

**Modernisation des parachutes
de transporteurs de mines**
Volet 3 – Perte de contrôle de la cage

Laurent Giraud, ing.
Bertrand Galy, ing.

RAPPORT D'EXPERTISE
DIFFUSION PUBLIQUE

QR-1158-fr



NOS RECHERCHES travaillent pour vous !

Solidement implanté au Québec depuis 1980, l'Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST) est un organisme de recherche scientifique reconnu internationalement pour la qualité de ses travaux.

Mission

Dans l'esprit de la Loi sur la santé et la sécurité du travail (LSST) et de la Loi sur les accidents du travail et les maladies professionnelles (LATMP), la mission de l'IRSST est de :

Contribuer à la santé et à la sécurité des travailleuses et travailleurs par la recherche, l'expertise de ses laboratoires, ainsi que la diffusion et le transfert des connaissances, et ce, dans une perspective de prévention et de retour durables au travail.

Pour en savoir plus

Visitez notre site Web ! Vous y trouverez une information complète et à jour.
De plus, toutes les publications éditées par l'IRSST peuvent être téléchargées gratuitement.
www.irsst.qc.ca

Pour connaître l'actualité de la recherche menée ou financée par l'IRSST, abonnez-vous gratuitement :

- au magazine *Prévention au travail*, publié conjointement par l'Institut et la CNESST (preventionautravail.com)
- au bulletin électronique [InfoIRSST](#)

Dépôt légal

Bibliothèque et Archives nationales du Québec, 2022
ISBN 978-2-89797-205-9 (PDF)

© Institut de recherche Robert-Sauvé en santé et en sécurité du travail, 2022

IRSST - Direction des communications, de la veille et de la mobilisation des connaissances
505, boul. De Maisonneuve Ouest
Montréal (Québec) H3A 3C2
Téléphone : 514 288-1551
publications@irsst.qc.ca
www.irsst.qc.ca

Modernisation des parachutes de transporteurs de mines

Volet 3 – Perte de contrôle de la cage

Laurent Giraud, ing., Bertrand Galy, ing.

IRSST

RAPPORT D'EXPERTISE
DIFFUSION PUBLIQUE

QR-1158-fr



Avis de non-responsabilité

L'IRSST ne donne aucune garantie relative à l'exactitude, la fiabilité ou le caractère exhaustif de l'information contenue dans ce document.

En aucun cas l'IRSST ne saurait être tenu responsable pour tout dommage corporel, moral ou matériel résultant de l'utilisation de cette information.

Notez que les contenus des documents sont protégés par les législations canadiennes applicables en matière de propriété intellectuelle.

Cette publication est disponible en version PDF sur le site Web de l'IRSST.



NOTE AU LECTEUR

Cette étude a été financée par l'IRSST.

Les conclusions et recommandations sont celles des auteurs.

Les résultats des travaux publiés dans ce document n'ont pas fait l'objet d'une évaluation par les pairs.

AVIS DE NON-RESPONSABILITÉ

L'IRSST ne donne aucune garantie relative à l'exactitude, la fiabilité ou le caractère exhaustif de l'information contenue dans ce document. En aucun cas l'IRSST ne saurait être tenu responsable pour tout dommage corporel, moral ou matériel résultant de l'utilisation de cette information.

Notez que les contenus des documents sont protégés par les législations canadiennes applicables en matière de propriété intellectuelle.

Cette expertise a été financée par l'IRSST. Les conclusions et recommandations sont celles des auteurs.

Mise en garde

Cette étude a été réalisée en 2014, il est possible que certains liens et sites Web mentionnés ne soient plus fonctionnels.

REMERCIEMENTS

La préparation de ce rapport a demandé la consultation de nombreuses références et la rencontre de plusieurs personnes que nous tenons à remercier.

Les inspecteurs et professionnels de la CNESST et de CanMet pour leur disponibilité, leur implication dans cette expertise et la volonté de partager leur expérience.

Les inspecteurs miniers spécialisés du Yukon pour les précisions apportées sur les réglementations minières en vigueur dans leur province.

Le personnel du centre de documentation de la CNESST et du centre de documentation de l'IRSST pour la recherche bibliographique, et l'aide fournie dans la localisation et l'obtention de certains documents (dont un rapport de 1947).

Le personnel des mines pour leur accueil lors de nos visites en février, avril et septembre 2014.

SOMMAIRE EXÉCUTIF

Cette étude a été initiée par une lettre datée du 25 octobre 2013 et signée par un membre de la partie syndicale du sous-comité sur les machines d'extraction de la Commission de la santé et de la sécurité du travail (CSST)¹, demandant au sous-comité de mandater l'Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST) pour évaluer les systèmes d'arrêt d'urgence des transporteurs de mine en usage à travers le monde (parachutes et autres systèmes), dans le but de moderniser les parachutes exigés sur les transporteurs de mine au Québec. Un premier volet, déposé le 5 juin 2014², a présenté une revue de la littérature générale sur les parachutes et les câbles d'extraction. Un deuxième volet, portant sur les solutions envisageables afin d'éviter la rupture du câble et l'écrasement de la cage consécutive à cette rupture, a été présenté au sous-comité en septembre 2014 et déposé en septembre 2015³. Ce troisième et dernier volet s'intéresse au cas de perte de contrôle du déplacement de la cage pouvant causer son écrasement, et plus précisément à la fiabilité des systèmes de commande et des systèmes instrumentés de sécurité. Sa structure s'appuie sur le concept de couches de protection.

Le deuxième chapitre présente les méthodes d'analyse de performance des moyens de prévention et de protection. En effet, ces méthodes d'analyse sont répandues dans le milieu de la sécurité des machines, mais n'ont été introduites que récemment pour le milieu minier aux États-Unis. La réflexion sur la sécurité du système doit être globale et initiée dès la conception. La défense en profondeur est une première méthode de protection : plusieurs couches imbriquées les unes dans les autres sont responsables de maintenir la sécurité du système, en cas de défaillance d'une couche, la couche suivante est censée contenir le problème. Les barrières de sécurité, aussi appelées mesures de maîtrise des risques, peuvent être techniques ou humaines ou les deux à la fois, et servent à remplir des fonctions de sécurité. La méthode LOPA (*Layer of Protection Analysis*) est une méthode d'analyse des risques qui s'appuie sur le concept de défense en profondeur (couches de protection) et intègre également la notion de barrières de sécurité. Cette méthode issue de l'industrie chimique peut néanmoins être étendue à tous les domaines industriels ayant une composante de sécurité. Il est possible de rajouter un critère d'indépendance des couches de protection afin d'éviter les défaillances de cause communes ou les défaillances de mode commun. Les concepts généraux présentés dans le chapitre 2 sont utilisés pour les chapitres suivants, qui détaillent les moyens de maîtrise des risques couche par couche.

La couche de protection 3 « alarmes et intervention humaine » est présentée au troisième chapitre. Parmi les alarmes et interventions humaines, on peut recenser les moyens de monitoring de la cage (emplacement, vitesse, direction, charge, accélération...). Les systèmes de commande du treuil interviennent aussi dans cette couche, qu'ils soient mécaniques ou électroniques. Enfin, l'arrêt d'urgence (système à intervention manuelle de sécurité - SAMS) est également inclus dans la couche 3. La chaîne de l'arrêt d'urgence, relativement simple du temps où il s'agissait d'un système électromécanique, comprend aujourd'hui un plus grand nombre d'éléments lorsqu'elle intègre un traitement logique.

¹ Maintenant Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST).

² Rapport d'expertise ([QR-1156-fr](#)) rendu public sous la référence Giraud et Galy 2022a.

³ Rapport d'expertise ([QR-1157-fr](#)) rendu public sous la référence Giraud et Galy 2022b.

Les systèmes instrumentés de sécurité (SIS), correspondants à la couche 4, sont discutés dans le chapitre 4. Les SIS ont pour fonction d'assurer une fonction de sécurité (par ex : fonction d'arrêt). La sécurité est assurée par les exigences de fonction de sécurité (ce que fait la fonction) et les exigences d'intégrité de sécurité (probabilité que la fonction soit réalisée correctement). Un SIS est généralement composé d'éléments de détection (capteurs), d'éléments de traitement et d'éléments d'action (actionneurs), et peut être réalisé indifféremment en technologie câblée ou programmable. Parfois, les SIS partagent des éléments avec le système de commande ou les boucles de régulation. Cela permet souvent de réduire les coûts, mais empêche de remplir le critère d'indépendance des couches. Les niveaux d'intégration du SIS et du système de commande sont variables et présentent des avantages et inconvénients en termes de sécurité (et de coûts). Les normes applicables aux SIS appartiennent à deux grandes familles : CEI 61508 et 62061 ou ISO13849-1. La norme ISO 13849-1 s'applique à tous les systèmes de commande de toutes les machines, alors que la CEI 62061 s'applique uniquement aux systèmes de commande de machines utilisant des systèmes électriques, électroniques ou électroniques programmables. Ces deux normes présentent des méthodes de conception et d'analyse des SIS. Elles permettent notamment d'évaluer la probabilité de défaillance des SIS (niveau SIL – *Safety Integrated Level* dans la famille CEI, et PL dans la famille ISO). Une tentative d'unification des normes ISO 13849 et CEI 62061 était en cours depuis 2012, avec pour objectif de n'en donner qu'une seule numérotée temporairement ISO/CEI 17305. Les SIS des machines d'extraction sont implicitement présents dans la réglementation de plusieurs provinces ou états, par exemple lorsqu'il est mentionné que la machine doit être arrêtée automatiquement si certaines limites sont dépassées. Pour le Québec, l'article 233 du règlement sur la santé et la sécurité du travail dans les mines (RSSM), qui indique les différentes conditions d'arrêt immédiat de la machine d'extraction, décrit par la même occasion les fonctions de sécurité du SIS correspondant. En bout de chaîne du SIS se trouve le frein de treuil ou de câble. Le frein de treuil est plutôt bien connu. Le frein de câble quant à lui a été expérimenté dans des mines aux États-Unis, soit sur des treuils à friction, soit sur des treuils à tambour.

La sécurité logicielle, touchant aussi bien la couche 3 que la couche 4, est présentée au chapitre 5. Un logiciel sécuritaire devrait ne pas contenir de faute lors de la conception, être capable de tolérer les fautes lors de l'exécution, et les concepteurs devraient anticiper les fautes et les éliminer lors des étapes de vérification. Plusieurs exemples de défaillance logicielle sont donnés dans le chapitre, notamment sur le Therac-25 et sur un dispositif d'injection électronique de voiture, ainsi que deux accidents survenus au Québec lors de la modification de logiciels de commande. Le concept de couches de protection peut être étendu à la partie logicielle du SIS. Le cycle de vie du logiciel va de la phase de spécification jusqu'à la mise hors service du logiciel, et couvre notamment le cas de la validation et de la modification. Par ailleurs, l'utilisation de morceaux de code récupérés d'autres applications n'est pas recommandée (cas de l'accident du Therac-25).

Le dernier chapitre concerne la couche de sécurité physique : en cas de perte de contrôle du déplacement de la cage malgré les barrières de niveau 3 (alarmes et intervention humaine) et 4 (SIS), seul un dispositif de sécurité physique - passif ou actif - en couche 5 peut intervenir et éviter l'écrasement. Les parachutes traditionnels n'ont qu'un seul mode de déclenchement (tension trop faible dans le câble), alors que les parachutes modernes pourraient éventuellement être programmés pour plusieurs conditions de déclenchement. Les parachutes sont des dispositifs de sécurité actifs et quelques pistes d'amélioration sont suggérées. Des dispositifs de sécurité passifs sont envisageables aux deux extrémités du puits, comme par exemple l'amortisseur de

fin de course au fond du puits. Enfin, le cycle de vie des dispositifs de sécurité est discuté, notamment le cas des tests et de l'entretien. Il en ressort notamment que si les essais et tests des différentes fonctions de sécurité sont exécutés à des intervalles de temps différents, et par des personnes différentes comme mentionné dans la partie 6 de l'annexe B de la norme CEI 61508, cela permet de conserver la probabilité de défaillance au plus bas niveau possible.

TABLE DES MATIÈRES

AVIS DE NON-RESPONSABILITÉ	i
REMERCIEMENTS	iii
SOMMAIRE EXÉCUTIF.....	v
LISTE DES TABLEAUX.....	xi
LISTE DES FIGURES.....	xiii
LISTE DES ACRONYMES, SIGLES ET ABRÉVIATIONS	xv
1. INTRODUCTION	1
2. MÉTHODES D'ANALYSE DE LA PERFORMANCE DES MOYENS DE PRÉVENTION ET DE PROTECTION	3
2.1 Moyens de protection et de prévention	4
2.1.1 Le concept de défense en profondeur	4
2.1.2 L'indépendance des couches	5
2.1.3 Les barrières de sécurité	6
2.2 Méthodes d'analyse de la performance des moyens de protection	7
2.2.1 Méthode Layer of Protection Analysis (LOPA).....	7
2.2.2 L'évaluation de la performance des barrières	8
2.2.3 Contribution à la réduction du risque	9
2.3 Synthèse.....	10
3. COUCHE 3 – ALARMES ET INTERVENTION HUMAINE.....	13
3.1 Système de surveillance globale.....	13
3.2 Systèmes de commande du treuil / de la cage.....	14
3.3 Système à intervention manuelle de sécurité - l'arrêt d'urgence	14
3.4 Recommandations	15
4. COUCHE 4 – SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ (SIS).....	17
4.1 Description d'un SIS	17
4.2 Cohabitation entre SIS et autre système de commande	19
4.3 Normes applicables	21
4.3.1 ISO 13849 (systèmes de commande des machines).....	22
4.3.2 CEI 61508, 61511 et 62061.....	24
4.3.3 Unification des deux normes	29
4.4 Niveaux de contribution à la réduction du risque (SIL ou PL).....	29

4.4.1	Selon les normes CEI 61511 et CEI 62061	29
4.4.2	Selon la norme ISO 13849-1	30
4.4.3	Équivalence SIL et PL	31
4.4.4	Influence de l'architecture du SIS sur la fiabilité et la disponibilité.....	32
4.5	SIS des machines d'extraction	33
4.6	L'élément terminal du SIS : le frein de treuil ou de câble.....	35
4.6.1	Freins du treuil (tambour / disque).....	35
4.6.2	Frein de câble.....	36
4.7	Recommandations.....	36
5.	COUCHE 4 – SÉCURITÉ LOGICIELLE	39
5.1	Exemples de défaillances logicielles	39
5.1.1	Therac-25.....	40
5.1.2	ETCS Toyota Camry 2005.....	41
5.1.3	Accidents au Québec enquêtés par la CSST.....	42
5.2	Cycle de vie du logiciel	43
5.2.1	Spécification et réalisation	44
5.2.2	Validation	45
5.2.3	Modification	48
5.3	Recommandations.....	50
6.	COUCHE 5 – SÉCURITÉ PHYSIQUE	53
6.1	Les dispositifs de sécurité actifs.....	54
6.1.1	Améliorations possibles des parachutes « classiques »	54
6.1.2	Amélioration possible des parachutes « modernes ».....	55
6.2	Dispositifs de sécurité passifs	56
6.3	Cycle de vie des dispositifs de sécurité.....	56
6.4	Recommandations.....	57
7.	CONCLUSIONS	59
	BIBLIOGRAPHIE	63
	ANNEXE I : DÉFINITIONS	67
	ANNEXE II : ARBRES DE DÉFAILLANCE	71

LISTE DES TABLEAUX

Tableau 1.	Exemples de couches de protection suivant la méthode LOPA.....	8
Tableau 2.	Moyens de maîtrise du risque utilisés au Québec en 2014 dans les puits.....	11
Tableau 3.	Avantages et inconvénients de la cohabitation SIS / autre système de commande	21
Tableau 4.	Catégorie et architecture associée recommandée	24
Tableau 5.	Indépendance des personnes responsables de l'évaluation de la sécurité fonctionnelle des systèmes E/E/PE concernés par la sécurité	26
Tableau 6.	Définition des niveaux SIL selon le mode de sollicitation.....	30
Tableau 7 .	Niveaux de performance (PL)	31
Tableau 8.	Équivalence SIL et PFHD	31
Tableau 9.	Comparaison des architectures 1oo1, 1oo2, 2oo2, et 2oo3	32
Tableau 10	Validation des logiciels selon la norme CEI 61508-3.....	47
Tableau 11.	Extrait du Tableau 1 de la norme, listant les exigences à chaque phase du cycle de vie du logiciel de sécurité	48

LISTE DES FIGURES

Figure 1.	Processus accidentel.....	1
Figure 2.	Concept de couches de protection.....	2
Figure 3.	Cadre conceptuel pour la sécurité des systèmes électroniques programmables (PES) selon le NIOSH.....	3
Figure 4.	Causes primaires des accidents par phase.....	4
Figure 5.	Les différentes catégories des barrières de sécurité.....	7
Figure 6.	Contribution à la réduction du risque.....	9
Figure 7.	Chaîne de l'arrêt d'urgence.....	15
Figure 8.	Schéma générique d'un SIS.....	18
Figure 9.	Architecture détaillée.....	18
Figure 10.	Capteur commun à la boucle de régulation et à la fonction de sécurité.....	19
Figure 11.	Élément final commun à la boucle de régulation et à la fonction de sécurité.....	19
Figure 12.	Capteurs et éléments finaux différents pour la boucle de régulation et l'IPL.....	20
Figure 13.	Domaine d'application des normes CEI et ISO.....	22
Figure 14.	Niveaux de performance dans la norme ISO 13849.....	22
Figure 15.	Calcul du niveau de performance d'une fonction de sécurité (SC/FS) incluant plusieurs composants (SRP/CS).....	23
Figure 16.	Structure normative.....	25
Figure 17.	Organisation de la norme CEI 61508.....	27
Figure 18.	Cycle de vie global selon la CEI 61508.....	28
Figure 19.	Couches de sécurité logicielle.....	42
Figure 20.	Domaines d'application de la norme CEI 61508-2 et 61508-3.....	44
Figure 21.	Cycle de vie de sécurité de logiciel (en phase de réalisation).....	45
Figure 22.	Développement « en V ».....	47
Figure 23.	Exemple de procédure de modification.....	49
Figure 24.	Extrait des lignes directrices de la CEI 61508 : Application de la CEI 61508-3.....	51
Figure 25.	Indisponibilité instantanée d'un dispositif testé.....	57

LISTE DES ACRONYMES, SIGLES ET ABRÉVIATIONS

BPCS :	système de contrôle de base (<i>Basic Process Control System</i>)
CCPS :	<i>Center for Chemical Process Safety</i>
CEI :	Commission électrotechnique internationale
CNESST :	Commission des normes, de l'équité, de la santé et de la sécurité du travail
CSST :	Commission de la santé et de la sécurité du travail (maintenant CNESST)
CSA :	Canadian Standards Association (Association canadienne de normalisation)
DC :	Couverture de diagnostic (<i>diagnostic coverage</i>)
E/E/PE :	électrique/électronique/électronique programmable (<i>electric/electronic/programmable electronic</i>)
ETCS :	Système de contrôle électronique du papillon des gaz (<i>Electronic Throttle Control System</i>)
HSE :	<i>Health and Safety Executive</i>
IPL :	Couche de protection indépendante (<i>Independant Protection Layer</i>)
IRSST :	Institut de recherche Robert-Sauvé en santé et en sécurité du travail
ISA :	<i>Instrumentation, Systems and Automation Society</i>
ISO :	Organisation internationale de normalisation (International Organization for Standardization)
LOPA :	<i>Layer of Protection Analysis</i>
MISRA C :	norme de programmation créée par la <i>Motor Industry Software Reliability Association</i>
MSHA :	<i>Mine Safety and Health Administration</i>
NASA :	<i>National Aeronautics and Space Administration</i>
NIOSH :	<i>National Institute for Occupational Safety and Healt</i>

OSEK :	norme de programmation créée par <i>Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug</i>
PE :	électronique programmable (<i>programmable electronic</i>)
PES :	système électronique programmable (<i>programmable electronic system</i>)
PFD :	probabilité de défaillance à la demande
PL :	niveau de performance (<i>performance level</i>)
PLC :	automates programmables industriels (<i>programmable logic controller</i>)
RSSM :	Règlement sur la santé et la sécurité du travail dans les mines
SAMS :	systèmes à action manuelle de sécurité
SC/FS :	système de commande de la fonction de sécurité
SIL :	niveau d'intégrité de sécurité (<i>safety integrity level</i>)
SIS :	système instrumenté de sécurité
SRECS :	système de commande électrique relatif à la sécurité (<i>safety related electric command system</i>). Note : le circuit de sécurité « traditionnel » fait partie du SRECS
SRP/CS :	partie d'un système de commande relative à la sécurité (<i>safety-related part of a control system</i>)

1. INTRODUCTION

Une lettre signée par un représentant de la partie syndicale du sous-comité sur les machines d'extraction du Comité n° 3.57 de révision du Règlement sur la santé et la sécurité du travail dans les mines (RSSM), datée du 25 octobre 2013, demandait de mandater l'IRSST pour évaluer les systèmes d'arrêt d'urgence des transporteurs de mine en usage à travers le monde (parachutes et autres systèmes) puis de soumettre des recommandations à la CSST pour moderniser les parachutes exigés sur les transporteurs de mine au Québec. Cette demande, appuyée par la partie patronale le 31 octobre de la même année, fait suite à deux accidents survenus en 2011 et 2013.

Le format général d'un processus accidentel est présenté en Figure 1. Pour le cadre de cette étude, le dommage est l'écrasement de la cage au fond du puits. Ainsi par exemple si l'événement dangereux envisagé est la rupture du câble, le facteur d'évitement du dommage est le fonctionnement du parachute. Ainsi le mandat donné à l'IRSST vise à répondre à plusieurs questions :

- Événement dangereux = rupture du câble (volet 2) :
 - Quels parachutes utiliser (facteur d'évitement) ?
 - Comment limiter la probabilité d'occurrence de l'événement dangereux ?
- Événement dangereux = perte de contrôle du déplacement de la cage (volet 3) :
 - Est-il possible d'envisager un facteur d'évitement, et lequel (ou lesquels) ?
 - Comment limiter la probabilité d'occurrence de l'événement dangereux (systèmes de commande, surveillance de la cage, automates programmables industriels - PLC...) ?

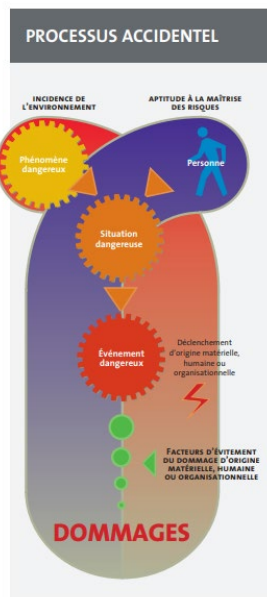


Figure 1. Processus accidentel.

De « Sécurité des machines : phénomènes, situations, événements dangereux et dommages », par S. E. Robert, L. Giraud et Y. Chinniah, 2017, p. 5 (<https://www.cnesst.gouv.qc.ca/sites/default/files/documents/dc200-1581web.pdf>).

©CNESST, 2017. Reproduit avec permission.

Le mandat comporte donc trois volets principaux :

1. Revue des systèmes parachutes, des systèmes de freinage d'urgence et des législations provinciales et internationales ;
2. Recommandations dans le cas où il y a rupture du câble d'extraction ;
3. Recommandations dans le cas où il y n'a pas rupture du câble d'extraction.

Dans le premier volet de l'expertise, l'arbre de défaillance proposé pour le cas où il n'y a pas de rupture du câble d'extraction identifie plusieurs événements élémentaires pouvant conduire à un écrasement de la cage :

- Une erreur d'opération ;
- Une défaillance du système de commande ;
- Une défaillance du système de sécurité ;
- Une défaillance du système de freinage.

La défaillance du système de freinage et les erreurs d'opération ne rentrent pas dans le cadre du mandat et ne seront donc pas détaillées dans ce rapport. Le rapport traite donc de la fiabilité des systèmes de commande et des systèmes instrumentés de sécurité et présente dans un premier temps les méthodes d'analyse de performance des moyens de prévention et de protection, et plus particulièrement le concept de couches de protection [Figure 2] (Iddir, 2012b). Puis les éléments faisant partie de la couche de protection 3 nommée « Alarmes et intervention humaine » et de la couche de protection 4 nommée « Systèmes instrumentés de sécurité » sont discutés. Le cas de la sécurité logicielle est présenté dans la section 4 de ce rapport, puisque celle-ci concerne les deux couches de protection précédentes. Enfin, la couche de protection 5 nommée « Sécurité physique » est discutée et les facteurs d'évitement possible sont présentés. Des recommandations sont formulées à la fin de chaque chapitre.

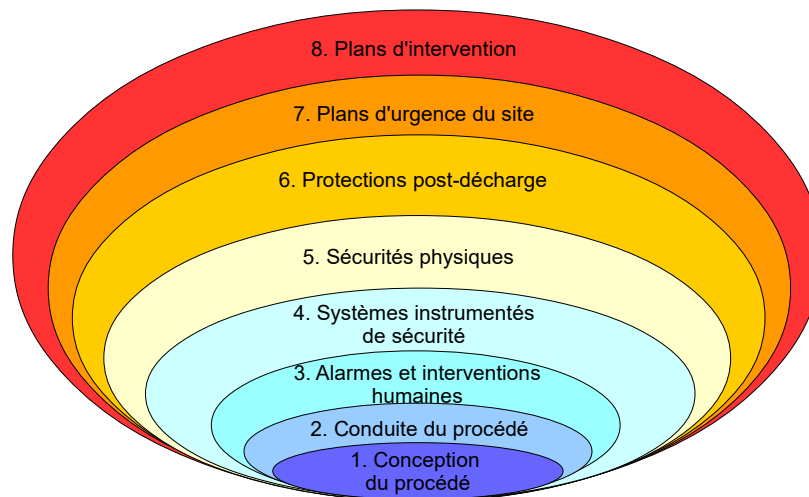


Figure 2. Concept de couches de protection.

Adaptée de « Méthode LOPA : principe et exemple d'application », par O. Iddir, 2012. ©Techniques de l'ingénieur, 2012.

À la fin du rapport sont présentées des annexes qui incluent :

- Des définitions générales afin d'aider le lecteur à la compréhension du texte ;
- L'arbre de défaillance pour le cas où la cage reste connectée au câble.

2. MÉTHODES D'ANALYSE DE LA PERFORMANCE DES MOYENS DE PRÉVENTION ET DE PROTECTION

La maîtrise du risque industriel repose de plus en plus sur une série d'éléments qui sont combinés les uns aux autres afin d'obtenir un niveau de risque résiduel inférieur au niveau de risque tolérable (Giraud et Galy, 2022b). En effet, les machines se complexifient : elles intègrent de plus en plus de modes de commande et de fonctions, elles ne sont plus mono énergie, et enfin leurs systèmes de commande et de supervision intègrent de nouvelles technologies programmables (et donc de nouveaux modes de défaillance). Il devient donc nécessaire de prendre du recul pour analyser les différents moyens de maîtrise des risques présents sur une machine d'extraction.

Entre 1995 et 2001, 11 incidents liés à de l'électronique programmable ont eu lieu aux États-Unis (4 d'entre eux se sont soldés par des décès), et durant cette même période, 71 incidents de ce type ont eu lieu au New South Wales (Dhillon, 2010). Ces incidents sont notamment dus à des infiltrations d'eau, des erreurs de programmation, des valves solénoïdes défectueuses ou des erreurs d'opération (Dhillon, 2010).

Aux USA, le *Mine Safety and Health Administration* (MSHA) a d'abord essayé de fixer des recommandations applicables après installation afin de réduire la fréquence de ces incidents. Il a cependant été rapidement conclu que cette approche était insuffisante pour les systèmes programmables complexes (Sammarco, 2002). Le *National Institute for Occupational Safety and Health* (NIOSH) a alors proposé une approche fortement inspirée de la norme CEI 61508 (Sammarco *et al.*, 2001b ; Sammarco *et al.*, 2001a ; Sammarco, 2005 ; Sammarco, 2006 ; Sammarco et Fisher, 2001 ; Sammarco et Flynt, 2006 ; Sammarco et Fries, 2003) [Figure 3].

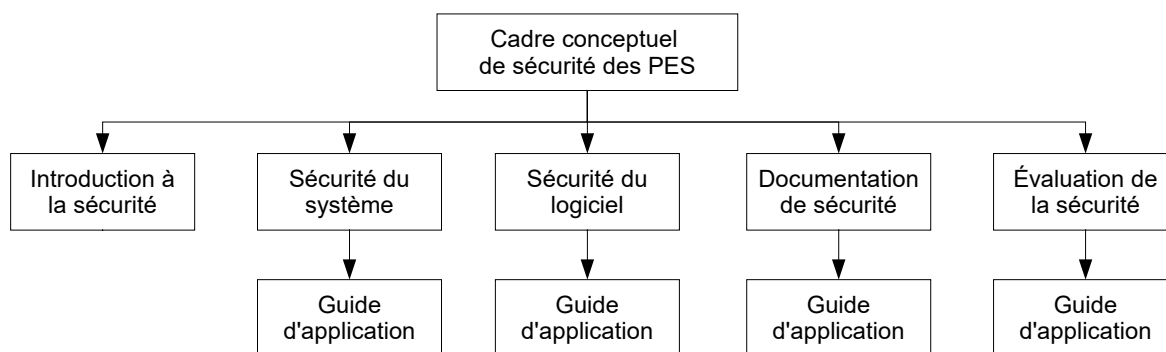


Figure 3. Cadre conceptuel pour la sécurité des systèmes électroniques programmables (PES) selon le NIOSH.

Adaptée de « *Addressing the safety of programmable electronic mining systems : lessons learned* », par J.J. Sammarco 2002. ©IEEE, 2002.

La réflexion sur la sécurité du système doit être globale et non uniquement centrée sur des éléments individuels (logiciel, capteurs, etc.). De plus, cette réflexion doit être initiée dès la conception, car les décisions prises lors de la conception influencent fortement la sécurité lors de toute la vie de la machine ou du processus. Une étude du *Health and Safety Executive* (HSE) menée en 1995 (HSE, 2003) sur 34 accidents impliquant les systèmes de commande mentionne que 44,1 % des causes primaires sont liées à des fonctionnalités déficientes dans le cahier des

charges (spécification du SIS, Système instrumenté de sécurité) et que 20,6 % des causes primaires sont liées à des modifications inappropriées après la mise en service, par méconnaissance des impacts des changements introduits dans la programmation [Figure 4].

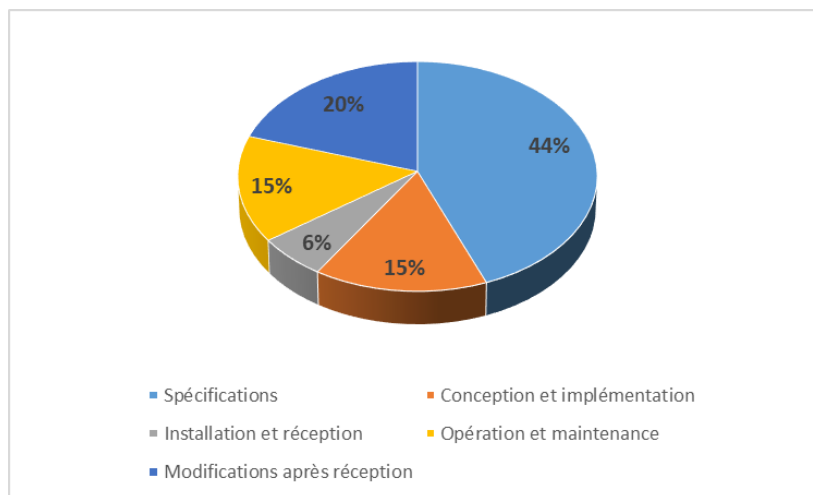


Figure 4. Causes primaires des accidents par phase.

Adaptée de « *Out of control - Why control systems go wrong and how to prevent failure* », par Health and Safety Executive 2003. ©HSE, 2003.

Pour gérer avec efficacité cette prise en compte de la sécurité au cours du cycle de vie complet de la machine, il faut s'appuyer sur des méthodes qui permettent de structurer le raisonnement. Dans le cadre de cette expertise, nous avons choisi trois concepts complémentaires qui apportent chacun un avantage structurel au processus de raisonnement. Il s'agit de la défense en profondeur (couches de protection), des barrières de sécurité et de l'indépendance des couches de protection.

2.1 Moyens de protection et de prévention

2.1.1 Le concept de défense en profondeur

Le concept de défense en profondeur (INSAG, 1996) a été développé dans le secteur militaire vers 2900 avant J.-C. à Hiérakonpolis en Égypte (Garbolino et Guarnieri, 2012), puis il a été utilisé dans l'industrie nucléaire civile dès les années 1960 dans le but de formaliser la sûreté des centrales. Au début, la défense en profondeur était basée principalement sur des éléments physiques successifs et indépendants de protection : la gaine de combustible qui entoure la matière radioactive, puis la cuve du réacteur et enfin l'enceinte de confinement. L'objectif étant que la défaillance de la première couche soit contenue par la deuxième, et que la défaillance de la deuxième soit contenue par la troisième, ce qui a fonctionné totalement dans le cas de l'accident de Three Mile Island, mais partiellement dans le cas de l'accident de Fukushima et pas du tout dans le cas de l'accident de Tchernobyl⁴.

⁴ La centrale de Tchernobyl ne disposait que de deux couches, la gaine et la cuve, ce qui explique l'ampleur de la dissémination de la radioactivité [Guérinot 2011, Le retour d'expérience, condition déterminante de la sûreté nucléaire, Préventique Sécurité, N119, 2011, pp. 26-31].

Mais après l'accident de Three Mile Island, les erreurs humaines ainsi que les défaillances organisationnelles ou matérielles ont été intégrées (Garbolino et Guarnieri, 2012).

Ce concept de défense en profondeur repose maintenant sur trois notions fondamentales (Garbolino et Guarnieri, 2012) :

1. La notion de « barrière » physique ;
2. La notion de « ligne de défense » qui touche les moyens humains, organisationnels et structurels ;
3. La notion de « niveau de protection » qui correspond à l'agencement des barrières et des lignes de défense selon des objectifs structurés.

Les lignes de défense vont donc intégrer des moyens physiques dont les caractéristiques recherchées sont liées au matériau utilisé et à son dimensionnement, mais aussi des mesures de maîtrise du risque qui peuvent intégrer les systèmes de commande qui supervisent des fonctions de sécurité.

2.1.2 L'indépendance des couches

Les différentes couches de protection doivent être indépendantes (*Independent Protection Layer*, IPL) les unes des autres afin de pouvoir jouer leur rôle indépendamment les unes des autres et donc éviter les défaillances de cause communes ou les défaillances de mode commun. La définition donnée par le *Center for Chemical Process Safety* (CCPS) (CCPS, 2001) est la suivante : « Une couche de protection indépendante (IPL) correspond à un équipement, un système ou une action capable de prévenir la survenue des conséquences associées à un scénario d'accident. Elle doit être indépendante de l'événement initiateur, mais aussi de toutes les autres couches de protection associées au scénario. L'efficacité et l'indépendance de chaque IPL doivent être vérifiables. »⁵

Cette notion d'indépendance va s'appliquer à toutes les barrières y compris à celle intégrant les systèmes de commande. Une barrière doit satisfaire trois critères afin d'être considérée comme étant une IPL :

- Efficace dans la prévention des conséquences quand elle fonctionne comme prévu ;
- Indépendante de l'événement initiateur et de tous composants d'une autre IPL déjà sollicitée pour combattre le même scénario ;
- Vérifiable, l'efficacité supposée en matière de prévention des conséquences et en termes de probabilité de défaillance à la demande (PFD) doit être capable d'être validée (documentation, tests, etc.).

⁵ Traduction libre des auteurs.

De fait, toutes les IPL seront aussi des barrières, mais toutes les barrières ne seront pas des IPL selon CCPS (2001). Les barrières suivantes, souvent utilisées dans l'industrie pour contribuer à la réduction du risque, ne sont pas des IPL, mais participent indirectement à cette réduction du risque :

- La formation et la certification des opérateurs : ces deux barrières peuvent être prises en compte lors de l'évaluation de la probabilité d'échec ou d'erreur d'un opérateur ;
- Les procédures : cette barrière peut être prise en compte lors de l'évaluation de la probabilité d'échec ou d'erreur d'un opérateur ;
- Les tests périodiques et l'inspection : ces deux barrières influent sur la probabilité de défaillance de certaines IPL (Bingham, 2005) ;
- La maintenance : cette barrière influe la probabilité de défaillance de certaines IPL ;
- Les communications : cette barrière influe la probabilité de défaillance de certaines IPL ;
- La signalisation : cette barrière peut influencer sur la probabilité de défaillance de certaines IPL, mais elle peut aussi faire défaut par ignorance, par manque de clarté, etc.

Cette notion d'indépendance est assez stricte du point de vue théorique, car elle implique que plusieurs IPL ne peuvent pas utiliser le même système de contrôle de base (*Basic Process Control System*, BPCS). Dans la réalité, cette solution est possible, mais ce choix doit être étayé par des données de fiabilité et le niveau de réduction du risque sera plafonné.

2.1.3 Les barrières de sécurité

Les barrières de sécurité, aussi appelées mesures de maîtrise des risques, peuvent être classées en trois catégories :

- Les barrières techniques ;
- Les barrières humaines ;
- Les barrières mixtes qui font intervenir les barrières techniques et humaines. Ces dernières barrières sont appelées systèmes à action manuelle de sécurité (SAMS).

La catégorie des barrières techniques de sécurité peut être scindée en deux, avec des dispositifs de sécurité ou de systèmes instrumentés de sécurité (SIS). Enfin, les dispositifs de sécurité peuvent être passifs ou actifs [Figure 5] (Mesures, 2009c).

Le système parachute installé sur les cages des machines d'extraction correspond bien à la définition d'un dispositif de sécurité donnée par Le et Dianous (2008) : « *Élément unitaire, autonome, ayant pour objectif de remplir une fonction de sécurité, dans sa globalité. On distingue des dispositifs actifs et des dispositifs passifs.* » Dans notre cas, le dispositif est actif, car il met en jeu des dispositifs mécaniques (ressort, levier...) pour remplir sa fonction.

L'activation de l'arrêt d'urgence de la machine d'extraction est un SAMS, car l'opérateur du treuil ou une autre personne doit appuyer sur le bouton d'arrêt d'urgence pour déclencher la fonction d'arrêt d'urgence lorsqu'une situation anormale, pouvant être contrée par l'activation de la fonction d'arrêt d'urgence, est détectée.

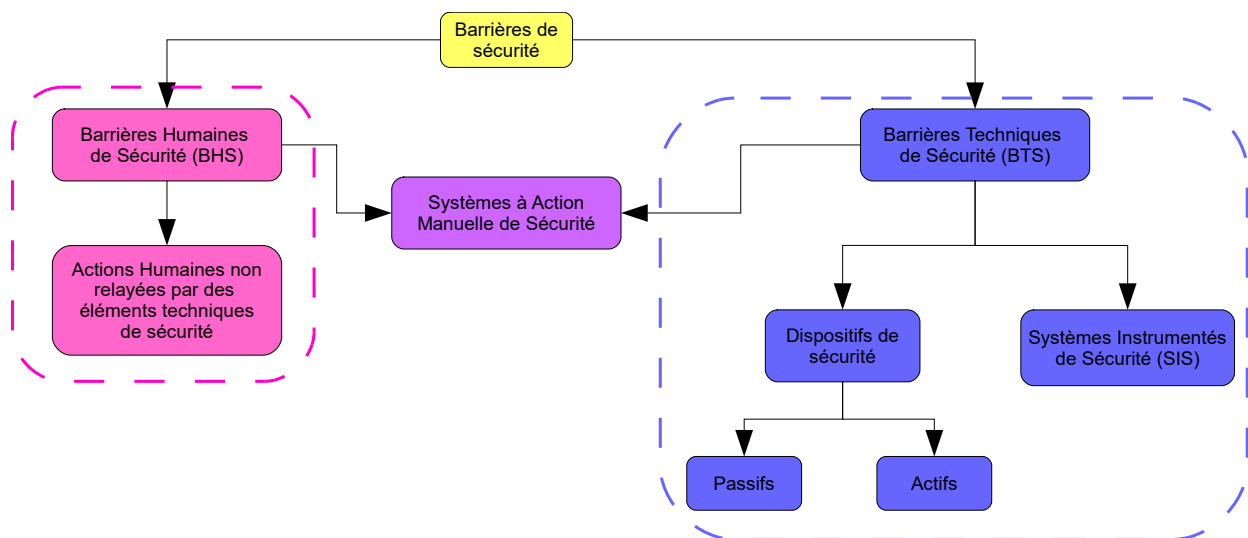


Figure 5. Les différentes catégories des barrières de sécurité.

Adaptée de « *NORME CEI 61511 - Définir, réaliser, maintenir la fonction de sécurité* », par Mesures 2009.
©Mesures, 2009.

Les barrières humaines (Miche et Perinet, 2009) sont essentiellement constituées d'une activité humaine (une ou plusieurs opérations) qui s'oppose à l'enchaînement d'événements susceptibles d'aboutir à un accident. D'un point de vue temporel, l'activité humaine peut être effectuée en amont et elle sera alors classée comme une « barrière humaine de prévention » (par exemple vérifier l'étanchéité d'un circuit), ou l'action peut être effectuée en aval et elle sera alors classée comme une « barrière humaine de rattrapage » (fermeture manuelle d'une valve suite à une montée en pression). Il ne faut pas oublier que le plus souvent, les barrières humaines sont associées à une composante technique (valve, vanne, etc.) qui peut faire défaut, d'où la case « Actions humaines non relayées par des éléments techniques de sécurité » de la Figure 5.

2.2 Méthodes d'analyse de la performance des moyens de protection

2.2.1 Méthode *Layer of Protection Analysis (LOPA)*

La méthode d'analyse des couches de protection LOPA (CCPS, 2001 ; Iddir, 2012b) utilise elle aussi la notion de barrières de sécurité, mais complétée par la notion de huit couches de protection physique, humaine ou mixte [Tableau 1 et Figure 2].

Tableau 1. Exemples de couches de protection suivant la méthode LOPA

	Industrie chimique	Machine d'extraction
Couche 1 : conception	Conception de procédés « sûrs »	Règles de l'art de la conception d'un treuil minier
Couche 2 : conduite	Conduite des procédés	Opérateur de treuil
Couche 3 : alarmes et intervention humaine	Salle de contrôle	Lilly
Couche 4 : systèmes instrumentés de sécurité (SIS)	Niveau haut de sécurité	Capteur d'évite-molette et système de commande associé Lilly
Couche 5 : sécurité physique	Soupape de surpression	Système parachute de la cage
Couche 6 : protection post-décharge	Cuvette de rétention	Système parachute de la cage
Couche 7 : plan d'urgence	Camion incendie	Secouristes miniers
Couche 8 : plan d'intervention	Protection de parties sensibles de l'usine	Secouristes miniers

Tout comme une analyse du risque ou lors de la création d'un arbre de défaillance, la méthode LOPA demande aussi de déterminer des scénarios qui seront analysés. Dans le cadre de cette expertise, pour une cage déplacée par une machine d'extraction, les deux scénarios à analyser sont la rupture du câble (situé *a priori* entre les couches 4 et 5) et la perte de contrôle du déplacement de la cage (situé *a priori* entre les couches 3 et 4), tous deux pouvant mener à l'écrasement de la cage au fond du puits. Les différentes couches de protection, qui peuvent intervenir avant ou après l'apparition de l'événement dangereux sont, dans le cas de la cage :

- Mesure de prévention : respect du RSSM, facteurs de sécurité du câble, contrôleur de supervision électromécanique ou électronique, arrêt d'urgence sur le pupitre de commande ;
- Mesure de mitigation : contrôleur de supervision électromécanique ou électronique faisant partie de la couche « SIS », système parachute sur la cage faisant partie de la couche « sécurités physiques », équipe de secouristes formés faisant partie de la couche « plans d'urgence ».

2.2.2 L'évaluation de la performance des barrières

Il ne faut pas oublier d'évaluer les barrières afin de juger de leurs performances. Ceci peut être fait en évaluant :

- La probabilité de défaillance de la barrière ;
- Le temps de réponse de la barrière ;
- L'efficacité de la barrière.

Dans le cas des parachutes, le temps de réponse de la barrière et son efficacité sont évalués à l'aide des tests de déclenchement rapide (temps de réponse) et du test de chute libre (efficacité).

Par ailleurs, il faut aussi que la performance des barrières ne diminue pas dans le temps à cause du phénomène de vieillissement. Dans le cas des parachutes, les tests de déclenchement rapide aux trois mois permettent de vérifier le bon fonctionnement du système de parachute et les dérives associées (usure des dents, grippage des axes, etc.).

2.2.3 Contribution à la réduction du risque

Une autre façon de représenter la contribution de chaque moyen de maîtrise du risque est illustrée à la Figure 6 (ISA, 2005). Dans cet exemple, les moyens de maîtrise du risque commande (PLC de commande ou *Basic Process Control System* - BPCS), informationnel (alarme), système instrumenté de sécurité (SIS), mécanique ou autre ont approximativement le même apport dans la réduction du niveau de risque.

Par rapport à un risque initial créé lors de la conception initiale d'une machine (ou d'un procédé), chaque moyen de maîtrise du risque va apporter sa contribution à la diminution du niveau de risque afin de rendre le risque résiduel acceptable.

Dans le cas des machines d'extraction récentes ou pour les machines d'extraction dont le système de commande a été modernisé, c'est le système de conduite automatisé ou semi-automatisé qui va assurer la plus grande part de réduction du risque dans le cas de l'événement dangereux « perte de contrôle du déplacement de la cage ». C'est donc vers lui que l'essentiel des efforts doit être concentré.

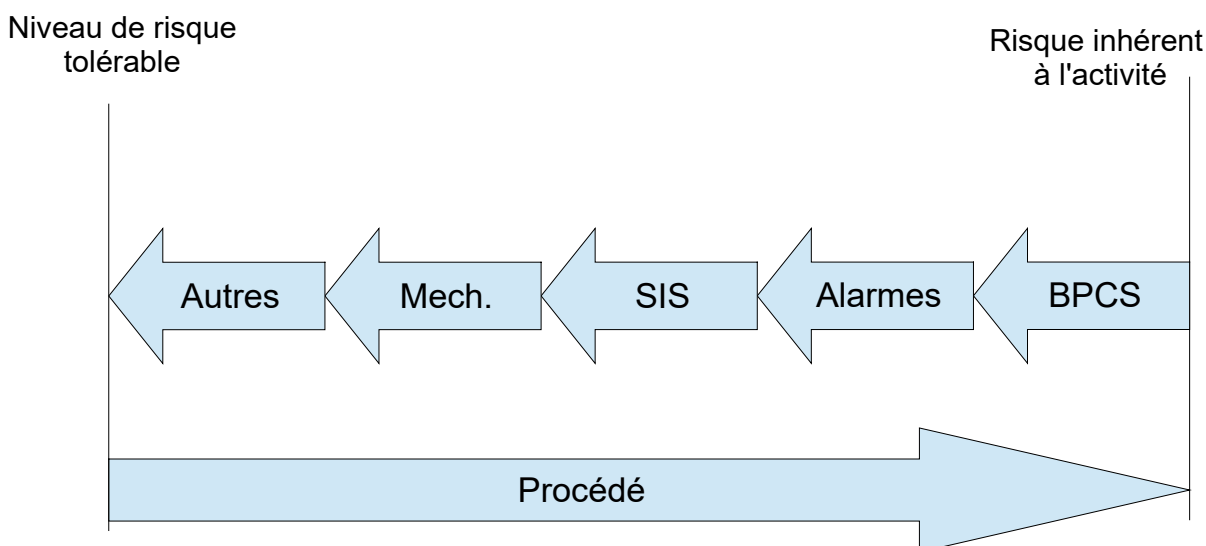


Figure 6. Contribution à la réduction du risque.

Adaptée de « Guide d'interprétation et d'application de la norme IEC 61508 et des normes dérivées IEC 61511 (ISA S84.01) et IEC 62061 », par Instrumentation, Systems and Automation Society 2005. ©ISA, 2005.

2.3 Synthèse

Dans le cas d'une cage déplacée par une machine d'extraction, les deux scénarios qui peuvent mener à l'écrasement de la cage au fond du puits sont :

- La rupture du câble (événement dangereux situé a priori entre les couches 4 et 5, donc problème émergeant dans les couches 1, 2, 3 ou 4) : ce cas est présenté au volet [2](#) de l'expertise ;
- La perte de contrôle du déplacement de la cage (événement dangereux situé a priori entre les couches 3 et 4, donc problème émergeant dans les couches 1, 2 ou 3). Ce cas est un peu plus complexe que le précédent, car un événement dangereux secondaire, la rupture du câble, est possible si le freinage est trop brutal lors d'un mouvement descendant.

Les dommages sont sensiblement les mêmes dans les deux cas : endommagement de la cage et décès des occupants (ou blessures importantes), endommagement irrémédiable du câble, fonds du puits ou chevalement à réparer, puits indisponible pour une longue période, etc. La machine d'extraction peut aussi être endommagée dans le cas de la perte de contrôle du déplacement de la cage (arrachement du câble sur le tambour, détérioration du tambour, etc.).

Du point de vue des moyens de maîtrise du risque pour les deux événements dangereux, le tableau 2 synthétise les éléments utilisés au Québec en 2015 ainsi que les couches correspondantes.

Pour le premier scénario, la rupture du câble, la mesure de mitigation active utilisée systématiquement au Québec est le système parachute de la cage qui est un dispositif actif. Deux systèmes à action manuelle de sécurité (SAMS - Figure 5) utilisés dans quelques mines du Québec ont été recensés : il s'agit du système de suivi en continu de l'état du câble ou de la charge dynamique pour l'un, et pour l'autre de l'une des options d'un système de communication sans fil entre la cage et la machine d'extraction. Il ne semble pas que soit utilisé, en 2015 au Québec, pour une cage, un système instrumenté de sécurité (SIS) permettant de réduire le risque de rupture du câble. Ce type de SIS est déjà utilisé pour des skips dans des mines au Québec.

Pour le second scénario, il n'existe actuellement pas de dispositif de sécurité, actif ou passif, qui puisse se déclencher une fois l'événement redouté présent : en effet, par conception, le système parachute traditionnel ne se déclenche pas si le câble n'est pas rompu (Giraud et Galy, 2022a ; Giraud et Galy, 2022b). Par contre, de nombreux moyens de maîtrise du risque sont utilisés : Lilly, PLC de commande, PLC de supervision et circuit de sécurité.

Tableau 2. Moyens de maîtrise du risque utilisés au Québec en 2014 dans les puits

Événement dangereux	Rupture du câble	Perte de contrôle du déplacement de la cage
Moyens de maîtrise du risque		
Couche 8 : plan d'intervention	/	/
Couche 7 : plan d'urgence	Sauvetage minier	Sauvetage minier
Couche 6 : protection post-décharge	/	/
Couche 5 : sécurité physique	Système parachute de la cage	/
Couche 4 : systèmes instrumentés de sécurité (SIS)	/	Contrôleur Lilly Circuit de sécurité
Couche 3 : alarmes et intervention humaine	Alarme de déclenchement intempestif du système parachute (SAMS) Suivi en continu de l'état du câble (SAMS) Automate programmable industriel (PLC) de supervision	Contrôleur Lilly Automate programmable industriel (PLC) de supervision Arrêt d'urgence (SAMS)
Couche 2 : conduite	Opérateur du treuil Automate programmable industriel (PLC) de commande Supervision des forces de freinage dynamiques	Opérateur du treuil Automate programmable industriel (PLC) de commande
Couche 1 : conception	Règles de l'art de la conception d'un câble et d'un treuil minier	Règles de l'art de la conception d'un treuil minier

La suite du document s'organise en abordant couche par couche les moyens de maîtrise du risque permettant d'éviter une perte de contrôle du déplacement de la cage. Les cas des couches 1 et 2 ne seront pas abordés, car elles sont en dehors du mandat de cette expertise.

3. COUCHE 3 – ALARMES ET INTERVENTION HUMAINE

Dans le document intitulé « Les machines d'extraction », Fortin et Demers (2011) listent 22 causes d'accident possibles avec une machine d'extraction. Compte tenu de la gravité possible des conséquences d'un accident avec une machine d'extraction, ces dernières doivent être équipées de dispositifs d'alarme et de dispositifs de sécurité automatiques et fiables.

Typiquement, la couche 3 de la méthode LOPA, intitulée « alarmes et interventions humaines », fait intervenir les systèmes à interventions manuelles de sécurité (SAMS) (voir la Figure 5).

Deux catégories de moyens de maîtrise du risque existent : les systèmes de monitoring global et les contrôleurs. Ces deux catégories peuvent être complétées par le système à intervention manuelle de sécurité classique qu'est l'arrêt d'urgence. C'est ce que nous allons développer ci-dessous.

3.1 Système de surveillance globale

Afin d'assurer la sécurité du système d'extraction au complet, certains chercheurs proposent une surveillance globale des composantes du système et une gestion par ordinateur des données afin de prendre les décisions adéquates. En effet, avec les anciens systèmes d'exploitation des systèmes d'extraction, l'opérateur travaillait « à l'aveugle » et communiquait avec les mineurs dans le puits uniquement à l'aide de signaux sonores codés (la cloche). Maintenant, il est possible d'installer des caméras aux différents niveaux afin que l'opérateur soit mieux informé. Mais certaines informations sont encore manquantes.

Un système de surveillance globale peut inclure les composantes suivantes (Beus et Ruest, 2002) :

- Cellule de charge pour mesurer la tension dans le câble ;
- Positionnement (avec checkpoints) et vitesse de la cage ;
- Potentiomètre pour mesurer l'alignement des guides (*shaft guide gage*), au-delà de ± 8 cm, une alarme est envoyée à l'opérateur ;
- Détecteur de température dans le puits ;
- Jauge de courant continu (*Direct Current*) sur le moteur du treuil ;
- Accéléromètre multi-axes ;
- Microprocesseur pour le traitement des informations et transmetteur radio sur la cage pour envoyer les données vers le haut du puits.

Certains chercheurs ont étudié les avantages et défauts des différents types de senseurs pour surveiller la position et la vitesse de la cage (Kovalchik et Duda, 1995).

L'idée de la surveillance de la vitesse et de la position de la cage n'est pas récente. Déjà en 1947, l'idée d'utiliser un limiteur de vitesse (*speed governor*) similaire aux ascenseurs civils était suggérée, mais son application était impossible du fait des très longs câbles (*governor rope*) nécessaires (Young, 1947).

3.2 Systèmes de commande du treuil / de la cage

La problématique de la fiabilité de la commande des treuils miniers est connue depuis les débuts des années 1900, et le système de supervision électromécanique fiable le plus courant qui permet de réduire la fréquence d'apparition d'un événement dangereux est le système Lilly (Fortin et Demers, 2011). C'est un contrôleur de sécurité électromécanique qui autorise l'utilisation sans entrave du treuil tant que certaines caractéristiques de vitesse et de positionnement restent à l'intérieur d'un gabarit de fonctionnement. Si une limite est dépassée, un avertissement est donné. Si l'opérateur ne réagit pas dans un délai donné, le contrôleur Lilly ouvre le circuit de sécurité qui coupe l'alimentation du moteur et applique les freins.

Le contrôleur électromécanique Lilly peut être considéré comme faisant partie des couches 3 et 4 :

- Couche 3 : lorsque la machine d'extraction dépasse la vitesse maximale autorisée en fonction de la position de la cage ou lorsque la décélération n'est pas conforme au profil de la came, une alarme alerte l'opérateur qui doit réagir en quelques secondes. Si l'opérateur réagit correctement, il garde le contrôle sur la machine d'extraction.
- Couche 4 : si l'opérateur ne réagit pas ou réagit trop lentement, ou si une came actionne le galet du contrôleur du Lilly, l'interrupteur d'excès de vitesse ouvre le circuit de sécurité et la cage est arrêtée le plus vite possible.

Depuis la fin du XXe siècle, les systèmes de commande sont devenus électriques puis électroniques et les machines d'extraction ne font pas exception (Paques et Germain, 2005 ; Sammarco *et al.*, 2001b). Les commandes mécaniques du treuil ont été remplacées par des commandes électromécaniques puis électriques ou électroniques branchées à un PES de commande. La fiche technique RF-412 de l'IRSST publiée en 2005 (Paques et Germain, 2005) aborde cette nouvelle réalité sous l'angle de la sécurité des machines. Les différentes évolutions de la norme CSA M421 (1985 ; 1993 ; 2000 ; 2011) reflètent bien cette évolution.

3.3 Système à intervention manuelle de sécurité - l'arrêt d'urgence

La couche 3 de la méthode LOPA correspond aux alarmes et interventions humaines. L'objectif est d'alerter l'opérateur qui supervise le fonctionnement de la machine du dépassement de certaines valeurs seuils afin qu'il puisse corriger le fonctionnement.

Globalement, pour que cette couche fonctionne bien dans le cas de l'arrêt d'urgence actionné par l'opérateur, en appuyant sur un des boutons d'arrêt d'urgence, il faut que :

- Le système de commande reçoive la bonne information ;
- Que l'interface homme-machine soit efficace ;
- Que l'activité humaine de l'opérateur soit adaptée au problème en cause (détection, diagnostic et action) ;
- Que l'arrêt d'urgence, action ultime de l'opérateur en cas de problème non réglé dans le but de réduire la gravité du dommage, fonctionne à la demande.

Le fonctionnement de l'arrêt d'urgence disponible minimalement au poste de commande du treuil est souvent régi par un code ou une norme (RSSM, art. 232 et 233 ; CSA M421-2011, etc.). Par contre la fréquence des tests est peu ou pas spécifiée. Peu de législations traitent spécifiquement de cet aspect de la sécurité hormis le New South Wales en Australie par le biais de l'ébauche de son guide MDG 33.6 « Mine Winders Part 6: Control Systems » (R-NSW, 2011b).

Du point de vue technique, la chaîne de l'arrêt d'urgence peut être représentée par la figure 7.

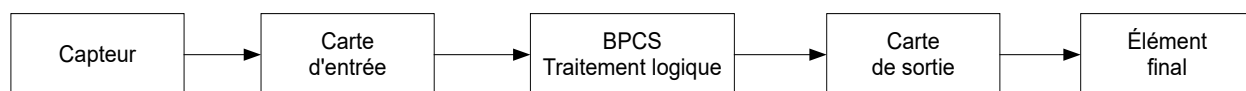


Figure 7. Chaîne de l'arrêt d'urgence.

Adaptée de « Méthode LOPA : principe et exemple d'application », par O. Iddir, 2012. ©Techniques de l'ingénieur, 2012.

Dans notre cas, le capteur est l'interrupteur d'urgence, et l'élément final est le frein, mentionnés à l'article 233 du RSSM.

Historiquement, la chaîne de l'arrêt d'urgence était plus simple et n'était constituée que de deux éléments, soit un capteur (bouton d'arrêt d'urgence) et un élément final (frein, solénoïde, etc.); ou était constituée de trois éléments, soit un capteur, une carte de sortie ou son équivalent (relais de sécurité, relais à contacts guidés) et un élément final (frein, sectionneur, etc.). Cette simplicité et cette indépendance étaient des éléments qui participaient à sa fiabilité. Ceci est par ailleurs mentionné à l'article 6.9.3.4 de la sous-section « Circuits de protection » de la norme CSA M421 (2011) et dans l'annexe C.

Sammarco s'est aussi penché sur la question de la fiabilité de la chaîne d'arrêt d'urgence avec un traitement logique (Sammarco, 2005 ; Sammarco et Fisher, 2001). Dans l'exemple utilisé, pour atteindre le niveau de fiabilité désiré, il faut un SIL3 (*Safety integrity level*). Plusieurs architectures sont proposées et la fiabilité associée est calculée. Il ressort de cet exemple que l'élément qui limite le plus l'atteinte du niveau de fiabilité SIL3 est l'API et qu'un API de sécurité est alors nécessaire pour atteindre le niveau de fiabilité requis.

La question plus générale de la fiabilité des fonctions de sécurité sera détaillée dans le chapitre suivant.

3.4 Recommandations

Afin d'améliorer la performance de la couche 3 de la méthode LOPA, intitulée « alarmes et interventions humaines », nous formulons la recommandation suivante. Il appartiendra au législateur de considérer si tout ou partie de cette recommandation doit être intégré dans les textes de loi, et aux industriels de mettre en place cette recommandation s'ils la jugent pertinente.

Recommandation 3.1 :

Implanter un système de monitoring global du système d'extraction, machine et puits, afin d'améliorer la prise de décision basée sur des données factuelles et probantes.

4. COUCHE 4 – SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ (SIS)

La couche 4 de la méthode LOPA, intitulée « Systèmes instrumentés de sécurité », fait intervenir des dispositifs ayant pour objectif de remplir une fonction ou sous-fonction de sécurité (Le et Dianous, 2008). Une fonction de sécurité est une fonction « devant être implémentée dans un système électrique, électronique, électronique programmable (E/E/PE) concerné par la sécurité dont le but est d'atteindre ou de maintenir un état sûr pour les équipements contrôlés, dans le cadre d'un événement dangereux particulier. » (ISA, 2005). L'ISO 13849-1:2006 (ISO 13849-1, 2006) et l'ISO 12100:2010 (ISO 12100, 2010) utilisent la définition suivante pour une fonction de sécurité : « fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du (des) risque(s) ».

Plusieurs fonctions de sécurité types sont citées par le tableau 8 de l'ISO 13849-1:2006 dont :

- La fonction d'arrêt ;
- Les fonctions initiées par un dispositif de protection (limiteur ou autre) ;
- L'arrêt d'urgence ;
- Le réarmement manuel ;
- etc.

Selon ISA (2005), deux types d'exigences sont nécessaires pour réaliser la sécurité fonctionnelle :

- Exigences des fonctions de sécurité (ce que fait la fonction) et ;
- Exigences d'intégrité de la sécurité (la probabilité que la fonction de sécurité soit réalisée correctement, niveau SIL).

Les exigences des fonctions de sécurité sont dérivées de l'analyse de risque et les exigences d'intégrité de la sécurité sont dérivées de l'évaluation des risques. Plus le niveau d'intégrité de la sécurité est élevé, plus la probabilité d'une défaillance dangereuse doit être faible.

Cette section présente en détail ce qu'est un SIS, positionne le SIS par rapport aux autres systèmes de commande, discute des normes applicables de manière générale, de la contribution du SIS à la réduction du risque, présente les SIS existants dans l'industrie minière et se conclue sur un des éléments terminaux importants des SIS des machines d'extraction qu'est le frein.

4.1 Description d'un SIS

Un SIS (Figure 8) est généralement composé d'éléments de détection (les capteurs), d'éléments de traitement et d'éléments d'action (les actionneurs).

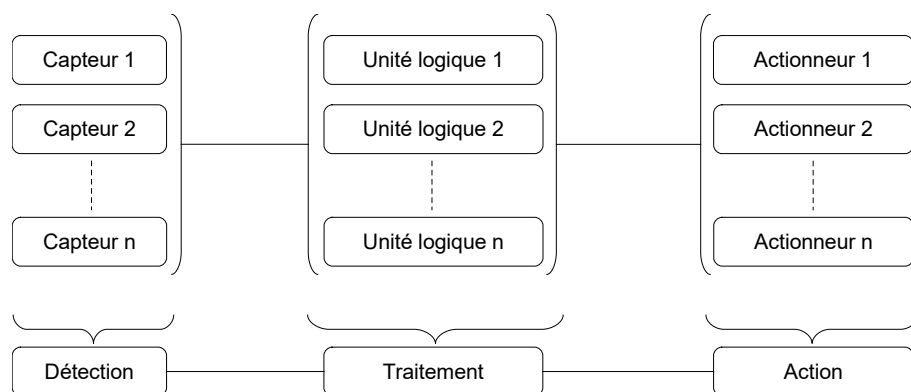


Figure 8. Schéma générique d'un SIS.

Adaptée de « *Évaluation des performances des Barrières Techniques de Sécurité Omega 10* », par N.T. Le et V. Dianous, 2008. ©INERIS, 2008.

Un détecteur comprend généralement deux sous-éléments : un capteur et un transmetteur [Figure 9]. Comme cela est indiqué sur la figure 9, il n'y a pas nécessairement d'unité de traitement entre le détecteur et l'actionneur.

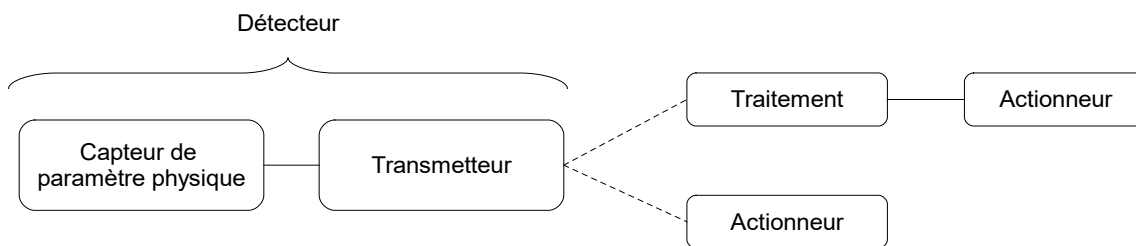


Figure 9. Architecture détaillée.

Adaptée de « *Évaluation des performances des Barrières Techniques de Sécurité Omega 10* », par N.T. Le et V. Dianous, 2008. ©INERIS, 2008.

Les sous-fonctions de traitement sont soit à technologie câblée (composants logiques élémentaires), soit à technologie programmable (Le et Dianous, 2008) (voir la section 2.3). Cependant, la technologie câblée commence à devenir désuète et elle tend à être remplacée par la technologie programmable (Paques et Germain, 2005).

Le SIS pourra assurer la fonction de sécurité totalement (détection, traitement, action finale) ou partiellement (le SIS assure par exemple la fonction de détection et de traitement jusqu'à une alarme, l'action finale peut ensuite être réalisée par une action humaine) (Le et Dianous, 2008). Dans ce cas, le SIS doit être appelé SAMS [Figure 5].

4.2 Cohabitation entre SIS et autre système de commande

La cohabitation entre le système de commande classique de la machine et le SIS mérite d'être regardée de plus près. Historiquement, le système de commande de la machine ne traitait pas les fonctions de sécurité qui étaient gérées par un système de sécurité séparé (CCPS, 1993). Aujourd'hui, avec l'évolution de la technologie et avec l'apparition de l'électronique programmable, la situation est moins tranchée.

Il arrive maintenant que des fonctions de sécurité ou le SIS partagent des capteurs ou des éléments finaux avec des boucles de régulations [Figure 10 et Figure 11]. Dans ces cas, la méthode LOPA indique que ces fonctions de sécurité ne peuvent pas être considérées comme une couche de protection indépendante (IPL), car elles partagent des éléments de la couche 2 (le capteur dans la figure 10 ou l'élément final dans la figure 11).

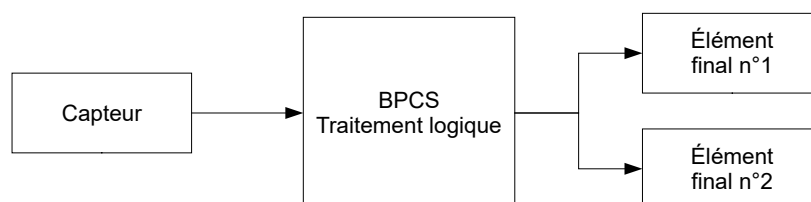


Figure 10. Capteur commun à la boucle de régulation et à la fonction de sécurité.

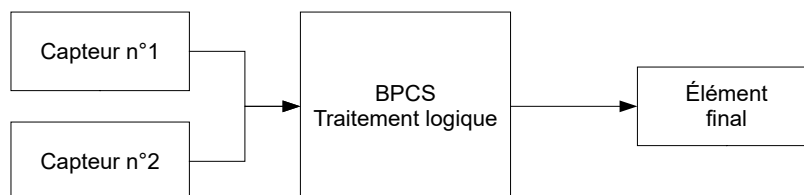


Figure 11. Élément final commun à la boucle de régulation et à la fonction de sécurité.

Par ailleurs, il arrive aussi que le traitement logique de plusieurs fonctions de sécurité soit effectué par une même unité ou que la même unité logique soit utilisée pour le traitement de boucles de régulation et pour le traitement de fonctions de sécurité [Figure 12]. Dans ce dernier cas, la méthode LOPA accepte cette architecture qui n'est pas strictement indépendante en réduisant l'effet du SIS compte tenu de l'utilisation de l'unité logique commune. Dans ce cas, le SIS ne pourra contribuer à la réduction du risque que d'un facteur 10 alors que s'il avait été indépendant, il aurait pu contribuer à la réduction du risque d'un facteur 100 ou plus.

D'un point de vue strictement fiabiliste, l'unité logique est responsable d'environ 1 % des défaillances (Iddir, 2012b). Dans le cas des procédés industriels, les capteurs seraient responsables de 35 % des défaillances dangereuses et les éléments finaux de 50% (Mesures, 2009a).

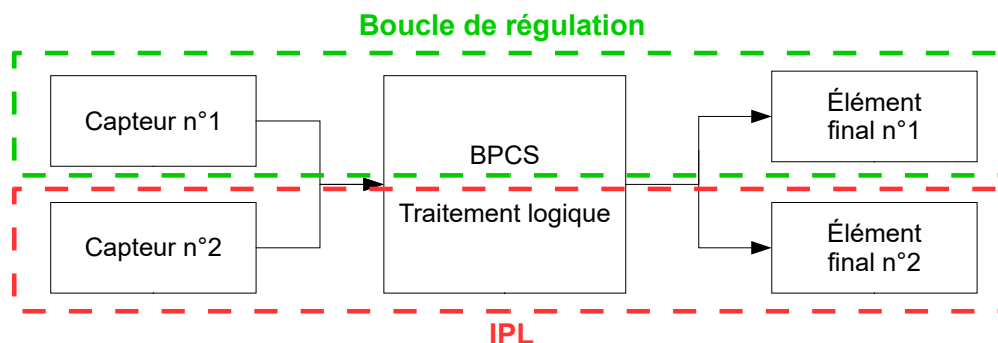


Figure 12. Capteurs et éléments finaux différents pour la boucle de régulation et l'IPL.

Au sujet de cette unité logique et des liens ou interfaces possibles entre le système de commande du procédé ou de la machine et le SIS, quatre écoles de pensée différentes (Mesures, 2009a ; Mesures, 2009b) coexistent :

- Le SIS et le système de commande sont communs : le SIS et le système de commande classique sont implémentés dans un même boîtier avec un programme unique ;
- Le SIS et le système de commande sont intégrés : deux boîtiers différents (ou deux programmes différents) traitent les deux fonctions (SIS et commande classique), mais fournis par un même fabricant qui peut utiliser des briques logicielles ou des éléments identiques dans les deux ;
- Le SIS et le système de commande sont interfacés : les deux systèmes sont différents et peuvent provenir de deux fournisseurs différents, mais ils dialoguent l'un avec l'autre via une passerelle ;
- Le SIS et le système de commande sont séparés : les deux systèmes sont totalement séparés et totalement indépendants l'un de l'autre. Il n'existe aucune communication entre les deux systèmes.

Chacune de ces solutions a des avantages et des inconvénients, du point de vue de la sécurité, comme cela est résumé dans le tableau 3. Du point de vue financier, des systèmes communs ou intégrés seront plus économiques que le système interfacé ou que les systèmes séparés compte tenu du partage d'informations possible, de la réduction du câblage et d'utilisation d'éléments identiques ou communs. Cependant, au début des années 1990, le CCPS (CCPS, 1993) indiquait dans une note de l'annexe B que rendre le SIS et le système de commande communs « ne donne pas le même degré de séparation que les techniques précédentes, et peut ne pas être acceptable pour les systèmes de plus haut niveau d'intégrité⁶ ». La norme CSA M421 (2011) mentionne, dans son annexe C non obligatoire, que deux automates programmables ou deux ordinateurs peuvent remplacer un contrôleur de sécurité mécanique et que l'un des automates ou ordinateurs peut aussi commander le treuil. Cette annexe mentionne aussi qu'il faut une séparation importante, tant physique que fonctionnelle, pour que les dispositifs soient réellement redondants.

⁶ This does not provide the same degree of separation as the previous techniques, and may not be acceptable for the highest integrity level systems.

Tableau 3. Avantages et inconvénients de la cohabitation SIS / autre système de commande

	Avantages / sécurité	Inconvénients / sécurité
SIS et système de commande communs	Dispositifs généralement certifiés par un organisme tiers (logique et logiciels).	La sécurité et le contrôle ne sont plus séparés : c'est une « boîte noire » pour l'utilisateur final. Une cause commune (eau, feu, choc...) peut entraîner la défaillance des deux systèmes. La gestion des modifications logicielles ou matérielles requiert plus d'attention.
SIS et système de commande intégrés	Présence de deux systèmes différents. Simplification du processus de gestion des modifications.	Une cause commune, matérielle ou logicielle, peut toujours entraîner la défaillance des deux systèmes.
SIS et système de commande interfacés	Le SIS peut dialoguer avec un autre système.	Une interface doit être développée pour le dialogue.
SIS et système de commande séparés	Aucune interférence possible d'un système à l'autre. Simplification du processus de gestion des modifications.	Le SIS doit être autonome (capteurs, logique, actionneurs) et son coût est plus élevé.

4.3 Normes applicables

Deux univers de normes internationales peuvent être utilisés pour dimensionner correctement un SIS associé à une machine d'extraction. Un troisième univers, canadien, peut aussi être utilisé pour compléter le dimensionnement.

D'un côté se trouve la norme **ISO 13849-1:2006** intitulée « *Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1: Principes généraux de conception* » (ISO 13849-1, 2006), encadrée par la norme de base en sécurité des machines, la norme de type A ISO 12100:2010 (ISO 12100, 2010). De l'autre côté se trouve la norme mère **CEI 61508** (IEC 61508, 2010) et les différentes normes filles dont deux sont pertinentes dans notre cas, la CEI 61511 (IEC 61511, 2003) pour le secteur des procédés industriels et la CEI 62061 pour les machines, cette dernière étant intitulée « *Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité* » (IEC 62061, 2005).

La norme ISO 13849-1 s'applique à tous les systèmes de commande de toutes les machines, alors que la CEI 62061 s'applique uniquement aux systèmes de commande de machines utilisant des systèmes électriques, électroniques ou électroniques programmables [Figure 13].

Pour sa part, la norme **CSA C22.2 No 0.8** « *Safety functions incorporating electronic technology* » peut aussi être utilisée pour concevoir les SIS (CAN/CSA C22.2 No 0.8-12, 2012). Par rapport aux normes CEI 61508, CEI 62061 et ISO 13849, elle est moins conceptuelle et elle se concentre sur des tests de sécurité normalisés pour les composants électroniques (comportement vis-à-vis des variations de tension, surtension, résistance aux champs magnétiques, etc.). La norme CSA

M421 (2011) peut aussi être consultée car l'article 6.9 traite spécifiquement des treuils de mines et du circuit de protection. Cependant, les notions de fiabilité des dispositifs électroniques sont reléguées à l'annexe C qui n'est pas normative.

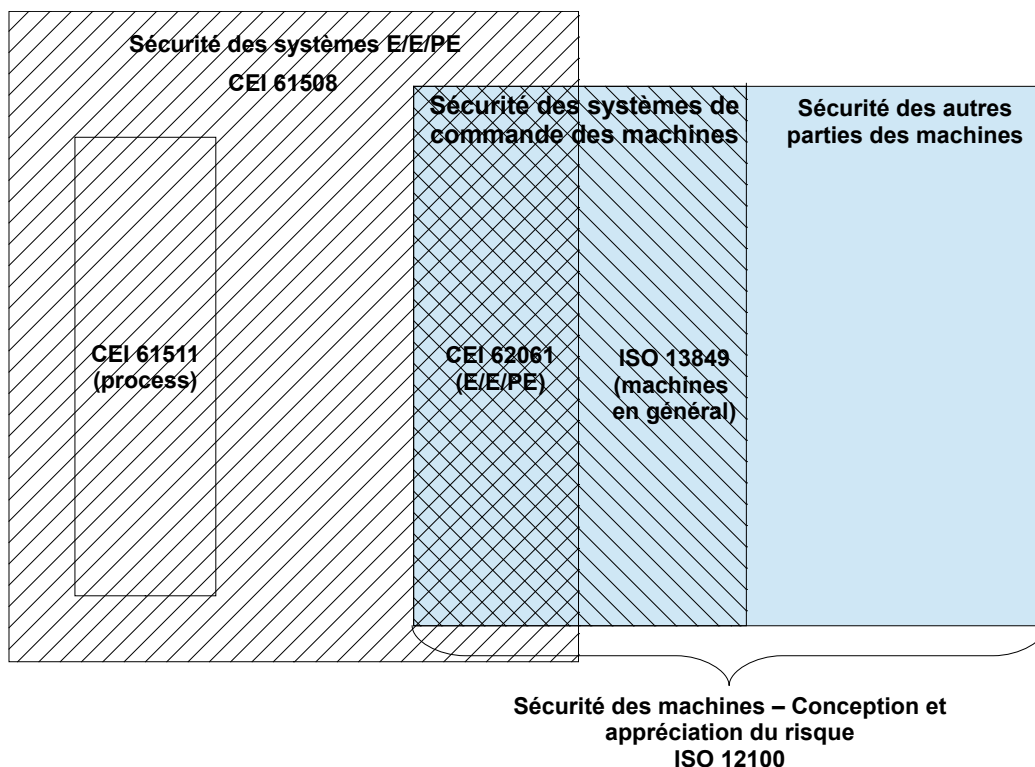


Figure 13. Domaine d'application des normes CEI et ISO.

4.3.1 ISO 13849 (systèmes de commande des machines)

Dans la norme ISO 13849, la capacité d'un SIS (SC/FS – Système de commande de la fonction de sécurité) à effectuer la fonction de sécurité est évaluée à travers le niveau de performance PL (5 niveaux de PLa à PLe) [Figure 14], ce qui est à peu près équivalent au niveau d'intégrité (SIL) dans la famille de normes CEI 61508. Le niveau de performance est déterminé *a priori*, lors de l'estimation de risque, qui permet de déterminer l'importance de la fonction de sécurité dans la réduction globale du risque (Beaudoin et Bello, 2013).

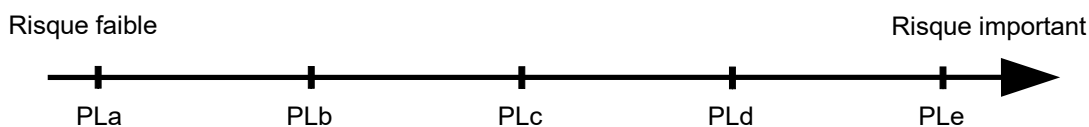


Figure 14. Niveaux de performance dans la norme ISO 13849.

Adaptée de « Aborder la norme NF EN ISO 13849-1 via la conception d'une fonction de sécurité basique », par J. Beaudoin et J.P. Bello, 2013. ©INRS, 2013.

Il faut faire attention pour le calcul du niveau de performance d'une fonction de sécurité intégrant plusieurs composants [Figure 15] (Beaudoin et Bello, 2013). Dans le cas où plusieurs parties d'un système de commande relatives à la sécurité (SRP/CS) sont utilisés en série, il faut définir le PL de chaque SRP/CS et ensuite le PL de du système de commande de la fonction de sécurité (SC/FS) globale. Globalement, le PL de la fonction de sécurité globale sera réduit, soit au niveau du PL le plus faible de la série [Figure 15 (a)], soit à un niveau inférieur si tous les PL sont égaux. La norme fournit un tableau qui permet d'estimer la baisse du niveau de PL selon la configuration. Par exemple, pour 4 SRP/CS de PLe en série, la SC/FS globale est alors de PLd [Figure 15 (b)]. Pour obtenir un résultat plus précis, il faut faire le produit de la fiabilité de chaque composant (fiabilité = 1 - probabilité de défaillances dangereuse), car la fiabilité d'un système série est égale au produit de la fiabilité des différents composants.

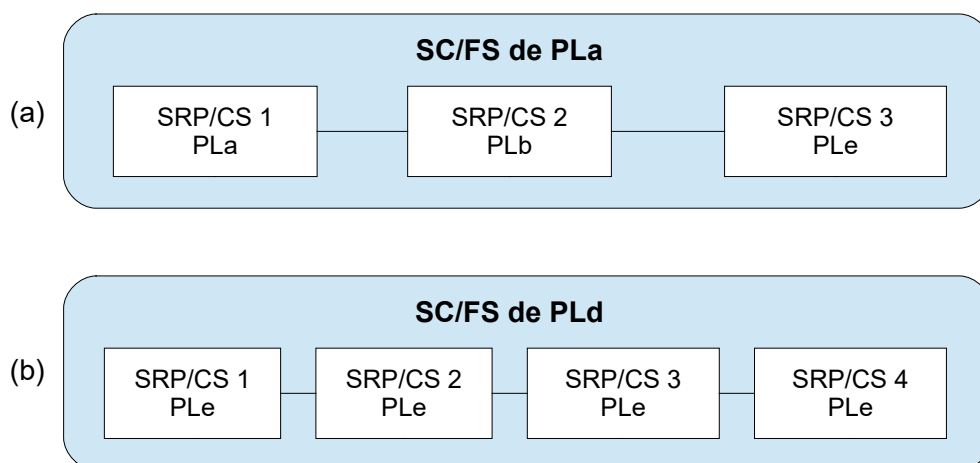


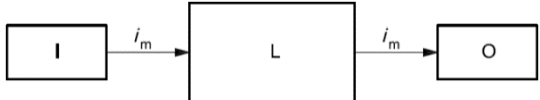
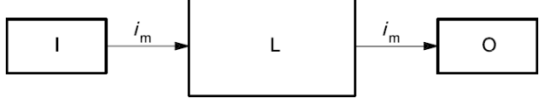
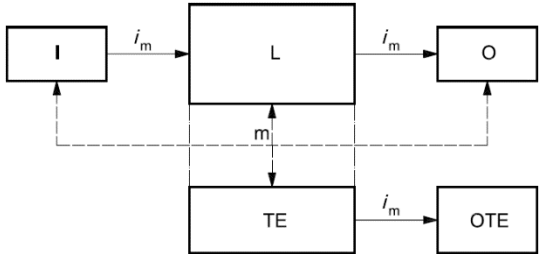
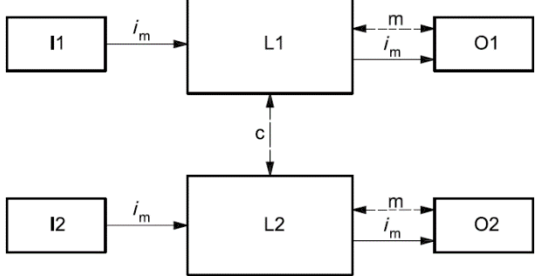
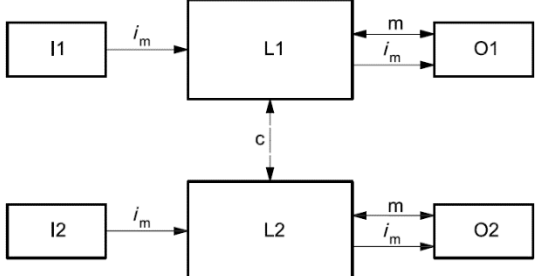
Figure 15. Calcul du niveau de performance d'une fonction de sécurité (SC/FS) incluant plusieurs composants (SRP/CS).

Adaptée de « Aborder la norme NF EN ISO 13849-1 via la conception d'une fonction de sécurité basique », par J. Beaudoin et J.P. Bello, 2013. ©INRS, 2013.

Différentes architectures de fonction de sécurité (catégories B, 1, 2, 3 et 4) sont proposées dans la norme et les exigences relatives à chaque catégorie sont détaillées [Tableau 4].

Tableau 4. Catégorie et architecture associée recommandée

Adapté de « Sécurité des machines -- Parties des systèmes de commande relatives à la sécurité -- Partie 1: Principes généraux de conception, ISO 13849-1:2006 », par International Organisation for Standardization, 2006. ©ISO, 2006.

Catégorie	Architecture associée recommandée	Caractéristiques principales
B		L'occurrence d'un défaut peut conduire à la perte de la fonction de sécurité. La sécurité est principalement assurée par la sélection des composants.
1		L'occurrence d'un défaut peut conduire à la perte de la fonction de sécurité, mais la probabilité de cette occurrence est plus faible que pour la catégorie B. La sécurité est principalement assurée par la sélection des composants.
2		L'occurrence d'un défaut peut conduire à la perte de la fonction de sécurité dans l'intervalle entre deux contrôles. La perte de la fonction de sécurité est détectée par le contrôle. La sécurité est principalement assurée par la structure de la fonction de sécurité.
3		Lorsqu'un défaut unique se produit, la fonction de sécurité est toujours assurée. Certains défauts sont détectés, mais pas tous. L'accumulation de défauts non détectés peut conduire à la perte de la fonction de sécurité. La sécurité est principalement assurée par la structure de la fonction de sécurité.
4		Lorsqu'un défaut unique se produit, la fonction de sécurité est toujours assurée. La détection de défauts accumulés réduit la probabilité de perte d'une fonction de sécurité (couverture DC élevée). Les défauts sont détectés à temps pour empêcher la perte de la fonction de sécurité. La sécurité est principalement assurée par la structure de la fonction de sécurité.

4.3.2 CEI 61508, 61511 et 62061

La CEI 61508 est une norme orientée « performances ». Ceci signifie que par opposition aux normes dites déterministes et prescriptives, c'est l'utilisateur qui, à travers son analyse et son évaluation du risque, détermine les performances à atteindre par son système E/E/PE concerné par la sécurité (ISA, 2005). La norme CEI 61508 est la norme « mère » et plusieurs normes sectorielles sont dérivées de la 61508 [Figure 16]. En effet, l'ISA rapporte que « L'IEC 61511

contient plus de renvois à l'IEC 61508 que de matière propre. L'IEC 61511 apporte surtout dans ses parties non normatives des réponses à des questions fréquentes » (ISA, 2005).

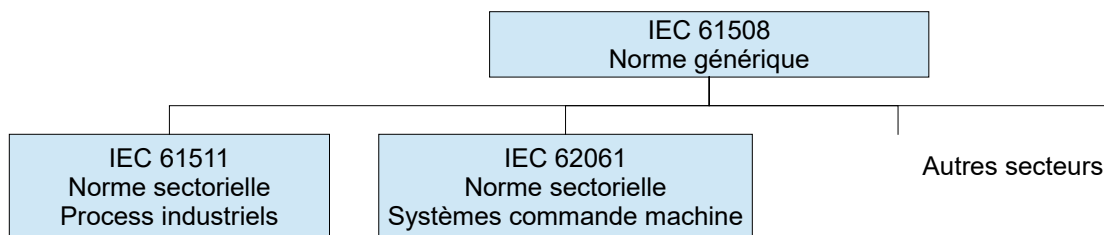


Figure 16. Structure normative.

Adaptée de « *Guide d'interprétation et d'application de la norme IEC 61508 et des normes dérivées IEC 61511 (ISA S84.01) et IEC 62061* », par *Instrumentation, Systems and Automation Society* 2005. ©ISA, 2005.

Le statut de la norme CEI 61508 lui permet d'être utilisée pour (ISA, 2005) :

- Disposer d'exigences génériques pour des systèmes E/E/PE concernés par la sécurité lorsqu'il n'existe aucune norme sectorielle ou produit, ou lorsqu'elles ne sont pas appropriées ;
- Les constructeurs de composants ou de sous-systèmes E/E/PE dans tous les secteurs (par exemple, matériel et logiciel pour capteurs, actionneurs intelligents, contrôleurs programmables) ;
- Les constructeurs / intégrateurs de systèmes pour atteindre les exigences des systèmes E/E/PE concernés par la sécurité ;
- Les utilisateurs pour spécifier les exigences en termes de fonctions de sécurité à réaliser ainsi que des performances de ces fonctions de sécurité ;
- Faciliter la maintenance des systèmes E/E/PE concernés par la sécurité au niveau d'intégrité de la sécurité "tel que construit" ;
- Fournir un cadre technique pour des services d'évaluation et de certification ;
- Disposer d'une base pour réaliser des évaluations des activités du cycle de vie de la sécurité.

Une des difficultés de la norme est que quelqu'un doit s'engager sur le risque tolérable. La norme CEI 61508 donne des balises sur le niveau minimum d'indépendance par rapport aux conséquences (dommage) possibles. Plus les conséquences sont graves, plus les exigences sur l'indépendance des décideurs doivent être grandes [Tableau 5]. Par exemple, pour des décès multiples ou une catastrophe (l'écrasement d'une cage transportant plus de 20 mineurs peut être considéré comme une catastrophe au même titre qu'une explosion dans une raffinerie), la norme recommande qu'une organisation indépendante soit responsable de l'évaluation de la sécurité fonctionnelle.

Tableau 5. Indépendance des personnes responsables de l'évaluation de la sécurité fonctionnelle des systèmes E/E/PE concernés par la sécurité

Adapté de « Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010 », par International Electrotechnical Commission, 2010. ©IEC, 2010.

Degré minimal d'indépendance	Conséquences			
	A	B	C	D
Personne indépendante	X	X1	Y	Y
Département indépendant		X2	X1	Y
Organisme indépendant			X2	X

Notes : Voir les paragraphes 8.2.15 à 8.2.17 pour les détails
A- blessure mineure temporaire, B- blessure permanente d'une ou plusieurs personnes, décès, C – décès multiples, D – très grand nombre de décès
X – niveau minimal, Y – insuffisant, X1 ou X2 – l'un ou l'autre, détailler et expliquer le choix (voir 8.2.16)

Les normes CEI 61508, 61511 et 62061 permettent de calculer les SIL des SIS (IEC 61511, 2003 ; IEC 61508, 2010). Il faut faire attention et ne pas confondre les méthodes pour calculer le SIL : la norme CEI 61508 s'adresse plutôt aux constructeurs de matériel, la norme CEI 61511 aux concepteurs et intégrateurs pour des processus industriels et la norme CEI 62061 s'adresse aux concepteurs ou intégrateurs des systèmes de commande E/E/PE relatifs à la sécurité pour les machines. De ce fait, pour une machine d'extraction utilisée dans une mine, c'est donc les normes CEI 61508 ou CEI 62061 qui s'appliquent. Cependant, la norme CEI 62061 ne considère pas le niveau SIL 4 qui existe dans la norme CEI 61508.

L'organisation de la norme CEI 61508 (IEC 61508, 2010) est présentée en figure 17.

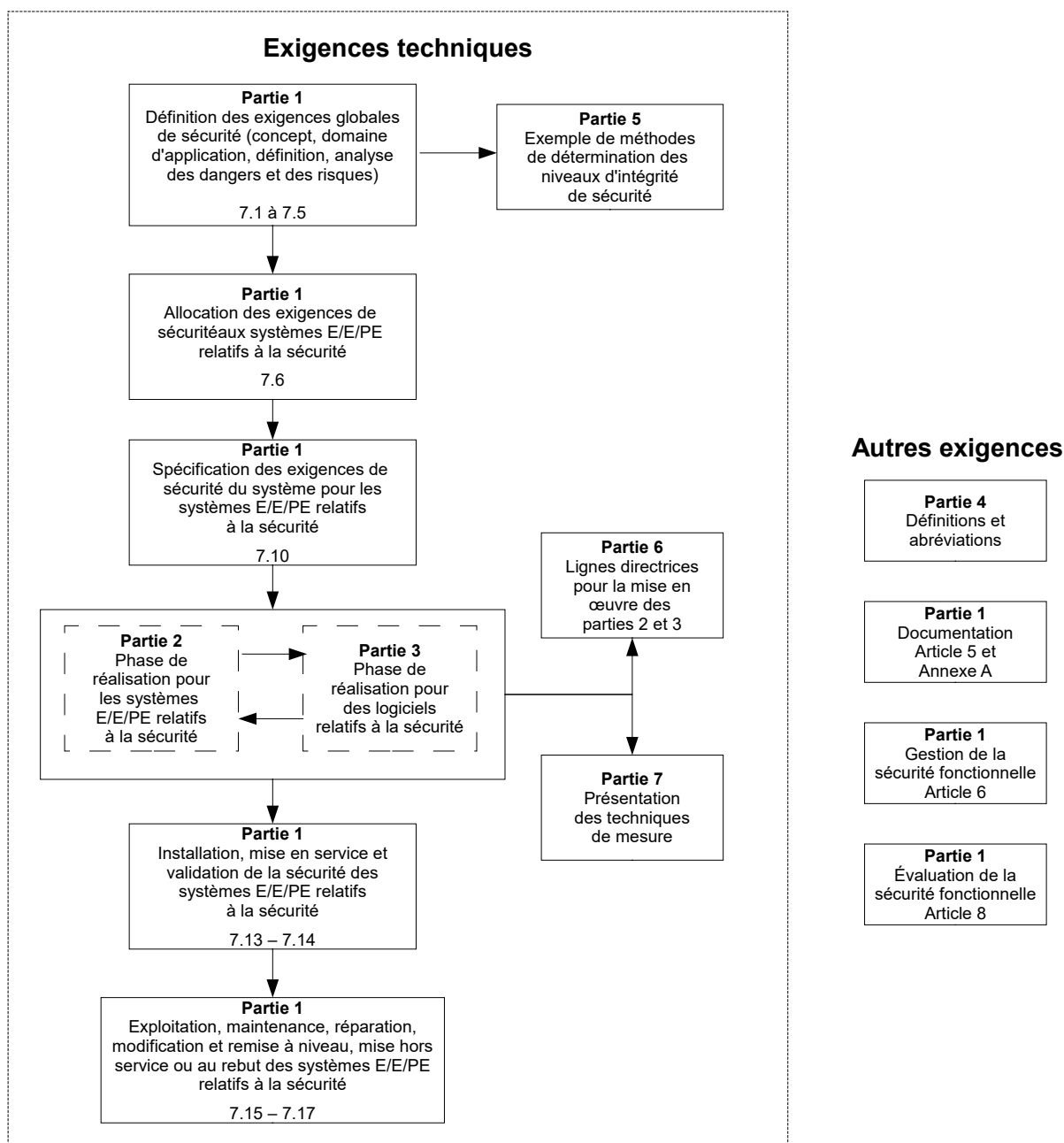


Figure 17. Organisation de la norme CEI 61508.

La CEI 61508 utilise un modèle global de cycle de vie de la sécurité [Figure 18] comme cadre technique pour les activités nécessaires pour garantir que la sécurité fonctionnelle est atteinte par les systèmes E/E/PE concernés par la sécurité (ISA, 2005).

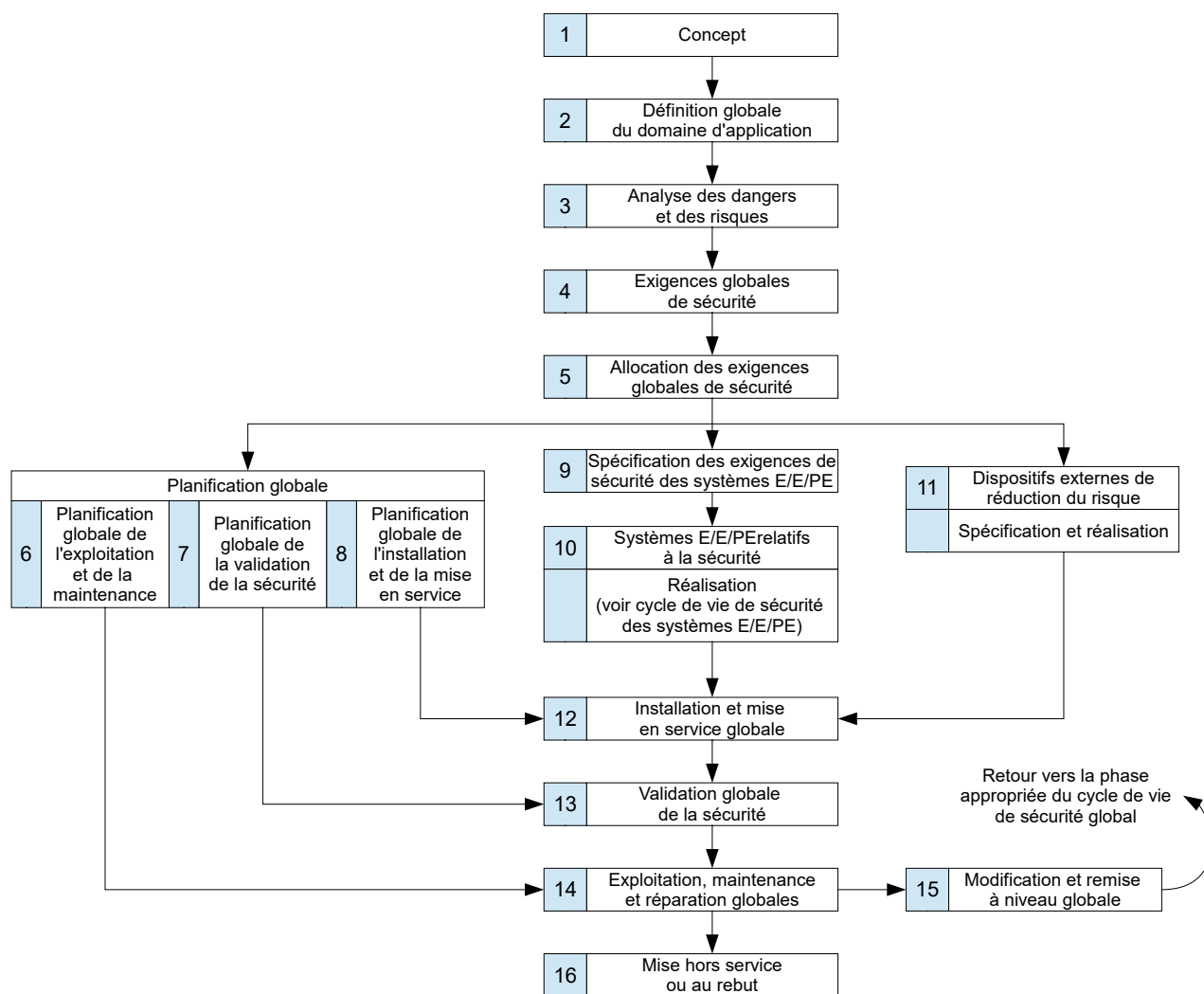


Figure 18. Cycle de vie global selon la CEI 61508.

4.3.3 Unification des deux normes

Entre 2012 et 2015, l'ISO et la CEI ont tenté de fusionner les deux normes ISO 13849 et CEI 62061 pour n'en donner qu'une seule numérotée temporairement ISO/IEC 17305 (ISO/TR 23849, 2010). Ceci posait certaines difficultés, car les niveaux d'intégrité de sécurité, notés SIL dans la CEI 61508, et les niveaux de performance, notés PL dans la 13849, ne sont pas de strictement équivalents. Il y a même des cas où ces niveaux de performance se contredisent parfois (Buchweiler, 2009) :

- À peu près moitié des cas : même niveau de SIL ;
- À peu près l'autre moitié : écart d'un niveau de SIL ;
- Quelques cas : écart de deux niveaux de SIL.

La conséquence est que cette divergence probable peut générer des conséquences dommageables pour la sécurité en diminuant le niveau de sécurité. La fusion de ces deux normes a été suspendu à la fin de l'année 2015 par les deux organismes.

4.4 Niveaux de contribution à la réduction du risque (SIL ou PL)

Pour identifier les SIS et définir leurs niveaux de contribution à la réduction du risque tel qu'illustré à la figure 6, il est nécessaire que les risques et leurs conséquences soient identifiés. Les données suivantes sont nécessaires (Adjadj et Charpentier, 2007 ; Lanternier et Adjadj, 2008) :

- Description des procédés et des installations ;
- Historiques des incidents et accidents répertoriés ;
- Identification et caractérisation des potentiels de dangers et estimation de leurs effets ;
- Analyses de risque réalisées.

La norme CEI 62061 conseille une méthodologie pour l'attribution des niveaux d'intégrité de sécurité (SIL) dans une annexe informative de la norme. Pour sa part, l'ISO 13849 indique qu'un niveau de performance requis PLr doit être déterminé et documenté, et réfère pour cela à des lignes directrices comprises dans une annexe, elle aussi informative.

4.4.1 Selon les normes CEI 61511 et CEI 62061

La norme CEI 61511 définit deux méthodes qualitatives pour déterminer le niveau de SIL : le graphe de risque et la grille de criticité (matrice probabilité/gravité). Il est aussi possible d'utiliser une méthode semi-quantitative, LOPA, pour déterminer la probabilité de défaillance du SIS.

La conception des SIS est fonction du niveau de SIL requis (Iddir, 2012a) et du mode de sollicitation du SIS [Tableau 6] : à faible sollicitation / à la demande (alarme de dépassement de niveau), ou à forte sollicitation / continu. Dans le premier cas, la demande doit être de l'ordre de 1 par année ou inférieure à la fréquence des tests périodiques afin de détecter une défaillance avant la survenue d'un événement dangereux. Dans le deuxième cas, le SIS est considéré répondre au critère de forte sollicitation lorsque la fréquence des demandes de fonctionnement est plus grande qu'une par an, ou supérieure à la fréquence des tests périodiques. Prenons un SIL 3 à faible sollicitation avec une probabilité de défaillance égale à $5 \cdot 10^{-4}$, ce même SIL3 lorsque considéré avec un mode de fonctionnement à forte sollicitation devra avoir une probabilité de défaillance de $5 \cdot 10^{-8}$ (soit 10 000 fois plus faible), car on considère une sollicitation à l'heure en

mode de fonctionnement à forte sollicitation et une sollicitation par an en mode à faible sollicitation.

Tableau 6. Définition des niveaux SIL selon le mode de sollicitation

Adapté de « *Évaluation de la probabilité de défaillance d'un Système Instrumenté de Sécurité (SIS)* », par O. Iddir, 2012. ©Techniques de l'ingénieur, 2012.

Niveau d'intégrité de sécurité	Probabilité de défaillance dangereuse par an	Facteur de réduction du risque
mode de fonctionnement à faible sollicitation		
SIL 1	10^{-1} à 10^{-2}	10 à 100
SIL 2	10^{-2} à 10^{-3}	100 à 1 000
SIL 3	10^{-3} à 10^{-4}	1 000 à 10 000
SIL 4	10^{-4} à 10^{-5}	10 000 à 100 000
mode de fonctionnement à forte sollicitation		
SIL 1	10^{-5} à 10^{-6}	10 à 100
SIL 2	10^{-6} à 10^{-7}	100 à 1 000
SIL 3	10^{-7} à 10^{-8}	1 000 à 10 000
SIL 4	10^{-8} à 10^{-9}	10 000 à 100 000

Dans le cas des machines d'extraction, un SIS qui est à faible sollicitation est par exemple l'évite-molette et le système de freinage associé alors qu'un SIS qui supervise la vitesse en fonction de la position de la cage est à forte sollicitation.

Pour les machines, la norme CEI 62061 conseille une méthodologie pour l'attribution des niveaux d'intégrité de sécurité (SIL). Cette méthode utilise quatre paramètres :

- La sévérité du dommage possible – Se ;
- La probabilité d'apparition du dommage – $CI = Fr + Pr + Av$, qui se décompose en trois autres paramètres :
 1. La fréquence et la durée de l'exposition – Fr,
 2. La probabilité d'apparition d'un événement dangereux – Pr,
 3. La probabilité d'évitement ou de limitation du dommage – Av.

Une fois Se et CI définis, une matrice permet d'identifier le niveau de SIL requis pour chaque fonction de sécurité (Buchweiler, 2008). Il faut noter que la norme CEI 62061 utilise les mêmes niveaux de SIL que la CEI 61511, mais le niveau SIL 4 n'existe pas dans la norme CEI 62061, comme si une machine ne pouvait pas créer de catastrophe équivalente à un procédé industriel. Or une machine d'extraction qui transporte 50 travailleurs et qui devient « folle » avec un arrêt d'urgence non fonctionnel peut créer une catastrophe équivalente à un procédé industriel.

4.4.2 Selon la norme ISO 13849-1

La norme ISO 13849-1 utilise cinq niveaux de performance (PL) qui sont définis en termes de probabilité de défaillance dangereuse par heure de la fonction de sécurité. Les cinq niveaux, numérotés de « a » à « e », sont basés sur une gamme de probabilités de défaillance dangereuse par heure [Tableau 7].

Tableau 7 . Niveaux de performance (PL)

PL	Probabilité moyenne d'une défaillance dangereuse par heure (1/h)
a	$\geq 10^{-5}$ à $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ à $< 10^{-5}$
c	$\geq 10^{-6}$ à $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ à $< 10^{-6}$
e	$\geq 10^{-8}$ à $< 10^{-7}$

Cependant, la norme ISO 13849-1 indique qu'il ne faut pas uniquement considérer la probabilité moyenne de défaillance dangereuse par heure pour obtenir le niveau de performance « associé » : il faut aussi considérer, par exemple, les défauts systématiques, les défaillances de causes communes, la couverture de diagnostic, etc.

Comme pour la norme CEI 62061, le niveau de performance requis (PLr) est fonction de l'importance du SIS à la réduction du risque pour une fonction de sécurité donnée. La norme indique que le PLa est principalement utilisé dans le cas d'un dommage faible et réversible.

4.4.3 Équivalence SIL et PL

Il est possible de comparer les niveaux de SIL et de PL des deux référentiels précédents [Tableau 8] (ISO/TR 23849, 2010). Cependant, cette équivalence n'est pas parfaite, car pour une fonction de sécurité fortement sollicitée (en mode continu), l'équivalence entre les probabilités de défaillance dangereuses par année et par heure est basée sur 10 000 heures de fonctionnement par an. Or une année calendaire correspond à environ 8766 heures en moyenne⁷, ce qui entraîne une différence de l'ordre de 14 %.

La norme ISO 13849-1 (4.5.1) indique qu'il n'y a pas d'équivalence entre le SIL 4 et un niveau PL. La justification donnée est que le niveau SIL 4 est réservé aux « événements catastrophiques » possibles dans l'industrie de transformation, et que cette échelle n'est donc pas pertinente pour traiter des risques machines. Or, comme mentionné précédemment dans la section 3.4.1, l'écrasement d'une cage avec le maximum de personnes autorisé à l'intérieur risque d'être perçu dans la société comme un « événement catastrophique ».

Tableau 8. Équivalence SIL et PFHD

Niveau d'intégrité de sécurité (SIL) CEI 61508	Probabilité de défaillance dangereuse par an	Probabilité de défaillance dangereuse par heure (PFHD)	Niveau de performance (PL) ISO 13849
-	-	10^{-5} à 10^{-4}	a
SIL 1	10^{-1} à 10^{-2}	3×10^{-6} à 10^{-5}	b
SIL 1	10^{-1} à 10^{-2}	10^{-6} à 3×10^{-6}	c
SIL 2	10^{-2} à 10^{-3}	10^{-7} à 10^{-6}	d
SIL 3	10^{-3} à 10^{-4}	10^{-8} à 10^{-7}	e
SIL 4	10^{-4} à 10^{-5}	10^{-9} à 10^{-8}	-

⁷ L'année tropique a une durée estimée de 365 jours 5 heures 48 minutes 45,25 secondes.

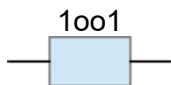
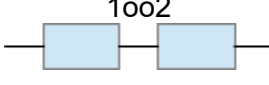
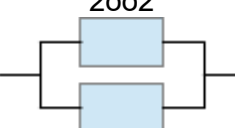
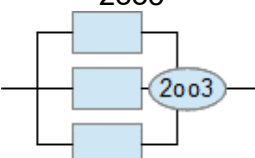
4.4.4 Influence de l'architecture du SIS sur la fiabilité et la disponibilité

Comme cela est mentionné explicitement dans la norme ISO 13849-1 et dans la norme CEI 62061, l'architecture de la fonction de sécurité influence la fiabilité de la fonction de sécurité et donc le niveau de contribution à la réduction du risque (SIL ou PL). Plusieurs architectures typiques sont recensées dans la littérature [Tableau 9] dont les systèmes en série, les systèmes en parallèle et les systèmes K parmi N (KooN). Dans ce dernier cas, la fonction n'est assurée que si K des N éléments sont fonctionnels. Globalement, les systèmes en série améliorent la fiabilité de la fonction alors que les systèmes en parallèle améliorent la disponibilité du système.

Une autre information doit être prise en compte : est-ce que l'élément final sera actionné par la coupure de l'alimentation (*deenergized to trip*) ou par une mise en alimentation (*energized to trip*) (CCPS, 1993). Le premier cas est représentatif des fonctions d'arrêt d'urgence sur les machines et est compatible avec le principe « *fail safe* ».

Tableau 9. Comparaison des architectures 1oo1, 1oo2, 2oo2, et 2oo3

Adapté de « *Évaluation de la probabilité de défaillance d'un Système Instrumenté de Sécurité (SIS)* », par O. Iddir, 2012. ©Techniques de l'ingénieur, 2012.

Architecture	Disponibilité	Sécurité
 <p>1oo1</p>	<p>La défaillance non dangereuse de l'élément entraîne un déclenchement intempestif</p> $P_{dnds} = P_{dnd}$	<p>Une défaillance dangereuse suffit pour que le système ne puisse pas remplir sa fonction</p> $P_{dds} = (P_{dd})$
 <p>1oo2</p>	<p>La défaillance non dangereuse de l'un des deux éléments entraîne un déclenchement intempestif</p> $P_{dnds} = 2 \times P_{dnd}$	<p>Deux défaillances dangereuses sont nécessaires pour que le système ne puisse pas remplir sa fonction</p> $P_{dds} = (P_{dd})^2$
 <p>2oo2</p>	<p>La défaillance non dangereuse des deux éléments est nécessaire pour observer un déclenchement intempestif</p> $P_{dnds} = (P_{dnd})^2$	<p>La défaillance dangereuse de l'un des deux éléments suffit pour que le système ne puisse pas remplir sa fonction</p> $P_{dds} = 2 \times P_{dd}$
 <p>2oo3</p>	<p>La défaillance non dangereuse de deux éléments sur trois est nécessaire pour observer un déclenchement intempestif</p> $P_{dnds} = 3 \times (P_{dnd})^2$	<p>Deux défaillances dangereuses sont nécessaires pour que le système ne puisse pas remplir sa fonction</p> $P_{dds} = 3 \times (P_{dd})^2$

Pdd : Probabilité de défaillance dangereuse d'un élément

Pdds : Probabilité de défaillance dangereuse du système

Pdnd : Probabilité de défaillance non dangereuse d'un élément

Pdnds : Probabilité de défaillance non dangereuse du système

Prenons un exemple de fonction de sécurité : « déclenchement d'un parachute amélioré ».

Le rôle des capteurs est de mesurer la tension dans le câble. Une unité de traitement analyse ensuite l'information envoyée par les capteurs et en deçà d'une certaine valeur, déclenche le parachute.

Défaillance dangereuse : le capteur indique une tension à l'attache alors qu'il n'y en a plus.

Défaillance non dangereuse : le capteur indique une tension nulle à l'attache alors qu'il y en a une.

Bien que certaines architectures permettent d'obtenir des fonctions de sécurité plus tolérantes aux défaillances, il faut faire attention aux défaillances de cause commune :

- Les erreurs logicielles ;
- Les agressions par le milieu naturel (rouille, mouvement de terrain, présence d'eau, températures extrêmes, etc.) ;
- Les perturbations engendrées par le milieu (colmatage des prises d'impulsion de capteurs par exemple) ;
- Les erreurs de maintenance ;
- Etc.

En effet, une des hypothèses utilisées dans le calcul de la fiabilité des systèmes est que les défaillances sont indépendantes les unes des autres et que deux défaillances ne peuvent pas survenir au même instant. Or plusieurs défaillances de cause commune peuvent apparaître dans un SIS si cela n'a pas été pris en compte lors de la conception. Par exemple, la conjugaison d'humidité, de chaleur et d'acidité peut entraîner la formation accélérée de rouille sur des capteurs ou des actionneurs et la défaillance simultanée de plusieurs composantes du SIS. De plus ce n'est pas parce que tous les composants d'une fonction de sécurité sont certifiés SIL 2 que cette fonction de sécurité sera de niveau SIL 2 (Mesures, 2009c).

« Un système E/E/PE concerné par la sécurité contient habituellement plusieurs fonctions de sécurité. Si les exigences d'intégrité de la sécurité pour ces fonctions de sécurité diffèrent, alors les exigences applicables au niveau d'intégrité de la sécurité le plus élevé s'appliquent à l'intégralité du système E/E/PE concerné par la sécurité, sauf si l'implémentation garantit une indépendance suffisante entre les fonctions de sécurité (ce qui doit être démontré). » (ISA, 2005)

4.5 SIS des machines d'extraction

En ce qui concerne les machines d'extraction, les SIS sont implicitement présents dans la réglementation de plusieurs provinces ou états, par exemple lorsqu'il est mentionné que la machine doit être arrêtée automatiquement si certaines limites sont dépassées. Ils sont aussi explicitement mentionnés à l'article 6.9.3 et implicitement mentionnés dans l'annexe C de la norme CSA M421 (2011).

La réglementation la plus explicite est celle du New South Wales (NSW, 2006 ; NSW, 2007) qui indique que des programmes de gestion des risques électriques et mécaniques doivent « fournir des protections pour les phénomènes dangereux électriques ou non électriques, avec une probabilité de défaillance appropriée au degré de risque des phénomènes dangereux⁸ ». Le

⁸ Clause 13 (1) ...

gouvernement du New South Wales a publié en 2007 une note d'interprétation et en 2011 une référence technique préliminaire (NSW, 2011) pour la conception des machines d'extraction. Cette dernière référence technique est essentiellement basée sur la norme CEI 61508.

Pour ce qui est du Canada, les SIS sont implicitement mentionnés dans plusieurs réglementations provinciales ou fédérales, par exemple :

- le Health, Safety and Reclamation Code for Mines in British Columbia de 2008, mentionne à l'article 7.6.8 intitulé Protective Circuits and Hoist Safety Devices que « [...] (2) The track limit switch shall be installed in each shaft hoisting compartment above the normal upper limit of travel, and so arranged and positioned that in the event of an overwind it will be operated directly by the shaft conveyance or counterweight to interrupt the hoist safety circuit and bring the hoist to a safe stop. » ;
- Le Règlement sur la santé et la sécurité dans les mines de charbon (DORS/90-97) mentionne à l'article 65. (1) que « La machine d'extraction de surface doit être conforme aux normes suivantes : [...] e) la machine d'extraction doit être munie d'évite-molettes et d'un régulateur de vitesse qui coupent le courant et actionnent le système de freinage lorsque la cage ou le convoi (i) soit dépasse une des extrémités de la course, (ii) soit se déplace à une vitesse supérieure à la vitesse maximale indiquée dans les procédures visées au paragraphe 59(1) » ;
- Au Manitoba, le Règlement sur l'exploitation minière de la Loi sur la sécurité et l'hygiène du travail mentionne à l'article 30.2(1) intitulé Dispositifs de sécurité — décélération et immobilisation que « Les employeurs veillent à ce que les appareils de levage soient munis des dispositifs de sécurité énumérés ci-dessous qui amorceront une décélération automatique et immobiliseront l'appareil en toute sécurité suivant toutes les conditions permises de charge, de direction de parcours ou de vitesse, avant que l'appareil de transport, le contrepoids ou leur attelage de câble ne puissent atteindre un obstacle permanent : a) des dispositifs d'évite-molettes et de limite inférieure du trajet [...]; c) des dispositifs limiteurs de vitesse s'enclenchant lorsque celle-ci dépasse de 12 % la vitesse maximale autorisée du câble [...]. » ;
- etc.

Les réglementations provinciales relatives aux SIS seront détaillées et comparées dans la mise à jour de la fiche technique RF-412.

Pour le Québec, l'article 233 du RSSM, qui indique les différentes conditions d'arrêt immédiat de la machine d'extraction, décrit par la même occasion les fonctions de sécurité du SIS correspondant.

-
- (e) **an electrical engineering management plan** covering the life cycle of electrical plant and installations, and electrical engineering practices, at the coal operation, that is developed, implemented and periodically reviewed through consultation with a qualified electrical engineer, to control risks as follows: ... (v) to provide electrical safeguards for electrical and non-electrical hazards, with a probability of failure appropriate to the degree of risk posed by the hazard, ...
 - (f) **a mechanical engineering management plan** covering the life cycle of mechanical plant and installations, and mechanical engineering practices, at the coal operation, that is developed, implemented and periodically reviewed through consultation with a qualified mechanical engineer, to control risks as follows: ... (viii) to provide safeguards for mechanical plant and installations, with a probability of failure appropriate to the degree of risk posed by any mechanical plant or installation, ...

Machine visée : Une machine d'extraction électrique

Action requise : l'alimentation du moteur de la machine *doit être* supprimée et la force de freinage nécessaire pour immobiliser la machine *doit être* appliquée automatiquement

Conditions :

- Lorsqu'un interrupteur d'urgence est en position ouverte ;
- Lorsque le transporteur ou le contrepoids circule au-delà d'un interrupteur évite-molette ou au-delà des interrupteurs de limite supérieure ou inférieure de parcours et ce, avant que le transporteur, le contrepoids ou les attaches de câbles puissent atteindre la molette ou tout autre obstacle dans le puits ou le chevalement ;
- Dans le cas d'une panne de l'alimentation électrique de la machine d'extraction ;
- Dans le cas où un limiteur de vitesse entre en action ;
- Lors d'une chute de tension préétablie ;
- Lorsqu'il survient un courant de surcharge qui dépasse, d'un pourcentage préétabli, le courant requis pour les opérations normales d'extraction ;
- Au cas d'un court-circuit dans l'installation électrique de la machine ;
- Avant que toute partie du mécanisme de commande d'un frein n'atteigne sa limite de course lors de l'application du frein.

4.6 L'élément terminal du SIS : le frein de treuil ou de câble

En règle générale, deux systèmes de freinage indépendants doivent être présents sur les machines d'extraction, chacun pouvant arrêter la cage tout en contrôlant la décélération (Galloway et Tiley, 1986). Ces freins assurent deux fonctions : freinage de service et freinage d'urgence. Ces systèmes de freins sont généralement dimensionnés pour retenir deux fois la charge maximale statique au fond du puits, afin de permettre des évolutions du puits et prendre en compte une perte de performance⁹ (Galloway et Tiley, 1986). En termes de décélération, une personne en bonne santé peut subir sans problèmes des décélérations de 20 ft/s² (0.6 g). Les guides du New South Wales¹⁰ (R-NSW, 2011a ; R-NSW, 2011b ; R-NSW, 2011c) contiennent beaucoup d'information sur les tests de freinage.

4.6.1 Freins du treuil (tambour / disque)

Les freins de treuil, généralement mécaniques, ont deux fonctions (ABB, 2014 ; Barkand, 1992b ; Galloway et Tiley, 1986) :

- Amener la cage à l'arrêt complet en utilisation courante. Le frein est alors enclenché à faible vitesse (ou à l'arrêt) ;
- Arrêter rapidement la cage dans les situations d'urgence. Le frein est alors enclenché à grande vitesse.

⁹ Selon l'article 225 du RSSM, il faut vérifier au début de chaque quart de travail que chacun des moyens de freinage est en mesure de retenir la charge maximale.

¹⁰ Certains guides ont été mis à jour : voir le lien Internet suivant pour plus de détails -

<https://www.resourcesregulator.nsw.gov.au/safety-and-health/applications/registration-and-licensing>

La difficulté lors de la conception du système de freinage mécanique d'une machine d'extraction consiste à choisir une capacité de freinage suffisante pour une utilisation à pleine charge sans pour autant engendrer des arrêts trop brutaux lorsque la cage a peu de travailleurs (Barkand, 1992b). En effet, dans le premier cas, c'est le coefficient de friction dynamique qui est important alors que dans le second cas, c'est le coefficient de friction statique ou quasi-statique qui est important. Enfin, pour la majorité des couples de matériaux, le coefficient de friction statique est plus grand que le coefficient de friction dynamique, ce qui peut entraîner du broutement lors de l'arrêt.

Les premiers systèmes de freinages mécaniques étaient des freins à tambour fonctionnant généralement à l'air comprimé ou avec de l'huile sous pression (ABB, 2014). Aujourd'hui des systèmes de freins hydrauliques à disque sont utilisés pour les nouvelles installations (Leonida, 2013). Il est aussi possible de mettre en place des systèmes de freinage qui contrôlent la décélération (ABB, 2014 ; Sparg, 1995) en fonction d'un certain nombre de paramètres.

4.6.2 Frein de câble

La première mise en place de frein sur le câble unique d'une machine d'extraction à tambour remonte à 1992 aux États-Unis (Barkand, 1992b ; Barkand, 2002). Ce type de frein secondaire est plutôt utilisé sur les machines à friction multicâbles et est utile pour éviter les accidents d'écrasement de la cabine au niveau du chevalement. Bien que ce type de freins soit efficace, l'autorité de sécurité minière de Pennsylvanie a refusé d'approuver son installation pour les câbles uniques, du fait de l'usure très marquée des garnitures de frein (Barkand, 2002).

Par ailleurs, sur les machines à tambour, les câbles sont régulièrement lubrifiés, ce qui peut allonger la distance de freinage. Par contre, sur les machines d'extraction à friction comportant plusieurs câbles, les freins de câble ont été testés avec succès (Barkand, 1990 ; Barkand, 1992a).

4.7 Recommandations

Afin d'améliorer la performance des systèmes instrumentés de sécurité, nous formulons les recommandations suivantes. Il appartiendra au législateur de considérer si tout ou partie de ces recommandations doivent être intégrés dans les textes de loi, et aux industriels de mettre en place certaines de ces recommandations s'ils les jugent pertinentes. Les recommandations sont présentées en ordre séquentiel sans organisation par niveau d'importance.

Recommandation 4.1 :

Qu'un organisme collige systématiquement toutes les informations relatives à un incident touchant une machine d'extraction ou son système de commande, synthétise ces données et les rende disponibles au secteur minier québécois afin d'améliorer la connaissance des taux de défaillance, dangereuse ou non, des éléments d'un SIS. (Ce principe de recueil de données existe déjà en Colombie-Britannique - article 7.9.20 intitulé *Record of Electrical Failures and Accidents* - ainsi qu'au Nouveau-Brunswick - NB, article 254).

Recommandation 4.2 :

Que les SIS d'une machine d'extraction soient conçus selon les exigences des normes CEI 61508 et CEI 62061 (ou ISO 13849-1), ou minimalement en intégrant les prescriptions de l'article 6.9.3 et en tenant compte de l'annexe C de la norme CSA M421 (2011).

Recommandation 4.3 :

Qu'une analyse de risque écrite et documentée soit réalisée avant la mise en service d'une nouvelle machine d'extraction ou lors d'une modification de la machine. Cette exigence est pour l'instant optionnelle dans la fiche technique RF-412 (3.2.4), mais est nécessaire dans la mise à jour publiée en 2019 sous le sigle RF-1049 (Giraud *et al.*, 2019).

5. COUCHE 4 – SÉCURITÉ LOGICIELLE

De plus en plus de SIS intègrent des API ou des API de sécurité qui eux-mêmes font appel à de l'électronique programmable. Les machines ou les systèmes industriels passent de fonctions de sécurité réalisées par de la logique câblée à des automates de sécurité pour de multiples raisons, tant financières que de mise à niveau ou de maintenance.

Or le logiciel « zéro défaut » n'existe pas. La présence de fautes logicielles systématiques, introduites à la conception d'un dispositif programmé, doit donc être considérée avec beaucoup d'attention, en particulier lorsque les conséquences de ces fautes peuvent influencer sur la sécurité d'un dispositif complexe (Charpentier *et al.*, 2000). La CEI 61508-3 exige une combinaison d'approches : un processus d'assurance qualité visant à éviter les anomalies et l'adoption d'architectures du logiciel tolérant les anomalies (IEC 61508, 2010). La prochaine loi sur les ingénieurs devrait apporter un éclairage quant aux responsabilités d'un ingénieur en charge de la conception d'une machine commandée par un automate.

Pour que le logiciel soit sécuritaire, il faudrait (Charpentier *et al.*, 2000) :

- Prévenir les fautes (se fait lors de la conception) ;
- Que le logiciel puisse tolérer les fautes (lorsqu'elles surviennent) ;
- Éliminer les fautes (lors des étapes de vérification du code) ;
- Prévoir les fautes : « La prévision des fautes est destinée à s'assurer que les techniques de tolérance et d'élimination mises en œuvre ont l'efficacité souhaitée ».

L'approche de la CEI 61508 présente certaines faiblesses dans le domaine logiciel (ISA, 2005). Cependant c'est la norme de référence, car même la norme ISO 13849-1 :2006 s'y réfère, par exemple dans le cas de la contribution du logiciel pour l'atteinte du plus haut niveau de sécurité, le PL_e.

5.1 Exemples de défaillances logicielles

Cette section présente des exemples concrets de défaillance logicielle avec des conséquences négatives en termes de sécurité pour les utilisateurs finaux ou pour les travailleurs :

- Therac-25 (Levenson et Turner, 1993) ;
- Système de contrôle électronique du papillon des gaz sur la Toyota Camry 2005 (*Electronic Throttle Control System*, ETCS) (Barr, 2012) ;
- Accident Blanchette & Blanchette inc. (2000), enquêtés par la CSST (CSST, 2002) ;
- Accident Kruger/Wayagamak inc. (2004), enquêté par la CSST (CSST, 2004).

Dans ces deux derniers cas, la modification du logiciel, bien qu'écartée des causes de l'accident, nous semble être un des éléments qui a concouru à l'accident. Outre ces accidents, le livre *Out of Control* du HSE (2003) répertorie d'autres cas d'accidents liés à la sécurité logicielle ou plus largement à la sécurité d'un PES (*Programmable electronic system*) de commande.

5.1.1 Therac-25

À la fin des années 1980, le Therac-25, une machine de radiothérapie contrôlée par ordinateur construite à 11 exemplaires, a conduit 6 personnes à des overdoses massives de radiation (Levenson et Turner, 1993). Deux patients en sont décédés.

Contrairement au Therac-20 son prédécesseur, le Therac-25 repose sur son logiciel pour le contrôle (alors que le Therac-20 n'utilisait l'ordinateur que pour faciliter la manipulation, mais aurait pu être opéré entièrement à la main). Par ailleurs, le logiciel du Therac-25 est également responsable de fonctions de sécurité comme le contrôle du flux d'électrons ou photons (Levenson et Turner, 1993). Le contrôle et la sécurité sont donc communs.

L'ordinateur prend en charge le positionnement de la table tournante (pour cibler précisément la zone à traiter), et gère aussi l'alignement du filtre atténuateur et de la chambre à rayon X. Traditionnellement, il y a un système d'interverrouillage électromécanique pour s'assurer que tous les éléments sont alignés. Quand le système a été mis en œuvre, les opérateurs se sont plaints du temps nécessaire pour remplir les champs d'identification du patient. En réponse, le développeur (Énergie Atomique du Canada limitée) a permis un remplissage à partir de la dernière utilisation, ce qui a été retrouvé dans plusieurs accidents. Par ailleurs, des messages d'erreur non expliqués s'affichaient régulièrement à l'écran, et les opérateurs finissaient par les ignorer. L'analyse de risque avait été faite en construisant un arbre de défaillance, mais en ignorant complètement la partie logicielle.

À la suite de ces accidents, des problèmes ont aussi été trouvés dans le logiciel du Therac-20, mais aucun dommage n'était survenu en raison des interverrouillages physiques de sécurité (couche 5 LOPA) qui avaient joué leur rôle. Une des façons de contrer ce type de défaillance est d'effectuer une analyse transitoire ou une analyse de conditions insidieuses (*Sneak analysis ou Sneak circuit analysis*), analyse qui peut permettre de détecter une condition insidieuse matérielle, logicielle ou intégrée latente, pouvant être à l'origine d'un événement indésirable sans défaillance d'un élément (IEC/ISO 31010, 2009, Annexe B23).

Les causes

- Trop de confiance accordée au logiciel (« un ordinateur ne fait pas d'erreurs »). La défaillance dangereuse de l'ordinateur pour « Computer selects wrong energy » était de 1×10^{-11} et celle pour « Computer selects wrong mode » était de 4×10^{-9} , mais sans justification ;
- Confondre la fiabilité et la sécurité : le logiciel à beau fonctionner des dizaines de milliers de fois sans erreur, ce n'est pas pour autant qu'elles ne peuvent pas survenir ;
- Le logiciel n'avait pas de modules de détection et de gestion d'erreurs. Les réactions du patient étaient les seuls indices du mauvais fonctionnement de la machine, il n'y avait pas de systèmes de vérification dans le Therac-25 (pour le dosage, au-delà d'un certain seuil le capteur saturait et indiquait que la dose était trop faible) ;
- Des protections contre les erreurs logicielles devraient être mises en place dans le logiciel et dans le système en général ;
- Une des causes des multiples accidents est un manque d'enquête approfondie après chacun des accidents ;
- L'illusion de la sécurité, due à un grand nombre d'années sans incident dans ce secteur particulier ;

- Analyse de risque irréaliste : tout d'abord sans considérer la partie logicielle, puis seulement de manière superficielle ;
- Pratiques de développement de code inadéquates :
 - Les spécifications et la documentation du logiciel ne devraient pas être négligées,
 - Des normes de qualité et de sécurité sur les logiciels devraient être établies et utilisées,
 - Des moyens de détecter les erreurs devraient être mis en place dans le code source dès le départ,
 - Le logiciel devrait être testé dès le développement et il ne fallait pas se limiter uniquement aux tests du système final,
 - L'interface utilisateur, en particulier les messages d'erreur, et la documentation devraient faire l'objet d'un soin particulier,
 - Le design devrait être le plus simple possible pour ce type de code qui est relatif à la sécurité, tel quel il n'était presque pas testable,
- Réutilisation de code (du Therac-6 et du Therac-20). L'utilisation de code commercial « *off the shelf* » peut également être dangereuse. Recoder complètement le logiciel peut être plus sûr dans bien des cas ;
- Adopter des interfaces sécuritaires en priorité, la facilité d'utilisation est secondaire.

5.1.2 ETCS Toyota Camry 2005

Le code du système de contrôle du papillon des gaz (ETCS) des Toyota Camry 2005 a été étudié en détail par la National Aeronautics and Space Administration (NASA) et par le Barr Group à la suite de plusieurs accidents ayant impliqué des conducteurs dont le véhicule accélérât tout seul.

Parmi les éléments dangereux repérés par le Barr Group ou la NASA, on note (Barr, 2012) :

- Certaines des variables ne sont pas protégées contre la corruption (absence de stockage en miroir, aucune protection matérielle contre les changements de bits) ;
- Il y a des sources de corruption de la mémoire (dépassement de capacité de la mémoire dû à un mauvais dimensionnement, bogues dans le code).

Par ailleurs, le processeur de sécurité gère plusieurs tâches en parallèle : certaines sont menées de front, d'autres sont mises en queue le temps que la tâche précédente soit traitée. Barr (2012) met en évidence qu'un changement de bit mal placé peut, non seulement stopper une tâche, mais éliminer toute la queue des tâches qui devaient être exécutées ensuite.

Ces erreurs sont en partie dues à ce que Barr appelle le « code spaghetti » : code complexe sans nécessité apparente et présentant un haut niveau de couplage entre les différents modules. Outre la difficulté à identifier les sources d'erreurs dans ce type de code, son maintien et sa mise à jour sont nettement plus compliqués. Le code ne répondait pas aux normes sur le code informatique, notamment OSEK (*Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug* - Systèmes ouverts et interfaces correspondantes pour l'électronique des véhicules automobiles), ou MISRA C, développée par la *Motor Industry Software Reliability Association* pour le langage C.

Il est possible d'appliquer les principes de couches de sécurité au code informatique [Figure 19].

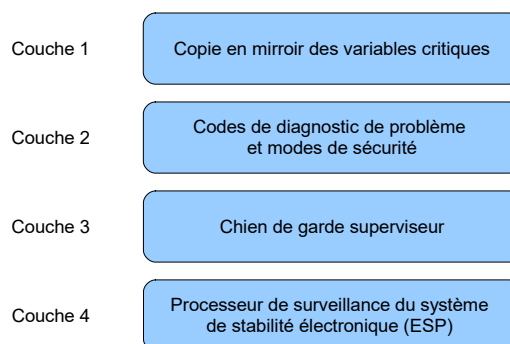


Figure 19. Couches de sécurité logicielle.

Adaptée de « 2005 Camry L4 Software Analysis », par M. Barr, 2012. ©Barr, 2012.

Le chien de garde logiciel (*watchdog supervisor*) était de plus incapable d'identifier les tâches mortes. Avec le code utilisé, et le découpage en de nombreuses tâches, le nombre de tests à mener est trop important pour pouvoir s'assurer de la robustesse du code (plus de 16 millions de combinaison de tâches mortes).

Enfin, il n'y a pas le log des erreurs : un redémarrage de la voiture efface toutes les données, ce qui empêche de pouvoir étudier les causes exactes des accidents. Idéalement, il faudrait prévoir un fichier de log des erreurs.

5.1.3 Accidents au Québec enquêtés par la CSST

Blanchette & Blanchette inc.

En août 2000, à l'usine Blanchette & Blanchette inc., une nouvelle ligne de sciage automatisée (CSST, 2002) est en cours d'installation. Un mécanicien est mortellement coincé dans la débiteuse alors que des essais sont en cours. Cet accident est dû à quatre causes selon la CSST : un bouton sélecteur non conforme au plan du fabricant, le contournement d'un dispositif de sécurité par le mécanicien, une mauvaise organisation du travail et la présence du travailleur dans la zone dangereuse non sécurisée d'une machine.

Lors de l'accident, un programmeur était en train de modifier le code permettant de rendre opérationnelle la console de maintenance qui intégrait le bouton sélecteur non conforme au plan. Cette cause n'a pas été retenue par la CSST lors de l'enquête, car, selon le rapport de la CSST, deux boutons sur la console permettaient de déclencher une fonction de sécurité qui désactivait l'automate et mettait la machine dans un mode d'arrêt sûr. Cependant, le fait qu'un programmeur ait accès au code de l'automate et qu'il puisse le modifier alors, qu'au même moment, d'autres travailleurs ont accès à la machine soulève des questions d'organisations du travail, de sécurité et de cycle de vie du logiciel.

Kruger/Wayagamak inc.

En 2004, un ouvrier d'une papeterie est coincé entre un butoir et le bâti du convoyeur et est gravement blessé. Précédemment, lors de la même journée, un programmeur a effectué des modifications dans le code de l'automate programmable.

Le rapport d'enquête précise que « selon le manuel de sécurité de cette entreprise, tout changement dans la programmation demande d'informer les employés de production », mais ceux-ci n'ont pas été avisés du changement qui avait été effectué peu auparavant. De plus, le rapport indique que « la séquence de l'automate programmable est modifiée. Normalement, le butoir demeure en position rétractée tant que la plate-forme du descendeur n'est pas localisée au niveau supérieur. Au moment du bris de l'équipement, le butoir est déjà déployé (...) ». La modification du programme de l'automate n'a pas été retenue comme cause indépendante par la CSST, mais a été englobée avec plusieurs autres éléments dans la cause « l'organisation du travail entourant l'événement est déficiente ».

5.2 Cycle de vie du logiciel

La norme CEI 61508-3 *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*, formule des exigences générales pour toutes les phases du cycle de vie du logiciel (IEC 61508, 2010). Le cycle de vie global est présenté à la figure 18 précédente. Toutes les phases ne sont pas détaillées dans cette section, mais certains points sont mis en avant puis discutés.

La conception de logiciels de sécurité est encadrée par la partie 3 de la norme CEI 61508, mais cette partie est intimement liée à la partie 2 - *Exigences concernant les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité* [Figure 20]. Du point de vue canadien, la norme CSA C22.2 No 0.8 porte sur les fonctions de sécurité incorporant des technologies électroniques (CAN/CSA C22.2 No 0.8-12, 2012). Cette norme s'appuie ouvertement sur la CEI 61508 et comprend une section portant sur le développement de logiciel (5.6).

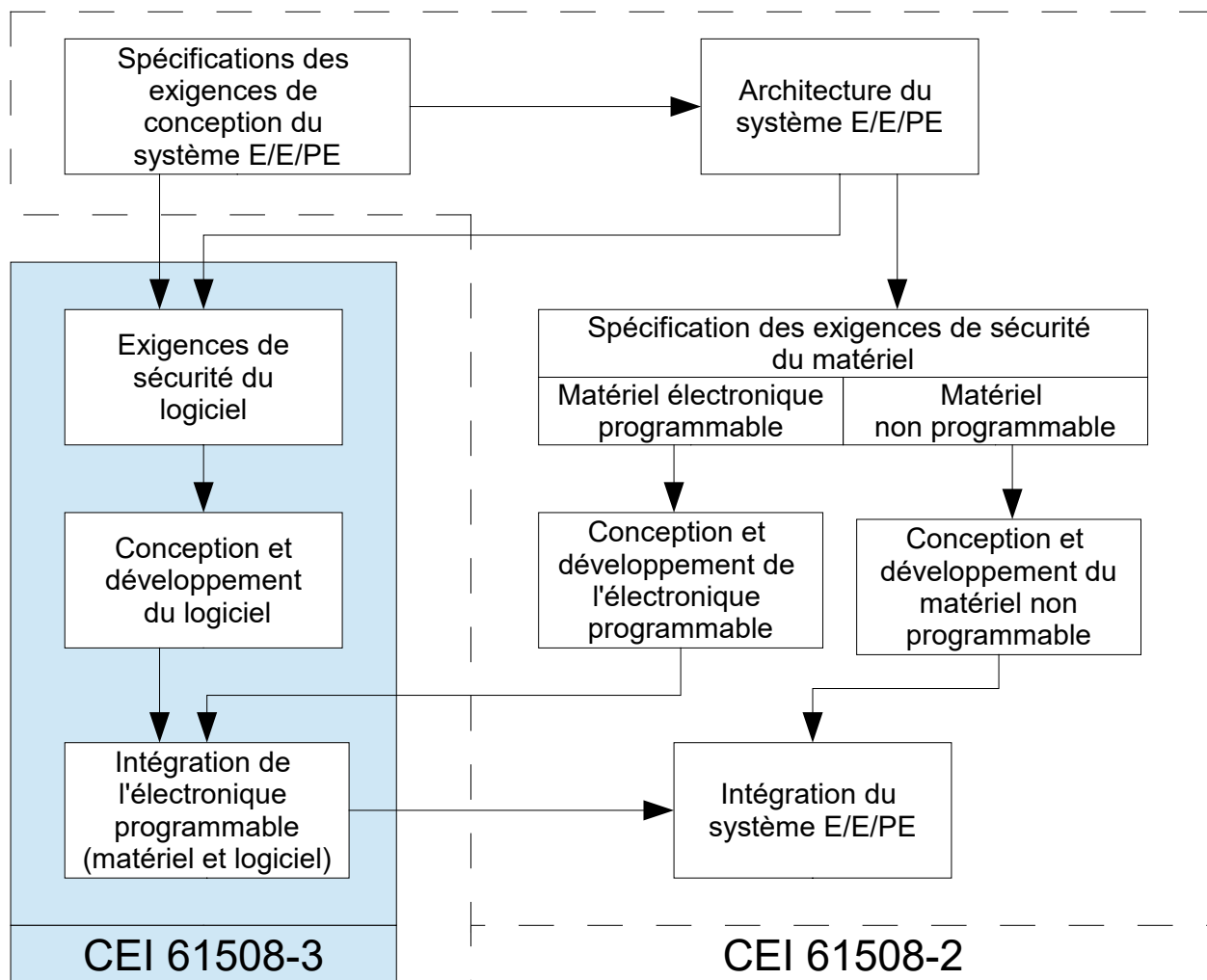


Figure 20. Domaines d'application de la norme CEI 61508-2 et 61508-3.

Adaptée de « Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010 », par International Electrotechnical Commission, 2010. ©IEC, 2010.

5.2.1 Spécification et réalisation

La phase de spécification est souvent prise avec légèreté alors que c'est l'une des phases les plus importantes : si des fonctions de sécurité sont mal définies, ou tout simplement oubliées, dans la phase de spécifications, un logiciel même très bien codé rendra la machine dangereuse par omission ou par définition.

Lors de cette phase de spécification, ou juste avant de rentrer dans la phase de réalisation, il faut prévoir un plan de validation de la sécurité du logiciel [Figure 21] (IEC 61508, 2010).

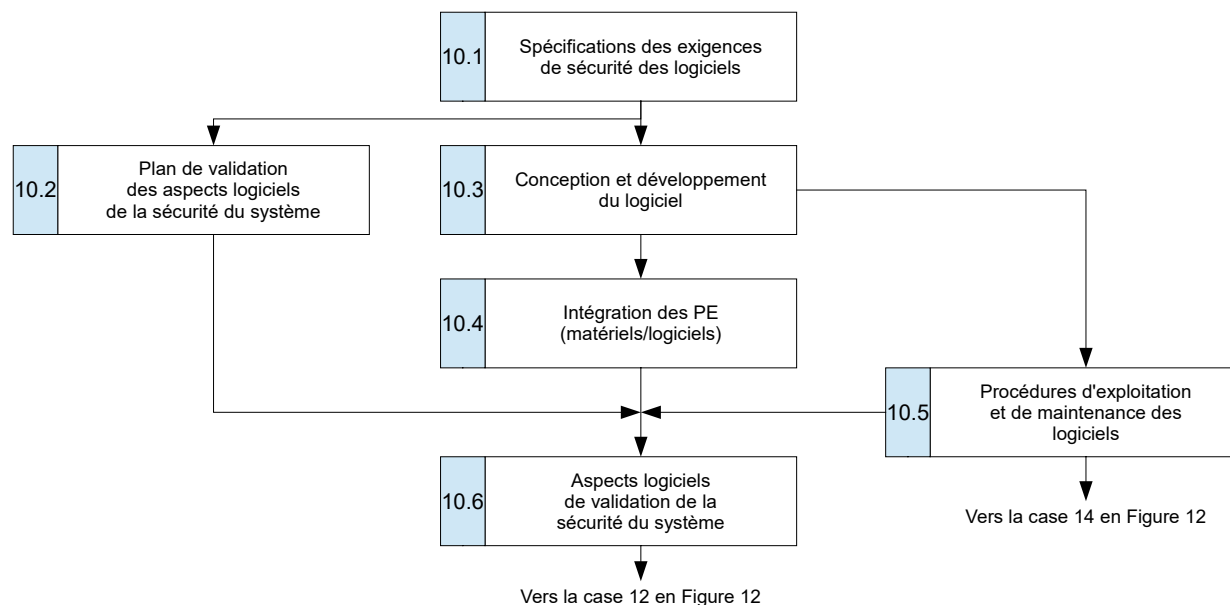


Figure 21. Cycle de vie de sécurité de logiciel (en phase de réalisation).

Adaptée de « Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010 », par International Electrotechnical Commission, 2010. ©IEC, 2010.

Lors de la phase de réalisation, l'architecture est une des questions à aborder. Cette architecture doit être :

- Conforme au niveau de SIL ;
- En corrélation avec l'architecture matérielle du système E/E/PE.

La norme CEI 61508 prescrit des objectifs très généraux quant au cycle de vie d'un logiciel relatif à la sécurité. Notamment lors de la phase de développement, une des prescriptions est de « Sélectionner un ensemble approprié d'outils d'aide à la vérification, la validation, réévaluation et la modification, y compris les langages et les compilateurs, les interfaces système d'exécution, les interfaces utilisateurs et les formats et représentations des données pour le niveau d'intégrité de sécurité requis au cours du cycle de vie de sécurité complet du logiciel ». Ceci peut notamment faire référence à la norme MISRA C lorsque le logiciel est développé en langage C.

5.2.2 Validation

La validation du logiciel vise à s'assurer que le programme est conforme aux codes et normes en vigueur et à détecter les fautes éventuelles (Charpentier *et al.*, 2000). L'article 7.9. de la norme CEI 61508-3 présente les exigences quant à la vérification des logiciels relatifs à la sécurité (IEC 61508, 2010). Les paragraphes 7.4.7, 7.4.8 et 7.5 constituent également des activités de vérification.

La norme CEI 61508-3 exige un document présentant la validation et tous les points qui seront couverts (y compris les détails techniques de la validation elle-même). Par contre, la norme ne donne pas de méthode particulière pour la vérification ou la validation du logiciel, elle se contente de formuler des exigences générales. Les vérifications suivantes doivent être faites (IEC 61508, 2010) :

- a. Vérification des exigences pour la sécurité du logiciel ;
- b. Vérification de l'architecture du logiciel ;
- c. Vérification de la conception du système logiciel ;
- d. Vérification de la conception des modules logiciels ;
- e. Vérification du code ;
- f. Vérification des données ;
- g. Vérification des performances de synchronisation ;
- h. Essai des modules logiciels (voir 7.4.7) ;
- i. Essai d'intégration du logiciel (voir 7.4.8) ;
- j. Essai d'intégration de l'électronique programmable (voir 7.5) ;
- k. Validation de sécurité du logiciel (voir 7.7).

Les tests du logiciel devraient être effectués par des tiers, plutôt que par l'équipe de conception / programmation (Charpentier *et al.*, 2000). Plus le niveau de SIL sera élevé, plus l'indépendance de l'équipe de vérification devrait être grande (Sammarco *et al.*, 2001a). Il faut également porter une attention particulière lors de la vérification : la correction de fautes elle-même peut introduire de nouvelles fautes ou rendre certaines parties du code non fonctionnelles (Charpentier *et al.*, 2000).

Selon Charpentier *et al.* (2000) [Figure 22], on distingue les types de tests suivants :

- Test unitaire : pour un module donné, test de logique ou test de calcul ;
- Test d'intégration : enchaînement entre modules, circulation de données, reprises en cas d'interruption ;
- Test de validation : vérifier que le logiciel correspond aux spécifications (interface matériel, fonctionnement en temps réel...).

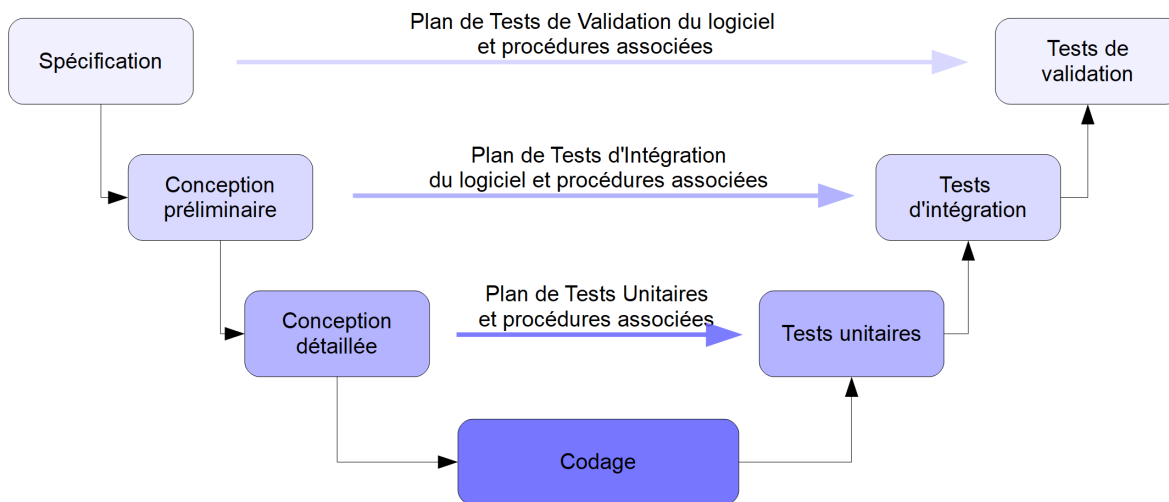


Figure 22. Développement « en V ».

Adaptée de « *Comment construire les tests d'un logiciel* », par P. Charpentier, N. Diette et F. Escaffre, 2000. ©Cahiers de notes documentaires, 2000.

Le logiciel est vérifié séparément du système dans son ensemble. Les tests peuvent être faits en boîte noire (on teste le logiciel sans regarder le code) ou en boîte blanche (les jeux de test sont produits en analysant le code source) (Charpentier *et al.*, 2000).

Le développement « en V » est aussi présenté dans la partie 3 de la norme CEI 61508, à condition que les exigences du Tableau 1 de la norme soient respectées (IEC 61508, 2010). Une des exigences de l'Annexe A normative de la norme CEI 61508 [Tableau 10] est notamment de prévoir des procédures de modification du logiciel.

Tableau 10 Validation des logiciels selon la norme CEI 61508-3

Adapté de « *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010* », par International Electrotechnical Commission, 2010. ©IEC, 2010.

Technique / mesure		SIL 1	SIL 2	SIL 3	SIL 4
1	Preuve formelle	-	R	R	HR
2	Animation de la spécification et de la conception	R	R	R	R
3	Analyse statique	R	HR	HR	HR
4	Analyse dynamique et essai	R	HR	HR	HR
5	Traçabilité ascendante entre la spécification de conception du logiciel et le plan de vérification du logiciel (y compris la vérification des données)	R	R	HR	HR
6	Traçabilité descendante entre le plan de vérification du logiciel (y compris la vérification des données) et la spécification de conception du logiciel	R	R	HR	HR
7	Analyse numérique hors ligne	R	R	HR	HR
Essai des modules de logiciels et intégration		Voir tableau A.5 de la CEI 61508			
Essai d'intégration de l'électronique programmable		Voir tableau A.6 de la CEI 61508			
Essai du système logiciel (validation)		Voir tableau A.7 de la CEI 61508			

Des détails sont aussi donnés dans les annexes B et C de la norme CEI 61508-3, annexes qui sont cependant informatives (par opposition à l'annexe A qui est normative).

5.2.3 Modification

L'article 7.8. de la norme CEI 61508-3 traite spécifiquement des modifications apportées aux logiciels relatifs à la sécurité (IEC 61508, 2010). La norme CSA C22.2 comprend également une section portant sur la modification du logiciel (5.8.5) (CAN/CSA C22.2 No 0.8-12, 2012). La norme CSA M421 (2011) mentionne elle aussi à l'article C1.2.2 de l'annexe que les modifications de programme doivent être documentées et réalisées par une personne compétente qui connaît les implications des changements.

Le tableau 11 présente un extrait de la norme CEI 61508 précisant les exigences relatives à la modification de logiciel. Avant de procéder à une modification du code, il est donc nécessaire d'avoir sous la main une procédure de modification du logiciel et de fournir, **avant la modification** [Figure 23], un document présentant une analyse d'impact de la modification. On est donc très éloigné des pratiques de codage sur site, à la volée, qui ont été recensées dans les deux accidents enquêtés par la CSST. La C22.2 exige également une procédure pour la modification des logiciels (CAN/CSA C22.2 No 0.8-12, 2012). Dans le cas de l'écrasement d'une cage en 2013, nous n'avons pas assez d'information pour indiquer si les exigences de modification d'un logiciel ont été suivies ou non.

Tableau 11. Extrait du Tableau 1 de la norme, listant les exigences à chaque phase du cycle de vie du logiciel de sécurité

Adapté de « *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010* », par *International Electrotechnical Commission*, 2010. ©IEC, 2010.

Phase du cycle de vie de sécurité	Objectifs	Article	Entrées (informations requises)	Sorties (informations fournies)
Modification du logiciel	Apporter des corrections, des améliorations ou des adaptations au logiciel valide en s'assurant du maintien de la capacité systématique du logiciel requise	7.8.2	Procédures de modification du logiciel Demande de modification du logiciel	Résultats de l'analyse d'impact de la modification du logiciel Journal de modification du logiciel

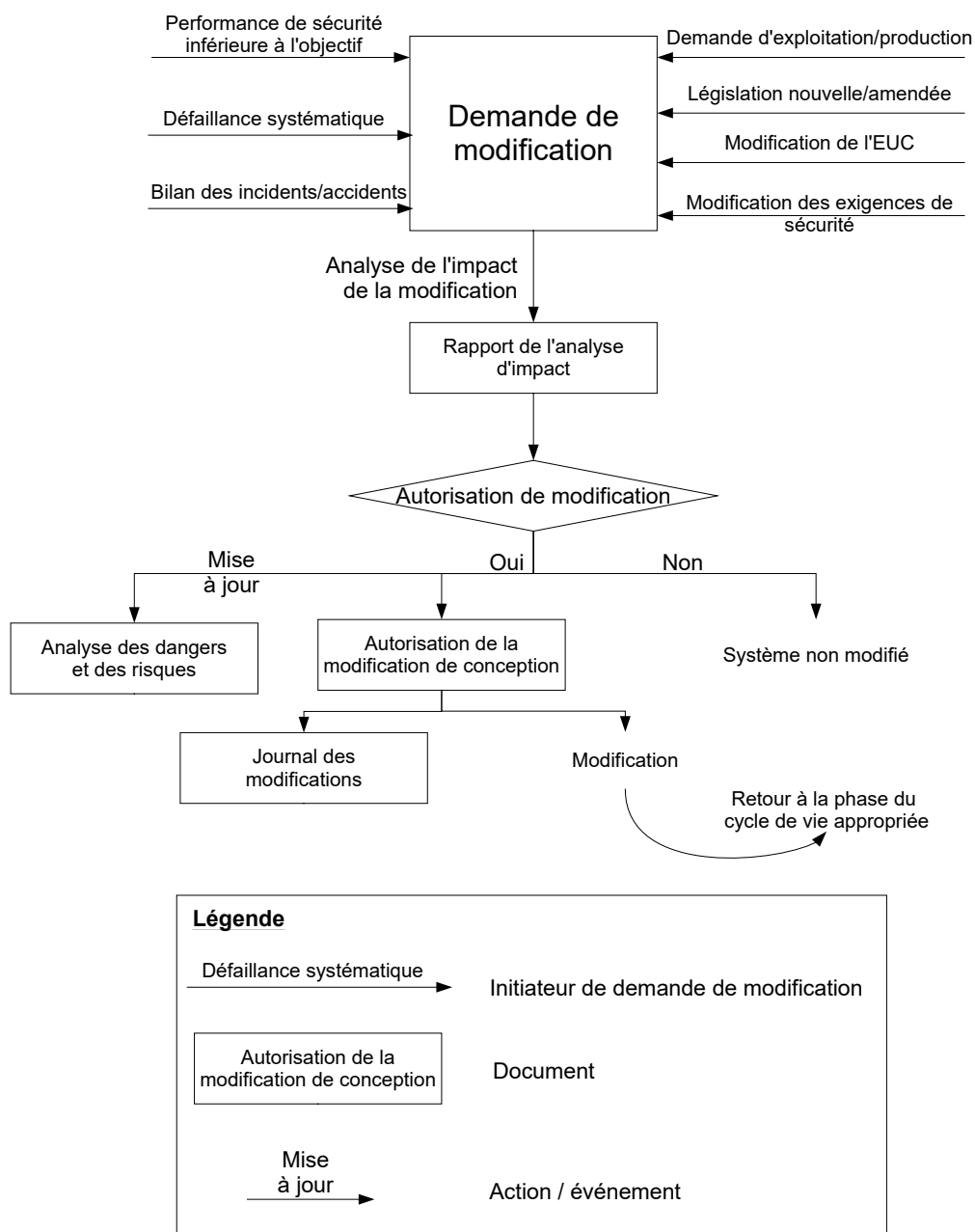


Figure 23. Exemple de procédure de modification.

Adaptée de « Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010 », par International Electrotechnical Commission, 2010. ©IEC, 2010.

Une analyse d'impact de la modification doit évaluer si une analyse de risque est nécessaire et identifier quelles phases du cycle de vie devront être répétées. La planification pour la modification du logiciel doit notamment : identifier le personnel et les compétences requises, planifier la vérification et le domaine de revalidation du logiciel. Tous les détails des modifications doivent être documentés selon les exigences de la norme CEI 61508. Comme dans le cas de la validation, des détails sont donnés dans l'annexe C (informatif) de la norme CEI 61508-3.

5.3 Recommandations

Afin d'améliorer la performance de la sécurité logicielle, nous formulons les recommandations suivantes. Il appartiendra au législateur de considérer si tout ou partie de ces recommandations doivent être intégrés dans les textes de loi, et aux industriels de mettre en place certaines de ces recommandations s'ils les jugent pertinentes. Les recommandations sont présentées en ordre séquentiel sans organisation par niveau d'importance.

Recommandation 5.1 :

Que les logiciels de commande des machines d'extraction soient conçus selon les exigences de la norme CEI 61508, en particulier en ce qui a trait au cycle de vie et à l'interfaçage entre le logiciel et le système E/E/PE [Figure 24, page suivante] et aux procédures de modification du code [Figure 23]. Il serait également souhaitable que l'équipe qui conçoit, valide ou modifie le code inclue un ingénieur compétent et que le code soit entièrement validé par un organisme externe indépendant.

Recommandation 5.2 :

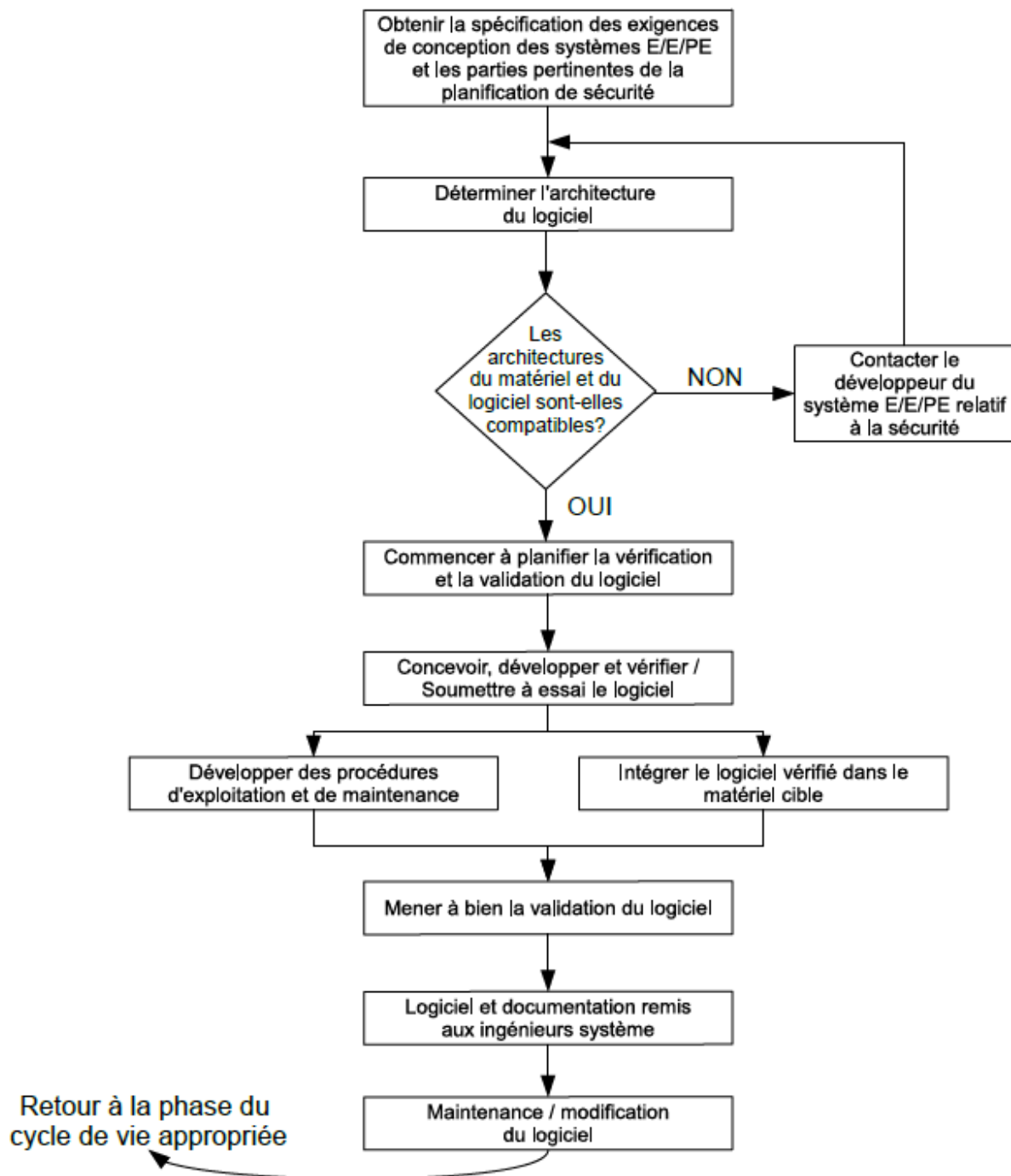
Que le concept de couches de protection soit appliqué au niveau logiciel, comme cela a été montré dans l'exemple du ETCS Toyota.

Recommandation 5.3 :

Que des codes différents soient utilisés pour la commande et pour la supervision de la machine d'extraction. Le code pour la supervision devrait être le plus simple possible, avoir été bâti uniquement pour la machine d'extraction considérée et ne pas s'appuyer sur des morceaux de code récupérés d'autres applications ou « *off the shelf* ».

Recommandation 5.4 :

Qu'une validation des fonctions de sécurité gérées par le logiciel soit effectuée in situ par des essais complets (ex. débranchement d'un détecteur).



**Figure 24. Extrait des lignes directrices de la CEI 61508 :
Application de la CEI 61508-3.**

Adaptée de « Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010 », par International Electrotechnical Commission, 2010. ©IEC, 2010.

6. COUCHE 5 – SÉCURITÉ PHYSIQUE

Dans le cas où une perte de contrôle du déplacement de la cage survient malgré les barrières de niveau 3 (alarmes et intervention humaine) et 4 (SIS), seul un dispositif de sécurité physique - passif ou actif - en couche 5 [Figure 2], comme un frein positionné sur la cage, peut intervenir et éviter l'écrasement de la cage au fond du puits. Ceci correspond au « facteur d'évitement » de la figure 1.

Plusieurs dispositifs physiques, tant actifs que passifs, sont mentionnés dans les législations fédérales ou provinciales du Canada. Citons par exemple pour les dispositifs actifs :

- Règlement sur la santé et la sécurité dans les mines de charbon (fédéral), l'article 84.3 mentionne que « Lorsque des wagonnets de transport des personnes sont utilisés dans un convoi sur des pentes de plus de 4 pour cent, ils doivent être munis de freins de sûreté qui : [...] c) peuvent être actionnés automatiquement par un régulateur de survitesse dans un des wagonnets du convoi advenant une survitesse de 20 pour cent ; [...] ».

Pour les dispositifs passifs :

- Le Health, Safety and Reclamation Code for Mines in British Columbia de 2008, mentionne à l'article 7.1.1 (1) que « A mine shaft shall [...] (e) where a friction hoist is installed and where workers are transported in a conveyance not equipped with safety catches, safety chairs shall be installed in each compartment at the extreme limit of overwind travel ; and the installation shall be so arranged so that if a conveyance or counterweights should break away from the rope as a result of an overwind, it would fall back the smallest practicable distance before landing on the safety chairs which, with their supports, shall be designed to stop and hold a fully loaded conveyance under these conditions ;
- Au Manitoba, le Règlement sur l'exploitation minière de la Loi sur la sécurité et l'hygiène du travail mentionne à l'article 30.6 intitulé Machine à poulie d'adhérence que « [...]b) le puits soit muni de guides coniques ou d'autres dispositifs appropriés disposés de manière à freiner et à immobiliser un appareil de transport mis aux molettes ou dépassant la limite inférieure de trajet lorsque l'appareil pénètre dans la zone terminale à la vitesse maximale que permettent les commandes de la machine. » ;
- Au Nouveau-Brunswick, le Règlement 69-105 mentionne à l'article 183(1) que « L'employeur doit s'assurer qu'un puits de mine [...] e) lorsqu'un treuil à friction est utilisé, dispose de pièces de guidage effilées ou d'autres dispositifs au-dessus et en dessous des limites du parcours normal du transporteur de puits et d'un contrepoids destiné à agir comme frein direct pour ralentir et arrêter le transporteur de puits et faire contrepoids en cas de dépassement du parcours normal. » ;
- Au Québec, le RSSM mentionne à l'article 240 que « Lorsque des personnes sont transportées au moyen d'une machine d'extraction à poulie d'adhérence multicâble, les compartiments d'extraction doivent être munis de taquets de sécurité à la limite supérieure de parcours. Ces taquets doivent retenir la cage, le skip et le contrepoids à pleine charge advenant la rupture des câbles d'extraction » ;
- Etc.

Dans le cas des parachutes traditionnels, ces derniers ne sont ni pensés, ni prévus pour se déclencher dans le cas où le câble est encore en bon état et connecté à la cage. En effet, leur **seul mode** de déclenchement est de ne plus avoir une tension suffisante à l'attache, ce qui se produit lorsque le câble casse, lorsque la cage rencontre un obstacle dans le puits ou lorsque la cage rebondit au bout du câble. Par contre, des systèmes évolués semblent être en mesure de freiner la cage pour des conditions de déclenchement prédéfinies **plus nombreuses** que les parachutes classiques.

Ces deux types de parachutes ainsi que leurs avantages et leurs défauts ont été largement discutés dans le volet 2 de l'expertise (Giraud et Galy, 2022b). Cette section présente quelques considérations générales qui pourraient servir à améliorer la définition des conditions de déclenchement de ces dispositifs de sécurité.

6.1 Les dispositifs de sécurité actifs

6.1.1 Améliorations possibles des parachutes « classiques »

Comme cela a été mentionné dans les volets précédents de cette expertise, les parachutes classiques sont conçus pour se déclencher uniquement en cas de perte de tension à l'attache (rupture du câble ou rebond). De plus, ils ne sont conçus que pour pouvoir arrêter un mouvement descendant de la cage.

Une amélioration possible des parachutes traditionnels serait de pouvoir les déclencher dans le cas d'une descente non contrôlée de la cage sans rupture du câble. Un dispositif permettant d'actionner les dents du parachute (hors rupture du câble) et une commande de ce dispositif seraient alors nécessaires. La commande pourrait être automatique, basée sur la survitesse ou sur le dépassement de positions prédéfinies par exemple, comme dans les puits inclinés aux États-Unis (MSHA, 2000 ; MSHA, 2001 ; MSHA, 2009). La commande pourrait aussi être manuelle et actionnable depuis la cage (boutons d'arrêt d'urgence déjà en place aux États-Unis) ou pourrait être actionnable à distance. Dans ce cas, le système parachute, qui est un dispositif de sécurité actif, devient aussi un système à action manuelle de sécurité (SAMS, voir la figure 5).

L'avantage de cette amélioration est qu'elle donnerait aux travailleurs dans la cage ou à un travailleur à proximité du bouton d'arrêt d'urgence, par exemple en haut du puits, la possibilité de déclencher le parachute pour arrêter le mouvement incontrôlé de la cage. *A priori*, dans les deux derniers écrasements de cage survenus au Québec en 2011 à la mine Doyon et en 2013 à la mine Westwood, ce dispositif aurait pu être déclenché pour arrêter la chute de la cage (ou du skip) dans le puits. Ce type de système ne règle cependant pas le problème de l'empilement du câble sur la cage, qui pourrait potentiellement entraîner la chute de la cage dans le puits.

L'inconvénient de cette amélioration est la possibilité de déclenchement intempestif du système parachute. Un actionnement intempestif entraînerait un mou de câble au-dessus de la cage arrêtée dans le puits. Pour éviter cela ou pour limiter l'accumulation de câble au-dessus de la cage, il faudrait alors coupler l'arrêt du déroulement du câble avec le déclenchement du système parachute.

6.1.2 Amélioration possible des parachutes « modernes »

Actuellement, les systèmes parachutes évolués ne sont pas prévus pour arrêter la chute de la cage en cas de perte de contrôle du déplacement (survitesse, non-arrêt à un niveau, dépassement des limites autorisées, etc.). En effet, leur système de commande copie le mode de fonctionnement des parachutes classiques pour déclencher l'arrêt uniquement lors d'un bris du câble (ou tension insuffisante à l'attache).

De plus, contrairement au système parachute classique, ils sont aussi prévus pour retenir la cage dans les deux sens de déplacement : montée ou descente. En effet, ils sont des évolutions d'un dispositif de positionnement (*chairing*) qui doit pouvoir maintenir en place la cage sujette tant à des mouvements descendants (chargement de la cage) qu'ascendant (déchargement de la cage).

Cependant, compte tenu de leurs caractéristiques, si les conditions de déclenchement du système étaient modifiées, ces dispositifs pourraient être déclenchés en cas de perte de contrôle du déplacement de la cage.

Par exemple, les conditions de déclenchement suivantes pourraient être utilisées par le système de commande du dispositif :

- Survitesse absolue, soit 115 % à 120 % de la vitesse maximale de la cage. L'article 84.3 du Règlement fédéral canadien sur la santé et la sécurité dans les mines de charbon mentionne 120 % alors que l'article 75.1400 du C.F.R. 30 aux États-Unis mentionne 115 %. L'article 241 du RSSM mentionne 120 % de la vitesse maximale d'opération. Par ailleurs, il faut que cette survitesse soit supérieure à celle du superviseur (Lilly) de la cage pour pas qu'il se produise de déclenchement intempestif ;
- Survitesse relative, soit 115 % à 120 % de la vitesse autorisée en fonction de la position de la cage dans le puits dans les zones d'accélération ou de décélération. Pour cela, il est nécessaire d'obtenir une information sur la position de la cage dans le puits ;
- Bouton d'arrêt d'urgence dans la cabine ou en haut du puits ;
- Dépassement des limites de parcours ;
- Dépassement du niveau à atteindre : si la cage franchit le niveau à atteindre sans s'arrêter, le dispositif est déclenché ;
- Détection d'obstacle dans le puits dans le sens du mouvement de la cage (systèmes de détection d'obstacle au-dessus et en dessous de la cage) ;
- Accélération de la cage trop importante.

Les données nécessaires à ces conditions de déclenchement devraient être traitées directement au niveau de la cage pour que le dispositif soit autonome. Idéalement, pour améliorer la fiabilité de ce dispositif de sécurité actif, le traitement de la fonction de sécurité devrait être le plus simple et le plus robuste possible.

Cette amélioration rendrait la cage autonome en termes de sécurité lors du dépassement des critères fixés précédemment (vitesse absolue, vitesse relative, position, etc.). Elle donnerait aussi aux travailleurs dans la cage ou à un travailleur à proximité du bouton d'arrêt d'urgence, par exemple en haut du puits, la possibilité de déclencher le parachute pour arrêter le mouvement incontrôlé de la cage. Cet arrêt d'urgence devrait également stopper la machine d'extraction pour éviter l'empilement du câble sur la cage.

Un inconvénient de cette amélioration est la possibilité de déclenchements intempestifs du système parachute. Si cet actionnement intempestif se produit en descente, ceci entraînerait un mou de câble au-dessus de la cage arrêtée dans le puits comme cela est décrit précédemment. Si cet actionnement intempestif se produit en montée, ceci entraînerait une surcharge dynamique dans le câble, surcharge qui pourrait provoquer sa rupture dans la situation la plus défavorable (pour le cas où un système de supervision de la tension dans le câble n'est pas en mesure de stopper la machine d'extraction).

Il existe une alternative afin d'éliminer l'effet indésirable du freinage intempestif en montée : c'est de concevoir un parachute moderne qui ne freine que dans le sens descendant. Dans ce cas, on a les mêmes avantages que le parachute traditionnel, à savoir l'absence de risque d'application intempestive en montée. Par contre, ce mode de fonctionnement empêche l'utilisation du système pour faire du positionnement.

6.2 Dispositifs de sécurité passifs

Outre les dispositifs de sécurité actifs que sont les parachutes, il est également possible d'envisager l'installation de dispositifs de sécurité passifs pour assurer la sécurité de la cage. Les deux extrémités du puits sont à privilégier, car ce sont les deux zones où la cage peut s'écraser.

Il serait par exemple possible de généraliser l'installation d'un amortisseur de fin de course au fond du puits comme c'est le cas en Afrique du Sud ou au Canada (cf. réglementation BC, MB, NB et QC pour les treuils à friction) pour les treuils à friction. Cela permettrait d'amortir la chute de la cage si les parachutes ne se déploient pas.

Un dispositif de freinage et de retenue de la cage au chevalement pourrait aussi être mis en place afin d'éviter qu'elle ne s'écrase puis ne tombe dans le puits en cas d'arrivée trop rapide au niveau du chevalement. De tels dispositifs de retenue sont déjà opérationnels pour les treuils à friction : en effet, les cages doivent être retenues au niveau du chevalement en cas de problème. Par contre, le dispositif de freinage est à développer.

6.3 Cycle de vie des dispositifs de sécurité

Les dispositifs de sécurité, qu'ils soient actifs ou passifs, doivent être testés régulièrement pour vérifier leur bon fonctionnement. Ces précautions sur le cycle de vie des dispositifs de sécurité ne sont pas uniquement théoriques. En effet, lors des derniers accidents de levage de funiculaires inclinés¹¹ (*hoisting*) enquêtés aux États-Unis (MSHA, 2000 ; MSHA, 2001 ; MSHA, 2009), les dispositifs de sécurité actifs sensés réduire le risque n'étaient pas fonctionnels : en 2000, le dispositif de survitesse centrifuge du frein magnétique du wagon de freinage, théoriquement réglé

¹¹ On pourrait également mentionner l'accident du funiculaire de Québec qui a fait 1 mort et 15 blessés en octobre 1996.

à 115 % de la vitesse maximale, ne s'est pas déclenché. En 2001, le dispositif de survitesse du frein magnétique du wagon de freinage, théoriquement réglé à 115 % de la vitesse maximale, ne s'est pas déclenché. De plus, lors de l'accident, la charge totale du convoi dépassait la capacité de freinage du wagon de freinage. En 2009 le frein du wagon de freinage a été activé manuellement, mais la charge totale du convoi dépassait d'environ 80 % la capacité de freinage du wagon de freinage. Le dispositif de survitesse n'a pas pu être testé, car il a été détruit lors de l'accident. Par ailleurs, l'usure dans le temps des dispositifs de sécurité, soit leur vieillissement, doit aussi être considérée, même dans le cas des systèmes passifs (Iddir, 2014).

Les tests et l'entretien des dispositifs de sécurité devraient être faits uniquement par des personnes compétentes et désignées. C'est notamment ce que mentionne la réglementation de Colombie-Britannique à l'article 7.6.13 intitulé *Safety Devices – Design and Adjustment* : « *Every safety and protective device installed at a hoisting installation shall [...] (2) only be adjusted and maintained by a qualified and authorized person.* ».

Les essais et tests des différentes fonctions de sécurité devraient être exécutés à des intervalles de temps différents, et par des personnes différentes comme mentionné dans la partie 6 de l'annexe B de la norme CEI 61508 (IEC 61508, 2010) afin de conserver la probabilité de défaillance au plus bas niveau possible. En effet, lors d'un test positif, l'indisponibilité instantanée du dispositif testé est remise à 0 (sa valeur minimale) étant donné que le dispositif est fonctionnel [Figure 25]. Puis cette indisponibilité va augmenter au fur et à mesure du temps qui passe pour être de nouveau remise à 0 au prochain test. Si toutes les fonctions de sécurité à faible sollicitation sont testées en même temps, alors elles seront toutes à leur plus bas niveau de fiabilité juste avant le test. Inversement, si les fonctions de sécurité sont testées à des instants différents, certaines seront alors plus fiables que d'autres à un instant donné, ce qui donnera un niveau moyen de fiabilité plus stable dans le temps. Le fait de les tester par des personnes différentes évite des défaillances de cause commune et la répétition d'erreur. Par contre, les tests doivent être planifiés, réalisés selon des procédures écrites et doivent être les plus simples possible afin de ne pas eux-mêmes générer des nouvelles causes de défaillance (Ciutat, 2011).

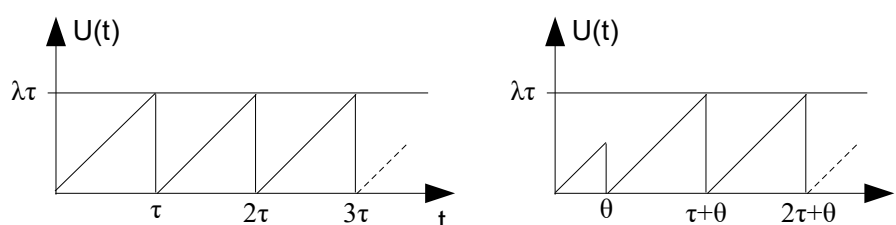


Figure 25. Indisponibilité instantanée d'un dispositif testé.

Adaptée de « *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010* », par *International Electrotechnical Commission*, 2010. ©IEC, 2010.

6.4 Recommandations

Afin d'améliorer la performance de la couche de sécurité physique, nous formulons les recommandations suivantes. Il appartiendra au législateur de considérer si tout ou partie de ces recommandations doivent être intégrés dans les textes de loi, et aux industriels de mettre en place certaines de ces recommandations s'ils les jugent pertinentes. Les recommandations sont présentées en ordre séquentiel sans organisation par niveau d'importance.

Recommandation 6.1 :

Réaliser une analyse de risque détaillée pour le système de parachute moderne installé sur une cage. Cette analyse de risque doit inclure une estimation de la fiabilité du système. D'un point de vue formel, le système parachute moderne pourrait être conçu en respectant la norme CEI 61508, à la manière d'un SIS.

Recommandation 6.2 :

Tout système parachute, classique ou moderne, devrait être totalement indépendant du système de commande ou de supervision de la machine d'extraction. Le système parachute devrait envoyer de l'information à la machine d'extraction afin d'éviter l'empilement du câble sur la cage. Le traitement de la fonction de sécurité du système parachute doit être le plus simple possible.

Recommandation 6.3 :

Mobiliser la recherche sur les systèmes parachutes, classiques ou modernes, afin de les améliorer : contrôle de la décélération, ajustement de la décélération en fonction de la charge dans la cage, définition précise des conditions de déclenchement (par exemple sens de déplacement de la cage, présence d'un bouton de déclenchement dans la cage ou en haut du puits, etc.), définition du niveau de fiabilité espéré du dispositif (par exemple pour éviter le déclenchement intempestif en montée).

Recommandation 6.4 :

Réaliser des essais in situ des parachutes modernes dans une mine, afin de s'assurer de la fiabilité du système et de son efficacité.

7. CONCLUSIONS

Ce troisième volet de l'expertise « Modernisation des parachutes de transporteurs de mines » porte uniquement sur le cas de la perte de contrôle du déplacement de la cage sans rupture du câble. Depuis leur conception initiale, les systèmes parachute ont pour objectif d'éviter l'écrasement de la cage à la suite de la rupture du câble. Historiquement, c'est cette cause qui était la plus fréquente. Maintenant, avec les progrès effectués tant dans la conception des câbles que dans le suivi de leur dégradation, la rupture du câble devient plus rare. Inversement, dans le passé, les machines d'extraction n'étaient pas la source principale des causes d'écrasement des cages. Maintenant, ces machines sont plus puissantes, plus complexes, plus rapides et plus ou moins automatisées. Cette évolution des machines d'extraction et de leur système de commande, conjuguée à l'évolution technologique rapide des systèmes de commande électriques, électroniques et programmables, rend plus présent le risque d'un écrasement de la cage dû à une erreur de commande.

Étant donné que les machines d'extraction et leur système de commande deviennent plus complexes, la première partie de ce rapport est consacrée à une revue de l'organisation des moyens de protection et de prévention ainsi qu'à un rappel des différentes méthodes d'analyse de la performance des moyens de protection. Cette partie permet de jeter un regard structuré et global sur la sécurité des machines d'extraction et des cages servant à transporter le personnel dans le puits. Les concepts de barrières de sécurité et de couches de protection selon la méthode LOPA ont été utilisés pour analyser les moyens de prévention et de protection en place dans les puits de mine au Québec. La conclusion est qu'il n'existe actuellement pas de dispositif de sécurité actif et indépendant de la machine d'extraction, qui puisse contrer la perte de contrôle du déplacement de la cage sans rupture du câble.

La section 3 est consacrée aux alarmes et aux interventions humaines de conduite de la machine d'extraction, éléments qui correspondent à la couche 3 de la méthode LOPA. Les moyens de maîtrise du risque existant, les systèmes de monitoring global et les contrôleurs y sont détaillés ainsi que le système à intervention manuelle de sécurité (SAMS) classique qu'est l'arrêt d'urgence. Il ressort de cette section qu'un système de monitoring global serait pertinent, permettant ainsi d'éviter de travailler « à l'aveugle » et d'améliorer la prise de décisions. L'utilisation de moyens mécaniques, électromécaniques ou électroniques pour traiter l'information aide aussi à la conduite de la machine par l'opérateur. En dernier recours, l'arrêt d'urgence devrait permettre de réduire la gravité du dommage imminent, mais la fiabilité de cette ultime sécurité n'est pas forcément assurée.

La section suivante, la plus importante de ce rapport, traite des systèmes instrumentés de sécurité (SIS) qui correspondent à la couche 4 de la méthode LOPA. En effet, compte tenu de l'évolution des machines d'extraction, la sécurité est maintenant assurée principalement par le système de commande et par la supervision de ce dernier. L'opérateur de la machine n'est presque plus devant les leviers mécaniques de commande de la machine en face du tambour, mais il est le plus souvent assis dans une salle de contrôle, déportée de la machine, devant un panneau de contrôle comportant de multiples écrans et manipulant de temps à autre des manettes électroniques. Il est passé d'un rôle d'acteur à un rôle de superviseur. La sécurité de la machine d'extraction est alors assurée par l'automate de commande. La sécurité d'une machine doit être envisagée de façon systémique, en incluant toutes ses composantes. Plusieurs écoles

de pensée existent concernant la séparation du SIS et du système de commande : séparation totale du SIS et des autres systèmes de commande, échange d'information unidirectionnel ou bidirectionnel, partage d'éléments physiques (capteurs, actionneurs, processeurs), et implémentation commune du SIS et du système de commande classique dans un même boîtier. Chacune de ces solutions a des avantages et des inconvénients du point de vue de la sécurité. Les normes applicables aux SIS appartiennent à deux grandes familles : CEI 61508 et 62061 ou ISO13849. Les normes 62061 et 13849 sont en train d'être fusionnées. Malgré des différences, elles poursuivent le même objectif, qui est de quantifier au mieux la fiabilité des fonctions de sécurité, et elles proposent des architectures associées aux niveaux de fiabilité visés. Nous proposons donc que les systèmes de commande et SIS soient conçus selon la famille de norme CEI 61508 et qu'une analyse de risque soit systématiquement faite pour la mise en service ou la modification d'une machine d'extraction. Par ailleurs, un organisme colligeant les informations relatives à chaque incident ou accident pour l'ensemble des mines au Québec permettrait de construire une base de données pertinente pour les analyses de risque futures.

La section 5 traite de la sécurité logicielle, car de plus en plus de SIS intègrent de l'électronique programmable. Le logiciel « zéro défaut » n'existe pas, comme plusieurs exemples donnés dans le chapitre le montrent. Les incidents et accidents survenus sont dus à des erreurs logicielles ou parfois à de mauvaises pratiques logicielles. Le chapitre introduit le concept de cycle de vie du logiciel qui est prescrit par la norme CEI 61508. Des solutions, techniques et organisationnelles sont proposées pour améliorer la fiabilité logicielle, tant dans sa phase de conception que dans celle de modification en cours d'utilisation. Les accidents survenus au Québec auraient potentiellement pu être évités si les préceptes de cycle de vie du logiciel introduits par la norme CEI 61508 avaient été respectés. Nous proposons donc d'appliquer les prescriptions normatives de la CEI 61508 pour le cycle de vie du logiciel. Par ailleurs, le concept de couches de protection pourrait être étendu à la partie logicielle (comme cela a été discuté sur l'exemple de l'ETCS de Toyota). Enfin le code devrait contenir le moins possible de parties ayant été développées précédemment et utilisées pour d'autres machines.

Enfin le rapport traite de la couche de sécurité physique, qui intervient pour minimiser les conséquences d'un événement dangereux qui vient de se produire. Le système parachute vient s'insérer dans cette couche comme un dispositif actif, car il doit se déclencher pour effectuer sa fonction de freinage, contrairement à un mur coupe-feu qui assure sa fonction de manière passive. Des pistes d'amélioration sont proposées pour les parachutes classiques (contrôle du freinage, déclenchement sans rupture du câble...) et modernes (conditions de déclenchement élargies). Les dispositifs passifs sont brièvement présentés pour les puits : systèmes de retenue de la cage en haut du puits, d'amortisseur en bas. Certains de ces types de systèmes sont déjà obligatoires dans une partie des provinces canadiennes. Les systèmes de sécurité physique, actifs et passifs doivent être testés régulièrement, afin d'éviter que des accidents similaires à ceux survenus aux États-Unis ne surviennent à nouveau. Il serait préférable que les essais et tests des différentes fonctions de sécurité soient exécutés à des intervalles de temps différents, et par des personnes différentes comme mentionné dans la partie 6 de l'annexe B de la norme CEI 61508 afin de conserver la probabilité de défaillance au plus bas niveau possible. Des personnes différentes pourraient être responsables des tests pour éviter les causes de défaillance commune. Quatre recommandations pour accroître la sécurité concluent ce dernier chapitre.

Il nous semble possible d'améliorer les parachutes classiques et modernes afin de les rendre opérationnels dans le cas d'une perte de contrôle du déplacement de la cage sans rupture de câble. Cependant, des efforts doivent aussi être fournis au niveau des systèmes de commande et de supervision (notamment la partie logicielle) maintenant que le référentiel normatif est plus stable et qu'un retour d'expérience est disponible.

BIBLIOGRAPHIE

- ABB, 2014, "Mine hoist disc brake systems - Improved safety, availability and productivity", Vol. Site web ABB
- Adjadj, A. et Charpentier, D., 2007, "Allocation de sil requis des fonctions instrumentées de sécurité d'une installation lorsque l'analyse de risque est incomplète", *Actes du 7ème congrès international Qualita, 20-22 mars 2007, Tanger, Maroc*, p. 207-14
- Anon, 2012, "Flsmidth Production Winder Being Manufactured for Mopani (Mining World website)", *Mining World*
- Anon, 2013, "Manufacturers invest in efficient mining hoists (OCH website)", <http://www.ochmagazine.com/features/manufacturers-invest-in-efficient-mining-hoists/>, *Overhead, Crane and Hoist magazine*
- Anon, 2014, "FLSmidth plans growth in mine shaft systems", <http://www.im-mining.com/2014/01/15/flsmidth-plans-growth-in-mine-shaft-systems/>, *International Mining*
- Barkand, T. D., 12-1-1990, "Elevator safety: Give the miner a brake", *Conference Record - IAS Annual Meeting (IEEE Industry Applications Society)*, n°pt 2, p. 1421-29
- Barkand, T. D., 1-1-1992a, "Ascending elevator accidents: Give the miner a brake", *IEEE Transactions on Industry Applications*, Vol. 28, n°3, p. 720-729
- Barkand, T. D., 1992b, "EMERGENCY BRAKING SYSTEMS FOR MINE HOISTS", *National Technical Information Service*, p. 14
- Barkand, T. D., 2002, "Application of a Suspension Rope Brake to a Single Rope Mine Hoisting System", *National Technical Information Service*, p. 14
- Barr, M., 2012, "2005 Camry L4 Software Analysis", *Barr group*
- Beaudoin, J. and Bello, J.-P., 2013, "Aborder la norme NF EN ISO 13849-1 via la conception d'une fonction de sécurité basique", *INRS - Département Ingénierie des équipements de travail - Laboratoire sûreté des systèmes automatisés*, Rapport n° NS 302
- Beus, M. J. et Ruest, M., 12-1-2002, "New technology for hoist conveyance monitoring and analysis", *CIM Bulletin*, Vol. 95, n°1065, p. 78-83
- Bingham, K., 2005, "Partial Stroke Testing Of Emergency Shutdown Valves", *PROCESSWest*, Vol. Summer 2005
- Bjerke, E., 1946, Safety means for mine cages, Patent n°U.S. 2,403,333
- Buchweiler, J. P., 2008, "Circuits de commande des machines - Un référentiel normatif pour leur conception", *Hygiène et sécurité au travail - Cahiers de notes documentaires*, Vol. 2e trimestre 2008, n°211
- Buchweiler, J. P., 2009, "IEC/EN 62061, ISO/EN 13849-1 - Dans la pratique, ce qui va changer pour la conception des circuits de commande relatifs à la sécurité", *In'Machine 2009*
- CAN/CSA C22.2 No 0.8-12, 2012, Safety functions incorporating electronic technology, CAN/CSA, Association Canadienne de Normalisation
- CAN/CSA-M421, 1985, "Use of electricity in mines"
- CAN/CSA-M421, 1993, "Use of electricity in mines"
- CAN/CSA-M421, 2000, "Use of electricity in mines"
- CAN/CSA-M421, 2011, "Use of electricity in mines"
- CCPS, 1993, "Guidelines for Safe Automation of Chemical Processes", *Center for Chemical Process Safety/AIChE*
- CCPS, 2001, "Layer of protection analysis - Simplified risk assessment", *Center for Chemical Process Safety*

- Charpentier, P., Diette, N., et Escaffre, F., 2000, "Comment construire les tests d'un logiciel", *Cahiers de notes documentaires - Hygiène et sécurité du travail*, Vol. 181, n°4ème trimestre
- Ciutat, F., 2011, "Sil Automatismes & Sécurité - Intégrité des Fonctions Automatisées de Sécurité", Vol. 2ème édition
- CSST, 2002, "Rapport d'enquête - accident mortel survenu à un travailleur le 30 août 2000 à l'usine de sciage Blanchette & Blanchette inc. à St-Gerard", *Rapport d'enquête*, Rapport n° EN-003311
- CSST, 2004, "Rapport d'enquête - accident grave survenu à un mécanicien le 24 juin 2004 à l'usine Kruger/Wayagamak inc. de Trois-Rivières", *Rapport d'enquête*, Rapport n° EN-003483
- Dhillon, B. S., 2010, "Mine Safety", *Springer*
- FLSmidth, 2014, "Systèmes de puits de mine", *Site web FLSmidth*
- Fortin, G. and Demers, R., 2011, "Les machines d'extraction", *Direction des communications et des relations publiques, CSST, Guide CSST*
- Galloway, L. C. et Tiley, G. L., 12-1-1986, "MINE HOIST BRAKING SYSTEMS", *CIM Bulletin*, Vol. 79, n°894, p. 50-60
- Garbolino, E. et Guarnieri, F., 2012, "Concept de défense en profondeur : contribution à la sécurité des ICPE", *Techniques de l'ingénieur - SE 2 065*
- Giraud, L. and Galy, B., 2022a, "Modernisation des parachutes de transporteurs de mines : volet 1 - État de l'Art", *IRSST, Rapport-n°QR-1156-fr*
- Giraud, L. and Galy, B., 2022b, "Modernisation des parachutes de transporteurs de mines : volet 2 - Cas de la rupture du câble", *Rapport-n°QR-1157-fr*
- Giraud, L., Galy, B., Germain, L. et Bourbonnière, R., 2019, "Sécurité des machines d'extraction commandées par systèmes programmables électroniques", *IRSST, Fiche technique, Études et recherche*, Rapport n° RF-1049
- HSE, 2003, "Out of control - Why control systems go wrong and how to prevent failure", *Health and Safety Executive*
- Iddir, O., 2012a, "Évaluation de la probabilité de défaillance d'un Système Instrumenté de Sécurité (SIS)", *Techniques de l'ingénieur - SE 4 058*
- Iddir, O., 2012b, "Méthode LOPA : principe et exemple d'application", *Techniques de l'ingénieur - SE 4 075*
- Iddir, O., 2014, "Mesures de maîtrise des risques instrumentées (MMRI)", *Techniques de l'ingénieur - SE 2 090*
- IEC 61511, 2003, Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation, IEC 61511:2003, IEC, International Electrotechnical Commission
- IEC 62061, 2005, Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité, IEC 62061:2005, IEC, International Electrotechnical Commission
- IEC 61508, 2010, Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, IEC 61508:2010, IEC, International Electrotechnical Commission
- INSAG, 1996, "Defence in Depth in Nuclear Safety", *International Nuclear Safety Advisory Group*
- ISO 13850, 2006, Safety of machinery - Emergency stop - Principles for design, ISO 13850:2006, International Organisation for Standardization

- ISO 13849-1, 2006, Sécurité des machines -- Parties des systèmes de commande relatives à la sécurité -- Partie 1: Principes généraux de conception, ISO 13849-1:2006, International Organisation for Standardization
- IEC/ISO 31010, 2009, Gestion des risques -- Techniques d'évaluation des risques, IEC/ISO 31010:2009, International Organisation for Standardization
- ISO/TR 23849, 2010, Lignes directrices relatives à l'application de l'ISO 13849-1 et de la CEI 62061 dans la conception des systèmes de commande des machines relatifs à la sécurité, ISO/TR 23849:2010, International Organisation for Standardization
- ISO 12100, 2010, Sécurité des machines -- Principes généraux de conception -- Appréciation du risque et réduction du risque, ISO 12100:2010, International Organisation for Standardization
- ISA, 2005, "GUIDE D'INTERPRÉTATION ET D'APPLICATION DE LA NORME IEC 61508 ET DES NORMES DÉRIVÉES IEC 61511 (ISA S84.01) ET IEC 62061", *Instrumentation, Systems and Automation Society - Section France*
- Koepe, F., 1878, Improvement in elevators, Patent n°US 206,251
- Kovalchik, P. G. et Duda, F. T., 12-1-1995, "Speed and position sensors for mine hoists and elevators", *Conference Record - IAS Annual Meeting (IEEE Industry Applications Society)*, Vol. 3, p. 2054-56
- Kumar, A. et Hem, P., 2012, "Technomine - Hoists (Infomine website)", <http://technology.infomine.com/reviews/Hoists/welcome.asp?view=full>, *Infomine*
- Lanternier, B. et Adjadj, A., 2008, "ALLOCATION DE NIVEAU D'INTÉGRITÉ DE SÉCURITÉ (SIL) REQUIS CONFORMEMENT A LA NORME CEI 61511", *Revue internationale sur l'Ingénierie des Risques Industriels*, Vol. 1, n°1
- Le, N. T. and Dianous, V., 2008, "Évaluation des performances des Barrières Techniques de Sécurité Ω 10", *INERIS*, Rapport n° DRA-08-95403-01561B - Û-10
- Leonida, C., 2013, "Taking the strain", *Mining Magazine*, Vol. 20 Feb 2013
- Levenson, N. et Turner, C., 1993, "An investigation of the Therac-25 accidents", *IEEE Computer*, Vol. 26, n°7
- Mesures, 2009a, "Instrumentation - Des équipements à surveiller de près", *Mesures*, Vol. 813, n°Mars 2009
- Mesures, 2009b, "Les systèmes de sécurité - SIS et SNCC cherchent à cohabiter en toute sécurité", *Mesures*, Vol. 813, n°Mars 2009
- Mesures, 2009c, "NORME CEI 61511 - Définir, réaliser, maintenir la fonction de sécurité", *Mesures*, Vol. 813, n°Mars 2009
- Miche, E. and Perinet, R., 2009, "Démarche d'évaluation des Barrières Humaines de Sécurité - Û 20", *INERIS*, Rapport n° INERIS-DRA-09-103041-06026B
- MSHA, 2000, "REPORT OF INVESTIGATION - Underground Coal Mine - Fatal Hoisting Accident Mine No. 2 (I.d. No. 15-09571) Excel Mining LLC Pilgrim, Martin County, Kentucky"
- MSHA, 2001, "REPORT OF INVESTIGATION - Underground Coal Mine - Fatal Hoisting Accident - November 8, 2001 -Nelms Mine - Cadiz Portal, AEP Ohio Coal, L.L.C., Cadiz, Harrison County, Ohio, I.D. No. 33-03349"
- MSHA, 2009, "REPORT OF INVESTIGATION - Underground Coal Mine - Fatal Hoisting Accident October 27, 2009", Rapport n° CAI-2009-14
- NSW, 2006, Coal Mine Health and Safety Regulation, NSW Department of Primary Industries and NSW
- NSW, 2007, Requirements for design registration of powered winding systems, Notice under clause 112A of Occupational Health and Safety Regulation 2001, Regan, R.

- NSW, 2011, Design of powered winding systems - A Functional Safety Approach, EES008-4, Mine Safety Operations Branch Industry and Investment NSW
- Paques, J.-J. and Germain, L., 2005, "Sécurité des machines d'extraction commandées par systèmes programmables", *IRSST, Fiche technique, Études et recherche*, Rapport n° RF-412
- R-NSW, 2011a, Guidelines - Mine winders - Part 3 : Vertical shaft winders, MDG 33.3, R-NSW
- R-NSW, 2011b, Guidelines - Mine winders - Part 6 : Control Systems, MDG 33.6, R-NSW
- R-NSW, 2011c, Guidelines - Mine winders - Part 7 : examination, testing and retirement of ropes, MDG 33.7, R-NSW
- Sammarco, J. J., 2002, "Addressing the safety of programmable electronic mining systems : lessons learned", *IEEE Transactions on Industry Applications*
- Sammarco, J. J., 2005, "Programmable Electronic Mining Systems: Best Practice Recommendations - Part 6 : 5.1. System safety guidance", *NIOSH*, Rapport n° 2005-150
- Sammarco, J. J., 2006, "Programmable Electronic Mining Systems: Best Practice Recommendations - Part 8 : 6.0 Safety file guidance", *NIOSH*, Rapport n° 2006-130
- Sammarco, J. J. and Fisher, T. J., 2001, "Programmable Electronic Mining Systems: Best Practice Recommendations - Part 2 : 2.1. System safety", *NIOSH*, Rapport n° 2001-137
- Sammarco, J. J., Fisher, T. J., and Jobes, C. C., 2001a, "Programmable Electronic Mining Systems: Best Practice Recommendations - Part 3 : 2.2. Software safety", *NIOSH*, Rapport n° 2001-164
- Sammarco, J. J., Fisher, T. J., Welsh, J. H., and Pazuchanics, M. J., 2001b, "Programmable Electronic Mining Systems: Best Practice Recommendations - Part 1 : 1.0 Introduction", *NIOSH*, Rapport n° 2001-132
- Sammarco, J. J. and Flynt, J. S., 2006, "Programmable Electronic Mining Systems: Best Practice Recommendations - Part 9 : 7.0 Independent functional safety assessment guidance", *NIOSH*, Rapport n° 2006-131
- Sammarco, J. J. and Fries, E. F., 2003, "Programmable Electronic Mining Systems: Best Practice Recommendations - Part 5 : 4.0. Independent Functional Safety Assessment", *NIOSH*, Rapport n° 2003-138
- Sparg, E. N., 1995, "DEVELOPMENTS IN HOIST DESIGN TECHNOLOGY APPLIED TO A 4000 METRE DEEP SHAFT", *Mining Technology*, Vol. 77, n°886, p. 179-84
- Tiley, P., 2011, "Mining engineering handbook - Chap 12.9 : Hoisting systems", in *Mining engineering handbook*, SME
- Young, C. R., 1947, "Investigations regarding the safety of hoisting equipment and hoisting practice in Ontario mines", *Province of Ontario, Department of mines*, Rapport n° Bulletin n°138

ANNEXE I : DÉFINITIONS

Quelques définitions générales sont données dans cette section afin d'aider le lecteur à la compréhension du texte.

Accident : tout événement non désiré ayant pour conséquence des blessures ou des décès parmi les travailleurs (avec potentiellement des dégâts matériels).

Arrêt d'urgence : la définition choisie est celle de la norme ISO 13850 (ISO 13850, 2006). La fonction d'arrêt d'urgence est destinée à :

- parer à des phénomènes dangereux en train d'apparaître ou atténuer des phénomènes dangereux existants pouvant porter atteinte à des personnes, à la machine ou au travail en cours ;
- être déclenchée par une action humaine unique.

Barrière technique de sécurité (BTS) (Le et Dianous, 2008) : Ensemble d'éléments techniques nécessaires et suffisants pour assurer une fonction de sécurité. On les appelle aussi des Mesures de Maîtrise des Risques (MMR).

Câble traînant : câble coupé entre la molette et le tambour, mais continuant de maintenir une tension suffisante au niveau de la cage pour empêcher le déclenchement des parachutes. Ce cas de figure survient lorsque la friction est importante entre le câble et le tambour, ou encore lorsque le câble s'empêtre autour de l'arbre de transmission. En anglais le terme *trailing rope* est utilisé.

Cage : dispositif servant à transporter dans un puits de mine des personnes uniquement au moyen d'une machine d'extraction.

Cage-skip : dispositif servant à transporter dans un puits de mine des personnes et des matériaux au moyen d'une machine d'extraction.

Cuffat : dispositif servant à transporter dans un puits de mine des personnes ou des matériaux au moyen lors des opérations de fonçage. En anglais : *kibble* ou *bucket*.

Dispositif de sécurité (Le et Dianous, 2008) : Élément unitaire, autonome, ayant pour objectif de remplir une fonction de sécurité, dans sa globalité. On distingue des dispositifs actifs et des dispositifs passifs.

Essais de débattement limité : essai visant à s'assurer du mouvement libre des pièces constituant le parachute jusqu'à application des mâchoires sur les guides en bois.

Essai de débattement total : essai visant à s'assurer du mouvement libre des pièces constituant le parachute jusqu'à déploiement complet des mâchoires (une encoche est préalablement creusée dans les guides en bois à l'endroit approprié).

Essai de dégagement rapide : nous reprenons la définition du RSSM « tout essai consistant à lâcher la cage, le skip ou l'ensemble cage-skip d'une position stationnaire pour que les mâchoires du parachute puissent mordre le guidage ». En anglais les termes varient : *drop test*, *quick release test*. La caractéristique de cet essai est que la vitesse initiale de la cage est nulle.

Essai de chute libre : le RSSM donne la définition suivante : « tout essai consistant à lâcher la cage, le skip ou l'ensemble cage-skip sous la charge maximale admise pour le transport de personnes, afin que les mâchoires du parachute puissent mordre le guidage lorsque la cage, le skip ou l'ensemble cage-skip descend à la vitesse maximale d'extraction ». Nous la généraliserons en considérant un essai de chute libre lorsque la vitesse initiale de la cage (lors de l'engagement des mâchoires dans les guides) est différente de 0. En effet, suivant les provinces cet essai se fait, à vitesse normale d'extraction, ou à une vitesse équivalente à 1.5 m de chute libre (5.42 m/s). En anglais, ce test est appelé *free-fall test*.

Facteur de sécurité : nous reprenons la définition du RSSM « le rapport entre la charge de rupture et la charge d'utilisation ».

Fonction de sécurité (Le et Dianous, 2008) : Fonction ayant pour but la réduction de la probabilité d'occurrence et potentiellement les effets et conséquences d'un événement non souhaité dans un système. Les fonctions de sécurité peuvent être assurées par des barrières techniques de sécurité, des barrières humaines (activités humaines), ou plus généralement par la combinaison des deux. Une même fonction peut être assurée par plusieurs barrières de sécurité.

En Anglais : SRCF, Safety related control function (Buchweiler, 2008).

Incident : tout événement non désiré ayant pour conséquence des dégâts matériels (sans blessure ou décès parmi les travailleurs).

Mâchoire : partie du parachute enserrant le guide en bois lors du déclenchement du système et enfonçant les dents (*dog teeth*) dans le guide.

Molette : nous reprenons la définition du RSSM « la roue à gorge, située entre la machine d'extraction et le transporteur, qui porte le câble d'extraction et le dévie dans l'axe longitudinal du puits ». En anglais *headsheave* ou *sheave*.

Niveau d'intégrité de sécurité (SIL – Safety integrated level) (ISA, 2005) : Niveau discret parmi quatre niveaux possibles pour la spécification des exigences de sécurité des fonctions de sécurité à assigner aux systèmes concernés par la sécurité (4 le plus élevé, 1 le plus bas). Le concept de SIL s'applique donc au système concerné par la sécurité dans son intégralité et pas à un sous-ensemble (par exemple un capteur).

Parachute : système fixé sur la cage, permettant d'arrêter sa chute dans l'éventualité d'une rupture du câble (ou d'un mou de câble). En anglais ce système est appelé : *safety catches*, *safety dogs*, *safety device*, ou même *gripper system* en Australie.

Pas de câble : Distance, mesurée de façon axiale le long du câble, entre la couronne (plus haut point) d'un toron et la prochaine couronne du même toron. En anglais *lay length*.

Probabilité de défaillance lors d'une sollicitation (PFD) (Le et Dianous, 2008) : Elle correspond à l'indisponibilité du système relatif à la sécurité à un instant donné.

Probabilité de défaillance moyenne lors d'une sollicitation (PFD_{avg}) (Le et Dianous, 2008) : C'est la valeur moyenne de la PFD sur un intervalle de temps donné.

Probabilité moyenne de défaillance par heure (PFH) (Le et Dianous, 2008) : Pour un système non réparable, elle correspond à la moyenne du taux de défaillance sur un intervalle de temps donné.

Proportion de défaillances en sécurité (SFF – Safe Failure Fraction) (Le et Dianous, 2008) : Proportion du taux global des défaillances aléatoires de matériel d'un dispositif qui a comme conséquence une défaillance en sécurité ou une défaillance dangereuse détectée (c'est à dire détectée par un test de diagnostic). On distingue ainsi deux types de défaillances :

- Défaillance en sécurité : Défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction ;
- Défaillance dangereuse : Défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.

Redondance (Le et Dianous, 2008) : Existence, dans un composant, de plus d'un moyen pour accomplir une fonction requise (CEI 6271-1974).

Système instrumenté de sécurité (SIS) (Le et Dianous, 2008) : combinaison de capteurs, d'unité de traitement et d'actionneurs (équipements de sécurité) ayant pour objectif de remplir une fonction ou sous-fonction de sécurité.

Système concerné par la sécurité (ISA, 2005) : système qui :

- Implémente les fonctions de sécurité nécessaires pour atteindre ou maintenir un état sûr pour les équipements contrôlés, et qui ;
- Est destiné à atteindre, seul ou avec d'autres systèmes E/E/PE concernés par la sécurité, l'intégrité de sécurité requise par les fonctions de sécurité.

En Anglais : SRECS, Safety related electrical control system (Buchweiler, 2008).

Skip : dispositif servant à transporter dans un puits de mine des matériaux uniquement au moyen d'une machine d'extraction.

Transporteur : nous reprenons la définition du RSSM « tout dispositif servant à transporter dans un puits de mine des personnes ou des matériaux au moyen d'une machine d'extraction tels une cage, un skip, un cuffat et un ensemble cage-skip ».

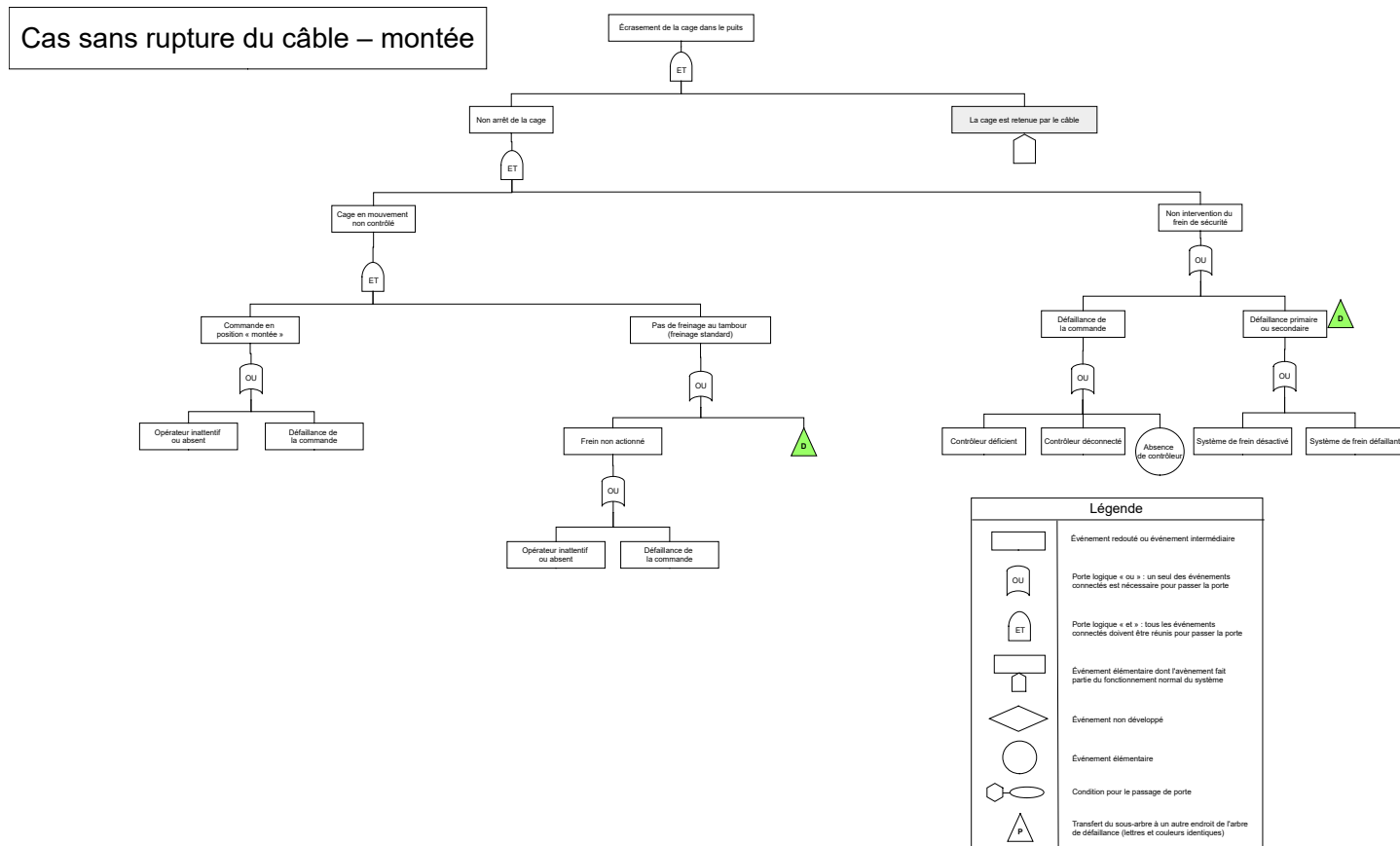
Treuil à tambour : terme générique couvrant les treuils à tambour, à tambour double, en anglais *drum hoist*, ou *drum winder en Australie*. Type de treuil le plus courant en Amérique du Nord : un seul câble par cabine.

Treuil à friction : également appelé treuil Koepe (du nom de son inventeur Carl Friedrich Koepe) (Koepe, 1878 ; Kumar et Hem, 2012 ; Tiley, 2011), ou machine d'extraction à poulie d'adhérence multicâble. En anglais *friction hoist*, ou *Koepe Hoist*. Ce type de treuil comprend plusieurs câbles : câble de frottement, câble d'équilibre. Ce type de treuil est minoritaire en Amérique de Nord. Il peut y avoir un ou plusieurs câbles par cabine. C'est le système le plus proche des ascenseurs commerciaux. En général, les câbles ne sont pas sollicités au-delà de 12 % de leur limite de rupture pour éviter une fatigue trop importante, ce qui limite les profondeurs d'utilisation autour de 1800-2000 m (Anon, 2013).

Treuil Blair : le treuil Blair a été inventé par Robert Blair en 1957 (Anon, 2012 ; Anon, 2013 ; FLSmidth, 2014). Les treuils Blair (en anglais *Blair Multi-Rope hoist* ou BMR) sont caractérisés par des tambours séparés pour chaque câble et plusieurs câbles soutenant le même skip. Un système de compensation est utilisé afin de répartir adéquatement le poids sur les deux câbles. Ce type de treuil permet de soulever de lourdes charges à très grande profondeur : 23 tonnes à 3150m pour Vaal River (FLSmidth, 2014). Ce type de treuil est surtout utilisé en Afrique du Sud, et environ 50 treuils de ce type sont en service dans le monde, dont 90 % environ ont été installés par FLSmidth (Anon, 2013 ; Anon, 2014).

ANNEXE II : ARBRES DE DÉFAILLANCE

Cette annexe présente les deux arbres de défaillance pour le cas de perte de contrôle du déplacement de la cage sans rupture du câble : en montée et en descente.



Cas sans rupture du câble - descente

