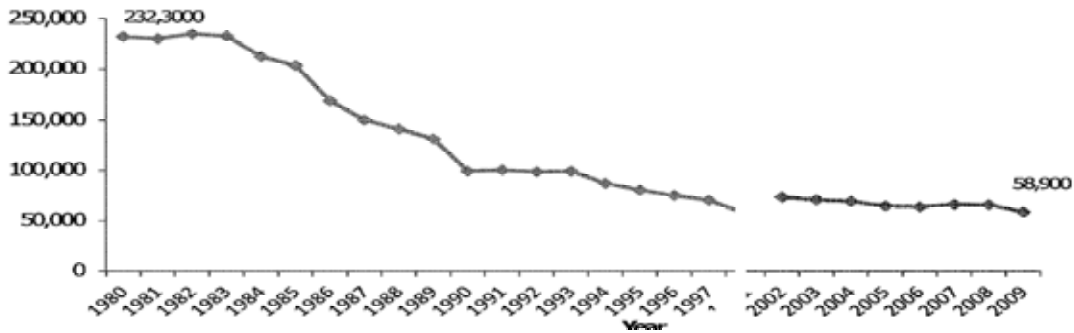


Fig. 1.2 Home heater lamp accidents by NFA Report Nov.2011

2. The Cause for the number of ignition is not reduced

The structure of an ordinary electric heater is shown in Fig. 2.1 (Block Diagram). Failure to open by thermal welding of the contacts (thermal fuse and thermostat) will occur in overheat protection device, which causes continuously energize state, deviation from the control normal, abnormal heating of the heater and so on. This situation is a failure to danger. In addition, electric heaters in the market today, the product was not equipped with fail-safe systems.

In safety of an electric heater in the ordinary system, there are two problems. In the worst case after the following, an ordinary heater will be continuously energized state, deviate from the normal control, and anomalous heating of the heater.

And ignition of an internal heater (and if this situation continues, from this state later to ignition)

- An ordinary heater does not have the ability to detect that the overheat protection device has failed.

Overheat protection device (thermostat, thermal fuse) becomes a failure of short-circuit conditions. The device does not detect by itself that it has failed. That is, only in accordance with the reliability of parts, failure to become dangerous. And ignition of an internal heater and continue from this state, further, and firing.

- An ordinary heater does not have the ability to shut off power when there is a failure in overheat protection device. When power feed element (triac, diode) fails, and overheat protection device (thermostat, thermal fuse) is short-circuited state, power cannot be turned off. Because there is no ability to detect that the overheat protection device fails, the device was not found to be defective. Currently, the use of highly reliable parts, reduce the failure of the components themselves, have made high reliability of the heater. Finally, it becomes a failure to danger. Equipment is not fail-safe systems (i.e. system which fails in the safe side only). The authors consider that the reason why number of accidents caused by fire is not reduced. There is a limit. As shown in Figure 2, in the circuit configuration of the current electric heater, if both (power element and overheat prevention device) has failed, electrical contacts is welded while it is energized and after the contact is welded it does not open even if

temperature reached to a predetermined temperature . Therefore, it is a dangerous failure that cannot be shut off power.

Electric power supply control element is a triac and diodes. Overheat protection device is a thermostat and thermal fuse.

2.1 Accident sample (Recall product)

Examples of the accidents and recalled products are shown in Table 1 and Photo 1. Photo 1 shows the RECALL product in US on 16th Feb. 2011 by Consumer Product Safety Commission (See Table 1 Recalls III). And Fig. 2.1 is Electric Heater's Block Diagram. This Block Diagram corresponds to CASE , , on Table 1 Recalls.



Photo 1 RECALL product in US

Photo 1 shows the RECALL product in US on 16th Feb. 2011 by Consumer Product Safety Commission on Table 1 Recalls .

Fig. 2.1 is Electric Heater Block Diagram. This Block Diagram shows CASE , , and on Table 1 Recalls.

Table 1 Recalls
(home heater lamp)

	Area	No.	Data	Product name	root cause
I [2]	CANADA Consumer Product Safety	RCL 12-26	May 1 2012	1500W LOW profile baseboard heater	Overheating poor electric connection
II [3]	UK Product safety and recalls in the European Union	RAPEX Ref. No. 1444/11	Dec. 23 2011	Electric heater Intertek 3113596	Overheating poor electric connection
III [4]	US Consumer Product Safety Commission	Release #11-130	Feb. 16 2011	TrueLiving Heater FAN Portable Quarts Radiant Heater	Overheating heater's plug, melting plastic casing

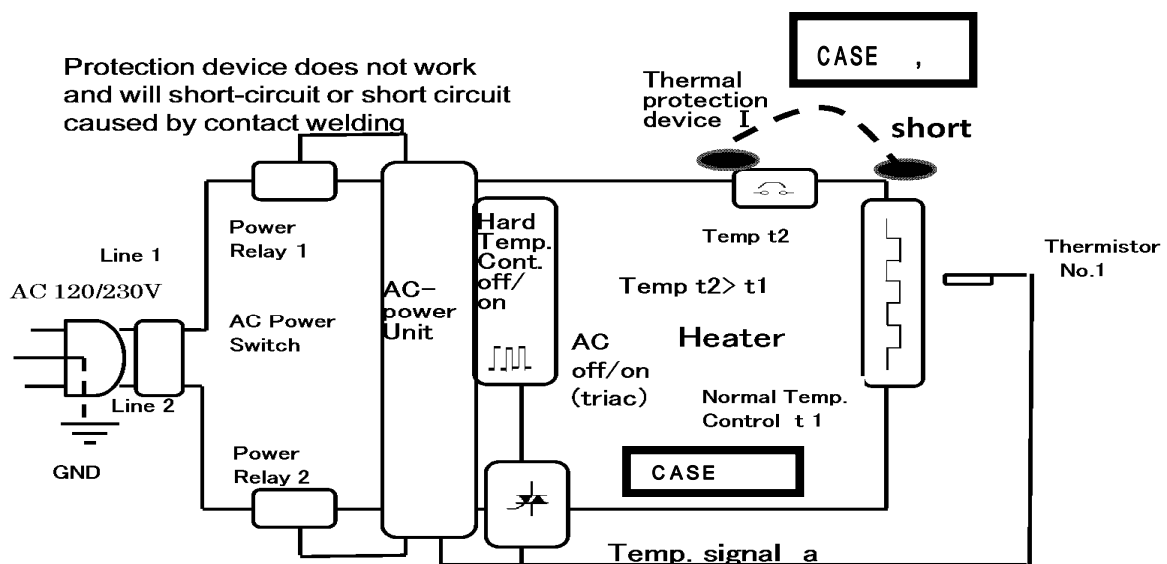


Fig. 2.1 Electric Heater Block Diagram (Currently)

3. Theory

EN standard “EN 764:2007 Pressure equipment - part 7: Safety systems for unfired pressure equipment” describes on the safety of pressure equipment. This standard declares that the mechanical structure is important. It requires control system adjustment, monitoring systems, safety systems are equipment in order to ensure safety by three-layer safety control architecture.

The safety system for pressure equipment system was established. In this paper, the authors tried to apply its concept to the electric heater.^[5] Then, the additional parts were added to improve safety. In the mechanism, shown in Figure 2, which shows safety protection against over-pressure, consist of three steps: regulating systems, monitoring systems, and safety systems.

3.1 Regulating systems

As shown in Figure 2, Regulating systems keep the pressure within the limits prescribed as normal operation. This system can controlled pressure within the appropriate pressure range, which is also to ensure the safety function simultaneously. This function is due to normal operation reliability; check the pressure value automatically, to maintain operation within the permissible limit value (maximum / minimum).

3.2 Monitoring system

When monitoring system, as shown in Figure 2, confirms the pressure system in normal condition by the pressure value, and when it detects pressure to exceed the limits of normal operation, then it releases the internal content to drop pressure and then stops the system. (And it also stops the pressure source if necessary.)

For restart after the cause of the overpressure is clarified, an ordinal startup procedure is required.

This function, using the pressure switch, is based on reliability.

Automatic restart is not permitted. Operation, a manual reset by the user, can be allowed. This system is shut down due to pressure switch when the pressure exceeds the maximum allowable limit.

3.3 Safety systems

Monitoring system has been secured by reliability. Therefore, when the pressure equipment has failed, that the monitoring system does not work, and it might be occurred even with low probability. Therefore, the safety system is necessary as the last protective layer, which intentionally installing consist pressure relief devices. Pressure release device does not have “failure to danger” mode. For this reason, the safety system is fail-safe structure based on physical characteristics.

Pressure release device is e.g. safety valve or rupture disk. These are not failure to danger, i.e. failure is the only safe side. This is a fail-safe condition. The reason is because it is in accordance with physical principles. Physical principles means the disk-shaped thin film is broken by a certain pressure and the spring force is limited determined by its dimensions. Therefore, when the pressure is larger than the specified force and release the pressure.

However, when it works, replacement of the safety valve or rupture disk is required.

Therefore, there is a safety system, in order to relieve pressure reliably in accordance with physical principle, that is not failure to danger, and (fail safe) only failure to safe. The safety system in the third layer will be fail-safe, and safety is ensured deterministically.

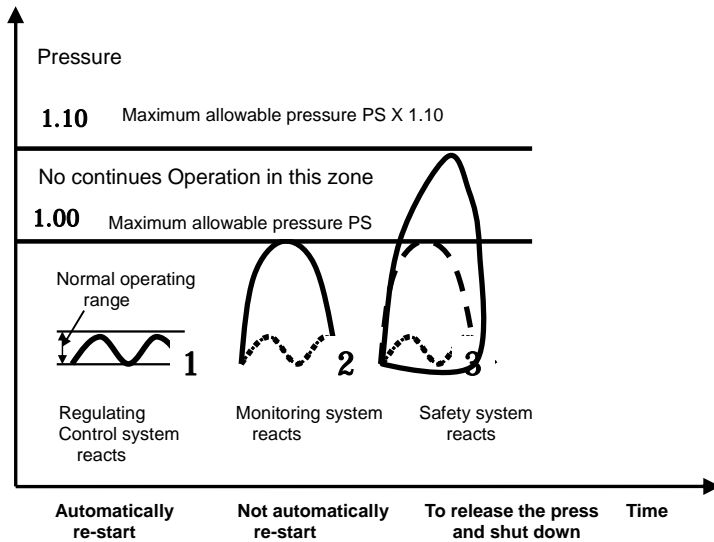


Fig.3 Response of regulating, monitoring and safety systems in relation to PS

4. The current problem and improvement

In EN764-7, the pressure release device to configure a safety system is a fail-safe. This is deterministic. On the other hand, the thermal system, there is no fail-safe. If the temperature sensor has failed, fail-safe is not guaranteed.

By using reliable parts, electric heater has made to reduce the failure of the component itself, and increase the reliability of the heater.

Here, there is a difference between system on pressure and on thermal system. In an electric heater for safety systems, in order to provide a fail-safe, there is a limit (the requirements of the standard EN764-7). To realize the fail-safe condition, several additional measures are required.

4.1 One fail

In ordinal heater, the hard circuit is available for single failure. However, if there are multiple cause failures, and the failure was beyond the expectations of designers, only the corresponding single failure, the hardware circuit, can support it. An ordinary heater cannot support the combined failure. Failure resulting from the complex factors is the failure by overlapping two or more factors.

Example: Complex factors are failure of triac and failure of overheat protection device (heater is installed near the wall (as a result, the heater is under the influence of radiant heat), cannot shut off power because of welding of the thermostat contacts inside.).

Ordinal heater supports to single failure. When 2 failures occur, the safety device cannot shut off power. For this reason, an insulating material such as plastic melts and the temperature of the heater goes to out of control, and overheating proceeds begin and expand to ignite at ignite parts, and to fire from the heater. So, in order to improve this, it is necessary to support a combined failure.

4.2 The combined fail

To avoid the accident, the following measure is necessary.

- Overheat protection device can operate in other failure.

The temperature of the heater has been rising.

- The hard circuit detects that the device was not able to shut off power.

And it is hard circuit to check the temperature.

- (Check the margin) to check the temperature of up to work the next overheat protection device

If one sensor fails, the temperature sensing circuit is impossible.

In addition, in multiple sensor system of the same type, there might be expected common failure; there is a need to use different kinds of sensors.

Therefore, it is necessary to install redundancy and diversity in hardware circuit.

. 4.3 To respond temperature quickly change

The ordinal circuit hardware was not able to respond quickly to changes in sudden temperature. Therefore, in order to improve this, temperature measurement by in the analog signal continuously is prepared and the system detect the measured temperature exceeds limit, the system cut off the power.

Then, it is necessary to monitor the temperature before and after the operating temperature exceeds the threshold temperature in order to avoid overheat device.

For defense ageist the CPU failure, the hardware circuit must be separated from the CPU, which continuity monitored temperature.

Hardware circuit to ensure that the temperature difference is within the designed range should be prepared. If the measured temperatures are different from each other, the hardware circuit determines that the system is in deviation from the normal condition. The temperature difference is between the operating temperature of the heat source and measured temperature by overheating protector.

4.4 Over heat protection device

Over-heat protection device cannot cut off power supply when the contact is welded.

Therefore to monitor the status of the overheat protection device is necessary based on the following reasons:

- To know that the temperature has reached at which the contact opens.
- To know that the contact is actually opened.
- To know that the temperature of the heater are turned down by the cut-off of power supply.

5. New fail safe system for electric heater

There isn't fail-safe device for thermal system. On the ordinal hardware of heater, the fail-safe system cannot be configured. To improve this situation, the authors propose the new fail-safe configuration: The configuration is based on redundancy and diversity constructed by multiple devices.

By the hardware, circuit configured with the redundancy and diversity, its failure can detect before it becomes dangerous failure, and power to heater is cut off. In this paper, we proposed a system in order to avoid this dangerous failure, and concentrated to the only safe failure.

6. Conclusion

1. The philosophy of this paper meets to ISO / IEC Guide 51. Also, there is a difference between the pressure and thermal system. But, the proposed electric heater has safety system based on architecture for safety of pressure equipment - EN764-7: 2007.
2. In this paper, by implementing diversity and redundancy into an electric heater to establish fail-safe system, When the temperature sensor and overheat protection device fails, then power is shut off. By this, failure to danger is eliminated. In this paper, we show solutions theoretically to avoid fire from electric heater.

References

- [1] NFPA , Fire Analysis and Research Division, Home Fire Involving Heating Equipment Report, November John R, Hall, Jr. issued.
- [2] Consumer Product Recalls-Consumer Product Safety, CANADA Recall Notice, May 1, 2012 RCL 12-26, Low Profile Baseboard Heater
- [3] Unsafe Products, Product safety and recalls in the European Union, United Kingdom December 23 2011, PAPEX Reference no. 1444/11
- [4] U.S. Consumer Product Safety Commission, NEWS from CPSC, February 16 2011, Release #11-130
- [5] Akira Matsuura, Takabumi Fukuda " Reliability Engineering Association of Japan "The concept for to avoid the risk of ignition by thermal energy hazard" 2011, 17th Spring Symposium REAJ

SIAS
2012

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



SESSION 5

ROBOTS SAFETY

Industrial Robotic: Accident analysis and Human-Robot Coactivity

Philippe CHARPENTIER, Adel SGHAIER
Institut National de Recherche et de Sécurité (INRS)
1 rue du Morvan - CS 60027
F-54519 VANDOEUVRE cedex
philippe.charpentier@inrs.fr, adel.sghaier@inrs.fr

Keywords: robotics, collaborative robot, gesture assistance robot

ABSTRACT

Robotics technology has experienced rapid growth in recent years and applications involving robots are more and more varied. Physical barriers between man and robot are tending to disappear, that cause the emergence of new problems associated with safety and accident prevention.

This paper firstly presents the results of an INRS accidentology study relating to the use of industrial robots in France. The study covers the 1997-2010 period and is based on accidents recorded on the EPICEA database. It provides information on the conditions under which accidents occur and on their main causes. Contrary to preconceived ideas, its demonstrates, for example, that robot-related accidents occur more frequently in operational phases than in maintenance phases (cleaning, repair).

This accidentology presentation will be followed by a discussion of man-robot coactivity in current industrial applications. Many of today's robots tend to be cooperative and are designed to interact with man in a shared workspace, in which the robot and the human can perform tasks simultaneously. The main characteristics that make this coactivity possible are listed and problems inherent to personal health and safety are described.

1 ACCIDENTOLOGY

INRS has conducted an accidentology study of accidents associated with the use of robots in an industrial environment: 31 accidents listed on the EPICEA1 database, which occurred during the 1997 – 2010 period, were analysed [1]. These accidents occurred on “conventional” robotic installations, on which access to the robot's workspace in operational mode was prohibited by adequate protective measures.

We retained the following information from the recorded data for each of the 31 studied accidents.

Activity phase

The first idea that springs to mind, when considering the robot usage in an industrial environment, is that they do not raise safety problems when in operation since protectors or protective measures prohibit operators from entering the area, in which the robot moves when it is operating. Accident analysis shows that this idea is utterly unfounded. Figure 1 in fact shows that a significant proportion of accidents occur during the operational phase.

¹ EPICEA is a French national, anonymous database containing more than 17,000 cases of occupational accidents sustained by employees covered by the general social security system. These accidents are fatal, serious or significant in to prevention. The EPICEA database is not exhaustive since not all occupational accidents are listed on it. Its aim is to reveal the causes and sequence of events underlying accidents of a given type.

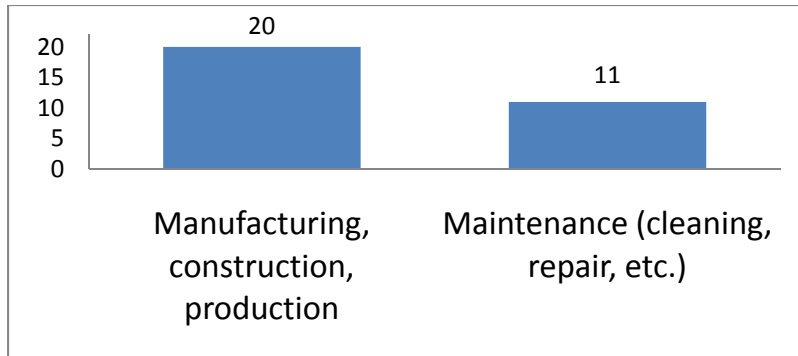


Figure 1. Accidents per activity phase

These operational phase accidents often occur because safety systems are inexistent, improperly installed or bypassed because they are unsuited to the task to be performed by the operator. For example, this was the case in the following accident: *The victim alerted his supervisor of a fault at his automatic welding station. He went to the station with his supervisor to solve the problem. The supervisor left to collect the keys allowing access via maintenance door. The victim slips into the robot area via the loading station. The operating cycle is still automatic; the robot head starts moving and, for an as yet unknown reason, fatally crushes the victim.*

Accident seriousness

As Figure 2 illustrates, accidents associated with robot usage are often serious. The reports recorded on the EPICEA database reveal the very serious nature of robot-related accidents.

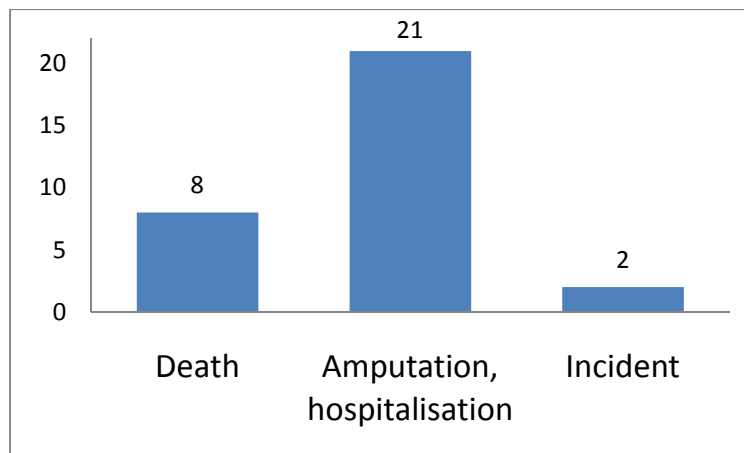


Figure 2. Accident seriousness

It is a fact that the EPICEA database mainly lists serious accidents, but it is important to stress that impact, crushing, etc. between robot and man do indeed cause major traumas that may even result in death of those involved.

Injury localization

There is a wide variety of injury localizations. We observe that every part of the body can be affected with a prevalence of the trunk and head. In many cases, several parts of the body are affected, especially in relation to crushing.

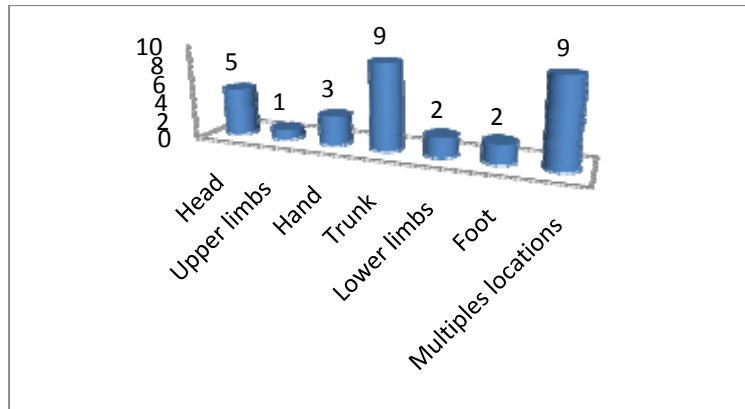


Figure 3. Injury localizations

Note. The categories “upper limbs” and “lower limbs” exclude hands and feet respectively; these extremities fall within specific categories.

Protectors installed

In most cases, access to the movement area of robots involved in the accidents listed on the EPICEA database was prevented by a protector or a protective device. We note that fixed or moving physical protectors prevail, while sensitive devices are little used. Configurations listed in the “No protector” category are those in which hazardous area protection was incomplete, leaving sufficient passages for operators to be exposed to risks.

The “Other safety device” category includes guard rail- or emergency stop-type measures, although an emergency stop cannot really be considered as a protector (EPICEA database terminology differing from that described in Standard ISO 12100).

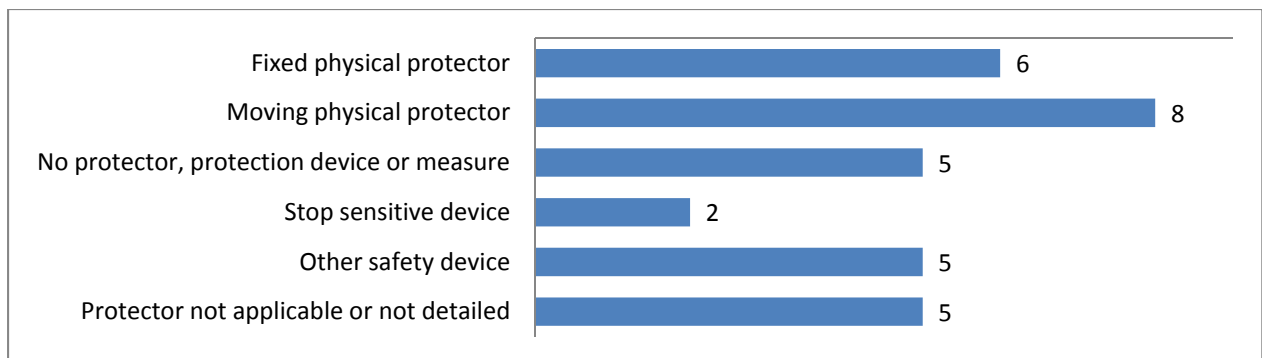


Figure 4. Installed protectors

Causes of protection system non-operation

Operator presence in the robot hazardous area most often results from incapacity of the implemented protectors and protection systems to fulfil their function.

The main cause of failure does not call into question the protector operation itself, but rather the usage to which it has been put: protectors are therefore frequently disabled, either temporarily or permanently. Protector disabling is usually due to improper design of the safety: this has not taken into account every installation operating mode, especially in non-operational mode phases such as maintenance or failure diagnosis. This results in inadequacy of the protector or protection system with respect to the task to be performed.

The following example is representative of protector disablement: *The company has just acquired two production systems for manufacturing plastic cutlery, each composed of a press and a manipulator robot, which transfers the moulded items to a small polystyrene box. Machine setting is difficult mainly because of production item shape and installation production rate, which has to be high to remain competitive. When the robot fails, the operator has to*

walk around the press to repair the robot. He then has to return to the operating console to restart the press because, during the robot repair operation, he manoeuvres a casing which sets the press in a non-operating position. The victim, a 29-year-old shift supervisor, had disabled the contactor. When the accident occurred, the operator observed that the press had stopped. He called the supervisor, who introduced his head and shoulders into the robot to observe the malfunction. He must have moved a small box, when the robot moved back towards him, striking his head fatally against the machine upright.

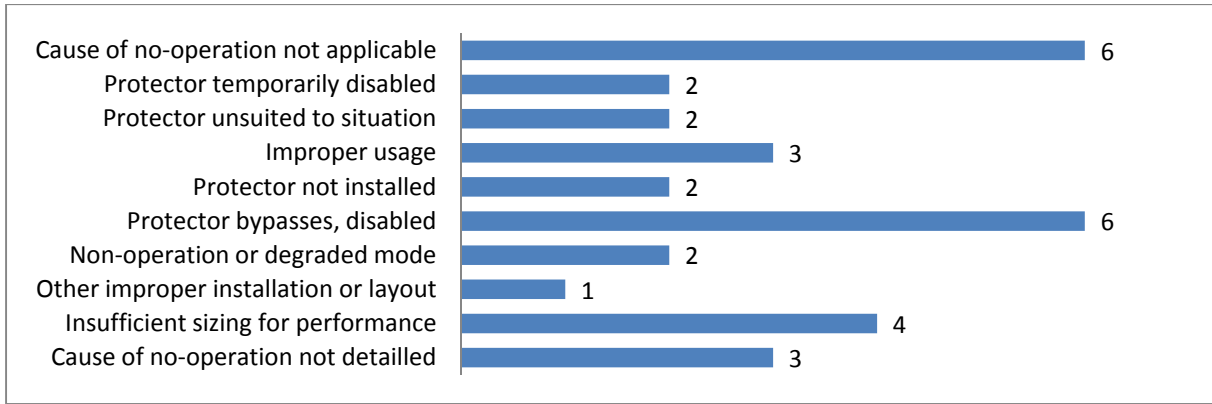


Figure 5. Cause of protector non-operation

2 MAN-ROBOT COLLABORATION

Technological advances

While most often involving robots isolated from operators by physical barriers, experience feedback described in the sub-section above clearly shows that a robot can create mechanical risks potentially leading to serious accidents. Even greater vigilance is therefore required, when physical barriers happen to be removed.

Protection removal is made possible by a number of recent technological advances, for example the design of robot moving parts and their control systems or the new electro-sensitive protective devices.

Favoured by newly published standards, especially Standard EN ISO 10218 (Parts 1 and 2) [2], these advances allow, for example, to:

- Design new collaborative working configurations such as robot loading or unloading of tools or other loads in common working areas with the robot still energized,
- Replace existing physical stops by software safe space and axes, enabling easy programming of a safe working area,
- Control safe low speeds and monitored stops with the robot still energized, but locked. This characteristic facilitates restarting after a collaborative task, shortening delays due to Category 0 stoppages.

Cooperative robots

These advances enable us to envisage cooperative working areas, within which robot and human can fulfil tasks simultaneously in production operating mode. There is no longer any physical separation between the robot's and the operator's workspace and the operator can, under certain conditions, access this so-called collaborative workspace, for example to undertake robot loading/unloading of tools or other loads. In most cases, the robot speed will depend on the operator's position with respect to this collaborative working area. Currently commercialised robots (see Figure 6) are capable of guaranteeing:

- Category 2 safe stop, while maintaining actuator power supply,
- Safe limitation of robot workspace,
- Safe limitation of robot speed.

Different technologies can be applied to detect the operator's position with respect to this workspace, such as laser scanners, sensitive mats or vision-based systems.

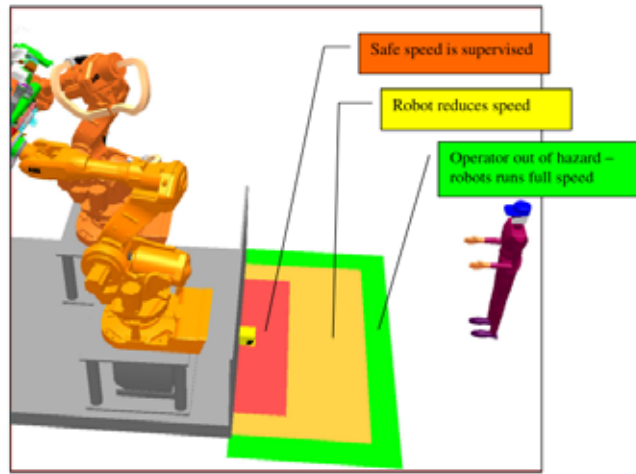


Figure 6. Example of collaborative robotised cell (ABB) configuration [3]

Gesture assistance robots

The technological advances listed above also allow us to envisage operator assistance robotics. For example, this is the case of the COBOT (contraction of the term "Collaborative Robot").



Figure 7. Example of gesture assistance robot – RB3D's Cobot [4]

This type of equipment assists the working man in industrial tasks, in which a force has to be exerted during operations such as sanding, grinding or handling. The operator therefore continuously operates/controls this tool, using an intuitive control system, to relieve himself of force exertion in his task. The user can concentrate on controlling the work to be performed and his chances of being exposed to MSD risks are reduced.

In the future, more consequential (e.g. exoskeleton-type) aids should arrive on the market.

3 POTENTIAL HEALTH AND SAFETY PROBLEMS

If we consider that robots placed on the market possess safe performance levels allowing them to be integrated into industrial applications, we still need to consider their implementation-related safety aspects.

In common with every machine, proper integration of these equipments for example into the assembly lines, requires preliminary risk assessment of the entire installation in its industrial environment. Given the absence of

physical barriers between the operator and the robot working area, it will be necessary to ensure, for example, that there are no:

- Mechanical risks, e.g. of wedging between a robot moving part and the body of the operator or a third party,
- Processed material- or product-related risks in relation which separation (in some cases inexistent) could prove to be a cause of danger.

Proper implementation of personal detection systems used to warn the robot of operator presence near its movement area and correct programming of both robot movements and software safety systems must also be ensured.

Concerning man-robot collaboration and more specifically collaboration created by gesture assistance robots, further issues are raised in relation to the health of operators involved. In particular, care should be taken to deal with potential problems associated with:

- Musculo-skeletal disorders:
Promoters of gesture assistance robots direct part of their communication towards MSD reduction. Again, we need to ensure that resorting to such equipment does not cause other assistance-related MSDs.
- Acceptability/Cognitive, psycho-affective consequences and chronic stress:
Man is led to work coactively with the robot, so issues may arise involving : some people's apprehension confronting a machine (may be - or not - curtailed by resorting to humanoid robots), dependence on technology to perform a task, fear of losing one's bearings and technical skills, user's feeling of diminished autonomy, stigmatisation and curtailment of capacities, etc.
Assistance applications must be accepted by the profession, employers and unions. Possible blockages may include considerations of not only an economic, but also an ethical, order such as fear of "robotising" the working man or keeping man at his work at all costs, irrespective of other considerations.
- Mental stress:
Robot design must ensure no increase in user mental stress compared with the work situation without a robot.

4 REFERENCES

1. Sghaier A., Charpentier P., *La problématique de l'utilisation des robots industriels en matière de sécurité*, Réalités industrielles, February 2012, pp. 24-31.
2. EN ISO 10218, *Robots et dispositifs robotiques - Exigences de sécurité pour les robots industriels - Partie 1*, 56 p. & *partie 2*, 106 p., 2011.
3. Behnisch K., *Safe collaboration with ABB robots, Electronic Position Switch and SafeMove*, ABB robotics, 2008. Available at :
[http://www05.abb.com/global/scot/scot241.nsf/veritydisplay/46e5494b3e5f9da6c12574e1003eb5be/\\$file/6904%20rop%20white%20paper%20safemove.pdf](http://www05.abb.com/global/scot/scot241.nsf/veritydisplay/46e5494b3e5f9da6c12574e1003eb5be/$file/6904%20rop%20white%20paper%20safemove.pdf)
4. <http://www.rb3d.com/fr/les-cobots>

Risk assessment and investigation of change from pressure feeling to pain

Matthias Umbreit, Berufsgenossenschaft Holz und Metall

The unusual term “kollaborierende” Roboter originates from the English term “collaborative” - which means cooperating. This kind of robot was initially called “assisting robot” in Germany. With the adoption of the international standard series ISO 10218 within the German body of standards, the new term had to be adopted as well.

Collaborative robots are designed for co-operation between human beings and robots. Up to now, industrial robots are only used in applications where the work process allows of a completely automatic configuration. Protective fences prevent access to the workspaces since motions presented by robots can lead to serious injuries. Workplaces requiring intervention of persons shall be separated from automated production areas (Fig.1).

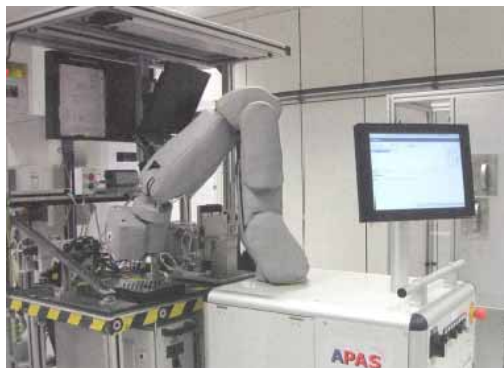


Fig. 1: Collaborative robot with test certificate. The robot is equipped with a force/pressure limitation at the tool and a “sensor skin” at the arms (Source Bosch)

On the one hand, this obstructs the progressing automation with a concomitant increase of productivity and product quality. However, it also means that for a certain part non-ergonomic tasks cannot be performed by machines. What is new now is that workplaces with collaborative robots are neither pure robot workplaces nor pure manual workplaces; but each one performs the tasks he/it can do best: the robot performs the tasks requiring speed, power, endurance and the human makes use of his special sensory and motor abilities.

Safe control systems

Why do those workplaces come only now? This is mainly due to modern control technology since collaborative robots must be provided with so-called safely monitored control systems. It is only possible by means of new efficient micro controllers to provide such control systems. They permit for instance the safe restriction of the robot working range, safe speed monitoring or keeping a certain position. The control systems shall at least meet the requirements of EN ISO 13949-1, category 3, PL d. This requires amongst other things a two-channel (redundant) control layout.

Basically, a distinction can be made between two principles of collaborative robots:

- Robots which have to slow down or come to a stop due to missing power and/or pressure limiting on approach.
 - These are, e. g.: safeguards which prevent the approach of a person to the hazardous robot movement. The safeguards are e. g. vision panels in traditional safety fences, in which parts of the production are presented to an employee for manual and / or haptic inspection. The vision panel by its dimensions permits an intervention with arms and hands only. Whole body access to the robot's workspace is prevented by the safeguards. During intervention, the movements of the robot including the tool are monitored by the safe control system.
 - Safeguards which detect the approach of a person and slow down or stop the robot movement, depending on the distance of the person. This can be achieved, e. g. by camera systems that transmit the position of the person entering the protective field to the safely monitored control system.

- Hand-guided robots:

They dispose of safe control elements, e. g. joy stick and enabling devices by means of which the robot can be moved at a safely limited speed.

Those semi-collaborative robots have in common that a collision between human and robot must be prevented by safeguards or by manual stopping.

- Power-limited and / or pressure-limited robots:
Those robots work without the traditional safeguards. They have been provided with design features which ensure that in case of a collision between a human and robot a specific power and pressure limit the human body is exposed to is not exceeded (biomechanical limit values).

There exist no usable biomechanical limit values in regulations and standards so far.

This is the reason for a research project at the University of Mainz (Germany) which is supported by the German Social Accident Insurance. In the project, the power and pressure limits are investigated a human body may be exposed to in case of collision between a human and a robot. The first results of a literature study which has been carried out by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) are summarized in table 1.

However, the robot application has to be configured in such a way that in the intended use no collision between human and robot can occur. The limit values indicated in the table below apply to the case when an unintended intervention of an employee takes place due to an unforeseeable malfunction. In this case, the machine has to be designed that way that at worst there occur effects to the skin or the tissue beneath, this means no deep penetration of the skin and the tissue. Fractures, bleeding wounds or other damages to the musculoskeletal system must be excluded.

Furthermore, it is important that the human is healthy enough for the teamwork with the robot, i. e. stress resistant. This ability is subject to regular checks by the employer in the scope of his duty of care.

Main body regions of the body model	Individual body regions	Limit values			CC [N/mm]
		CSF [N]	IMF [N]	PSP [N/cm]	
1. Head with neck	1.1 Skull/Forehead	130	175	30	150
	1.2 Face	65	90	20	75
	1.3 Neck (sides/neck)	145	190	50	50
	1.4 Neck (front/larynx)	35	35	10	10
2. Trunk	2.1 Back/Shoulders	210	250	70	35
	2.2 Chest	140	210	45	25
	2.3 Belly	110	160	35	10
	2.4 Pelvis	180	250	75	25
	2.5 Buttocks	210	250	80	15
3. Upper extremities	3.1 Upper Arm/Elbow joint	150	190	50	30
	3.2 Lower arm/Hand joint	160	220	50	40
	3.3 Hand/Finger	135	180	60	75
4. Lower extremities	4.1 Thigh/Knee	220	250	80	50
	4.2 Lower leg	140	170	45	60
	4.3 Feet/Toes/Joint	125	160	45	75

Table 1: Limit values for clamping/squeezing force (CSF), impact force (IMF), pressure/surface pressing (PSP), compression constant (CC) (Source IFA)

CE mark

If collaborative robots are applied in companies, attention should always be given to the GS mark, since according to the Machinery Directive, a collaborating robot is a machine like any other. Care has to be taken as well that in the scope of the risk assessment, the work environment, i. e. the robot tools and devices are included as well. Reason: As long as protective fences were present the CE mark comprising area was obvious. If there is no protective fence it may be necessary to look twice to realize the machine associated elements. The risk assessment and the instruction manual are documents which are stipulated by legislature for each machine.

Well-known companies of collaborative robots have their product additionally tested on compliance by an independent testing body. Especially the resulting certificate creates confidence in such a new and complex technology. For such a kind of certification, it is important to have the robots tested in a suitable and typical application. That's the only way to examine whether the above mentioned limit values are kept under conditions of practice (see fig. 1).

The technical requirements for industrial robots including collaborative robots have been defined in two international standards: EN ISO 10218-1 and EN ISO 10218-2. They are also intended to accomplish the Machinery Directive, i. e. they have the "presumption of conformity" status. However, the requirements for power / pressure-limited robots are not yet fully described in these standards. The results of the above mentioned research will be incorporated in the technical specification ISO/TS 15066 for the time being. Its publication is expected for 2014. As soon as the research is completed, an adoption of the specification ISO/TS 15066 in the standard series EN ISO 10218 is intended.

For non-industrial robots, e. g. service robots, international and Europeans standards are in preparation as well.

Dr. Matthias Umbreit
Berufsgenossenschaft Holz und Metall
Wilhelm-Theodor-Römheld-Str. 15
55130 Mainz

Evaluation of Injury Level and Probability for Risk Assessment of Mobile Robots

Tatsuo Fujikawa and Masami Kubota

Japan Automobile Research Institute (JARI), 2530 Karima, Tsukuba, Ibaraki, 305-0822, Japan
E-mail: ftatsuo@jari.or.jp

Yoji Yamada

Nagoya University, Aichi, Japan

Hiroyasu Ikeda

National Institute of Occupational Safety and Health, Japan (JNIOSH), Tokyo, Japan

KEY WORDS: Robot, Collision, Severity, Probability, Validation

ABSTRACT

To introduce mobile robots into human-robot collaborative environments, risk assessment should be performed considering the risks of collisions. This paper proposes a method of estimating the severity of harm (injury level) and the injury probability for the risk assessment and the collision test method for validation. We first propose using injury data from automobile accidents by expressing the data as the probability of injury, since the results of the collision vary, depending on human body properties and other fluctuating factors. The probability of each injury level is a function of mechanical parameters that are applied to the human body on collision. Second, we propose a test method using automotive crash-test dummies to validate the risk level estimated in the risk assessment.

1 INTRODUCTION

To introduce mobile robots into human-robot collaborative environments, risk assessment should be performed considering the risks of collisions. This paper proposes a method of estimating the severity of harm (injury level) and the injury probability for the risk assessment and the collision test method for validation. We first discuss human injuries (e.g., head, chest, and pelvis injuries) due to collisions with robots. The injury level in collisions with mobile robots is difficult to estimate because of the lack of accident data. Therefore, we explore injury data from automobile accidents. Using this data, we develop a method of risk assessment considering injury level and probability. Second, we discuss a method to validate the risk level estimated in the risk assessment. Numerical simulations and representation tests are possible methods of validation but simulations are unsuitable for validation at this stage of simulation method development. Therefore, we developed test methods that represent typical collisions between humans and robots.

2. LEVEL OF INJURY

The level of injury in collisions with mobile robots is difficult to estimate because of the lack of accident data, so we use data obtained in automotive fields. Automotive safety regulations focus mainly on injuries with severity higher (AIS 3, 4, and 5) than we consider in robotic fields (AIS 1 or 2), but automobile accident researchers have reported data of AIS 1 or 2. The following examples, which involve injuries of children, may be used to introduce mobile robots into non-industrial environments.

The National Highway Traffic Safety Administration [1] reported on formulas for injury probabilities as

functions of mechanical parameters that are applied to the bodies of one-year-old, three-year-old and six-year-old children as well as adults. They derived the formulas based on accumulated injury data and techniques for analysis reported in previous research. The effects of age variation are introduced into the formulas using a scaling ratio determined by the size and mechanical properties of body parts.

They derived formulas for head injury probability at AIS 2+ and AIS 3+. The head injury probability formulas for six-year-old children are [1]

$$P_{Head2+} = [1/\{1 + \exp(2.49 + 140/HIC_{15} - 0.00690 * HIC_{15})\}] \times 100\% \quad \text{and} \quad (1)$$

$$P_{Head3+} = [1/\{1 + \exp(3.39 + 140/HIC_{15} - 0.00531 * HIC_{15})\}] \times 100\% . \quad (2)$$

Here, P_{Head2+} is the probability of head injury at severity level AIS 2 or higher, and P_{Head3+} is that at AIS 3 or higher. HIC_{15} is the Head Injury Criteria defined [2] as

$$HIC_{15} = \left[\frac{1}{t_2 - t_1} \int_{t_1}^{t_2} a(t) dt \right]^{2.5} (t_2 - t_1), \quad (3)$$

where $a(t)$ is the head acceleration in g (acceleration of gravity), and t_1 and t_2 are times during the acceleration pulse with 15 ms intervals. They also provided probability values for specific levels of HIC_{15} for AIS 1, although they did not present a formula. For example, when $HIC_{15} = 300$, the probability of AIS1+ injury is 69% (Figure 1).

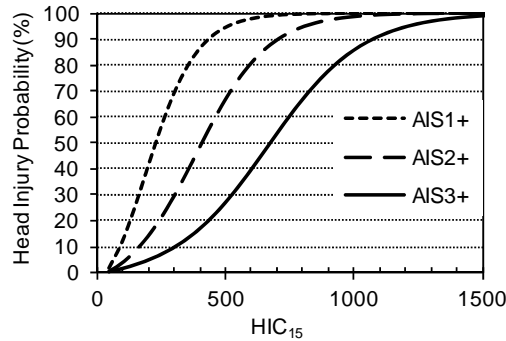


Figure 1 Head injury probability of six6-year-old child [1].

The formulas for neck injury probability at AIS 2+ and AIS 3+ for six-year-old children are [1]

$$P_{Neck2+} = [1/\{1 + \exp(2.0536 - 1.1955 * Nij)\}] \times 100\% \quad \text{and} \quad (4)$$

$$P_{Neck3+} = [1/\{1 + \exp(3.2270 - 1.9690 * Nij)\}] \times 100\% . \quad (5)$$

Here, P_{Neck2+} is the probability of neck injury of AIS 2 or greater, and P_{Neck3+} is the probability of neck injury of AIS 3 or greater. Nji is Neck Injury Criteria defined [2] as

$$Nij = \frac{F_z}{F_{zc}} + \frac{M_{ocy}}{M_{yc}} . \quad (6)$$

Here, F_z is the axial force in tension or compression, and F_{zc} is the critical intercept value of load used for normalization (i.e., $F_{zc} = 3096$ N in tension and 2800 N in compression), M_{ocy} is the occipital condyle bending moment in flexion or extension, and M_{yc} is the critical intercept value for moment used for normalization (i.e., $M_{zc} = 93$ Nm in flexion and 42 Nm in extension). The probabilities expressed by formulas (5) and (6) somehow contradict each other, as plotted on the left side of Figure 2. In the region where Nij exceeds 1.7, the probability of AIS 2+ is lower than that of AIS 3+, although it must be larger. Formulas for injury probability sometimes exhibit such contradictions since they are obtained by statistical processes. We need further analysis of the original data from which formulas (5) and (6) are derived.

The formulas for chest injury probability at AIS 2+ and AIS 3+ for six-year-old children are [1]

$$P_{Chest2+} = [1 / \{1 + \exp(1.8706 - 0.06991 * d)\}] \times 100\% \quad \text{and} \quad (7)$$

$$P_{Chest3+} = [1 / \{1 + \exp(3.7124 - 0.07481 * d)\}] \times 100\% . \quad (8)$$

Here, $P_{Chest2+}$ is the probability of chest injury of AIS 2 or greater, $P_{Chest3+}$ is that for AIS 3 or greater, and d is chest deflection (mm). The probabilities expressed by the formulas are plotted in the right side of Figure 2.

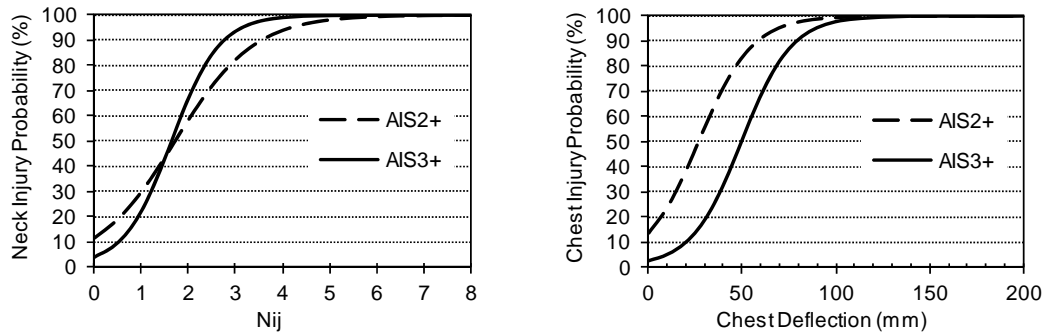


Figure 2 Injury probability of six-year-old child [1]. Left: neck injury. Right: chest injury.

3 RISK ASSESSMENT

As mentioned above, the injury level is provided as injury probability. We propose to introduce this probability into the risk estimation, in addition to other parameters of probability (e.g., frequency and duration of exposure, probability of occurrence of a hazardous event, and probability of avoiding or limiting harm) (Figure 1). Introducing injury probability enables us to consider the fluctuating injury levels that vary depending on the unpredictable conditions of accidents.

In estimating risk, the mechanical parameters for collision of the robot are assumed based on measurements or data from former examples. The predicted parameters are introduced into the formulas for injury probability in order to calculate the potential injury level and injury probability. For example, when the assumed chest deflection is 20 mm, the probability of an AIS 2+ injury is 38% and that of an AIS 3+ injury is 10%. Injury at the AIS 2 level, which corresponds to fractures of two or more ribs, may not be acceptable unless the probability is extremely low. We also note that the probability of AIS3+ is not negligible here. These results mean that the frequency and duration of exposure and the probability of hazardous event occurrence should be kept low and the probability of avoiding or limiting harm should be kept high, and/or the robot design should be changed to decrease the chest deflection.

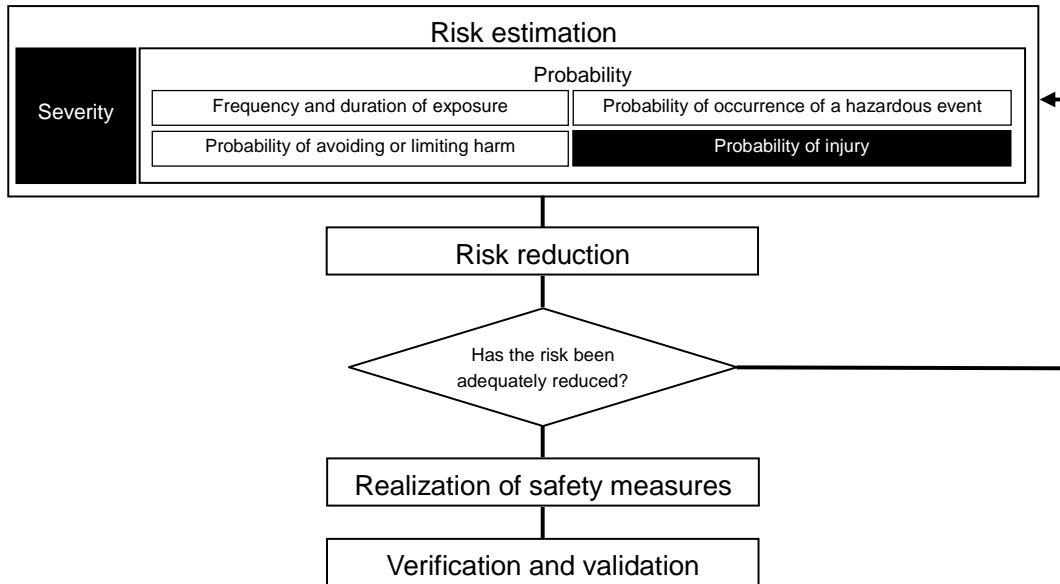


Figure 3 Flow of risk assessment, realization of safety measures, and validation.

4. VALIDATION METHODS

Methods are needed to validate the risk level estimated in the risk assessment. Several studies have attempted to establish methods to evaluate injury levels in accidents by numerical simulations or representation tests. Numerical simulations are useful for estimating the effects of robot design change but unsuitable for validation at this stage of simulation method development, since human body responses in collisions have not been modeled precisely enough. Therefore, we developed test methods that represent typical collisions between humans and robots.

4.1 Test Dummy

The tests require measuring systems that represent human body responses (e.g., acceleration and deflection) in collisions. We propose using automotive crash test dummies, since they are standardized to represent typical responses of human bodies and equipped with detectors for measuring responses during collision.

4.2 Test Procedures

We developed test procedures based on automotive crash test procedures. First, a dummy is placed in the path of a moving robot. Second, the robot tested is fixed to a steel wire that is driven by electric power. After the robot has reached the test speed, the robot is released from the wire. During the collision between the robot and the dummy, mechanical data from sensors installed in the dummy are recorded. The left of Figure 4 depicts the typical set-up of the test, which represents a collision between a child standing in front of a wall and a mobile robot.

Test conditions should represent the most serious cases assumed in the risk assessment. For example

- The test speeds should include the highest speed at which the safety control system fails.
- Dummy types should include the human classification that is most vulnerable to injury (e.g., a child dummy should be included if the robot is used in an environment with children).

Measured mechanical parameters are introduced into the formulas for injury probability in order to calculate potential injury levels and injury probabilities. The results are compared with the injury levels and the probabilities predicted during risk estimation in order to validate the results of the risk assessment.



Figure 4 Left: Collision between a child dummy in front of a wall and a moving object that represents a mobile robot with a steel structure. Right: Object that represents a mobile robot with an elastic polystyrene panel.

5. EXAMPLES OF TEST RESULTS

Figure 5 presents examples of head acceleration of a six-year-old dummy colliding with two kinds of moving objects that represent mobile robots. The dummy was crushed between the wall and the mobile robots. Collision with the robot with a steel structure (left side of Figure 4) at a velocity of 6 km/h resulted in $HIC_{15} = 323$ (left side of Figure 5). This corresponds to 75% probability of AIS 1+ injury and 33% probability of AIS 2+ injury, based on Figure 1 and Eq. (5). HIC_{15} decreases remarkably at a lower velocity of 2 km/h (center of Figure 5). We also tried to reduce HIC_{15} by covering the robot structure with an elastic polystyrene panel (right side of Figure 4). However, HIC_{15} was not reduced (right side of Figure 5).

Figure 6 presents examples of chest deflection. Collision with the robot with a steel structure at a velocity of 6 km/h resulted in $d = 10$ mm (left side of Figure 6). This corresponds to a 24% probability of AIS 2+ injury and a 5% probability of AIS 2+ injury, based on Eqs. (7) and (8). Deflection remarkably decreases at a lower velocity of 2 km/h (center of Figure 6). However, it was not reduced by covering the robot structure with an elastic polystyrene panel (right side of Figure 6).

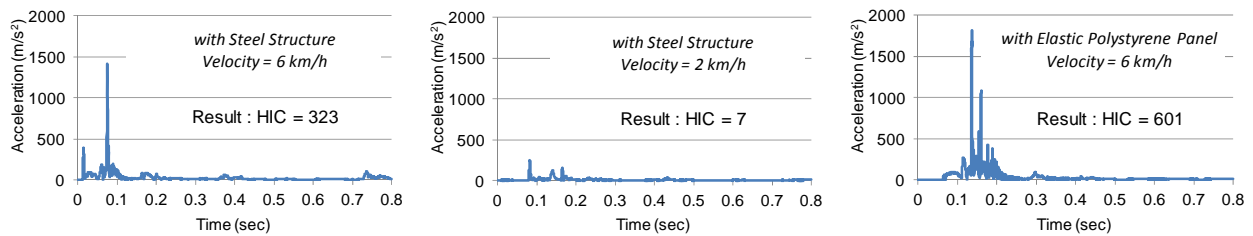


Figure 5 Head acceleration measured in collision between a six-year-old dummy in front of a wall and a mobile robot with a steel structure or an elastic polystyrene panel. Velocity, 2 or 6 km/h. Robot mass, 200 kg.

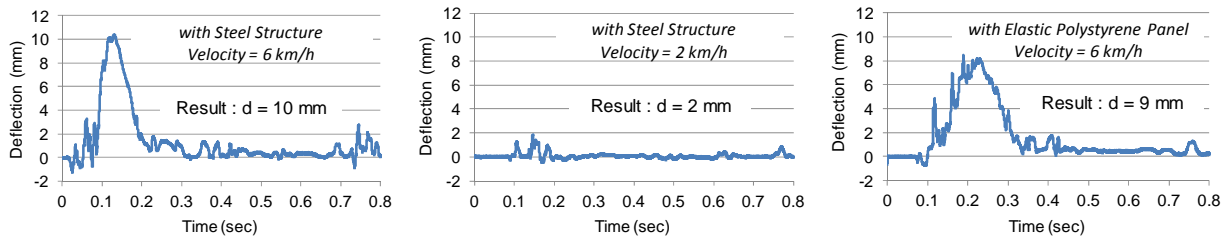


Figure 6 Chest deflection measured in collision between a six-year-old dummy in front of a wall and a mobile robot with a steel structure or an elastic polystyrene panel. Velocity, 2 or 6 km/h. Robot mass, 200 kg.

6. DISCUSSION

This study explored the injury data of automobile accidents. Most formulas for injury probability in the automotive field deal with injuries more severe than AIS 2, although some raw data for less severe injuries have been reported. These raw data should be studied to derive AIS 1 formulas suitable for risk estimation and validation in the robotic field.

This paper does not address injuries of the extremities because of lack of information. Arm injury was not the focus in automotive accidents until side-impact tests were introduced. Studies should be performed to summarize information on arm injuries by referring to data on side impacts. Leg injuries of automobile passengers differ from those of people who collide with mobile robots. The former have compression mode caused by steep deceleration during accidents, whereas the latter have bending mode caused by contact with part of the robot, which are similar to pedestrian accidents. Studies should be conducted using data from pedestrian accidents.

7. SUMMARY

We propose the following methods of risk assessment and validation on the safety of mobile robots.

- Use formulas for injury probability developed for automotive safety to estimate the severity of injury.
- Introduce injury probability into risk estimation. This enables us to consider the fluctuating severity of injury, which varies depending on unpredictable conditions of accidents.
- Conduct representative tests using automotive crash-test dummies for validation.
- The test conditions should represent the most serious cases assumed in the risk assessment; for example, test speeds should include the highest speed at safety related control system failure.

Further studies should address injury level AIS 1 and injuries of extremities.

8. ACKNOWLEDGEMENTS

This work is a part of “Project for practical applications of service robots” by New Energy and Industrial Technology Development Organization.

9. REFERENCES

1. National Highway Traffic Safety Administration, *Proposed Amendment to FMVSS No 213 Frontal Test Procedure*, U.S. Department of Transportation, 2002.
2. National Highway Traffic Safety Administration, *FMVSS 208 Occupant crash protection*.

Collaborative Robotics: Measuring Blunt Force Impacts on Humans

Joe Falco, Jeremy Marvel, Rick Norcross

joseph.falco@nist.gov, jeremy.marvel@nist.gov, richard.norcross@nist.gov

National Institute of Standards and technology (NIST)

100 Bureau Drive

Gaithersburg, MD 20899

KEY WORDS: collaborative, robot, safety, standards, injury

ABSTRACT

Robot manufacturers are developing a new generation of industrial robots that are designed to work in collaborative environments in close proximity to humans. In parallel, an international standards effort is developing a technical specification to support a new set of robot safety standards that include provisions for collaborative robot operation. As these two developments merge, industry needs measurements and test methods to determine if this new generation of robots conforms to the emerging collaborative robot safety standards. Furthermore, the standards effort is in need of measurement implementations to validate the proposed collaborative metrics. Power and force limiting, one aspect of the evolving safety standards, is a robot function that performs a protective stop if any force or pressure limit is exceeded when a robot makes contact with a human during collaborative operations. The standard defines a set of injury metrics based on predetermined medical/biomechanical requirements and parameters. These parameters and requirements include a defined human body model with main and subcomponent regions, relevant injury criteria with per-region limit values, and characteristic values for the deformation constants for the established body regions. The permissible forces and surface pressures for the affected individual body regions must be verified according to potential collision area points after setting up a collaborative robotic workcell. This paper provides an overview of the injury metrics currently proposed, and describes a prototype measurement device that replicates the deformation constants of the various body regions and measures static and dynamic collision forces during robot collisions. Initial testing of the device is presented along with evaluation of the metrics currently proposed by this standards activity.

1 INTRODUCTION

A new class of robots is emerging that are fundamentally different from classical industrial robotics [1,2]. Traditional industrial robots are designed to achieve positioning accuracy with high repeatability, high speed, and stiffness. These performance characteristics, however, result in massive robots in comparison to their rated payloads, and may have a load-to-weight ratio on the order of 1:10. Newer robot designs are smaller and use lighter materials to achieve load-to-weight ratios closer to 1:1, but at the expense of having lower payload capacities and lower stiffness. These next-generation robots, although still largely only in prototype stages, are lighter, potentially safer, and easier to deploy and reconfigure, effectively making them ideal for deployment in collaborative manufacturing environments.

A barrier to widespread adoption of these collaborative robots in manufacturing, however, is the lack of performance standards certifying their safety when working with humans. Standards efforts are now underway to provide guidance for collaborative robotics. The latest release of the ISO 10218 industrial robot safety standards [3,4] has requirements for addressing collaborative robot safety in the areas of:

- Speed and Separation Monitoring (SSM): a robot system function that maintains a safe operation distance from humans located in a collaborative workspace, and
- Power and Force Limiting (PFL): a robot system function that performs a protective stop if any force or pressure limit is exceeded when a robot makes contact with a human during collaborative operations.

The ISO TC184/SC2 WG 3 standards committee on safety of industrial robots is currently working on technical specification TS 15066 to provide additional guidance in the areas of SSM and PFL modes of robot collaboration [5]. As part of the PFL efforts, injury severity criteria are being developed to establish maximum forces that a robot can impose on a human during a collision. This paper describes the NIST effort to develop a measurement device to assess the ability of an industrial robot system to stay below the defined force and pressure limits.

2 INJURY CRITERIA FOR POWER AND FORCE LIMITING (PFL)

The injury severity criteria under consideration by the TS 15066 working group were developed by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA – formally BGIA) [6]. The injury criteria are based on a literature survey establishing maximum allowable limit values on individual body regions that avoid exceeding:

1. skin/tissue penetrations that are accompanied by bloody wounds, fractures, or other skeletal damage
2. the injury severity category 1 of the Abbreviated Injury Scale (AIS1) [7]
3. injury severities with the codifications for surface injuries of the ICD-10-GM 20062 [8]

The German study shows that during collisions between a collaborative robot and a human, elastic and plastic deformations of the soft tissue component of body regions can occur. Among other medical factors, deformations are dependent on the duration of the contact. Short periods of contact create more elastic deformations of the soft tissue, and longer periods of contact produce more plastic deformations resulting in a residual three-dimensional deformation area of the soft tissue in contact with the robot component. In order to limit the degree of injury as the result of a collision, a set of medical/biomechanical limits (force and pressure) and associated soft tissue deflection properties are defined in Table 1 relative to a body model. The model establishes four main body regions and 15 individual body regions within the main regions so all anthropometric points of the body surface can be allocated force limits and tissue properties. The body model indicating the individual body regions is shown in Figure 1a.

Body model Main and individual regions with codification ^a		Maximum allowable Limit values of the injury severity criteria (CSF, IMF, PSP) and arranging factor (CC) ^b			
Main body regions	Individual body regions	CSF [N]	IMF [N]	PSP [N/cm ²]	CC [N/mm]
1. Head with neck	1.1 Skull/Forehead	130	175	30	150
	1.2 Face	65	90	20	75
	1.3 Neck (sides/neck)	145	190	50	50
	1.4 Neck (front/larynx)	35	35	10	10
2. Trunk	2.1 Back/Shoulders	210	250	70	35
	2.2 Chest	140	210	45	25
	2.3 Belly	110	160	35	10
	2.4 Pelvis	180	250	75	25
	2.5 Buttocks	210	250	80	15
3. Upper extremities	3.1 Upper arm/Elbow joint	150	190	50	30
	3.2 Lower arm/Hand joint	160	220	50	40
	3.3 Hand/Finger	135	180	60	75
4. Lower extremities	4.1 Thigh/Knee	220	250	80	50
	4.2 Lower leg	140	170	45	60
	4.3 Feet/Toes/Joint	125	160	45	75
^a BR - Body region with codification Regions - Name of the individual body region		^b CSF - Clamping/Squeezing force IMF - Impact force PSP - Pressure/Surface pressing CC - Compression constant			

Table 1: BGIA Injury Criteria

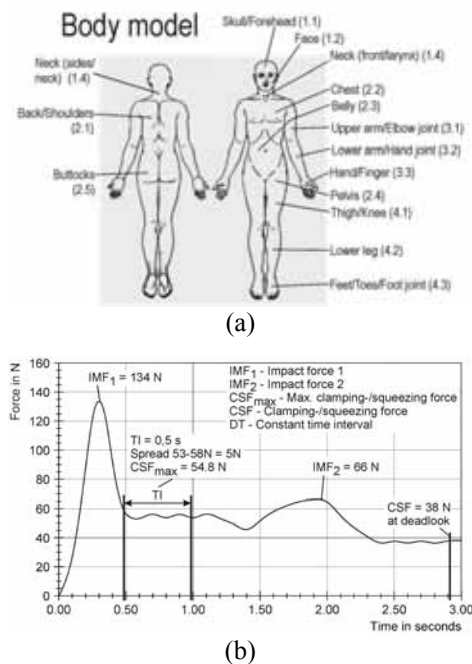


Figure 1: (a) BGIA Body Model and (b) BGIA Force Characterization

These limits and properties are defined as follows:

1. Impact Force (IMF) – The maximum permissible force acting on a body region resulting from a robot collision where the period of contact results in an elastic deformation of the soft tissue. An impact force is defined to occur when the difference between the maximum force and other forces before and after the maximum is more than 5 N over a time interval of 0.5 s or less as depicted in Figure 1b
2. Clamping/Squeezing Force (CSF) – The maximum permissible force acting on a body region resulting from a robot collision where the period of contact results in a plastic deformation of the soft tissue. A clamping/squeezing force can be detected by a spread of the force signal of not more than 5 N over a time interval of more than 0.5 s within any time of the whole measurement as depicted in Figure 1b.
3. Pressure/Surface Pressing (PSP) – The maximum permissible partial pressure load in the case of both IMF and CSF where the contact area (CA) of the collision is small as to reduce the defined IMF and CSF limits. The critical contact area is defined as:

In the case of an elastic deformation: $CA = IMF/PSP$

In the case of a plastic deformation: $CA = CSF/PSP$

4. Compression Constant (CC) – is the deformation constant of a body region through which the maximum compression path is established assuming linear deformation behavior throughout the soft tissue body region.

3 PFL MEASUREMENT DEVICE

3.1 Design

Based on the proposed injury criteria and associated testing guidance provided in the BGIA report [3], NIST developed a mechanical measurement system that replicates the defined body region compression constants and measures the maximum forces applied by a robot during a collision. The following requirements were extracted from the BGIA report:

1. Devices measuring static and dynamic collision forces should be deformable along one axis and have a linear deformation behavior. The malleable components of the devices (such as linear springs) must reproduce compression constants of the individual body regions and allow loads at least up to the limit values of the forces. The linearity of the malleable components must lie within $\pm 5\%$ of the specified CC.
2. The measuring devices must have leveled, plane-parallel guided and sufficiently large collision areas in the direction of the effected collision force where the malleable measuring device components can be found between them. No permanent deformations may occur on the measuring devices as a result of the collision.
3. The force acting in a collision simulation must be measured with a suitable force measuring system in discrete time. Data must be of sufficient resolution to capture all dynamic parts of the collision force. No filtering effects may affect the measurement of the collision force, which must be determined with a maximum error of $\pm 1\%$ from the measured value.
4. It must be possible to verify the limit values for the pressure/surface pressing with these measuring devices. The pressure measuring sensory system may not cause a distorting damping of the impact impulse and have no influence whatsoever on the forces being measured, especially the peak forces. The pressure measuring devices must measure at least the highest partial pressure, but if possible the total pressure distribution within the colliding surface. The measuring sensory system must be able to measure the entire collision area and partial pressures with sensor areas $\leq 10 \text{ mm}^2$. Partial or peak pressure measurements must be carried out with a maximum error of $\pm 2.5\%$ from the measured value.

The current design of the PFL measurement device is shown in Figure 2. Based on industry feedback, the device should have a target cost of \$10,000. This device measures force and displacement and supports both fixed and free

space collisions along a single axis. The injury criteria compression constants are incorporated into the device through the use of ten custom compression springs with the same outer dimensions that are easily interchangeable by removing the strike plate cap. Force measurements are made using a piezoelectric force transducer which is housed between the base of the force/displacement assembly and the base support for the spring. To support performance evaluations of the device, the design also incorporates a linear variable displacement transducer (LVDT) coincident with the device axis.

A series of weights can be added to the linear slide carriage assembly during free space collisions to replicate the mass of the human body regions being struck by the robot. Also shown in Figure 2 as transparent components is the concept of incorporating future spring/damper parameters to replicate response of the human body during free body collisions. Currently there is no guidance provided for free body collisions and this is a topic of discussion within the TS 15066 working group.

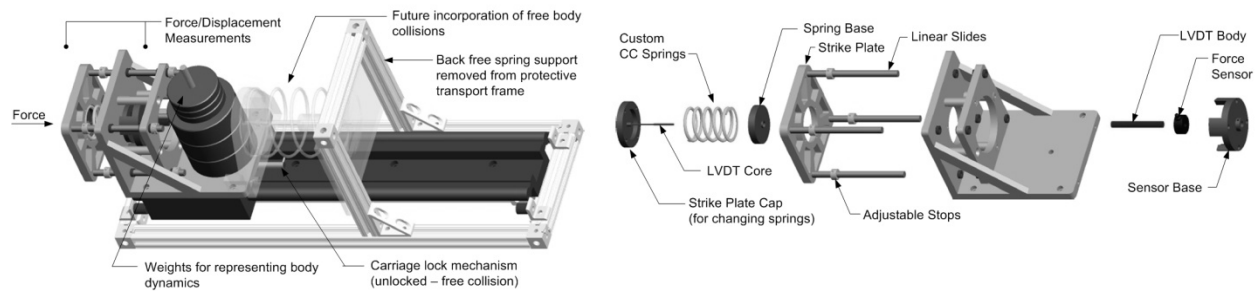


Figure 2 (left) Assembled and (right) sub-components of the NIST PFL measurement device design.

This first prototype design does not include an explicit sensor system for mapping contact pressure in order to verify the limit values for the pressure/surface pressing. After a market search of available tactile sensor pressure pads at costs ranging from \$20,000-\$35,000, NIST is investigating alternative solutions for making these measurements in order to keep the cost of the entire measurement device close to the \$10,000 target. We are currently experimenting with a pressure sensitive paper containing microcapsules that rupture producing an instantaneous and permanent high resolution color-based topographical image of pressure variation across a contact area.

Software was developed for parameter configuration, data acquisition, and data analysis. Parameters are loaded based on the selected body region under test. The device is fixtured to a rigid surface and a robot trajectory is applied along the device axis centered on the strike plate. Data collection is triggered at the start of the impact and data is recorded for 3 seconds, based on proposed TS 15066 testing requirements. The software displays force and displacement data vs. time and graphically identifies force types and maximum force values. LVDT displacement data is also displayed and can be used to calculate forces using spring data with close correlation to the piezoelectric force transducer readings.

3.2 Test and Evaluation

A spring manufacturer was chosen to fabricate the springs. A lot of 10 springs was produced for each of the 10 injury criteria CC values. To date, a single spring from each lot was tested in a compression testing machine to validate the nominal CC values. Initial results showed a variation in linearity during initial deflection due to uneven seating which was eliminated by regrinding the spring ends to be parallel. The actual values of spring CC constants for a single set of springs were measured following the regrinding process. Five springs met the BGIA specified tolerance of $\pm 5\%$ while three were relatively close (see Table 2). The 75 N/mm^2 and 150 N/mm^2 springs were significantly out of tolerance which may be attributed to the fact that the springs were tested to just above the maximum expected force value, which results in small deflections for these springs of approximately 3 mm and 1.5 mm, respectively. The stiffness of the springs in these regions was observed to be non-linear.

We established a calibration procedure using the free body collision weights. The device was placed in a vertical position with the carriage in a locked position. Weights were added to the impact plate to verify the force and displacement readings. Results of a calibration procedure where two 2.27 kg (5 lb) weights were placed consecutively on the strike plate are shown in Figure 3. The arrows indicate the settled force reading after the placement of each weight.

Nominal CC (N/mm ²)	Actual CC (N/mm ²)	Error %
10	10.0	0.8
15	14.7	2.0
25	23.0	8.0
30	28.4	5.3
35	32.9	6.0
40	38.3	4.3
50	47.7	4.6
60	57.5	4.2
75	64.0	14.7
150	119.0	20.7

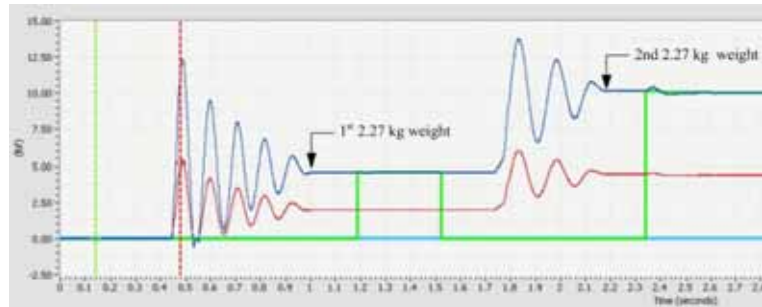


Table 2: Results of the CC validation

Figure 3: Calibration results for consecutive 2.26 kg (5 lb) weights

The NIST prototype PFL measurement device is shown in Figure 4. The overall performance of the device was tested using two different robots. NIST used a typical 20 kg payload industrial robot fitted with a 6-axis force transducer to perform initial testing of the device using position-based trajectories as shown in the right side of Figure 4. These tests were used to verify sensor readings from the device and included correlations between piezoelectric force transducer data, forces calculated from the LVDT displacement data and actual spring constants, and force readings from the robot force transducer. We also field tested the performance of our PFL measurement device on a prototype commercial robot.

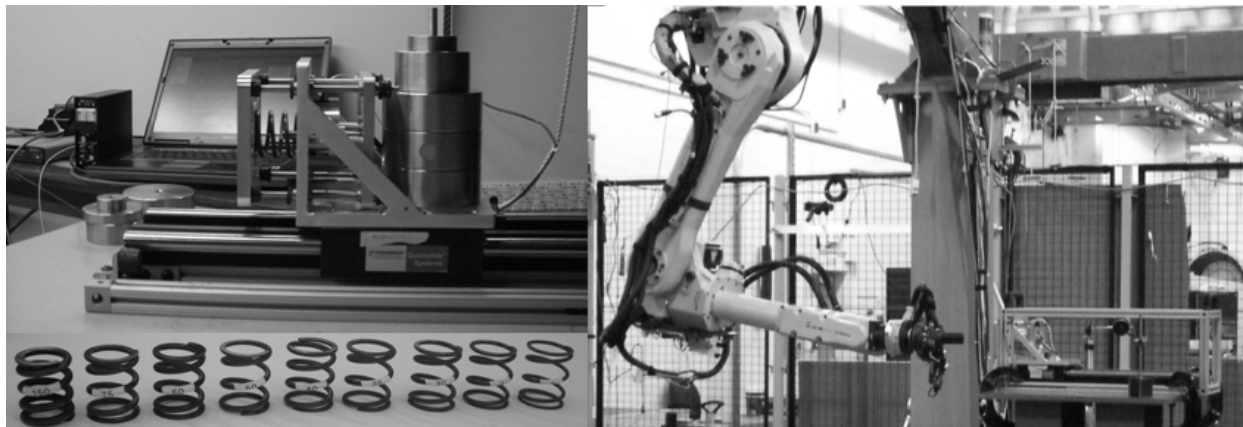


Figure 4: The NIST PFL device prototype (top-left), CC springs (bottom-left), and test set-up using an industrial robot (right)

4 CURRENT ACTIVITIES

While the BGIA/IFA injury criteria are being used in TS 15066, work continues to develop injury criteria to ensure that maximum values chosen are not so conservative as to limit potential applications for robots operating under the Power and Force limiting mode of operation as defined in ISO 10218. NIST is collaborating with a biomechanics expert who is currently evaluating the IFA/BGIA injury severity criteria and is also investigating injury severity criteria and standardized maximum force values that resulted from studies from the transportation industry on blunt force impact injuries caused by bus and train doors. As mentioned previously, the current injury criteria do not

specify parameters associated with free body collisions. NIST is working with the biomechanics expert to develop a set of spring-damper parameters to enable the NIST PFL measurement device to be configured to support free body collisions. NIST is also investigating alternative methods to measure pressure to avoid the high cost associated with pressure sensor array systems. In addition, IFA is currently working on refinements to the current injury criteria that attempt to more accurately define the soft tissue regions using two compression constants (CC1 and CC2). CC1 defines soft tissue deflections during the initial soft tissue deflection of an impact and CC2 defines the tissue properties at the bounds of its maximum deflection. IFA is also funding a pain discomfort study in an attempt to develop a minimum level of force that causes discomfort. The idea is that these reduced forces can be used to develop robot PFL collaborative applications where there are expected robot collisions with humans and forces should be limited to below injury levels. In addition to the NIST efforts, IFA and Fraunhofer IPA, also participants in the development of TS 15066, are working to develop measurement devices.

5 CONCLUSIONS

The device performed as designed during robot impacts. We found that during testing, it was difficult to reposition and rigidly fixture the device to test different strike points along the length of a robot arm. We also identified improvements for the device software for more automated repeated captures of impact trials. Finally, we came to the understanding that rate of energy transfer varies significantly with the properties of the striking surface. A high peak impact was observed when the metallic strike plate was impacted as compared to striking the device with a conformable rubber pad over the strike plate. There is currently no requirement in TS 15066 for impact surface properties.

The feasibility of using springs to represent body regions of higher stiffness and small displacements needs to be investigated. Deviations in spring properties in these regions appear significant; however more analysis is needed to determine if they were induced by the manufacturing process. NIST needs to closely track modifications to the current injury severity criteria and offer input from our studies, as well as incorporate changes into future device designs.

IFA's specification of CC1 as a substrate on the strike plate shows promise to better replicate the properties of soft tissue regions and provides a basis for a standardized strike plate substrate material. The TS 15066 working group must develop more detailed test device requirements and associated test methods to ensure that the results of performance tests for robots with PFL functionality are not device dependent. Finally, a standard method of device calibration is needed to validate these PFL measurement devices.

6 REFERENCES

1. A. Albu-Schaffer, S. Haddadin, Ch. Ott, A. Stemmer, T. Wimbock, G. Hirzinger, *The DLR Lightweight Robot: Design and Control Concepts for Robots in Human Environments*, Industrial Robot: An International Journal, Vol. 34, No. 5, 2007.
2. J. Kruger, T.K. Lien, A. Verl, *Cooperation of Human and Machines in Assembly Lines*, CIRP Annals – Manufacturing Technology, Vol. 58, 2009, pp 628-646.
3. ISO TC 184/SC2/WG3, ISO 10218-1:2011 – *Robots and robotic devices — Safety requirements — Part 1: Industrial robots*, 2011.
4. ISO TC 184/SC2/WG3, ISO 10218-2:2011 – *Robots and robotic devices — Safety requirements — Part 2: Industrial robot system and integration*, 2011.
5. ISO TC 184/SC2/WG3, *ISO/PDTS 15066 Robots and Robotic Devices – Industrial Safety Requirements Collaborative Industrial Robots*, Draft Document, 2012.
6. *BG/BGIA Risk Assessment Recommendations According to Machinery Directive: Design of Workplaces with Collaborative Robots*, U 001/2009e October 2009 editions, revised February 2011.
7. Association for the Advancement of Automotive Medicine (AAAM), *Abbreviated Injury Scale*.
8. World Health Organization (WHO), *International Classification of Diseases (ICD)*.

Development of Safety Technology for Outdoor-use Person Carrier Robots that Achieve the Optimal Safety and Usability in the Ageing Society with a Declining Birthrate

Kazuya Okada¹, Tatsuyoshi Kuriyama¹, Osugi Norifumi¹,
Dohi Masao¹, Toshihiro Fujita¹

¹ IDEC CORPORATION

7-31, Nishimiyahara 1-chome, Yodogawa-ku Osaka 532-8550, Japan

KEY WORDS: outdoor-use, person carrier robot, safety wireless technology, environment resistance,

Abstract




As Japan is faced with a growing issue of aging society with a declining birthrate, various robots and mobile utility to assist elderly people have gained attention. The robot technology has greatly advanced for industrial applications, however, the conventional safety measures for industrial applications do not fully meet the requirements of person carrier robots that assist people in daily lives, because they are mostly used outdoors. Utilizing the technologies accumulated in industrial applications, we developed the obstacle detection sensor and also the safe wireless emergency stop technology, both for outdoor use, which can be utilized to achieve the mobile robots for assisting the people's daily life. Moreover, we developed the deceleration/stop control technology of the safety products as a part of functional safety control system developed according to the requirements of international standard IEC 61508 [2-3]. In this study, we chose the electromagnetic guiding golf cart, an electric-powered vehicle widely used in actual applications, as a model case study of person carrier robots to apply our safety measures. We focused on golf carts because most golf carts used in Japan are automatic and electromagnetic guided devices that move along the guide wires buried in the ground. And also because the quiet, electromagnetic guided golf carts which have replaced the noisy-gas-powered vehicles, have caused serious injury to elderly players recently.

In this paper, we report on the feasibility study of the safety measure with safe wireless emergency stop technology which optimizes the safety and usability of person carrier robots.

1 Introduction

In recent years, the types of robot used in a wide variety of industrial applications have also been adapted to support people's lives, especially in the field of transportation or to provide services at commercial and public facilities. In Japan, with its aging society and decreasing number of children, the emphasis placed on such life-supporting robots is increasing. The application of robotic technology, which has previously been limited to industrial uses, to society at large may increase convenience and efficiency. However, greatly increasing the amount of direct contact between people and machines or robots may also generate new types of risk. This study focuses on the people carrier type of life-supporting robot (people carrier robot) which will be an important means of outdoor transportation in the future. Table 1 shows the level of difficulty associated with the technological development required to ensure the safe operation of AGVs or unmanned vehicles, indoor mobile work robots, and the people carrier robots designed for outdoor use. In almost all cases, a higher level of

Table 1. Comparison of weatherability and safety measures for indoor and outdoor

Limitation on machinery use		Indoor-use AGV 	Indoor-use personal care robot 	Outdoor-use people carrier robot 
Location		Indoors	Indoors	Outdoors
Weatherability	Road surface	Flat	Flat	Rough (irregular)
	Rain	Indoors	Indoors	Rain, snow
	Sunlight	Indoors	Indoors	Outdoors (direct sunlight) and afternoon sun
	Other	Oil and other	None	Fog
Electromagnetic disturbance		Large amount of noise	Depend on environment	Depend on environment
Safety for humans	Riding	Not for riding	Not for riding	Riding
	User's skill	Experts and professionals	Experts and professionals	General public (children, elderly people)
	Pedestrian	Experts and professionals	General people (children, elderly people)	General public (children, elderly people)
	Separation of pedestrian and vehicle	Separated, without guard	None (commonly used)	None (commonly used)

technology is required to ensure safety during outdoor use (to cope with misdetection issues caused by rainy, snowy or foggy conditions, or detection failures in direct sunlight, for example). Using electromagnetically guided golf carts (which are already widely used at golf courses) as a base model, appropriate safety technologies were developed to enable the people carrier robots to be used outdoors. The results are as follows.

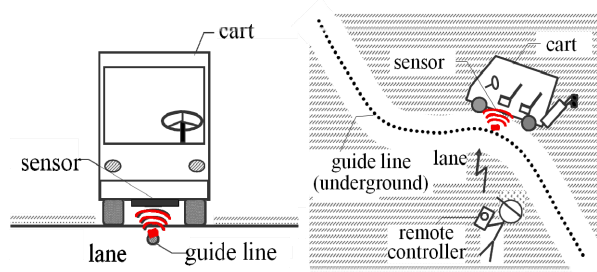


Figure 2. Operation of the electromagnetically guided golf cart

2 People carrier robot for outdoor use

The people carrier robot designed for outdoor use can greatly expand a person's range of mobility and freedom of travel. Using the existing electromagnetically guided golf cart as a base model, appropriate safety technologies were developed to enable operation without the need for a driver.

2.1 Electromagnetically guided golf cart

The electromagnetically guided cart is not an autonomous vehicle. Instead, it is equipped with a sensor to detect the gap between the center of the chassis and a guide line buried underground, and an actuator to change the direction of the wheels in order to correct the gap, when required. The cart can then travel along a guide lane without the need for an operator and can, therefore, act as an automatic, self-driving people carrier robot. In recent years, 98% of all golf courses in Japan have introduced the people carrier golf cart and they are becoming electromagnetically increasingly common. Almost half of the carts being introduced to golf courses in Japan are now of this type. Because of their widespread adoption, the electromagnetically guided golf cart was, therefore, selected as a base model for the people carrier robot.

3. Risk assessment for the person carrier robot

3.1 Risk assessment procedure

As shown in Figure 3, risk assessment was based on international standard ISO 12100:2010: "Safety of machinery - General principles for design - Risk assessment and risk reduction" [1].

3.2 Assessment principles

The safety measures adopted were based on the risk evaluation procedure used in risk assessment, involving the use of evaluation criteria. The evaluation criteria used for risk assessment were as follows:

[Evaluation criteria for risk assessment]

Level of risk $R = S \times Ph$

Severity of damage: S

Serious disability (long-term treatment)	4 points
Medical treatment (short-term recovery)	3 points
Recovery with first-aid treatment	2 points
Slight injury or temporary pain	1 point

Probability of an accidents: $Ph (Ph = F + Ps + A)$

Frequency/time of exposure: F

Continuous/always	4 points
Frequent operation/ for a long time	3 points
Occasional operation/for a short time	2 points
Few times/momentary	1 point

Possibility of avoidance: A

Possible	3 points
Impossible	1 point

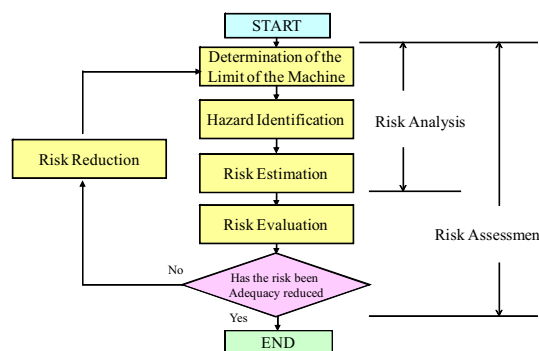


Figure 3. Risk assessment process

Probability of a dangerous situation: Ps

High probability	4 points
Can happen	3 points
May happen	2 points
Rarely happens	1 point

[Criteria for assessing the risk]

$3 \leq R \leq 6$	Low enough to ignore
$7 \leq R \leq 14$	Low to medium/acceptable with conditions/ requires study
$15 \leq R \leq 44$	High/ not acceptable

Table 2. Risk assessment result for the golf carts

No.	Operation mode	Subject	Hazard	Hazardous situation/ hazardous event	Hazardous zone	Subject	Severity of harm S	Probability of occurrence of harm				Risk Point R	Risk evaluation
								Ph	Frequency	Probability	Avoidance		
									F	Ps	A		
1	Automatic operation	Employee or players	Robot (golf cart)	Passenger thrown out of the cart when it stops suddenly	Seats on the cart	Passengers on the cart	3	5	3	1	1	15	Risk reduction measures are necessary
2				Pedestrian hit by the cart, causing bruising	On the guide lane	Pedestrian	2	8	3	2	3	16	Risk reduction measures are necessary
3				Pedestrian hit the cart and thrown to the ground	On the guide lane	Pedestrian	3	8	3	2	3	24	Risk reduction measures are necessary
4				Pedestrian hit by the cart as it stops	On the guide lane	Pedestrian	2	5	3	1	1	10	Risk reduction measures are necessary
5				Passenger thrown out of the cart	Seats on the cart	Passengers on the cart	3	3	1	1	1	9	Risk reduction measures are necessary
6				The remote controller used to stop the cart does not work, due to external factors, and the cart collides with pedestrians	On the guide lane	Pedestrian	3	5	3	1	1	15	Risk reduction measures are necessary
7				The remote controller used to stop the cart works, due to external factors, and the cart collides with pedestrians	On the guide lane	Pedestrian	3	5	3	1	1	15	Risk reduction measures are necessary
8				The remote controller used to stop the cart does not work, due to external factors, and the passenger thrown out of the cart	Seats on the cart	Passengers on the cart	3	5	3	1	1	15	Risk reduction measures are necessary

3.3 Usage environment for golf carts

The golf carts used at golf courses are characterized by a unique set of usage conditions, such as being outdoors, operated on hilly courses in mountain areas, or being remotely controlled (without the need for a driver). In addition, battery-powered golf carts also operate very quietly. As a result, the following dangerous situations can occur.

- Remotely controlled, electromagnetically guided carts may be operated from a distance, without checking the situation in the immediate vicinity, and may bump into pedestrians along the guide lane.
- Because many golf courses in Japan are located in mountainous areas, the guide lane have many irregularities and curves, restricting the view. Such geographical features may hinder the wireless signal from the remote controller and the carts may not always stop when ordered to.
- In the case of battery-powered carts which operate without making any noise, pedestrians may not always be aware of unmanned carts approaching from behind and can be hit.

Table 2 shows some of the results for risk assessment conducted on golf carts in order to evaluate their feasibility as a people carrier robot for outdoor use.

4. Protective measures of the people carrier robot

4.1 Hazards, hazardous situations and safety function

Table 2 shows that the major source of danger when using the electromagnetically guided golf cart is the cart itself. There are 3 types of dangerous situation that can arise:

- Collisions between the cart and pedestrians
- Passengers being thrown out of the cart when it stops suddenly
- Cart function failures due to external factors such as EMC

The major safety measures adopted in order to address these causes of danger and dangerous situations were as follows:

- A trip device to detect obstacles (including human beings) and stop the cart
- An emergency stop for the cart, activated by pressing an emergency stop switch
- An emergency stop for the cart, activated by pressing a wireless emergency stop switch

With all these safety measures, it is necessary to adjust the level of operation in proportion to the risks, such as “ensuring that the cart suspension is correctly adjusted in order to detect obstacles”, “ensuring that the cart can make an emergency stop when the emergency stop switch is activated”, or “ensuring that the cart stops when an abnormality is detected which affects the safety functions”.

4.2 Safeguards - safety laser scanner for outdoor use

One protective safety measure we investigated was the spatial and temporal separation of people and golf carts. Dangerous situations arise when golfers and golf carts share the same space used for transportation at the same time, so protective measures include the installation of protective fences and safe crossing points. However, when golf carts are regarded as people carrier robots for outdoor use, it is difficult to completely isolate them as they are part of the social infrastructure. Instead, it is necessary to equip the cart with a trip device to detect the presence of anyone in front and stop the cart - thereby ensuring spatial and temporal separation [5]. In such

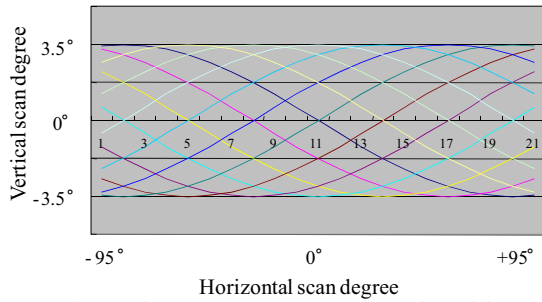


Figure 4. Laser scan pattern produced by gimbal-mechanism



Figure 5. Safety laser scanner for outdoor use installed on the golf cart

cases, a laser scanner, already utilized as a safety device for some applications, can also be used as a detection device.

However, because existing scanners are made for indoor use in factories rather than for outdoor use, a gimbal-mechanism was added to allow the laser beam to move vertically. By scanning both horizontally and vertically, 3-dimensional scanning of the area ahead of the cart could then be carried out, as shown in Figure 4. As a result, it is possible, in theory, to cancel out effects caused by the incidence of sunlight and successfully use such scanners outdoors as well as indoors.

Figure 5 shows a golf cart equipped with the modified laser scanner developed for outdoor use.

Another important consideration is the braking function. Golf carts may carry passengers, so an emergency stop (stop category 0) may throw the passengers out of the cart, creating a dangerous situation. In order to ensure a safe stop when carts are being operated at their maximum speed of 8 km/h, the protective safety range of the laser scanner was set at a radius of 2 m (allowing any object within a 190° field of view and with more than 1.8% surface reflectance to be detected). These specifications also allow the warning area to be adjusted within a radius of 8.5 m in order to provide adequate warning for people in front of the carts.

The detection range of the laser scanner can be freely adjusted so that trees or other geographical features in the surrounding area will not be confused with pedestrians. When an obstacle ahead of the cart is detected, the safety cutout turns the laser scanner off, stopping the cart. In order to avoid the unnecessary detection of obstacles encountered at specific points along the route, the detection range can be adjusted to take account of the locations of these obstacles and to ensure that the cart continues to operate correctly.

4.3 Complementary safety measures: Wireless emergency stop switch

Because electromagnetically guided golf carts operate automatically, it is necessary to adopt additional protective measures to avoid collisions in dangerous situations. Battery-powered golf carts are very quiet, so it is sometimes difficult for pedestrians to avoid them. Pedestrians crossing the guide lane may also generate sudden changes in the operating environment. In these cases, it can be necessary for third parties such as caddies to take emergency action to avoid a collision. Alternatively, since many of these carts are also carrying passengers, an emergency stop switch (Figure 7) can be installed for them to use, as well as a wireless emergency stop switch (Figure 8) for third party use.

4.3.1 Wireless emergency stop system

An emergency stop switch using wireless technology was developed to allow golf carts to be brought to an emergency stop, safely, by remote control.

The development process for the emergency stop switch was divided into 4 evolutionary phases, reflecting the types of technology employed:

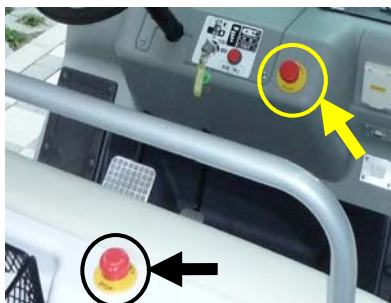


Figure.7 Emergency stop switch

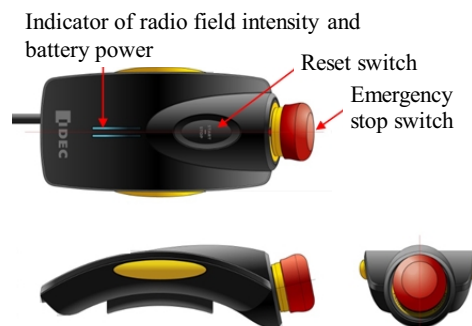


Figure.8 Wireless emergency stop switch

- Phase 1: General wired technology with a direct connection to the switch
- Phase 2: Reduced wiring, using communication technology
- Phase 3: 1:1 communication system, using wireless technology
- Phase 4: N:M communication system, using wireless technology

In phases 1 to 3, the switch was developed simply to serve as an emergency stop system. However, it was also necessary to realize N:M communication using wireless technology to allow a number of robots to be operated at the same time, so the technology needed to accomplish this was developed in phase 4. In order to ensure that the communication system would operate safely and reliably, the wireless emergency stop switch design was based on international standard IEC61508 and the wireless communication system was based on IEC61784-3, which stipulates the procedures and methods of communication to be used for industrial devices [2-4].

The N:M communication system used in phase 4 is the most appropriate for mobile robots. A large number of emergency stop switches can be linked to several carts.

By using this wireless emergency stop switch, as shown in Figure 9, whenever communication is lost due to electrical interference or when carts are out of communication range, they stop automatically [8,10].





4.4 Safety-related part of a control system

Figure 10 illustrates the safety-related components which receive output from the laser scanner, wireless emergency stop switch, described above, and the conventional emergency stop switch. The signal received is then used by the operation controller to stop the guided golf carts. A safety control unit is also used - receiving input from the laser scanner, the safety wireless emergency stop switch and the conventional emergency stop switch, then generating a safety output in order to transmit the correct signal to the drive controller of the golf carts [6-7,9].

5. Effectiveness of next-generation safety measures

The laser scanner developed for outdoor use and the wireless emergency stop switch were installed on electromagnetically guided golf carts in order to conduct the outdoor experiment. The ability of the golf carts to function safely in fine weather was confirmed. Evaluation of the safety functions is still continuing.

Table 3. Evolution phases for emergency stop switches and the required technology for each phase

Phase		Emergency stop switch evolution phase			
		Phase 1 Wired (Parallel wiring)	Phase 2 Wired (Reduced wiring)	Phase 3 Wireless (1:1 communication)	Phase 4 Wireless (N:M communication)
Appearance	Required technology				
	Mechanical technology	Developed	Phase 1 technology can be used	Phase 1 technology can be used	Phase 1 technology can be used
Functional safety technology	Safety operation mechanism	Developed	Phase 1 technology can be used	Phase 1 technology can be used	Phase 1 technology can be used
	Direct opening Mechanism	Developed	Phase 1 technology can be used	Phase 1 technology can be used	Phase 1 technology can be used
	Safety software Technology	Not required (no software)	Developed	Phase 2 technology can be used	Development needed
	Safety wireless communication technology	Not required (no communication)	Not required	Developed	Development needed
Safety location detecting technology	Safety location detecting technology	Not required	Not required	Developed	Development needed
	Safety login/logout technology	Not required	Not required	Developed	Development needed

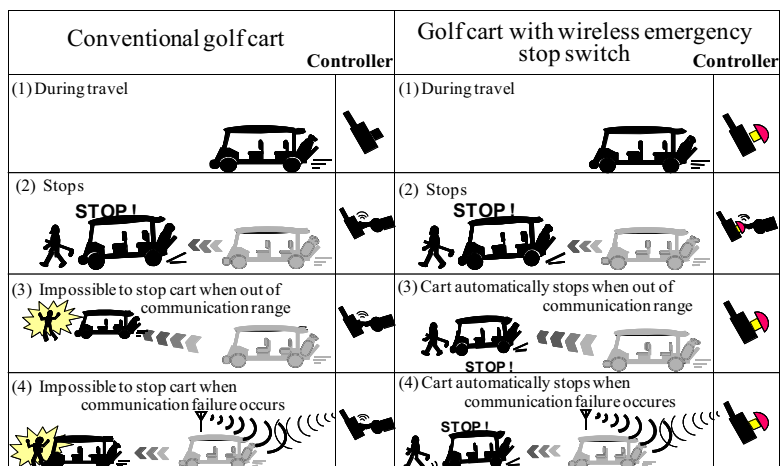


Figure 9. Effectiveness of the wireless emergency stop switch

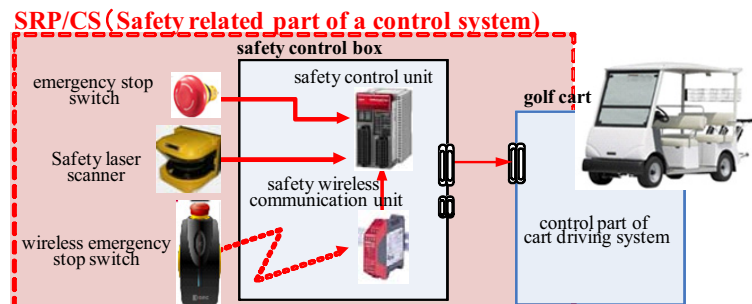


Figure 10. Block diagram showing the safety-related part of a control system

6. Conclusion

Simply converting existing industrial technology and safety measures for use with people carrier type of life-supporting robots is not always sufficient to deal with problems posed by the outdoor environment or the emergency stop requirements for an unmanned moving body. A gimbal-mechanism was, therefore, combined with a laser scanner to realize 3-dimensional scanning over the required range and to cope with external factors such as sunlight. A wireless emergency stop safety switch, incorporating wireless technology in the emergency stop system to enable a third party to control unmanned carts, was also found to be an effective safety measure for people carrier robots.

However, the following issues still need to be addressed:

- The impact of weather, such as rain, snow and fog, on the laser scanner
- Overcoming the problem of communication shutdown due to geographical features such as forests and hills, and determining the most appropriate communication distance for wide area communication
- The question of environmental durability when exposed to ultraviolet rays and vibration when people carrier robots are used outdoors

In order to promote the adoption of people carrier type of life-supporting robots with advanced safety features, as shown in Figure 11, and address the issues highlighted above, further development will be focused on the following areas:

- i) Development of a laser scanner with excellent environmental durability when exposed not only to sunlight but also to rain and fog
- ii) Development of suitable safety-related wireless communication technology for outdoor use – taking geographical features such as forests and hills which can interfere with wireless communication into consideration
- iii) Development and validation of durable technology which can withstand rain, ultraviolet rays and vibration during cart operation

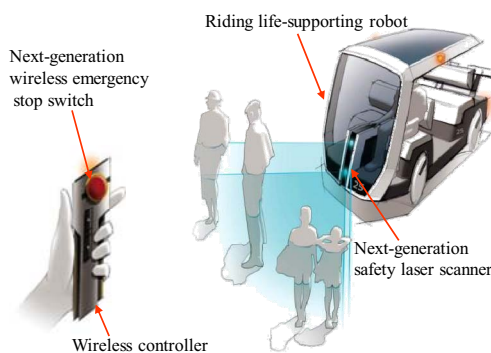


Figure 11. Conceptual illustration of person carrier robot for outdoor use with incorporated safety measure

Acknowledgements

This research study on the “Development of safety engineering technology for electromagnetically guided golf carts as outdoor mobile personal care robots”, including their demonstration, was conducted as a joint project in cooperation with Osaka University as part of the “Project for Practical Applications of Service Robot”, commissioned by the New Energy and Industrial Technology Development Organization (NEDO) in 2011.

References

1. ISO12100:2010, Safety of Machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology, -Part 2: Technical principles
2. IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements
3. IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements
4. IEC 61784-3:2010, Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses -General rules and profile definitions
5. IEC61496-3:2008, Safety Of Machinery - Electro-Sensitive Protective Equipment - Part 3 : Particular Requirements For Active Opto-Electronic Protective Devices Responsive To Diffuse Reflection
6. M. Mukaidono, Machine System Safety Technology in the Age of Globalization, The Society of Safety Technology and Application, The Nikkan Kogyo Shimbun, Ltd., 2000
7. IDEC, Safety Concept Book, 2005
8. Manabu Shutto, Hitoshi Aisu, Takayoshi Shimizu, Masao Dohi, Tomonori Nishiki: *Proposal of next-generation emergency stop switch utilizing safe wireless communication for mobile robot applications*; 6th International Conference “Protective devices and systems” SIAS2010, Finland, 14-15 June, 2010
9. Norifumi Ohsugi, Takayuki Shimizu, Masao Dohi, Tomonori Nishiki: *Development of the next-generation easy-to-use safety controller suitable for various industrial applications*; 6th International Conference “Functional Safety” SIAS2010, Finland, 14-15 June, 2010
10. Eisuke Masuda ,Takayoshi Shimizu , Norifumi Ohsugi , Manabu Zenmani ,Tatsuyoshi Kuriyama , Kazuya Okada, and Masao Dohi:” *APPLICATION OF THE NEXT-GENERATION EMERGENCY STOP SYSTEM UTILIZING FUNCTIONAL SAFETY WIRELESS TECHNOLOGY INTO OUTDOOR LIFE-SUPPORTING ROBOTS*; ISA Automation Week 2011, USA, 17-20 Oct, 2011

Safety of Industrial Robots: From Conventional to Collaborative Applications

Jeff Fryman, Robotic Industries Association, Ann Arbor MI, USA, JFryman@robotics.org
Björn Matthias, ABB Corporate Research, Ladenburg, Germany, Bjoern.Matthias@de.abb.com

KEY WORDS: industrial robots, safety, human-robot collaboration, standardization

ABSTRACT

Industrial robots, previously completely separated from human access when in operation in the factory, are acquiring control capabilities rendering them capable of new forms of operation, with suitably controlled risks to allow human workers access to the robot work space during operation. We survey the developments of industrial robots and of robot safety standards, outlining the steps that have brought us to the present status, the opening of possibilities for human-robot collaboration in industrial production. The four basic types of collaborative operation are summarized and open research questions in this area are formulated.

1. INTRODUCTION

Industrial robots have been used increasingly in production for over five decades in widely varying applications, ranging from spot welding in the manufacturing of automobiles to the pick-and-place operations in the packaging industry. The successful deployment of presently over one million industrial robots has rested traditionally on a number of factors: on repeatability as a tool to achieve consistent quality, on the speed and force they make available to manufacturing processes, on the flexibility brought about by programmability, on the possibility to delegate hazardous production tasks to machines to a greater extent, and also on the reduction of the manufacturing work force. But since the installation and commissioning of robot applications is still today associated with appreciable effort and cost, the underlying assumption in their large-scale deployment in production environments still rests on the economy of scale brought about by large product lot sizes and a comparatively rare need for retooling or changeover. In addition, since robots as a rule are hazardous machines that require safeguarding against human intervention, investments in protective guards and safety equipment are non-negligible. The floor space use of a fenced robot installation is also associated with increasing costs for real estate.

Recent years have seen a rapid development of more complex safety functionality for industrial robots, driven from the technological side by advances in microprocessors and safety-certifiable components on all levels. The business opportunity this addresses aims at introducing robots into new application environments, in which the traditional business paradigm does not hold. In order to reduce the need for floor space and for conventional safeguarding while maintaining advantages of robotic automation associated with quality and increasing flexibility further, robots must be enhanced to be able to operate in closer quarters with human workers in the production environment. While the approach of human-robot collaboration (HRC) in industrial production is only now beginning to make its way into practical applications, the relevant expert communities have been very active in the development of the related functionality, of the required safety capabilities residing increasingly in sensors and processors, and in the standardized documentation of the requirements to be fulfilled by industrial robots and robot systems.

2. HISTORICAL OVERVIEW OF INDUSTRIAL ROBOTS AND SAFETY REQUIREMENTS

Robots play an extremely important role in our society today, most notably for industrial manufacturing applications on a global scale. Worker productivity and corporate competitiveness are key elements in a healthy economy, and both are enhanced by the use of industrial automation and robots. This is obvious by the number of robots in use today – an estimated 1.4 million units worldwide – as reported by the International Federation of Robotics statistical analysis [1].

Even as the numbers increase, industrial robots continue to evolve to the benefit of workers around the world, both in productivity and safety. Since the beginning of the robotics industry, safety has been a central issue and a success

story for the industry. The early hydraulically powered industrial robots caused much concern for safety. These robots were large and powerful, with huge mechanical advantage compared to other devices of the time. The controls were simple and not truly reliable. While the early robot manufacturers were justifiably pleased with the technology advances in automation that these machines brought to industry, the concern for the safety of humans working around these machines led to the obvious conclusion of caging them off from personnel. Thus, safety was achieved – at least for normal operations that did not require human intervention.

Early robots did much to remove humans from hazardous, tough and dirty jobs, much improving the working conditions around the factory. Examples include foundry, forging and stamping tasks. To ensure safety in the workplace, efforts began in the United States and in Europe to codify the safety requirements for humans working around industrial robots. In the USA, the Robotic Industries Association (RIA) developed the R15.06 robot safety standard through the American National Standards Institute (ANSI) [2]. In Europe, ISO brought forth the first edition of ISO 10218 in 1992 [3], which was subsequently adopted by CEN as EN 775.

Robot technology development continued, and newer, more capable electric drive robots with servo controls greatly expanded the use of industrial robots in the work place. While still not as reliable from a safety standpoint to the extent today's robots are, these new technologically advanced machines went on to transform many more industrial jobs that required more precision and repeatability, most notably in welding applications. For many years, welding accounted for about half of all robot applications and welding continues today as a leading use of industrial robots.

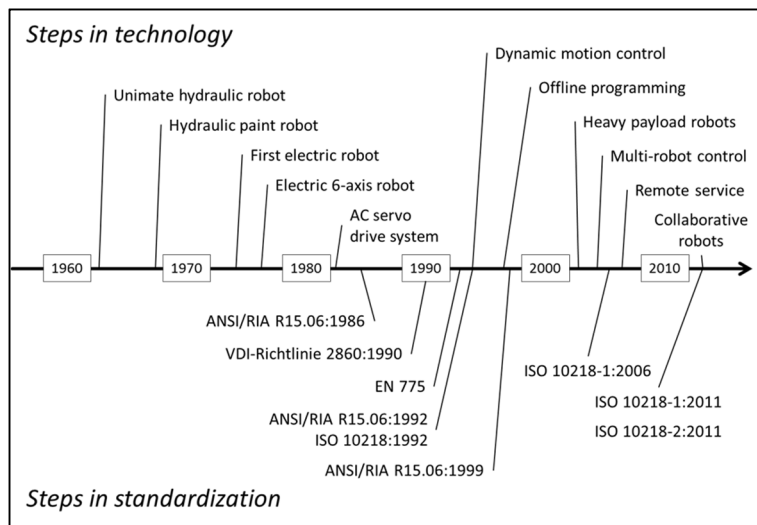


Figure 1. History of industrial robots and their safety standardization

Safety requirements also evolved over time with the issuance of ANSI/RIA R15.06-1992 [2] and of ISO 10218:1992 [3] (EN 775). While similar in scope – industrial robot safety – these two documents did not address personnel safety in the same context, with the USA document providing more detailed information for the integration and use of robots, while the ISO document put more emphasis on requirements for the manufacturers of robots. An overview of the development of technology as well as of standardization is given in Figure 1.

The prevailing safety concept of fencing off robots continued, with thought now given to the need for humans to interact with robots, particularly for maintenance and setting. Significant consideration was given to the proper control and operation and the selection of the appropriate safeguarding.

Because each robot installation is unique from its application, location, and operation, it became generally understood that risk assessment, particularly a structured risk assessment, was needed to properly assess the levels of harm possible in a designed system. The importance of understanding both the task and the hazard associated with that task led to the suggested task-based risk assessment methodology introduced in the ANSI/RIA R15.06-1999 [2].

Robot technology continues to evolve, but after the turn of the century so many new elements of robot control had been introduced that it was time to evolve the safety standards to recognize the improvements and provide new and better guidance for the human interaction with industrial robots. Work was begun to bring ANSI/RIA R15.06-1999 [2] from the USA into the ISO 10218 standards arena, initiating work on a truly global standard for robot safety.

The fruits of this work, carried out under the auspices of the ISO TC184/SC2 WG3 for Industrial Robots [4], first resulted in the publication in 2006 of ISO 10218-1 dedicated to the robot only [5]. This was a comprehensive document to provide guidance for the robot manufacturer in building suitable industrial robots, including improved controls requirements, but also a first description of requirements for collaborative robots. Work continued into 2011, developing safety requirements for the robot system and integration, which was published in July as ISO 10218-2:2011, together with the second edition of ISO 10218-1:2011 [5]. The two parts of ISO 10218 have been published as harmonized standards in the European Union; and work is ongoing in other countries to officially recognize them as their national standards. In fact, work is ongoing in the USA and Canada to produce an integrally combined document as ANSI/RIA R15.06 or CAN/CSA Z434 respectively, which also contains the ISO 10218 series of standards. A tabular overview of the present status of robot safety standards is given in Table 1.

Table 1. Present status of safety standards for robots and machinery applicable in Europe and North America

	Europe	North America
Robot safety standards	ISO 10218-1:2011 (robot) ISO 10218-2:2011 (robot systems)	ANSI/RIA R15.06-2009 CAN/CSA Z434-2008 (robots and robot systems)
Machinery safety standards	ISO 12100:2010 (risk assessment) ISO 13849-1:2006 (functional safety) IEC 62061:2005 (functional safety)	ANSI B11.0-2011
Machine safety legislation	European Machinery Directive	(no equivalent)
Workplace safety regulations	e.g. Berufsgenossenschaft directives (DE)	OSHA 1910 (US) Provincial regulations (CA)

The new ISO standards for industrial robot safety are leading documents enabling the safe use of new technologies and capabilities of present-day industrial robots. The advent of new safety-rated software controls make new applications possible and allows the introduction of new automation capabilities into new markets. Most notable is the advent of the “collaborative robot”, by which the human and the machine now can work in close proximity.

3. MOVING HUMANS AND ROBOTS CLOSER TOGETHER IN THE FACTORY

The past decade has seen growing interest in the technology for and economic relevance of bringing humans and robots closer together in the manufacturing working environment [6], [7]. As flexibility requirements continue to increase, the optimal degree of automation can be less than 100% and the role of the human worker remains important [8], [9]. Due to their contributions to product quality and their inherent flexibility, industrial robots will also retain an important role in the manufacturing environment of the future.

The conventional deployment of industrial robots to automate manufacturing processes is seen to have its particular economic advantages over hard automation and over manual labor for a medium range of lot sizes. Softening the limits of robotic automation to allow a distribution of tasks between humans and robots introduces a new dimension into this argument and widens the applicability of robots for industrial production. In Figure 2 we show how the introduction of HRC applications increases the area of relevance of industrial robots for automation.

Standard industrial robot systems pose hazards to humans due to their inertia, structure and process forces. Protection strategies, as outlined in safety standards, must be applied to assure operator safety. The present challenge is realizing safely the flexible manufacturing environment of the future with a mixture of human workers and robots. Here, humans and robots each take on the tasks for which they are best-suited, with frequent interaction and shared procedures. The strict temporal and spatial separation between them is lifted.

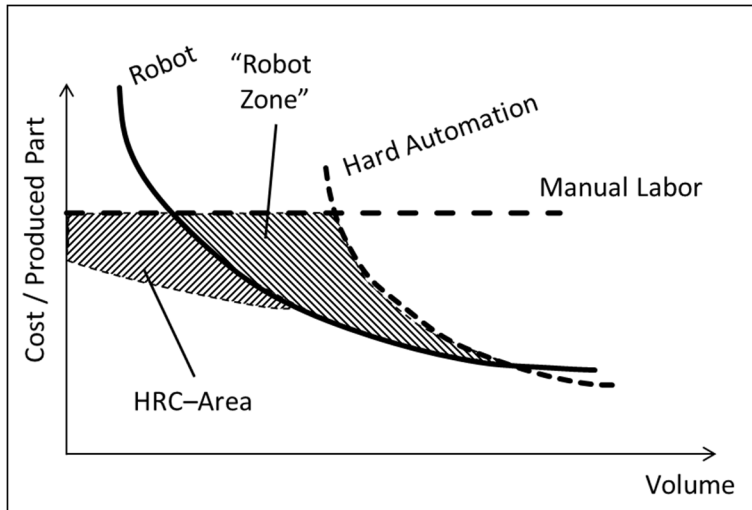


Figure 2. Introduction of HRC extends the applicability of industrial robots to a larger part of industrial production (adapted from IFR World Robotics Report, 2007)

Several versions of these collaborative types of operation have been envisioned and enabling requirements are established in the ISO 10218- standard [5]. These will be considered in more detail in the following section.

4. TYPES OF HUMAN-ROBOT COLLABORATIVE OPERATION

Until recently, robot users interested in more close collaboration between robots and humans in their applications have found that there was little guidance for safety aspects of such installations and have, therefore, shied from exploratory work not backed by standards. With the recent revision of ISO 10218 [5], explicit consideration has been paid to the needs of users wishing to deploy HRC. While the tried and proven basic safety functionality of industrial robots remains relevant and present in the text of the standard, the new functions associated with HRC are not yet based on extensive practical use. This is unlike usual standardization projects, in which groups of experts consolidate the known body of best practices. In the case of HRC, the effort is a close cooperation between technical experts in industry, academia and research organizations aiming to develop simultaneously the body of knowledge governing the safety aspects of HRC as well as documenting this in the text of standards documents.

The two parts of ISO 10218 presently give a brief description of safety requirements for four basic types of collaborative operation. More details will become available in a future document, the technical specification ISO/TS 15066 [10], which is presently under development in the committee ISO/TC 184/SC 2/WG 3 [4]. The objective is to bring forth a document with quantitative guidance for HRC applications.

These applications can be classified in various ways, but any such classification rests on the observation that there will be a portion of the work space in the cell that is accessible both to the robot and to the human in a physically unobstructed way. This volume is called the “collaborative work space” (CWS). For the purposes of standardization, the possible basic types of collaborative operation have been chosen to reflect a number of fundamentally different methods to reduce risk in this situation. Using the titles of the sections in the standardization documents, together with the main measure for risk reduction for each case, these are:

- **Safety-rated monitored stop**
While the worker is in the CWS, the robot is not permitted to move. Rather it must hold its position, even if its drives are still energized.
- **Hand guiding**
Here, the worker has direct control of the robot. Motion is only possible when the worker purposefully activates an input device to cause the desired motion. The robot speed must be limited to a value obtained by risk assessment.
- **Speed and separation monitoring**
Contact between the moving robot and the human worker is prevented by supervising the worker’s position and adapting speed and/or position of the robot to maintain this condition.

- **Power and force limiting**

Contact between the robot and the human worker is considered possible as a normal event during the application, but the nature of these contacts is controlled by inherent design measures of the robot and/or by measures of safety-rated control. In either case, the objective is to limit static and transient forces that the robot is able to impart to exposed parts of the worker's body.

Realistic applications can consist of combinations of these methods. Practical applications of HRC may, therefore, require that the motion of the robot manipulator be supervised, as is possible today with many safety controller options available with commercial robot controllers.

In addition, however, there are capabilities that are presently under development. These include sensory capabilities providing safety-related information on the position of the human worker and reliable predictions of braking distances in real-time when worker and robot interact in the same workspace, but should not come into contact.

Furthermore, when physical interaction is included in the application, especially stringent requirements hold on the nature of this contact. This may be the most challenging of the new methods for operation, since contact is no longer a taboo. It is possible, may be part of the application, and must therefore be understood and controlled. This is a change of paradigm compared to the applications of conventional industrial robots and will lead to the development of new types of robot control as well as to new types of robot manipulators.

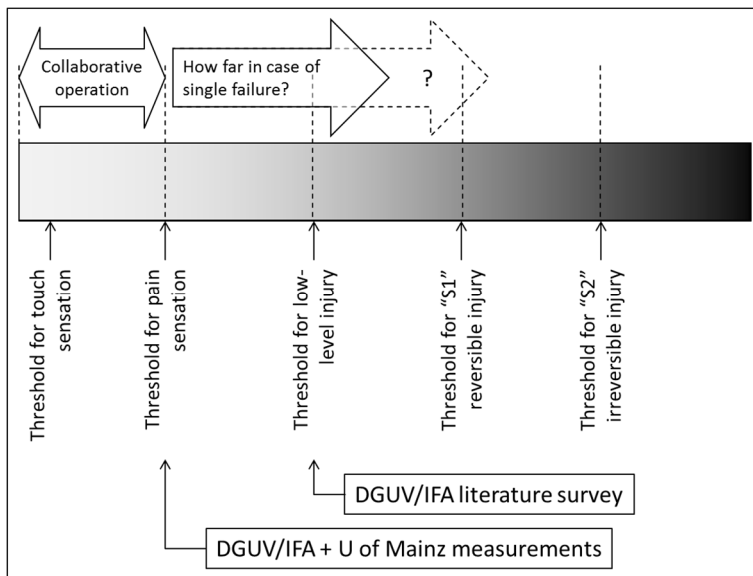


Figure 3. Overview of various thresholds relevant for describing contact events between robots and humans

Significant research effort is being invested into the study of the different thresholds that must be invoked in a full understanding of low-level mechanical loading of the human body [11], [12], and [13]. Efforts range from modeling the dynamics of the robot and of the human body to deriving practically usable limit criteria that can be followed when designing robots and applications. The underlying biomechanical data is, however, still very scant.

As yet unpublished work is ongoing at the University of Mainz and elsewhere to establish the thresholds delimiting touch sensations from pain sensations in various zones of the body. Thresholds for injuries as such cannot be investigated directly, but must be inferred [14] from other source in the medical literature. A simplified schematic of the hierarchy of these thresholds is shown in Figure 3.

5. CONCLUSIONS AND OUTLOOK

While the “simpler” types of HRC operation by way of a safety-rated monitored stop or by hand guiding can be realized with present day technology, the full implementation of the other two types are still pending additional research results and product development.

Maintaining a specified separation distance between any part of the moving robot and the worker means that the control system must at all times have information not only on the pose and motion state of the robot, but also on the position and anticipated motion of the worker, as long as he is in the CWS. To date, sensors suitable for use in safety-rated systems are limited to delivering binary information on the presence of an object in one or more statically defined regions in space (zones). One may anticipate, however, that safety sensors will become available with the capability of delivering safety-rated position information on objects detected in their field of view.

Finally, the proper limiting of both static and dynamic forces that a collaborative robot shall be able to impart to exposed parts of the worker's body requires fundamental understanding of the biomechanical mechanisms involved and how they correlate to the dynamical properties of robot motion and to the specifics of the affected body part.

6. ACKNOWLEDGEMENTS

The authors thank the working group WG3 of the ISO TC184/SC2 and the corresponding national working groups for the manifold input and discussions that have brought us all to the present status in standardization work. One of us (B.M.) acknowledges support through the European Community's Seventh Framework Programme FP7/2007-2013 – Challenge 2 – Cognitive Systems, Interaction, Robotics – under grant agreement No 230902 - ROSETTA.

7. REFERENCES

1. World Robotics – Industrial Robots: Statistics, Market Analysis, Forecasts, Case Studies and Profitability of Robot Investment, International Federation of Robotics, Frankfurt am Main (2012).
2. ANSI/RIA R15.06 “American National Standard for Industrial Robots and Robot Systems – Safety Requirements”, Robotic Industries Association, Ann Arbor (1992, 1999).
3. ISO 10218 “Manipulating industrial robots – Safety”, ISO Copyright Office, Geneva (1992).
4. ISO/TC 184/SC 2 “Robots and robotic devices”; working group WG3 “Industrial safety” is one of five active working groups in this subcommittee. See committee web site:
http://www.iso.org/iso/iso_technical_committee.html?commid=54138
5. ISO 10218 “Robots and robotic devices – Safety requirements for industrial robots”, with parts 1 (“Robots”) and 2 (“Robot systems and integration”), ISO Copyright Office, Geneva (2006, 2011).
6. M. Hägele, W. Schaaf, and E. Helms, “Robot assistants at manual workplaces: Effective co-operation and safety aspects,” In: International Symposium on Robotics ISR 2002 / CD-ROM: Proceedings. October 7-11, 2002, Stockholm, Sweden. Stockholm, 2002.
7. A. De Santis, B. Siciliano, A. De Luca, and A. Bicchi, “Atlas of physical human-robot interaction,” *Mechanism and Machine Theory*, Vol. 43, No. 3, March 2008, p. 253-270.
8. J. Krüger, T. K. Lien, and A. Verl, “Cooperation of human and machines in assembly lines,” in: *CIRP Annals Manufacturing Technology*. 58 (2009), No. 2, p. 628-646.
9. R. D. Schraft, M. Hägele, and A. Breckweg, “Man and robot without separating systems,” In: *World of Automation and Metalworking*. Frankfurt/M.: VDMA Verlag, 2006, p. 4-5.
10. ISO/TS 15066 “Robots and robotic devices – Industrial safety requirements – Collaborative industrial robots”; ongoing standardization project in draft stage and not publicly available at this time.
11. S. Haddadin, A. Albu-Schäffer, and G. Hirzinger, “Soft-Tissue Injury in Robotics,” *IEEE / Robotics and Automation Society*, 2010 IEEE International Conference on Robotics and Automation, Anchorage, Alaska USA, 2010, on DOI - 10.1109/ROBOT.2010.5509854, p. 3426-3433.
12. O. Ogorodnikova, “How Safe the Human-Robot Coexistence Is? Theoretical Presentation,” *Acta Polytechnica Hungarica*, Vol. 6, No.4, p. 51-74 (2009).
13. S. Oberer, R. D. Schraft, “Robot-dummy crash tests for robot safety assessment,” *IEEE / Robotics and Automation Society: 2007 IEEE International Conference on Robotics and Automation*, Rome, Italy, 2007, p. 2934-2939.
14. BG/BGIA Risk Assessment Recommendations according to Machinery Directive – Design of Workplaces with Collaborative Robots, Ed. BGIA – Institute for Occupational Safety and Health of the German Social Accident Insurance, U 001/2009e October 2009 edition, revised February 2011.
http://www.dguv.de/ifa/en/pr/kollaborierende_roboter/index.jsp

How to approve Collaborating Robots - The IFA force pressure measurement system

Michael Huelke, michael.huelke@dguv.de; Jürgen Ottersbach, hans-juergen.ottersbach@dguv.de;
Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA),
Alte Heerstrasse 111, 53757 Sankt Augustin, Germany

KEY WORDS: Collaborating Robots, ISO 10218, ISO/TS 15066, force, pressure

ABSTRACT

In the industrial robot sector, a growing number of workplaces at which people work very closely with robots have been created in the last few years. During such work processes, there is a residual risk of collisions between humans and robots. In the required risk assessment, the loading arising in critical collision processes has to be measured with a biofidelic, i.e. mechanically human-like, measuring instrument. At the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), such a force/pressure measuring instrument has been developed for use in industry. It records and assesses the external overall force exerted by the robot and the local maximum pressure in the area affected by the collision. The measuring instrument has a two-stage compression structure that simulates the deformability of the relevant colliding parts of the body. The inertia and movement behaviour of the human body cannot be directly mechanically replicated with a fixed measuring instrument. This behaviour is therefore flexibly realised in the measuring instrument through correction functions with appropriate software. The KDMG-KOLROBOT force/pressure measuring instrument helps companies to design a workplace with the collaborating robot and set the parameters in such a way that the mechanical loading of the body is confined to the normatively permissible range.

1 INTRODUCTION

In the industrial robot sector, a growing number of workplaces at which people work very closely with robots have been created in the last few years. By combining human abilities and dexterity with the exact and precise execution functions of the robot, highly efficient production can be achieved while reducing the workload of the persons involved. In the safety strategies applied, occupational safety for the persons involved must be ensured by designing the workplace and particularly the robot system in conformity with the relevant standards [1], [2], [3]. Collisions between the human and the machine must be prevented as far as possible. A large number of risk-minimising measures are available for this.

However, in such work processes, there is still a residual risk of collisions between the human and the robot, and "foreseeable misuse" has to be adequately considered in the risk assessment. In connection with the current revision of the standards for industrial robots, the IFA has drawn up new safety requirements specifically for the biomechanical/medical stressing of humans in collisions (see [4] "Recommendations for the design of workplaces with collaborating robots" (EGU), 02/2011, abbreviated in the following as "Recommendations"). These Recommendations specify, among other things, limit values for load forces and pressures that must not be exceeded in these collisions. Furthermore, compliance with them must not therefore entail unacceptable stressing of the body.

If the risk assessment required for a workplace application with a collaborating robot reveals that collisions can occur, the arising loading in critical collision processes in collaborative activities must be measured and checked against the maximum permitted limit values. A biofidelic, i.e. mechanically human-like measuring instrument must be used for this to simulate the biomechanical behaviour of the affected parts of the person's body in the work activity concerned and measure the pressures and forces exerted by the robot.

The IFA is currently running several research and development projects, where technological, medical / biomechanical, ergonomic and work organizational requirements for such workplaces are being investigated (further information at [5]).

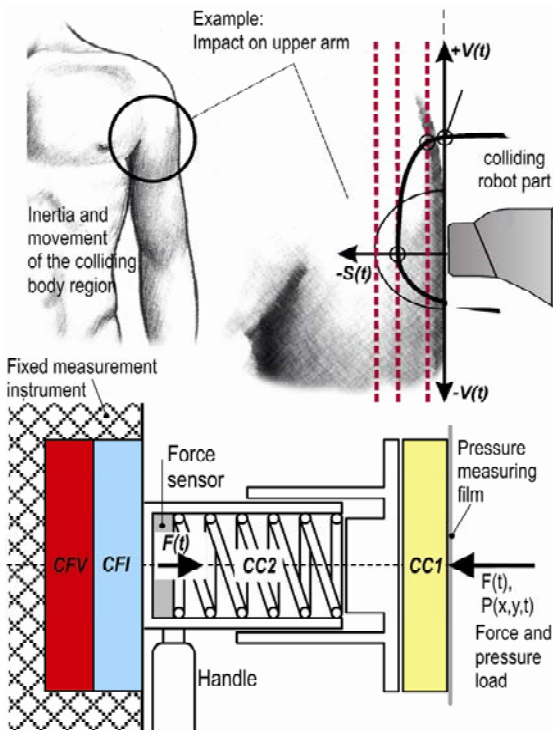
2 DEVELOPMENT OF IFA'S MEASURING INSTRUMENT

For the above-mentioned simulation of biomechanical body behaviour and for the measurement of the mechanical loading, IFA has developed the KDMG-KOLROBOT pressure/force measuring instrument, which can be used for risk assessments in industrial practice. Figure 1 shows the biofidelic measuring strategy and Figure 2 the most important technical features.

The measuring instrument's features take account of the main biomechanical body properties, i.e. deformability, inertia behaviour and movement behaviour of colliding body parts, and measure and assess the external overall force arising from the collision and local maximum pressures in the collision area. Two measuring instrument types are available for body simulation and recording of the clamping/squeezing and impact impulses for flexible use in different collision scenarios (Figures 3 and 4). The dimensions of these instruments are relatively small, so the instruments are handy to use. They can be built up in a variety of ways and thus permit an extensive range of practical applications. This is highly advantageous in view of the goal of the future worldwide standardisation of such biofidelic instruments.

2.1 PHYSICAL AND BIOMECHANICAL PROPERTIES

Force-displacement signals for the deformation of many body parts show a large spectrum of deformation characteristics. Deformation characteristic curves with marked linearity can be observed as well as characteristic curves with a gentle rise at the beginning followed by a rapidly changing, steeper increase in force. Depending on the body point and body posture, the deformability of a body part is also affected by the stiffness of the surrounding area of the body and the connective stiffness of extremities in relation to the trunk. Starting with this complex diversity of deformation characteristics, the biofidelic replication of deformability in a measuring instrument must be reduced to simple mechanical deformation elements to which parameters can be clearly assigned. For the measuring instrument, these deformation characteristics have been derived from measurements with test persons with the aid of linear regression. The characteristic curves are piecewise linear – initial straight line through the origin – with two coefficients of increase.



The procedure was applied to many available characteristics, structured according to the 15 individual body regions described in the Recommendations. From these data, a typical pair of coefficients of increase – CC1/CC2 (Figure 1) – was then specified for each individual body region. In the instrument, the overall deformability is then technically realised with these parameters with the aid of two compression elements one behind the other (CC1: synthetic sheet, CC2: spring). This makes it possible to sufficiently and reproducibly specify the biofidelic deformability of relevant body regions. A more complex model of deformability and also a higher resolution on regions of the body as a basis for technical realisation in a biofidelic instrument are not expedient for applications in industrial practice.

Figure 1. Strategy of the biofidelic measuring instrument with the main biomechanical and measuring properties (CC1 and CC2: compression elements; CFI and CFV: software adaptation of the measurement signals to the inertia and movement behaviour of the colliding body region by correction functions).

If a colliding body part is not trapped, inertia effects usually arise at the point of collision. The body region, e.g. the head or hand-arm extremity, is accelerated by the impact with the colliding body. This body behaviour has a greater or lesser damping effect on the forces and pressures applied and these have to be considered during measurement. Compared to measurements with a firmly fixed measuring instrument with which measurements can be performed precisely and reproducibly, the actual impulse is lower due to the inertial movement of the affected body region. The signals measured with a fixed measuring instrument have to be adapted to this inertia. In cooperation with the Fraunhofer Institute for Factory Operation and Automation IFF in Magdeburg, correction functions have been systematically determined for the inertia behaviour of certain body points (individual body regions) and typical body postures by means of pendulum tests on test persons [6]. The damping effect of body inertia is therefore accommodated with a correction function – CFI (Figure 1) – in the software evaluation of the measured collision impulse. By defining the affected body point and body posture on impact, the evaluation software automatically defines a correction value to take account of the real inertia behaviour and thus to adapt the measurement signals (Figure 3, 4).

A further correction function – CFV (Figure 1) – takes account of the effect of any collision speed of the body part in the collision. Compared to measurements with a firmly fixed measuring instrument, the actual collision impulse is greater with a movement component of the colliding body part. If a collision speed of the body point at the time of impact is given, the evaluation software automatically defines a correction value to take account of the real movement behaviour, and the measurement signals are again adapted accordingly.

2.2 MEASURING PROPERTIES OF THE MEASURING INSTRUMENT

The total force and the pressure distribution are monoaxially measured with the two types of measuring instrument. The force measurement range is 0 to 300 N. The force signal is recorded by means of a logger with a sampling frequency of 25 kHz. The maximum measuring time for this can be up to 40 s. The force signal is filtered with a CFC 1000 Butterworth low-pass filter conforming to SAE J211 (specification from automotive vehicle testing). In the force evaluation, the force signal is investigated with algorithms for impacts and clamping/squeezing. To determine clamping/squeezing, a sliding mean with a time window of 0.5 s is employed, which is maintained for the entire measurement signal. Clamping/squeezing is given if the spread of the force values in such an interval is ≤ 5 N. From these intervals, the most critical clamping/squeezing effect is identified as that with the largest mean force value. The clamping/squeezing effect is then deemed acceptable if this mean is smaller than or equal to the corresponding limit value for clamping/squeezing force (CSF) given in the Recommendations.

Signal portions that lie outside the intervals with clamping/squeezing are then investigated for impacts (peaks). A maximum peak calculated in this way is then interpreted as an acceptable load if the peak value is in turn smaller than or equal to the corresponding impact force limit value (IMF) given in the Recommendations.

Pressure measurement is performed with thin pressure measuring films with geometrical and temporal pressure resolution. The required geometrical resolution of the pressure distribution measurement depends on the shape of the colliding object and its stiffness and has to be selected to suit the specific situation. A resolution of less than 1 mm² makes no sense on the basis of experience to date and is therefore defined in this measuring instrument as the limit resolution. By using different film types, it is possible to gradually determine the pressure-critical range in the collision area and hence the required geometrical resolution of the pressure elements. For time-discrete measurements, the single pressure sensor time signal is also filtered with the CFC 1000 Butterworth low-pass filter conforming to SAE J211. On the same principle as for force evaluation, the pressure distribution measurements are investigated algorithmically for impacts and clamping/squeezing and assessed.

The impact or clamping/squeezing faces of the measuring instrument modules are flat in the standard version. The flat surface measures 160 x 160 mm, and a further attachable surface of 160 x 250 mm is optionally available. Other surface shapes, however, are also possible.

2.3 TECHNICAL REALISATION

An overview of the measuring system currently realised at IFA is presented in Figure 2. It has a modular design and has two different biofidelic measuring instrument types: instrument 1 with a piezoelectric sensor and large axial impact surface and instrument 2 with a DMS sensor and external fork configuration for narrow gap widths. With the design features of these two instrument types, it is possible to simulate many forms of collision in industrial practice.

Type 1 instruments have a two-stage compression structure of plastic synthetic elements and springs to simulate deformability at the relevant body points. Depending on the individual body region concerned, such elements and springs are employed with their linear coefficients, as specified in the requirements for the individual body region. The force is measured with a piezoelectric force sensor behind the compression elements against a fixed position. A data logger is available to record the data. After the test, the force data are transferred to the PC. The entire measurement and evaluation system is operated entirely with a specially developed measurement and evaluation system via a mini-PC. Figure 2 (lower right corner) shows instrument type 2 in two variants with different collision surfaces (flat and finger-shaped). On type 2, compression is brought about in the lateral fork configuration, which can be assembled in different ways to yield the shapes required for specific applications.

At present, two different pressure measuring sensors are available: Fujifilm pressure measuring films and TEKSCAN pressure measuring films. The Fujifilm pressure measuring film is a pressure peak measuring system with a geometrical resolution of 200 dpi. After use of the Fujifilm pressure measuring film, the pressure-exposed film, showing a pressure-related red density in the collision area, is scanned with a resolution of 200 dpi and the individual pixels converted into pressure values. Different film types with different measuring ranges can be used. A suitable scanner and the associated software from Fujifilm are included in the system. The TEKSCAN pressure measuring film system is a time-discrete pressure measuring system, and different films with different geometrical resolutions and measuring areas down to less than 1 mm² can be employed.

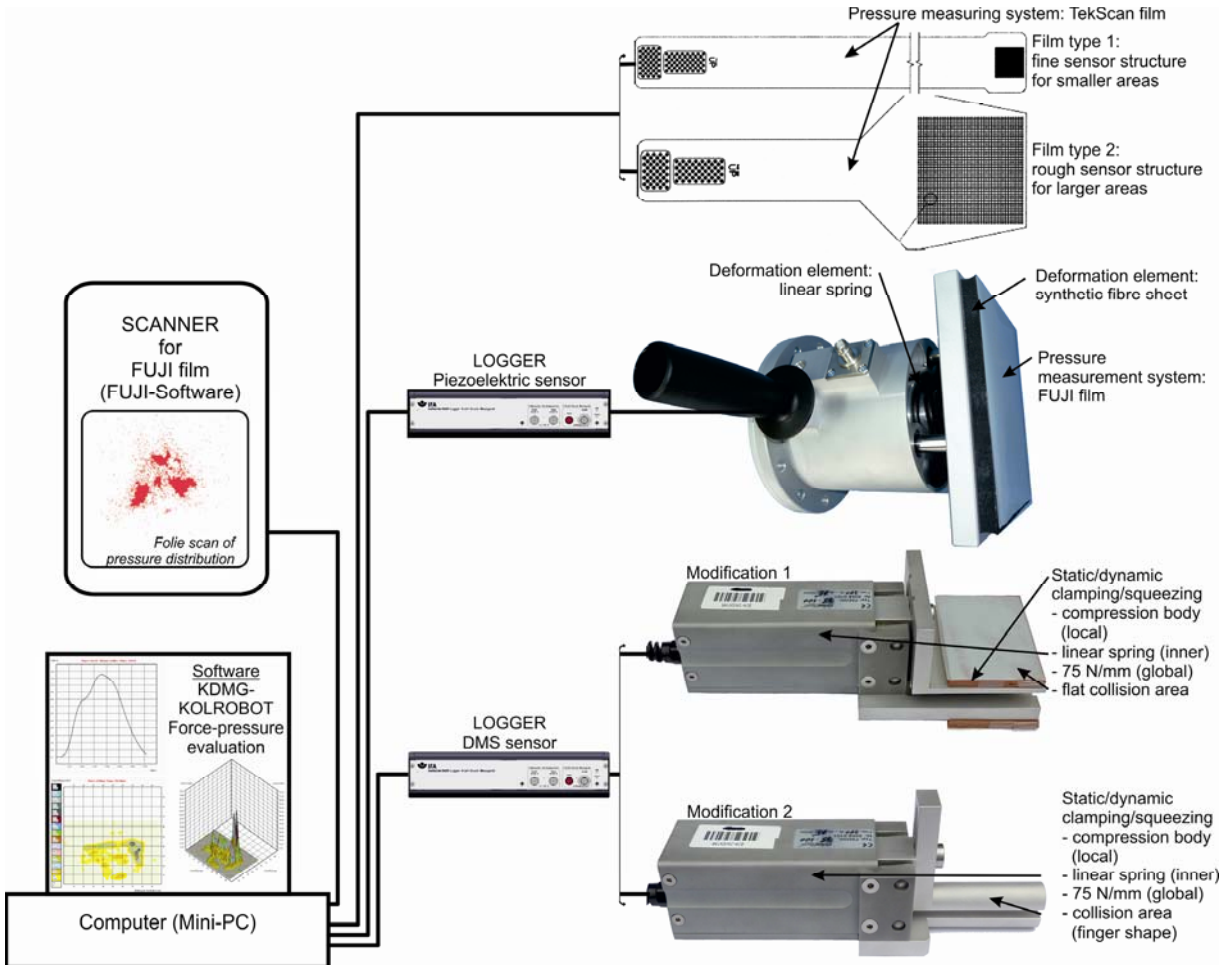
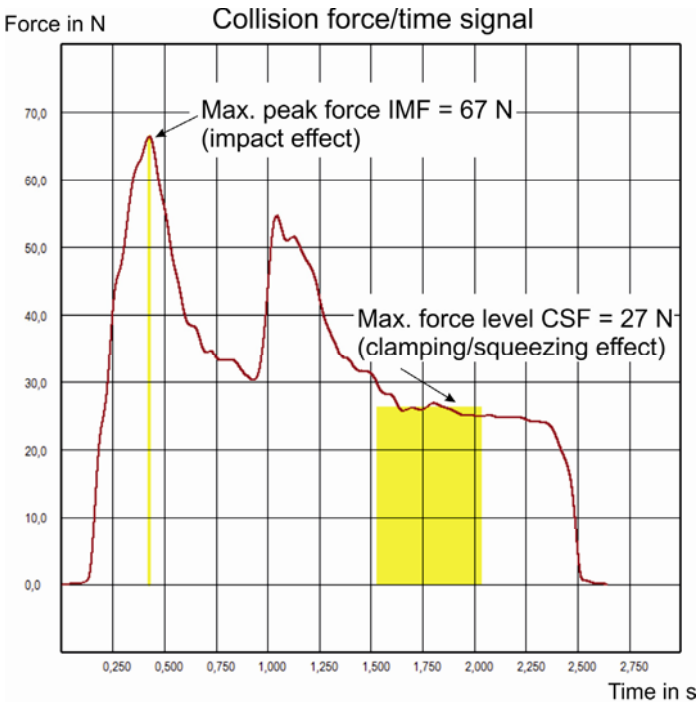


Figure 2. Technical components of the instrument with an overview of the functions of the overall measuring system

4 MEASUREMENT EXAMPLES



Figures 3 and 4 show examples of force and pressure measurements. Figure 3 shows a force-time curve lasting for about 2.5 s. The signal curve shows two successive force peaks and a plateau characteristic at the rear. The measurement signal was evaluated using the method described in paragraph 2.2. The two signal peaks were accordingly identified as impact forces, and the maximum peak value of both of them was checked against the permissible limit value. In this case the simulation replicated an impact in the chest region, for which an impact force limit value of 210 N is applicable. The maximum first peak for the force signal (IMF) of 67 N can therefore be interpreted as an acceptable load. In the rear portion of the signal, several intervals of 0.5 s were found in which the force spread was ≤ 5 N. The interval with the highest mean (CSF) of 27 N is from 1.5 s to 2.0 s. The associated clamping/squeezing risk is assessed with the permissible limit value of 140 N for the chest region. Here again, the force of 27 N can be deemed acceptable.

Figure 3. Force-time signal of a critical collision impulse on a specific body part

As a further measurement example, Figure 4 shows the force curve and pressure distribution for clamping/squeezing of the simulated hand between two gripper fingers of a robot tool. Clearly visible in the pressure distribution are the decline in loading with increasing distance from the clamping position and the design of the gripper fingers. Here again, the evaluated values for impact and clamping/squeezing were determined and assessed along with the maximum pressures.

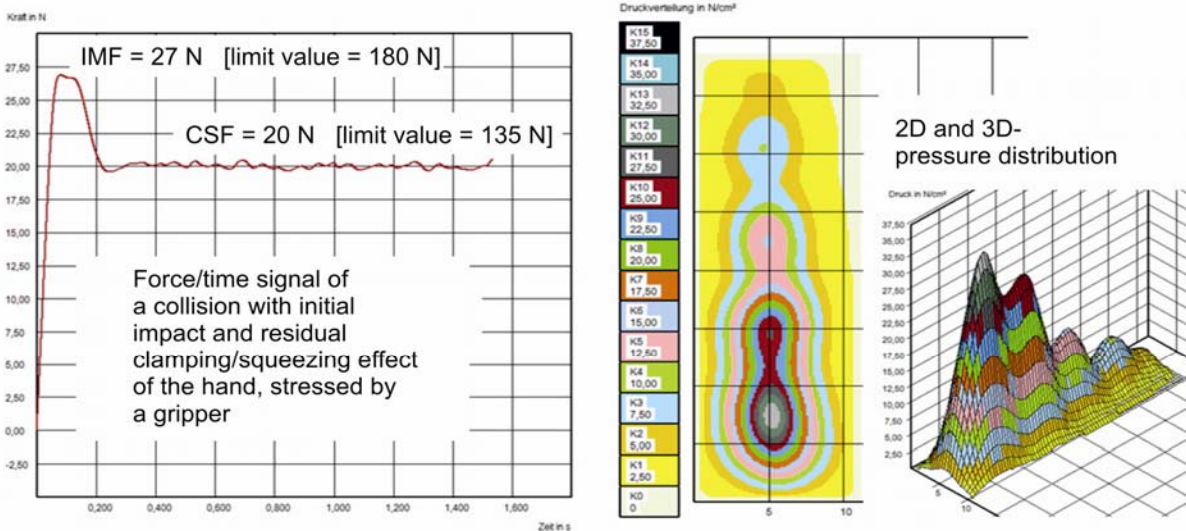


Figure 4. Force-time signal and pressure distribution

5 CONCLUSION

Thanks to its design with the measuring and evaluation principle on which it is based, the KDMG-KOLROBOT measuring and evaluation instrument of the IFA takes sufficient precise account of the mechanical/biomechanical properties and movement behaviour of differentiated body regions in structured activity postures. Developed in accordance with the specifications for critical collision processes given in the "Recommendations for the design of workplaces with collaborating robots" (EGU), 02/2011 [4], it represents a good basis for a standardised reproducible measuring method. The instrument can thus be used for testing the safety requirements demanded in standards at the current technical level. This is confirmed by ongoing tests and certifications of collaborating robots. Owing to its modular design, its development is open-ended and further instrument types can be integrated. This also applies to its measuring characteristics and components.

Given appropriate technical design of the workplace or suitable parameter assignment for the robot system, the instrument can be used for reducing harm to the body in the event of any collision processes beneath the limit loads given in the Recommendations. This measuring instrument design based on the loading model given in the Recommendations can accommodate the research findings [5] and changes in standards [1], [2], [3] expected in the coming years. In the medium term, KDMG-KOLROBOT is to be built under licence and marketed by external measuring instrument manufacturers.

6 REFERENCES

1. Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots (ISO 10218-1:2011)
2. Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robot systems and integration (ISO 10218-2:2011)
3. Robots and robotic devices - industrial Safety requirements Collaborative industrial robots (ISO/TS 15066 in draft)
4. Ottersbach J. et.al., *BG/BGIA risk assessment recommendations according to machinery directive - Design of workplaces with collaborative robots (edition 2011)*, Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), Sankt Augustin, 2011, http://publikationen.dguv.de/dguv/pdf/10002/bg_bgia_empf_u_001e.pdf
5. Internet portal "Collaborative Robots": http://www.dguv.de/ifa/en/fac/kollaborierende_roboter/index.jsp, Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), Sankt Augustin, 2012
6. Behrens R., Elkmann N, Ottersbach H. J., *A Contribution for Standardized Risk Assessment: Examination of Constrained and Unconstrained Human-Robot-Collisions*, 2012 IEEE International Conf. on Intelligent Robots and System (IROS), Submitted for Proceedings of Workshop on Safety in Human-Robot Coexistence & Interaction, October 2012, Vilamoura, Portugal

Development of a Self-Check Sheet for Safety Design of Human-Collaborative Robots

Hiroyasu Ikeda

National Institute of Occupational Safety and Health, Japan (JNIOSH), 1-4-6, Umezono, Kiyose, Tokyo, Japan
E-mail ikeda@s.jniosh.go.jp

Kuniyuki Niwa

Japan Certification Corporation, Osaka, Japan

Yuichiro Shimizu

Japan Quality Assurance Organization, Tokyo, Japan

KEY WORDS: Check sheet, Safety design, Human-collaborative robot, Concept verification

ABSTRACT

In order to ensure the safety of human-collaborative robots, protective measures based on safety control should be taken. Into the safety control system of such robots, functional safety concept should be introduced. Design and development process including this safety control system starts with concept analysis. In preparing safety requirement specifications, safety concept specifications and functional safety plans, which are all essential to the concept analysis, the authors have just developed a self-check sheet for use by robot designers in self-checking these documents. The self-check sheet consists of 3 parts. In a question form, the 1st part describes check items on safety concept to be checked in the designing stage, and the 2nd and 3rd parts describe check items on safety detailed specifications of hardware and software, respectively. The degree of attainment of each check item is to be answered in 3 levels. The answer to each question in each part of the self-check sheet is scored for each field. The total scores are displayed in a radar chart, and the degree of attainment is judged for each field. The self-check sheet was used on trial as a concept verification tool in designing a number of human-collaborative robots.

1 INTRODUCTION

To human-collaborative robot providing service to humans, it is difficult to apply safeguarding by means of “segregating humans from robots” in use for conventional industrial robots. Also, in order to carry out the objective task of a human-collaborative robot, since intrinsically controlling the force and speed of the robot has limitations, there is no choice but to introduce safeguarding based on safety control. Therefore, robots of E/E/PE (electrical/electronic/programmable electronic) safety control system are requested to meet the safety requirements specified in the functional safety standards (e.g., IEC 61508).

In the robot developing process under the functional safety standards, it is necessary to verify the conformance of the process to the safety requirements. This verification has 2 stages like that of the development process for general mechanical equipment: to verify the safety concept in the course of robot designing, and to verify the conformance of robots in actual operation to the safety requirements and standards for relevant tests. Robot designers have to prepare various relevant documents for the purpose of such verification, but since they have a lack of understanding of the functional safety standards as a reason, it is not easy for them to complete just enough documents. Although they can have their documents checked by some relevant certification authority, professional or consultant, if they are not qualified for documentation on their own, it is impossible to expect the acceleration and cost reduction in their robot development.

In view of the above, the authors propose a self-check sheet composed of 3 parts designed for robot designers to check the safety concept specifications and safety detailed specifications in the first stage of verification for the omission of required information and to determine how much each safety requirement can be fulfilled. The

self-check sheet is so structured that they can automatically score and evaluate the degree of attainment so that unattained fields can be presented to robot designers in order to support the appropriate safety designing of robots and the smooth proceeding to the 2nd stage of the verification.

2 CONCEPT ANALYSIS AND REQUIRED DOCUMENTS IN THE ROBOT DEVELOPMENT PROCESS

The robot development process including the safety control system, into which the functional safety concept has been introduced, is interpreted as a basic life-cycle process. In each of the development phases ranging of this process from designing to operation and maintenance, documents related to plan, specification, test and verification are prepared, and development is carried forward in accordance with these documents. Figure1 shows the robot development phases based on the functional safety and the relevant documents corresponding to each phase. In the first-half design phases, as a task of analyzing and verifying the design concept, the basic and detailed specifications for safety are determined after planning the development (1st stage of verification). In the second-half phase, based on the results of test on the manufactured robot, the safety validation is evaluated and certified (2nd stage of verification).

In Figure 1, at the 1st stage of verification of the first-half design phase, which is called “concept analysis,” robot designers have to clarify the safety requirements of the target robot, and prepare for the safeguarding to be implemented to satisfy the safety requirements, the system and process for implementing the safeguarding, and document such safeguarding and its implementing system and process. Particularly, the relevant documents listed below are taken important when the 2nd stage of verification is assumed to be certified, their substantial contents and quality are required:

- a. Functional safety plans: Control of relevant personnel, organizations and technology
- b. Safety concept specifications: Safety design concept and safety policy
- c. Safety requirement specifications: Required specifications for safety requirements

For the safety control and the relevant document control, as long as they are conformable to the quality management standards (e.g., ISO 9001), the contents, format, etc. of the documents prepared in the conventional, ordinary development process may be used. For the following specifications describing the safety detailed specifications,

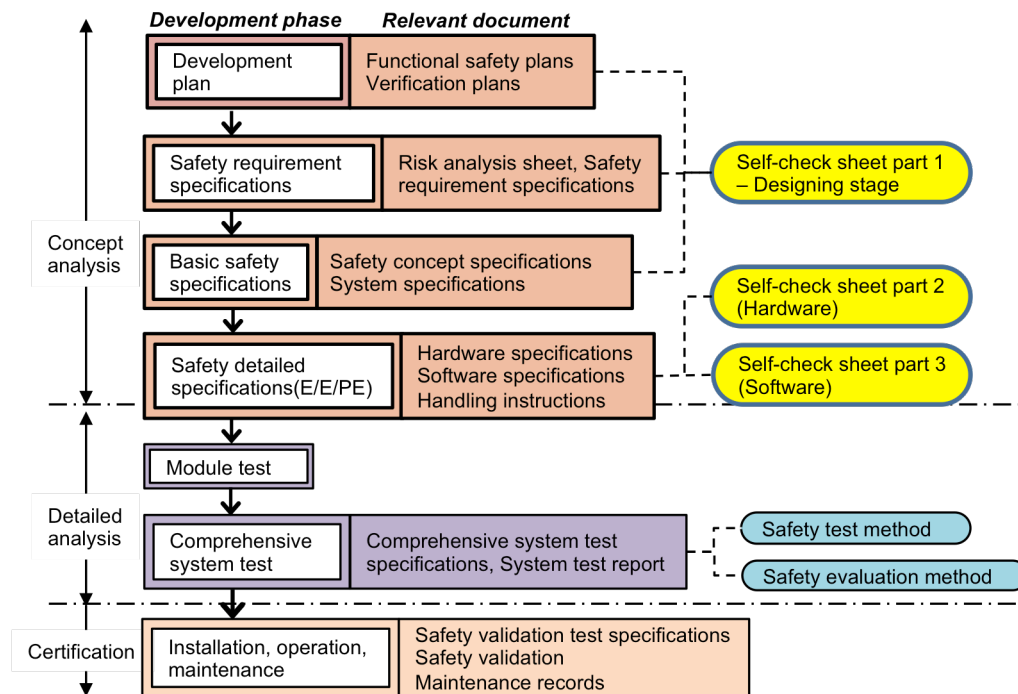


Figure 1 Correspondence of the functional safety design phases / relevant documents with the check sheets

through some of them are contained in the detailed analysis, it is necessary to select just enough safety requirements and sufficient description:

- d. Hardware specifications: Safety requirements under IEC61508-2 (including the intrinsic safety design requirements)
- e. Software specifications: Safety requirements under IEC61508-3

In order for robot designers to prepare the above 5 different documents of importance, they have to understand the contents of the standards, including the functional safety standards, and comprehend all descriptions of the documents.

3 CREATION OF A SELF-CHECK SHEET

3.1 How to Check and Judge with the Self-Check Sheet

The authors have created a self-check sheet consists of 3 parts as a tool for robot designers to self-check for the excess/deficiency of the requirement information indicated in the above 5 different relevant documents and the correctness of their descriptions in the course of robot designing and development. Figure 1 shows the correspondence between each part of the self-check sheet and the relevant documents. The 3-part self-check sheet is positioned to check the safety concept analysis contents and the required documents aiming at the certification of the safety concept, and to check the safety requirements of the hardware and software that can satisfy the safety integrity level SIL2 or SIL3 specified in the functional safety standards.

Each part of the self-check sheet is created on Microsoft Excel, the items to be checked in the designing stage and in the embodiment stage are described as questions, and all questions are classified by category. In checking the self-check sheet, a common rule is that the degree of attainment on each question is defined as shown in Table 1, and when the applicable check mark is selected and entered, the scorers are automatically aggregated for each category under the scoring rules described in Table 1. Here, a check mark of “N” means that the question itself is not applicable due to robot type or function, and therefore excluded from scoring.

The grand total score of the self-check sheet is shown on a radar chart, where the degree of attainment of each category is linked together for quick comparison. The total score of a category is judged OK if it is equivalent to 80% or more of the full score. Since the judgment of a category has nothing to do with that of the other categories, the chart can be used as a scale of the degree of attainment of each category or to grasp weak-point items.

Table 1 Checking with the self-check sheet and the rules for scoring

Check code	Progress in “checking”	Basic rules for scoring
A	Checking completed (Questions almost satisfied)	Point×1
B	Checking under way (Questions partly satisfied)	Point×0.5
C	Checking not yet started (Questions hardly satisfied)	Point×0
N	N/A	Point deducted from the full points of each category

3.2 Outline of the Self-Check Sheet (1)

In the self-check sheet part 1, as shown in Table 2, questions are about a total of 59 items in 6 categories mainly in the design concept. Some questions excepted from the self-check sheet are shown in Figure 2. A question with the colored checking column affects the score of other questions (e.g., Points allocation is affected according to the check code). The questions of the categories II and III refer mainly to the requirements of the basic machine safety standards ISO 12100 and IEC 60204 and industrial robot safety standard ISO 10218, and the questions of the categories IV and VI are cited mainly from the standard of IEC 61508.

Table 2 Main check items of the self-check sheet part 1

No.	Category	Main question item	Purpose (excerpt)
I	Safety securement policy	Robot configuration, safety design policy, roles of man and robot	To check the preparation for design considering safety
II	Risk assessment	Usage environment and condition setting, implementation system, risk reevaluation	To check assumed using conditions, to check the risk reevaluation considering risk reduction effect
III	Risk reduction	Intrinsic safe design, protective devices (stop, control, human body detection), functional safety introduction, additional protective measures, residual risk handling, management policy	To check the hazard control on the design drawing, to check protective measures and their functions, to check the usage information provision to users
IV	Safety management	Organizational structure and management, responsible system, documentation, management, supervision	To clarify the organization and personnel positioning and responsibility, to check the operation and information control
V	Document management	General documentation, management plan	To check basic requirements common to all documents
VI	Documents on safety-related operations	Required information, safety request related plans and specifications, hardware/software-related test plans and specifications	To check the documentation of information, to check the required documents

III Risk reduction

No	Item	Purpose	Question	Check	Point	Remarks	Score
9	Risk reduction method	Check of standards with which risk reduction method is conformable	1 Is risk reduction implemented as per 3-step method under ISO12100?	A	3		3
			2 Are other standards (including internal standards) referred to? Describe the standard names and numbers in the remark column or in a separate sheet together.	N	1		
⋮							
(Weighted point) × (Ratio corresponding to check code)							
18	Protective equipment (Stop)	Check of protective means applied in order to secure safety by stopping	1 Is a man-attended emergency stopping device installed?	A	2		2
			2 Is protective stopping (by interlock) function provided?	B	2		1
			3 Is unintended start after stopping considered?	C	2		0

Figure 2 Entry example for the self-check sheet part 1 (excerpt)

The grand total score of each category is judged on a radar chart. The grand total score equivalent to 80% or more is judged A, and grand total score equivalent to 40% or more but under 80% is judged B. Only the grand total score judged A is determined as OK. The results of using the self-check sheet for robot designing are shown in Figure 3.

3.3 Outline of the Self-Check Sheet (2)

The self-check sheet part 2 treats the hardware related to safety control for robots, assuming the single to redundant architectures. For this purpose, whether the safety integrity levels SIL2 and SIL3 of IEC 61508 have been realized is checked by questioning. However, since the required safety requirements vary according to the safety control system,

Fig.3 Angular velocity variation during stopping and total travel distance

Then the safe condition during the upward process is shown with the relations (3).

$$\int_t^{t+T_{stotal}} V_m(t) dt + P_m(t) > 360(\text{deg.}) - (3)$$

As shown in Fig.3 , "Tstotal" is a parameter that consists of the reaction time(Tr) of the braking system and the braking time . "Tstotal" must be considered the worst case. The braking time is usually proportional to the speed of the press machine. But the reaction time(Tr) of the braking system is variable by the air pressure of the mechanical brake release. The worst case of "Tstotal" is usually obtained by the measured stopping characteristics at highest air pressure of the mechanical brake release.

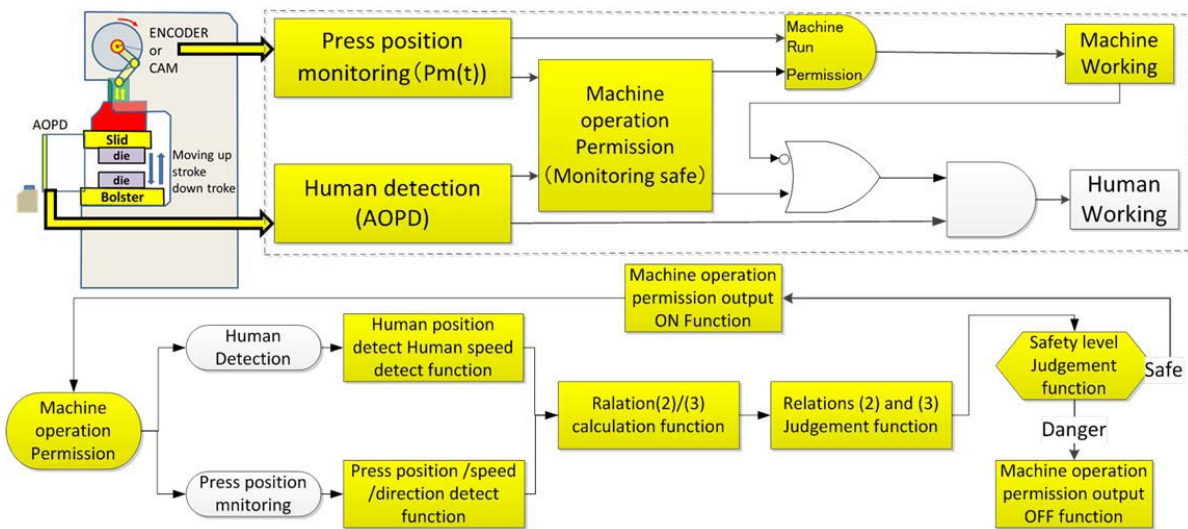


Fig.4 Function block of the Press safety monitoring system

Fig.4 is the Function block diagram of the Press safety monitoring system that we considered to achieve the safety collaboration work of a machine and a human. Safety category of each function in Fig.4 needs SIL3 IEC62061 [3] . Because the collaboration work of the Press machine. Safety category of each function in Fig.4 needs SIL3 IEC62061, because severity of harm from the hazard in the tool area of the Press machine leads to a serious injury.

4 Effect and Evaluation of the concept of the Press Safety Control

If this safety control for collaboration work of press machine and person based on safety level defined by position and velocity vector is applied to the press machine, the improvements can be anticipated not only in the safety but also in the productivity are expected. The followings are the improvements on the present press machine.

- 1) The safety condition will be kept with all press operation mode if the control system shown with Fig.4 is always applied to all the press modes and situations.
- 2) Especially, the press machine can reduce the risk of the "overrun" , because the ability to stop at TDP is monitored at all the time during the collaborating operation.
- 3) The muting position automatically changes by detecting the dynamic safety distance, and moreover by utilizing this control system the productivity will improve at higher speed because of the increase

A.2. Software safety requirement specifications - Software structural design						
No	Item	Purpose	Question	Check		Point
				SIL2	SIL3	
1	Failure detection	Failure detection/ diagnosis	Is failure detection implemented in the minimum unit or single function unit of software?			
			1 Is the self-diagnosis method used for failure detection?			
			2 Is the redundant method is used for failure detection?			
			3 Is the diversity method used for failure detection?			

Figure 5 Setting example for the self-check sheet part 3 (excerpt)

3.4 Outline of the Self-Check Sheet (3)

The check sheet part 3 covers the safety requirements related to the software. For the techniques specified by IEC 61508-7, those items that are “highly recommended” on the safety integrity levels SIL2 and SIL3 are questioned. When the SIL of the software set as a goal in relation to the hardware is selected first, only those questions corresponding to the applicable SIL are scored. Some excerpts of the questions in the check sheet are shown in Figure 5.

The self-check sheet of this part scores 10 categories of the software, and the judgment results are shown on a radar chart (Figure 6).

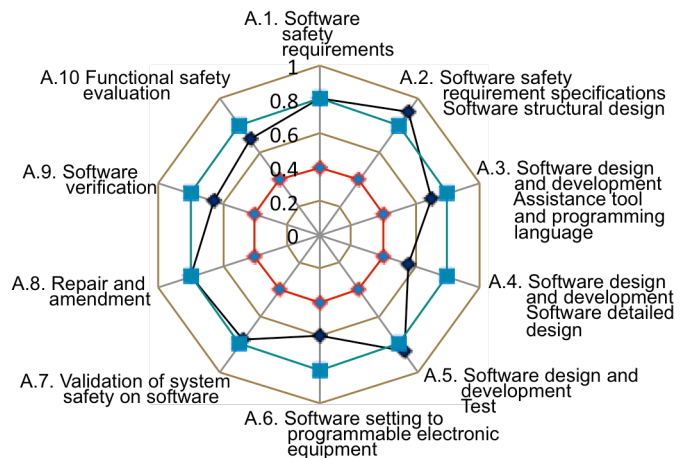


Figure 6 Categories and judgment result example of the self-check sheet part 3

4 TRIAL VERIFICATION OF LIFE-SUPPORT ROBOT CONTENT

The created self-check sheet part 1 was provided to designers of 5 different life-support robots of 3 types (autonomous mobile type, boarding type, wearing type), and had them self-check the degree of attainment as to the safety concept at the time. Although the final judgment results varied due to difference in the degree of preparation of robot development system, the designers were able to identify the category at which they were not good in going clear the safety concept verification in person. Also, in an attempt to verify the safety of the life-support robot beforehand, simulated conceptual verification was implemented, and based on the judgment results from the self-check sheet, the authors were able to provide pieces of useful advice to robot developers. Although there are still a small number of cases of applying the self-check sheet, the authors have confirmed its effectiveness.

5 POSTFACE

The self-check sheet created this time can be used as a tool for life-support robot designers to verify the safety concept in person. The authors will continue to amend and revise the self-check sheet of each part and provide the up-to-date self-check sheet to robot designers as a useful tool.

This work is a part of “Project for practical applications of service robots” by New Energy and Industrial Technology Development Organization.

Serial Kinematics based Motion Simulator - Evaluation of safety of the Passenger

Karan Sharma, Sami Haddadin, Johann Heindl, Tobias Bellmann, Sven Parusel, Tim Rokahr, Sebastian Minning
and Gerd Hirzinger

Robotics and Mechatronics Center, German Aerospace Center (DLR), 82234 Oberpfaffenhofen, Germany
Tel. +49 (0)8153 28 1080, Fax +49 (0)8153 28 2243, Email karan.sharma@dlr.de, Web <http://www.dlr.de/rm/en>

KEY WORDS: Accident investigation results, Safety related software, Robocoaster, Motion Simulators

ABSTRACT

Serial kinematics based motion simulation is a recent development and was ushered in by the introduction of the KUKA Robocoaster in 2001. The Robocoaster employs a 6-DoF industrial robot (KUKA KR-500) equipped with 2 seats at its tool centre point (TCP). Since 2001, the Robocoaster (and derived systems) has been a subject of active research and has been successfully transferred to the amusement industry. DLR has developed various iterations of the Robocoaster: In 2004-05, we presented the 'KUKA Mars Mission'; this was the first time visual cues were incorporated with the Robocoaster system. Next, we developed the 'RoboSim 4-D' simulator that addressed the shortcomings of the earlier efforts, was lower in cost and had improved safety features. This version is in-use (as an offline simulator) at several amusement parks. The latest version, called the 'DLR Robot Motion Simulator' (DLR-RMS) includes an additional linear axis at the base of the robot; which makes the setup a 7 DoF simulator. This version is used for both, online and offline simulations.

Adaptation of an industrial robot into a motion simulator introduces a new set of challenges with regards to human and robot safety (i.e. prevention of damage to the setup as a secondary safety aim) and hence an appropriate safety infrastructure was deployed. To validate the potency of this system, it was subjected to several tests which involved effectuating high accelerations at the TCP by inducing sudden braking. The resulting accelerations were initially measured using an inertial measurement unit (IMU) and later, using an Anthropomorphic test device (ATD) commonly known as 'crash test dummy'. In this paper, we present the finding of safety analysis tests undertaken with an ATD placed in the simulator cell. We focus our attention to critical motions (e.g. flexion, inflexion etc.) of the head-neck region and also illustrate the software features such as the 'watchdog application' which offers extra functionalities that complement the existing safety features.

1. INTRODUCTION

While developing this system we've encountered numerous challenges pertaining to passenger safety. We've made some efforts to address these issues and these are highlighted in the following sections.

We have been developing Serial Kinematics based Motion simulators since circa 2004 and have been working with several different iterations of these motion simulators. The current iteration features a linear axis and new simulator cell design which mandates a new safety setup. This setup differs to a larger extent from the older setups, but some of the safety features developed and implemented on the older iterations are also used in this version. The primary goal of our safety setup is to protect the passengers and other people in the vicinity of the simulator. As a secondary goal, the setup should also prevent the simulator from inflicting any self-induced damage.

We can divide the safety setup into two broad categories: (a) *external* and (b) *internal* safety systems. The term *internal* system refers to the checks that are implemented within the simulator software setup and *external* systems are checks/monitors which are not part of this setup. Some of the *external* safety features are listed as follows:

- *Workspace and its environment*: fence around the workspace, auto-stop when the workspace is intruded, energy absorbing hardware stops at the axes of the robot, emergency stop (e-stop) buttons, position sensors near the ends of the linear axis etc.
- *Control room*: safety management console to monitor the simulator and to intervene in the case of emergencies.
- *Simulator cell*: smoke detectors, temperature sensors, intercom system, ventilation through fans, five-point seatbelt, sensor to detect if the seatbelt is 'locked', 'abort simulation' button etc.

An elaborate introduction to the safety systems, design of the simulator cell etc. is available in one of our earlier publications [1].

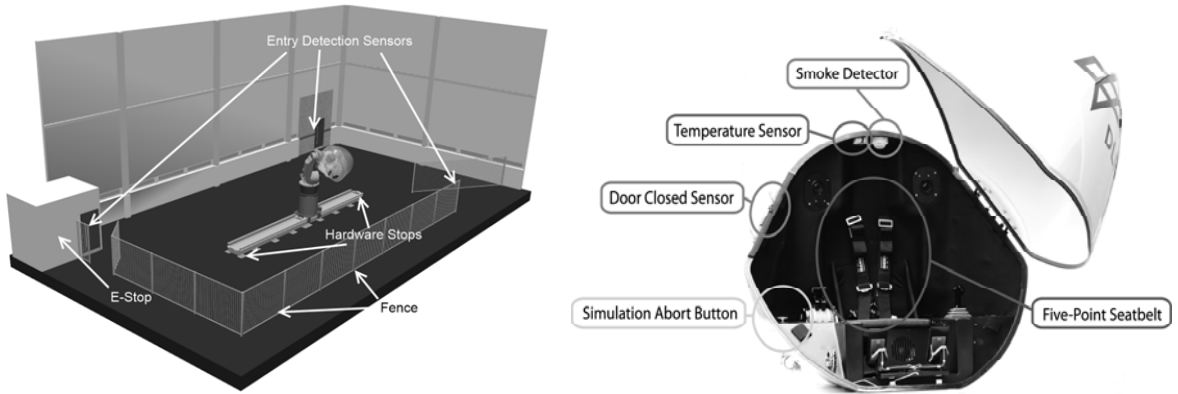


Figure 1. Left: schematic showing the workspace of the simulator and its environment. Right: the gondola.

The simulator software setup can be sub-divided into three major categories:

1. *Vehicle simulation:* simulation of kinematic and dynamic behaviour of the vehicle (car, aeroplane etc.)
2. *Visualization of the environment:* visualization and projection of the vehicle and its environment.
3. *Motion planning & execution:* generation of the trajectories from passenger input (e.g. Pilot joystick) and communication with the robot control system.

Pertaining to the safety of the simulation system, *motion planning & execution* section of the system software is the most critical. Most industrial robots use propriety software which serves as the programming interface and monitors the critical scenarios encountered during operation. In our setup we bypass certain aspects of this propriety software and interact at a lower level with the robot using the KUKA-Robot Sensor Interface (KUKA-RSI) framework [2]. This allows us to generate trajectories (instantaneously) on an external PC and then command them to the robot, over an Ethernet connection. The cost of this flexibility is that this framework is deprived of several safety features which are included with propriety software.

This necessitates the development & integration of safety features into the *Motion planning and execution* software. These features are from here on collectively referred to as the *watchdog application* [1] and they act as an additional safety layer monitoring for critical scenarios. These features are discussed in detail in the following section.

2. WATCHDOG APPLICATION

In addition to the issues discussed in the last section, the *watchdog application* also aims to address the issue of passenger comfortability. This is an interesting issue and requires deep and thorough analysis and we consider it to be of paramount importance in a motion simulator. Our motion simulator is derived from an industrial robot whose safety setup was designed for an industrial setting and not for human transport. This implies that the incorporated e-stops and brakes can lead to sudden decelerations of the tool center point (TCP), where the passenger is seated. To address this, we have incorporated certain features in the *watchdog* that allow us to control the rate of braking in emergency situations and bring the simulator to a halt slowly, thereby improving the ‘comfortability’ in case of sudden stops. This and other software based features are elaborated in table 1:

Table 1. Elaborating different types of Stops and Checks

<i>Brake- all axes</i>	-calculates the current velocity of the axes and achieves braking by applying a velocity in the opposite direction. Once all the axes have stopped moving, it returns command to the software and communication between the robot controller and external PC is maintained.
<i>Halt motion</i>	-sets an internal system parameter which in turn forces the robot controller to engage the mechanical brakes, bringing the robot to a sudden halt. This is equivalent to pressing the e-stop found on robot systems. As a result of this brake, the execution of all programs is stopped and the communication between the robot controller and external PC breaks down.

<i>Bring robot to rest</i>	-is similar to <i>Brake-all axes</i> , but the braking acceleration applied here is less in comparison to <i>Brake-all axes</i> . So, the robot is brought to a stop at a much slower rate. This is more 'comfortable' for the human. The communication between the robot controller and the external PC is maintained.
<i>Acceleration check</i>	-checks if the calculated motion profile exceeds the maximum permitted acceleration values. If the limits are exceeded, the robot is brought to a stop using <i>Brake- all axes</i> .
<i>Hardware limits check</i>	-using the current position and velocity of the robot axes, calculates the braking distance required to safely bring the robot to stop e.g. if the robot axes moving with very high velocity near the joint limits; this feature executes a brake in anticipation of a scenario which can be critical to the passenger and robot safety.

The software features in the table 1 in tandem with other external safety features, are entrusted with ensuring passenger and robot safety. During normal simulator operation these features are active and should abate most situations that are critical to passenger safety. However, for comprehensive safety analysis & planning; it is important to examine situations involving malfunctions relating to these and other safety features. These situations would involve sudden decelerations being exerted on passenger due to emergency braking (e-stop). We undertook several experiments, where we attempted to recreate these critical situations. These experiments and their results are presented in the following sections.

3. SAFETY ANALYSIS

3.1 Preliminary Tests

The simulator was subjected to tests, where the axes were driven at high velocities and/or accelerations. During the course of these motions, an e-stop was triggered to generate sudden decelerations. These tests were carried out using different motion profiles and an inertial measurement unit (IMU) (mounted near the usual head position inside the simulator cell) was used to measure the decelerations resulting from the e-stop. More information on these tests and a discussion of the results is presented in [1].

One of the tests involved driving the Axis 2, 3 and 5 of the robot to their maximum velocities (using a sinusoidal trajectory for each axes) and subsequently triggering the e-stop (Figure 2, *left*). By executing this test, we aim to generate a maximum Cartesian velocity in the passenger's cranial direction.

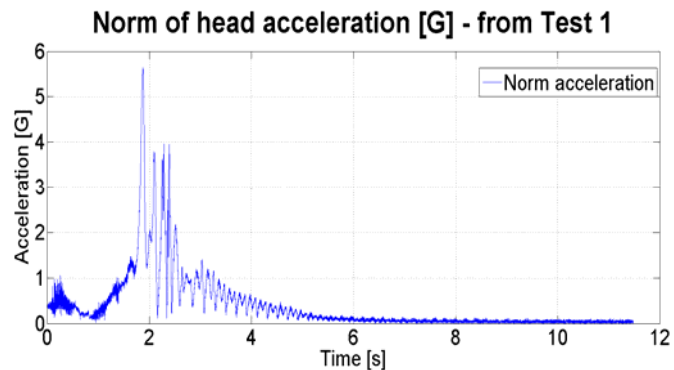
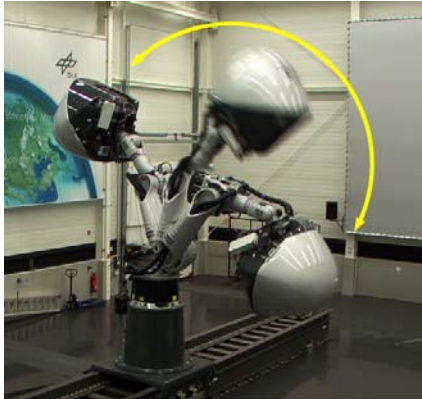


Figure 2. *Left:* Movement of the Simulator during test from Sec.3.1 and Test 1&2 in Sec. 3.2.2. *Right:* Norm of the acceleration data from the head sensor (excludes acceleration due to gravity) during Test 1 from Sec.3.2.2.

The peak value of acceleration recorded during the emergency stop is 3g (including gravity). This is within the 5g (harmless acceleration) limit for whiplash related injuries, as defined by a German jurisdiction on the same [3]. But, in our opinion the results of these tests are not truly representative of the accelerations that would've been

experienced by the passenger, as the sensor is mounted on the simulator cell. This way the effects induced by the motion of head relative to the cervical spine can't be analyzed correctly. A proper analysis mandates the usage of an anthropomorphic test device (ATD) (popularly known as 'crash test dummies') which are mechanical surrogates of the human body and are used for safety analysis and validation in several industries like automobile, aerospace etc. [4]. The resulting accelerations on a human can be better analyzed by using an ATD.

3.2 Tests using an Anthropomorphic Test Device

3.2.1 Background

Effects of acceleration on human bodies can be classified into two major subgroups depending upon the nature of accelerations, these are: (a) *impact accelerations*; and (b) *sustained accelerations* [5]. Acceleration pulses of up to 200ms are considered as '*impacts*' e.g. sudden decelerations due to car crashes, slapping someone's back etc. and accelerations lasting longer than 200ms are considered as '*sustained*' accelerations e.g. in rollercoasters, fighter planes etc. *Sustained* accelerations (in a range of few G's) can lead to *G-Induced Loss of Consciousness* (abbreviated as G-LOC) e.g. an acceleration with an onset rate of 0.5G/s in the +G_z leads to G-LOC within 6s [6]. These types of acceleration cannot be executed on our motion simulator due to workspace constraints.

Impact accelerations can be further sub-divided into two parts (a.1) '*direct*' impact (on hard surface); and (a.2) *inertial loading* (no 'direct' impact) [7]. Direct impacts result from accelerations experienced due to contact between the passenger (i.e. the ATD in this scenario) and a 'hard' surface e.g. head of an automobile driver colliding with the steering wheel. These type of accelerations can have large values (of upto 60Gs, which can cause severe injuries) and are exerted for short durations (<200ms). These kinds of accelerations would (theoretically) be only possible in the simulator; when it crashes against itself, the ground and/or some external structure e.g. a wall. These scenarios are prevented by: (a) enclosing the robot in a cell, (b) usage of hardware stops that use aluminum blocks which deform to absorb the energy in case of these crashes and prevent the robot from colliding with itself.

So, we primarily focus on injury analysis pertaining to *inertial loading*. *Whiplash associated disorders (WADs)* that can be caused at relatively low accelerations, are an example of injuries due to *inertial loading* [3, 8]. We placed an ATD in the simulator cell (Figure 3) and executed trajectories that we presumed would lead to maximum 'loading' on the ATD. The ATD is fitted with acceleration sensors in the head, upper spine and the lower spine (Figure 3, right) and data is recorded for a few seconds before and after the emergency stop.

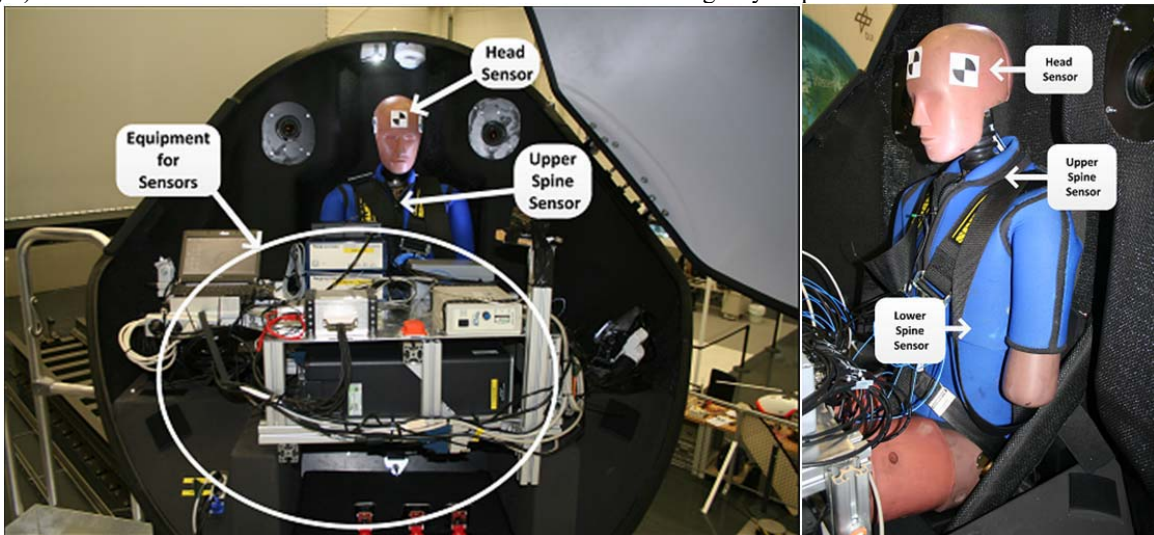


Figure 3. Left: ATD with equipment (e.g. power supply, signal box) inside the cell. Right: Locations of various sensors within the ATD.

During preliminary tests, we noticed the resultant accelerations measured by the head sensor to be much higher than those measured from the upper and lower spine sensors. This is an expected result; as the cervical spine and head are not constrained. On the contrary, the 5-point seatbelt restricts the motion of the ATD torso resulting in lower accelerations. On excitation, the head and the cervical spine region behave dynamically like an inverted pendulum whose base has been disturbed [9].

3.2.2 Test methodology

Based on these initial findings, we developed four tests that aim to induce motion of the head relative to the cervical spine when an emergency stop is triggered. These motions result from the *inertial loading* property of the head and can be classified into 4 types: (a) *flexion*, (b) *extension*, (c) *lateral bending* and (d) *rotation* [7]. The Test 1 and 2 are the same as the tests mentioned in Section 3.1 (also Figure 2, *left*). Test 1 is a clockwise motion that induces *flexion* on e-stop and Test 2 is an anti-clockwise motion inducing *extension*.

Test 3 involved driving the Axis 1 and the linear axis (referred to as E1) with a maximum possible velocity to the point where the tangential velocity of simulator cell is parallel to the velocity of E1 and then triggering the e-stop at this point. Test 4 is the same motion as Test 3, but differs in the direction (Figure 4, *left*). Tests 3 and 4 induce a composite of *lateral bending* and *rotation* on the head, when the e-stop is triggered.

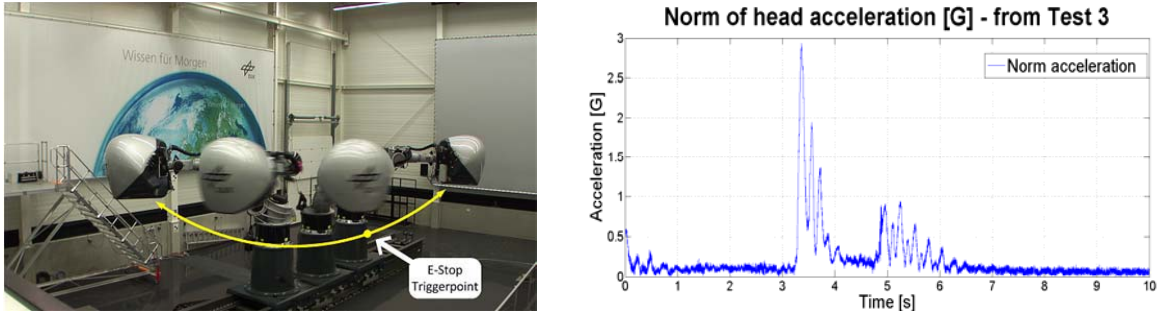


Figure 4. *Left:* Movement of the Simulator during Tests 3&4 mentioned in Sec.3.2.2. *Right:* Norm of the acceleration data from the head sensor (excludes acceleration due to gravity) during Test 3 from Sec. 3.2.2

3.2.3 Results

To determine prospects of injury to the passenger during these braking motions (e-stop) we use the *Head Injury Criteria (HIC)* [10] and the *Neck Injury Criteria (NIC)* [11] indices for head and neck regions, respectively. Both these indices are based on accelerations experienced by the head and neck regions during sudden decelerations e.g. collisions etc. and are widely used in automobile industry for ‘crash’ testing. Several indices e.g. *Nkm*, *LNL*, *SI*, *PI* etc. can be used for analysis of injuries inflicted on the head and neck region during sudden decelerations [7, 12]. Most of these indices use acceleration data, but a large variety use force-torque data for calculation of severity value of neck injuries [12]. Out of a multitude of severity indices, we choose *HIC* and *NIC* as we are limited to the availability of only acceleration data for calculation of injury severity. The values of *HIC* and *NIC* for Tests 1-4 are provided in the Table 3.

Table 3. *HIC* and *NIC* values for Tests 1-4

	Test 1	Test 2	Test 3	Test 4
HIC₃₆ Tolerance value: 1000	1.44	0.80	0.45	0.35
NIC_{max} (in m ² s ⁻²) Tolerance level: 15m ² s ⁻²	0.90	0.16	n.a.	n.a.

A detailed discussion on the procedure for calculation of these indices is presented [12, 13] for *NIC_{max}* and [10, 14] for *HIC₃₆*. The procedure is not mentioned here due to space constraints.

For Tests 3 and 4, the value of *NIC_{max}* is not presented; as in the knowledge of the authors this index can only be used for measuring injuries resulting from rear-end collisions i.e. injuries caused due to *flexion* and *extension* of the head-neck region.

4. CONCLUSIONS & FUTURE PLANS

The HIC_{36} and NIC_{max} calculated for Tests 1-4 are on the very low end of the injury severity scale. To achieve the HIC_{36} tolerance value of 1000 (i.e. beyond this value the human is severely injured); an average acceleration value of 60G over a period of 36ms needs to be applied on the passenger [14]. Such kinds of accelerations are only possible in cases of extreme decelerations resulting from e.g. a car crash (car hitting a tree etc.). As observed in the figure 2 (*right*) and figure 4 (*right*), the resultant acceleration values in the case of e-stop for Test 1 and Test 3 are 5.5G and 2.8G respectively. These accelerations are unlikely to cause any head injury due to *inertial loading*. In the case of *direct impact*, these acceleration values will be much higher and can therefore be dangerous for the passenger. Similarly, the NIC_{max} values for Tests 1 and 2 are on the lower end of severity index and are unlikely to cause any injury to the passenger. However, the NIC_{max} doesn't account for forces and torques developed in inertial loading scenarios mentioned above; neither is it applicable to *lateral bending* and *rotation* scenarios.

We plan to repeat the Tests 1-4 with a force-torque sensor mounted at the point of connection of the neck and the head and analyze the resulting data. We would also like to carry out more tests which are similar to conditions persistent in motions that result in *whiplash associated disorders (WADs)*. These types of disorders need a thorough analysis, as injuries to the neck have been observed for impact accelerations as low as 5G. Aside from prevention of injury to the passenger, another topic that needs deep analysis is passenger comfortability. This motion simulator is used for amusement and research purposes alike and one of our goals is to ensure passenger comfortability. But this is not easily quantifiable and varies a lot based on size, sex, age and prior simulator experience of the passengers. We plan to look into this criterion and hope to address this in the near future.

ACKNOWLEDGEMENTS

The authors would like to thank KUKA Roboter GmbH for funding and supporting this work. They also wish to thank Miguel Neves, Simon Haddadin, Christian Nissler, Genny Scalise, Theodoros Stouraitis, Daichi Hirano and Bao-Anh Dang-Vu for their help with the experiments.

BIBLIOGRAPHY

- [1] Bellmann, T. et al., The DLR Robot Motion Simulator Part I: Design and Setup, in *Robotics and Automation (ICRA), 2011 IEEE International Conference on*, pages 4694–4701, 2011.
- [2] KUKA Roboter GmbH, *KUKA Robot Sensor Interface 2.2*, 2008.
- [3] Regional court Bochum, Decision ref. 6 o 225/95, 22.5.1996.
- [4] Multiple, Anthropomorphic Dummies for Crash and Escape Systems Testing, Technical report, Advisory Group for Aerospace Research and Development, NATO, 1996, AGARD Advisory Report 330 (1996).
- [5] Physiological Effects of Acceleration, online.
- [6] Voshell, M., High Acceleration and the Human Body, (2004).
- [7] NRTO-NATO, Chap.3, Test Methodology for Protection of Vehicle Occupants Against Anti-Vehicular Landmine Effects, Technical report, NATO RESEARCH AND TECHNOLOGY ORGANIZATION NEUILLY-SUR-SEINE (FRANCE), 2007, RTO-TR-HFM-090.
- [8] Mertz and Patrick, Investigation of the Kinematics and Kinetics of Whiplash, *SAE Technical Paper 670919*, 1967.
- [9] Mertz and Patrick, Strength and Response of the Human Neck, *SAE Technical Paper 710855*, 1971.
- [10] FMVSS208, 1999.
- [11] Bostroem, O. et al., A New Neck Injury Criterion Candidate-Based on Injury Findings in the Cervical Spinal Ganglia after Experimental Neck Extension Trauma, in *PROCEEDINGS OF THE 1996 INTERNATIONAL IRCOBI CONFERENCE ON THE BIOMECHANICS OF IMPACT, DUBLIN, IRELAND*, Number 00767056, pages 123–36, 1996.
- [12] Muñoz, Mansilla, López-Valdés, and Martín, A Study of Current Neck Injury Criteria used for Whiplash Analysis. Proposal of a New Criterion Involving Upper and Lower Neck Load Cells, Technical Report 05-0313, University of Valladolid – Spain, 2005.
- [13] Boström, O., Håland, Y., and Fredriksson, R., A Sled Tests Procedure Proposal to Evaluate the Risk of Neck Injury in Low Speed Rear Impacts using a New Neck Injury Criterion (NIC), in *Proceedings of 16th ESV Conference*, number 98-S7-O-07, 1998.
- [14] Henn, H.-W., Teaching Mathematics and its Applications (1998) 162.

Study on Law and Social Systems for the Safety of Social-care Robots

Masahiro Kato

Manufacturing Science and Technology Center
 1-17-1, Toranomon, Minato-ku, Tokyo 105-0001, JAPAN
kato@mstc.or.jp

KEY WORDS: Life supporting robot, safety attestation, Asian market for life-supporting robots and safety attestation business

ABSTRACT

In NEDO's (New Energy and Industrial Technology Development Organization) project, "Life supporting robot deployment project -- Research and development of method for verifying safety of life supporting robots", MSTC is studying law systems to be taken into account for deploying life-supporting robots, based on domestic and overseas public information. Building to the result, it is making proposals. From this fiscal year, we plan to study law systems focusing the attestation business for life-supporting robots. Since it is naturally assumed that markets for attested products are established in nations and regions for developing attestation businesses, this paper analyses possibility of potential markets in Asia, classifying requirements of the business in its early stage, and study methods for preventing accompanied risks in the assumption of business risks.

1. INTRODUCTION

Since 1990s, Japanese economy has remained stagnant. Meanwhile, the US recovered and NIEs (Newly Industrializing Economies) and BRIC's (Brazil, Russia, India and China) are developing. It has been a long time since people were saying "The US is good at creating knowledge, China at manufacturing and Japan at producing trial pieces". In 2004, Palmisano report which proposed strategies against NIE's and BRICs was published. This report proposes strategies for creating profit in business models together with NIEs and BRICs involved there in following manner. That is to say, European and US companies modularize core-competence technologies in a form such as MPU, create comprehensive scenario up to finished products, and develop standards to be open to NIE's and BRIC's companies. In the mean time, NIE's and BRIC's companies develop cheaper products based on the scenario. These are strategies proposed in the above report. It is said that these strategies are those for driving vertically-integrated Japanese companies into a corner^[1] (Figure 1-1). Safety attestation, theme of the project for deploying life-supporting robots is part of this global strategy. In fiscal year 2011, we visited European and US safety attestation bodies and universities for investigation. As the result, it was understood that overseas major attestation bodies have high potentialities for peripheral standards of ISO 13482, and that it is difficult for Japanese safety attestation to be granted, even if Japan proceeds in commercializing life-supporting robots.

Mutual-coexistence –type Business Strategies with NIEs and BRIC involved

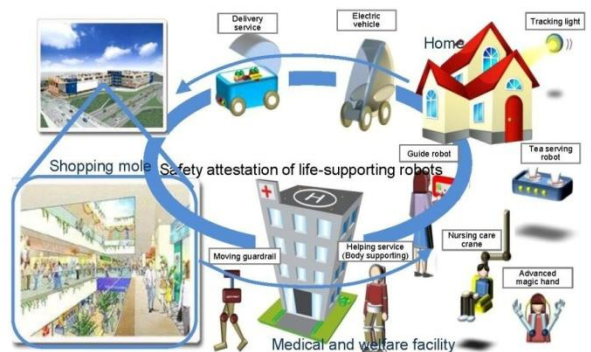
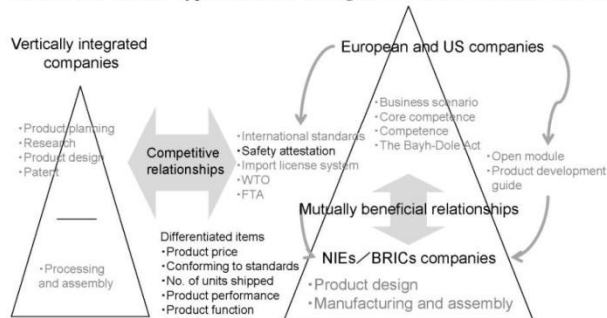


Figure 1-1 Business strategy proposed by Palmisano Report Figure 1-2 Services by life-supporting robots

Last year, we visited European and US attestation bodies. There they explained that they were prepared to swiftly develop safety attestation based on their nation's business strategies, once new products came onto the market. Further, in NEDO's intermediate evaluation implemented in August 2011, it pointed out "It is reasonable to develop attestation bodies and others. However it cannot be denied that they might be only established but not used. There is lack in strategies to be really recognized worldwide and to be de facto standard. Therefore, it is not defined what is required and how they might be realized".

Therefore, during two years in the latter phase, research study on requirements for safety attestation will be conducted, building to three years study result, items pointed out in NEDO's intermediate evaluation, as well as taking account of characteristics of each nation's attestation, standards and distribution. This paper examines strategies for our safety attestation system to be recognized really worldwide, targeting services using life-supporting robots as shown in Figure 1-2. The paper also takes a general view of relations among attestation, standard and distribution, which are the framework of this study. For attestation, standard and distribution, examples already implemented are listed up. In chapter 3, potentiality of markets for life-supporting robots in Asia is confirmed. In chapter 4, conditions for Japanese business in life-supporting robots to be realized are rearranged. Chapter 5 is for conclusion.

2. FRAMEWORK OF ATTESTATION BUSINESS

2-1. Framework of attestation business

This paragraph takes a general view of relationships among attestation, standard and distribution which are the framework of this study. The purpose of this study is that Japanese attestation bodies exceed overseas attestation bodies with high potentialities on the international stage and succeed in new attestation businesses. Attestation businesses are developed in the framework of attestation, standard and distribution. It is necessary to consider measures overlooking the whole framework since they affect each other.

For safety standard of life-supporting robots, ISO 13482 is under developed. Safety attestations based on this standard are conducted through local attestation system in individual companies. For example, EU adopts those in standards for evaluating the conformance to EC directives, and safety attestations are conducted through the CE marking system. The only attestation bodies qualified for these attestations are those certified by EU as notified bodies (NB). In the US, AHJ (Authorities having jurisdiction) in each area conducts safety attestation based on NEC (National Electric Code). However, as this NEC refers ANSI/UL standards, ISO 13482 is also adopted in ANSI/UL for attestation. The only attestation bodies for attesting ANSI/UL are UL's. In the mean time, also in Asia, China has its China Compulsory Certificate system, where only bodies certified by the Chinese government can conduct safety attestation domestically. As described above, global development of attestation business is realized only by clearing various constraints in attestation, standards and distribution.

In paragraphs described below, examples are listed up which can be purposes and references for Japan in advantageously developing safety attesting businesses of life-supporting robots.

2-2. Scheme of targeting attestation first

(1) Scheme of launching attestation business before others in new fields

Investigation visits in fiscal year 2011 showed that the field of life-supporting robots is also very much attractive for overseas attestation bodies. Japan, preceding in the new field, holds a dominant position. Overseas attestation bodies are on the watch for the chance, preparing for immediately launching attestation business if specifications of new products are provided by Japan and other countries.

(2) Scheme of utilizing overseas attestation bodies (Netherlands)

For example, RvA, Dutch attestation body, certified STQC, Indian attestation body, as the one based on IEC and EN standards. If a Japanese attestation body involves overseas bodies with a certain competent, Japan can develop life-supporting businesses in the overseas market.

(3) Scheme of cooperating with insurance companies (US)

Until 1916, UL had been conducting attestation business with the assistance from an insurance company. In this case, there is also a mutually beneficial relationship for insurance company, such as including UL certification as a condition of subscription.

2-3 Scheme of targeting standards first

(1) Activities in ISO standardization committee (Japan)

With regard to life-supporting robot deployment project, Japan is participating in ISO 13482 SC2 for making aggressive proposals so that standard developed by Japan can be adopted.

(2) Scheme of raising attestation standards to the national standards (US)

UL is privileged by ANSI (American National Standards Institute) to issue American national standards. However, even without the privilege, ANSI standards can be established if standards being submitted to ANSI standards board and they are approved.

2-4 Scheme of targeting distribution first

(1) Scheme of acquiring distribution license from local authorities having jurisdiction (US)

To apply for an import license of new products to Authorities having jurisdiction (AHJ), it is necessary to study local laws and systems at first hand and make preparations required. Based on a list distributed from AHJ, it is necessary to judge which law is actually concerned in those of an area regulated by AHJ and make preparations required including safety attestation, in order to have judgment. Therefore, having know-how on characteristics of those nations and areas allows advantageous development of global attestation businesses[*1].

[*1] Source: CSA INTERNATIONAL Hearing (November, 2011)

(2) Scheme of alleviating other nation's restriction in attestation under FTA (Free Trade Agreement)

On the occasion of entering into FTA with EU, Korea promised to adopt SDoC (Supplier's declaration of conformity) in products safety regulation within five years from the day FTA taking effect. Korea intends further alleviation of products safety regulation through examining the expansion of products subject to SDoC with EU every five years from its adoption.

(3) Scheme of creating new distribution systems (EU)

There is a scheme, in EU, to create new distribution systems such as the CE marking system established through the resolution of the New Approach Directives by EC (European Committee)

3. POTENTIAL MARKET FOR ROBOTS IN ASIA

Establishment of market for attested products is a basic assumption in nations and areas for attestation businesses to be developed. This chapter confirms there are potential markets for robot in Asia.

3-1. Analogical reasoning taking example of Denmark

Various life-supporting robots from supporting daily life of non-handicapped person to disabled or elderly people are developed according to usages. Here, focusing on life-supporting robots for elderly care, analogical reasoning is made for demand in Asia, taking example of Denmark. Denmark is attracting attention as a welfare state aggressively promoting the use of life-supporting robots. Three fundamental rules, forming the root of elderly welfare system in this country, are 1) Continuity in life (realization of lifelong worker), (2) Respect for the right of self-determination of elderly people and 3) Utilization of residual ability^[2]. These three fundamental rules were created, based on Danish people's wishes including, for example, for longer working years as long as possible even

if supported by robots and spend healthy and independent life without relying on care. These rules are also consistent with policies such as for nursing care, labor saving which are promoted by the Denmark government as national policies. Wishes, which are the origin of three fundamental rules, can be separated from wishes coming from the state where personal dependence is lost by infirmity and some care services must be relied on. The result of hearing research so far shows that wishes of people relying on care services tend to lead not to use of robots but to warm care services.

Three fundamental rules previously mentioned are not limited in Denmark but will be common wishes of mankind. Therefore, also in Asian countries behind in development of welfare system for elderly people, wealthy people with elderly family members are potentially users of life-supporting robots based on the above three fundamental rules.

Table 3-1 Wealthy populations in Asia

Ranking	Nations	Rich population [person] (2010)	Rate of aging (%)	
			2010	2020
2	Japan	1,739,000	26	30
4	China	535,000	9	13
16	Korea	146,000	13	18
17	India	153,000	5	7
19	Taiwan	94,000	—	—

Table 3-2 Comparison of markets of manufacturing robots based on the record of FY 2011

Field	US	Europe	Asia	Japan
Welding and Coating	20,300	48,250	71,050	24,650
Actuator	1,940	2,260	5,470	18,430
Assembly and Conveyance	16,250	24,600	46,710	36,290
Green conveyance	23,970	1,250	39,230	18,950
Total	62,460	76,360	162,460	98,320

Table 3-3 Real world economic growth rate (%)

Nations	2005	2006	2007	2008	2009	2010	2011
Korea	17	13	10	-11	-11	21	12
China	17	20	29	29	10	18	11
India	17	12	27	9	1	21	11
UK	4	7	15	-5	-19	3	10
Japan	-1	-4	0	11	3	8	7
Germany	2	5	14	10	-9	-1	6
US	6	6	5	2	-2	4	4

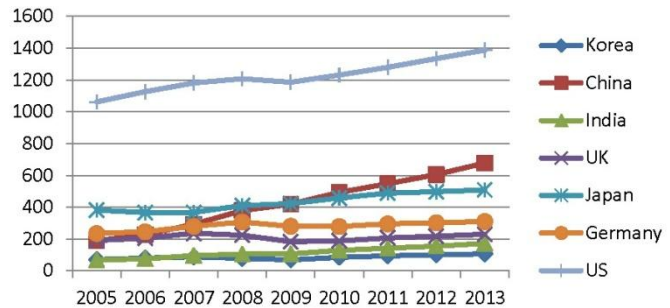


Figure 3-1 Real world GDP (Unit: Trillion yen)

Table 3-4 Domestic market of life-supporting robots^[4]
Unit: Million yen

Fields	2011 Recorded	2012 Expected	2013 Forecasted	2014 Forecasted	2015 Forecasted	2020 Forecasted
House work	9,465	11,860	15,065	18,570	23,075	56,150
Medical treatment/nursing/welfare	5,870	10,360	15,850	22,450	29,650	73,500
Job (Guide, inspection, etc.)	730	870	1,050	1,300	1,660	3,320
Total	16,005	23,090	31,965	42,320	54,385	132,970

Table 3-5 Global market of robots for manufacturers^[4]
(Europe, US and Asia) Unit: Million yen

Fields	2011 Recorded	2012 Expected	2013 Forecasted	2014 Forecasted	2015 Forecasted	2020 Forecasted
Welding and Coating	164,250	174,800	176,670	181,730	186,290	212,150
Actuator	28,100	32,200	34,850	37,550	40,650	52,050
Assembly and Conveyance	123,850	141,750	158,850	177,800	198,900	294,700
Green conveyance	83,400	76,800	80,220	83,070	85,770	105,250
Total	399,600	425,550	450,590	480,150	511,610	664,150

This is why wealthy populations of Asian countries, objective of this study, are shown in Figure 3-1. This data is abstracted from world censuses of wealthy populations, “World Wealth Report 2011” and “Asia-Pacific Wealth Report 2011”. The definition of wealthy people in this report was people with personal asset of 1 million dollars (80 million yen) or more, excluding residential property.

Especially, Japan (4 trillion dollars) and China (2 trillion dollars) ranked within top four have many wealthy people. The demand of life-supporting robots contributing to healthy and independent daily life without nursing care is expected to increase in corresponding to increasing wealthy populations in the Asian-Pacific region. At the same time, it is expected that increasing rates of aging^[3] shown in Table 3-1 will accelerate demand increase.

3-2 Analogical reasoning by comparison of economies between Europe, US and Japan, and Asia

Manufacturing industries are the driving force behind Asian economies, which are going to catch up with Europe, US and Japan. Comparison of market scales of manufacturing robots based on records in 2011 shows that Asian market of manufacturing robots is overwhelmingly large among whole markets including Europe, US, Japan and Asia. It account for approximately 40% of all. The stronger the Asian economy becomes, the more their living standard are improved. Conditions of Asian economy can be estimated using the real economic growth rate and the real GDP, which are indexes for economic power. First, seeing from the real economic growth rate shown in Table 3-3, we can find that Korea, China and India keep high growth rates. From these results, it is estimated that economic power of Korea, China and India will catch up with that of Europe, US and Japan in the near future. Next, seeing from the comparison of economic power using the real GDP shown in Figure 3-1, China has been ranked second since 2010. The living standard of Asian nations is estimated to catch up with that of Japan in the near future. In other words, if market for life-supporting robots is developed in Japan, it will be also done in Asian market.

Accordingly, take a look at conditions of the market for life-supporting robots in Japan based on the latest information from FUJI KEIZAI shown in Tables 3-4 and 3-5. In Table 3-4 showing the domestic market for life-supporting robots, the growth rate of 2020 is 5.8 times as much as that for the record of 2010. Comparing to the growth rate of global market for manufacturing robots at 1.7 times, further higher rate is expected. Comparing market scales of FY 2020 shown in Tables 3-4 and 3-5, it is estimated that the domestic market for life-supporting robots will grow up to one-fifth of the global market for manufacturing robots. Further, in these days, the market for life-supporting robots will have been revealed also in Europe, US and Asia.

4 SUMMARY OF CONDITIONS FOR ESTABLISHING ATTESTATION BUSINESSES OF LIFE-SUPPORTING ROBOTS IN JAPAN

We consider we should put safety attestation businesses of life-supporting robots on track, looking ahead of those markets that will have been revealed in FY 2020. For attaining those businesses, we have the theme of studying methods for preventing risks on the assumption of those business risks in safety attestation.

To begin with, the following four assumptions can be considered:

As assumption 1, assume the case where laws do not allow product sales without certification marks. In this case that operation profit of sales minus development and attestation costs is expected, attestation business is realized. Therefore, manufacturers will sell their products with certification marks.

As assumption 2, assume the case where products without certification marks do not sell well, although there is no legislation for certification marks. Even in this case, robot business is realized.

As assumption 3, even in the case where there are high risks without certification marks, robot business is realized if manufacturers can secure operation profit.

As assumption 4, in cases other than the above, certification marks cannot be attached. However, Japanese robot

business would be realized if manufacturers can secure operation profit. Current Japan is in this situation. Therefore, consider assumptions from 1 to 3 comparing each other. Assumption 1, for example, corresponds to the case where public bodies designated by the national government conduct safety attestation based on laws. However, if the government request those public bodies for price-down, there generated a risk that safety attestation business does not pay. In general, even in this case, governmental support is uncertain. Therefore, avoid this case and adopt assumptions 2 and 3. These cases, for example, correspond to the case where nation's reliability for safety attestation is promoted, and they are educated to understand that safety attestation is effective for preventing PL suits and brand damages in advance.

When look at the world, each country is interested in ISO 13482 and looking out for opportunities for include it into its attestation system. For Japanese attestation business to globally develops, it is considered as a way to conclude mutual attestation treaties with other countries. However, if there is no definite safety attestation system, negotiations with other countries become difficult.

5 CONCLUSION

Since it is a fundamental assumption for markets of certified products to be established in countries and regions for developing attestation business, this paper, in the first place, analyzed the possibility for potential markets in Asia. As the result, following knowledge was acquired, which will be a base for study research for the latter two years.

- 1) For studying the possibilities for potential markets of life-supporting robots in Asia, Denmark was taken as a reference example. The origin of the welfare system for the elderly in Denmark, wishes for “Healthy and independent life without relying on care even if supported by robots”, are common to mankind. Therefore, wealthy people in Asia might be users of life-supporting robots.
- 2) The demand in Asia for life-supporting robots contributing to healthy and independent daily life without relying on care is expected to increase corresponding to increase of wealthy people and the rate of aging in the Asian region. In addition, since the influence of the rate of aging is excluded, seen from only domestic aspect, the increase rate of wealthy people will have a strong correlation with economic growth in each country.
- 3) Real economic growth of Asia has been consistently showing a high value since 2005. As the result, its economic power (real GDP) is expected to catch up with that of Europe, US and Japan.. In the meantime, the domestic market for life-supporting robots is expected to be 5.8 times during the period from 2011 to 2020. In 2020, also the global market for life-supporting robots is expected to have revealed.
- 4) As conditions for attestation business to be established, it is desirable lead those conditions to the situation where “products without certification marks do not sell well, although there is no legislation for certification marks”. To attain to these conditions, it is essential to promote nation's reliability on safety attestation and educate them to understand that safety attestation is effective for preventing PL suits and brand damages in advance.

(Special remark) This research and development was conducted as a part of NEDO's commissioned project “Project for deploying life-supporting robots”.

REFERENCES

- (1) Kenichiro Senoo, *Why Japan defeated in business though advantageous in technological strength—Reason for completely defeated in sales of innovative new products*, Diamond Inc. (July, 2009) (Japanese)
- (2) 2.2.1.2 *Trial of Denmark, Study report for building the roadmap of agricultural robots, 2011*, Supervised by Japan Machinery Federation and edited by Manufacturing Science Technology Center (March, 2011) (Japanese)
- (3) *White paper on aging society, 2012*, edited by the Cabinet Office (Japanese)
- (4) *Present status of worldwide robot market and its future prospect, 2012*, edited by Fuji-Keizai (March, 2012)

Empirical Approach to Assessing Foot Injury Level Resulting from being Run Over by a Mobile Robot

Masami Kubota and Tatsuo Fujikawa

Japan Automobile Research Institute (JARI), 2530 Karima, Tsukuba, Ibaraki, 305-0822, Japan

E-mail: mkubota@jari.or.jp

KEYWORDS: Foot Injury, Mobile robots, Run-over

ABSTRACT

Risks of run-over should be assessed before introducing mobile robots into human-robot collaborative environments. This requires information on injuries caused by robots running over human feet. It should include the relationship between injury levels and design parameters (e.g., robot mass, type of mobile mechanism, and robot velocity). This study seeks to clarify these relationships through experiments. First, we conducted experiments with a moving device representing a typical mobile robot. The moving device's pneumatic tire ran over the foot of a human dummy. The relationship between the forces acting on the foot and the conditions (e.g., mass, tire inflation pressure, and robot velocity) were examined. Second, a bear's foot (intended for use as food) having a bone structure similar to that of a human foot was run over in several conditions, and the resultant foot injuries were investigated. We obtained information on foot injuries by comparing the results of the two sets of experiments.

1 INTRODUCTION

Robots are at the stage of practical introduction into human-robot collaborative environments such as factories, offices, homes, and other public spaces. The injury risk must be assessed before these robots are introduced, focusing on contact between human bodies and robots. This study addresses the risk of run-over by mobile robots, since almost no such information is available in the literature.

2 EXPERIMENTS USING A HUMAN DUMMY

2.1 Experiment Procedures

Foot injury risk is thought to depend on the load acting on the foot during run-over. We measured the load by using load cells installed in the floor of a test lane. A dummy foot was placed in the load cells (Figure 1). A mobile robot was represented by a trolley with four tires. In the run-over tests, the trolley was fixed on a steel wire from traction equipment driven by an electric motor. After the required speed was reached, the trolley was released from the wire and allowed to run over the dummy foot at a specific speed. Two types of tires (Figure 2) were used as trolley wheels. The dummy foot was the foot of the Hybrid III 50th Percentile Male Crash-Test Dummy (Figure 3), which is widely used in car crash tests worldwide and for many non-automotive applications (e.g., wheelchairs, and medical and sports equipment). It is considered to have excellent biofidelity and instrumentation capability.

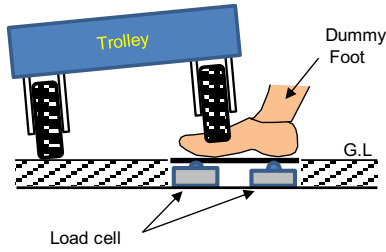


Figure 1. Test configuration.

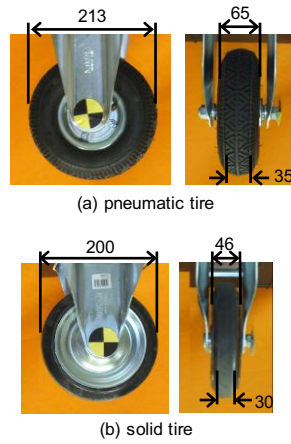


Figure 2. Types of tires.



Figure 3. Human dummy.

2.2 Results

Figure 4 indicates that the maximum load acting on the foot increases with increasing speed. Thus, foot injury risk in a run-over accident increases with increasing robot speed.

Figures 4 and 5 also indicate that the maximum load is lower for pneumatic tires than for solid tires. Figure 6 indicates that the maximum load is lower for a pneumatic tire inflated to 100kPa than for one inflated to 350kPa. Tires with lower stiffness deform during run-over, reducing the maximum load. This indicates that using a pneumatic tire and lower inflation pressure decreases foot injury risk in run-over accidents. All results are summarized in Table 1.

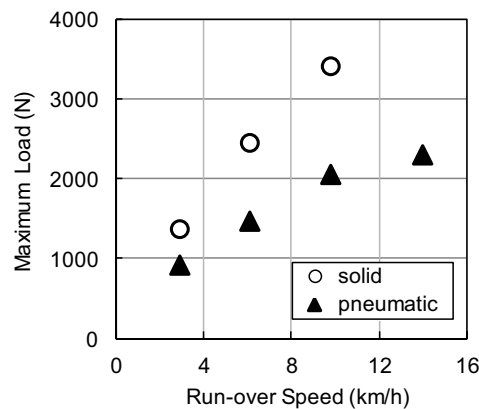


Figure 4. Effects of difference in tire type and run-over speed on resultant maximum load on foot. Robot mass: 110 kg. Tire type: Solid tire and pneumatic tire inflated to 350kPa.

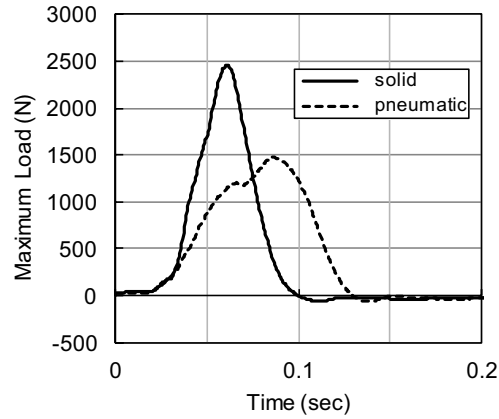


Figure 5. Load on foot during run-over. Run-over speed: 6km/h. Robot mass 100kg. Tire type: Solid tire and pneumatic tire inflated to 350kPa.

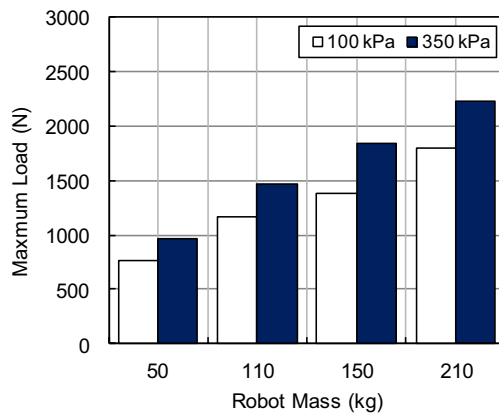


Figure 6. Effects of difference in tire inflation pressure and trolley mass on resultant maximum load on dummy foot during run-over. Trolley speed: 6km/h. Tire inflation pressure: 100kPa for white bar and 350kPa for black bar.

Table 1. Summary of test results

Robot Mass (kg)	Run-over speed (km/h)	Tire	Tire inflation pressure (kPa)	Region	Maximum load (N)
50	6	pneumatic	350	toe	967
50	6	pneumatic	100	toe	760
110	3	pneumatic	350	toe	922
110	6	pneumatic	350	toe	1,473
110	10	pneumatic	350	toe	2,060
110	14	pneumatic	350	toe	2,306
110	3	solid	—	toe	1,373
110	6	pneumatic	100	toe	1,167
110	6	solid	—	toe	2,456
110	10	solid	—	toe	3,418
150	6	pneumatic	350	toe	1,843
150	6	pneumatic	100	toe	1,384
210	6	pneumatic	350	toe	2,229
210	6	pneumatic	100	toe	1,801

3 EXPERIMENTS ON BEAR'S FOOT

3.1 Bending Tests

In order to determine the mechanical properties of feet, we conducted experiments using actual parts of animal bodies that are available as food. Bear's feet were used for the test since their bone structure is similar to that of human feet (Figure 7). As the first step of the study, we deal with AIS (Abbreviated Injury Scale) 2 injuries that correspond to fractures of foot bones.

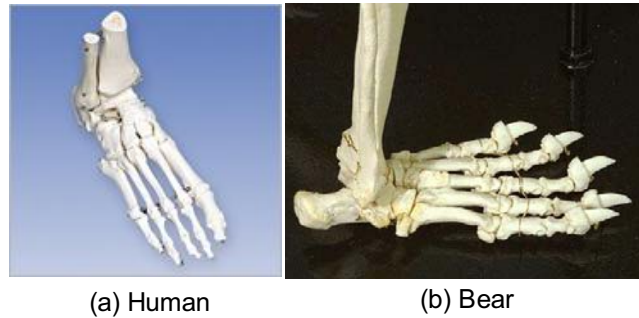


Figure 7. Skeletal structures of human foot and bear's foot.

Although bears' feet and human feet have similar structures, they have different sizes and strengths. A bending test was conducted using a bear's foot to obtain data on mechanical strength. The test mode represents the bending of a bone supported at two thick ends of bone during run-over by a robot's solid tire. A single bone removed from a foot was bent by pressing the loading head of a testing machine on the center of the bone. Figures 8 and 9 indicate the results of the test. The fracture load was 4150N. This exceeds the largest load, 3418N, acting on the foot of a human dummy in the run-over test (Table 1). The results indicate that the bear's foot bone may not be fractured by run-over under the conditions considered in this study, but we must note that the human foot bone may fracture because it is smaller and has different mechanical properties. Simulation to clarify the fracture load of human feet is needed in the next step of the study.

For simulation, the mechanical strength of the bear's foot bone and the human foot bone must be determined. Ultimate Bending Strength, which is expressed by tensile stress (MPa), was calculated from the test results by

$$\text{Ultimate Bending Strength} = \frac{8P_b LH}{\pi BH^3}, \quad (1)$$

where, P_b is the bending load at fracture, L is the span of supports, H is the specimen height, and B is the specimen width. The Ultimate Bending Strength of the bear's foot bone tested here was 180MPa. This value is comparable to that of the human tibia (200MPa) reported by Yamada [3], additional measurements are needed to obtain reliable data.

We also conducted a bending test on a whole foot in order to analyze robot tire run-over of several bones simultaneously. As depicted in Figure 10, no fracture was observed in the load range of the testing machine. The load was supported by more than one bone. The results of the two tests indicate that run-over of the single bone (e.g., the toe part of the foot) may cause more serious injury than run-over of the whole foot.

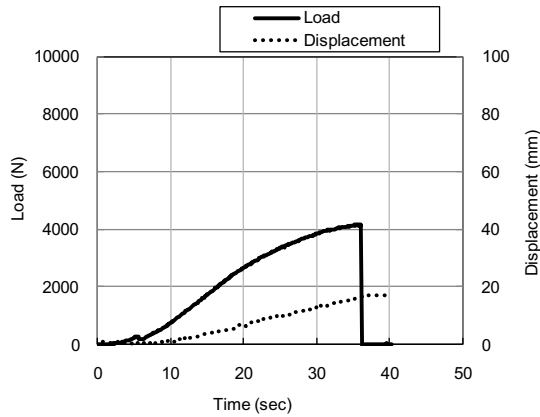


Figure 8. Load-bearing characteristics of a bear's foot bone. Figure 9. Bone fracture by bending test.

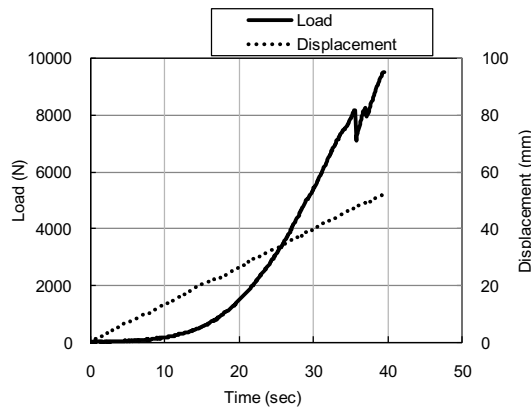


Figure 10. Load-bearing characteristics of a bear's foot.

3.2 Run-over Tests

We conducted run-over tests using a bear's feet in order to investigate foot injury. In the experiment, a bear foot was run over by the trolley, as described in Chapter 2. Figure 11 presents an example of a CT image after a run-over test. No fracture was observed, since the resultant load on the foot was 2803N, which is less than the fracture load of the single bone described above. Although the test procedures are confirmed to be appropriate to obtain injury data, experiments using more severe conditions are needed in the next step of the study.



Figure 11. CT image of a bear's foot after run-over test. Trolley mass: 210kg. Traveling speed: 14km/h. Tire: Pneumatic tire inflated to 350kPa.

4 CONCLUSIONS

The results of run-over experiments using a human dummy with a moving device representing a typical mobile robot indicate the following.

- (1) Foot injury risk from a run-over accident increases with the increasing robot speed.
- (2) Using a pneumatic tire decreases foot injury risk in run-over accidents compared with using a solid tire.
- (3) Using lower inflation pressure for a pneumatic tire decreases foot injury risk in run-over accidents.
- (4) Running over the toe may cause more serious injury than running over the entire foot.

Further research is required, including experiments under additional conditions and simulation to compensate for differences between human feet and bear feet.

5 ACKNOWLEDGEMENTS

This work is a part of “Project for practical applications of service robots” by New Energy and Industrial Technology Development Organization.

6 REFERENCES

1. Stanley H. Backaitis, *Hybrid III: The First Human-Like Crash Test Dummy*, Society of Automotive Engineers, 1994
2. <http://www.humaneticsatd.com/>
3. Ymamada, H., *Strength of Biological Materials*, The Williams and Wilkins Company, Baltimore 1970, pp 20- 21.

SIAS
2012

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



SESSION 6

**MACHINE SAFETY;
PRACTICAL APPLICATIONS
AND KNOWLEDGE DISSEMINATION**

New Focus on safety at machinery work places

Michael Schaefer, michael.schaefer@dguv.de; Michael Huelke, michael.huelke@dguv.de;
Peter Nickel, peter.nickel@dguv.de

Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), Alte Heerstr. 111,
53757 Sankt Augustin, Germany

KEY WORDS: safety, machinery, Human-Machine-Interfaces, functional safety

ABSTRACT

A global approach on safety is necessary to guarantee safety at machinery work places; especially at automated systems. The presentation will give an overview about IFA activities in this field. The following questions have to be raised when dealing with such a global approach:

Does the machinery work in a robust and reliable way (basic requirements)?

Does the machinery react safely in case of technical problems (functional safety)?

Does the machinery react on human error in a safe and economical way (functional safety and human machine interaction, usability)?

Does the machinery produce in an economical sense (synergy between safety requirements and economical aspects)?

How can machinery conform to all needs of operating companies, operators and the OSH?

1 INTRODUCTION

In the field of industrial machinery there are some well known requirements for safety. The above raised questions lead to answers to establish safe working places. This presentation shows first attempts of a (hopefully not) never ending story of reaching the optimal aim making optimal safe and social workplaces. The European Machinery directive [1] requires some basic activities to ensure safety of machinery:

“1.1.2 Principles of safety integration

(a) Machinery must be designed and constructed so that it is fitted for its function, and can be operated, adjusted and maintained without putting persons at risk when these operations are carried out under the conditions foreseen but also taking into account any reasonably foreseeable misuse thereof. The aim of measures taken must be to eliminate any risk throughout the foreseeable lifetime of the machinery including the phases of transport, assembly, dismantling, disabling and scrapping.

(b) In selecting the most appropriate methods, the manufacturer or his authorised representative must apply the following principles, in the order given:

- eliminate or reduce risks as far as possible (inherently safe machinery design and construction),
- take the necessary protective measures in relation to risks that cannot be eliminated,
- inform users of the residual risks due to any shortcomings of the protective measures adopted, indicate whether any particular training is required and specify any need to provide personal protective equipment.”[1]

The main keywords written in these unimpressive sentences is basis for a much more global approach, which is unfortunately different from practise of the state-of-the art industrial systems:

1. inherent safe design
2. use of protective measures
3. user information on residual risk

Only a further view what this means is written in the introduction of this clause:

- The machinery is fitted for its function,
- can be operated, adjusted and maintained without putting persons at risk.

At another clause of the directive we can find the following:

“1.1.6. Ergonomics

Under the intended conditions of use, the discomfort, fatigue and physical and psychological stress faced by the operator must be reduced to the minimum possible, taking into account ergonomic principles such as:

- allowing for the variability of the operator's physical dimensions, strength and stamina,
- providing enough space for movements of the parts of the operator's body,
- avoiding a machine-determined work rate,
- avoiding monitoring that requires lengthy concentration,
- adapting the man/machinery interface to the foreseeable characteristics of the operators.”[1]

These are clear but very generalized requirements. Especially the last indent for HMI (“foreseeable characteristics of the operators”) is in the author’s opinion a hard to realize.

So there are the following basics to fulfil the essential health and safety requirements of this directive:

Safety and Ergonomics (physiological und psychological).

2 DEVELOPMENT ON OSH TASKS AT MACHINERY

Since several years safety of machinery is a widely examined field by many organisations. Today safety is often established by intelligent electronically safety components. Starting in the early 80th programmable logic controls were established in the market. Standardization organisations [2] accompanied this by developing requirements and procedures to guarantee the safety of such new technologies. In the field of logic units, many organizations have the know-how to implement safety measures, today. One of the IFA tasks, as of other OSH institutes is and was to do research on new technologies to prevent operators against potential emerging risks.

Table 1 gives a small impression about the historical evolution e.g. in the IFA (former BGIA). Nevertheless this historical development is also seen outside of IFA and stands for the respective zeitgeist. In the first years, up to two decades, main interest went into Functional Safety (FS). In the near past Human-Machine-Interfaces took more and more centre stage. This does not mean that FS is today not so important, but more and more a standard routine task, even a complex one.

Title	Year	Genre
Design of electrical machinery controls with diverse redundancy	1986	FS
Passive infrared sensors for personal protection when using industrial trucks	1988	FS
Principles for computers in safety-related systems	1990	FS

Functional safety of software	1995	FS
Provisions governing safety bus systems on machinery and plant	1998	FS
Programming guidelines for the design of software of safety-related systems (1998)	1998	FS
Safety of Industrial Automated Systems- Innovation and Prevention through Research 1999 (SIAS)	1999	FS
Safety-related microprocessor control systems for sensing, controlling and bus communication 1999 (SIAS)	1999	FS
Safe bus systems for automation (2001)	2001	FS
Development of Metrics for Safety-Related Software in Machinery (2003)	2003	FS
The new approach of Safety Standard EN 954-1 (rev.): Balancing deterministic categories and probabilistic failures	2004	FS
prEN ISO 13849: A practical standard to evaluate control systems for safety (SIAS)	2005	FS
Reasons for the manipulation (tampering) of protective devices (SIAS)	2005	HMI
A methodology for the safety quantification of mechatronic systems (SIAS)	2007	FS
Functional safety of machine controls - Application of DIN EN ISO 13849 -1	2008	FS
Safety of Machinery - Perpetuating the systemic approach and the integration of human factors into machinery (2008)	2008	FS
The human-machine interface as an emerging risk (2009)	2009	HMI
Verification and validation of an interactive virtual environment for the analysis and design of human-machine interfaces	2010	HMI
Cave automatic virtual environments for research into occupational safety and health - Practical recommendations and solutions for the construction (SIAS)	2010	HMI
Prozesse menschlicher Informationsverarbeitung in realer und virtueller Roboterzelle. 2012	2012	HMI
FS = Functional Safety, HMI = Human Machine Interface, All these articles are not in the reference list, for information see: IFA/IAG-Database publications: http://www.dguv.de/ifa/en/pub/ueb/index.jsp		

Table1: Historical consideration

3 FUNCTIONAL SAFETY ("HE WHO HEALS IS RIGHT")

As mentioned above, functional safety is more and more a routine task, because many problems using electronics in safety devices are solved. Today, the challenge is to adapt the requirements to much more complex architectures of safety components. This is still a task for highly educated engineers and scientist. For more simple architectures, as e.g. defined in EN ISO 13849-1 [2] there was done a lot of new work, to help also SME to find the correct design of their control systems. One important task was to give practical aids on this standard to companies. Several projects in IFA with totally more than 10.000 person hours dealt with the development of a handbook the BGIA Report 2/2008 [3] and the examples of different technology. On-Peak IFA had 20.000 downloads a month for the online version over a period of more than 2 years. The printed version is now out of stock, with more than 15.000 copies. Another very challenging task was the development of the SISTEMA-tool [4-6]. Even if it looks so, this tool is not only some graphical user interface assisting the safety engineer, but it is an enormous think tank. Many of complex decisions are made in the background when SISTEMA evaluates the inputs of the user. These decision are of course not of artificial intelligence but done by a team of scientist before programming. If you look at the authors list of the BGIA Report 2/2008 you see that 20 experts of IFA have contributed their knowledge not only to this report, but do this permanently for the development and maintenance of SISTEMA. Today, more than 30.000 users are registered

(see fig.1). More than 50 component manufacturers support SISTEMA by offering free libraries. In different press articles SISTEMA is called the “de facto standard”.

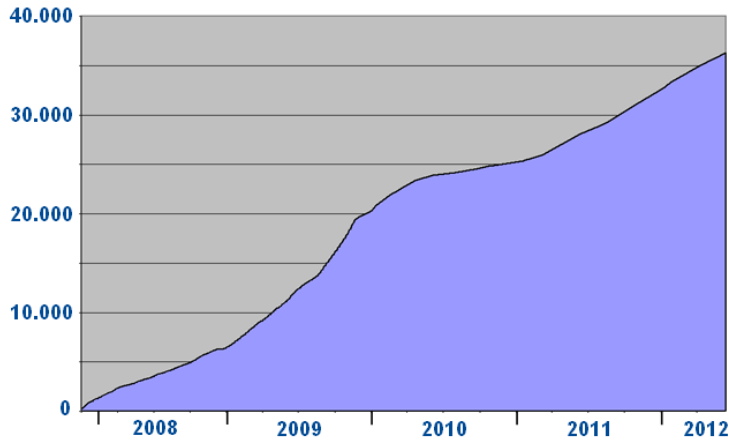


Figure 1: Number of registered users of SISTEMA

What can be future task in Functional Safety?

There are many tasks to deal with, which are directly connected with the second aim of this article, the aim of HMI or usability. The following list raises some examples (not complete list):

- Software engineering for SME, e.g. safe programming of application software
- Establishing software development kits to program safety related software
- Software validation with modern methods and tools for application and embedded software
- Development of new and safe sensor systems e.g. camera systems which are fast and have differential capabilities
- Development of assistive systems at machinery to operate the machine in an optimal and safe way
- New task of combining safety and security for open systems
- Development of safety components for collaborative robots and other machinery

4 HUMAN MACHINE INTERFACE (HMI)

The following clause deals with the necessity of improvements of HMI at machinery in respect to safety. As mentioned in the introduction the key requirement comes e.g. from the Directive [1]. “adapting the man/machinery interface to the foreseeable characteristics of the operators”

As mentioned above, the author now lifts the secret, why in his opinion this requirement is hard to fulfil.

The technical party of scientist are familiar with the fact, that almost everything is measurable. And in terms of safety there are a lot of established tools to characterise safety. This is not correct for the so called soft skills (e.g. psychology). The citation above raises three major questions:

1. What is the man/machinery interface at a specific workplace?
2. What are foreseeable characteristics of the operators?

3. How can we adapt the man/machinery interface to the operator's characteristics?

The first question is perhaps the question which can be answered most easily. But remember, that a machinery has different modes of operation. The answer of the third question comes at least from the risk assessment. An experienced safety expert knows that this is sometimes a highly sophisticated work. But to be with the mathematicians the problem can be solved.

Let's now look at the other questions.

The reader may guess that the second question is more problematic. Humans are not of uniform size, education, behaviour, intelligence ...

So in this question the epidemiological sciences are very relevant. Therefore this question requires a fundamental statistical background of all relevant parameters. This means an experiment with test persons has first to decide about the control sample. Now, we are lucky to exclude several parameters e.g. age from the whole population. If we have a good control sample we could then determine the foreseeable characteristics of the operators. But which of the characteristics are important for the individual task? In practise, that can not be determined without having the application in mind. This is a dilemma for trying to determine these "foreseeable characteristics" top down, which means collecting a universal set of data e.g. for standardization.

The second question leads to the third question of introducing the characteristics of the operators to a method for adapting the HMI. So we have to "measure" whether a HMI is good or bad. Because there is no top down procedure we can only analyze the characteristics of operators by doing experiments with the individual workplace. This is done many years e.g. for musculoskeletal disorders by work place observations. This is hard but easy to do by different possible measuring methods, because wrong behaviour of the operator will lead to an occupational disease after a long time.

This can not be done in accident examinations. To estimate the characteristics of the operator to "measure" erroneous behaviour can not be done in the real world. One has to set up experiments which simulate the work environment without introducing real hazards to the test persons. There are a lot of studies which do this, one possible way is to simulate the whole workplace by Virtual Reality (VR). Nevertheless before using a simulation, we raise up the next consecutive important question:

How real is the simulation, in term for VR: How real is Virtual Reality.

IFA has developed an inimitable simulation laboratory SUTAVE (Fig. 2, Safety and Usability through Applications in Virtual Environments) [7].

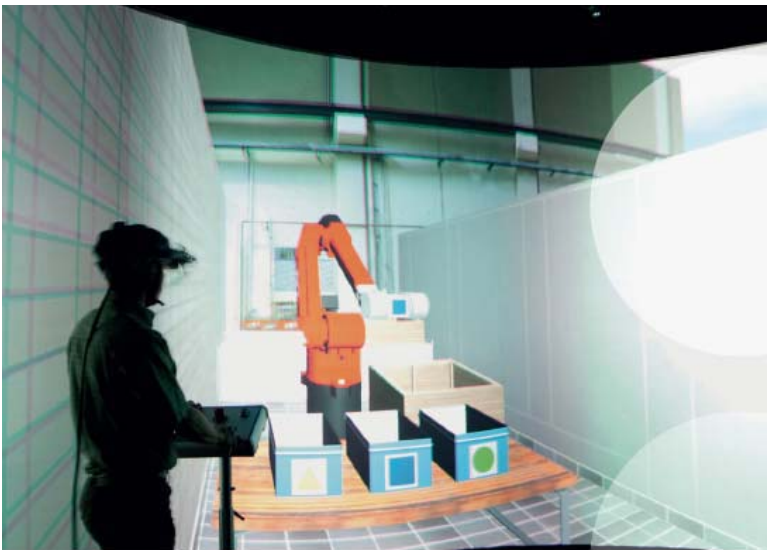


Fig 2: SUTAVE laboratory

To come back to the last question, the following project has determined the quality of this platform:

“BGIA5110: Validation of a system for the simulation of interactive virtual environments”

“In an experimental study the effects of intensity of human-robot interaction on human information processing has been investigated by means of task performance measures, psychophysiology and questionnaires. Also included were tests for simulator sickness and the level of immersion and presence under human-robot interaction in VR. The results of the pilot study suggest a high quality of the VR system with simulator sickness not being an issue and immersion and presence experienced at medium to high levels.”[8]

After optimization of the VR-environment, SUTAVE started its work with several projects dealing directly with application coming from practical problems, e.g. three of the projects are (longer list see [9-23]):

IFA5116: Protective equipment for 3D zone monitoring: Effects of zone design on machinery safety using virtual reality (in German)

IFA5118: Evaluation of a built-in safety function for an actuator for elevating work platforms using virtual reality (in German)

IFA5122: Risk assessment of river locks under development in virtual reality (in German).

4 CONCLUSION

Matching the essential health and safety requirements IFA started the task to simulate different workplaces not only under the aspect of functional safety, but also under the new emerging aspect of HMI. As shown, today there is not a possible top down approach as hoped by a lot of experts, but after dealing with some experiments on different applications there might be the chance to get more and more generalized data. This seems to be a long way, but the results of each new experiment can be introduced directly into practise.

5 REFERENCES

1. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). OJ EC L 157 (2006), p. 24; with corrigendum to Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC of 9 June 2006. OJ EC L 76 (2007), p. 35, <http://eur-lex.europa.eu>
2. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006)
3. Hauke M. et.al., *BGIA Report 2/2008e - Functional safety of machine controls - Application of EN ISO 13849*, German Social Accident Insurance, Sankt Augustin, 2009, ISBN: 978-3-88383-793-2 <http://www.dguv.de/ifa/en/pub/rep/rep07/bgia0208/index.jsp>
4. Safety Integrity Software Tool for the Evaluation of Machine Applications, www.dguv.de/ifa, webcode e34183
5. Apfeld R. et.al., *SISTEMA Cookbook 1- From the schematic circuit diagram to the Performance l – quantification of safety functions with SISTEMA*, Institute for Occupational Safety and Health of DGUV (IFA), Sankt Augustin, 2010, <http://www.dguv.de/ifa/en/prasoftwa/sistema/kochbuch/index.jsp>,
6. Lungfiel A., Huelke M., *SISTEMA Cookbooks 2 and 3*, Institute for Occupational Safety and Health of DGUV (IFA), Sankt Augustin, 2010, <http://www.dguv.de/ifa/en/prasoftwa/sistema/kochbuch/index.jsp>
7. SUTAVE, Safety and Usability through Applications in Virtual Environments, http://www.dguv.de/ifa/en/fac/virtual_reality/sutave_flyer_en.pdf

8. Nickel, P.; Lungfiel, A.; Nischalke-Fehn, G.; Pappachan, P.; Huelke, M.; Schaefer, M., Evaluation of Virtual Reality for Usability Studies in Occupational Safety and Health, 6. International Conference on Safety of Industrial Automated Systems - SIAS 2010, 14th.-15th. June 2010, Tampere/Finland - Ed.: Finnish Society of Automation, Helsinki/Finland 2010. ISBN: 978-952-5183-40-5
9. Naber, B.; Lungfiel, A.; Nickel, P.; Huelke, M.: Einfluss von Geschwindigkeit und Nähe eines Roboters auf Leistung und Beanspruchung in virtueller Mensch-Roboter-Kollaboration. Gestaltung nachhaltiger Arbeitssysteme – Wege zur gesunden, effizienten und sicheren Arbeit. 58. Kongress der Gesellschaft für Arbeitswissenschaft, 22-24 February 2012, Kassel – Lecture. Proceedings and CD-ROM, pp. 227-230. Ed.: Gesellschaft für Arbeitswissenschaft, GfA-Press, Dortmund 2012
10. Nickel, P.; Lungfiel, A.; Huelke, M.; Schaefer, M.: Evaluationsstudien zur Tiefenwahrnehmung in realer und virtueller Roboterzelle. Gestaltung nachhaltiger Arbeitssysteme – Wege zur gesunden, effizienten und sicheren Arbeit. 58. Kongress der Gesellschaft für Arbeitswissenschaft, 22-24 February 2012, Kassel – Lecture. Proceedings and CD-ROM, pp. 243-247
11. Hoyer, G.; Hauke, M.; Lungfiel, A.; Nickel, P.; Huelke, M.; Bömer, T.: Gestaltungsanforderungen an dreidimensionale Schutzräume für Fertigungszellen mit Mensch-Roboter-Interaktion – Eine Pilotstudie in virtueller Realität. Gestaltung nachhaltiger Arbeitssysteme – Wege zur gesunden, effizienten und sicheren Arbeit. 58. Kongress der Gesellschaft für Arbeitswissenschaft, 22-24 February 2012, Kassel – Lecture. Proceedings and CD-ROM, pp. 643-646
12. Nickel, P.; Lungfiel, A.; Hauke, M.; Nischalke-Fehn, G.; Huelke, M.: Virtuelle Realität im Arbeitsschutz zur Verbesserung der Sicherheit und Gebrauchstauglichkeit von Produkten. A+A 2011. 32th International Congress for Safety, Security and Health at Work "Safety, health, ergonomics", 18 to 21 October 2011, Düsseldorf - Poster
13. Nickel, P.; Lungfiel, A.; Hauke, M.; Nischalke-Fehn, G.; Huelke, M.; Schaefer, M.: Einsatz von Virtueller Realität zur Unfallverhütung und zur Usability. In: "4. Fachgespräch Ergonomie 2010". IFA-Report 6/2011, pp. 25-30
14. Nickel, P.; Huelke, M.; Lungfiel, A.: SUTAVE - Safety and Usability through Applications in Virtual Environments - Virtual reality in occupational safety and health. Leaflet. Hrsg.: Deutsche Gesetzliche Unfallversicherung (DGUV), Berlin 2011
15. Nickel, P.; Lungfiel, A.; Hauke, M.; Nischalke-Fehn, G.; Huelke, M.: Virtuelle Realität zur Verbesserung von Sicherheit und Gebrauchstauglichkeit in der Arbeit mit Hubarbeitsbühnen. Mensch, Technik, Organisation - Vernetzung im Produktentstehungs- und -herstellungsprozess. 57. Congress of Gesellschaft für Arbeitswissenschaft, March 23 - 25, 2011, Chemnitz - Lecture. Proceedings and CD-ROM. Ed.: Gesellschaft für Arbeitswissenschaft, GfA-Press, Dortmund 2011
16. Nickel, P.; Lungfiel, A.; Hauke, M.; Nischalke-Fehn, G.; Huelke, M.; Schaefer, M.: Virtuelle Realität im Arbeitsschutz für mehr Sicherheit und Gebrauchstauglichkeit. Technische Sicherheit 1 (2011) No. 4, pp. 43-47
17. Huelke, M.; Nickel, P.; Lungfiel, A.; Nischalke-Fehn, G.; Schaefer, M.: Cave automatic virtual environments for research into occupational safety and health – Practical recommendations and solutions for the construction. In: Finnish Society of Automation (Ed.): Proceedings of 'The 6th International Conference on Safety of Industrial Automated Systems' (SIAS), June 14-15, 2010, Tampere, Finland. pp. F6044 1-4. Finnish Society of Automation, Helsinki/Finland 2010
18. Nickel, P.; Huelke, M.; Lungfiel, A.: SUTAVE - Safety and Usability through Applications in Virtual Environments. Flyer. Ed.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2010
19. Nickel, P.; Pappachan, P.; Lungfiel, A.; Nischalke-Fehn, G.; Huelke, M.; Schaefer, M.: Verifikation und Validierung einer interaktiven virtuellen Umgebung zur Analyse und Gestaltung von Mensch-Maschine-Schnittstellen. In: Trimpopp, R.; Gericke, G.; Lau, J. (Ed.): Sicher bei der Arbeit und unterwegs – wirksa-

me Ansätze und neue Wege. 16. Workshop Psychologie der Arbeitssicherheit und Gesundheit. pp. 59-62. Asanger, Kröning 2010

20. Nickel, P.; Pappachan, P.; Lungfiel, A.; Nischalke-Fehn, G.; Huelke, M.; Schaefer, M.: Gebrauchstauglichkeit einer interaktiven virtuellen Umgebung zur Evaluation von Mensch-Maschine-Schnittstellen. In: Gesellschaft für Arbeitswissenschaft (GfA) (Ed.): Neue Arbeits- und Lebenswelten gestalten. pp. 889-892. GfA-Press, Dortmund 2010
21. Pappachan, P.: Using virtual reality to prevent occupational accidents. Focus on IFA's work, No. 0299. Ed.: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2010
22. Pappachan, P.; Nickel, P.: Mit Virtual Reality gegen Unfälle. Arbeit und Gesundheit spezial 61 (2010) No. 5, pp. spezial 20
23. Flaspöler, E.; Hauke, A.; Pappachan, P.; Reinert, D.; Bleyer, T.; Henke, N. et al.: The human-machine interface as an emerging risk. European Risk Observatory Literature Review. European Agency for Safety and Health at Work, Luxemburg 2009

Safety functions of automated mobile work machines

Timo Malm

VTT, P.O.Box 1300, FIN-33101 Tampere, Finland, timo.malm@vtt.fi, www.vtt.fi

Marita Hietikko

VTT, P.O.Box 1300, FIN-33101 Tampere, Finland, marita.hietikko@vtt.fi, www.vtt.fi

Risto Tiusanen

VTT, P.O.Box 1300, FIN-33101 Tampere, Finland, risto.tiusanen@vtt.fi, www.vtt.fi

Ari Ronkainen

MTT Agrifood Research Finland, FI-31600 Jokioinen, Finland, ari.ronkainen@mtt.fi

KEY WORDS: Safety functions, mobile work machines, control systems

ABSTRACT

In the near future workers, manually driven mobile work machines and automated mobile machines may be working at the same time in large worksites. It is difficult to arrange adequate safety for workers while the production interruptions need to be minimised. This paper presents an idea of a toolbox, which helps the designer to create a safety system by applying suitable safety functions dynamically according to the existing risk. Typical safety functions are presented including stopping functions, reduced speed, movement towards safe direction, restricted area and dynamically changing safety distance. The user can invent other safety functions too, but then also the corresponding safety requirements need to be determined. The main goal is to keep the distance between persons and moving mobile work machines all the time longer than the stopping distance.

Another aspect is how the safety system can apply uncertain information received from sensors. Current sensors, which have adequate detection range, are not reliable enough and therefore additional measures are required to compensate the uncertainty of information. Several sensors and methods for detecting the position of a person are needed and all uncertainty or disparity in information increase the safety distance between a person and the machine. Complete stopping of the machine is tried to be avoided even under malfunction of the system. For example manual limping mode offers limited performance, but it is adequate to drive the machine out of a dangerous place.

When there is both manual and automated driving in the production site, it is essential to consider the responsibility of each party. Basically, automation is responsible for safety in automated drive and humans in manual drive. However, automation has always the major responsibility when it is applied. The automation and the safety system may be considered to be responsible for accidents caused by malfunction of machines or even foreseeable human mistakes.

1 INTRODUCTION

Automation in mobile work machines is increasing. The automation can be related to single machines or systems containing a fleet of mobile work machines. The safety functions can be related to the protection of a machine (person inside a cabin) or protection of persons. This text is concentrating on human protection in cases where the mobile machine or the boom of the machine may move towards a person.



Figure 1. Examples of mobile work machines.

The machines considered in this paper have automated functions and the area where they are operating is safeguarded by sensors. The risk for a crushing accident would be probable if a person were at the danger zone and the machine were moving. The working area of mobile work machines can be one km long (e.g. ore transport systems with automated loaders) and stationary work machines can move its boom 10 m or more. In both cases it is considered how different safety functions can be applicable when the risk changes as the operation phase changes. One goal of the study is to make cooperation with the work machines safely without unnecessary stops of the system. For example drilling rigs may have three booms, which are controlled individually. The operator may need to maintain one boom of the machine while the other boom is still working or the operator may have a task close to mobile work machine and the machine should be operating with specific conditions. There is a need to keep the production going on without interrupting it too much and yet the safety may not be jeopardized.

The work presented is part of project FAMOUS (Future Semi-Autonomous Machines for Safe and Efficient Worksites), which is part of Fimecc's (Finnish Metals and Engineering Competence Cluster) research program EFFIMA (Energy and Life Cycle Efficient Machines). The main financier of the project is Tekes (Finnish Funding Agency for Technology and Innovation).

2 RESPONSIBILITY AND REQUIREMENT ASPECTS OF SAFETY FUNCTIONS

The performance level (PL) of the safety function is associated to the safe operation of machine functions. The PL is defined in standard ISO 13849-1 [2]. The required PL can be determined by using machinery standards, risk graphs or comparing the risks to similar systems. High risks related to the safety function mean more specific requirements. Typically, the required PL for manual drive is "a", "b" or "c" and for automated drive and safety sensors "d" [5].

Human responsibility of safety is an important and much discussed subject. The evaluation of human responsibility and machine responsibility is relevant, as it affects the PL-requirement of a safety function and the actual evaluation

of safety criticality itself. The distribution of responsibilities between operator and machine is related to the level of automation (LOA). Several scales to describe the level of automation have been developed and one such scale is given in Table 1 [10]. Using this scale, it can be stated that the current LOA in safety-critical functions in mobile work machinery is 5 or less and in non safety-critical functions the LOA can be as high as 7 or 8. An example of LOA 7 function is a traction control, which applies the brakes of vehicles, while giving a warning that the system is use to the operator. An example of LOA 8 function is a crane swing control, in which the crane applies small counter movement against the control input to attenuate the swing of the load. The step from LOA 5 to 6 is the most critical, as in this step the responsibilities of the machinery will increase dramatically and this will impose more requirements to the machine's systems in terms of performance. Also in LOA 6 the responsibility in decision making starts to move from the operator. Giving the final control to the operator is a traditional and easily accepted approach, but also other justified opinions exist. This subject has been discussed, for example, by Inagaki [11]. Inagaki gave examples for professional and non-professional operators, where the operators had failed to avoid accidents while using systems containing advanced safety systems that had no total control over machinery. In case of non-professional operators, the operators either ignored safety-systems warnings or were unable to comprehend the situation and risk. In case of professional operators, the operators either made different decision for corrective action than the safety-system and gave conflicting command inputs or failed to complete the corrective action properly. In these cases the situations were difficult to comprehend and the operators were lacking correct and sufficient situational awareness. Inagaki claimed that if the safety-systems in these cases would have had more control over machines actions these accidents would have been avoided [11]. Low LOA is beneficial to human situational awareness. It can be claimed, that autonomous safety functions might be most beneficial where high situational awareness and complex decision making is needed in a limited time frame. In these situations human ability to intervene correctly is already questionable. Lately in automotive industry safety systems that will automatically act if the operator does not take corrective action in a specified time frame. Examples of these kinds systems are pre-crash safety systems and more advanced lane keeping systems (LKS), which will control the car if the driver does not act [12][13]. These systems are first signs of mature technology and therefore safety-critical systems can also start to move to higher levels of automation; LOA 6 or above.

Table 1 Scale of levels of automation [10]

1	The computer offers no assistance, human must do it all.
2	The computer offers a complete set of action alternatives, and
3	The computer narrows the selection down to a few.
4	The computer suggests one.
5	The computer executes that suggestion if the human approves.
6	The computer allows the human a restricted time to veto before automatic execution.
7	The computer executes automatically, and then necessarily informs humans.
8	The computer informs human after execution only if he asks.
9	The computer informs him after execution if the computer decides it.
10	The computer decides everything and acts autonomously, ignoring the human.

3 SAFETY FUNCTIONS UNDER EXAMINATION

The safety functions studied here are related to the situation where a person meets an automated mobile work machine. The person is approaching the machine and many different safety functions can be applied to maintain the safety.

3.1 Safety functions and the requirements

A lot of possible safety functions are already defined in automation related standards, which are not necessarily most suitable for mobile work machines. However, they give a good basis for making own system requirements. It is good to have possibilities what to do when safety need to be maintained. With larger selection of possible safety functions a major problem is defining and designing correct function for all foreseeable hazard scenarios.

The most common safety function is stopping or emergency stopping and it is often a good solution to maintain safety - but not always. In some cases the stopping may cause even a hazardous situation. The machine may not stop at a crossing or a hazardous place (for example there is a risk of falling rocks). There are also new emerging needs

for new and more advanced safety functions. Productivity is increasingly often the reason why some other safety functions are applied instead of stopping. The variety of safety functions include for example reduced speed, manual driving mode, change of direction and change of task. Usually it is more difficult to realize other safety functions than stopping since in most of the cases cutting power stops the machine. Table 2 shows a set of safety functions with references to standards. The functions can be applied as tools in the design of the safety system.

Table 2. Safety functions related to persons beside mobile work machines.

Function	Remarks
Emergency stopping SFS EN 60204-1	Emergency stop function is intended to - avert arising, or reduce existing, hazards to persons, damage to machinery or to work in progress, - be initiated by a single human action. Stop category 0 or 1. Reset is always manual.
Protective stop ISO 10218-1.	This stop circuit shall control the safeguarded hazard by causing a stop of all robot motion, removing power from the robot drive actuators, and causing any other hazard controlled by the robot system to cease. This stop may be initiated manually or by control logic. Reset can be manual or automatic. [1]
Reduced speed (safety speed) for stationary machines SFS-EN ISO 11161	Examples of reduced speeds are: - less than 10 mm/s for presses, - less than 250 mm/s for robots, - less than 250 mm/s for non-shearing hazards, - less than 33 mm/s for shearing hazards. [7]
Reduced speed of AGVs. EN 1525	Safety speed is 0.3 m/s, but additional safety devices are required to stop the AGV (e.g. safety bumpers or laser scanners). Safety function performance is (depending on the case) Cat 1, 2 (stability) or 3 (person detection) according to EN 954-1. [8]
Safety distance (for stopping) SFS-EN ISO 13855	Typically S (safety distance) = $1.6\text{m/s} \cdot (\text{stopping time}) + 0.85\text{m}$. 1.6 m/s is walking speed. This does not include machine speed towards a person; it must be added if needed and in addition there is uncertainty related to the measurement. [3]
Restricted space ISO 10218-1.	Restricted space is a portion of the maximum space restricted by limiting devices that establish limits which may not be exceeded. [1]
Mode change related to level of automation ISO 10218-1	Machine turns from automated to manual mode or operator controls with enabling device (and remote control). Typically the machine stops, when mode is changed as well as level of automation. [1]
Limping mode ISO 15988	Limping mode means reduced speed and limited performance. It is needed when the machine must be driven out of a dangerous place (e.g. crossing) when normal driving is not possible because of a system failure. [4]
Movement towards safe direction EN 280	Related especially to movements towards stable position (e.g. movable elevating work platform) and away from end stop (e.g. with cranes). Some principles can be applied with other systems. [6]
Safety gap EN 349	Safety gap is typically 500 mm for human body. [9]

3.2 Safety functions related to an approaching person

Table 3 shows actions what can be done when the operator is approaching the mobile work machine area. Before the operator enters the area he may prepare the system for the approach by selecting proper operation mode. When the sensors detect the person then the safety distance must be kept feasible by controlling the speed of the machine. If the sensors miss the person although the person should be there then the system must assume that the person may be walking towards any direction. This means that the area occupied for the operator must be increasing until the

person is detected again. This reasoning presumes that there is only one person in the area. If there were two persons in the area then in most cases manual acknowledgement is needed to free an occupied area.

Table 3. Safety functions and actions associated to a person approaching a dangerous mobile work machine.

Situation	Actions to be considered
Human enters the area, but is far from the machine and local sensors	<ul style="list-style-type: none"> – The operator may express his intention with buttons before entering the working area. – A specific operating mode may be chosen. – Specific tasks far from the person may be chosen for the machine. – Machine may be driven to a safe position. – Machine movements can be limited and restricted area function applied for the machine.
First local sensors can detect the person	<ul style="list-style-type: none"> – A specific operation mode may be used – Person should be detected continuously. A missing signal causes an enlarging occupied area for the person. – Specific tasks far from the person may be chosen for the machine.
Human enters the area where stopping distance from full speed is too short for safe stopping	<ul style="list-style-type: none"> – Reduced speed is required. – If reduced speed is not activated, stopping function is activated.
Human is close to the machine. Stopping distance is longer than distance to a person.	<ul style="list-style-type: none"> – Speed is reduced until stopping performance is adequate. – Stopping function can be activated. – Slow movement towards safe direction is possible. – Manual driving is possible
Human may touch the machine	<ul style="list-style-type: none"> – Any specific risks (e.g. rotating parts) may cause additional measures. The height of the dangerous part may affect safety distances.
System failure	<ul style="list-style-type: none"> – First protective stop is activated. If only specific part has failed, some parts of the system may be applied if it does not cause additional danger. – If needed the operator may turn limping mode on, which enables slow movement and/or limited performance.

To keep the safety distance between a person and the mobile work machine adequate all the time the position of the person need to be known, but the accuracy depends on the case. Here is a list of some possible methods to estimate the position of the person:

- The position of the person can be detected with sensors. Sensors can be located on the environment or on the machine. The person may also have, for example, GPS, tag or emitter (UWB), which is applied to measure the location.
- The area can be surrounded by a fence or light curtain, and the opening of the gate is detected. The complete area can be divided into several smaller areas and the entering is detected. The entering occupies the area for the person and other areas need to be released (manually) for the machine operation.
- Person can inform his position by pressing a button or sensors detect the specific workplace. After the person leaves the specific workplace the person occupies increasing area, which is calculated according to the walking speed (1.6 m/s) until the person is detected again.
- The route of the person can be predicted (person can give e.g. a task plan) and verified in specific places along the way.

In order to realize the adequate safety distance also the machine position needs to be determined. This can be related to the movement of a single boom or the complete mobile work machine. Here is a list of methods used to estimate the position of the machine:

- Internal or external sensors can detect the position of the machine. Sensors, which are on the machine, can give information relative to the distance between the person and the machine (e.g. laser scanners).
- The position of the machine can be calculated. Accurate position can be detected in specific places and in other places the position is either calculated or measured with methods, which are not safety rated.

- The machine can have a forbidden area. The area can be continuously the same or it may change according to the production phase.

One important safety-related issue are the conditions to machine movement. Basically the machine should stop if a person is too close to automatically running machine, but there can be exceptions. If the machine is moving towards safe direction the movement can be allowed. There can be also specific modes, which require slow motion of the machine. These situations can be related to troubleshooting, teaching/programming/testing, or removing the machine out from a dangerous place (e.g. crossing). One specific case is related to automatically moving machines, which are passing each other in close distance (different virtual tracks). Also such machines, which come behind a corner without any predefined plan, can be a challenge to safety engineers.

4 DISCUSSION

There is an increasing need to allow safe collaboration in close range between operator and an automated mobile work machine. Usually the goal is to have increased productivity, easier troubleshooting and/or specific performance after failure. In most cases it would be safe to shut down the machine, but it would decrease productivity. The safety area and observation area should change dynamically according to (predefined) risks. Human can stay safely nearby a mobile work machine if the safety distance is smaller than the distance required for stopping the machine movement. The safety distance may occasionally be even shorter if we separate risks into high and low risks. Impact hazard means low risk and slow speed whereas crushing hazard means high risk and protective stop. In many cases, it would be possible for the safety system of the machine to distinguish high and low risk cases if only reliable distances need to be considered.

An important issue is the responsibility of automation in comparison with operator responsibility. In the past, machines were driven by operators and they were responsible for the safety. Currently machines can have automated or semi-automated movements and then the responsibility for safety is not always clear. In limping mode the machine needs to be moveable although there is a system failure and it may be hazardous to apply the machine. Such cases are related to driving a machine away from a dangerous place (limping mode) or applying a machine during troubleshooting. In these cases typically the machine is driven manually and the driver has the main responsibility. During automatic run the automation has responsibility for safety and practically it means that all persons must be kept at a safe distance from the moving machine.

5 REFERENCES

1. ISO 10218-1. Robots and robotic devices - *Safety requirements for industrial robots* - Part 1: Robots. 2011. 43 p.
2. SFS-EN ISO 13849-1. 2008. Safety of machinery — Safety-related parts of control systems – Part 1: General principles for design. Finnish Standards Association SFS 180 p.
3. ISO 13855. Safety of machinery. *Positioning of safeguards with respect to the approach speeds of parts of the human body*. 2010. 40 p.
4. ISO 15988. Earth-moving machinery — Machine control systems (MCS) using electronic components — *Performance criteria and tests for functional safety*. 2008. 33 p.
5. ISO/DTR 15988-2. Earth-moving machinery — Machine control systems (MCS) using electronic components — Part 2: *Guidelines for the use and application of ISO 15988-1*. 2011. 102 p.
6. SFS-EN 280: 2001+ A2:2009. *Mobile elevating work platforms*. Design calculations. Stability criteria. Construction. Safety. Examinations and tests. 2009. 146 p.
7. SFS-EN ISO 11161. Safety of machinery. *Integrated manufacturing systems*. Basic requirements. 2010. 81 p.
8. SFS EN 1525. Safety of industrial trucks. *Driverless trucks and their systems*. 1998. 23 p.
9. SFS-EN 349. Safety of machinery. *Minimum gaps to avoid crushing of parts of the human body*. 2008. 23 p.
10. Sheridan, T.B., 1992. *Telerobotics, Automation, and Human Supervisory Control*. MIT Press, Cambridge, MA
11. Inagaki, T. 2003. *International Journal of Industrial Ergonomics* 31 (2003) p.169-174
12. Pre-crash Safety System. http://www.toyota-global.com/innovation/safety_technology_quality/safety_technology/pre-crash_safety/ (visited 24.8.2012)
13. Lane Keeping Assist. http://www.toyota-global.com/innovation/safety_technology_quality/safety_technology/technology_file/active/lka.html (visited 24.8.2012)

Design of fault-tree-based software to improve the safety of printing press operators

Laurent Giraud, Sabrina Jocelyn – IRSST, Mechanical and Physical Risk Prevention
505, Boulevard de Maisonneuve Ouest, Montréal, Québec, Canada, H3A 3C2 – giraud.laurent@irsst.qc.ca

KEY WORDS: fault tree, safety, printing press, nip point, knowledge transfer

ABSTRACT

In the occupational health and safety field, the different actors create new knowledge every day. However, if this knowledge is not transferred to workplaces, it may not be used by workers. This transfer can occur in several ways: legislatively (the most coercive), scientifically (peer-reviewed articles), classically (guides, brochures) or in a modern way (software, applications).

Printing presses are machines with numerous hazards associated with nip points for the workers who use them. Several studies have been devoted to this subject from different angles (machine, ergonomics, work organization, etc.). Following a request from an OHS organization in this industry, the IRSST conducted a study to improve workers' safety during five operations on an offset printing press. The main question was to determine whether the intervention could be carried out without locking out the press. If it could, safe intervention procedures had to be developed based on a fault tree produced by the researchers. A scientific report and a guide were produced following this study.

To establish better contact with the printing industry and to provide added value to the knowledge, the IRSST research team and ASP Imprimerie (joint sector-based printing association) created an interactive application, based on the previous research results, for safeguarding printing presses.

The application invites users (OHS managers in companies, OHS advisors, etc.) to produce a list of their printing presses, and then requires them to evaluate the safety of each of the presses by means of a questionnaire. Once the questionnaire has been completed, a corrective action plan can be generated if needed. Then, a logic diagram allows the user to validate his needs for hazardous area intervention without lockout. For this, the results of the questions are used by logical formulas to verify the consistency of the answers and to validate logical conditions. Finally, safe generic intervention procedures for the five identified tasks can be generated. At any time, the user can also consult the related fault tree to visualize the possible sequence between the different causes of the accident involving a nip point.

The main contribution of this software is at two levels. First, it makes it possible to go from a static tool (guide) to a dynamic tool. Second, based on logical formulas, it validates the hazardous area intervention conditions according to the principles used in machine safety (example: section 4.11.9 of ISO 12100:2003). This points the user towards the type of intervention most adapted to his work situation (safeguarding of the hazardous areas, lockout, safety stop, etc.).

1 INTRODUCTION

Printing presses, while essential to the printing sector, have numerous hazardous areas, including nip points, more or less accessible by the workers using these machines. The risk associated with these machines has been known for a long time. In his book "Machine Guarding," Roberts [1] mentions many patents filed in the United States, such as: the first guard was patented for use on a printing press (Patent No. 185 241 - 1876) to limit access to a nip point, a mechanically locked guard (Patent No. 865 800 - 1907) was patented to be used on a printing press. Closer to home, accidents occur with these machines [2, 3]. Many studies have been carried out, in numerous fields (machine, ergonomics, work organization, etc.), by the INRS [4, 5, 6] and by the IRSST [7] to reduce the risk associated with the use of these presses. Finally, these machines are generally designed with a control system that integrates the principles of intrinsic protection [8, 9] by means of a function called *Safe* that allows the operator to maintain control of the press. The most recent study by the IRSST focused on utilization practices, related to the work in the printing sector, during which the operators are exposed to hazards related to nip points during the five following operations:

- Inking roller cleaning,
- Blanket cleaning,
- Plate removal and insertion,
- Blanket removal and installation,
- Paper feeding/threading.

The research objective was to validate a fault tree (FT) associated with the undesired event: “crushing of part of the worker’s body by one or more rollers/drums of the printing press during an operation.” It was shown that lockout was not an appropriate solution and that the use of safe work procedures was necessary. Once solutions are found, this knowledge must be transferred to the designers and users so that it can be used. In the occupational health and safety field, this transfer can be achieved by means of several vectors (Table 1): legislatively (law [10], regulation [11], recommendation [12]); scientifically (peer-reviewed articles [5], books); normatively (international [13], multinational [14], national [15]); classically (guides [16], brochures, posters, investigation report [2, 3]); or in a modern way (software, applications).

Table 1. Transfer vectors in OHS

Vector	Target population	Advantages	Disadvantages
Legislative Law Regulation	Any person or organization targeted by the law or regulation	Text accessible by everyone	Legal document, little detail, limited updating
Scientific Report Article	Researchers, peers, motivated readers	Informative, precise, detailed, references	Length, scientific language, complicated language
Normative Standard	Designers, educated users, motivated readers	Mandatory if mentioned in legislation or in a contract	Acquisition cost, knowledge of its existence, difficult to understand, numerous sources
Classical Brochure Guide	Fieldworkers, OHS advisors, supervisors, workers	Simplification of the text and ideas, illustrations	Static, and in our case: necessary recopying of procedures, no navigation in the FT
Modern Software Computer-based tool	OHS advisors, foremen, supervisors, workers	Dynamic, easy to use, management of company machines, links to the mentioned references	In our case: limitations imposed by Excel®, computer-based tool and updates to be manually downloaded

2 CHOICES FOR KNOWLEDGE TRANSFER

In the case of the study carried out at the IRSST [7], the research team decided to transfer the results in four ways: a research report (for peers), a guide (for OHS advisors, supervisors, workers), a pocket guide (for workers), and a computer-based tool (for OHS advisors, foremen, supervisors, workers). The emphasis in knowledge transfer was on the workers because they are the ones who use these machines. To date, the pocket guide has been abandoned, the report and guide have been published, and the computer-based tool is awaiting dissemination. The aim of this article is to present the operation of the computer-based tool, the knowledge that it generates, as well as the different aspects of its design.

3 THE COMPUTER-BASED TOOL

3.1 Operation

The application, under Excel®, asks the user (OHS manager in the company, OHS advisor, press operator, etc.) to create a list of the company’s printing presses. Then, to continue to use the computer-based tool, the safety of each of the presses must be evaluated by means of a questionnaire. The questionnaire associated with each press must be completed to be able to move on to the subsequent steps.

Once the questionnaire is filled out, a corrective action plan can be generated if answers are not valid. Then, by means of a dynamic logic diagram, the user can validate his intervention needs without locking out the hazardous area. For this, logic functions verify the consistency of the responses to the questions and the logical conditions.

Once this step has been completed, generic safe intervention procedures for the five identified operations can be visualized and generated. At any time, the user can also consult the associated fault tree to visualize the possible link between the different causes of accidents involving a nip point.

3.2 Knowledge to be transferred

The knowledge to be transferred in the computer-based tool was mostly contained in the research report [7] and the published guides [16, 17].

It consists of:

- Application logic diagram of article 186 of the ROHS [17];
- Safe work procedures associated with five operations: cleaning of inking rollers, cleaning of blankets, changing of printing plates, changing of blankets, and threading of paper;
- Fault tree and cited references;
- Links between procedures and fault tree;
- General evaluation grid of machine hazards for a printing press.

However, going from a report or a guide to a computer application requires the introduction of new knowledge. In fact, static information must be converted into dynamic information. For example, each procedure contains references to the fault tree, which have to be made dynamic. As well, in creating the computer-based tool, the team considered it advisable for the user to adopt the same principle of referring to the fault tree for the questionnaire. Therefore, the most relevant elements of the fault tree had to be identified for the selected questions.

4 DESIGN OF THE COMPUTER-BASED TOOL

4.1 The questionnaire and the action plan

The questionnaire used in the computer-based tool is an adaptation of the tool available in a machine safety guide [17]. The architecture of this guide's questionnaire was retained. The questionnaire has 72 questions, two more than the guide. Nine questions were added in a second section, to specify the technical means for reducing the risks present on the press.

The advantages of the dynamic questionnaire are:

- Real-time validation of the answers;
- Displaying of the correction to be made in the event of an incorrect answer;
- Links to the fault tree to explain the relevance of the question;
- The help available (to explain terms such as "positive mechanical action").

Once the questionnaire has been completed, the user can produce, if desired, an action plan that reconsiders all the invalid answers as well as all the proposed corrections. He can then select one of the five operations to meet the conditions of the logic diagram.

4.2 The logic diagram

The logic diagram in the computer-based tool was produced in a two-phase evolution (Table 2): going from section 186 of the ROHS [11] to the static logic diagram of the guide [17] (not done by the research team), and then to the dynamic logic diagram of the computer-based tool. These evolutions required many hours of reflection and work, mainly for the dynamic logic diagram. In fact, even though the principle was known, its application is never as simple as expected.

Table 2. Evolutions in relation to section 186

Step	Situation	Evolutions
0	Section 186 of the ROHS	
1	Static logic diagram	Breakdown of section 186 into 6 sequential logical conditions Proposal of means of risk reduction in relation to the different possible answers at each step
2	Dynamic logic diagram	Answers asked directly to the user for the first three logical conditions Use of the answers to the questionnaire for the next three logical conditions Verification of compliance (regulatory, normative), of the consistency and logic of the answers used by means of logical rules

The central point of the computer-based tool is section 186 of the ROHS [11], equivalent to section 4.11.9 of ISO 12100-2:2003 [8]: “Adjustment, repair, unjamming, maintenance and apprenticeship: When a worker must access a machine's danger zone (LC2)* for adjustment, unjamming, maintenance, apprenticeship or repair purposes, including for detecting abnormal operations (LC 1), and to do so, he must move or remove a protector (LC 4), or neutralize a protective device, the machine shall only be restarted (LC 3) by means of a manual control or in compliance with a safety procedure specifically provided for allowing such access. This manual control (LC 4) or this procedure shall have the following characteristics:

1. it causes any other control mode or any other procedure, as the case may be, to become inoperative (LC 6);
2. it only allows the operation of the dangerous parts of the machine by a control device requiring continuous action (LC 5) or a two-hand control device;
3. it only allows the operation of these dangerous parts under enhanced security conditions, for instance, at low speed, under reduced tension, step-by-step or by separate steps (LC 5).”

* LC 1, LC 2, LC 3, LC 4, LC 5 and LC 6 refer to the logical conditions detailed below.

4.3 The logical conditions

Six logical conditions (LC) in series are used to validate access to the safeguarding procedures. The first three (LC 1, LC 2, LC 3) are simple questions that the user must answer. The last three (LC 4, LC 5, LC 6) are validated by the software by finding the information in the previously answered questionnaire.

Validation of each logical condition allows the user to advance to the next one. However, non-validation of one of them generates a message questioning the user, and interrupts the process. This allows the user to be directed (Table 3) towards the type of intervention most adapted to his work situation (safeguarding of the hazardous area, lockout, safety stop, etc.) or towards improvement of the safety of his machine if he wants to apply section 186.

Table 3. Flowchart of the logical conditions

LC	If YES	If NO
LC 1	Go to LC 2	Control the hazardous area (cf. ROHS, sec. 182)
LC 2	Go to LC 3	Lockout not required. Control the hazardous area (cf. ROHS, sec. 182)
LC 3	Go to LC 4	Lockout necessary (cf. ROHS, sec. 185)
LC 4	Go to LC 5	Lockout necessary (cf. ROHS, sec. 185) as long as the conditions of section 186 have not been satisfied
LC 5	Go to LC 6	Lockout necessary (cf. ROHS, sec. 185) as long as the conditions of section 186 have not been satisfied.
LC 6	Access to procedures	Lockout necessary (cf. ROHS, sec. 185) as long as the conditions of section 186 have not been satisfied.

The logical conditions used are:

- LC 4: If Q312 = YES and (Q411 or Q421 or Q461) = YES, then LC 4 = YES (Table 4)
 - Questions Q411, Q421 and Q461 deal respectively with the presence of a locking device, interlocking device, or of some other type (optical curtain) associated with the *Safe* function (Q312). This logical condition makes it possible to verify the link between the guard and the control system in compliance with section 186 of the ROHS (legislative).
- LC 5: If (Q321 and Q322 and Q323) = YES or (Q331 and Q332 and Q333) = YES, then LC 5 = YES (Table 5)
 - Question Q321 deals with the presence of a hold-to-run control device, and questions Q322 and Q323 with its correct operation (crawl and stop if the control is released); questions Q331, Q332 and Q333 are similar and deal with the presence of a step-by-step or a separate-steps control device. This logical condition is legislative (verification of the existence of a control requiring continuous action, or hold-to-run control device) and normative [9] (verification of the correct operation of the control requiring continuous action). The case of a two-hand control is not dealt with by the computer-based tool on purpose, because only a minority of presses have such a control device.

- LC 6: If (Q311 = YES and Q313 = YES and Q314 = NO and Q315 = NO and Q511 = NO), then LC 6 = YES (Table 6)
 - Questions Q311, Q313, Q314 and Q315 deal with the *Safe* function: Q311, availability in each unit (legislative compliance), Q313, priority over all the other modes of control (legislative compliance), Q314, impossibility of operating the press in crawl speed (legislative compliance) and Q315, single control point (consistency of *Safe* function – Warning: this *Safe* function is different than the Stop/SAFE device mentioned in ANSI B65.1, sec. 11.2.3.1.2 [15]); question Q511 verifies the impossibility of having the press operate at production speed when a guard is open (consistency of the answers to the questionnaire).

Table 4. Validity conditions of LC 4

Q312	Q411	Q421	Q461	LC 4
1	1	0	0	1
1	0	1	0	1
1	0	0	1	1
1	1	1	0	1
1	1	0	1	1
1	0	1	1	1
1	1	1	1	1
1	0	0	0	0
0	0 or 1	0 or 1	0 or 1	0

Table 5. Validity conditions of LC 5

Q321	Q322	Q323	Q331	Q332	Q333	LC 5
0 or 1	0 or 1	0 or 1	1	1	1	1
1	1	1	0 or 1	0 or 1	0 or 1	1
Any other combination						0

Table 6. Validity conditions of LC 6

Q311	Q313	Q314	Q315	Q511	LC 6
1	1	0	0	0	1
Any other combination					0

4.4 The generic safeguarding procedures

Other foolproof rules were also used to block or allow the use of generic safe work procedures based on the answers to the questionnaire. Five procedures are available, one per operation.

The computer-based tool can block their use for several reasons:

- Non-validation of a logical condition (LC 4 or LC 5 or LC 6);
- Lack of normal stopping device for the press (legislative - ROHS sec. 190);
- Lack of emergency stop (legislative - ROHS sec. 192);
- Lack of a reverse control (legislative - ROHS sec. 190).

The computer-based tool was programmed not to integrate, for certain procedures, technical means of risk reduction if they are not present on the machine:

- Nip point guard;
- Trip nip guard;
- Independent units;
- Guide for winding the plate;
- Reliable design of the control system (allowing the installation of a roller washer instead of the movable guard – inhibition of the movable guard).

When all the conditions have been met, an “.xls” version of the procedure is exported and the user must, if necessary, adapt it to the press. He can also add pictures or comments to make his application easier.

4.5 The fault tree

Finally, a lot of work was done to make the fault tree dynamic and to create links between the questionnaire or the procedures and the fault tree.

The main part of the work dealt with the dynamic navigation inside the tree: the user can start with the undesired event and go down and then up each of the branches of the tree. When the legislative or normative references provide additional information, these references are cited in the tree, next to the causes of failures involved. Once the copyright agreements have been obtained, the user will have access to a relevant extract from the cited reference. A non-negligible part of the work dealt with the graphical aspect of the tree.

The creation of dynamic links between the questionnaire and the fault tree (to explain the importance of the questions asked), as well as between the procedures and the fault tree (to situate each cause of failure in relation to the accident) also required time and reflection.

5 CONCLUSION

There are numerous modes of knowledge transfer that can be used in the OHS field and particularly in machine safety. The transfer vectors can be legislative, scientific, normative, classical or modern. In the context of this study on printing press safety, the research team used a modern vector (computer-based tool) to make not only knowledge transfer more dynamic, but also its use in the framework of the generation of safe work procedures. This passage from static information to dynamic information required reflection and effort, but on the other hand, it guides the user and warns him of his mistakes and errors. This guiding is based on the use of a questionnaire and logical rules. The questionnaire makes it possible to assess the safety of the press, and its results are handled by logical rules that translate the applicable regulatory requirements and good practices. Through this computer-based tool accessible at no charge, the research team's goal is to reduce accidents on printing presses not locked out due to the necessary presence of energy to perform certain operations.

6 REFERENCES

1. Roberts V. L., *Machine Guarding – A Historical Perspective*, Durham, North CA., Institute for Product Safety, 1980.
2. Commission de la santé et de la sécurité du travail du Québec, *Rapport d'enquête d'accident : accident mortel survenu à un travailleur, écrasé par une presse platine, le 10 septembre 2007 à l'entreprise Montage et découpage Promag inc., 8451, rue Parkway à Montréal*, CSST, Québec, EN-003718, 2008.
3. Commission de la santé et de la sécurité du travail du Québec, *Rapport d'enquête d'accident : accident grave survenu à un travailleur le 29 novembre 2006 à l'entreprise Québécois World inc., 8000, rue Blaise-Pascal à Montréal*, CSST, Québec, EN-003662, 2007.
4. Fadier E, Neboit M., Cicotelli J, *Intégration des conditions d'usage dans la conception des systèmes de travail pour la prévention des risques professionnels - Bilan de la thématique 1998 – 2002*, Les notes scientifiques et techniques de l'INRS, NS 0237, 2003, 40 p.
5. Fadier E., De La Garza C., Didelot A., *Safe design and human activity: construction of a theoretical framework from an analysis of a printing sector*, Safety Science, Vol. 41, N° 9, 2003, pp. 759-789.
6. Abecassis P., Andeol B., Auburtin G. et al. *Évaluation et prévention des risques dans les petites imprimeries offset*, Documents pour le médecin du travail, INRS, No 94, p. 109-146.
7. Giraud L., Jocelyn S., Aucourt B. et al., *Intervenir sur les presses à imprimer - Validation d'un arbre de défaillance associé aux risques mécaniques*, Études et recherches / Rapport R-671, Montréal, IRSST, 2011.
8. Organisation internationale de normalisation, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 2: Principes techniques*, ISO, Genève, ISO 12100-2, 2003.
9. Organisation internationale de normalisation, *Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque*, ISO, Genève, ISO 12100, 2010.
10. Gouvernement du Québec, *Loi sur la santé et la sécurité du travail*, Québec, L.R.Q., c. S-2.1, 2012
11. Gouvernement du Québec, *Règlement sur la santé et la sécurité du travail*, Québec, S-2.1, r.13, 2012.
12. Caisse nationale de l'assurance maladie des travailleurs salariés, *Prévention des accidents du travail et des maladies professionnelles dans les industries du livre – Recommandation R 121*, INRS, Paris, 1991.
13. Organisation internationale de normalisation, *Sécurité des machines – Distances de sécurité empêchant les membres supérieurs et inférieurs d'atteindre les zones dangereuses*, ISO, Genève, ISO 13857, 2008.
14. Association française de normalisation, *Sécurité des machines - Prescriptions de sécurité pour la conception et la construction de machines d'impression et de transformation du papier - Partie 1 : prescriptions communes*, AFNOR, Paris, NF EN 1010-1, 2004.
15. American National Standards Institute, *Graphic technology – Safety standard – Printing press systems*, ANSI B65.1, 2005.
16. Giraud L., Ménard M., *Comment se protéger des angles rentrants en imprimerie – Procédures sécuritaires recherchées*, ASP imprimerie / IRSST, Montréal, 2010.
17. Laurenzi N., *Comprendre les risques associés aux machines en imprimerie – Pour agir en prévention*, ASP imprimerie, Montréal, 2^e ed., 2011.

The Improvement of Industrial Safety achieved by the Introduction of Safety Assessor / Safety Basic Assessor Qualification System and its International Operations.

Masahiro Tochio*1, Kyota Nakayama*2, Takahiko Arai*2, Shunsuke Nonoaka*2,
Masaru Shiomi*2, Hiroo Knamaru*2, Hisao Toyama*1, Toshihiro Fujita*2,
Hiroyuki Takaoka*3, Masao Mukaidono*4

*1 Japan Certification Corporation, 2-7-53 Nishimiyahara , Yodogawa-ku, Osaka, Japan, e-mail:tochiom@j-cert.com

*2 Nippon Electric Control Equipment Industries Association, 2-1-17 Hamamatsucho, Minato-ku, Tokyo, 105-0013, Japan

*3 Asahi Glass Co., Ltd., 1-5-1, Marunouchi, Chiyoda-ku, Tokyo 100-8405 JAPAN

*4 Meiji University, 1-1-1 Higashimita Tamaku, Kawasaki, Kanagawa, Japan

KEY WORDS: safety assessor, safety basic assessor, qualification system, risk communication

ABSTRACT

The safety of machinery based on ISO 12100^[1] is absolutely necessary in order to realize the safety of industrial automation systems and to prevent occupational accidents. Its essential concept is an engineering method for the design of the machines utilizing the risk assessment and the three-step- method. However, the safe machine itself is not enough to decrease occupational accidents. If machine users do not have any knowledge on the safety of the machinery, they operate machinery with the residual risk in inappropriate way such as the defeating of the protective devices and the modifying machine. Everyone who deals with the machine during its lifecycle should have enough knowledge on the safety of the machinery.

Nippon Electric Control Equipment Industries Association (NECA), Japan Certification Corporation (JC), The Society of Safety Technology and Application (SOSTAP) and TUV Rheinland Japan established Safety Assessor qualification system (SA)^{[2][3][4]} and Safety Basic Assessor qualification system (SBA)^{[5][6]} in order to develop engineers, machine users and managers who understand safety technology and safety knowledge for ensuring machine safety and safety control. The qualification system contains education programs and certifying tests on international safety standards. The SA course is suitable for machine designers, while the SBA course is for machine users. The person qualified as SA can design safe industrial automation systems, and the person qualified as SBA can use the machine and the system safely. The requirements for SA are the skill of performing the risk assessment and ability of machine design with the three-step-method. The requirement for SBA is the basic knowledge on the safety of machinery. Today the number of qualified persons of SA is more than 3,000 and more than 800 for SBA.

In this paper we report a case study of SA and SBA systems which shows company's effective introduction of SA and SBA systems to achieve industrial safety in Japan and overseas. We also report the implementation and the expansion of SBA systems not only in Japan but also in East Asia and ASEAN countries, Korea, Taiwan, Indonesia, China, Thailand, and Philippines.

1. BACKGROUND

It took more than 10 years, from many standards for safety including ISO12100 are put into international standards. These standards show that how to design safety machines. And these standards are applied on the industrial field of many countries. Though, many industrial accidents take lots of lives of workers. This is partly due to a lack of risk assessment, risk reduction and inappropriate treatment of residual risks. Machine safety is still on the way to disperse.

On 2003, Nippon Electric Control Equipment Industries Association (NECA), Japan Certification Corporation (JC), The Society of Safety Technology and Application (SOSTAP) and TUV Rheinland Japan established Safety Assessor Qualification System (SA) for risk assessment and risk reduction. Now there are more than 3,000 holders. Eligible persons are increasing more and more.

In addition, NECA and JC established Safety Basic Assessor Qualification System (SBA) for treatment of risk reduction on 2010. Today more than 800 holders are certified. These 800 holders include more than 200 Asia country's holders. This qualification system is getting around the world.

However, to prevent accidents, effort of each certified person has limitations. One designer can design only part of a machine. One operator can treat few machines. Organized activity that manages certified persons is effective. Designer's team can design whole of a machine. Operator's team can treat whole of factory. For success of machine safety, coordinated effort is significant.

In this paper, first we make brief of SA and SBA and its expansion. Then case study of SA and SBA systems which shows company's effective introduction to achieve industrial safety in Japan and overseas.

2. SAFETY ASSESSOR AND SAFETY BASIC ASSSOR QUALIFICATION SYSTEM

2.1 Relationship of Safety Assessor and Safety basic Assessor

Basically machine safety is methodology for machine designers as ISO12100 says. Machine designers know about a machine and its hazards rather than machine users. But even machine designers cannot eliminate hazards and risks of a machine completely. A machine should have residual risks. And machine users must treat residual risks to prevent their injury. Machine users should accept residual risks.

If machine designers design without users opinions, a machine might be awkward to use. A machine might be hard to access, often stops and has any troubles to use. Then machine users might remove safety measures like guards and interlock switches. And they are exposed to hazards.

To avoid these unfortunate situation, machine designers and machine users should make communication with result of risk assessment. This communication is called risk communication. Machine designers and machine users show conditions (purpose, quality, cost, deadline and etc.) each other. Through this conversation, adequate safety measurements are determined and residual risks are clearly specified. (see Figure 1)

For this risk communication, Safety Assessor Qualification System aims machine designers and safety Basic Assessor Qualification System aims machine users.

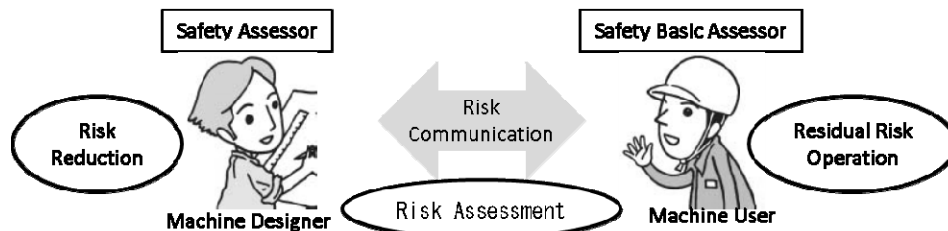


Figure 1. Relationship of Safety Assessor and Safety Basic Assessor

2.2 Framework of Safety Assessor and Safety basic Assessor

Figure 2. shows conceptual hierarchy diagram of qualifications in Safety Assessor and Safety Basic Assessor . and table 1. shows major requests for each qualification.

Safety Assessor Qualification System is classified into three levels (Safety Lead Assessors (Gold level), Safety Assessors (Silver level) and Safety Sub Assessor (Blonde level)). Safety Sub Assessor qualifies who has ability for risk assessment. Safety Assessor qualifies who has ability for risk assessment and risk reduction. Safety Lead Assessor qualifies who has explanation capability for risk assessment and risk reduction.

Safety Basic Assessor Qualification System is classified into one level. Safety Basic Assessor qualifies who has basic knowledge of risk assessment and risk reduction.

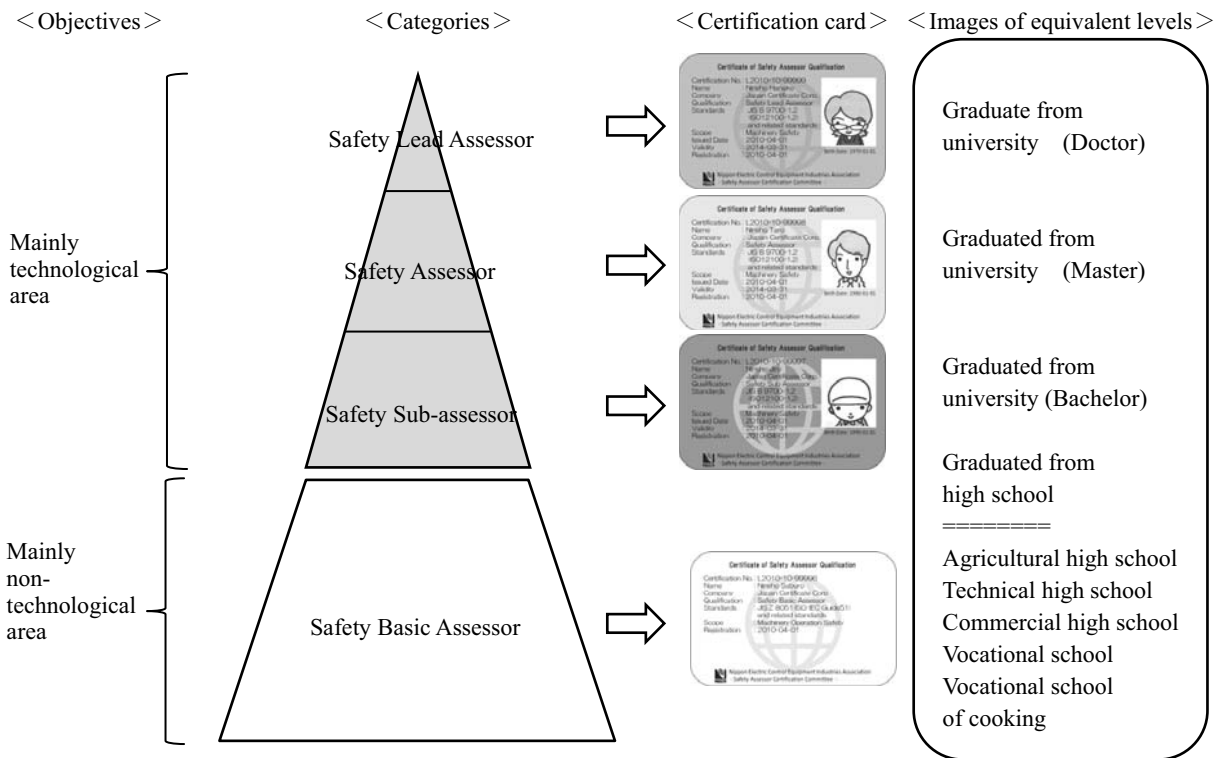


Figure 2. Conceptual hierarchy diagram of qualifications in Safety Assessor and Safety Basic Assessor^[6]

Table 1. Outline of qualifications in Safety Assessor and Safety Basic Assessor^[6]

Areas	Categories	Qualifications	Objectives
Machine safety	Safety Lead Assessor	Having abilities for risk assessment and guidance of manufacturing facilities	Leader
	Safety Assessor	Having abilities for risk assessment (evaluation and measures) of manufacturing facilities	Design and development
	Safety Sub Assessor	Having abilities for risk evaluation of manufacturing facilities	Design, development, sales and maintenance
Safety in machine operation	Safety Basic Assessor	Having basic knowledge on safety for maintenance, operation and management of manufacturing facilities with risk assessment, in each stage of their lifecycles	Manufacturing operators, persons in departments, general affairs, personnel, purchase, sales and maintenance

2.3 Increase in the number of Safety Assessor and Safety Basic Assessor holders

Figure 3. shows changes in total number of certificate holders from 2004 to 2011. As of March, 2011, the numbers of Safety Lead Assessors, Safety Assessors and Safety Sub Assessors are 34, 468, 2536 respectively and total 3038. Safety Basic Assessor are total 949 (including 265 Asian holders).

Figure 4. shows changes in total number of companies, from 2004 to 2011, where certificate holders belong. Today total 479 (Safety Assessor 374, Safety basic Assessor 105) companies have holders.

In Japan numbers of these holders become have social power.

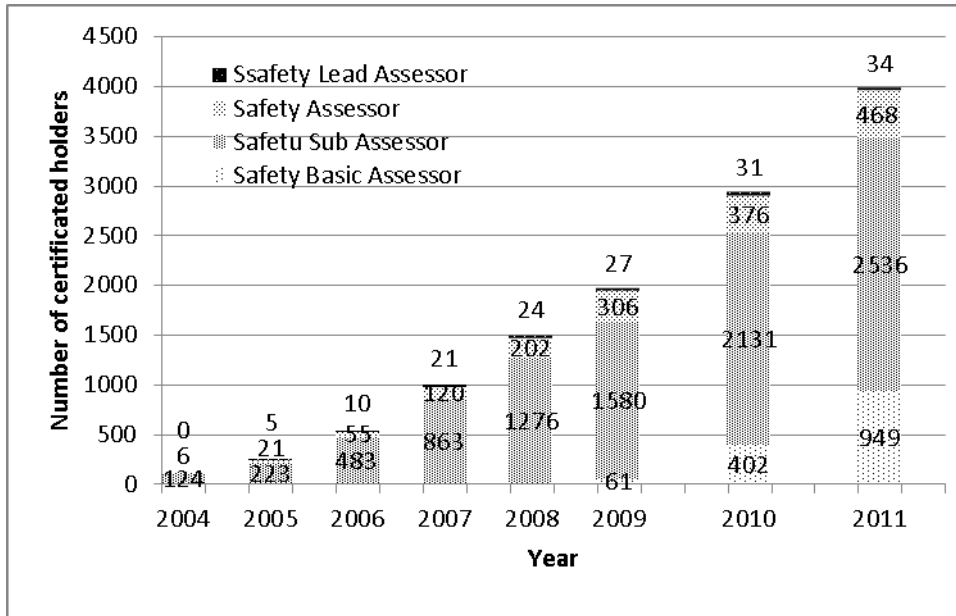


Figure 3. Changes in total number of certificate holders



Figure 4. Changes in total number of companies where certificate holders belong

3. CASE STUDY OF ASAHI GLASS Co., Ltd.

3.1 Purpose and strategy of application of Safety Assessor and Safety Basic Assessor

Safety Assessor and Safety Basic Assessor Qualification System is private qualification. Hence application of this qualification system can be arranged freely. Here shows application of ASAHI GLASS Co., Ltd.(AGC) that uses this qualification system effectively.

AGC has a strong policy “We do not accept machine equipment without design risk assessment”. For this policy, AGC assigns Safety Sub Assessor and Safety Assessor to not only “equipment design department”, “equipment maintenance department”, “environment and safety department” but also “business partner”. By this assignment, adequate person implements design risk assessment for their equipment. Especially “business partner” assumes a crucial role. In Japan, small and medium-sized companies do not have enough knowledge and skill of risk assessment. Support by leading company is very effective and important to disperse risk assessment.

AGC’s next problems were cheating and dangerous reconstruction. To prevent these, AGC assigns Safety Basic Assessor to “production department”, “machine equipment department of oversea” and “production department of over sea”. For global company, using same policy and machine specification make high business efficiency.

3.2 Result Example of this case study

Figure 5. shows comparison between before test and after test for Safety Basic Assessor. After test, average point increases about 12 points and dispersion decreases about 45 points. This means that Safety Basic Assessor increases and homogenizes ability of person.

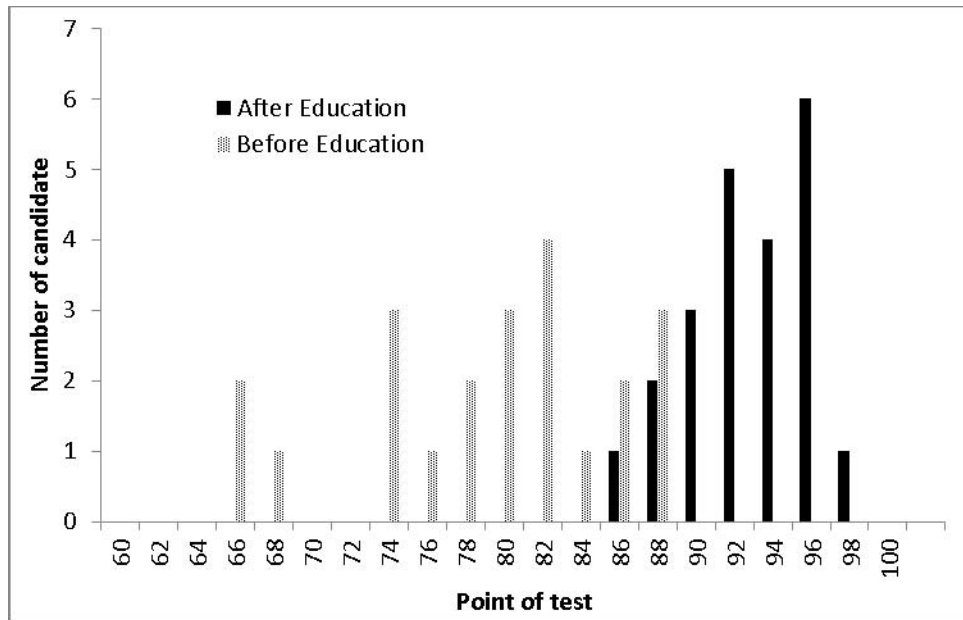


Figure 5. Effect of Safety Basic Assessor

Figure 6. shows Global launch of Safety Basic Assessor. This qualification system is getting accepted all over the world as effective safety qualification.

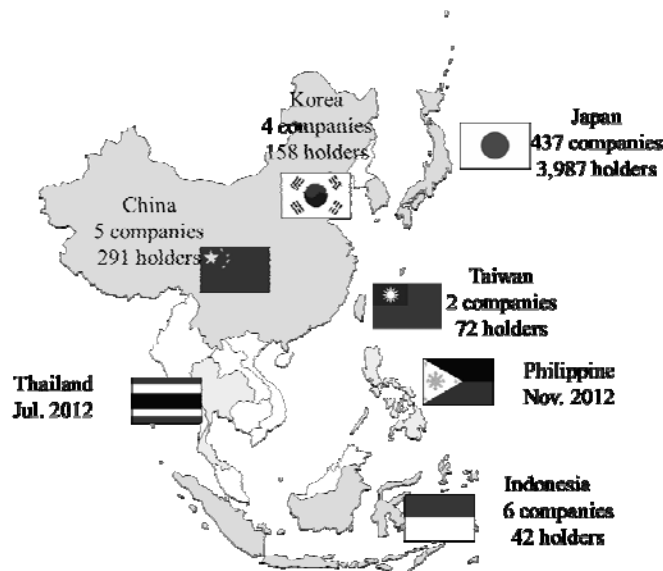


Figure6. Global launch of Safety Basic Assessor

AGC's safety approaches are not only Safety Assessor and safety Basic Assessor but also other many activities. From 2006 to 2010, they could decrease occupational accident about 50% by all safety activities including Safety Assessor and Safety Basic Assessor.

4. SUMMARY

This paper introduced the progress in Safety Assessor Qualification System and Safety Basic Assessor Qualification System. Then AGC's very aggressive applications are introduced as case study.

Authors will develop these systems widely in the world to contribute to realization of safe society. Further, we plan to be involved in standardization activities from the international point of view. We always welcome frank opinions from experts involved in safety and people in workplaces.

5. Acknowledgements

We would like to sincerely express our appreciation to Naotake Fujishiro, Ministry of Economy, Trade and Industry, Masatoshi Suzuki, Society of Safety Technology and Application, Japan for kindly providing guidance, and other people for devoted cooperation in promoting the Safety Assessor Qualification System. We would also like to thank all the members of the certification committee for discussing the Safety Basic Assessor Qualification System.

6. REFERENCES

- [1] ISO12100 Safety of machinery-Basic concepts-General principles, International Organization for Standardization, 2003
- [2] NECA 0901 Criteria for certification of Safety Assessor Qualification, Nippon Electric Control Equipment Industries Association, 2007
- [3] Y.Ishida, T.Yamamoto, Y.Matsueda, R.Maeda, M.Mukaidono, T.Fujita, The Creation of a the Safety Assessor Accreditation System in Japan, SIAS, 2005
- [4] I.Kumazaki, R.Maeda, T.Arai, Y.Ishida, M.Mukaidono, Safety Assessor Program Assessment, SIAS, 2007
- [5] NECA 0902 Criteria for certification of Safety Basic Assessor Qualification, Nippon Electric Control Equipment Industries Association, 2009
- [6] M.Tochio, K.Nakayama, S.Nonaka, M.Shiomi, H.Kanamaru, H.Kojima, H.Toyama, T.Fujita, H.Kasai, M.Mukaidono, The implementation of Safety basic Assessor system to expand the awareness of safety complied with inter national standards for engineers and non-engineers in Japan and Asian Countires, SIAS, 2010

Designing and Building Machines Really Safe: How to Pass from Myth to Reality?

Patrik Doucet, Université de Sherbrooke
patrik.doucet@usherbrooke.ca

Alain Brassard, Roche Ltd
alain.brassard@roche.ca

Key-words: design for safety, safe machines, standard, law

SUMMARY

In an investigation, the Quebec Occupational Health and Safety Commission (CSST) hired an expert to explain the reasons leading to the accidental starting of a machine, which caused a fatal accident. In his defense, the employer hired another expert. Thus, two experts, sharing similar knowledge, found themselves in front of a judge to oppose their respective views. In this case, the CSST mainly argued that the method of maintenance of the machine was dangerous and that the management of health and safety during machine maintenance was deficient. However, according to normative literature, working methods are useful means of risk reduction, but less effective than other solutions, such as using protective devices or achieving intrinsic prevention. On the other side, the employer argued that the machine was not fully safe and had not been designed according to state of the art. For example, the removal of a guard was necessary to make adjustments, which could be made effectively only when the machine was running, thus exposing the workers to a pinch point. In addition, there was a program error in the PLC, which induced dangerous startup. In short, there were a number of design defects in line with safety aspects'. Thus, the question asked by the defense was: Why did a recently designed and built machine present such major deficiencies, while the state of the art is becoming more established, documented and disseminated? In this case, it became clear in the eyes of the experts that their views on the accident were not opposed, quite the contrary: they were complementary. While the establishment of safe work practices and training of workers is needed, these means of risk reduction are not sufficient. The machine itself must be designed while considering anticipated interventions and reasonably foreseeable misuses; safety standards are unanimous on this point. This is also a requirement for engineers, who must participate in the design of all machines: safety of the users must be taken into account at the early design stages. So, how can we explain the verdict given by the judge, namely that the employer was solely responsible for the accident? In this paper, the authors propose to present their analysis of this fatal accident, based on regulations in force and on relevant standards. The question that will emerge is, What can the community of machine safety experts do so that "safe machine design" can become a reality?

1 INTRODUCTION

In 2006, a fatal accident occurred in a Quebec business. While attempting to remove a piece of debris that had become lodged between the belt and tail pulley of a conveyor, a worker was dragged in by the re-entrant angle created when the machine suddenly started up. After investigation, the Quebec Occupational Health and Safety Commission (*Commission de la santé et de la sécurité du travail du Québec*, or CSST) brought the case against the employer to court. To elaborate its report, the CSST hired a machine safety expert. For the defense, the employer called upon the services of a law firm, which also hired a machine safety expert. In court, these two engineers—who knew each other and shared similar knowledge—presented their points of view on the possible causes of the accident. While they were required to present opposing views in this particular context, it appeared evident to them that they agreed on the same basic idea: certain causes, more fundamental in this accident, had not been taken into consideration by the CSST.

This report relates the essentials of the investigation, the expertise involved, and the decision made in the case. Section one describes the accident in question, which is used to illustrate the points of the authors. However, it is important to understand that this is only one example among others, whether real or potential. Section two examines the causes cited to explain the accident, from three points of view: that of the CSST, the employer, and the court. In light of this threefold perspective on the accident, a discussion will be presented on the conditions needed to improve machine safety. The discussion sets the stage for a crucial question: Is a change in legislation required in order to take the design of truly safe machines from a myth to a reality?

2 EXPLANATION OF THE ACCIDENT

To preserve the anonymity of the parties involved, the accident will be described in general terms. Nevertheless, this section will present the details needed to understand its causes.

A few days before the tragedy, a production incident caused a conveyor belt to lose its alignment. The fixed guard around the tail pulley had to be removed in order to be able to access an adjustment screw. This part of the equipment is easy to access since it is located at ground level. However, as with a number of adjustments of this type, aligning the belt is more efficiently done while the machine is running. This is very common in practice, in any case within Quebec businesses. Once the belt was aligned, two employees worked to put the guard back in place. At this moment, one of them noticed a piece of debris. Since the conveyor was running, one of the employees flipped the nearby position switch. This switch is used to prevent damage to equipment (by detecting an absence of movement in the tail pulley, while the motor is running). This is not a safety switch, but it does turn off the machine. The other employee approached the meeting point between the belt and the tail pulley to remove the debris. Without warning, the conveyor suddenly started back up. The worker was dragged into the in-running nip, where he was severely injured. He was pronounced dead on site. Figure 1 presents two images of the conveyor's tail pulley. One shows its state during the machine's normal functioning, while the other shows its state during the intervention.

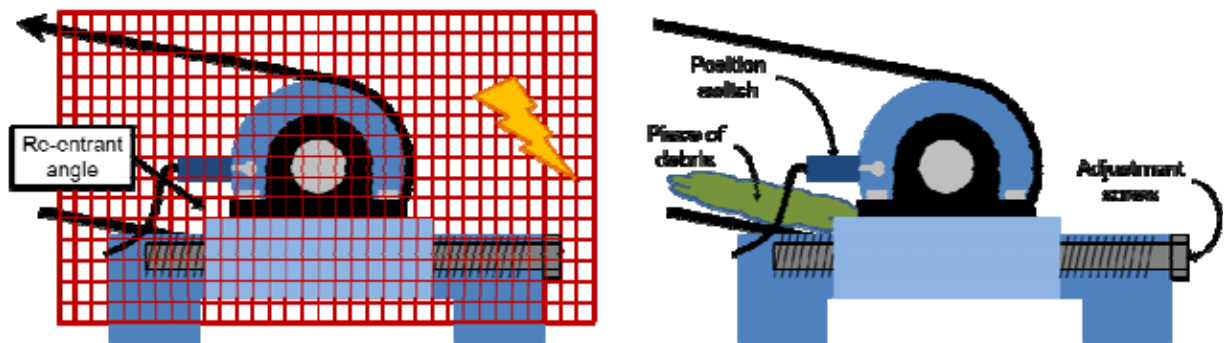


Figure 1: State of the tail pulley during normal functioning (left) and during the intervention (right).

3 CAUSES OF THE ACCIDENT, ACCORDING TO THE CSST

In their investigation, the CSST inspectors suggested three causes for the accident [5]. The first is the fact that the worker was dragged into the in-running nip of the tail pulley when the conveyor unexpectedly started up. They observed that the belt was stopped using a position switch that did not maintain the stop command, to the contrary. The expert commissioned by the CSST pointed out a programming error in this regard: activating the switch ordered the belt to stop, but the machine momentarily started back up because it was programmed to be reactivated in a given sequence and in a given time. Because this switch aimed to prevent damage to the belt, it normally should have maintained the stop command. The expert reiterated several times that this switch was not meant for safety functions and should not have been used for the intervention that was carried out.

The second cause put forward had to do with the method used to maintain conveyor belts, which the inspectors deemed to be hazardous. They stated that at the time of the accident, the equipment was not locked out. They further cited article 185 of the Act Respecting Occupational Health and Safety [7], which prescribes lockout of all equipment before work is undertaken in a hazardous zone, subject to article 186. This article states the conditions to respect when a worker must access a hazardous zone in order to properly perform an action. The activation of the position switch certainly did not respect these conditions.

The third cause suggested had to do with the management of health and safety in line with maintenance work, which, in their view, presented certain deficiencies. In particular, they advanced that the employer did not have specific training in place regarding the risks associated with this equipment; had not established lockout procedures; and had not provided employees with the manufacturer's operating manual. In sum, it was brought to light that several organizational aspects in line with the Occupational Health and Safety Act (OHSA) were breached [6].

4 CAUSES OF THE ACCIDENT, ACCORDING TO THE EMPLOYER

The expert commissioned by the employer was mandated to identify other causes that might explain the occurrence of the accident. To proceed as systematically as possible, the expert produced a tree structure of causes. Beginning with the death of the worker (harm), three necessary, immediate and sufficient causes were identified: the presence of an unprotected re-entrant angle (hazardous phenomenon), the worker's exposure to this re-entrant angle (hazardous situation); and the sudden and unexpected startup of the machine (hazardous event). Each of the causes was then analyzed systematically. The essentials of this analysis are presented in the next sections.

4.1 Unprotected re-entrant angle (hazardous phenomenon)

The lower part of the conveyor belt forms a re-entrant angle with the tail pulley when the machine is running. It is well known that this zone is hazardous: 48% of serious or fatal accidents associated with conveyors are related to such an in-running nip; 56% of these accidents occur during maintenance operations [3]. To protect this hazardous zone, a fixed enclosing guard was produced by the equipment's manufacturer. Two causes explain why this zone was not protected at the time of the accident.

The first is that the enclosing fixed guard had to be removed in order to be able to align the belt, since the adjustment screws were not accessible (see Figure 1). If the adjustment screws had been accessible, the accident probably would not have occurred. Hence, the manufacturer could simply have lengthened the screws so that they would protrude from the fixed enclosing guard. This is shown in the left part of Figure 2. A second cause explaining why the re-entrant angle was not protected after the removal of the fixed enclosing guard is that the manufacturer had not anticipated other physical means of protection. For example, a fixed nip guard could have been installed, as suggested in the right part of Figure 2. In addition to protecting the hazardous zone, this type of guard can push away debris in some cases, thus limiting the need for interventions.

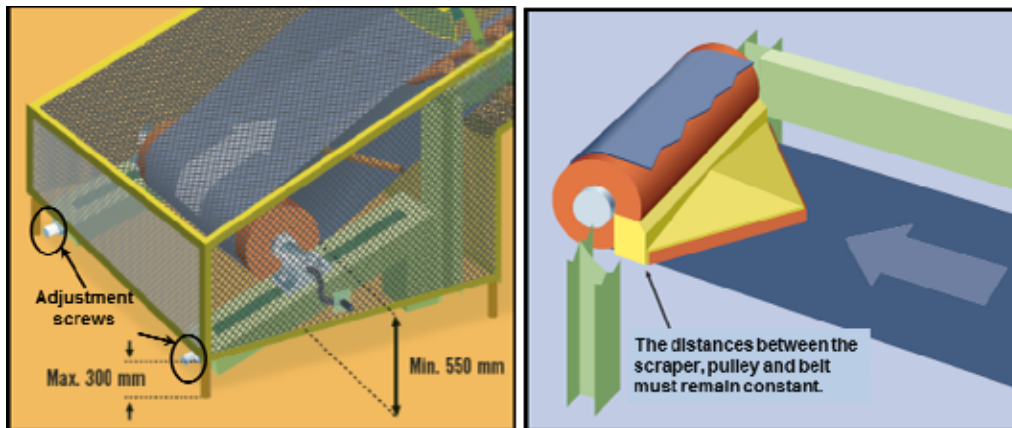


Figure 2: Examples of solutions to avoid an unprotected re-entrant angle [4]

These practices were well known at the time of the accident. In fact, a guide to conveyor design published by the CSST stipulates that “preventive measures must be implemented to ensure that work on or near conveyors be performed safely. Right from the design stage, it is necessary to find means to limit worker exposure to hazards . . .” (our translation) [4]. The equipment design stage is foremost the responsibility of the manufacturer and not the employer. It was therefore the employer's responsibility to anticipate ways to limit interventions or make them safe.

4.2 Worker exposure to the re-entrant angle (hazardous situation)

Worker presence is a common cause in the type of accident that occurred. As previously explained, if it had not been necessary to remove the fixed enclosing guard to realign the belt, then debris would maybe not have accumulated in the re-entrant angle, hence precluding the need for intervention in this hazardous zone; the worker would not have had to be present to put it back in place on the day of the accident. In sum, the removal of the fixed enclosing guard—because it did not provide access to the adjustment screws—is closely tied to the occurrence of the accident.

4.3 Sudden and unexpected startup of the machine (hazardous event)

Three causes were identified to explain the sudden and unexpected startup of the machine.

The first is that the machine was running at the time of the accident [5]. The only preventive means during maintenance operations anticipated by the manufacturer was lockout. However, although it is true that this means provides a high level of safety, it is important to emphasize that:

- The reliability of this work method relies solely on human behaviour, which makes it less effective than other risk reduction measures [1];
- This protection method does not always take into account the needs of users, who must sometimes activate a machine to perform tasks, such as aligning a conveyor belt; and
- Other technical solutions existed at the time the equipment was designed, but the manufacturer did not consider them, even though they were well documented at the time [2] [3] [4] [7].

The second cause is that the machine was incorrectly activated [5]. Indeed, the business that installed the equipment made a programming error, so that the conditions for the safe activation of the equipment were not reinitialized after the detection of a problem, such as the obstruction of the conveyor. Therefore, after having activated the position switch, the worker may have inadvertently activated the switch a second time, provoking an activation command through an unexpected logical path. The position switch was certainly not meant to safely stop the machine. However, it was in the proximity of the workers; its incorrect use was predictable, especially since the workers were aware that it could be used to stop the conveyor. To bring to light this programming error, the CSST had to call upon an expert. The expert pointed to certain existing techniques or means for reducing the possibility of a programming error leading to undesirable behaviour on the part of the machine. The related trials are normally conducted during the design stage; when a piece of equipment is activated; and following any change in design. For these tasks, the employer relied on the separate businesses to which he had entrusted them.

The third and final cause is that at the time of the accident, the audible and visual alarm located near the control panel did not signal that the conveyor had been reactivated. Yet the API program commands the activation of the audible and visual alarm when the machine is reactivated. Because of the programming error, the command of this warning was bypassed by the API [5]. The victim knew that, normally, the conveyor did not start up without this warning. This was, once again, an error committed by a business trusted by the employer.

5 CAUSES OF THE ACCIDENT, ACCORDING TO THE COURT

After hearing both parties and their respective experts, the judge deliberated to study the case. In rendering his decision, he began by recalling that the goal of the LSST is “the elimination, at the source, of dangers to the health, safety and physical well-being of workers” [6]. Then, based on judicial precedent, he went on to say that the employer plays a key role among the involved parties, in particular because he has the ownership and control of his facilities. The judge’s entire judgment rested on this last consideration.

The judge stated that a better designed guard, enabling normal adjustments without requiring removal, may have avoided the tragedy. He considered this proposition interesting, and mentioned that article 63 of the LSST [6] confers obligations upon equipment suppliers. However, he added that this does not diminish the obligations of the employer. He then rejected the idea that the installer, who made the programming error, was partly responsible for the accident, in spite of the fact that the business involved was reputed to be competent and was trusted by the employer. The judge underscored various breaches on the part of the employer, which are set out in the CSST investigation report: he neglected to become familiar with the manufacturer’s manual, had not planned a means for manual control or another procedure for interventions in the hazardous zone, etc.

In sum, the court rejected all the arguments put forth by the defense. The judge recalled that the employer is responsible for and has complete control over his equipment. He also emphasized article 51 of the LSST, which states that the employer must “supply safety equipment and see that it is kept in good condition” [6].

6 CONDITIONS FOR IMPROVING MACHINE SAFETY

In this case, all parties did competent work:

- The CSST inspectors noted significant breaches on the part of the employer, including insufficient training for workers and the absence of procedures for safe maintenance;
- The defense pointed out important faults in the design and installation of the equipment (including the need to remove the guard to make a fairly common adjustment as well as an error in system programming), arguing that the employer does not have the expertise to identify this type of error and that, under these conditions, he completely trusts the competence of the manufacturer and installer; and
- The judge based his decision on legal precedent and on the relevant legislative articles, including those of the LSST [6].

Even so, all experts in safe equipment design should conclude that the equipment that killed this worker had significant shortcomings, for which very simple and proven solutions existed well before it was manufactured and installed. The question now arises: Why did the judge not take these professional breaches into account?

Indeed, the aim of the LSST is “to work at the source to eliminate hazards to the health, safety and physical integrity of workers.” Article 3 specifies that “the fact that collective or individual means of protection or safety equipment are put at the disposal of workers where necessary to meet their special needs must in no way reduce the effort expended to eliminate, at the source, dangers to the health, safety and physical well-being of workers” [6]. Yet the fact that the only means for intervention anticipated by the manufacturer were lockout and training is not consistent with the spirit of the LSST. Moreover, this is echoed by standard CSA Z432-04 (article 5.6.4, our translation): “All means must be taken to eliminate hazardous phenomena or to reduce risks by design or by protective measures before turning to other preventive measures ... ,” explicitly referring to warnings, information, work methods (such as lockout), training, use of individual protective equipment, and supervision [1]. Why, then, did the judge only take into account breaches in work methods and employee training, rather than those relating to equipment safety itself?

We are not jurists, but rather two engineers specialized in machine safety. Nevertheless, it is our belief that part of the answer lies in the same article 63 of the LSST [6] (our translation): “No one can manufacture, supply, sell, rent, distribute or install a product, procedure, equipment, material, contaminant or hazardous substance unless these are safe and meet the standards prescribed by regulation [emphasis ours].” However, it seems that no standard relative to the safe design of machines is prescribed by regulation. In other words, manufacturers are required to release safe machines on the market, but there is no obligation—and no incentive—to meet the standards in force. Yet these standards are the state of the art. They establish the good practices discussed by experts on the subject. In our view, planning lockout and employee training as the only means for reducing risk is inconsistent with professional practice. Can this state of affairs be improved? It seems to us that the answer is affirmative.

An interesting avenue can be found in the European legislation. In 1989, a machine directive was adopted [10]. Ever since, various changes have been made and today, the directive in force is Directive 2006/42/EC [8]. Its goal is to “lay down the essential health and safety requirements in relation to design and manufacture in order to improve the safety of machinery placed on the market.” In addition, according to this directive, “Manufacturers should retain full responsibility for certifying the conformity of their machinery to the provisions of this Directive.” In this regard, the manufacturer can undergo self-certification or use the services of a recognized firm. Then, it affixes the initials CE, “the only marking which guarantees that machinery conforms to the requirements of this Directive.” The requirements include the manufacturer’s obligation to complete a risk evaluation, which is recorded in the machine’s technical file [10].

To illustrate the scope of this directive, it seems useful to briefly relate an accident that took place on February 14, 2004 at Frouzins ski centre in France. On that day, an eight year old girl was struck by the head pulley of a treadmill. She died choked by the belt. The investigation revealed that both the employee on supervision duty and the maintenance electrician had bypassed a safety feature that frequently caused the belt to stop. The sentences pronounced on November 25, 2008 were harsh for the two employees and for the manager. Moreover, the manufacturer of the conveyor belt was sentenced for errors in design [9].

In brief, this directive is a very strong incentive for manufacturers to meet standards, which helps to ensure that machines released on the market are provided with truly effective means for risk reduction.

7 CONCLUSION

The object of this article was to shed light on a fault that seems to curb any significant improvement to the safety of machines in Quebec: the lack of responsibility that is legally incumbent upon the manufacturer. The case here described to present this idea is far from being the only one. Indeed, it is fairly frequent to observe solutions to risk reduction that may be described as “political”: they strive to meet the requirement of releasing safe machines (article 63 of the LSST [6]), but they hardly take into account the realities of users. Faced with the impossibility of performing certain basic functions while respecting the safety measures devised by the manufacturer, the employer often has no choice but to bypass these same functions. From this moment on, the manufacturer is no longer held responsible.

The current legislation states only that evaluating a machine’s safety is the responsibility of the employer. But how can the employer complete this task if he is not an expert on the subject? The employer, with reason, trusts in the competence of the machine’s manufacturer. In addition, even if the employer evaluates the safety of a machine after it is installed, it is still widely recognized that the solutions he finds to improve its safety are not as effective as those put in place right from the design stage. Why does the manufacturer play such a small part in the overall process of designing a safe and functional machine?

If we truly wish to improve the situation, in Quebec at least, it appears that a change is needed in the legislation. The European model seems to offer an interesting possibility: requiring the manufacturer to carry out risk assessment and reduction. When properly performed, this exercise provides a way to take into account various modes of functioning of the equipment (including normal production, unblocking a jam, adjustments, and maintenance). For each risk identified, effective solutions must be found. These solutions are integrated at the design stage of the machine, well before it is released. Residual risks can then be managed by procedures and other administrative methods incumbent on the employer, but only after the risks directly associated with the machine are reduced to their lowest possible level.

The idea here is not to allow employers to sidestep their obligations, but rather to broaden the manufacturer’s responsibility. Without such a change, it is difficult to see how the myth of seeing functional and safe machines in factories can become a reality.

REFERENCES

- [1] CSA (2005). *CSA Z432-04 - Safeguarding of Machinery*. Mississauga (ON).
- [2] CSA (2005). *CSA Z460-05 - Control of hazardous energy - Lockout and other methods*. Mississauga (ON).
- [3] CSST (2003). *A User’s Guide to Conveyor Belt Safety. Protection from Danger Zones*. Bibliothèque nationale du Québec, 2nd ed., 70 p.
- [4] CSST (2004). *Sécurité des convoyeurs à courroie. Principes de conception pour améliorer la sécurité. Guide du concepteur*. Bibliothèque nationale du Québec, 125 p.
- [5] CSST (2007). *Rapport d’enquête*. Available from Patrik.Doucet@Usherbrooke.ca on request.
- [6] Éditeur officiel du Québec (2009a). *Loi sur la santé et la sécurité du travail*. <http://www.canlii.org/en/qc/laws/stat/rsq-c-s-2.1/latest/rsq-c-s-2.1.html>.
- [7] Éditeur officiel du Québec (2009b). *Règlement sur la santé et la sécurité du travail*. http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/S_2_1/S2_1R13_A.HTM.
- [8] Official Journal of the European Union (2006). *Directive 2006/42/CE of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:EN:PDF>
- [9] La Dépêche (2008). *Frouzins : la station de ski condamnée à une lourde amende*. Newspaper article published November 25, 2008. <http://www.ladepeche.fr/article/2008/11/25/498096-Frouzins-La-station-de-ski-condamnee-a-une-lourde-amende.html>.
- [10] Lubineau, P. (2005). *La Directive Machines, ses fondements et son champ d’applications*. Mesures 777, p. 56-58. <http://www.mesures.com/archives/777reglementation.pdf>.

Analysis of the contribution of equipment reliability problems in the chain of causality of industrial incidents and accidents in a pulp and paper plant

François Gauthier, Dominic Bourassa, Georges Abdul-Nour
Industrial Engineering Department, Université du Québec à Trois-Rivières, C.P. 500 Trois-Rivières
(Québec) Canada, G9A 5H7 (francois.gauthier@uqtr.ca).

KEYWORDS: Accidents, Reliability, Failure, Manufacturing.

ABSTRACT

An industrial accident is defined in Quebec's *Act respecting industrial accidents and occupational diseases* as "a sudden and unforeseen event, attributable to any cause, which happens to a person, arising out of or in the course of his work and resulting in an employment injury to him." As revealed by the numerous investigations undertaken in a majority of organizations after incidents and accidents, many factors can contribute to these "sudden and unforeseen events." These factors include the work methods and procedures, a lack of training, and the design and reliability of the equipment, to name only a few. Regarding reliability aspects more specifically, even though this topic is extensively studied for the optimization of production and maintenance activities, it is not covered at length in the literature with respect to the safety of common industrial production equipment. This study is aimed at determining the contributions of equipment reliability problems of common industrial equipment such as machines, tools, material handling equipment, etc., in the chain of causality of industrial accidents and incidents or mishaps. Starting with the analysis of existing incident and accident data in a large pulp and paper company, the paper examines the number, types and importance of the reliability problems involved in these events. The characteristics of the failures that contributed directly or indirectly to these events are also discussed.

1 INTRODUCTION

Occupational accident prevention is a concern of many companies worldwide. It contributes not only to protecting the most important asset of companies, namely workers, but also to increasing their profitability and efficiency. Despite the fact that these companies are primarily seeking to eliminate accidents leading to workers' injuries, it is generally accepted that occupational accident prevention is also achieved by reducing the number of minor incidents that occur in a workplace.

An incident is generally defined as an accidental event leading or not to material damage, but not to injury to workers. Furthermore, an industrial accident is defined in Quebec's *Act respecting industrial accidents and occupational diseases* as "a sudden and unforeseen event, attributable to any cause, which happens to a person, arising out of or in the course of his work and resulting in an employment injury to him." In an extensive American study carried out on 297 companies and dealing with 1,753,498 accidental events (accidents and incidents), it was shown that the probability that a serious accident would occur increases with the number of incidents [1]. This study produced Bird's pyramid (Figure 1), a principle widely recognized by preventionists.

Therefore, if a company succeeds in reducing the number of events located at the bottom of the pyramid by identifying their causes and by implementing corrective measures to eliminate them, the number of events at the top of the pyramid will also be lower. In short, the fewer the number of incidents, the lower the probability of serious and fatal accidents.

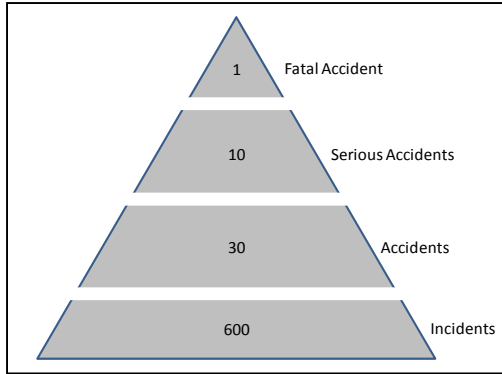


Figure 1: Bird's pyramid (Mélançon, 2010)

Also, accidental events rarely result from a single cause. They are generally the consequence of a combination of different factors in a more or less complex causal chain. As revealed by the numerous investigations undertaken in a majority of organizations after incidents and accidents, factors that can contribute to these “sudden and unforeseen events” are the work methods and procedures, a lack of training, and the design and reliability of the equipment, to name only a few.

Regarding reliability aspects more specifically, even though this topic is extensively studied for the purpose of optimizing production and maintenance activities, it is not covered at length in the literature with respect to the safety of common industrial production equipment. It is true that reliability and safety are distinct properties when talking about systems [2]. A system can be reliable and unsafe, or safe and unreliable. Nevertheless, good maintenance practices resulting from a culture focused on equipment reliability generally have the effect of increasing the efficiency of machines while reducing the occupational accident rate [3] [4].

However, there exists a significant difference between the different activity sectors in the application of good practices in equipment reliability improvement. For obvious reasons, the relationship between reliability and safety has been an integral part of the culture of the nuclear energy and aviation sectors for several decades now [5] [6] [7]. This preoccupation is also seen in the commercial fishing sector [8] [9], the mining industry [10] [11], and in the hazardous materials storage sector [12] [13]. The chemical and petrochemical industries also seem sensitized to this issue [14] [15] [16].

In the manufacturing industry, however, studies on the subject are less common, despite the significant number of incidents and accidents affecting this sector. The literature is in fact very complete regarding occupational accidents related to machines in this sector, but contains very few studies that mention the impact of equipment reliability on the occurrence of these accidental events. A study carried out in Finland [17] indicates that 88% of fatal accidents occur in the manufacturing environment, which places this activity sector far ahead of other sectors. This same study also concludes that poor machine operation is one of the factors contributing to the most common fatal accidents. A study by the INRS [18] on automated machines concluded that 20% of accidents that caused injuries are due to untimely operation of automatic control. This same study mentions that non-operation of guards is due to malfunction in 11% of cases, and wear in 4% of cases. In a similar study [19], Dźwiarek analyzed 700 occupational accidents and concluded that 54 (7.7%) were caused by incorrect operation of the control system.

2 OBJECTIVES OF THE STUDY

Despite the fact that equipment reliability is frequently studied in the optimization of production and maintenance activities in the manufacturing sector, it is quite rare in the literature involving the safety of common industrial production equipment. Thus, the aim of this study is to determine the contributions of

equipment reliability problems of common industrial equipment such as machines, tools, material handling equipment, etc., in the chain of causality of industrial accidents and incidents or mishaps.

Starting with the analysis of existing incident and accident data in a large pulp and paper company, the main objective of this study is to identify the number, types and importance of the reliability problems involved in these events. The study also aims to characterize the failures that contributed directly or indirectly to these events.

3 METHODS

3.1 Description of the database

The accidental event database used in this study comes from a commercial paper manufacturing plant that is part of a large company working in pulp and paper and lumber production, with plants in Canada, the United States and South Korea. The plant is characterized by the fact that it has been in operation for more than 125 years. Clearly, several modernization projects have been carried out over the years. To make it more competitive, considerable effort has been invested in the last decade in implementing a health and safety culture, and more recently, a culture focused on equipment reliability.

The electronic database contains analysis reports of accidental events (incidents and accidents) for the entire plant from 2010 to 2012. These reports are generally filled out by management employees, or by unionized employees with the status of replacement managers. When a worker is involved in an accident or incident, he reports to his immediate supervisor to complete with the latter an event analysis report. Event analysis reports are completed from an interface accessible via the plant's intranet. The report's author must fill in several fields, some with drop-down menus or boxes to be checked: identification, results, description of the event, immediate action to control the hazards, potential severity of the accident, immediate causes of the accidental event, fundamental causes, corrective measures, and additional information.

3.2 Identification of accidental events related to equipment reliability problems

The recognition of events related to reliability problems was an important aspect of this study. Since construction of the database did not allow automation of the classification of event reports, specific criteria had to be established in order to ensure rigorous differentiation of accidental events related to a reliability problem from other events. Four key fields in the report were used to determine whether the event was related to a reliability problem or not.

- Description of the event;
- Immediate causes of the event;
- Fundamental causes of the event;
- Recommended corrective measures.

Figure 2 presents the decisional algorithm applied to each accidental event in the database to determine whether the event was linked to a reliability problem.

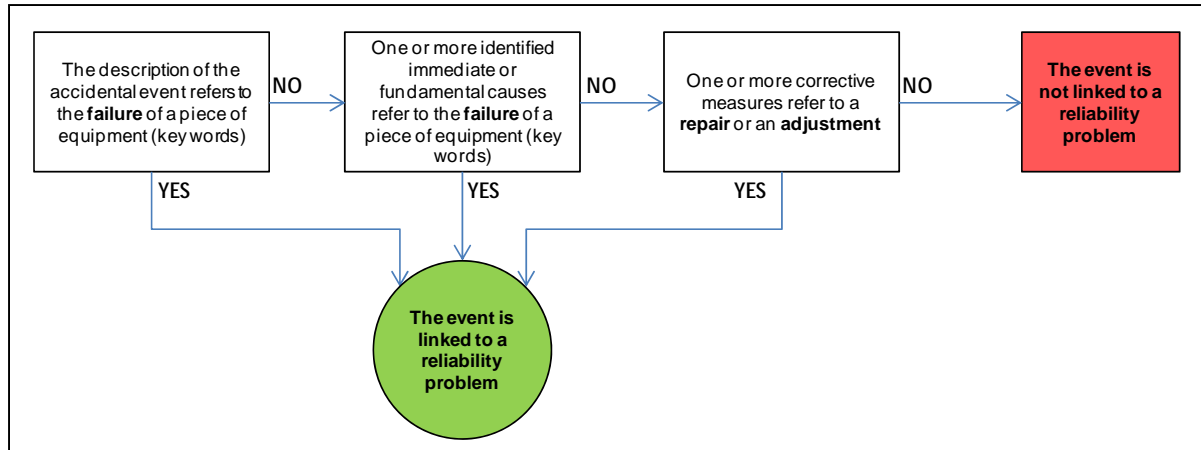


Figure 2: Decisional algorithm for determining whether the event is linked to a reliability problem

3.3 Classification of accidental events related to equipment reliability problems

Once identified, the accidental events related to reliability problems were classified according to different parameters for characterizing not only the events themselves, but also the failures that contributed to them and their consequences. The events were classified according to their usual descriptive characteristics: department in the plant, type of equipment, worker’s job, etc. Failures were classified according to their type (mechanical, electrical, of the control system, etc.), the type of component involved, their causal link to the event (direct or indirect), as well as according to the failure classification criteria proposed by Villemeur [20]. Finally, the event consequences were characterized according to their nature (no damage, material damage, injury) and their amplitude based on plant criteria.

4 PRELIMINARY RESULTS

The preliminary analysis was carried out on 306 accidental events documented between January and August 2012. Of these 306 events, 114 (37%) were categorized as being related to an equipment failure according to the criteria established by the decisional algorithm presented in Figure 2. Clearly, these failures contributed more or less directly to the analyzed events. The examples below illustrate a typical case of each of the cases.

Example 1 – Direct link – In this example, sudden failure of the pump is the direct and immediate cause of the accident:

“Around 11:25 a.m., the employee was emptying the well of pump XXX-YYY. The task was to siphon the pulp by means of a steam pump permanently installed in this well. Emptying of the well was progressing normally and the employee diluted the pulp in the well with a fire hose. When transferring the fire hose from the other side of the well, the employee was hit behind his right thigh by a blast of steam (like a gunshot) from the outlet of this pump.”

Example 2 – Indirect link – In this example, wheel wear can be considered as one of the factors that contributed indirectly to the accident by increasing the effort required by the worker to move the bin.

“In recovering the bin of wood splinters, I felt a pain in my back in pulling the roller bin. The wheels of the bin are worn and difficult to pull.”

Therefore, of the 114 events related to equipment failures, 69 contributed directly and 45 indirectly to the events. One therefore notes that a significant proportion of the accidental events that occurred were in fact related to a reliability problem, and that more than 1 accidental event in 5 was directly caused by an equipment failure. Figure 3 illustrates these results.

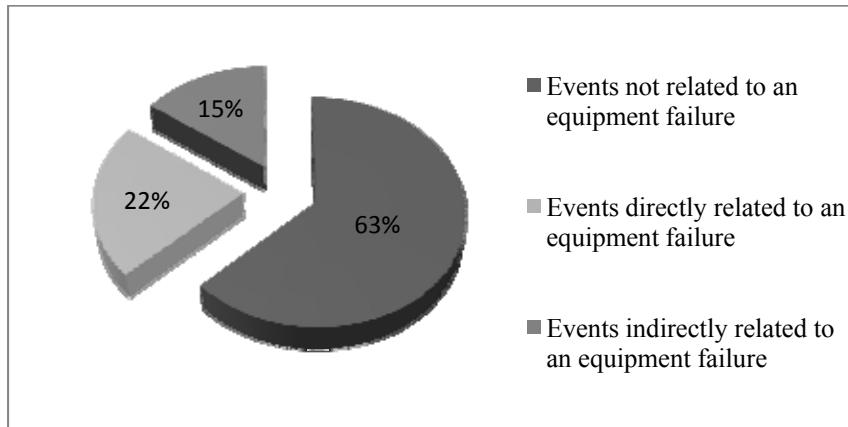


Figure 3: Breakdown of the accidental events according to the degree of relationship to an equipment failure

Of the 114 accidental events directly or indirectly caused by equipment failures, 53% involved employees from the production departments, 25% the services departments, 14% the mechanical maintenance department, 3% the electrical maintenance department, and 4% the administrative team. As could be expected, the majority of workers affected by these events were production employees.

Furthermore, an analysis of the distribution of the accidental events caused directly or indirectly by equipment failures based on their consequences yielded the following results:

- Incidents with or without material damage (other than the failure in question): 109 (95.6%)
- Accident with minor injury requiring only first aid: 4 (3.5%)
- Accident with injury causing a loss of time beyond the day of the event: 1 (0.9%)

None of the events related to equipment failures documented in this study caused serious injuries. Therefore, by combining the two types of accidents, one notes that 4.4% of these accidental events caused slight to minor injuries, which seems consistent with the results of Bird and Germain [1]: $30 \text{ accidents} / (600 \text{ incidents} + 30 \text{ accidents} + 10 \text{ serious accidents} + 1 \text{ fatality}) = 30/641 = 0.046 = 4.6\%$.

The failures that contributed to these accidental events were also classified according to different criteria. Inspired by the classification by types of failures proposed by Villemeur [20] among others, each of the failures was analyzed and categorized. The preliminary results of this analysis indicate that the great majority of the failures involved mechanical components. Also noted is that 61.4% of the failures were sudden, compared to 30.7% progressive, and that 40.4% were partial failures and 59.6% were complete failures.

5 CONCLUSION

The results of this study can be used as a starting point for other more specific work, aiming among other things to develop models of quantification of the types of industrial equipment failures that have the potential of contributing most to occupational accidents.

6 REFERENCES

1. Bird, F. E., & Germain, G. L. (1966). *Damage control: a new horizon in accident prevention and cost improvement*: American Management Association.
2. Leveson, N. G. (2011). Applying systems thinking to analyze and learn from events. *Safety Science*, 49(1), 55-64.

3. Moore, R. (2004). Maintenance Practices and Safety Performance *Making Common Sense Common Practice: Models for Manufacturing Excellence* (pp. 258-259). Burlington, MA USA: Third Edition Elsevier.
4. Moubray, J. (1997). *Reliability-centered maintenance*. New York: Second Edition Industrial Press Inc.
5. Centers for Disease Control and Prevention. (2011). Occupational aviation fatalities – Alaska, 2000-2010. *MMWR. Morbidity and mortality weekly report*, 60(25), 837-840.
6. Baker, S. P., Shanahan, D. F., Haaland, W., Brady, J. E., & Li, G. (2011). Helicopter crashes related to oil and gas operations in the Gulf of Mexico. *Aviation Space and Environmental Medicine*, 82(9), 885-889. doi: 10.3357/asem.3050.2011
7. Sovacool, B. K. (2011). Questioning the safety and reliability of nuclear power: An assessment of nuclear incidents and accidents. *GAIA*, 20(2), 95-103.
8. Antão, P., Almeida, T., Jacinto, C., & Guedes Soares, C. (2008). Causes of occupational accidents in the fishing sector in Portugal. *Safety Science*, 46(6), 885-899. doi: 10.1016/j.ssci.2007.11.007
9. Wang, J., Pillay, A., Kwon, Y. S., Wall, A. D., & Loughran, C. G. (2005). An analysis of fishing vessel accidents. *Accident Analysis and Prevention*, 37(6), 1019-1024. doi: 10.1016/j.aap.2005.05.005
10. Kecojevic, V., & Radomsky, M. (2004). The causes and control of loader- and truck-related fatalities in surface mining operations. *Injury control and safety promotion*, 11(4), 239-251.
11. Md-Nor, Z., Kecojevic, V., Komljenovic, D., & Groves, W. (2008). Risk assessment for loader- and dozer-related fatal incidents in U.S. mining. *International journal of injury control and safety promotion*, 15(2), 65-75. doi: 10.1080/17457300801977261
12. Chang, J. I., & Lin, C. C. (2006). A study of storage tank accidents. *Journal of Loss Prevention in the Process Industries*, 19(1), 51-59. doi: 10.1016/j.jlp.2005.05.015
13. Atherton, W., & Ash, J. W. Review of failures, causes & consequences in the bulk storage industry. [Universitaire].
14. Uth, H. J., & Wiese, N. (2004). Central collecting and evaluating of major accidents and near-miss-events in the Federal Republic of Germany - Results, experiences, perspectives. *Journal of Hazardous Materials* 111 (1-3), 139-45.
15. Konstandinidou, M., Nivolianitou, Z., Kefalogianni, E., & Caroni, C. (2011). In-depth analysis of the causal factors of incidents reported in the Greek petrochemical industry. *Reliability Engineering and System Safety*, 96(11), 1448-1455.
16. Vaidogas, E. R., & Juocevičius, V. (2008). Sustainable development and major industrial accidents: The beneficial role of risk-oriented structural engineering. *Technological and Economic Development of Economy*, 14(4), 612-627.
17. Nenonen, S. (2011). Fatal workplace accidents in outsourced operations in the manufacturing industry. *Safety Science*, 49(10), 1394-1403.
18. Svaldi, D. S., & Charpentier, P. (2004). Une étude des accidents en automatisme à partir de la base de données Epicea. *INRS*.
19. Dźwiarek, M. (2004). An analysis of accidents caused by improper functioning of machine control systems. *International journal of occupational safety and ergonomics : JOSE*, 10(2), 129-136.
20. Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels: fiabilité, facteurs humains, informatisation* (pp. 795). Paris: Eyrolles.

Adaptive safety concepts for automated mobile work machine systems – simulator assisted research approach

Risto Tiusanen,
VTT, P.O.Box 1300, FIN-33101 Tampere, Finland, risto.tiusanen@vtt.fi, www.vtt.fi
Timo Malm,
VTT, P.O.Box 1300, FIN-33101 Tampere, Finland, timo.malm@vtt.fi, www.vtt.fi
Ari Ronkainen,
MTT Agrifood Research Finland, FI-31600 Jokioinen, Finland, ari.ronkainen@mtt.fi

KEY WORDS: Adaptive safety, concept, mobile machine, risk assessment

ABSTRACT

Safety is one of the most important quality and competitiveness factors in mobile work machine development. Machinery safety requirements are tightening in all industrial sectors. Mobile work machines are not an exception. Risks related to mobile work machine applications are dependent on several operation condition factors such as mode of operation, performed work task and working environment. Machine safety risk levels change when these operation conditions change for example from semi-automated operation to full automated operation. Today's safety concepts are based on traditional inflexible isolating arrangements around the automated mobile work machines and simple system shutdown principles if someone tries to enter into the operating area during automatic or remotely controlled operation. In the future autonomous systems are operating in more complex and less controlled environments. Safety strategies should also change depending on the current situation and local conditions. The idea in "adaptive safety concepts" is that safety system continuously monitors and controls the behaviour of the work site machinery systems so that the system safety is ensured in all situations. This paper discusses the terms "adaptive safety" and "dynamic risk assessment" and describes the on-going research work in Finland on safety concepts for mobile work machine applications.

1 INTRODUCTION

Most of the mobile work machines (also called mobile work equipment) in industrial work sites are manually operated machines. Mobile work machines are used for instance in construction and building work sites, harvesting work sites, mines, logistic centers, harbors, container terminals and warehouses. Mobile work machines are typically diesel-powered or electrically operated and equipped with hydraulic actuating mechanisms and electrical or electronic control systems. Fully electric versions are becoming more and more common in many applications. Control systems in modern mobile work machines are based on distributed CAN-bus implementations with automated functionalities and they can have several operating modes from manual operation to fully automatic operation. Increasing needs for better productivity, better mobile work machine utility and higher work quality in work sites is driving the work process management towards automated production control or construction process control instead of improving the management separate manual work machine operations. Automated machine control functionalities are developed to support the machine operator with for instance boom handling, hook positioning, lifting, load gripping or to improve the work tasks in case of frequently repeated operations or machine movements.

Automated functionalities in this context can include, in addition to automatic control functions, automatic data collection and transfer, condition monitoring and diagnostics, automatic information management to support the work process (position information, work orders, instructions, warnings, driving assistant information etc.). In factories and warehouses automatic guided vehicles and similar automatic material handling machine systems have been used for years. In the open-air conditions there are already some large scale machinery systems, which apply automated or autonomous working machines (e.g. automatic container handling systems in harbours and autonomous ore transportation systems in mines).

Clear message from mobile work machine manufacturing industry is that traditional machine safety solutions, safety standards and risk management practices are not enough anymore when designing and building automated mobile work machine systems. There is increasing need to understand system level aspects and need for knowledge on how

to analyse, assess and manage safety risks in complex machinery applications in work site level. To get the best possible productivity and benefits out of the new automation technology in mobile work machine applications safety concepts and measures must be developed to ensure the safety in all circumstances but also minimise the interruptions, unnecessary stops and system shut downs. Safety solutions should be adaptive and safety functions should adapt in real time to the dynamically changing safety risks on site.

This paper discusses the terms “adaptive safety” and “dynamic risk assessment” and describes the on-going research work in Finland on safety concepts for mobile work machine applications. Research work on these “adaptive safety concepts” is going on in Finland in close co-operation with mobile work machine manufacturers, machine control system designers, universities and research institutes. This research work is part of the project “Future Semi-Autonomous Machines for Safe and Efficient Worksites” (FAMOUS), which belongs to the Fimecc’s (Finnish Metals and Engineering Competence Cluster) research program “Energy and Life Cycle Efficient Machines” (EFFIMA). For more information about the EFFIMA program, please visit the FIMECC web page [1]. More information about FAMOUS research project can be found from Forum for intelligent Machines (FIMA) web page [2]. The main financier of the project is TEKES (Finnish Funding Agency for Technology and Innovation).

2 VISIONS OF THE FUTURE WORKSITE

Generally accepted vision of industrial worksites using mobile work machines seems to be that future worksites will be more sustainable, more automated, more efficient and safer work places. In future worksites machine operators and other workers could work in collaboration with automated mobile work machines so that work machines need not always to be stopped when persons enter their operation area. In future worksites automated work machines could change their operation mode flexibly from one mode to another mode depending on the situation awareness perception and dynamic risk assessment. To enlarge this vision even more it could be possible that mobile work machine system composed of one or more work machines, which are operating in the same worksite, could then adapt to the changing operating conditions and risks by combining the situation awareness information shared with various systems and actors at the worksite.

3 DYNAMIC RISK ASSESSMENT AND ADAPTIVE SAFETY

Research interest on adaptive safety or dynamic risk assessment in the context of mobile work machine application is still very new, although highly automated mobile work machine applications have been implemented and used since mid-1990. One major reason for that has been that the safety legislation and safety standardisation have been based on those earlier mentioned fixed safety solutions. This has practically ruled out the possibility to develop adaptive and flexible safety concepts. Only just few years the mobile work machine sector has brought up these issues and initiated research and development work on adaptive safety concepts. Strongly improved safety technology such as programmable safety devices and safety systems has been in an important role in this development.

Dynamic risk assessment and adaptive safety in a work site can be understood from different perspectives. A human centred point of view and a technology oriented point of view could be the two opposite views. In the former case persons assess work and environment related risks continuously while working in a work site. They decide and adapt their own actions and machine control actions based on the risk assessment. In the opposite case automatic safety system monitors continuously the work site environment, machine operations, hazardous substances, and persons’ position and so on, and calculates the risk dynamically based on the pre-programmed rules. Automatic safety system adapts to the current situation and risks and controls the machinery and equipment in a safe way and gives guidance to the persons how to work safely.

Definitions for the terms dynamic risk assessment and adaptive safety in mobile work machine context can be derived from the general definition of situation awareness in dynamic human decision making:

Situation awareness: “is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future” [3]

Dynamic risk assessment: Based on the situation awareness information the risk of the momentary situation is evaluated by a human or by a system before initiating next machine operations or setting in next manual tasks in the work process.

Adaptive Safety: Safety of persons and the work site environment is ensured and the next allowed machine operations or manual tasks are controlled on the basis of dynamic risk assessment results.

3.1 References and research work in other sectors

A practical reference to this discussion of dynamic risk assessment and adaptive safety can be taken from our everyday life - driving a car in a heavy traffic. A driver makes dynamic risk assessment and adapts his/her own driving to the changing traffic situation and other drivers manoeuvres. A driver also tries to foresee how the traffic situation changes and makes route changes to be able to keep to the planned time schedule. Various driver assistance systems have been developed to support car drivers' decision making and to improve traffic safety. Intelligent collision avoidance systems and adaptive cruise control, which can take over the driving control, have been developed to prevent collision, if the driver him/herself makes an error, lose control of the car or the traffic situation seems to become too risky. [4]

Another example of human centred dynamic risk assessment in a demanding "work site" can be taken from fire and rescue work. The rescue group had to adapt to "work site" as they arrive to the target building or accident place and immediately make risk assessment for their own safe work procedures and for the actions how to prevent further damages. As the fire fighting or rescue work proceeds, rescue persons have to assess risks continuously and adapt their actions to the situation on site before they take can move on. In this context dynamic risk assessment has been defined as follows: "Dynamic risk assessment is the continuous process of identifying hazards, assessing risk, taking action to eliminate or reduce risk, monitoring and reviewing, in the rapidly changing circumstances of an operational incident" [5]

In the other end of dynamic risk assessment scale could be a situation where the risk assessment and decisions are made automatically by the automation system. System controls are generated automatically based on the situation awareness information and adaptive safety algorithms. The issues related to so called adaptive automation and its relation to human factors issues and situation awareness in complex systems have been studied by Endsley and Kaber since late-1980. They have defined Adaptive automation so that it is "a type of automation that allows for dynamic changes in control function allocations between a machine and a human operator based on states of the collective human-machine system". [6] Kaber et al. (2001) have concluded that, in the context of human-computer communication under adaptive automation, there is a lack of operator awareness of the mode of automation because the states, intentions, and actions of control system are not predictable or they are not clearly communicated to the human. [6] An interesting research results and an application of adaptive automation has been presented by Yi et al. (2008). They have outlined architecture and functionalities of an adaptive safety critical middleware (ASCM) for distributed and embedded safety critical systems. It is a concept of a multilevel embedded safety-critical middleware that is designed to provide timeliness, distribution, availability and adaptability services for the development and implementation of embedded safety-critical applications. [7].

The important questions, who is in charge of the flexibility of a system to adapt to changing circumstances, and what is the difference between "adaptive" and "adaptable" systems, have been discussed among others by Oppermann et al. (1997) [8] and Miller et al. (2005) [9]. According to their studies two kinds of systems have been developed for supporting the user in his/her tasks. Systems that allow the user to change certain system parameters and adapt their behaviour accordingly are called "adaptable". Systems that adapt to the users automatically based on the system's assumptions about user needs are called "adaptive". [8][9] Miller et al. claim that adaptive systems can achieve among others higher performance, reduced workload, greater range of flexibility and less training time than human-centred adaptable systems. But on the other hand, if operator is taken out of the control, adaptive systems can run to risks in decision making. High levels of automation in decision-making may reduce the operator's awareness of certain system and environment dynamics. [9]

4 NEW ADAPTIVE SAFETY CONCEPTS FOR MOBILE WORK MACHINE SYSTEMS

The idea in “new adaptive safety concepts” in mobile work machine applications is that “work site level safety system” continuously monitors and controls the behaviour of the work site machinery systems so that the human safety is ensured in all situations. Control actions can vary depending on the mode of operation and assessed risk levels: immediate actions or warning or assisting information; stopping a movement, slowing down the speed, limiting the movements, restricting the operation, delays, waiting times, holding position etc. Novelty in adaptive safety concepts is especially the utilization of the adaptive functionalities of a modern mobile work machine system and the possibilities to proactively prepare for the changing work site conditions. The practical implementations could be a sort of mixture of adaptive and adaptable concepts depending on the level of automation.

Adaptive safety performance of a mobile work machine can be based on several safety zones or safe operating modes, which can be treated separately. Safety zones can be defined as safety distances to hazard points or they can be defined by following machine operations in the work process phases. Control actions can then vary depending on the safety zones, work tasks and dynamically assessed risk levels: immediate actions or warning or assisting information; stopping a movement, slowing down the speed, limiting the movements, restricting the operation, using waiting times, holding position etc.

Measures to dynamically manage risks in mobile work machine systems can be carried out in many levels: manually by authorised persons; automatically in a single machine level, automatically by machine fleet or even worksite level. Automatic safety functions may be needed also in manual machines when the operator is unable to maintain safe operation of the machine, for example when movements of the machine are fast or it is too difficult for the operator to get an adequate view of the environment and machine condition. Automatic safety functions mean that the machine on-board safety system gets more responsibility of the local safety performance.

Our research work on these “new adaptive safety concepts” is focusing on three areas: concepts and methods for adaptive safety for mobile work machine systems; design criteria for distributed and scalable safety functions in mobile work machine systems; and new modeling and simulation based systems for safety design. Simulator assisted research approach integrates these three areas together and gives a good possibility to demonstrate the adaptive safety concepts and system functionalities.

4.1 Simulator assisted research approach

Simulator assisted approach in our research in “Future Semi-Autonomous Machines for Safe and Efficient Worksites” (FAMOUS) project has two main areas: development of simulator and virtual reality environments to support hazard identification and risk estimation; and evaluation of safety concepts and safety functions using simulator and virtual reality environment.

In the former area research work focuses on how modelling and simulation can support the mobile work machine risk analysis, system requirement specification and finally specification of adaptive safety functions. In the first phase of this research a structured exercise has been conducted to go through systems engineering phases from system requirement specification ending up to the platform dependent safety function specification (Figure 1). The study was carried out using a simplified drill rig application as a target system (Figure 2). The research continues with a more complex multi machine case study.

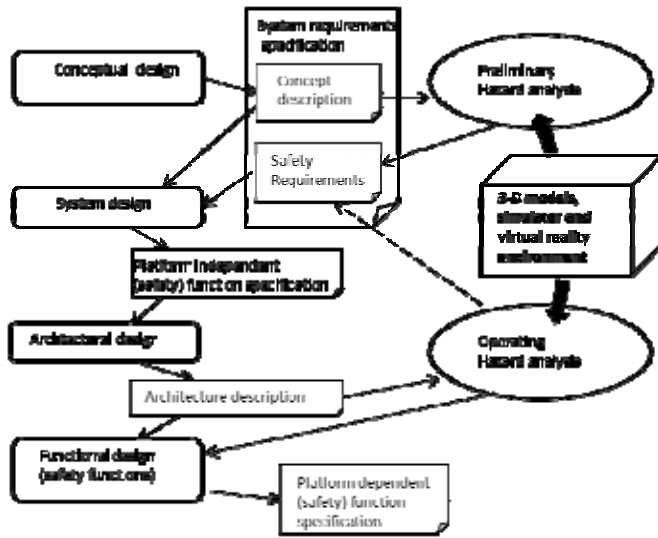


Figure 1 Simplified model of the process for adaptive safety functions requirement specification, where risk analyses are assisted with simulator and VR environment.

Implementations of dynamic risk assessment and adaptive safety concepts are complicated and difficult to evaluate. Simulator environment offers a good possibility to develop, test and demonstrate different concepts with different machine functionalities and in different work site situations. The selection of the case machine and simulator environment for this project was based on agreement in the research consortium and an available existing simulator platform. In the simulator environment a special interface has been developed to study the functionality of special safety SW block that manipulates the machine operations as a human is detected in the vicinity of machine (Figure 2). Usability of the HIL simulator in safety research has been demonstrated and the development of the simulator environment continues. It is important to notice that in this study the situation awareness data is generated by virtual sensors, and the safety functionalities and the safety block is developed only for this research purposes. The demonstrated safety functionalities are not available for the machine type in question. The main focus in the further research will be on the multi-machine situation and adaptive safety in worksite situation where more than one machines are operating simultaneously.

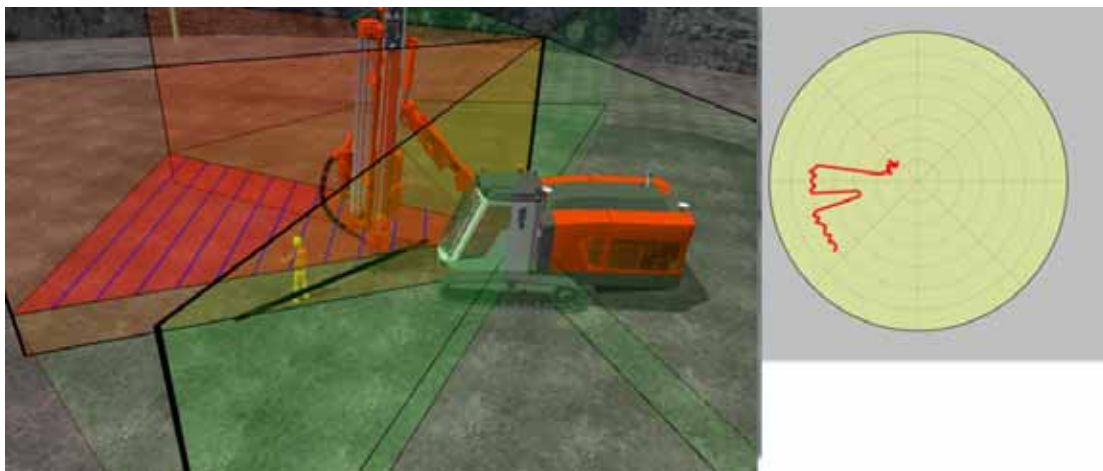


Figure 2 An example of adaptive safety function simulation: Safety zones around the hazard point (picture on the left) and a perception of human position in certain time period (picture on the right). [12]

6 DISCUSSION

The development of automation for mobile work machines is not an intrinsic value because of the available technology. The added value for the end users comes from improved productivity, efficiency, safety and sustainability compared with operations using traditional manual machines. References of dynamic risk assessment and adaptive automation and proven in use safety concepts from other industrial sectors can be used as baseline for the development of new innovative safety concepts for the specific work site conditions where mobile work machine systems are used.

To gain acceptability with these novel adaptive solutions will need willingness to accept new ideas in very conservative industrial sectors. Novel reference solutions and use cases, in which rigorous care is put into the development process of safety system as well as documenting and presenting systems safety performance, are needed to prove the fitness of adaptive safety systems in use in actual worksites. These systems have the potential to exceed the level of safety guaranteed by conventional systems and current standard based solutions.

Design of a complex automated work machine system is a challenging task and integration with adaptive safety concepts makes it even more complicated and difficult to specify, implement and verify. Modern simulator and virtual reality environments in this sense offer good possibilities to develop test and demonstrate automation solutions, different concepts with different machine functionalities and in different work site situations. Simulator assisted research approach in this project continues the research in Finland on advanced methodology for machinery risk analysis and safety design. Kuivanen (1995) has studied methodology for simultaneous robot system safety design including risk analysis assisted with robot system 3-D models and animation. [11] Määttä (2003) studied virtual environments in machinery safety analysis. Virtual environment and participative ergonomics approach and work safety analysis were utilized in work environment and machinery risk analysis. [12]

7 REFERENCES

- 1 FIMECC. (2012, February 6). EFFIMA - Energy and Life Cycle Cost Efficient Machines. Retrieved August 27, 2012, from Finnish Metals and Engineering Competence Cluster: <http://www.fimecc.com/content/effima-energy-and-life-cycle-cost-efficient-machines>
- 2 FIMA. (2012, June). FIMA news 1/2012. Retrieved August 27, 2012, from FIMA - Forum for intelligent Machines - Hermia: http://www.hermia.fi/fima/in_english/fimanews/fimanews-1-2012/
- 3 Endsley, M.R. (1995) Towards a theory of situation awareness in dynamic systems. Human factors and ergonomics society. Human factors, 1995, 37(1), 32-64
- 4 Vahidi, A., & Eskandarian, A. (2003, September). Research Advances in Intelligent Collision Avoidance and Adaptive Cruise Control. IEEE transactions on intelligent transportation Systems, 4(3), 143-153.
- 5 ACT. (2011, December 12). Dynamic risk assessment overview. Retrieved August 27, 2012, from ACT Emergency Services Agency / ACT Fire & Rescue / Community Fire Units / Documents: <http://www.esa.act.gov.au/wp-content/uploads/dynamic-risk-assessment-overview.pdf>
- 6 Kaber, D.; Riley, J.; Tan, K.-W.; & Endsley, M. (2001). On the Design of Adaptive Automation for Complex Systems. International Journal of Cognitive Ergonomics, 5(1), 37-57.
- 7 Yi, Z., Cai, W., & Yue, W. (2008). Adaptive Safety Critical Middleware for Distributed and Embedded Safety Critical System. Fourth International Conference on Networked Computing and Advanced Information Management (pp. 162-166). Gyeongju: IEEE.
- 8 Oppermann, R.; Rashev, R. & Kinshuk (1997) Adaptability and Adaptivity in Learning Systems. Knowledge Transfer (Volume II) (Ed. A. Behrooz), 1997, pAce, London, UK, pp173-179
- 9 Miller, C.; Funk, H.; Golman, R.; Meisner, J.; & Wu, P. (2005). Implications of Adaptive vs. Adaptable UIs on Decision Making: Why “Automated Adaptiveness” is Not Always the Right Answer. (pp. 22-27). American Association for Artificial Intelligence.
- 10 Creanex. (2012). R&D Testing Environments. Retrieved August 31, 2012, from Creanex Oy: http://www.creanex.fi/hil_1.html
- 11 Kuivanen, R. (1995) Methodology for simultaneous robot system safety design. Technical Research Centre of Finland, VTT Publications 219. 142 p. + app. 13 p.
- 12 Määttä, T. (2003) Virtual environments in machinery safety analysis. Espoo 2003. VTT Publications 516. 170 p. + app. 16 p.

SIAS
2012

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



SESSION 7

**MACHINE SAFETY;
MAINTENANCE AND OTHER ASPECTS**

Preliminary results and observations for the study on the application of lockout/tagout in sawmills in Quebec

Pascal POISSON¹, Yuvin CHINNIAH

¹ ppoisson@interventionprevention.com

POLYTECHNIQUE MONTREAL
DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL
C.P. 6079, Succursale Centre-ville, Montréal (Québec), H3C 3A7, CANADA

Abstract – In Quebec, workers intervening in hazardous zones of machines and processes during maintenance, repairs, and unjamming activities have to apply lockout procedures. Lockout is defined in the Canadian standard, the CSA Z460-05 (2005), as the placement of a lock or tag on an energy-isolating device in accordance with an established procedure, indicating that the energy-isolating device is not to be operated until removal of the lock or tag in accordance with an established procedure. However, several questions still exist regarding the concept of lockout and the regulations which describe it. In 2008, the Occupational Health and Safety Commission for Quebec (CSST) revealed that (an average of) 6 fatalities and 5225 accidents take place annually during installation, maintenance or repairs of machines due to the absence of or incorrect lockout procedures. In a previous study, the similarities and differences among lockout programs from enterprises, regulations, standards and guides were compared and analyzed. The objective of this study is to analyze and evaluate the practical application of lockout programs and procedures on machines in the forestry and wood transformation sector (i.e. sawmills) in Quebec. Lockout procedures in this sector have been applied for more than 30 years. In this article, the methodology used in this study as well as the tools which have been developed and which are being applied are presented. Moreover, preliminary results of the study reveal that major steps of the lockout procedures (e.g. verification of the absence of energy) are not applied by workers, although being prescribed by the companies.. Interventions on machinery involving several workers (i.e. the application of lockout by all the workers) remain a challenge. This study also looks at the various challenges faced by the companies and workers in relation to lockout procedures.

Mots clés - Cadenassage; Maintenance; CSA Z460; Machine; Procédure.

Keywords – Lockout/tagout; Maintenance; CSA Z460; Machine; Procedure

1 INTRODUCTION

Many fatalities and accidents happen during interventions of maintenance on industrial machines. Automation tends to reduce the number of operators on machines. The maintenance interventions remain complex and dangerous. As maintenance is often overlooked by machines designers, many residual risks associated with maintenance interventions on machines have to be managed by users in companies. Furthermore, considering the risks associated to machine repairs and maintenance, most of regulations in industrialized countries, including Canada, are referring to a risk reduction method, such as lockout of equipment (and/or tagout). In Canada, a number of accidents are caused by the absence of or incorrect lockout procedures. Canadian Standard CSA Z460-05 prescribes requirements related to the control of hazardous energy associated with machines. CSA Z460-05 defines lockout as a principle consisting of installing a lock and/or a tag on an energy-isolating devices following an established procedure, indicating that the energy-isolating devices shall not be activated before the lock or tag is removed as per the established procedure.

In Quebec, the Occupational Health and Safety Commission (CSST) annually compiles an average of 5225 accidents and 6 fatalities related to an absence of or an incorrect lockout on machine during maintenance interventions. within spite of legal obligations and apparent simplicity of lockout, it is not often used for unknown reasons.

Recent publications show that the absence of lockout is an important factor in machinery accidents in the United States, France and Great Britain [Shaw, 2010]. In 1996, the French National Research and Safety Institute (INRS) published a technical report on the equipment lockout [INRS, 1996]. In 2008, the INRS introduced the lockout time and operation time ratio and has concluded that lockout is yet too often presented as the rule and it can bring important constraints., Moreover the safety level it allows is based on the respect of strict procedures [INRS, 2008]. Furthermore, books explaining the distinct elements of lockout programs have been published [Kelly, 2001 and Bulzacchelli and coll., 2008].

In the United States, the lockout obligations are described by the Occupational Safety and Health Administration (OSHA)'s article OSHA 1910.147 [OSHA 1910.147, 1989]. In this country the US, approximately 3 million workers that are proceeding involved with maintenance are facing important risks of injury if the lockout application is not properly followed. This number shows the importance and accessibility of lockout in the industrialized world [US Department of Labor, 2005]. Even with these legal liabilities imposed to companies, it seems that the industrial sector experiences difficulties in the appropriation, development and application of lockout. Therefore, the OSHA has counted, in 2000 only, a total of 4,149 infringement of article OSHA 1910.147 for the application of lockout procedures. One third of these infringements were related to the absence of lockout program and/or procedure in the organization [Mutawe, 2002]. More recently, in 2005, the lockout was the 5th most encountered category by the OSHA in its reports and 90% of these references were, there again, due to the absence of lockout [US Department of Labor, 2005]. Furthermore, 10% of the most important occupational accidents would have been caused by the absence of lockout [Nadeau, 2006]. A study managed by the United Auto Workers (UAW) indicates that 20% of accidents (83 out of 414), occurred by members of the Union between 1973 and 1995, were caused by an inappropriate lockout procedure [US Department of Labor, 2005]. Furthermore, the OSHA considers that it's lockout standard has saved 122 lives, 28,400 lost working days by injuries and 31,900 lost working days in wasted time in lost time since its introduction in 1989.

In order to better understand the issues related to lockout, a research topic thematic on the subject has been developed to understand the difficulties, the factors promoting lockout, the types of lockout procedures in use and eventually promote the application of lockout in Quebec companies. With this study, we have decided to concentrate ourselves on the wood transformation industry, a sector field that owns has a lockout history in Quebec. This sector remains dangerous to the workers using machines. This article focuses on the development of the methodology and tools that will be used during that study. An analysis tool has been developed and validated in companies, and has been used, until now, within 4 organizations. In total, 10 companies will be visited but the partial results currently presented are related to these first 4 organizations. All visits have been done in sawmills in the province of Quebec.

2 LITERATURE

2.1 Literature Review on Lockout

Scientific articles directly related to lockout machines are limited. One statistical study on the accidents related to lockout in the US [Bulzacchelli and coll., 2008] and two studies – one on the systemic and behavioural approach related to occupational health and safety [Garand and coll., 2005] and the other on the lockout programs in Quebec [Chinniah and coll., 2008] – have been reviewed.

Bulzacchelli realized a doctorate thesis on accidents statistics related to lockout in the United States [Bulzacchelli, 2006]. It discusses the fatal accidents, non-fatal accidents, costs associated to accidents, accidents related to machines and accidents related to hazardous energy. In 2005, out of 5700 workers fatalities, 18% of them, i.e. approximately 1000 fatalities, are related to a contact with equipment or objects. It represents the second cause of fatalities after road accidents in the United States. From this number, 38% are production employees and 27% are maintenance, installation and repairs employees. Maintenance employees are those with the highest risk at 7.6 per 100000 workers for fatality risks, as opposed to 2.9 for production employee and 4.0 for other employees [Bulzacchelli and coll., 2008]. On the 624 accidents indexed in this study, 183 cases are due to the lack of or incorrect lockouts, 59% of that number ended up with a fracture and 41% with a minor injury as a consequence of the accident. Electrocutation at work appeared in 164 cases as the cause of the accident and appears to be the second most important hazard for the workers. For 348 cases, the authors specify the absence of lockout of equipment. In 31 cases, human mistake is in cause and within 1.2% of cases, lockout procedure had been followed but the accident still occurred. Cleaning and repairs activities show the highest frequency of accidents related to lockout.

A first study on the lockout was carried out by the IRSST [Chinniah and coll., 2008] and the researchers found and analysed 5 standards directly related to lockout, 28 rules in different Canadian provinces and other countries, 6 documents published by OHS sector-based associations, 1 guide published by the National Research and Safety Institute (INRS), 2 documents on the lockout produced by the CSST and 31 lockout programs collected from companies in Quebec.

In conclusion, this first study shows that:

- Lockout concept has a different sense or definition in the literature, especially within regulations. However, lockout definitions within standards show some similarities;
- Legal requirements around lockout vary among Canadian provinces and other countries;
- Lockout standards tend to include similar requirements, except for ISO 14118 (2000). However, some differences exist among standards related to lockout programs components;
- Lockout programs content as described in numerous documents varies; and
- Lockout programs collected from 31 plants in Quebec are not entirely in line with provincial regulations and show a number of weaknesses in comparison with Standard CSA Z460-5 (2005).

3 RESEARCH OBJECTIVES AND QUESTIONS

3.1 Objectives

This project's goal is to analyse and evaluate the application of lockout on machine in companies operating in the wood transformation industry in Quebec. More specifically, we want to : (i) identify the difficulties related to the application of lockout in Quebec companies and (ii) understand the factors promoting the application of lockout programs and procedures, as well as (iii) to identify lockout's best practices. Based on the literature, but more importantly in studying the application in companies, we characterize technical, organizational and human difficulties, the factors promoting it and the reasons of the non-application of lockout. This research will enable us to identify the best practices on the subject within an industrial sector and potentially transpose them to other industries. The study will likely enable to define the lockout applicability criteria, identify the difficulties associated with its application and the design of auditing tools to evaluate the application of lockout in companies.

The objective of this article is to briefly describe the methodology and the tools that have been used, as well as to present preliminary results. More specifically, we are targeting to respond to the following questions:

1. Are lockout placards used during the application of lockout procedures and can we do lockout without placard ? If so, under which conditions?
2. Is it possible to apply lockout to all types of energy on machines? Is the lock in use? Are the workers using other lockout accessories (e.g. tag)?
3. Are all maintenance tasks done and/or can they be done when applying lockout procedures? What about the adjustment, cleaning and unjamming tasks? Are they done following a lockout procedure?
4. Are workers always doing the verification steps? If so, what methods are they using?
5. Is software dedicated to lockout needed? What are the selection criteria?
6. Is it possible to use a simplified lockout program for small-medium enterprise versus large organization? If so, what elements of the program are involved?

4 RESEARCH METHODOLOGY

The methodology is mainly based on the analysis of lockout documents, questionnaires and observations collected within organizations that are using lockout for many years. Companies operating in the sawmill sector are participating in this study. Data collection tools, such as questionnaires, checklists and observation checklists have been developed and used in organizations in order to respond to the questions exposed previously. Individuals included in this study are workers practicing lockout in organization, as well as managers from these companies.

4.1 Company Selection

Selection criteria have been set for identifying the organizations. The study includes small, medium and large enterprises which are practicing lockout for a long time. Approximately 10 sawmills with at least 5 years of experience in practicing lockout have been chosen in the province of Quebec. The Association of Health and Safety in Forestry Industry (ASSIFQ) has accepted to contribute in the company selection. Currently, a number of sawmills have accepted to collaborate and 4 of them have been visited so far.

4.2 Company Visits

The visits in the sawmills have started by sending a confidential letter and a consent form to workers. The documents to be used during the visits are communicated to them prior to our visit. The duration of each visit is 2 days and is done by two researchers from Polytechnique.

During the visits, the workers responded to a series of questions during semi-structured interviews. The health and safety officer in the organization acted as liaison to plan the work (visits and data collection) and forwarded the documents and tools to the selected individuals. The goal for involving the management and workers was to identify the similarities and differences between responses, and to try to identify the driving factors and difficulties related to the application of lockout. Workers have been chosen randomly while the managers were predetermined before the selection.

4.3. Development, Validation, Treatment and Analysis of Observation Tools

Various types of tools have been developed in order to study the lockout management (program, procedure, etc.) and application. The application of lockout has been observed using checklists. Afterwards, semi-structured interviews with the manager and the workers were conducted separately.

Four observation tools (data collection checklists) have been developed based on the 2 visits in the organizations. The tools have been validated in 2 companies and 2 additional organizations have been visited afterwards. Data collection checklists enable us to process the previously identified problems and to gather unanticipated data. Those checklists have been developed based on the knowledge available from the standards, the reference documentation (books, guides, training, etc.) and as per the actual experience of the researchers. The data collection checklists are numbered, allowing us to link the questionnaires and enabling comparison at the end of the study. The tool validation step enabled us to (i) ensure they are meeting the research objectives, (ii) improving the tools when possible and (iii) to understand the limits of their use.

After every company visit, the data collected were organized in a data collection checklist (e.g. Excel), which contained and organized the company information by topic. Each question from each checklist is linked to a reference number, making the comparison easier at the end of the visits. It is easier to compare the responses to each question and to compare the data afterwards.

5 PRELIMINARY RESULTS

The 4 sawmills visited have produced and integrated lockout placards internally. The majority of lockouts were observed during operation tasks (e.g. unjamming, changing saw) and maintenance (chain changing, machine greasing). Table 1 shows a summary of the preliminary results obtained.

Table 1: Preliminary results of 4 visits in sawmills

	Sawmill 1	Sawmill 2	Sawmill 3	Sawmill 4
Number of lockout (and unlocking) observed	5	6	10	8
Number of times the placard was used	1 (maintenance)	0	0	3 (2 operation, 1 maintenance)
Operation	3	3	6	6
Maintenance	2	3	4	2
Use of lock(s)	5	6	10	8
Use of tag()	0	0	0	0
Use of lockout box	5	6	10	8
Start-up test (verification step)	5	1	0	7
Use of lockout software	No	No	No	No

Out of 29 lockout observed, the lockout placard was used only 4 times, including twice for maintenance and twice for operation. The placard has never been consulted for unlocking. Afterwards, within the 4 plants observed, the placards were available for all tasks related to the equipment. Placards were as valid for maintenance work as for operations. Tasks related to electrical installation (from main entrance to local distribution) were not done nor included in any program. Note that placards were built on an equipment basis and not based on tasks on the equipment, therefore the whole equipment would be locked out. Furthermore, sawmills do not use protective devices (e.g. safeguards) for equipment, and safety interventions are only related to the lockout procedure. Plants seem to link the lockout to the risk from the machine instead of electrical risk.

All sources observed and all isolating devices can be locked out. Following interviews with managers and workers, it has been confirmed that all sources of energy on their machines can be isolated and locked out. During the observed interventions, only the lock was present, the tags were not in use. Lockout boxes in all cases with lock series were used.

The verification step, i.e. the absence of energy when doing the lockout, is practiced in 2 sawmills. Out of 29 observations, only 13 of them proceeded with a start-up test after the lockout. Microsoft Word or Excel software were used by the 4 plants in order to create and modify the lockout placards. They do not use a software dedicated to lockout placards or the management of lockout.

Regarding the question « Is it possible to have a simplified lockout program for SME versus large organization, and if yes, which elements of the program are involved? » we believe that, following the results obtained with the 4 first plants, it is more important to consider simplifying the lockout and not to make a distinction between large and small organizations when determining the rules. Lockouts observed have shown that the worker is looking for the quickest way to comply with the requirement from his employer. Comments made during the interviews revealed that the closest energy isolating points possible and the simplification of the unlocking steps (energy resetting of the machine) to ease the lockout are example of factors promoting lockout.

6 CONCLUSION

The objective of this study is to analyse and evaluate the application of lockout on machines in companies operating in the wood transformation industry in Quebec. Expected results will be translated into: (i) a better comprehension of the difficulties experienced by companies during the application of lockout, (ii) a better comprehension of the factors or criteria for promoting the application of lockout and (iii) suggestions to ease the application of lockout programs and procedures. The knowledge acquired will enable the suggestion of multidisciplinary solutions to solve the problems identified related to lockout. As shown by the preliminary results, sawmills do have lockout programs and procedures and they apply them. Over the years, they have developed certain practices that may help other organizations. In spite of the efforts deployed in this industry, non compliance of all the steps by workers remains an issue. This study is not completed and additional elements will certainly arise during the next visits.

7 REFERENCES

- Blaise J.C. and Welitz G., *Operating on machinery out of production modes: principles and accidentology*, Proceedings of 6th International Conference on Safety of Industrial Automated Systems, 2010.
- Bulzacchelli, M.T., (2006). *An evaluation of the impact of OSHA's control of hazardous energy (lockout/tagout) standard on fatal occupational injury*. Thesis, The Johns Hopkins University. Baltimore, Maryland.
- Bulzacchelli M.T., and al. *Circumstances of fatal lockout/tagout related injuries in manufacturing*. American journal of industrial medicine, 2008, Vol. 51, p 728-734.
- Bulzacchelli, M.T., Vernick, J.S., Sorock, G.S., Webster, D.W., Lees, P.S.J., (2008). *Circumstances of fatal lockout/tagout related injuries in manufacturing*. *American journal of industrial medicine*, 51 728-734.
- Bulzacchelli, M.T., Vernick, J.S., Webster, D.W., Lees, P.S.J., (2007). Effects of the occupational Safety and health administration's control of hazardous energy (lockout/tagout) standard on rates of machinery-related fatal occupational injury.
- Chinniah Y., Champoux M., Bulet-Vienney D., Daigle R. (2008). *Analyse comparative des programmes et procédures de cadenassage appliqués aux machines industrielles*, R-587, *IRSST*, Montréal.
- CSA Z460-05 (2005). Control of hazardous energy: Lockout and other methods, Canadian Standards Association.
- CSA Z460-05, *Maîtrise des énergies dangereuses : cadenassage et autres méthodes*, Association Canadienne de Normalisation, 2005.
- CSST (2005). Cadenassage – dérogations, du 2 août 2001 à 2004, Données observées au 5 avril 2005, DCGI, Service de la statistique, CSST. Présentation de Christyne Côté, Direction prévention-inspection, dans le cadre d'une réunion du Comité multisectoriel sur le cadenassage le 14 avril 2005.
- CSST (2008). La CSST invite les milieux de travail à cadenasser, Communiqué disponible sur http://www.csst.qc.ca/portail/fr/actualites/2008/29_septembre_cadenassage.htm, Commission de la santé et de la sécurité du travail au Québec, Montréal.
- Daoust A., *Le cadenassage, une question de survie*, Le Groupe de Communication Sanssectra Inc., 2003.
- Garand, P., Roy, M., Desmarais, L., (2005) *L'observation des comportements sécuritaires par les pairs dans une usine d'assemblage : Le cas Paccar*. *Pistes*, 1 (7).
- INRS (1996). *Consignations et déconsignations*, Institut National de Recherche et de Sécurité (INRS), ED 754, 1996.
- INRS (2008). *Intervention sur un équipement de travail. Réflexions sur la sécurité lors des arrêts*, Institut National de Recherche et de Sécurité (INRS), ED 6038, 2008, 24 p.
- Kelly S., *Lockout Tagout: A Practical Approach*, American Society of Safety Engineers, 2001.
- Murphy, S.R., (1989). *Effects of attitudes on behavior after participation in an industrial safety training program*. Thesis, Wayne State University, Detroit, Michigan.
- Mutawe, A.M., Tsunehara, R., Glaspey, L.A.. (2002). OSHA'S lockout/tagout standards: a review of key requirements, *Professional safety*, Vol. 47, no. 2, p. 20-24.
- OSHA 1910.147. Regulations Standards – 29 CFR, The control of hazardous energy (lockout/tagout), http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9804
- Shaw S., *Machinery accidents- Contributory factors*, Proceedings of 6th International Conference on Safety of Industrial Automated Systems, 2010.
- US Department of Labor (2005). Bureau of Labor Statistics, National Safety Council: 2005.

Integration of maintenance at design stage: the machinery directive lays down objectives

Jean-Christophe BLAISE
Institut national de Recherche et de Sécurité (INRS)
1 rue du Morvan - CS 60027
F-54519 VANDOEUVRE cedex
jean-christophe.blaise@inrs.fr

Keywords: maintenance, machinery directive, engineering

ABSTRACT

Safety for work equipment production-related modes is taken into account fairly comprehensively by regulatory and normative benchmarks. Manufacturers of work equipment have applied these benchmarks throughout the 20 years of their existence and development. On the other hand, other modes, such as machinery setting or those involving maintenance, remain scarcely integrated because they have been little researched from a safety standpoint. This has resulted in a migration of accidents towards modes other than production. INRS-conducted accident analysis and maintenance process formalisation research highlight yet again the multidisciplinary nature of these accidents; equipment design is one of these causes. Regulatory requirements exist, specifically in the “Machinery” directive, along with normative provisions, which impose objectives on designers to ensure maintenance operation safety.

Based on the above research and documents emerging from the European campaign undertaken by the Bilbao agency, we briefly recall the various sources of maintenance activity criticality. Different requirements of the “Machinery” directive directly or indirectly concerning maintenance are specifically examined. Comments, partly based on the directive’s application guide, reveal more specifically the impact they can have on greater integration of safety into design. Even though maintenance is an activity and its relevant organisational factors are of great importance because of this, design of the equipment concerned by this activity is none the less an essential component.

1 MAINTENANCE CRITICALITY: VARIOUS CAUSES

Unlike company “production” activities, which have been the subject of extensive research, few studies have focused on maintenance activities [1]. Yet, an analysis of the few available studies reveals that these activities are strongly accident causing [2]. EUROSTAT data provide the following figures: 15 to 20% (depending on the country) of the total number of accidents and 10 to 15% of fatal accidents are associated with maintenance operations.

We observe more globally that risks related to work equipment operation tend to be deferred to maintenance operations. In practice, work equipment operation in automatic mode generally takes place without direct intervention of the operator. However, any type of malfunction frequently leads to operation in degraded mode (semi-automatic or manual with the operator present) or even failure, then requiring a maintenance operation. Furthermore, maintenance activity is changing due to the growing complexity of industrial systems. A veritable mutation in maintenance is currently in progress due to increasing complexity of the maintained object: introduction of mechatronics, for example, means that the maintenance operation is no longer performed only on the mechanical, but also on the electronic component. Finally, while conventionally ensured by the company via an independent, centralised service or department composed of specialised operators, maintenance organisation has changed and now assumes multiple forms: subcontracting, maintenance task transfer to operational structure, geographical maintenance, versatility of operators, etc. These organisational choices are not always without consequence for safety.

We may also question the target of prevention measures. While it would seem that the repair phase is the most hazardous, should all prevention measures be directed towards this phase? Is the source of the criticality of the repair phase not located somewhere in its upstream phases? For example, a preparation phase subjects the operator to almost no major risk, yet incomplete preparation may prove to be a determining factor during an operation on the work equipment!

Similarly and even further upstream, the characteristics of the equipment to be maintained turn out to be a determining factor in relation to performing the maintenance operation. We can distinguish intrinsic, design-related characteristics, such as equipment maintainability and operating characteristics, i.e. the energy state of the equipment during the maintenance operation. During the European maintenance campaign, five basic rules were established: plan the operation, secure the operating area, use suitable equipment, work according to plan, and perform final inspection. The first and last of these rules are specific to machinery usage but, although they also have powerful implications during usage, the other three originate right from machinery design phase. We indeed find these design-related risk factors (maintainability, accessibility, devices missing) in an analysis of maintenance accidents (Figure 1).

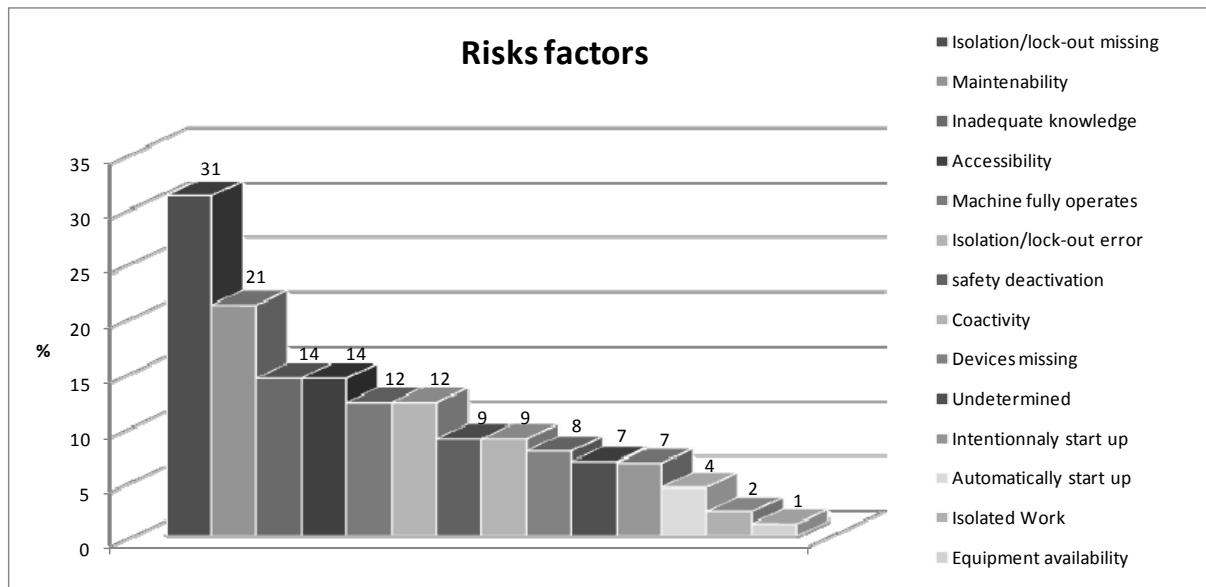


Figure 1. Distribution of non-production accidents per risk factor. [3]

2 ESSENTIAL REQUIREMENTS OF THE DIRECTIVE

In every case, the objective laid down by Directive 2006/42/CE [4] is effectively to intervene based on a guaranteed safe working area for the operator. It is therefore up to the designer to foresee safety measures for all equipment operating modes. However, finding technical solutions suited to operating outside production is not necessarily obvious for the designer, who may therefore be tempted to transfer the safety requirement to organisational measures. Annex 1 of the “Machinery” directive lays down essential health and safety requirements relating to the design of work equipment. Maintenance-related requirements are included in a dedicated section of the directive, but are also found more or less explicitly at various places in the text.

The purpose of this section is to address the regulatory aspects at design stage, but we may also cite Directive 2009/104/CE [5], which applies to machinery in operation at workplaces. During the life of the machinery, through adequate maintenance, the employer must ensure that this machinery is kept at such a level that it continues to meet the conditions applicable when it was made available for the first time at the company or establishment. This does not mean that machines must be maintained “as new” since they are subjected to wear. However, the necessary maintenance must be performed to guarantee that they continue to comply with applicable health and safety requirements.

Without reviewing the entire text of the directive (shown in italics in this paper), direct comments are made in relation to the principal requirements in phase with the directive’s application guide [6].

2.1 Sections impacting on maintenance

These are fairly rare, in fact, but it should be recalled that Section 1.1.2 concerning safety integration principles requires that the machinery be designed without exposing anyone to a risk during any of the machinery's phases of life, including maintenance. Three sections effectively impact explicitly on maintenance.

- Section 1.1.4 concerning lighting: "*Internal parts requiring frequent inspection and adjustment, and maintenance areas must be provided with appropriate lighting.*": maintenance is often performed in dark areas, so specific systems must ensure better visibility.
- Section 1.3.2 concerning risk of breaking up during operation: "*The instructions must indicate the type and frequency of inspections and maintenance required for safety reasons. They must, where appropriate, indicate the parts subject to wear and the criteria for replacement.*" Certain machinery parts, subjected to wear leading potentially to break-up, may require inspection by the user and repair or replacement, if need be. The manufacturer's instruction manual must indicate the type of inspection to be undertaken on these parts (e.g. visual inspections, functional inspections or tests), the frequency of these inspections (e.g. in terms of number of work cycles or usage time) and criteria for repairing or replacing the relevant parts.
- Section 1.4 concerning required characteristics of guards and protective devices, in particular two bullet marks in Section 1.4.1 concerning general requirements: "*Guards and protective devices must [...] not be easy to by-pass or render non-operational, [...]enable essential work to be carried out on the installation and/or replacement of tools and for maintenance purposes by restricting access exclusively to the area where the work has to be done, if possible without the guard having to be removed or the protective device having to be disabled.*" Positioning of adjustment, machinery setting and servicing points to avoid the need to remove guards for routine servicing operations; this point is covered in Section 1.6.1.

The sixth bullet mark in Section 1.4.1 requires guards and protective devices to be designed and built, as far as possible, such that they are not an obstruction to the operator's view of the machinery working area. Inadequate knowledge of this aspect increases the risk of guards and protective devices being disabled or by-passed by operators. Working area visibility can be improved by installing transparent guards or, when there is no object ejection or emission risk, by installing guards featuring openings or protective devices. The seventh bullet mark in Section 1.4.1 states that guard and protective device design and construction must consider the need to access danger zones either during machinery operation or for maintenance purposes. Guards and protective devices must restrict access to the area, in which the work is to be performed. Positioning of adjustment, machinery setting and servicing points outside danger zones may prevent the need to remove guards for routine operations. However, the wide variety of operations to be performed means that this compromise is not always easy to implement.

2.2 A section specific to maintenance

Section 1.6 is dedicated to maintenance. It includes five sub-sections:

- Section 1.6.1. *Machinery maintenance*

The first paragraph of Section 1.6.1 cites important general principles of machinery design aimed at ensuring safe performance of maintenance operations. Locating adjustment and servicing points outside danger zones prevents operators in charge of maintenance from having to enter danger zones to perform their tasks by disabling protective devices. *It must be possible to carry out adjustment, maintenance, repair, cleaning and servicing operations while machinery is at a standstill.* As an example, at locations where tools have to be changed or removed for cleaning, the machinery must be fitted with devices allowing them to be released without starting the machinery. If special equipment is required for this purpose, it must be delivered with the machinery. In some cases, it may not be necessary to stop the whole machine insofar as parts, on which the work is performed, and parts likely to affect operator safety, are at a standstill.

The second paragraph of Section 1.6.1 recognises that it is not possible, in every case, to avoid the need to enter danger zones to perform maintenance and that it may be necessary to perform some adjustment or machinery setting operations with the machinery running. In these cases, the machinery control system must include an appropriate safe operating mode, as stated in Section 1.2.5. This reference corresponds to the requirements relating to control or operating mode selection. It turns out that this concerns mostly the notion of maintenance. The old directive (98/37/CE) already anticipated that "*for certain operations, the machinery must be able to operate with its protection devices neutralised*" and listed all the conditions to be complied with. The new directive now adds that, "*If these four conditions cannot be fulfilled simultaneously, the control or operating mode selector must activate other protective*

measures designed and constructed to ensure a safe intervention. From a “practical” standpoint, this is a step forward since there are indeed operations that can only be performed with the protection system disabled or neutralised, without complying with all the conditions stated in the text. However, compensation measures are reflected in some standards by implementation of organisational measures and making safety dependent on only operator training. “Quick” interpretation of this requirement therefore opens the door to “minimum” protection measures, while the text demands implementation of other measures. Technical principles are proposed [7] for meeting this requirement.

The third paragraph of Section 1.6.1 requires that the machinery be equipped, if necessary, with means of mounting equipment required for diagnostic fault-finding. It is possible to go even further by installing predictive maintenance systems.

The fourth paragraph requires the manufacturer to design automatic machinery to facilitate removal and replacement of components, which must be frequently changed. A safe operating mode for these maintenance operations must be planned and clearly detailed in the instruction manual.

- Section 1.6.2. *Access to operating positions and servicing points*

The requirement stated in Section 1.6.2 must be taken into account when establishing operating positions and servicing points. Location of operating positions and servicing points in easily accessible zones, e.g. on the floor, avoids the requirement for special means of access. When special mean of access is unavoidable, operating positions and servicing points, to which frequent access is required, must be located such that they can be easily reached using appropriate equipment. Means of access must be located outside danger zones in the same way as adjustment and servicing points. The machinery manufacturer is responsible for ensuring that equipment required for safe access is supplied with the machinery. This requirement also applies to cases in which machinery construction is completed in the user buildings. In these cases, the machinery manufacturer may take into account any means of access already existing in the buildings; this must be detailed in the technical package.

Means of access for operating positions must be designed taking into account the tools and equipment required for machinery maintenance. Special means of access for exceptional operations, in particular performing exceptional repairs, may be specified in the manufacturer’s instructions.

- Section 1.6.3. *Machinery isolation from energy sources*

The requirements stipulated in Section 1.6.3 are intended to keep the machinery safe during maintenance operations. For this purpose, operators performing maintenance operations, while the machinery is stopped, must isolate the machinery from its energy sources prior to starting the operation. The aim is to prevent hazardous situations, such as untimely starting of the machinery, whether this is due to machinery faults, and action of persons possibly unaware of the presence of maintenance operators or inadvertent actions by maintenance operators themselves. For this purpose, means of isolation allowing operators to disconnect the machinery and reliably isolate it from all sources of energy, including mechanical, hydraulic, pneumatic or thermal, must be provided.

The third paragraph of Section 1.6.3 imposes a duty to fit the machinery with means enabling all accumulated energy, potentially hazardous for operators, to be “normally” dissipated. Such accumulated energy may include, for example, kinetic energy (inertia of moving parts), electrical energy (capacitors), pressurised fluids, springs or machinery parts that may move under their own weight.

The fourth paragraph states that, as an exception, certain circuits can remain connected to their energy source to allow, for example, parts to be held, information to be protected, internal parts to be lit, etc. In this case, special measures must be taken to ensure operator safety. An exception to the requirements specified in the first three paragraphs is therefore allowed, when energy supply to certain circuits must be conserved during maintenance operations in order to guarantee safe working conditions. For example, it may be necessary to maintain the electrical supply to safeguard stored information, for lighting, for tool operation or for extracting dangerous substances. In such cases, the electrical supply must only be maintained on circuits, for which it is really necessary, and measures must be taken to guarantee operator safety, for example by preventing access to the parts concerned or by providing necessary warnings or alarm systems.

The manufacturer’s instructions for adjustment and maintenance operations must include information on isolating energy sources, locking isolation devices, dissipating residual energy and checking the safe state of the machinery. Standard EN 1037 [8] provides general specifications for isolation and locking means in relation to different energy sources. For machinery falling within its scope of application, Standard EN 60204-1[9] contains specifications for reliable disconnection of the electrical supply.

- Section 1.6.4. *Operator intervention*

Section 1.6.4 re-states a general requirement: "*Machinery must be so designed, constructed and equipped that the need for operator intervention is limited. If operator intervention cannot be avoided, it must be possible to carry it out easily and safely*".

- Section 1.6.5. *Cleaning of internal parts*

The requirement stated in Section 1.6.5 addresses an example of the type of operator intervention referred to in the preceding section, which may be particularly dangerous. The fact of entering parts of the machinery, e.g. silos, tanks, vessels, containers or pipes, which have contained dangerous substances or preparations, may give rise to a risk of intoxication or asphyxiation for both the operators involved and the persons attempting to rescue them. The general rule, stated in the first sentence of Section 1.6.5, is that it must be possible to clean or unblock these parts from the outside so that they do not have to be entered. When entering these parts is unavoidable, protection measures must be taken, for example installation of an adequate ventilation system, monitoring of dangerous substance concentration or oxygen deficiency in the air and measures for watching and safely rescuing operators.

2.3 Instruction manual

The instruction manual is often referred to in previous paragraphs. Technical measures must be not only integrated into the machinery, but they must be also accompanied by information facilitating their usage. This is the purpose of the instruction manual. Section 1.7.4.2 stipulates requirements concerning its content.

Point e) deals with information and explanations required for safely using, maintaining and repairing machinery, as well as for checking its proper operation (more detailed requirements concerning instruction manual content in relation to these aspects are given in the following sections). Simple, clear drawings, diagrams, graphs and tables are generally preferred to long written explanations; necessary written explanations should be placed next to the illustrations, to which they refer.

Point f) deals with workstations likely to be occupied by operators. Aspects to be covered include, more specifically for maintenance, a description of the different workstations, operating and control modes, as well as relevant protective and prevention measures. This confirms the importance of identifying maintenance-, adjustment- and observation-related modes. These modes indeed cannot be described, if they are not identified and thus integrated right from machinery design phase.

Point k) deals with instructions for operator training. This includes maintenance operators for the workstations and modes described in point f).

Point q) requires the machinery manufacturer to anticipate potential improper operation of the machinery and details the procedures to be followed for dealing with emergency situations. The instruction manual must also describe the procedure to be followed in the event blocking of moving parts and explain the usage of any protective device or special tool provided for this purpose.

Point r) states that the manufacturer is duty-bound to describe the adjustment and maintenance operations to be performed by the user. Specifically, the instruction manual must state the frequency of these operations. It must also include a list of machinery parts or components, which must be regularly inspected for any excessive wear, state the frequency of these inspections (expressed in terms of time of usage or number of cycles) and detail the type of inspections or tests required and the equipment to be used. Criteria to be complied with for determining whether a worn part requires repair or replacement must also be specified.

Point s) details the methods and procedures to be followed to ensure that the operations described in point r) are safely performed. Adequate protection measures and precautions to be taken during maintenance operations must be indicated.

Finally, point t) refers to spare parts information. In general, spare parts supply is not covered by the provisions of the "Machinery" directive and this issue therefore depends on the contractual agreement concluded between the manufacturer and the user. However, when components subject to wear need to be replaced specifically to protect user health and safety, suitable spare parts specifications must be communicated.

Naturally, these requirements remain very general. The purpose of the directives is to establish objectives, but without providing the means of achieving them. This purpose falls within the scope of standards such as EN ISO 14122 (Permanent Means of Access to Machinery), EN 547-1 (Human Body Measurements), EN 1037 (Safety of Machinery - Prevention against Unexpected Start-up) and ISO 12100; However, their application not always easy and requires significant thought of the part of the designer.

3 CONCLUSION

Safety for production-related modes is taken into account fairly comprehensively by regulatory and normative benchmarks. Manufacturers of work equipment have applied these benchmarks throughout the 20 years of their existence and development. On the other hand, other modes (e.g. degraded) and different machine stoppage states have been little studied from their safety angle. These are indeed neither defined nor characterised by manufacturers, whose aim is to build machinery that “produces”. This observation is the same for users, who consider their equipment simply as means of production. “Non-productive” modes are in fact not worthwhile. Yet, maintenance operations remain necessary; apart from the fact that machinery is not above damage or even failure, it also quite simply needs to be maintained.

The “Machinery” directive establishes objectives to be achieved to make equipment maintenance operations safe. However, the major difficulty resides in taking into account, at design stage, of the future needs of work equipment intervention. To facilitate identification, we must establish dialogue between designers and future users through drawing up specifications or seeking user experience feedback, when available.

Another difficulty involves compatibility of the measures adopted for one mode with another mode. Dangerous phenomena can effectively differ, depending on the mode of intervention; means of protection can also be different, depending on the mode, for the same dangerous phenomenon. Finally, a means of protection for an operating mode may turn out to be a cause of damage in another mode. Prevention solutions are therefore not easy to optimise and it is, of course, risk assessment that must enable prioritisation of prevention measures and ultimately prohibit certain energised operations by resorting to ... isolation!

4 REFERENCES

1. Grusenmeyer C., *Les accidents du travail liés à la maintenance. Importance et caractérisation*, Hygiène et sécurité du travail, Cahiers de notes documentaires, ND 2238, 4^{ème} trimestre 2005, 201, pp. 31-44.
2. European Agency for Safety and Health at Work, *Maintenance and Occupational Safety and Health: A statistical picture*, Bilbao, EU-OSHA, 2010.
3. Blaise J.C., Welitz G., *Operating on machinery out of production modes: principles and accidentology*, Proc. of the 6th Int. Conf. Safety of Industrial Automated System, Tampere Hall, Finland, 2010.
4. DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, Official Journal of the European Union, L157, 2006, pp. 24-86.
5. DIRECTIVE 2009/104/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work, Official Journal of the European Union, L260, 2009, pp. 5-19.
6. European Commission Enterprise and Industry, *Guide to application of the Machinery Directive 2006/42/EC*, 2nd Edition, 2010.
7. Blaise J.C., Welitz G., *Intervention on Machines - Operating Modes with “disabled safeguarding”*, Proc. of the 7th Int. Conf. Safety of Industrial Automated System, Montreal, Canada, 2012.
8. European Committee for Standardisation, *EN 1037:1995+A1:2008 - Safety of machinery - Prevention of unexpected start-up*, Brussels, 2008.
9. European Committee for Electrotechnical Standardisation, *EN 60204-1:2006/A1:2009 - Safety of machinery - Electrical equipment of machines - Part 1: General requirements*, Brussels, 2009.

Intervention on Machines: Operating Modes with “disabled safeguarding”

Jean-Christophe BLAISE, Guy WELITZ
Institut National de Recherche et de Sécurité (INRS)
1 rue du Morvan - CS 60027
F-54519 VANDOEUVRE cedex
jean-christophe.blaise@inrs.fr
guy.welitz@inrs.fr

Keywords: maintenance, process observation, safeguarding defeating

ABSTRACT

Accidentology findings highlight the persistence of problems involving machine lockout. Technical solutions exist for properly locking out work equipment and are extensively described, yet their application often remains improper. Although based on a strong technical focus, it is the nature itself of this solution that nevertheless remains a direct instruction requiring compliance with organisational measures. Moreover, machine manufacturer instruction manuals recommend general machine lockout for all maintenance operations without considering actual operating conditions and related constraints. Most often, this type of instruction will not be applied because it is considered a procedure that is onerous to implement, especially due to the operation time/lockout time ratio or, simply because the operation requires full or partial energy conservation.

We propose researching these energized operations, which require implementing operating modes with “disabled safeguarding”, and determining which principles enable operations to be safely performed by implementing other risk prevention measures. We will specifically focus on one type of operation: process observation. This is most frequently performed for diagnostic purposes in order to assess proper operation (e.g. in terms of installation performance or product quality), malfunctions or failure causes and their localisation. Decisions are made based on this observation operation: actions involving process validation, adjustment, maintenance, etc. We will demonstrate that prevention measures should be considered based on two operating modes, namely with Production Protection Devices Active (PPDA) and with Production Protection Devices Neutralised (PPDN), to safeguard these operations. The latter type involves implementing a specific so-called “observation” mode, which is designed to protect operators located in the observation zone.

1 INTRODUCTION

Operators need to intervene on work equipment during both production and maintenance activities. Whenever possible, these operations must be defined by the designer, but they are performed at the user’s initiative.

A recent INRS study provides a review of operations performed on work equipment outside normal production. Different possible operations on a machine have been identified and architectures for work equipment life phases, from design to decommissioning, have been proposed with a view to ensuring terminological uniformity. Additionally, analysis of accidents on the EPICEA¹ database has confirmed the safety problems associated with operating on energised machinery due to not implementing lockout procedures or the need to conserve fully or partially its energies [1] [2].

Moreover, one mode has been specifically analysed: process observation. Based on regulatory texts, an approach to safeguarding this mode has been proposed in compliance with the assessment and risk reduction methods recommended by Standard ISO 12100 [3]. This approach fulfils the need to observe an area based on designing a suitable operating and safety mode. Studied examples of safeguarding for the “process observation” mode show that integrating such modes into design requires identification of the operation need and hence dialogue between the designer and “future” users.

¹ EPICEA is an anonymous, non-exhaustive, French national database consolidating more than 17,000 cases of occupational accidents that have been sustained by employees covered by the general social security system since 1990. These accidents were fatal, serious or significant in prevention terms.

2 AN OPERATION REQUIREMENT: PROCESS OBSERVATION

Process observation is most frequently performed for diagnostic purposes in order to assess proper operation (e.g. in terms of installation performance or product quality), malfunctions or failure causes and their localisation. Decisions are made based on this observation operation: actions involving process validation, setting and adjustment, maintenance, etc.

For example, for goods with high added value, operators feel the need to observe proper production performance. Design must therefore take into account this “culture”.

At design stage: designer/user dialogue enriches possible experience feedback, enabling identification of the operation need and thus relevant machine design. For a machine in service: if the need for observation is identified when the machine possesses no mode provided with suitable safety devices, then modifications will be necessary, but will be more difficult to implement since they may require all or part of the machine, including the control system, to be re-designed.

Process observation actions must be undertaken without exposing anyone to a risk. Prevention measures following risk assessment involve, in the following order:

1. Favouring inherently safe design, for example by eliminating the operation need,
2. Implementing alternative measures ensuring a safe operation, such as cameras, diagnostic aids, a suitable inspection hatch prohibiting access to hazardous parts, etc.,
3. Implementing a specific mode.

Prevention measures should therefore be considered for two types of operation:

- PPDA: operation with Production Protection Devices Active. This covers “conventional” production operation in automatic, manual and derived modes with related protection devices active (see points 1 and 2 above).
- PPDN: operation with Production Protection Devices Neutralised. In this case, protection devices that are active in production mode are totally or partially neutralised (i.e. their effect is annulled) either by removing guards or by de-activating protection devices. PPDN-based operation must be linked to integration of a so-called specific "observation" mode designed to protect operators present in the observation zone (see Figure 1).

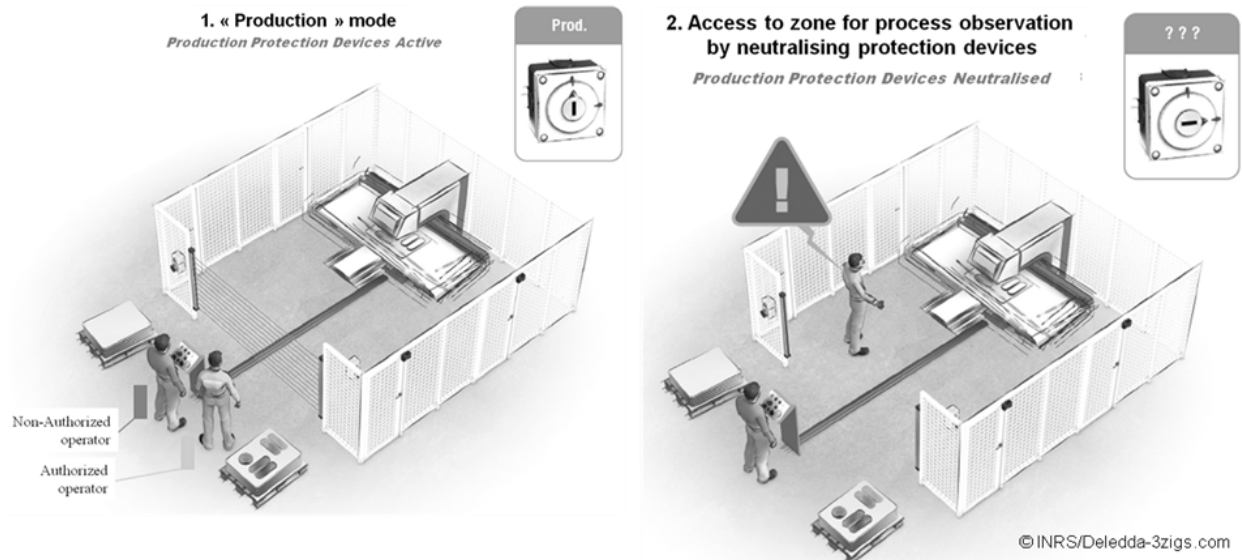


Figure 1. Need to access a hazardous zone to observe a process

3 OPERATING CONDITIONS BASED ON “PROTECTION NEUTRALISATION”

Preference should be given to performing the operation with PPDN. However, if the need for operating with PPDN is justifiable, the four conditions described in Section 1.2.5 of Directive 2006/42/EC [4] must be complied with when setting up the “observation” mode.

" If, for certain operations, the machinery must be able to operate with a guard displaced or removed and/or a protective device disabled, the control or operating mode selector must simultaneously:

- 1. Disable all other control or operating modes,*
- 2. Permit operation of hazardous functions only by control devices requiring sustained action,*
- 3. Permit the operation of hazardous functions only in reduced risk conditions while preventing hazards from linked sequences,*
- 4. Prevent any operation of hazardous functions by voluntary or involuntary action on the machine's sensors.*

For process observation purposes, compliance with some of the above conditions may prove impossible. This case has been foreseen by the directive, which introduces a “derogation”: *If these four conditions cannot be fulfilled simultaneously, the control or operating mode selector must activate other protective measures designed and constructed to ensure a safe intervention zone. In addition, the operator must be able to control operation of the parts he is working on from the adjustment point.*

Note. The term “adjustment point” in the directive may be taken too restrictively; the idea of a “point” should be understood in its widest sense. The requirement of the directive is therefore just a valid for an “observation point”.

Circumstances leading to inability to comply with the four conditions described above may be respectively:

- A necessity to observe machine operation with normal operation characteristics (e.g. in automatic mode); protection devices installed for this operation may prevent access to the observation zone and they must therefore be neutralised
- Continuous action controls cannot be maintained, if the operator needs both hands, if maintaining the control device creates ergonomic problems or if untimely stop due to releasing a continuous action control is hazardous (breakage, ejection), etc.
- The risk cannot be reduced because the operation requires a normal machining speed, for example
- Linked sequences at normal speed need to be checked (e.g. program restoration)
- Some operations, especially those that are diagnostic, require intentional action on sensors implementing hazardous functions.

Furthermore, some applications require simultaneous derogation from more than one of the four conditions. However, the objective is to fulfil as many of the four conditions as possible! In this case, other compensation protection measures must be implemented. These must be designed and built to guarantee the safest possible working area. To achieve this, Appendix D of Standard ISO 11161 [5] on setting up a process observation mode recommends an analysis logic diagram. However, this “too easily” leads the machine designer to merely provide usage information and to fall back on measures taken by the user. Despite their importance, operator training and work organisation alone cannot substitute for protection measures to be implemented.

The manufacturer has a duty to ensure that the machine technical documents include “proof” that this additional PPDN-based operating mode is effectively necessary. For special machines, this mode must form the subject of detailed discussions between the manufacturer and the future user.

There is no “universal” measure for safeguarding the observation mode during PPDN-based operation. “Conventional” analysis, based on Standard ISO 12100, should be conducted to assess and reduce the risk and to define what technical protection measures may be adopted. Prevention measure hierarchy must be respected, specifically: inherently safe design, safeguarding and complementary protective measures, information of use.

It is important that PPDN-based operation is not used for purposes other than those required for observation mode, e.g. by limiting speed and clearances, by allowing only a certain number of goods produced in this mode or by limiting observation time.

These limitations will only be realistic in the wake of detailed analysis of the operation need and its related activity; otherwise the installed safety devices may be by-passed [6]. The aim is to prevent other operations, such as repair or production restoration, being performed in this mode.

4 PREVENTION MEASURES FOR PROCESS OBSERVATION

The following inherently safe design measures eliminate the need to operate in hazardous zones and allow one to be in PPDA-based operating mode to observe the process:

- Make equipment reliable and specify wear part replacement criteria in instruction manual; the user must comply with these instructions, e.g. by scheduling preventive maintenance actions and not postponing them.
- At design stage, opt for solutions that eliminate malfunctions, e.g. involving jamming, variability of processed materials, constraints (mechanical, environmental, etc.).
- Integrate diagnostic aids, e.g. video and image analysis systems, PLC-based diagnostic functions, vibration analysis, oil monitoring, infrared thermographic systems, etc.
- Choose an arrangement suited to parts to be observed and use protection devices allowing good visibility in relation to these parts when maintaining PPDA-based operation.

Furthermore, very detailed description of machine performance characteristics and limits in the sales documentation facilitates selection of a machine suited to user needs and prevents improper usage from causing hazardous interventions during operation.

In PPDN-based operation, solutions meeting the four conditions in Section 1.2.5 of the directive should be favoured; otherwise protection measures need to be implemented. The wide variety of situations requiring PPDN-based operation does not allow us to describe fully the measures that could be implemented. However, it should be noted that in all cases:

- Any change of mode must be activated by a selector and must therefore include a stop between the two modes: switching to “observation” mode does not derogate from this!
- Personal Protective Equipment (PPE) must be worn in an observation zone, if there are residual risks of ejection, radiation, etc.
- Each control point in an observation zone must be equipped with an operational device ensuring normal stop and, if need be, stop for operational reasons or emergency stop (cf. Section 1.2.4 of the directive and ED 6038) based on the risk assessment.
- Access to observation zones must be restricted to accredited personnel (i.e. competent, qualified and trained, to whom specific authorisations have given).

5 EXAMPLE OF SAFEGUARDING FOR PROCESS OBSERVATION

In this section, we provide an example of a solution basis for safeguarding a process observation situation (see Figure 2).

The safeguarding principle involves entering the controlled space (defined by perimeter protection devices) with the machine stopped, enclosing oneself therein and positioning oneself in a “safe” observation zone, from which it will be possible to restart the process. The location of the observation zone and the type of protective measures it depend on the risk and the observation to be performed. For example, this could be embodied by:

- Perimeter protection ensured by fixed guards and access to the observation zone by moving guard and/or protection devices for zone exit detection. Standard ISO 13855 [7] and Standard ISO 13857 [8] can be referred to in relation to their layout,
- A continuous action operational device installed to keep the operator away: ranging from a simple pushbutton to a two-hand control device depending on the risks and observation needs. Standard EN 574 [9] may be referred to for two-hand control device selection and location.

The principles are illustrated by Figure 2 and broken down into four steps:

- Step 1. Machine operating with its production protection devices active.
- Step 2. Access to process controlled space requires “Observation” mode to be selected. Machine hazardous functions are then stopped. In this mode, all other control or operating modes are deactivated, except for emergency stop. An accredited operator can therefore enter the controlled space.
- Step 3. In “Observation” mode, the operator reactivates the controlled space perimeter protection to prohibit third party access (resetting of moving guard or protection device from within the controlled

space for each access option). Operator enclosure in this zone must exclude any possibility of the machine being restarted from outside the controlled space, e.g. via a key-lockable selector (operator must therefore keep the key) to prevent a mode change.

- Step 4. From the observation zone, the operator confirms activation of the process control system to be observed and can then start the functions required for process observation:
 - Case involving perimeter protection: operator confirms by closing the guard or activating the personal detection device.
 - Case involving continuous action operational device for keeping operator away: operator confirms using a specific control device (e.g. a pushbutton).

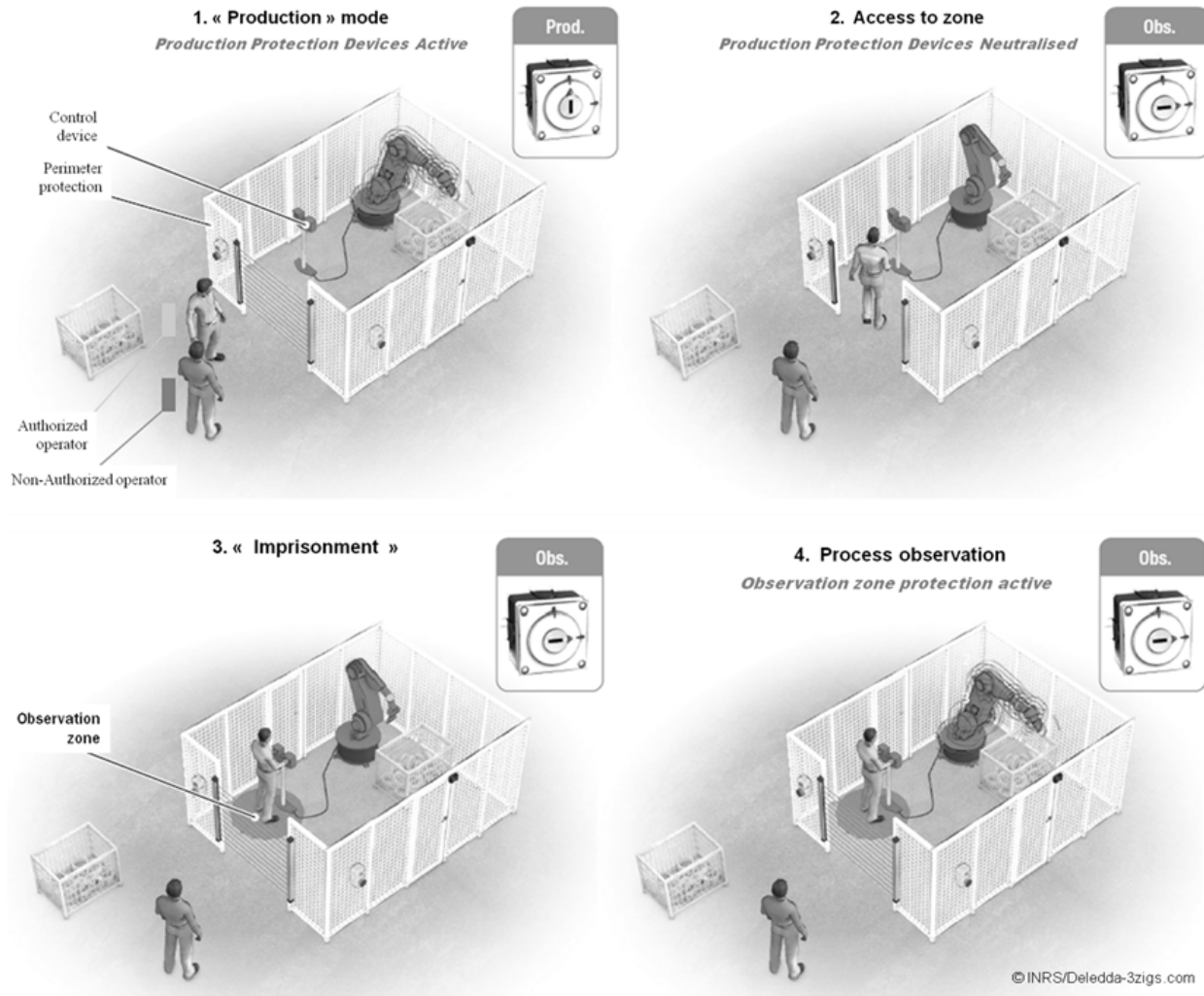


Figure 2. Safeguarding principles for process observation

The hazardous functions will stop, if the guard opens or if the detection device is by-passed or if the continuous action device for keeping the operator away is released. The following recommendations apply in the event of third party attempted intrusion into the controlled space, when cycle observation is in progress:

- For moving guards: these should be interlocked to prohibit untimely emergency stop,
- For personal detection devices: these should indicate the operation in progress to prohibit access (lock-out compliance, prohibited direction, pre-alarm before crossing or passing, etc.).

When the operator is in the controlled space, he must be able to leave it easily (e.g. anti-panic door).

6 CONCLUSION

Selecting protection measures to be implemented for process observation responds to the same approach as that used for selecting primary protection measures. A number of devices specific to safeguarding this mode have been developed, but they mainly involve implementing compensation measures (e.g. a portable emergency stop device) or managing organisational measures (RFID badges for accessing hazardous zones [10]).

Process observation is certainly not new, but installation complexity in terms of size and automation level calls for in-depth thinking in relation to safeguarding, especially through emergence of the idea of zones (ISO 11161).

However, the major difficulty resides in taking into account, at design stage, the future needs of work equipment intervention. To facilitate identification, we must facilitate dialogue between designers and future users or seek experience feedback from these users, when it is available.

Another difficulty involves compatibility of the measures adopted for one mode with another mode:

- hazardous phenomena can be different, depending on the operation mode,
- for the same hazardous phenomenon, protection means can also be different, depending on the mode,
- finally, a means of protection for an operating mode may prove to be a cause of damage in another mode.

Prevention solutions are therefore not easy to optimise and it is, of course, risk assessment that must enable prioritisation of prevention measures and ultimately prohibit certain energised operations by resorting to ... lockout!

7 REFERENCES

1. Blaise J.C., Welitz G., *Operating on machinery out of production modes: principles and accidentology*, Proc. of the 6th Int. Conf. Safety of Industrial Automated System, Tampere, Finland, 2010.
2. Institut National de Recherche et de Sécurité, Sécurité des machines – Modes de fonctionnement protections neutralisées – INRS ED 6129, Paris, 2012.
3. European Committee for Standardisation, *ISO 12100:2010 - Safety of machinery - General principles for design - Risk assessment and risk reduction*, Brussels, 2010.
4. DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 May 2006 on machinery, Official Journal of the European Union, L157, 2006, pp. 24-86.
5. European Committee for Standardisation, *ISO 11161:2007 - Safety of machinery - Integrated manufacturing systems - Basic requirements*, Brussels, 2007.
6. Apfeld R., *Stop Defeating the Safeguards of Machines*, Proc. of the 6th Int. Conf. Safety of Industrial Automated System, Tampere, Finland, 2010.
7. European Committee for Standardisation, *ISO 13855:2010 - Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body*, Brussels, 2010.
8. European Committee for Standardisation, *ISO 13857:2008 - Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs*, Brussels, 2008.
9. European Committee for Standardisation, *EN 574:1996+A1:2008 - Safety of machinery - Two-hand control devices - Functional aspects - Principles for design*, Brussels, 1996.
10. Rothenburg J., *New machinery directive: operating with disabled protective devices, new chances and new specifications*, Proc. of the 6th Int. Conf. Safety of Industrial Automated System, Tampere, Finland, 2010.

Development of knowledge about the practice and the specificities of lockout in the municipalities in Quebec

Damien Burlet-Vienney

Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST)
505, boulevard de Maisonneuve Ouest, Montréal, QC, Canada, H3A 3C2

Tel. +1 514 288-1551 ext. 408, Fax +1 514 288-0998, E-mail dambur@irsst.qc.ca, <http://www.irsst.qc.ca>

Yuvlin Chinniah

Polytechnique Montreal, Department of Mathematics and Industrial Engineering
P.O Box. 6079, Station. Centre-ville, Montréal, QC, Canada, H3C 3A7

Tel. +1 514 340-4711 ext. 2268, Fax +1 514 340-4173, E-mail yuvlin.chinniah@polymtl.ca

Keywords: Lockout, municipality, procedure, machine

ABSTRACT

In Quebec, the mandatory method for controlling hazardous energy during maintenance, repair or unjamming works on machines is lockout in accordance with Article 185 of the Quebec's Occupational Health and Safety Regulation. Lockout procedures involve shutting down the equipment, isolating it, applying individual locks, applying tags, releasing residual energies, and verifying the absence of energies.

Despite this legal requirement, lockout doesn't seem to be implemented as much as it should be in the municipal sector in Quebec. Therefore, this study aims to analyse the organisation and the characteristics of lockout in the municipal sector in Quebec. To meet this objective, (i) accidents in the municipal sector related to the problem of hazardous energy control were identified and analyzed, (ii) a literature review on lockout in the municipal sector has been achieved, and (iii) 12 municipalities in Quebec and 23 municipal sites were visited with a questionnaire based on documents such as the Canadian standard CSA Z460-05 (2005). This study has led to results such as:

- The moving machinery used during winter activities (e.g., truck, spreader, grooming, etc.) is the main equipment involved in serious accidents linked with our subject.
- Seven potential areas for application of lockout in a municipality were identified: (i) water treatment plants, (ii) public works, (iii) workshops, (iv) public buildings, (v) public parks and green areas, (vi) waste treatment plants, and (vii) public transport network. Some of these areas are outside which is a feature of the municipal sector.
- The visits allowed to describe the practice of lockout for each type of site, and to notice that:
 - Implementation of lockout is beginning in many municipalities. Lockout program and/or procedures don't exist or aren't usable in 8 of 12 municipalities.
 - Municipalities have questions regarding resistance to change, use of external assistance, equipment inventory in all sites, harmonization of the coding facilities, and management of documentary system.
 - Structures of municipalities seem to create problems on the harmonization of practices between departments, localisation of lockout procedures, working alone, and working outdoors.
 - Little emphasis on lockout was put on moving machinery by the municipalities which tend to focus mainly on fixed equipment even if such equipment was involved in serious accidents.
 - Many types of equipment are remote controlled, especially in water treatment and ventilation systems, which is an incentive to apply lockout procedures.
 - Technical difficulties were encountered for the application of lockout on street valves.

These results on lockout should help municipalities to improve the application of lockout.

1 INTRODUCTION

Broadly, it is estimated that 10-15% of workplace fatalities and 15-20% of all accidents are related to maintenance [1]. In Quebec, the mandatory method for controlling hazardous energy during maintenance, repair or unjamming works on machines is lockout in accordance with Article 185 of the Quebec's Occupational Health and Safety Regulation [2]. Lockout procedures involve shutting down the equipment, isolating it, applying individual locks, applying tags, releasing residual energies, and verifying the absence of energies [3].

Unfortunately, in 2008, the Quebec's Occupational Health and Safety Commission (CSST) has revealed that 5225 accidents and 6 deaths occur annually during maintenance, repairs and installation of machines in Quebec due to the absence of, or errors in lockout procedures [4]. The municipal sector is also affected by this issue.

In Quebec, there are approximately one thousand municipalities and the municipal sector employs around 80 000 workers. Among these employees, many of them may be involved in lockout activities during installation, maintenance, repair, and unjamming of equipment. These include blue collar workers or subcontractors hired by municipalities. Despite this, lockout doesn't seem to be implemented as much as it should be in the municipal sector in Quebec. Thus, a study was carried out in order to analyze the organisation and the characteristics of lockout in the municipal sector in Quebec [5]. In this context, the objectives and the methodology implemented were:

- Identify accidents associated with the subject of study.
- Identify work activities and equipment involved in lockout in the municipal sector.
- Documenting practice and difficulties associated with its application in the municipal sector.

The following sections summarize results in relation to the previous three points.

2 SURVEY OF ACCIDENTS

A survey of accidents in the municipal sector in Quebec between 1985 and 2009 which were linked to the presence of hazardous energies was carried out by using the database of the CSST where investigation reports due to serious and fatal accidents are available. In addition, an exploration of the database of the French occupational health and safety institute (INRS) was carried out with the same criteria for the category *Local Government authorities and hospitals*.

Finally, fourteen serious workplace accidents were selected. The synthesis of these accidents reveals that:

- Accidents are related to interventions on machinery in operation, and not to uncontrolled release of energy.
- The moving machinery used during winter activities (e.g., truck, spreader, grooming, etc.) is the main equipment involved in serious accidents linked with our subject.
- Half of all accidents occur during outdoor activities.
- The four types of activity involved were cleaning, maintenance, unjamming and inspection. These operations were usually improvised by the worker since no energy control procedure seemed to be used.
- In half the cases, the worker was alone to do its job.

3 LOCATIONS AND EQUIPMENT

A literature review was done to identify documents where a complete or partial description of lockout in the municipal sector was provided. Documents which were targeted were standards, regulations, guides, scientific articles, training documentation, and labour laws for different trade associations. The research was conducted in 2010 by keywords (e.g. lockout, lockout program, municipality, city, etc.) on different databases including Compendex, Inspec, and ScienceDirect. Thus, an analysis of 26 references which described lockout procedures with reference to the municipal sector was carried out. The references were 14 guides, 8 leaflets, 1 book, 1 standard, 1 article and 1 video [6] [7] [8].

The principal themes which were covered by those references led to the identification of the different locations and departments concerned by lockout procedures in municipalities. Workers may intervene on equipment found indoors or outdoors and those interventions usually occur at the seven locations:

- water treatment plants,
- public works,

- workshops,
- public buildings,
- public parks and green areas,
- waste treatment plants, and
- public transport network.

The different equipment found in these locations can be grouped into: electrical installations, mobile machinery, fixed machinery, conduits and ventilation systems, and confined spaces.

4 IMPLEMENTATION OF LOCKOUT

During the study, 12 municipalities in Quebec were visited. Those visits were carried out mainly in large municipalities from September 2010 to April 2011. Eight regions in Quebec were included in this study. More precisely, 23 municipal sites were visited (e.g. water treatment plant, workshop, etc.). The selection criteria of these municipal organizations were municipality size, tasks performed, equipment used, and human resources available.

These visits were used to collect the lockout program of the municipality and to identify (i) the context and the application of lockout, and (ii) the specificities of the municipal sector regarding lockout activities.

Before the visits, a questionnaire and an observation checklist were developed based on an IRSST manual used for verifying the content of lockout programs [9]. The main topics covered in the questionnaire were on:

- lockout program,
- the application of lockout procedures at the site,
- roles and responsibilities,
- training on lockout,
- material for lockout,
- audit of lockout,
- external personnel and lockout, and
- difficulties experienced in the application of lockout

The questionnaire was filled by two members of the research team by asking questions to the OHS representative as well as the worker authorized to perform lockout. Afterwards, the two members of the research team confronted, compared and validated the data collected.

The visits revealed that the implementation of lockout is beginning in many municipalities. Lockout program and/or procedures don't exist or aren't usable in 8 of 12 municipalities. During these visits, the organizational and technical issues experienced by municipalities for the implementation of lockout have been identified. These include:

- Organizational issues :
 - Resistance to change: It is a known fact that the implementation of lockout programs leads to changes in the work methods. To manage this resistance, managers must involve internal resources in the project. Moreover, involvement of internal resources during the identification and codification of equipments allow them to gain a better understanding of the facilities and the benefits linked (e.g., facilitate troubleshooting, support to sub-contractors, etc.).
 - Equipment inventory in all sites, harmonization of the coding facilities: The inventory of equipment and isolating devices in all sites can be challenging due to their number and distribution, the lack of technical plans, and the constant evolution of the municipalities. In order to facilitate the codification, it seems be to interesting to harmonize all from the start in the different departments of the same municipality.
Moreover, structures of municipalities seem to create problems on the harmonization of practices between departments, localisation of lockout procedures, working alone, and working outdoors.
- Technical issues:
 - Moving machinery: Little emphasis on lockout was put on moving machinery by the municipalities which tend to focus mainly on fixed equipment even if such equipment was involved in serious accidents.
 - Remote control: In water treatment plants and pumping stations, valves and pumps are mainly remote controlled. Ventilation systems in buildings can also involved remote controlled equipment. The increased use of remote controlled equipment acts as an incentive to apply lockout procedures. Indeed,

- people involved must have a local control over the hazardous energy in order to prevent accidental starting.
- Street valves: Technical difficulties were encountered for the application of lockout on street valves. Currently, no efficient and effective device can lockout all of them due to varying diameters for the access conduits and ice in winter.

5 CONCLUSION

These results on lockout should help municipalities to improve the application of lockout. The CSA Z460-05 (2005) implementation model for lockout, which is pretty generic, can be adapted by municipalities by incorporating the specificities of the municipal sector identified in this study.

In addition, some elements deserve further analysis to improve the practice of lockout in the municipal sector. These elements include:

- lockout procedures for mobile equipment and portable tools,
- methods to lockout street valves, and
- evaluating the use of new technologies such as portable wireless tablet to access to records, barcode scanners.

6 REFERENCES

- [1] European Agency for Safety and Health at Work, *Maintenance and occupational safety and health: a statistical picture*, Publications Office of the European Union, Luxembourg, 2010.
- [2] Publications Quebec, *Regulation respecting occupational health and safety, c. S-2.1, s. 223*, Éditeur officiel du Québec, Quebec, 2012.
- [3] Canadian Standard Association, *Control of hazardous energy: Lockout and other methods (CSA Z460-05)*, The Association, Mississauga, 2005.
- [4] Commission de la Santé et de la sécurité du Québec, *La CSST invite les milieux de travail à cadenasser* [Internet], Commission de la santé et de la sécurité du Québec, Montreal, 2008. Available from http://www.csst.qc.ca/portail/fr/actualites/2008/29_septembre_cadenassage.htm
- [5] Chinniah, Y., Burlet-Vienney, D., Boivin, G., & Paques, J.-J., *Secteur des affaires municipales au Québec – Étude exploratoire du cadenassage (R-741)*, Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail, Montréal, 2012. Available from <http://www.irsst.qc.ca>
- [6] Yakemchuk, M.T., *Municipal safe work procedures: guideline manual*, Water and Wastewater Operators, Calgary, 1995.
- [7] Mulloy, K.B., Orris, P., & August, J., *Municipal workers*, Hanley & Belfus Inc., Philadelphia, 2001.
- [8] Ontario Forestry Safe Workplace Association, *Mobile machine lockout: safety meeting topics*, Ontario Forestry Safe Workplace Association, North Bay, 2004.
- [9] Burlet-Vienney, D., Jocelyn, S., Chinniah, Y., Daigle, R., & Massé, S., *Verifying the content of lockout programs (RF-635)*, Institut de Recherche Robert-Sauvé en Santé et en Sécurité du Travail, Montréal, 2010. Available from <http://www.irsst.qc.ca>

A study on Nullification of Safeguards for Industrial Machinery in Japan

Kohei Okabe, Hiroyasu Ikeda, Shigeo Umezaki

National Institute of Occupational Safety and Health, Japan (JNIOSH), 1-4-6, Umezono, Kiyose, Tokyo, Japan

E-mail okabe@s.jniosh.go.jp

KEY WORDS: Safe management, Nullification motive, Labor-saving, Tamper proof

ABSTRACT

This paper discusses safety design for preventing occupational hazards arising from the nullification of safeguards for industrial machinery. The reasons for disabling safeguards are classified from cases of industrial machine accidents. A viewpoint from labor-saving is adopted as classification index. Nullification motives are categorized into three types. Industrial machine issues that must be addressed are shown to differ with classes. Current safety design issues are discussed in terms of nullification motives. Safety design requirements to be considered are clarified.

1 INTRODUCTION

Occupational safety now arouses strong consciousness in society, but many occupational accidents still occur because workers disable protective devices or other safeguarding devices installed on machines. How the actions to disable the safeguards are viewed by those concerned may be deeply involved in this situation.

Excessive desire for productivity and disregard of safety are generally considered as motives for disabling safeguards. Intentional nullification of protective devices often contravene the appropriate use of machines. Accident causes are uniformly processed as safety rule violation or safety management deficiency. Specific motives and situations for disabling safeguards are not studied in detail or depth. Detailed accident analyses have not been reported in Japan.

Unless reasons of nullification are clarified, drastic safety design measures cannot be undertaken. The performance and usability of protective devices are not improved, and similar accidents are repeated. Discussion of disablements from the viewpoint of management and operation is not enough to prevent the recurrence of accidents.

This paper classifies and exemplifies motives for intentional disablements and studies specific measures for preventing the recurrence of accidents by focusing on safety design. Tamper-proof is overviewed as current countermeasure against nullification, and the effectiveness of tamper-proof is discussed.

2 ANALYSIS OF REASONS FOR DISABLING SAFEGUARDS

1) Analytical Method

Reasons for intentional disablements in industrial machines are extracted from occupational accidents in the manufacturing industry and classified into three types. The criteria for classifying the disabling reasons are presented and applied to fatal accidents whose details are reported. The characteristics of disabling reasons in specific classes are shown. The classes derived from the analysis of fatal accidents are applied to the analysis of frequent accidents involving specific machines.

2) Proposed Classification Criteria

To grasp the actual conditions and patterns of disablements, the disabling reasons (e.g., removal of fixed guards) were extracted from accident investigation reports on 129 fatal accidents with industrial machines in the manufacturing industry. Referring to nine identified disabling reasons, the following three classification criteria were proposed from the viewpoints of (1) necessity of work, (2) improvement of productivity, and (3) labor saving [1]:

- Implementation of maintenance
- Response to productivity
- Response to workability

Labor saving means man-hour reduction and equated with time and effort saving in this study. The difference between workability and productivity is whether or not the main objective is labor saving. Labor saving is one response to productivity but not to workability.

Workability improvement contributes to productivity improvement. The main purpose of workability improvement is to complete the specified task normally by spending time and effort, not to improve productivity by sparing time and effort. Maintenance has high necessity for disabling safeguards as work pattern and is essentially not intended to improve productivity.

3) Analytical Results

Nine identified machine types and other details, and classes are shown in Table 1. The following characteristics are recognized in the respective classes of disabling reasons:

(1) Implementation of maintenance. The safeguards were disabled to perform maintenance. The maintenance workers probably disabled the safeguards by themselves.

(2) Response to productivity. The safeguards were probably disabled to eliminate or simplify safety assurance-related tasks. Sparing of time and effort necessitated by the use of safeguards was considered to have caused the disablements. It is confirmed that the safeguards themselves did not obstruct the performance of work.

(3) Response to workability. The safeguards were disabled to prevent them from interfering with the ongoing work. Each work was within the range of proper machine usage. The safeguards were disabled before the accident occurred. The condition of work floor suggests that the accident victims did not disable the safeguards. The problem is not the safeguard nullification itself, but the risk of nullification that disablements were not announced, and they were left unprotected against. This kind of accident type is strongly correlated with the deficiency of machine maintenance management.

4) Discussion for the Classes.

Reducing unnecessary man-hours is an important activity. To improve the work process, it is indispensable to distinguish between steps that can be reduced and steps that must not be reduced. In response to productivity, the time and effort required for safety assurance are not spent. Here lies a safety management problem. In response to workability, on the other hand, the time and effort for safety requirement are expended. Against this background is the fact that machines are often used outside the range assumed by machine designers. Motives for disabling safeguards are presumed to derive from the conflict between design specifications and use requirements.

5) Case Study 1: Analysis of Reasons for Nullification in Press Machines

To add to analytical cases, press accidents were analyzed next. The analytical objects are 460 fatal accidents that occurred with friction clutch presses from 2003 to 2005 in Japan. The reasons for disabling safeguards are classified as well as above.

Table 1. Cases in which disabling reasons were identified.

Index	Machine	Safeguards	Disabling reason	Disabled by	Class
1	Wire drawing machine	Cover	Cover interfered with and obstructed work.	Machine manager	Workability
2	Mixing machine	Enclosure	Enclosure was removed to clean machine.	Victim	Maintenance-cleaning
3	Printing press A	Limit switch	Limit switch was disabled for single worker to operate machine.	Unknown	Productivity – labor saving
4	Printing press B	Limit switch	Limit switch was disabled to work while checking inside cover.	Unknown	Workability
5	Washing machine	Safety cover	Safety cover was left removed because it was heavy and difficult to remove as needed.	Machine manager	Productivity – trouble saving
6	Molding machine A	Safety door	Safety cover was removed because it hit workers nearby and was dangerous to them.	Machine manager	Workability
7	Molding machine B	Side cover	Side cover was left removed to change molds.	Maintenance worker	Productivity – trouble saving
8	Rolling machine	Safety fence	Safety fence was opened to adjust machine.	Victim	Maintenance - adjustment
9	Transfer machine	Safety fence	Safety fence was opened to check cause of machine failure.	Victim	Maintenance - repair

Among the cases of safeguards involved in the occurrence of accidents are 5 cases where the enclosures were deficient and 306 cases where the protective devices were deficient. These cases account for more than 60 percent of the total cases. There are many protective device-related deficiencies, but there are only 5 fatal accidents due to protective device failures. The disablement of safeguards was responsible for the following 60 cases, or nearly 20 percent of the total cases:

- Removal of enclosure: 2 cases
- Nonuse of protective device: 48 cases
 - Disablement of protective device for tool change: 13 cases
 - Disablement of protective device for trial hit: 9 cases
 - Failure to reset protective device after disablement: 26 cases
 - * Tool change: 13 cases
 - * Others: 13 cases
- Modification of protective device: 10 cases

The reasons for disabling the safeguards in these accident cases are classified further as shown in Table 2. Many safeguards were disabled to change tools or adjust tool positions. There were also many failures to reset the safeguards after disablement. The reason of reset failure is equally important to be analyzed. It is necessary to distinguish nullification motives: inattention, laziness, haste, etc. Tool change is classified here among maintenance tasks. Ordinary workers also change tools as part of regular work. This is one factor responsible for habitual nullification and must be improved. Characteristics of the reasons for disabling the safeguards are described below.

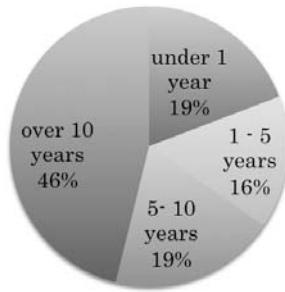
(1) Implementation of maintenance. The proportions of accident victims during tool change are classified by years of experience in Fig. 1. Workers with less than 1 year of experience are high in percentage. The fact that unskilled accident victims with one year of experience account for nearly 20 percent cannot be ignored. The ratio (Number of failure to reset/Number of not failure to reset) of unskilled victims is smallest as shown in Fig. 1-(b). Protective devices should be disabled by skilled workers with over 1 year of experience. Work tasks that occur frequently in the work process will become irregular, hazardous tasks when their protective devices are disabled. The work pattern where such tasks are assigned to less-experienced workers is taken as labor saving from the viewpoint of safety assurance. This is not a management problem that can be addressed by conducting safety education with ease.

Machines structures are also to blame. There were many cases where the protective devices could be easily disabled. Mechanism improvement is required. Especially, an interlock structure is not formed that controls the machine to stop or inching when the protective device is disabled. The cases where inching mode is activated are 8 or less than a half of the 26 cases. Establishment of a structure standard should be studied.

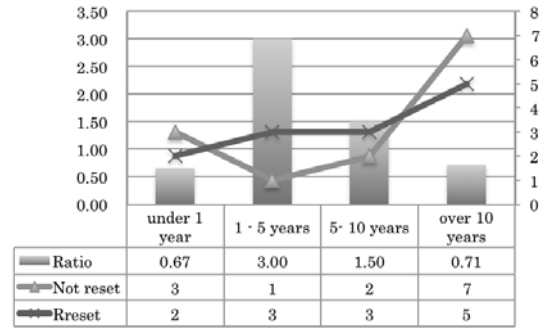
(2) Response to productivity. Concerning response to productivity, many two-hand protective devices were modified for one-hand operation at the sacrifice of safety assurance. These modifications were probably made to perform work by supporting the workpiece or slightly adjusting the position of the workpiece. The protective devices were disabled to allow two or more workers to perform a task difficult to do so alone. This is taken as labor saving.

Table 2. *Classes of disabling reasons for presses.*

Class	Total number of cases	Motive	Disabling reason	Number of cases
Maintenance	27	Adjustment	Tool change	13
			Failure to reset after tool change	13
		Education	Explanation of tool change	1
Productivity	8	Labor saving	Modification	7
		Trouble saving	Failure to reset	1
Workability	16	Work accomplishment	Trial hit	9
			Removal of enclosure	1
			Failure to reset	6
Miscellaneous	9			



(a) Total: 26 accidents



(b) Ratio of failure to reset protective device

Figure 1. Experience of victims in case of tool change accident

(3) Response to workability. Concerning response to workability, protective devices were often disabled temporarily because long workpieces or new type workpiece actuated the protective devices to no avail. The necessity for the disablement is evident from the purpose of work, but subsequent resetting is a problem. This is a typical example where the performance limitation of the protective device hinders workability.

It was confirmed that the worker who disabled the safeguard was an accident victim in some cases and was not an accident victim in other cases.

6) Case Study 2: Analysis of Reasons for Nullification in Food Processing Machines

To increase the number of cases by machine type, 200 accidents in food processing machines were analyzed. Food processing machines are available in various types and extensively used in the tertiary industry, and have many accidents.

The disablement of safeguards was confirmed in 4 of 25 fatal accidents and in 20 of 175 leave accidents. Disablement of safeguards accounts for 10 percent of total accidents in food machines. Further 22 accidents were ascribed to the disablements. Their classes are shown in Table 3. There are many cases in which the safeguards were disabled to remove residues and interlock structure were not formed. The lid of an agitating machine, for example, has a role of movable guard to protect the worker from hazardous parts rotating at high speed. Like the inching mode, the lid essentially requires an interlock structure that synchronizes with low-speed operation. This also applies to fixed guards. If the fixed guard is removed, frequently or not, it requires ingenuity to limit the operation of the machine.

Food machines should be structurally designed to clear the stop/brake condition only when the machine need be started. The characteristics of reasons for disabling safeguards in food machines are described below.

(1) Implementation of maintenance.

The safeguards were often disabled to clean the machines. Since its purpose is justifiable, this disablement is classified among the implementation of maintenance. Almost machines can be cleaned after stopping them. The safeguards were disabled without stopping the machines. This disablement for cleaning can be also taken as response to productivity. These cases could be prevented by use of interlocks.

Table 3. Classification of reasons for disabling safeguards in food machines.

Class	Total number of cases	Motive	Disabling reason	Number of cases
Maintenance	9	Cleaning	Cleaning	3
			Residue removal	2
		Adjustment		1
		Repair		1
Productivity	5	Trouble saving		5
Workability	5	Work accomplishment	Residue removal	4
			Cleaning	1
Miscellaneous	3	Machine trouble	Troubleshooting	3

(2) Response to productivity.

There are many cases in which the covers were opened during processing without stopping the machines. Since there was the need to open the cover, this nullification may be considered as response to workability. When disabling the safeguard, however, the machine was not stopped. This kind of nullification can be thus taken as trouble saving. Interlock devices could also prevent these cases. Workers who disabled the safeguards were accident victims in some cases and were no in other cases.

(3) Response to workability.

There are many cases in which the covers were opened to remove the residues. The machines had to be operated to remove the food residues. The victims themselves probably operated the machines. Using simply interlock devices to stop a machine cannot prevent this kind of accidents. Two-hand enabling devices or inch functions are required to prevent workers from easily operating machines in an unsafe condition. One-hand control devices are not sufficient and actually resulted in accidents. Ingenuity is desired to reduce the need for opening the lids and covers. It is extremely important to design for visibility so that the lids and covers do not conceal the residues.

3 CURRENT STATUS OF COUNTERMEASURES AGAINST NULLIFICATION

1) Interpretation of nullification.

Intentional modification and other disabling actions for protective devices that are recognized to be illegal are generically called tampering. Tampering generally refers to malicious, intentional actions and do not include unmalicious, faulty actions like human errors. Essentially, malicious, illegal actions alone should be taken as tampering, but the term “tampering” is not strictly defined yet, and whether or not action is tampering is not clearly distinguished. For this reason, intentional disabling actions tend to be interpreted as tampering. This paper limits tampering to intentional, illegal actions, restudies from a tampering point of view the three types of disablement classes presented in the previous chapter, and discusses general measures to prevent tampering.

2) Classification as tampering

To grasp the reasons for disabling the safeguards from the viewpoint of tampering, it is inappropriate to interpret as tampering the disabling actions during maintenance. Most of the actions taken to disable the safeguards meet the essential work objectives, are justifiable, and cannot be declared patently illegal. They must be clearly distinguished from tampering. Current measures against these disabling actions are mostly left to machine managers. Machine designers should also participate positively as part of performance of product liability.

Necessary motives can be discerned for the disabling actions as responses to productivity and workability, but these disabling actions are prohibited in proper use of machines and can be regarded as tampering. As for responses to workability, the following can be confirmed:

- Motives for disablement occur within the range of regular work.
- Machines must be operated by disabling safeguards.
- Accident victims may not be workers who disabled safeguards.

Disabling actions as responses to workability can be interpreted as tampering, but are different from responses to productivity and must not be treated equally as responses to productivity. Responses to workability leave enough room for machine design to make improvements on machines as products.

3) Effect of tamper-proof

Techniques and means against tampering are generally called tamper-proof or tamper-resistant. Double packaging to prevent the foreign matter contamination of drug product containers is a good example. These tamper-proof are distinguished from fool-proof measures, including measures against faulty actions. Methods of achieving tamper-proof can be distinguished as follows:

1. Disable (or potentialize) tampering.
2. Prevent tampering.
 - 2-1. Prevention: Make it more difficult to perform tampering.
 - 2-2. Uselessness: Render tampering unnecessary.

Disablement of tampering is prevention of the effect of tampering from appearing by some means when tampering is performed. In this paper, this is described as potentialization of actions.

Tamper-proof measures have long been introduced into industrial machines. In industrial machines, greater focus is placed on the prevention, rather than the potentialization of, tampering. Measures by potentialization of tampering have the possibility of being broken by further tampering and are not drastic measures.

This possibility is particularly high in responses to workability, and the effect of potentialization cannot be expected. In responses to workability, the motive for disabling safeguards is not labor saving but work performance. If tampering is potentialized, regular work cannot be performed sometimes. When some trial hits are restricted by protective devices of presses, for example, affected parts cannot be produced at all. Workers must continue to make changes until trial hits are feasible. This is also true of prevention of tampering. Worker must make changes until regular work becomes feasible, although it is difficult to perform tampering. In responses to workability, rendering tampering useless is only expected to be effective.

In responses to productivity, prevention of tampering is considered to be effective, depending on the ingenuity employed. The motive for disabling the safeguards in relation to productivity is labor saving. If tampering call for a considerable amount of labor, workers are more readily dissuaded from taking tampering. Tampering can be prevented by demanding workers of concomitant time and effort to do so. What is important here is that the time and effort required for tampering should be made clear to workers.

As an example, consider such an interlock structure that forces transition to the condition under which removal of a cover from a machine causes the affected circuit to self-destruct like a fuse and renders the machine totally useless unless the circuit is repaired. If the machine is not used, removal of the cover is not an unsafe action. The interlock structure is one kind of potentialization of tampering. If workers are not aware of this self-destruct mechanism, however, it does not prevent them from removing the cover. The self-destruct mechanism should be made known to workers in the form of instructions and signs so that workers must remove the cover at their own risk. The effect of prevention can be expected as a result.

4 CONCLUSIONS

This paper has classified and exemplified the reasons for intentionally disabling protective devices and other safeguards in industrial machines to promote the more appropriate operation of safeguarding devices. The disabling reasons have been divided and analyzed in three main types: implementation of maintenance, response to productivity, and response to workability. As a result, the following findings have been obtained.

- 1) In many of the cases where the safeguards were disabled for performing maintenance, some necessity and validity are evident in the disabling actions. It is not appropriate to take these disabling actions as tampering. Issues to be improved on the machine side were described.
- 2) Thoroughgoing adoption of an interlock structure is one measure for preventing accidents during maintenance. Interlocks are expected to help prevent accidents in many cases.
- 3) In many of the cases, the disabling actions as responses to productivity can be taken as tampering and cannot be prevented by interlocks alone.
- 4) To prevent accidents in responses to productivity, it is desired to ensure tamper-proof safety and improve tamper resistance. It also is judged necessary to increase penalty against inappropriate uses of the machine.
- 5) Many of the disabling actions in responses to workability are taken as tampering. Interlock structures and tamper-proof practices are not expected to be effective in preventing the recurrence of accidents in many of the cases studied.
- 6) As effective measures in responses to workability, it is necessary to increase usability of the machine by improving the machine in many of the cases studied. It is desirable to reconsider safety design on the basis of the actual uses of the machine.

REFERENCES

- [1] K. Okabe and S. Umezaki: A system design based on safety benefit of affording inconvenience affairs, Proc. of SICE 2010.

PRESENT SITUATIONS OF RECENT SURGE OF COUNTERFEIT ELECTRIC CONTROL EQUIPMENT AND THREATENED INDUSTRIAL SAFETY OF AUTOMATED MACHINERY SYSTEMS USING THOSE PRODUCTS

Koji Sagawa, Yasushi Nishioka, Toshiyuki Kasama,

Makoto Okuda, Toshiya Matsufusa,

Nippon Electric Control Equipment Industries Association (NECA),

2-1-17, Hamamatsucho, Minato-ku, Tokyo, 105-0013, Japan

Tel:+81 (0)3 3437 5727, Fax:+81 (0)3 3437 5904,

E-mail: sagawa.koji@jp.panasonic.com, <http://www.neca.or.jp/>

KEY WORDS: counterfeit, counterfeit judgment, social safety, B to B , cooperation

ABSTRACT

With the promotion of economical globalization and technology innovation, counterfeits of Japanese product as well as European's are prevailing mainly over Asian countries. It is said that the total amount of damages comes up to 80 trillion yen. Propagation of counterfeit products could be a cause of the risk to threaten the safety of the social system and health as well as profit loss of companies. To effectively cope with intricate tricks in growing worldwide importance of measures for intellectual property infringement, it is necessary to take strong measures through cooperation among major countries.

Electric control equipment industry is the one supporting other industries such as automobile, semiconductor, robot, etc. Measures for intellectual property infringement are the urgent theme related to safety in manufacturing sites and of users, as well as quality and reliability of products.

As an example of counterfeit problems, following scenario is considered:

A counterfeit emergency stop switch integrated in a unit could be a serious safety problem threatening human lives. This report discusses examples of counterfeit industrial products exposed by member companies and their initiatives for preventing counterfeits.

1. INTRODUCTION

For electric control equipment industry, measures for counterfeit products are important themes for safety in manufacturing sites and of users, as well as quality and reliability of products.

In an example of counterfeit problem in B to B (Business to Business) product, if an emergency stop switch integrated into a unit, shown in Figure 1, is counterfeit and doesn't correctly function because of its low quality, this could lead to a serious safety problem threatening human lives since it doesn't stop where it should do. In the same way, a pressure sensor could lead to a serious accident including explosion if it cannot measure a correct pressure. This time, we discuss examples of counterfeit industrial products(Refer to Figure 2) for ours and initiatives for preventing counterfeits based on consideration of influence on automated machinery systems with industry products.



Figure 1. Emergency stop switch

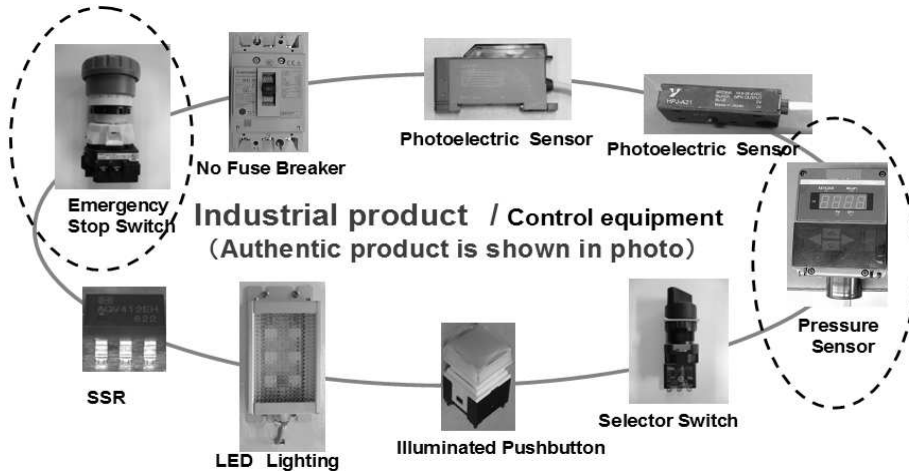


Figure 2. Example of counterfeit product in industrial product

2. RECOGNITION OF CURRENT SITUATIONS AND THEIR THEMES

2.1 Research on recognition of current situations

To identify themes in measures against counterfeits and take those measures, a research on our member companies' recognition of current situations was conducted in 2004 and 2011. Particularly, damages by counterfeits of industrial control equipment have been expanded in China. Refer to Figure 3.

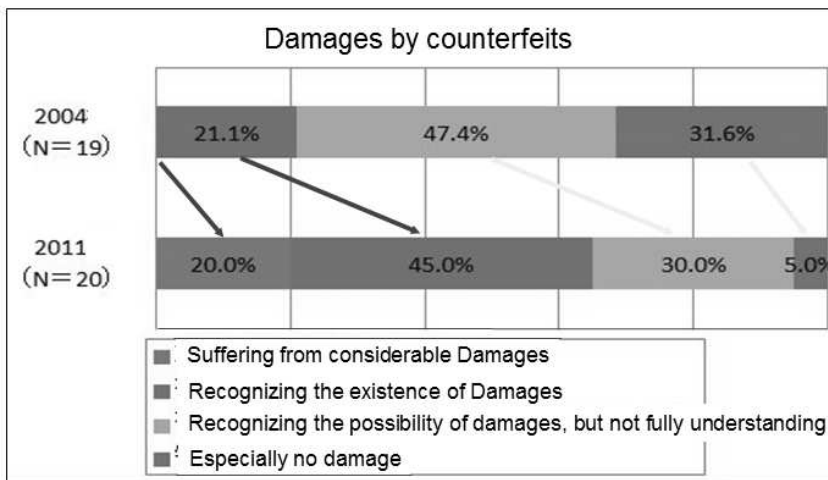


Figure 3. Damages by counterfeits

The result is summarized as following:

- Importance of business activities in China is increasing.
- Only half the member companies or less have sections for measure against counterfeits.
- Damages by counterfeits are certainly increasing
- Half the member companies take measures against counterfeits, but feel difficulty in confirming the effect.
- Half the member companies are at a loss for measures against counterfeit manufacturers by lack of information.
- Desire to know concrete routes for implementing measures.

That is to say, we recognized that each company has a limitation in conducting measures against counterfeits by itself, and many ones have an opinion that it is important to cooperate with related organizations.

2.2 Examples of damages by counterfeit products to date and their features

Features of counterfeits found so far are listed below:

- Imitation level varies from those with elaborate exterior which cannot be distinguished from authentic products to poor-quality ones which can be easily recognized as counterfeit.
- Performances (qualities) are lower than authentic products although exterior is elaborate.
- Many of them are 50 percent cheaper or less than authentic products.
- Most popular ones are dead copies with same design, structure and trade mark.
- Part of them has only same design and structure with trademarks of counterfeit companies.
- Hybrid-type examples are found with structure and design of company A and with trademark of company B.

As described in 1. INTRODUCTION, most of those products is categorized in B to B (Business to Business). Features of counterfeits in this business type are as follows:

1. In the case of uncertain purchase routes, it becomes much difficult to find counterfeits. Even though they were found, a company's products have been delivered for the research as final ones. It is usually difficult to make inquiries on purchasing routes with manufacturers of assembled products, as they are related to their management strategies.

(For identifying purchase routes, selection of distributors and intermediary seller is an important factor.)

2. Since many consumers purchase a product without thinking it is counterfeit, company's brand value decreases and its image is damaged if it is a counterfeit with poor quality and short life.

In the case of B to C products, some consumers will buy them although they know they are counterfeits.

3. Scale of B to B is considered to be far larger than that of B to C, since B to C is finally the only one in typical supply chain.

(Example: Only one time in case of final products are sold to final consumers)

However, as a matter of course, many B to Bs exist where parts and raw materials are processed for final products.

(Example: Parts are manufactured using various materials, and they are assembled for final products in turn.)

That is to say, in this type of business, it is difficult to understand how many counterfeit products are on the market and how much damage is generated through it.

2.3 Themes

Considering from companies' recognition of current situations and features of cases of damages by counterfeits mentioned above, following themes are considered:

- No clear ideas for taking measures against counterfeits
- Difficult to distinguish authentic products from counterfeits as an immediate judgment is impossible
- No idea for initiatives in the situation where supply chain becomes complicated with globalization of business and supplier are diversified

Measures against counterfeits in line with those themes are introduced below:

3. MEASURES AGAINST COUNTERFEITS

3.1 Guideline for measures against counterfeits

For companies which have been behind with activities for measures against counterfeits, being at a loss for coping with those problems, "Guideline for measures against counterfeits" is under developed. In this guideline, general measures against counterfeits are readjusted by items, time for measures, measures, purpose, themes in implementing measures and cases, as shown in Table 1.

Period of measures	Measures	Purposes	Themes in implementing measures	Cases
Before the fact - Before on the market - Before counterfeits generated	Acquisition of intellectual property right	Restraining counterfeit manufacturers Preventing generation of counterfeits Exposing counterfeits	Cost Limitation to exposing based on intellectual property right	① ⑦
	Use of counterfeit-preventing technologies such as using black boxes and encoding	Preventing generation of counterfeits	Cost More Specialized and elaborate counterfeits Improvement in use of black box and encoding	
	Use of attesting system (Testifying the fact that the right was applied before being done by others)	Avoiding risks by illegal application	Cost	
	Custom registration	Preventing distribution of counterfeits Ban on importing counterfeits Exposing counterfeits	Import in the form other than control unit itself (In the form of being integrated into a machine)	
	Research (Market, exhibition or official gazette)	Finding out counterfeits	Improvement of researcher' s skill and human resources development	①,② ⑤,⑥ ⑦
	Cooperative activities with industry groups	Finding out counterfeits	Continuously maintaining information sharing system	
	Declaration of taking measures against counterfeits	Restraining counterfeit manufacturers Preventing generation of counterfeits	Cost	
After the fact - After counterfeits generated	Calling for attention through web site	Avoiding risks by poor quality of counterfeits	Promoting awareness of other than web site visitors Counterfeit judgment	
	Provision of information on counterfeits to users	Avoiding risks by poor quality of counterfeits	Promoting awareness of other than existing users Counterfeit judgment	
	Exposing distributors	Seizing counterfeits and punishing	Selection of relevant organizations Recurrence prevention Cost	①,② ⑤,⑥ ⑦
	Exposing manufacturers	Seizing counterfeits and punishing	Selection of relevant organizations Recurrence prevention Cost	①,② ③,④ ⑥,⑦
	Exposing on-site at exhibitions	Seizing counterfeits and punishing	Selection of relevant organizations Recurrence prevention Cost	
	Warning	Orders to suspend manufacturing and marketing counterfeits	No legal bidding force	

Table 1. General measures against counterfeits

3.2 Techniques for counterfeit judgment

In exposing counterfeit products, it is necessary to catch the manufacturer along with products at the manufacturing site.

To perform this, it is important to have techniques (techniques for counterfeit judgment) to distinguish between authentic products and counterfeit ones.

In these cases, for preventing counterfeits, it is indispensable that counterfeit judgment on products is available “at sites” such as shops, manufacturing works or custom houses in exporting or importing them.

In the case of industrial products, different from other brand products, many ones are small without spaces for attaching or printing barcode seals and their prices are cheaper.

Therefore, in many cases, there are limitations in costs for preventing counterfeits.

Important requirements for techniques for counterfeit judgment are as follows:

- 1 Counterfeit judgment is allowed at individual sites
- 2 Low cost
- 3 Difficult for counterfeit manufacturers to imitate

Introduced below as an example is identification without needs for affixing seals and printing:

It is the identification method using “Wave Length Division Coding Technology”. This technology is not established so far. This fluorescent substance is the one which glows when the specific excitation ray is irradiated. Same substance can generate rays with various wavelength by changing particle diameter or composition ratio. Leveraging those features, generally invisible “codes” can be attached on units when existence of irradiation at each wavelength is treated as digital signals. In other words, this means that the identification method has changed from visible and physical processing type to stealth one.

(Refer to Figure 4 e.g. [3])

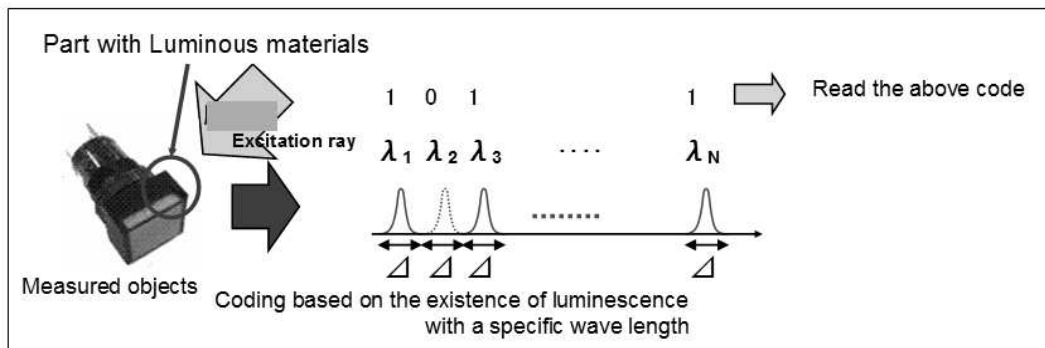


Figure 4. Identification method using “Wave Length Division Coding Technology”

3.3 Initiatives for business globalization

Business globalization has brought more complicated supply chain. In addition, suppliers have become diversified. In those situations, how we should cope with measures against counterfeits? We thought it is important to establish strategic collaboration through international cooperation. Consequently, considering the increasing importance of measures against counterfeits, EUIJ Kansai and EUSI Tokyo jointly held a symposium “European-Japanese strategic collaboration toward settlement of counterfeit problems” on February 7 and 9, 2012 inviting many participants (116 from Osaka and 160 from Tokyo).

Participants had lectures on introduction of successful cases of exposing counterfeit manufacturers from an EU company; initiatives of Japanese government including latest information on international negotiations, content of consulting services, etc. from the Ministry of Economy, Trade and Industry (Office for Intellectual Property Right Infringement) ; and cases of exposing counterfeits of control equipment and initiatives for measures for preventing counterfeits from us.

The symposium contributed for reinforcing the cooperation between Europe and Japan in the future.

Note) EUIJ(EU Institute in Japan) kansai and EUSI(EU Studies Institute) Tokyo:

These organizations are contributing to strengthen relationships between EU and Japan through promotion of publicity activities and information transmission, in order to strengthen cooperation with industrial sector as well as promote education and academic study on EU (European Union) .

4. SUMMARY (Direction in the future)

In order to improve measures previously described for making them more helpful, we will conduct hearing on the guideline for measures against counterfeits with our relative companies and continue updating the table of measures for further integrity of them. Needless to say, we will improve the level of counterfeit judgment as well as be involved in collecting information on systems practically with easy use. Meanwhile, we will promote public awareness of the importance of cooperation beyond nations.

We consider, further effectiveness of those measures will contribute to the social safety through correct operation of automatic machine system with our industrial products being integrated.

5. REFERENCE

- 1.NECA, Guideline for measures against counterfeits,2012 (in Japanese)
- 2.Nikkei Business Publications,Inc. ,*Nikkei Monozukuri*, April 2012 (in Japanese)
- 3.NECA, "*Strategy for International Standardization* "report for Ministry of Economy, Trade and Industry ,2011 (in Japanese)

“SAFETY EVALUATION OF DC POWER SUPPLY DEVICES, A FUNDAMENTAL FACTOR OF THE SMART CITY.”

*Koji Sagawa¹, Koichiro Sawa², Kazutomo Oishi¹,
Eiji Matuyama¹, Masatoshi Turuoka¹*

¹Nippon Electric Control Equipment Industries Association (NECA),

2-1-17, Hamamatsucho, Minato-ku, Tokyo, 105-0013, Japan

Tel: +81 (0)3 3437 5727, Fax: +81 (0)3 3437 5904,

E-mail: sagawa.koji@jp.panasonic.com, <http://www.neca.or.jp/>

²Keio University,3-14-1,Hiyoshi,Kouhoku-ku,Yokohama,Kanagawa, 223-8522, Japan

Tel:+81 (0)45 563 1141, sawa@sd.keio.ac.jp

KEY WORDS: direct current, smart city, control equipment, arc , international standardization

ABSTRACT

Toward realization of environment-conscious society (Low-carbon society), it is strongly encouraged to establish a direct current method using technologies including solar power generation. Many IT devices are operated on direct current. Further, components in a device are operated on DC, since inverter method is adopted for current air conditioners and refrigerators in many cases.

Conversion from AC to DC for input (voltage) to those devices leads to the reduction of CO₂, decreasing frequencies of converting from AC to DC.

Also in Japanese industries, data centers tend to adopt direct current method before others. We assume an input voltage around 400V (5A) as a required standard for switches.

We planned to launch to develop standards for safety of control equipment corresponding to around 400V, to meet the trend of increasing interests in recent direct current method. In October, 2010, it applied for the International Joint Study Project 2011 under the theme of "Standardization of control equipment for safety in direct current power supply method", in the field of "Standardization of technologies, mechanisms and maintenance for safety in creative design and manufacturing in industrial automation", and adopted in May, 2011. It aims at developing a proposal for international standards within three years from 2011 to 2013.

1. INTRODUCTION

Many IT devices are operated on direct current and components in a device are operated on DC, since inverter method is adopted for recent air conditioners and refrigerators in many cases. However, alternative current is a mainstream for input to devices. Energy loss generated by this AC/DC conversion has been a theme.

By changing these input method from AC to DC, frequencies of conversion from AC to DC decrease, leading to energy saving and the reduction of CO₂. Consequently, DC power supply method is inclined to increase.

Meanwhile, recent renewable energies (Solar power, wind-power and geothermal power generations) are direct current. It is highly possible that DC power supply will largely increase in the future.

In the mean time, safety standards, test method, etc. are specified in the international standards on the assumption that alternative current is used. Therefore, it is necessary to develop new standards for responding to the increase of , in order to safely use control equipment and control systems in dispensable for DC power supply with a symptom for rapid dissemination.

Therefore, we will develop a proposal for standards, "General requirements for DC power supply method", added to the standard, "IEC61058-1 Switches for appliances". After discussions with the domestic committee, we will assess the safety with devices of switches for appliances through promoting standardization, making proposal to the domestic committee for IEC/TC23/SCJ (Switches for appliances).

The content of our study is described below:

First it begins with "What is DC power supply?".

2. WHAT IS DC POWER SUPPLY?

DC power supply uses direct current (DC) in stead of alternative current (AC) generally used for supplying power to power sources of products. They are classified as follows according to sites they are used:

1. Method where power is transmitted in direct current within a region and optimized (Smart-grid concept)
2. Method where power is distributed in direct current within houses and works, and the power supply is optimized

In both cases, direct current is initially required to coexist with alternative current.

Attention has been shifted from the method of one-way power supply system from existing power plants to smart grid, which recognizes real-time power demand, using IT technologies, to supply power.

In this method, DC power supply with an easy link with renewable energies has become a topic. Refer to Figure 1. Also in DC power supply for household, the AC/DC hybrid wiring system, as shown in Figure 2, is proposed

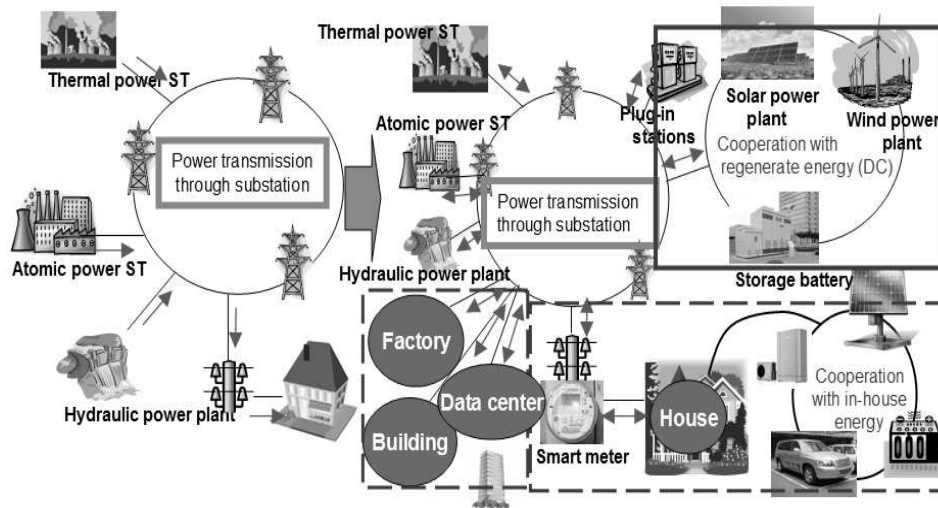


Figure 1. direct current within a region

Note) Smart-grid means a smart power network which connects power companies of existing supply side and houses and works of existing demand side, with IT network in addition to power network. This method allows end-to-end communications through not one-way but interactive information exchange to optimize power demand supply balance.

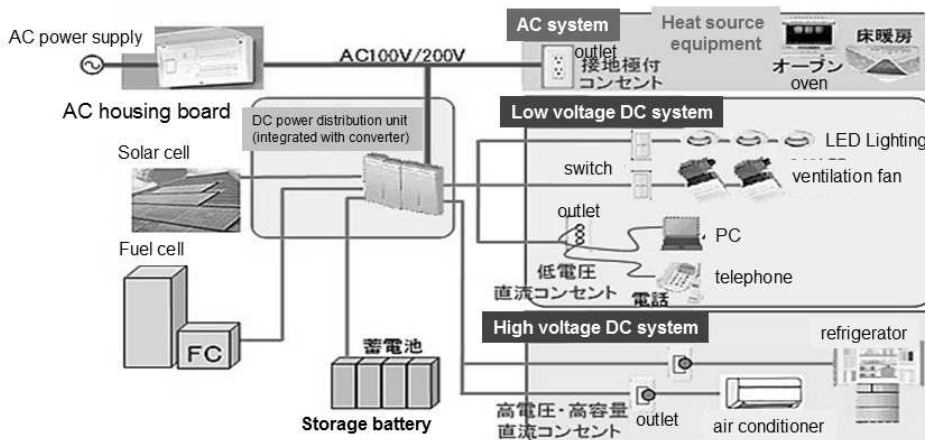


Figure 2. direct current within houses

Both cases are indispensable for effective development and operation of infrastructures such as energy, sewerage and traffic systems with a full use of IT (Information technology).

In this context, as shown in Figure 3 e.g[2], four hundred or more Smart City concepts are developed in the world, and the total scale of projects for 2030 is said to reach four quadrillion yen.

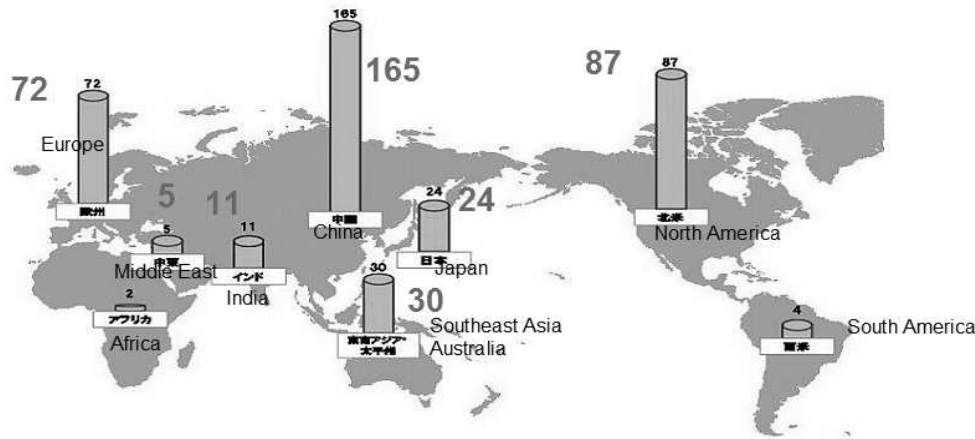


Figure 3. Smart City Project

3. BACKGROUND OF ATTENTION FOR DC SUPPLY

Why DC power supply has been paid attentions? The background is discussed below using an example of data centers:

Power is supplied to the power source of AC commercial power source at the entrance of a building from a power station via substations. In this case, conversion loss is decreased through conversion to direct current, direct supply of DC power to devices and decrease of conversion frequencies. This concept is considered to expand not only to data centers but general buildings and works. The trend for reduction of CO₂ emission will accelerate this tendency in the industrial sector and commercial building.

Thus, if power is converted to direct current at entrances of buildings and works, devices inside are operated in DC supply areas even though existing infrastructures for AC power supply are used. Naturally, control equipment used there is required to apply to direct current method in a safe manner.

The merit of DC power supply is shown in Figure 4.

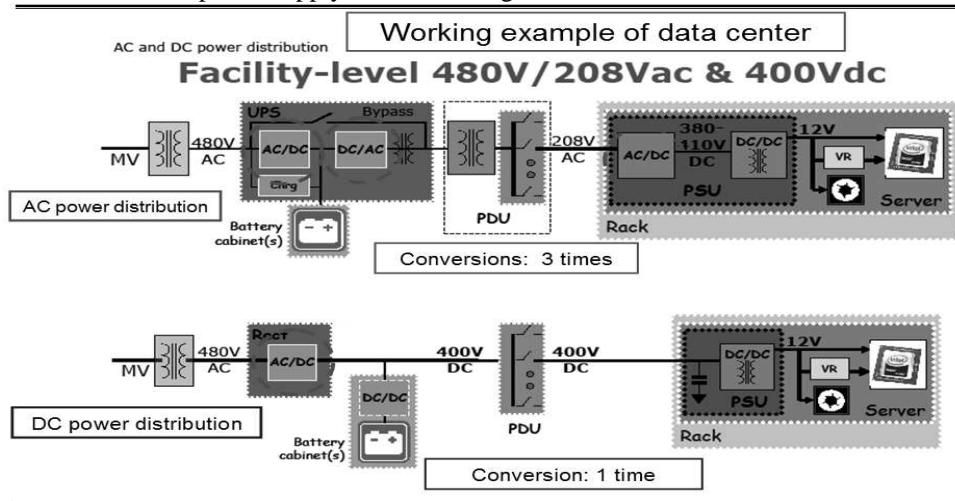


Figure 4. The merit of DC power supply

Further, there is currently a movement for DC power supply in limited areas specified. Renewable energies including solar power are directly supplied on DC in those limited areas. Actually, demonstration tests are conducted as that for micro-grid (Area DC power supply) in Akita prefecture,

Japan. The system is easily linked with the smart-grid previously mentioned, and contributes to the reduction of CO₂ emission by stable power supply and improvement of supply efficiency.

In around the lower right of Fig. 1, the possibility for DC power supply is to expand even in household even though power sources are these for AC commercial use. Here, an AC/DC hybrid system is proposed since AC and DC are commonly used. DC devices are considered to be adopted also in household in the future, even though it will take a certain time.

That is to say, as the strongest measure for reducing household CO₂ emission, needs for those energy saving houses will increase especially in case of building new houses. In addition, battery charge for EVs is also done on direct current. Currently, battery is charged after AC/DC conversion. However, method of direct DC charge is more efficient, time saving and energy saving.

Based on the above background, is existing control equipment safely operated in the case that DC power supply is disseminated in the future? Will the content of existing domestic standards be appropriate? It is currently necessary to define the above themes to propose solutions for them.

4. SAFETY THEMES CONSIDERED IN CONTROL EQUIPMENT

Safety themes for devices on adopting DC power supply include those of standardization and in addition to technological ones.

1. Technological themes
 - Protection technologies including overcurrent breaker (securing safety)
 - Grounding technologies, noise and measures for EMC(Electro-Magnetic Compatibility)
 - Safe plugs and socket outlets
2. Development of standards and legal system (for items listed below)
 - Standardization of power supply voltage, method, etc.
 - Securing safety such as protecting human body, devices, etc.
 - Establishment of methods for design, construction and maintenance

In the case of high-voltage direct current, arc (spark) often continues when switches are opened. So to speak, risks of fire and electric shock increase. Refer to Figure 5.

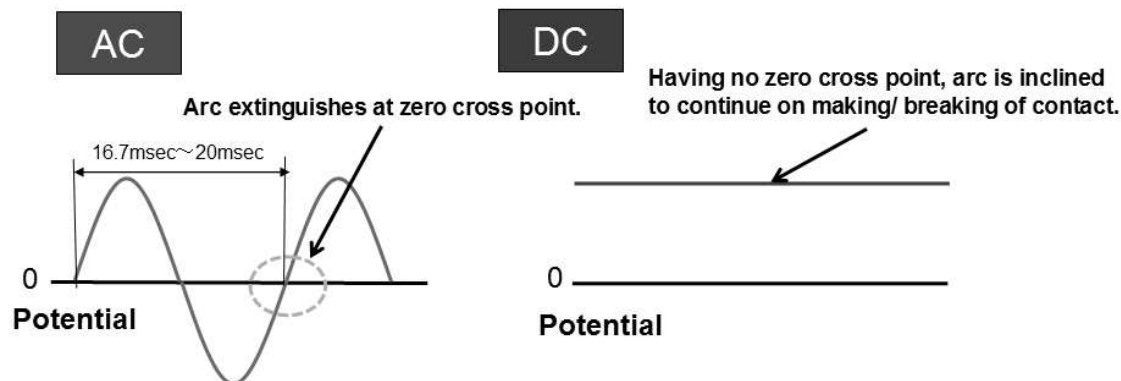


Figure 5. Technological theme (Arc)

Actually, existing standards are established on the assumption of AC power source. Therefore, in order to secure the safety required for control equipment for high-voltage DC power supply method with around DC400V, it is deadily needed to standardize standard test which allows safety use direct current as well, in addition to solve safety problems. This topic is discussed in the next paragraph.

5. SAFETY EVALUATION ON DEVICES FOR DC POWER SUPPLY (SWITCHES FOR APPLIANCES)

In Japanese and American industries, data centers tend to adopt direct current method before others. Servers operated on around 400V have begun to appear on the market. We also assume an input voltage around 400V (5A) as a required standard for switches.

A theme in current international standards for switches for appliances is that test methods and evaluation criteria are specified based on the use of general alternate power source (AC600V or less). Therefore, it is considered that they include items not able to satisfy safety requirements for DC power supply method with DC300 to DC400V which will be disseminated in the future.

For example, also in judgment criteria for electrical endurance test, judgment criteria for accepted and not accepted is not well defined seeing only from IEC standards. Therefore other standards must be referred for actual use. Refer to "Study on evaluation criteria in DC circuit break" shown below.

[Investigation on evaluation criteria in DC switching]

[Outline]

For studying criteria in DC circuit break, factual investigation (questionnaire) was implemented on criteria which current manufacturers adopt.

[Content of questionnaire]

We implemented the investigation focusing items shown below, regarding products concerned in each manufacturer, under the framework of our machinery products classification.

- Standards for applying test
- Judgment criteria for electrical durability test
-

[Result of questionnaire]

Standards which tests were applied

- NECA C 4520 6.10.2 (former JIS C 4520 6.10.2)
- NECA C 4005 8.2.8
- UL 1054 17
- IEC/EN61058-1 (JIS C 4526-1 17.2)

That is to say, there are emerging necessity to solve problems in safety evaluation on machinery switched as listed below.

1. Themes in standardization
 - ◇ Arc duration in switching test in direct current
 - Relations between GAP length between contacts and arc duration
 - Definition of judgment criteria (duration)
 - ◇ Prevention of electric shock and damages
2. THEME FOR CONTROL EQUIPMENT (SWITCHES)
 - ◇ Study on measures effective for breaking arc (use of magnets with action for extinction of arc)
 - ◇ Study on structures not allowing arc to leak out
 - ◇ Study on prevention of contact deterioration by arc

6. CONCLUSION

Settlement of these problems relative to safety evaluation for machinery switches leads to the safe use of devices in the direct current power supply method which are considered to be disseminated in forthcoming era of smart city, and to the development of environment for their safe use, as well as to contribution to the realization of low carbon society.

Therefore, This will be an important theme to be continuously involved.

7. REFERENCE

1. NECA, "Standardization of control equipment for safety in direct current power supply method"

report for Ministry of Economy, Trade and Industry ,2011 (in Japanese)
2.Nikkei Business Publications,Inc. , *Smart Energy 4* ,2011 (in Japanese)

SIAS
2012

THE 7TH INTERNATIONAL
CONFERENCE ON THE SAFETY
OF INDUSTRIAL
AUTOMATED SYSTEMS



MERCI À NOS COMMANDITAIRES / THANKS TO OUR SPONSORS:



UNIVERSITÉ DE
SHERBROOKE

