Université d'Oran 2
Institut de Maintenance et de sécurité Industrielle

THESE

Pour l'obtention du diplôme de Doctorat « L.M.D »
En Electromécanique

Contribution à la maîtrise des Systèmes Instrumentés de Sécurité (SIS)

Présentée et soutenue publiquement par :
ASKLOU Noureddine

Devant le jury composé de :

HACHEMI Khalid	Professeur	Université d'Oran 2	Président
NOUREDDINE Rachid	Maître de Conférences A	Université d'Oran 2	Rapporteur
ZEBIRATE Soraya	Professeur	Université d'Oran 2	Examinateur
FASLA Souad	Professeur	ENP Oran	Examinateur
HASSINI Noureddine	Professeur	Université de Mostaganem	Examinateur

Année 2018 / 2019

Remerciements

Tout d'abord je remercie Dieu tout puissant de m'avoir donné la force pour accomplir cette thése.

J'exprime mes profonds remerciements à mon directeur de thèse, NOUREDDINE Rachid, Maître de Conférences à l'université d'Oran 2 Mohamed Ben Ahmed, pour son aide inestimable, sa patience et ses encouragements tout au long de ce travail. Ces compétences ont été un atout indéniable à la réussite de ces travaux et m'ont permis d'apprendre énormément durant ces quatre années de collaboration.

Je tiens à exprimer toute ma reconnaissance envers les membres du jury.

Je remercie :

- M. HACHEMI Khalid, Professeur à l'université d'Oran 2 Mohamed Ben Ahmed, pour avoir accepté de présider ce jury et pour l'intérêt qu'il a porté à ce travail.
- M. ZEBIRATE Soraya, Professeur à l'université d'Oran 2 Mohamed Ben Ahmed,
- M. FASLA Souad, Professeur à Ecole Nationale Polytechnique d'Oran Maurice Audin,
- M. HASSINI Noureddine Professeur à Université Abdelhamid Ibn Badis-Mostaganem,

pour avoir accepté d'examiner cette thèse de Doctorat et pour l'intérêt qu'ils ont porté à ce travail.

Ainsi bien à mes chers parents et mon frère Izak et mes sœurs Amel, Radia et Soumia pour leurs aides durant ma vie, et mes amis Tahar, Asmaa, Zohra, Khadija.

Il me reste à remercier toutes les personnes avec qui j'ai travaillé durant ces quatre années.

Table des matières

Table des figures

Liste des tableaux

Acronymes

ALARP As Low As Reasonably Practicable

AMDE Analyse des Modes de Défaillances, de leurs Effets

AMDEC Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité

API Application Program Interface

ATS Automatic Train Stop

BPCS Basic Process Control System

CCF Common-Cause Failure

CCPS Center for Chemical Process Safety

CEI Communauté des États indépendants

DD dangereuses détectées

DGF Dangerous Group Failure

DPS Dynamic Positioning System

DU dangereuses undétectées

E/E/PE Electriques/Electroniques/Electroniques programmables de sécurité

EC Evénement Contact

ED Événement Dangereux

EHSR essential health & safety regulations

ER Événement Redouté

ESD Emergency ShutDown

EUC Equipment Under Control

FE final element

GAME Globalement Au Moins Equivalent

HIPPS High-integrity pressure protection system

IEC International Electrotechnical Comission

ISA Instrument Society of America

ISO International Organization for Standardization

LAHH level alarm high high

LS logic solver

MEM Mortalité Endogène Minimale

OHSAS Occupational Health and Safety Assessment Series

OSHA Occupational Safety and Health Administration

PFD Probability of Failure on Demand

PFH Probability of Failure per Hour

PFS Probability of failing safely

RT Rapport Technique

S sensor

SA Situation d'Accident

SD sécurité détectés

SD Situation Dangereuse

SDV ShutDown Valve

SE Situation d'Exposition

SIF Safety Integrity Function

SIL Safety Integrity Level

SINTEF Stiftelsen for industriell og teknisk forskning qui signifie « Fondation pour la recherche scientifique et industrielle »

SIS Safety Integrity System

SRS Safety Requirements Specification

STR Spurious trip rate (average)

SU sécurité undétectés

UE union européenne

Symboles

t_{CE} Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all the components in the channel of the subsystem) [h]

t_{GE} Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group) [h]

T Proof tests interval [h]

β CCF proportion (® factor) [%]

β_D β for dangerous detected (DD) failures [%]

γ Safety of the proof test [%]

λ Failure rate [/h]

λ_D Dangerous failure rate [/h]

λ_{DD} Dangerous detected failure rate [/h]

λ_{CCF} Dependent failure rate [/h]

λ_{DU} Dangerous undetected failure rate [/h]

λ_{DU1} Dangerous failure rate that can be detected by proof test [/h]

λ_{DU2} Dangerous failure rate that cannot be detected by proof test [/h]

λ_S Safe failure rate [/h]

λ_{SD} Safe detected failure rate [/h]

λ_{SU} Safe undetected failure rate [/h]

ξ Ability of the periodic test to reveal latent failures

Introduction générale

L'industrie de process devient techniquement de plus en plus compliquée et le potentiel des dangers augmente en conséquence si leurs flux ne sont pas convenablement contrôlés. Ainsi lorsque les installations industrielles présentent des risques potentiels pour les personnes, l'environnement et les biens, diverses barrières de sécurité sont mises en œuvre. Celles-ci participent soit à la prévention soit à la protection.

La sécurité des process est une préoccupation majeure pour quiconque travaille dans une usine de production. Selon une estimation de l'OSHA (Occupational Safety and Health Administration) (URL-1), 25 000 installations concernées par la réglementation relative à la gestion de la sécurité opérationnelle des substances chimiques hautement dangereuses disposent probablement de systèmes instrumentés de sécurité (SIS), également connus en tant que systèmes d'arrêt d'urgence.

Pendant plusieurs décennies, les industries de transformation ont utilisé différentes formes de sécurité, selon ce qui était disponible sur le marché. Les relais sont utilisés dans des applications de sécurité depuis les années 1930. Des systèmes à semi-conducteurs, n'utilisant pas de logiciels, ont été développés pour remplacer les relais et sont utilisés dans des applications de sécurité depuis les années 1970. Des automates programmables, ayant recours à des logiciels, ont été développés en vue de remplacer les relais et sont également utilisés dans des applications de sécurité depuis les années 1970. Des directives et normes relatives à la conception et à l'implémentation de systèmes de sécurité ont été instaurées dans diverses industries depuis les années 1990.

Les SIS sont utilisés pour exécuter des fonctions de sécurité, ils sont aussi appelés boucles de sécurité. Ils comprennent les matériels et logiciels nécessaires pour obtenir la fonction de sécurité désirée. Ces systèmes peuvent atteindre un niveau d'intégrité de sécurité important en conformité avec les normes en vigueur telles que la norme CEI 61508 (CEI_61508 2010) et la norme CEI 61511 (CEI_61511 2003), qui traitent de la sécurité fonctionnelle des systèmes. Les SIS ont pour objectif de mettre le procédé qu'ils surveillent en position de repli

de sécurité lorsqu'il évolue vers une voie comportant un risque réel (explosion, feu,..), c'est-à-dire dans un état stable ne présentant pas de risque pour les opérateurs humains et équipements.

Les normes CEI 61508 et CEI 61511, spécifient pour une fonction de sécurité, quatre niveaux possibles de performance de la sécurité. Ils sont appelés niveaux d'intégrité de la sécurité (SIL : safet integrity level). Ces deux normes de sécurité fonctionnelle introduisent une approche probabiliste pour l'évaluation quantitative de la performance du système instrumentés de sécurité et la qualification de cette performance par des niveaux de sécurité références. L'utilisation des probabilités pour la mesure du niveau d'intégrité entraine la mise en place de concepts tels que la probabilité de défaillance a la sollicitation ou la probabilité de défaillance par unité de temps.

La performance des SIS doit être prouvée par l'utilisation de modèles adaptés. Toutefois la CEI 61508 ne définit pas ces modèles. Différentes techniques sont néanmoins préconisées dans les annexes de la norme sans toutefois exclure toute méthode pertinente de calcul probabiliste. Parmi les méthodes citées, on trouve les blocs diagrammes de fiabilité, les arbres de défaillances, les réseaux de Pétri, les chaines de Markov ainsi que les équations simplifiées. La performance ainsi calculée permet de qualifier le niveau d'intégrité de sécurité (SIL) du SIS selon les niveaux définis dans la norme. Cette évaluation consiste à calculer l'indisponibilité moyenne de la fonction de sécurité ou encore la probabilité moyenne de défaillance à la demande (PFD_{avg}: Average Probability of Failure on Demand) pour les SIS faiblement sollicites.

Les méthodes usuelles de calcul de l'indisponibilité des SIS tels que les équations simplifiées, les arbres de défaillances, etc., sont des méthodes probabilistes. Dans ces méthodes issues des études classiques de la sureté de fonctionnement, les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation, …) présentent souvent des imprécisions car le retour d'expérience est malheureusement insuffisant pour valider avec précision les paramètres de défaillance. En plus l'évolution constante de l'environnement et de la complexité des installations industrielles, font que les conditions d'utilisation des composants des SIS utilisés dans les installations peuvent changer pour un même composant et réduit donc la connaissance de leurs processus de dégradation. L'idéal est de disposer d'une quantité d'information suffisante concernant les défaillances des composants pour pouvoir estimer avec précision leurs paramètres de défaillance.

Nous nous situons dans cette problématique et nous nous intéressons plus particulièrement dans ce travail de thèse a la modélisation de l'évaluation des performances des SIS tout en tenant compte des imperfections pouvant entrainer des incertitudes sur leur efficacité.

Cette thèse est structurée en quatre chapitres :

Dans le premier chapitre on présente la problématique de la gestion de risque dans les installations industrielles. Nous avons tout d'abord examiné les définitions des termes fondamentaux dans le domaine de la sécurité, le risque, et le danger et nous avons cherché à faire le lien entre ces différents termes. On a mis en évidence aussi les différentes barrières de sécurité nécessaires. Parmi elle on trouve les barrières techniques qui sont assurée par les systèmes instrumenté de sécurité (SIS) et qui ont pour rôle de mettre le process dans une situation de sécurité. Ceux sont ces systèmes qui font l'objet de notre travail de thèse. Les éléments essentiels des normes liées à ces systèmes sont étudiés et présentés à la fin de ce chapitre.

Dans le deuxième chapitre nous avons étudié les méthodes de conception et d'évaluation des systèmes instrumentés de sécurité. On a d'abord détaillé la constitution et les modes de fonctionnement d'un SIS. Ensuite on a montré comment effectué leur évaluation à travers les niveaux d'intégrité de sécurité (SIL). A la fin on s'est intéressé. Aux différentes méthodes utilisées pour l'allocation de ces SIL. Parmi ces méthodes, la méthode analytique (méthode quantitative) est celle choisie pour la suite de ce travail.

Dans le troisième chapitre on s'intéresse en détail à l'évaluation des performances des systèmes instrumentés de sécurité qui sont exploités en mode faiblement demandé et fortement demandé. Respectivement la probabilité moyenne de défaillance dangereuse à la demande (PFD_{avg}) et la probabilité de défaillance dangereuse par heure (PFH), sont utilisée pour quantifier analytiquement leur fiabilité. On présente à la fin une synthèse des expressions analytiques des PFD_{avg} et PFH permettant l'évaluations des performances des SIS selon le standard de la CEI pour différentes architectures.

Enfin, dans le quatrième chapitre on présente les contributions apportées pour l'évaluation plus précise des performances des SIS. On traite l'imperfection des valeurs de la probabilité moyenne de défaillance à la demande (PFD_{avg}) qui crée une incertitude en ce qui concerne l'efficacité du SIS. Pour surmonter ce problème, de nombreux paramètres tels que les défaillances dangereuses, les défaillances de cause commune, le taux de couverture de diagnostic et les proof tests (tests périodique) sont pris en compte. Afin de souligner l'importance des proof tests (test périodique) et de montrer leurs effets sur les performances de sécurité du SIS quatre études de cas ont été réalisées. Deux nouvelles formules analytiques sont proposées et développées, dans la dernière étude de cas, permettant l'amélioration de l'évaluation des performances de sécurité des SIS.

1

Concepts et exigences de la sécurité

1.1 Introduction

Le terme « sécurité » de manière générale ou globale exprime en réalité une préoccupation légitime, partagée par tous les responsables, quel que soit leur niveau, de maintenir les objectifs potentiels, qu'ils soient des personnes, des populations, des biens et du matériel ou l'environnement, à l'abri des agressions, intentionnelles ou non. Autrement dit, le premier type d'agression est traditionnellement lié à la sécurité, mais il est désormais de plus en plus inclus dans les étapes de prévention des risques industriels. Le deuxième type d'agression, à savoir les agressions non intentionnelles englobant, les accidents que l'on pourrait considérer comme des événements instantanés et localisés et, des types de phénomènes chroniques et différents, y compris les menaces de pollution, qui sont essentiellement liés à la santé publique, à la sécurité sanitaire et à la protection de l'environnement.

Les industries déploient beaucoup d'efforts pour éviter les accidents. Malgré ces efforts, de nombreux accidents se produisent dans le monde et causent des dégâts sur les biens et l'environnement (Ajka en Hongrie (2010), Kazan en Russie (2008), Skikda à Alger (2004), …). L'ampleur et la fréquence de ces accidents ne cessent de susciter de l'intérêt sur les études de sécurité afin de mieux maîtriser les risques (Mechri 2011). Dans les études de sécurité, l'étude de dangers reste l'outil d'information privilégié. Il doit permettre d'identifier les dangers que peut présenter l'exploitation de l'installation et les moyens de réduire la probabilité et les effets des potentiels de dangers.

Dans ce chapitre, on présente les différents aspects qui composent la sureté de fonctionnement, ainsi que les normes de sécurité fonctionnelle.

1.2 Notions élémentaires

1.2.1 Notion de système

Le mot système constitue un concept capital, car il souligne l'importance des liaisons existantes entre les variables qui définissent une situation donnée. « Système » dérive du grec « systema » qui signifie « ensemble organisé » (Perilhon 2004). Plusieurs définitions ont été proposées pour le mot système. Nous nous limitons cependant à celle proposée par J. L. Le Moigne (Le Moigne 1994), figure 1.1, qui considère un système comme : « un objet doté de finalité qui, dans un environnement, exerce une activité et voit sa structure interne évoluer au fil du temps, sans qu'il perde pourtant son identité ». D'une manière générale, un système peut être vu comme :

- Quelque chose (n'importe quoi présumé identifiable),

- Qui fait quelque chose (activité, fonctionnement),EN
- Dans quelque chose (environnement),
- Pour quelque chose (finalité, projet),
- Par quelque chose (structure = support de l'activité),
- Et qui se transforme dans le temps (évolution).

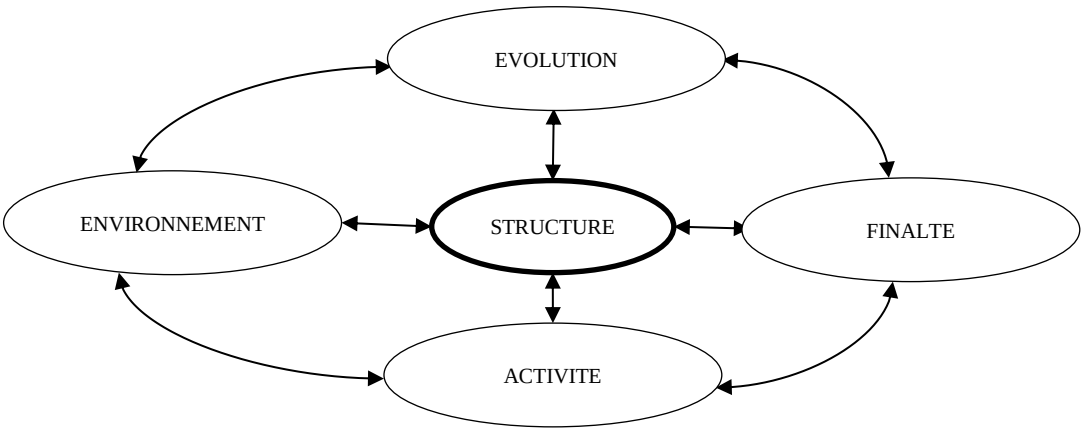


Figure 1.1 Définition du mot système

1.2.2 Notion de sécurité

La sécurité est un état où les dangers, et les conditions pouvant provoquer des dommages d'ordre physique, psychologique ou matériel sont contrôlés (mondiale de la Santé 1998).

Selon Villemeur (Villemeur 1987), « la sécurité est l'aptitude d'une entité à éviter de faire apparaitre, dans des conditions données, des évènements critiques ou catastrophiques ».

Et suivant le guide ISO/CEI 73 (ISO/CEI_Guide_73 2002) élaboré par l'ISO (International Organization for Standardization) sur la terminologie du management du risque, « la sécurité est l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à l'environnement ».

Par ailleurs, la sécurité ne doit pas être définie en termes d'absence totale de danger. En effet, l'absence totale de danger n'est pas nécessairement un idéal à atteindre. À la rigueur, cela peut même être hasardeux (Maslow 2013). La sécurité ne suppose donc pas l'élimination de tous les dangers mais plutôt leur contrôle de manière à préserver la santé et le bien-être des individus et de la communauté.

Dans le cadre des systèmes industriels, la sécurité consiste à mettre en œuvre des moyens évitant l'apparition de dangers. Elle s'énonce alors par l'absence de risque inacceptable, selon la norme CEI 61508 (CEI_61508 2010).

1.2.3 Notion de danger

Selon (Desroches 1995) et la norme de sécurité CEI 61508 (CEI_61508 2010)le danger est défini comme une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes.

Et selon le référentiel OHSAS 18001 (OHSAS_18001 1999) « un danger est une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments ». Les dangers liés à un système sont inhérents au fonctionnement ou au dysfonctionnement du système, soit extérieur au système.

Selon Mazouni (Mazouni 2008), le danger se définit comme une propriété intrinsèque inhérente à un type d'entité ou un type d'évènement qui a la potentialité de provoquer un dommage.

1.2.4 Phénomènes dangereux et situations dangereuses

Un phénomène dangereux désigne en général une source potentielle de dommage. On regroupe sous cette appellation l'ensemble des sources et des facteurs pouvant contribuer à la création du dommage. Ainsi, un bord coupant est un élément dangereux, mais cela ne provoquera pas obligatoirement un dommage.

Une situation dangereuse désigne une situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs phénomènes dangereux.

Selon (Desroches 2005), la situation dangereuse (ou à risque), notée (SD), résulte de la conjonction d'un danger (D) et d'un événement contact (EC) qui met le système en présence ou au contact du danger.

Cette configuration de l'état du système en présence de danger est modélisée par l'expression (CEI_61508 2010) :

$$SD = D \cap EC \tag{1.1}$$

La situation à risque est définie par la nature et le potentiel de dangerosité et la vraisemblance de ce potentiel. De même l'événement redouté final ou accident (A) résulte de la conjonction de la situation dangereuse et d'un événement amorce (EA) qui déclenche la dangerosité sur le ou les éléments vulnérables du système. Cette configuration accidentelle est modélisée par l'expression (CEI_61508 2010):

$$A = SD \cap EA = D \cap EC \cap EA \tag{1.2}$$

La gravité des conséquences directes et indirectes de l'accident, notée G(A) correspond

au montant des dommages en termes de perte ou préjudice mesurable. Le scénario d'accident qui en résulte est visualisé sur le diagramme de la figure 1.2.

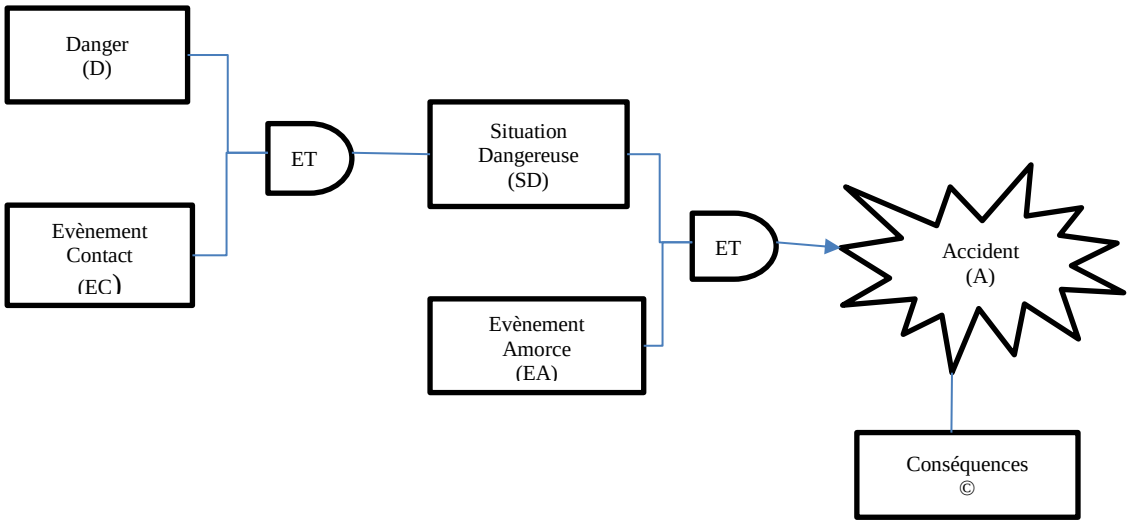


Figure 1.2 Scénario d'accident (adapté de Desroches 2005)

Selon Mazouni et al. (Mazouni et al. 2007), une situation dangereuse se caractérise par le développement d'un phénomène dangereux dès l'apparition d'un événement dangereux. Un phénomène dangereux est une libération de tout ou partie d'un potentiel de danger. Cette concrétisation produit des effets (dispersion d'un nuage de gaz toxique, dérapage d'une voiture, etc.). Ces effets n'entraînent des dommages que si des entités cibles de danger s'exposent, dans un espace de danger pendant une durée suffisante au phénomène dangereux. Le diagramme état/transition du processus accidentel est représenté sur la figure 1.3.

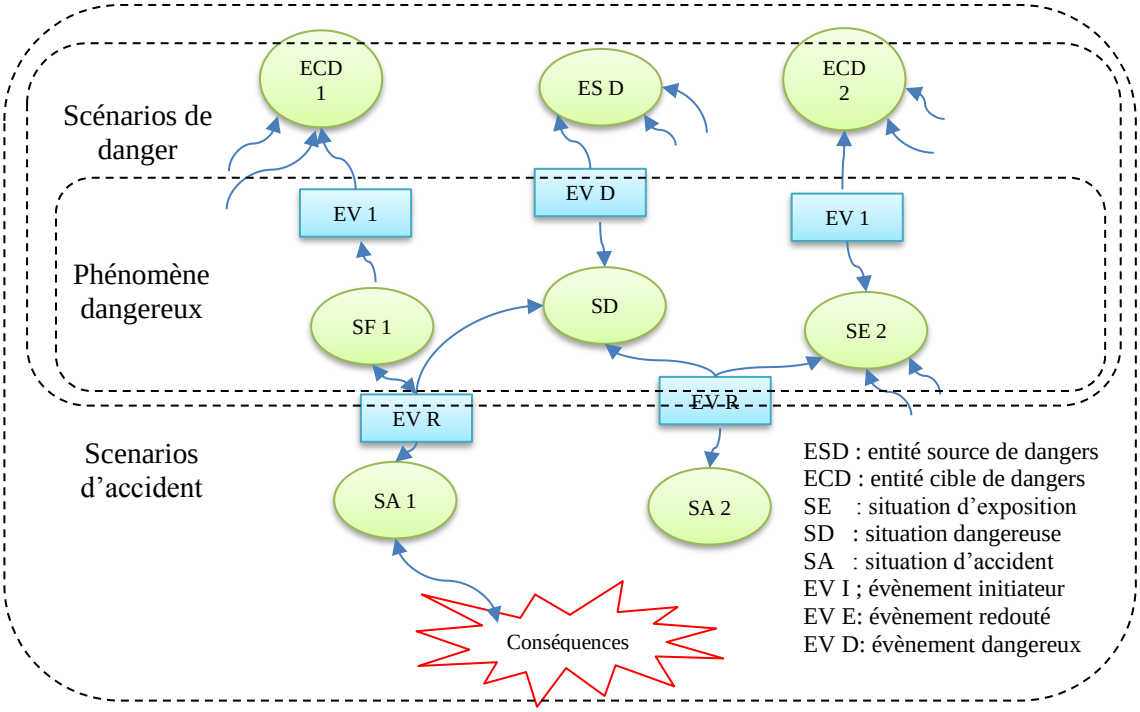


Figure 1.3 Diagramme état/transition du processus accidentel (adapté de Mazouni et al. 2007)

1.3 Risque et analyse des risques

(Rausand 2011) définit le risque comme la réponse combinée aux trois questions suivantes :

- Qu'est-ce qui peut mal tourner ?
- Quelle est la probabilité ?
- Quelles sont les conséquences ?

Pour répondre à la première question, on doit identifier les événements indésirables possibles. La plupart des événements indésirables sont liés à une forme d'énergie et se produisent lorsque cette énergie est libérée. Les fuites de gaz, les réactions d'emballement, les incendies, les explosions, les chutes d'objets, etc. sont des exemples d'événements indésirables dans l'industrie des procédés. Pour répondre à la deuxième question, on doit souvent étudier les causes de chaque événement indésirable et utiliser les données d'expérience et le jugement d'experts pour estimer la probabilité ou la fréquence de l'événement indésirable. La plupart des équipements sous contrôle (EUC : Equipment Under Control,) sont protégées par une ou plusieurs barrières de sécurité qui sont installées pour éliminer ou atténuer les conséquences des événements indésirables. Les réponses aux questions deux et trois dépendent donc du bon fonctionnement des barrières de sécurité.

Le processus de réponse aux trois questions est appelé analyse des risques est parfois illustré par un diagramme en nœud papillon, comme le montre la figure 1.4, où les barrières de sécurité sont illustrées sous forme de rectangles gris. Une introduction approfondie à l'analyse des risques est présentée dans (Rausand 2011).

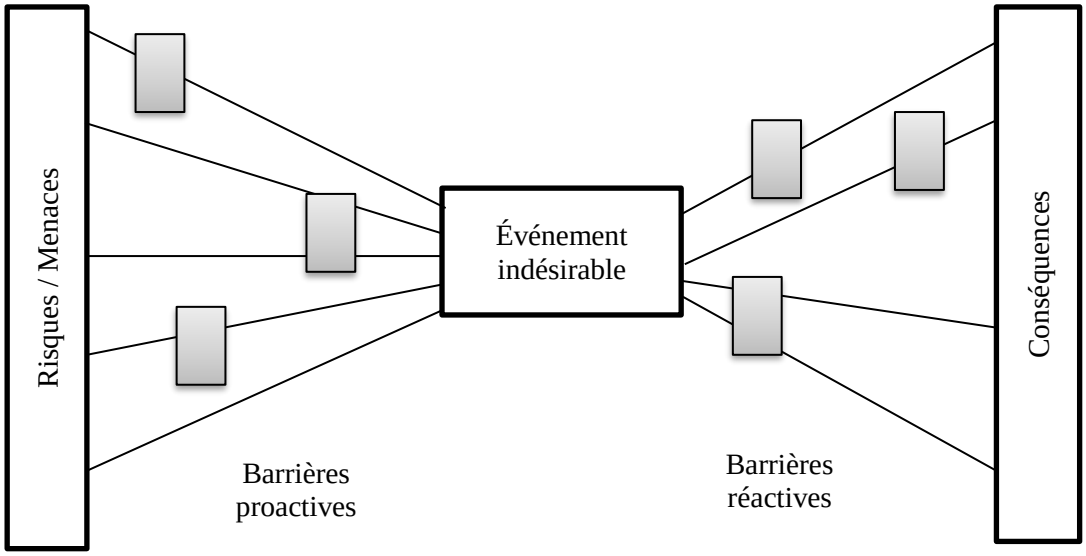


Figure 1.4 Schéma d'un nœud papillon.

Les définitions du risque à deux dimensions sont assez proches. Selon (Villemeur 1988), le risque est une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences.

Et selon le référentiel OHSAS 18001 (OHSAS18001 1999), un risque est la combinaison de la probabilité et de la (des) conséquence(s)de la survenue.

Cependant, il existe des définitions légèrement plus complexes que celle de (Villemeur 1988) et du référentiel OHSAS 18001 (OHSAS18001 1999) dans lesquelles apparaît une troisième dimension : l'acceptabilité du risque, seuil en dessous duquel on accepte l'existence du danger bien que sa gravité et sa probabilité d'occurrence ne soient pas nulles. Par ailleurs, il faut noter que Périlhon (PERILHON 2003) propose une méthode logique pour mettre en évidence la majorité des risques d'une installation : la méthode organisée systémique d'analyse des risques ou MOSAR. Elle fait appel à une décomposition de l'installation en sous-systèmes et une recherche systématique des dangers présentés par chacun d'entre eux, ces sous-systèmes sont remis en relation pour faire apparaître des scénarios de risques majeurs. La démarche peut se poursuivre par une analyse détaillée de type sûreté de fonctionnement. Elle se termine sur la construction des plans d'intervention.

1.3.1 Mesure de risque

Le risque peut être modélisé d'une façon générale et élémentaire par la mesure de sa criticité C, qui est fonction de sa gravité G et de sa probabilité d'occurrence P (CEI_61508 2010):

$$C = P. G \tag{1.3}$$

En général, le risque se rapporte au couple (gravité, probabilité). Le plus souvent cela quantifie le produit de la gravité d'un accident par sa probabilité d'occurrence. Farmer (Farmer 1967) a classifie les risques en deux catégories ; risque acceptable et risque inacceptable en se basant sur la fonction G = f(P), comme le montre la courbe représentée à la figure 1.5.

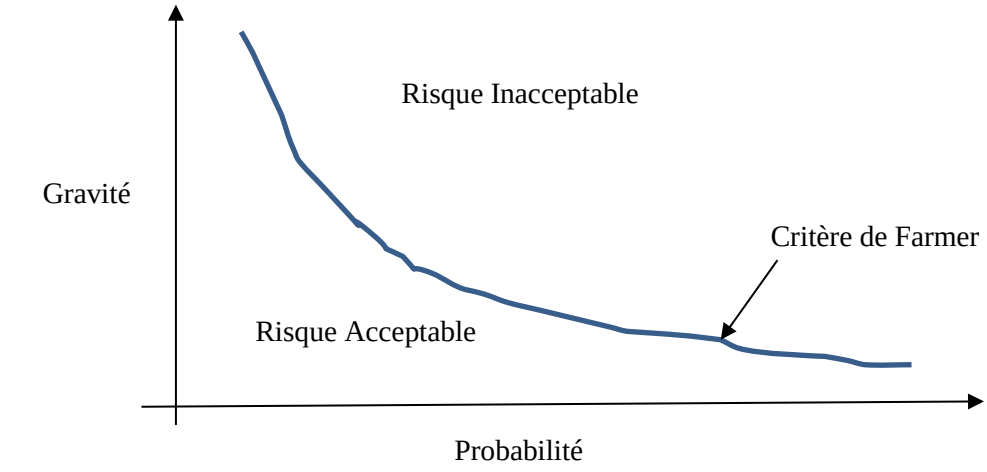


Figure 1.5 Courbe de Farmer (Farmer 1967)

La courbe de Farmer permet une classification du risque en deux sous-ensembles disjoints, correspondants au domaine du risque acceptable et à celui du risque inacceptable.

Selon Gouriveau (Gouriveau 2003), le risque peut être défini par l'association d'événements causes et conséquences d'une situation donnée. Les événements causes peuvent être caractérisés par leur occurrence (P) et les événements effets par leur impact (I) (figure 1.6). La corrélation de ces grandeurs permet de construire un indicateur de risque R = f (occurrence, impact).

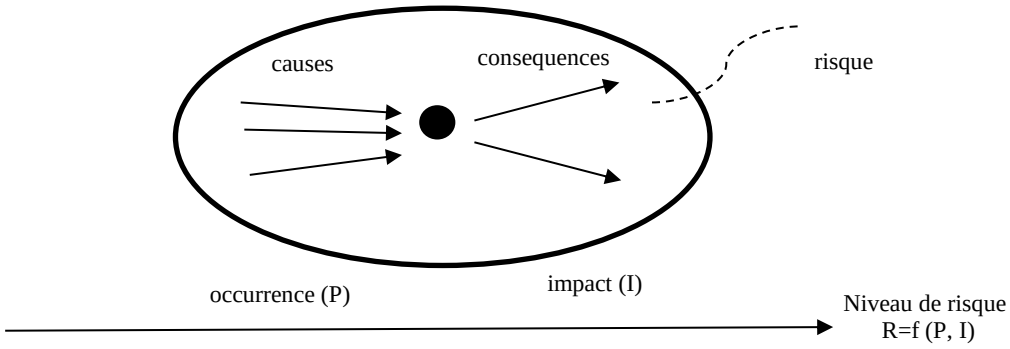


Figure 1.6 Caractérisation du risque (adapté de Gouriveau 2003)

1.3.2 Classification des risques

Dans la littérature, on trouve plusieurs classifications des risques. Selon (Tanzi and Perrot 2009), l'analyse des risques permet de les classer en cinq grandes familles :

- Les risques naturels : inondation, feu de forêt, avalanche, tempête, séisme, etc. ;
- Les risques technologiques : d'origine anthropique, ils regroupent les risques industriels, nucléaires, biologiques, ruptures de barrage, etc. ; les risques de transports collectifs (personnes, matières dangereuses) sont aussi considérés comme des risques

technologiques.

- Les risques de la vie quotidienne : accidents domestiques, accidents de la route, etc. ;
- Les risques liés aux conflits.

Une des classifications les plus répandue est de classer les risques en deux catégories ; les risques naturels et les risques liés à l'activité humaine.

Selon cette classification, les risques peuvent être naturels dans le sens où ils ont trait à un événement sans cause humaine directe avérée. Les causes directes supposées ou indirectes ne doivent pas modifier cette distinction.

Les risques liés à l'activité humaine recouvrent un ensemble de catégories de risques divers :

- Les risques techniques, technologiques, industriels, nucléaires ;
- Les risques liés aux transports ;
- Les risques sanitaires ;
- Les risques économiques, financiers, managériaux ;
- Les risques médiatiques.
- Les risques professionnels.

Finalement, on peut caractériser l'opération de classification des risques par les deux types de classement suivants :

- Classement « subjectif » fait par des individus à partir de l'idée qu'ils se font du risque en se fondant sur leur expérience et leurs connaissances ou « objectif » fait à partir de données statistiques, d'enquêtes, etc. ;
- Classement « qualitatif » caractérisé par l'établissement d'un système d'ordre comparatif ou « quantitatif » basé sur le calcul de probabilités.

1.3.3 Risque acceptable

La notion de risque est essentielle pour caractériser la confiance attribuée à un système. En effet, si nous admettons souvent comme potentiels des dommages sévères, seule leur faible probabilité d'occurrence nous les font accepter (Lamy, Levrat et al. 2006; Simon, Sallak et al. 2007). Par exemple, nous continuons à prendre l'avion malgré les accidents possibles du fait que la probabilité d'un écrasement conduisant aux décès des passagers est extrêmement faible. Nous établissons généralement cet arbitrage en fonction des risques que nous encourront par ailleurs, comme ceux induits par des phénomènes naturels : tremblements de terre, avalanches, inondations, etc.

Selon le référentiel OHSAS 18001 (OHSAS_18001 1999), le risque acceptable est un risque qui a été réduit à un niveau tolérable pour un organisme en regard de ses obligations légales et de sa propre politique de santé et de sécurité au travail.

Selon le Guide 51 ISO/CEI (ISO 1999), le risque acceptable est un risque accepté dans un contexte donné basé sur des valeurs courantes de notre société.

Notons que l'acceptabilité concerne le risque et non la gravité du dommage ou sa probabilité d'occurrence considérées séparément. Ces définitions soulignent également le fait que l'acceptabilité dépend de valeurs courantes de notre société souvent fondées sur des données associées à des phénomènes naturels. Ainsi, nous acceptons de prendre le risque de mourir en prenant l'avion si la probabilité de ce décès par cette cause est identique voire inférieure à la probabilité de décès induit par un séisme ou une crise cardiaque (pour un corps sain) (Beugin 2006).

Les définitions précisent par ailleurs que l'acceptabilité est fonction du contexte. Ce contexte peut tout d'abord caractériser l'état d'un savoir sur des pratiques ou sur une technologie de mise en œuvre.

1.3.4 Risque majeur

D'une manière générale, le risque majeur se caractérise par ses nombreuses victimes, un coût de dégâts matériels, des impacts sur l'environnement (Tanzi and Perrot 2009). Le risque majeur est caractérisé par deux critères qui définissent sa fréquence et sa gravité :

- (a) Une faible fréquence.
- (b) Une énorme gravité (nombreux morts et blessés).

1.3.5 Risque industriel

Le risque industriel se caractérise par un accident se produisant sur un site industriel et pouvant entraîner des conséquences graves pour le personnel, les populations, les biens, l'environnement ou le milieu naturel.

Les actions de prévention des risques industriels majeurs s'appuient sur la connaissance des phénomènes redoutés notamment au travers de l'étude de dangers. Cette prévention s'articule autour de quatre axes principaux.

- La maîtrise du risque à la source ;
- La maîtrise de l'urbanisation ;
- L'organisation des secours ;
- L'information préventive et la concertation.

1.3.6 Concept ALARP

Le principe ALARP (CEI_61508 2010) (As Low As Reasonably Practicable, aussi bas que raisonnablement possible) appliqué au Royaume-Uni (figure 1.7) intègre une zone pour un risque inacceptable, une zone d'acceptation de risque et une zone ALARP dans laquelle les objectifs globaux de sécurité sont fixés. Si le risque analysé se trouve dans cette zone, les moyens mis en œuvre pour atteindre le niveau de sécurité désiré doivent être évalués ainsi que la réduction du risque qu'ils apportent.

La notion de raisonnable considère en particulier le coût lié à la réduction de risque et le ratio gains obtenus / niveau d'investissement.

La figure 1.7 illustre le principe ALARP. Elle fait apparaître trois zones, une zone d'acceptation du risque, une zone de rejet de risque et une zone appelée zone ALARP dans laquelle les objectifs de sécurité sont fixés. Les zones sont délimitées par des fréquences (par heure) de risques donnés. A titre d'exemple, la zone ALARP peut être délimitée par l'intervalle [10^{-9} ; 10^{-6}] (CENELEC–NF-EN-50126 2000). Si le risque analysé se trouve dans cette zone, les moyens à mettre en œuvre pour atteindre le niveau d'intégrité de sécurité désiré doivent être évalués ainsi que la réduction du risque qu'ils apportent.

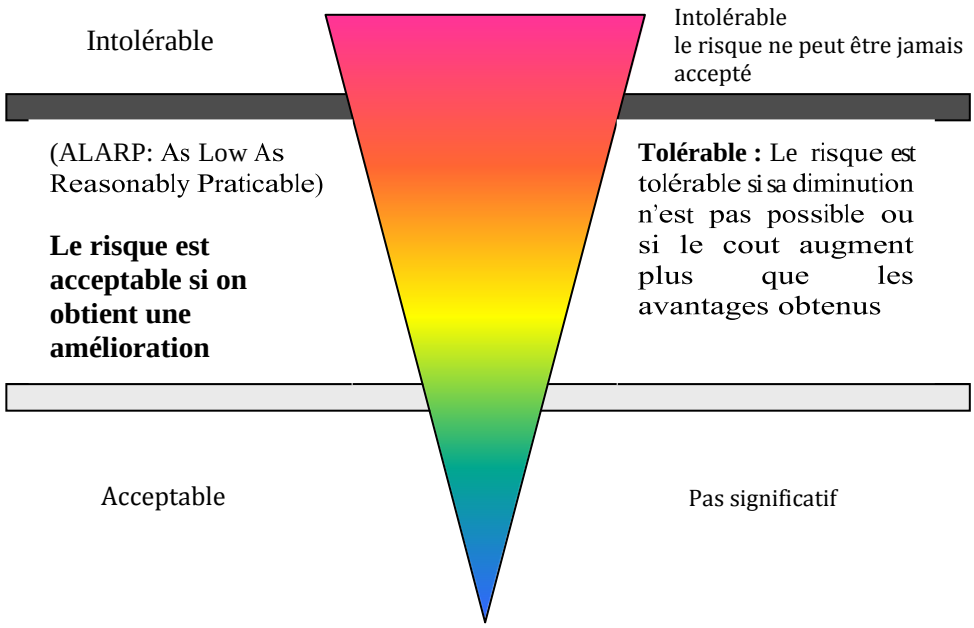


Figure 1.7 Risque tolérable et ALARP (CEI_61508 2010)

D'autres principes d'acceptation de risques existent tels que le principe allemand MEM (Mortalité Endogène Minimale) et le principe français GAME (Globalement Au moins Equivalent) (CENELEC–NF-EN-50126 2000).

Le principe MEM fixe les objectifs globaux de sécurité par référence à la mortalité endogène minimale d'un individu, c'est-à-dire le risque ambiant pour une personne âgée de 5 à 15 ans (fixé à 2.10^{-4}/an). Les risques liés aux systèmes techniques sont considérés comme contribuant à 5% du risque individuel.

Le principe français GAME impose pour un nouveau système le respect des mêmes exigences de sécurité qu'atteint un système équivalent existant. Ce principe nécessite de connaître les objectifs de sécurité et le comportement relatif à la sécurité du système de référence.

1.4 Sécurité fonctionnelle

Chaque jour, des personnes sont blessées et tuées, des biens matériels et financiers importants sont perdus et l'environnement est pollué à cause des défaillances des systèmes critiques de sécurité et du manque de sécurité fonctionnelle. Les accidents peuvent aller d'un seul accident à des catastrophes telles que l'accident de Macondo dans le golfe du Mexique en 2010 et l'accident nucléaire de Fukushima Daiichi au Japon en 2011. Si les systèmes essentiels à la sécurité avaient fonctionné comme prévu, beaucoup de ces accidents auraient pu être évités.

Suivant la norme CEI 61508, la sécurité fonctionnelle est le sous-ensemble de la sécurité globale qui dépend du bon fonctionnement d'un système ou d'un équipement en réponse à ses entrées. La sécurité fonctionnelle veille donc à contrôler l'absence de risques inacceptables qui pourraient :

- Engendrer des blessures,
- Porter atteinte, directement ou indirectement, à la santé des personnes,
- Dégrader l'environnement,
- Altérer la propriété.

La sécurité fonctionnelle couvre les produits ou systèmes mettant en œuvre des solutions de protection fondées sur diverses technologies : Mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable, optique, etc. Ou toute combinaison de ces technologies.

Pour atteindre une fiabilité suffisamment élevée, un certain nombre d'analyses de fiabilité détaillées doivent être effectuées, en particulier dans la phase de conception. Les concepteurs de systèmes sont formés pour développer des systèmes capables d'exécuter les fonctions souhaitées, mais ils oublient souvent de considérer comment les systèmes peuvent échouer. C'est le rôle des ingénieurs de fiabilité et des analystes de fiabilité qui devraient faire partie de l'équipe de conception. Un certain nombre de méthodes analytiques sont disponibles

pour identifier les défaillances potentielles du système et les causes de ces défaillances. Certaines méthodes sont qualitatives, d'autres sont quantitatives et d'autres sont à la fois qualitatives et quantitatives. Le résultat le plus important des analyses de fiabilité est la meilleure compréhension de la façon dont le système peut se comporter et comment il peut échouer dans les différentes situations opérationnelles. Cette connaissance peut aider l'équipe de conception à améliorer la fiabilité du système et à éviter les échecs.

1.5 Barrières de sécurité

Le terme « barrière de sécurité » est un terme courant dans la plupart des analyses de risques et se chevauche en partie avec la définition d'un système critique pour la sécurité. Un système de barrières de sécurité peut être un système technique ou un effort humain et organisationnel. La barrière de sécurité n'est donc pas le même concept que le système critique pour la sécurité. Une procédure d'urgence peut, par exemple, être une barrière de sécurité mais n'est pas un système critique pour la sécurité.

Les systèmes de barrières de sécurité sont également appelés défenses, protections, contre-mesures ou couches de protection. Un système de barrière de sécurité peut exécuter une ou plusieurs fonctions de barrière de sécurité et peut généralement être divisé en plusieurs sous-systèmes et éléments de barrière de sécurité.

1.5.1 Classification des barrières de sécurité techniques ou humaine.

Les barrières de sécurité peuvent également être classées en fonction de leur nature.

- Barrières techniques de sécurité. Une barrière technique de sécurité est une barrière de sécurité dont la fonction de barrière est assurée par un système instrumenté de sécurité (SIS). Le système instrumenté de sécurité est un système avec une ou plusieurs fonctions instrumentées de sécurité (SIF : Safety Integrity Function). Il se compose de capteurs (S), d'unités logiques (LS), et d'actionneurs (FE).
- Barrières de sécurité humaines et organisationnelles. Une barrière humaine est une barrière de sécurité dont la fonction de barrière est assurée par une ou plusieurs personnes, parfois en utilisant des éléments techniques de barrière de sécurité. Le terme barrière de sécurité organisationnelle est utilisé pour désigner les barrières de sécurité sous forme de lois, de règlements, de procédures, de formation, etc.

Les barrières de sécurité peuvent être classées selon qu'elles sont actives ou passives, techniques ou humaines / organisationnelles Figure 1.8.

Barrières de sécurité proactives ou réactives. Les barrières de sécurité proactives et réactives sont illustrées dans le diagramme du nœud papillon de la figure 1.4.

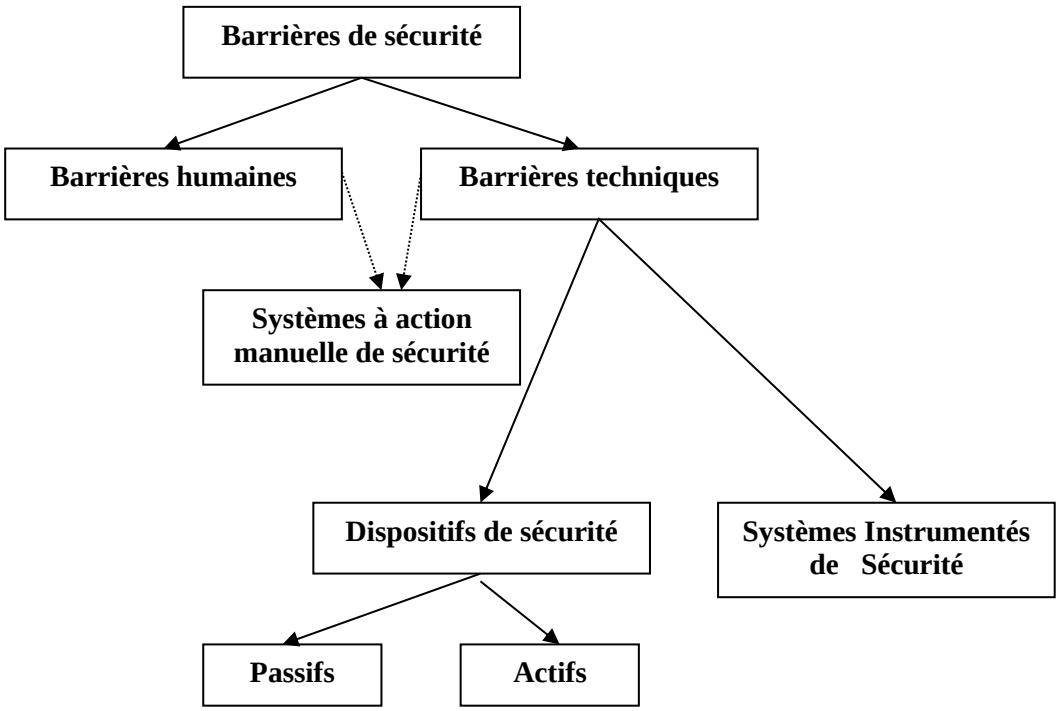


Figure 1.8 Typologie des barrières techniques de sécurité

- Barrière de sécurité proactive. Une barrière de sécurité qui est installée pour empêcher un ou plusieurs événements indésirables dans l'EUC de se produire. Une barrière de sécurité proactive est aussi appelée barrière réductrice de fréquence parce qu'elle devrait réduire la fréquence des événements indésirables.
- Barrière de sécurité réactive. Une barrière de sécurité qui est installée pour éliminer ou atténuer les conséquences d'un ou plusieurs événements indésirables dans l'EUC (s'ils se produisent). Une barrière de sécurité réactive est également appelée barrière réductrice de conséquences.

Barrières de sécurité passive ou active. Les barrières de sécurité peuvent également être classées comme barrières de sécurité passive ou active :

- Barrière de sécurité passive. Une barrière dont la fonction de sécurité est toujours disponible en tant que propriété inhérente de l'EUC ou du lieu de travail. Des exemples de barrières de sécurité passive sont les murs coupe-feu, les moyens de séparation physique (p. ex. clôtures, boucliers), les logements utilisés pour protéger l'équipement contre l'intrusion de gaz ou d'eau, etc.
- Barrière de sécurité active. La fonction de sécurité d'une barrière de sécurité active n'est pas toujours disponible, mais sera exécutée en réponse à certains événements. Un système d'arrêt d'urgence (ESD : Emergency shutdown) dans une installation de traitement est une barrière de sécurité active et n'est activé que lorsqu'une situation dangereuse se produit.

1.5.2 Classification des barrières de sécurité selon le mode de fonctionnement

. Les barrières de sécurité peuvent être classées en fonction de la fréquence à laquelle les fonctions de la barrière sont demandées tableau 1.1. Nous distinguons entre :

- Mode demandé. Ces fonctions de barrière de sécurité ne participent pas activement à la commande de l'EUC et ne sont activées que lorsqu'une situation dangereuse (c'est-à-dire une demande, un événement indésirable) se produit. On distingue souvent entre :
  - Mode à faible demande. On dit qu'une barrière de sécurité fonctionne en mode de faible demande lorsque sa fonction n'est exigée qu'une seule fois par an. Le système d'airbags dans une automobile est un exemple de barrière de sécurité fonctionnant en mode faible demande.
  - Mode haute demande. On dit qu'une barrière de sécurité fonctionne en mode de forte demande lorsqu'elle est exposée à des demandes distinctes qui surviennent plus d'une fois par an. Un dispositif de sécurité à détection de présence pour un robot en mouvement est (généralement) un exemple de barrière de sécurité fonctionnant en mode haute demande.
- Mode continu. On dit d'une barrière de sécurité qu'elle fonctionne en mode continu alors que sa fonction est toujours cruciale. Dans ce cas, la barrière de sécurité est intégrée au système de commande EUC et un événement indésirable se produit lorsque la barrière de sécurité tombe en panne. Les exemples de barrières de sécurité fonctionnant en mode continu sont :
  - Les systèmes de commande de vol électriques pour les commandes de vol des aéronefs
  - Les systèmes de positionnement dynamique (DPS : Dynamic Positioning System) pour les navires et les plates-formes offshore.

Le tableau 1.1 donne quelques exemples de systèmes de barrières de sécurité qui fonctionnent en mode de faible et de forte demande.

Barrière de sécurité	Faible demande	Demande élevée
Système d'arrêt d'urgence (ESD) dans une usine de traitement	X	
Détection d'incendie et de gaz dans une installation de traitement	X	
Système de signalisation pour les applications ferroviaires		X
Système d'airbag dans une automobile	X	

Système de freinage antiblocage dans un véhicule automobile		X

Tableau 1.1 Modes de demande pour certaines barrières de sécurité sélectionnées.

1.6 Couches de protection

Dans l'industrie de process, les barrières de sécurité sont souvent appelées couches de protection et sont parfois visualisées comme sur la figure 1.9, où les couches sont représentées dans l'ordre dans lequel elles sont activées. En suivant cette séquence, on fait la distinction entre :

- Conception du processus (en utilisant des principes de conception intrinsèquement sûrs).
- Contrôle, à l'aide de fonctions de commande de base, d'alarmes et de réponses de l'opérateur pour maintenir le système dans un état normal (stable).
- La prévention, à l'aide de systèmes à instruments de sécurité (SIS) et d'alarmes critiques pour la sécurité, afin d'agir en cas d'écart par rapport à l'état normal et d'empêcher ainsi la survenue d'un événement indésirable.
- Mitigation, à l'aide de SIS ou de fonctions mises en œuvre par d'autres technologies, pour atténuer les conséquences de l'événement non désiré. C'est le cas, par exemple, de la protection assurée par les soupapes de surpression.
- La protection physique, en utilisant des barrières de sécurité permanentes (et plus robustes) pour améliorer l'atténuation. Par exemple, la protection obtenue grâce à la mise en place de digues et de barricades.
- Détection des incendies et des gaz et distinction, en tant que troisième stratégie visant à atténuer les conséquences en évitant l'inflammation, et donc un accident, des gaz et mélanges explosifs.
- Intervention d'urgence, en utilisant divers moyens pour limiter la gravité de l'accident, aussi bien localement que dans la communauté. Par exemple, les procédures de sauvetage, la mobilisation des équipes de sauvetage et l'utilisation des issues de secours.

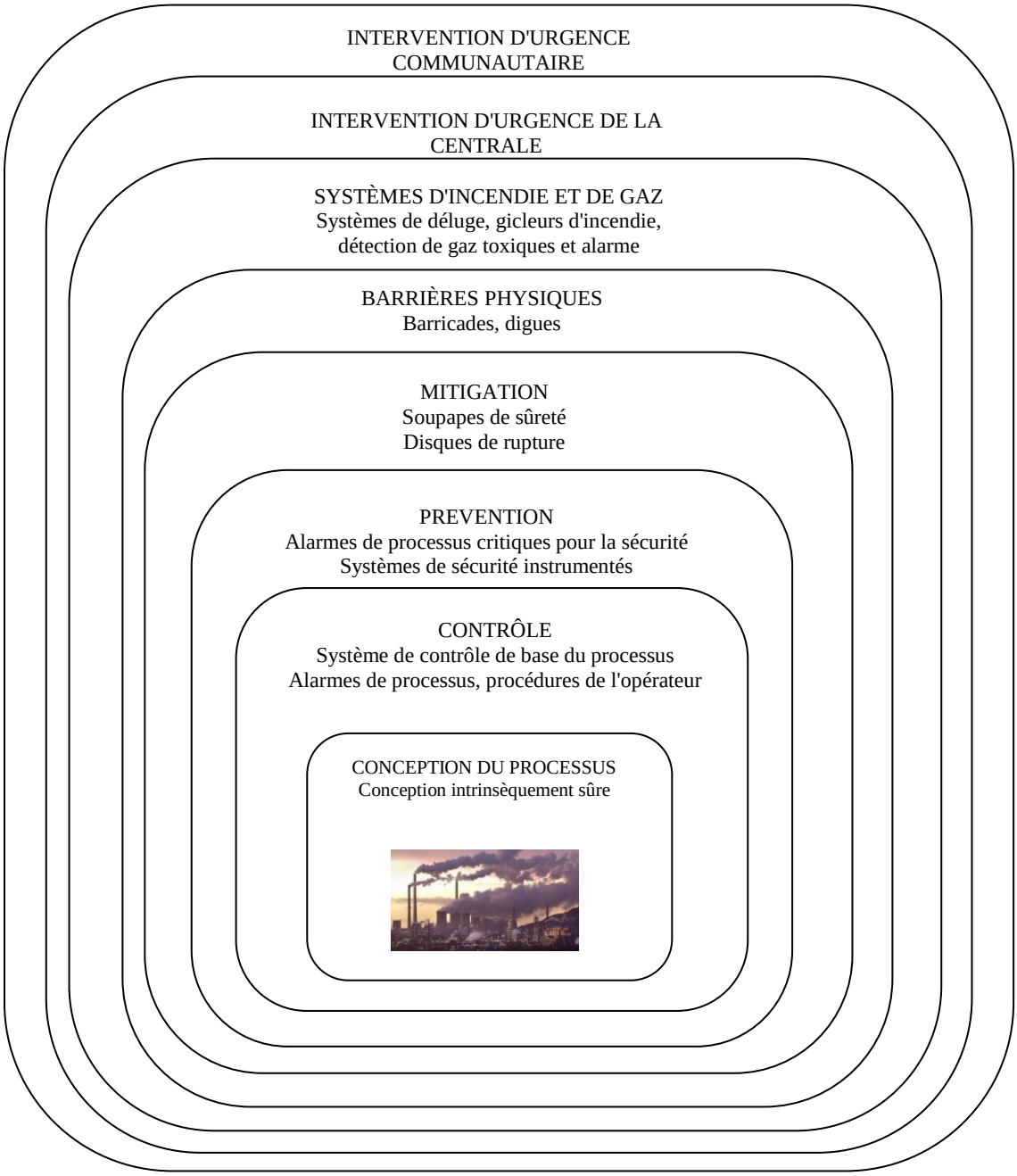


Figure 1.9 Couches de protection pour les usines de traitement (Rausand 2014)

1.7 Normes de sécurité fonctionnelle

Parmi les normes de sécurité fonctionnelle utilisées, on peut citer la norme ISA-84 (ISA-84.00.01–2004 2004), la norme CEI 61508 (CEI_61508 2010) et la norme SINTEF (SINTEF 2013b).

On présente ici la norme CEI 61508, qui est la plus répandue et utilisé par la communauté scientifique et le secteur industriel, et ses normes sectorielles.

1.7.1 Norme générique CEI 61508 Standard

La norme internationale Sécurité fonctionnelle des systèmes électriques/électroniques/programmables liés à la sécurité CEI 61508 (CEI_61508 2010) est une norme générique basée sur les performances pour les systèmes liés à la sécurité qui impliquent la technologie E/E/PE. La CEI 61508 fournit une base pour la spécification, la conception et l'exploitation de tous les types de SIS. L'objectif de la norme est de donner des exigences globales et de servir de base à l'élaboration des normes sectorielles.

La norme CEI 61508 présente plusieurs caractéristiques principales. La première est l'approche du cycle de vie qui définit les exigences nécessaires pour un SIS « du berceau à la tombe ». Une autre caractéristique principale est qu'elle est fondée sur les risques, de sorte que les exigences relatives au SIS doivent être fondées sur une évaluation des risques (Rausand 2014).

La norme comporte sept parties (voir encadré) et introduit 16 phases du cycle de vie, qui peuvent être divisées en cinq étapes principales.

- Évaluation des risques (couvrant les phases 1 à 5), dont le résultat est la formulation des fonctions de sécurité requises et des objectifs de fiabilité associés.
- Conception et construction (couvrant les phases 9-11), dont le résultat est un SIS comprenant des éléments matériels et logiciels.
- Planification de l'intégration, de la validation globale et de l'exploitation et de la maintenance (couvrant les phases 6-8).
- Exploitation et maintenance, y compris la gestion du changement (couvrant les phases 14-15). Toute modification apportée au SIS devrait entraîner le retour à la phase de cycle de vie la plus appropriée lorsqu'une modification a été demandée.
- Élimination, qui met fin à la vie du SIS.

1.7.2 Normes sectorielles

Les normes sectorielles liées à la norme CEI 61508 ont été élaborées pour plusieurs secteurs, tels que l'industrie des procédés, les systèmes de machines, les centrales nucléaires, les applications ferroviaires et l'industrie automobile. La présente section donne une brève introduction à certaines de ces normes.

Industrie de processus. La norme Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le secteur industriel CEI 61511 (CEI_61511 2003) est basée sur la norme CEI 61508 et constitue la norme principale pour l'application des SIS dans l'industrie des procédés, y compris l'industrie pétrolière et gazière.

CEI 61508 : Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité.

Parties normatives :

PARTIE 1 : Exigences générales

Définit le modèle global de cycle de vie de sécurité. La norme utilise des techniques qualitatives ou quantitatives pour identifier le risque de processus pour le système lié à la sûreté. Ces techniques se concentrent sur la gestion de projet, l'assurance qualité et la gestion de la configuration.

PARTIE 2 : Exigences pour les systèmes électriques / électroniques / électroniques programmables liés à la sécurité

Fournit des objectifs pour le développement de la sécurité de l'E / E / PES. Le logiciel est défini plus en détail dans la partie 3. Cependant, il convient de noter que la partie 2 conserve sa compétence.

PARTIE 3 : Exigences logicielles

Fournit des objectifs pour le développement de la sécurité des logiciels résidant dans l'E/E/PES.

PARTIE 4 : Définitions et abréviations

Contient des définitions, des abréviations et la terminologie utilisée dans le processus de sécurité qui doit être respectées afin d'établir et de maintenir la cohérence.

Pièces informatives :

PARTIE 5 : Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité

Fournit l'approche formelle pour déterminer le niveau d'intégrité de sécurité (SIL : Safety integrity level) du système de sécurité (SIL est décrit dans la section 5.5).

PARTIE 6 : Directives sur l'application de la CEI 61508-2 et de la CEI 61508-3

Fournit des directives spécifiques pour l'application des parties 2 et 3 de la norme CEI 61508.

PARTIE 7 : Aperçu des techniques et mesures

Fournit des détails sur les techniques et mesures de sécurité pertinentes pour les parties 2 et 3.

Supplément :

PARTIE 0 : Sécurité fonctionnelle et CEI 61508

Il s'agit d'un rapport technique (RT) portant le numéro CEI / TR 61508-0 et qui ne fait pas formellement partie de la CEI 61508. La partie 0 explique et commente la norme.

La CEI 61511 concerne principalement les SIS fonctionnant en mode à faible demande, c'est-à-dire lorsque les demandes pour la SIF sont des événements discrets qui se produisent

plutôt rarement. Le SIS est par conséquent une couche de protection indépendante en plus du BPCS (Basic Process Control System, système de contrôle de processus de base). Le SIS ne joue aucun rôle actif pendant le fonctionnement normal et n'est activé que s'il y a une demande.

La CEI 61511 s'applique lorsqu'un SIS est basé sur une technologie éprouvée ou une technologie dont la conception a été vérifiée par rapport aux exigences de la CEI 61508. Le développement de nouvelles technologies dépasse le champ d'application de la CEI 61511. Pour cette raison, la norme CEI 61511 est parfois appelée la norme de l'utilisateur final et de l'intégrateur de système, tandis que la norme CEI 61508 est appelée la norme du fabricant.

CEI 61511 : Sécurité fonctionnelle Systèmes instrumentés de sécurité pour le secteur de l'industrie de transformation PARTIE 1 : Cadre, définitions, système, matériel et logiciels requis PARTIE 2 : Lignes directrices pour l'application de la norme ICE61511-I PARTIE 3 : Directives pour la détermination des niveaux d'intégrité de sécurité requis La CEI 61511 est la norme sectorielle pour l'industrie des procédés, y compris l'industrie pétrolière et gazière. Dans ce cas, les SIS sont supposés fonctionner principalement en mode à faible demande.

Des lignes directrices ont été publiées pour faciliter l'application de la CEI 61508 et de la CEI 61511. Deux lignes directrices notables sont :

- Lignes directrices pour des systèmes de protection instrumentés sûrs et fiables publiées par le Centre pour la sécurité des procédés chimiques (CCPS 2007).
- Application de la CEI 61508 et de la CEI 61511 dans l'industrie pétrolière norvégienne publié par l'Association norvégienne du pétrole et du gaz (NOG-070 2004) .

Systèmes de machines. La sécurité des machines en Europe est régie par la Directive Machines de l'UE (EU-2006/42/EC 2006). La première édition de cette directive a été approuvée en 1989 et elle a été modifiée et mise à jour à plusieurs reprises. La Directive Machines de l'UE donne les exigences essentielles de santé et de sécurité (EHSR : Essential health and safety requirements) relatives à la conception et à l'utilisation des machines et laisse les détails aux normes harmonisées. Il n'est pas obligatoire de suivre les normes, mais si l'on se conforme à une norme harmonisée, l'EHSR associé est respecté.

Les premières lignes de ces exigences sont :

Les systèmes de commande doivent être conçus et construits de manière à éviter les situations dangereuses. Par-dessus tout, ils doivent être conçus et construits de telle sorte que :

- Ils peuvent résister aux contraintes d'exploitation prévues et aux influences extérieures,
- Un défaut dans le matériel ou le logiciel du système de commande n'entraîne pas de

situations dangereuses,

- Les erreurs dans la logique du système de contrôle n'entraînent pas de situations dangereuses,
- L'erreur humaine raisonnablement prévisible pendant le fonctionnement n'entraîne pas de situations dangereuses.

La première norme développée pour les systèmes de commande de machines a été l'EN 954-1 (EN_954-1 1997). Comme les exigences de la Directive Machines de l'UE ont été acceptées et mises en œuvre dans les lois nationales de nombreux pays à travers le monde, l'accord de l'UE sur les machines a été conclu. Les normes EN ont été transférées dans des normes internationales. La norme EN 954-1 était la suivante a donc été transféré, sous une forme légèrement modifiée, dans la norme ISO 13849-1 (ISO_13849-1 2006). Le L'EN 954-1 a été développée avant la fabrication de la CEI 61508 et n'est donc pas une norme entièrement conforme à la norme CEI 61508. Il en va de même pour la norme ISO 13849-1.

Une autre norme, CEI 62061 (CEI_62061-1 2010) « Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables liés à la sécurité » a donc été développée sur la base de l'CEI 61508. Aujourd'hui, les normes ISO 13849-1 et CEI 62061 sont acceptées en tant que normes harmonisées relatives aux systèmes de commande des machines basés sur l'E/E/PE. La relation entre ISO 13849-1 et CEI 62061 est décrite dans le rapport technique CEI TR 62061 -1.

. Une norme spéciale a été élaborée pour l'évaluation des risques des machines. Il s'agit de la norme ISO 12100 (ISO_12100 2010) « Sécurité des machines - Principes généraux de conception - Évaluation des risques et réduction des risques ». Les SIS des systèmes de machines fonctionnent principalement en mode haute demande ou en mode continu et sont souvent intégrés au système de contrôle des machines.

Industrie nucléaire. La norme CEI 61513 (CEI_61513 2004) a été élaborée en tant que norme sectorielle pour l'industrie nucléaire, sur la base de la norme CEI 61508. Dans la CEI 61513, un SIS est appelé système d'instrumentation et de contrôle (I&C) et défini comme un « système, basé sur la technologie électrique et/ou électronique et/ou électronique et/ou électronique programmable, exécutant des fonctions I&C ainsi que des fonctions de service et de surveillance liées à l'exploitation du système lui-même ».

Industrie automobile. ISO 26262 (ISO_26262 2011) est la norme sectorielle pour les véhicules routiers selon la norme CEI 61508. Il a été développé pour les systèmes électriques et/ou électroniques installés dans les voitures particulières de série d'une masse totale maximale de 3 500 kilogrammes. La norme comporte neuf parties normatives et une ligne directrice pour l'utilisation de la norme ISO 26262 en tant que partie 10.

Transport ferroviaire. Trois normes européennes : Les normes EN 50126, EN 50128 et EN 50129 ont été développées avec un champ d'application similaire à CEI 61508. Les trois normes EN ont ensuite été transférées dans les normes CEI.

- CEI 62278 (EN 50126) (CEI_62278 2002). Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (RAMS).
- CEI 62279 (EN 50128) (CEI_62279 2002). Applications ferroviaires - Systèmes de communication, de signalisation et de traitement - Logiciels pour systèmes de contrôle et de protection ferroviaire.
- CEI 62425 (EN 50129) (CEI_62425 2007). Applications ferroviaires - Systèmes de communication, de signalisation et de traitement - Systèmes électroniques de sécurité pour la signalisation.

Les trois normes n'ont pas le format des normes sectorielles liées à la CEI 61508, mais le respect des exigences de ces normes est considéré comme suffisant pour garantir le respect des exigences de la CEI 61508.

1.8 Conclusion

Ce chapitre a souligné la problématique de la gestion de risque dans les installations industrielles. Nous avons tout d'abord examiné les définitions des termes fondamentaux dans le domaine de la sécurité, le risque, et le danger et nous avons cherché à faire le lien entre ces différents termes.

En utilisant la notion de risque tolérable et l'identification / évaluation des risques inhérents au processus, la quatrième partie de ce chapitre nous a permis de définir les différentes barrières de sécurité.

Les systèmes instrumentés de sécurité (SIS) sont des barrières techniques qui ont pour rôle de mettre un process dans une situation de sécurité. Ceux sont ces systèmes qui font l’objet de notre travail de thèse. Les éléments essentiels de la norme CEI 61508, liées à ces systèmes, sont étudiés et présentés dans ce chapitre.

Dans le second chapitre, on traite en détail les systèmes instrumentés de sécurité (SIS).

2

Systèmes instrumentés de sécurité

2.1 Introduction

Dans d'industrie, la source prédominante de danger est le processus lui-même à travers ses déviations incontrôlées, qui sont toujours possibles. L'ampleur de ces écarts est normalement limitée, régulée par un système de contrôle, qui peut néanmoins échouer. Dans ce cas, l'action de régulation défaillante du système de commande est remplacée par une intervention d'un opérateur et/ou de systèmes de sécurité. Parmi ceux-ci, on trouve les systèmes instrumentés de sécurité (SIS) qui sont au cœur même de la sécurité fonctionnelle. C'est ce sous-ensemble mondial de sécurité qui constitue le cadre de nos travaux.

Les systèmes instrumentés de sécurité sont utilisés pour exécuter des fonctions de sécurité dans les industries de production par processus (ou de transformation). Ce sont des moyens de sécurité chargés de surveiller que le procédé ne franchit pas certaines limites, au-delà desquelles il pourrait devenir dangereux, et d'actionner les organes de sécurité lorsqu'un tel danger se présente.

L'objet de ce chapitre est de définir dans un premier temps ce qu'est un SIS et de présenté ses principes de conception. Dans la dernière partie, on s'intéresse aux différentes méthodes, citées par les normes de sécurité, utilisées pour allouer les niveaux SIL des SIS

2.2 Systèmes instrumentés de sécurité

2.2.1 Définition d'un SIS

La norme CEI 61511 (CEI_61511 2003)définit les systèmes instrumentés de sécurité de la façon suivante : système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux).

La norme CEI 61508(CEI_61508 2010)définit quant à elle les systèmes relatifs aux applications de sécurité par : un système E/E/PE (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.

Les systèmes instrumentés de sécurité sont installés pour protéger un équipement sous contrôle (EUC). Selon l'application, l'EUC est aussi appelé processus, machines et plusieurs autres noms. La CEI 61508 ne donne pas d'exigences particulières sur la manière de définir une EUC, et l'utilisateur a donc une grande liberté dans la définition du champ d'application et des limites de l'EUC. Un système instrumenté de sécurité est un système visant à mettre le procédé en état stable ne présentant pas de risque pour l'environnement et les personnes lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement

(explosion, feu…).

Les systèmes suivants en sont des exemples :

- Système d'arrêt d'urgence (ESD : Emergency Shutdown Systems), utilisé, par exemple, dans les industries chimique et pétrochimique.
- Système d'arrêt automatique de train (ATS : Automatic Train Stop), utilisé dans le domaine ferroviaire.
- Système de freinage de l'automobile.
- Airbag.
- Système de détection de surface d'un avion.
- Equipements médicaux critiques de traitement et de surveillance.

2.2.2 Constitution d'un SIS

Un SIS se compose de trois sous-systèmes, figure 2.1:

- Sous-système de capteurs - détecte un danger potentiel et produit un signal électrique approprié qui est envoyé à l'unité logique. Exemples de capteurs de pression des transmetteurs, des transmetteurs de niveau, des jauges de température, etc.
- Sous-système unité logique - détecte le signal électrique dépassant un seuil donné et envoie un signal aux éléments finaux. Les unités logiques peuvent être des ordinateurs, les contrôleurs électroniques programmables (API : Application Program Interface) et les circuits de relais.
- Sous-système de l'élément final - exécute la fonction de sécurité. Des exemples d'éléments finaux sont les vannes d'arrêt, les disjoncteurs, les moteurs, les ventilateurs, etc.

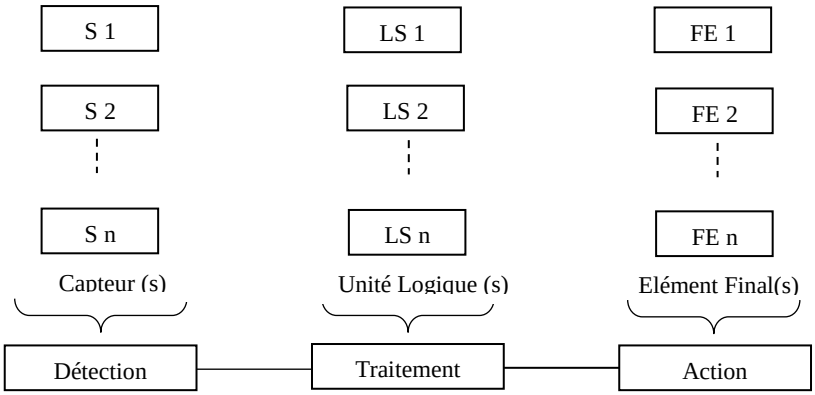


Figure 2.1 Structure générique d'un SIS

Les trois sous-systèmes doivent agir de concert pour détecter la déviation (c.-à-d. la demande) et mettre l'EUC dans un état sûr. En résumé, un SIS doit détecter, réagir et éviter la

production d'un évènement indésirable.

Un exemple industriel (Iddir 2009) d'un SIS simple utilisé pour la protection contre la pression d'un pipeline est illustré à la figure 2.2.

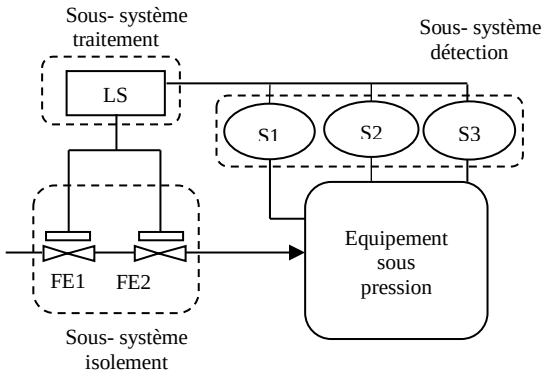


Figure 2.2 SIS de protection contre les surpressions dans une canalisation (adapté de Iddir 2009)

Trois transmetteurs de pression surveillent la pression dans la canalisation et envoient cette information au sous-système unité logique. L'unité logique compare les valeurs reçues avec des points de consigne prédéfinis et, en cas de pression élevée, un signal est envoyé aux deux vannes d'arrêt (SDVs : Shutdown valve) pour fermer le flux dans le pipeline.

Chaque sous-système peut avoir un ou plusieurs canaux. Le sous-système de capteurs de la figure 2.2 comporte trois canaux (c.-à-d. des transmetteurs de pression) et le sous-système de l'élément final comporte deux canaux (c.-à-d. des vannes d'arrêt).

2.3 Conception des SIS

2.3.1 Redondance majoritaire KooN- Groupe voté

La redondance Koon signifie avoir deux éléments ou plus, de sorte qu'en cas de défaillance d'un élément, le système peut continuer à fonctionner en utilisant le(s) autre(s) élément(s). Ce principe de conception est également appelé tolérance aux défaillances. La redondance peut être mise en œuvre de différentes manières. Deux catégories principales sont :

- Redondance active. Tous les éléments redondants remplissent activement de leurs fonctions. Si les éléments portent une charge, ils se partagent la charge (p. ex. les pompes qui devraient fournir un volume donné d'un fluide).
- Redondance passive. Un ou plusieurs éléments remplissent les fonctions, tandis que les autres éléments sont en attente et attendent d'être mis en service si l'un des éléments actifs échoue. En mode veille, les éléments peuvent être en attente froide ou

partiellement chargés. Les articles en veille froide sont généralement considérés comme neufs lorsqu'ils sont activés. Les articles peuvent parfois être activés et désactivés sur une base programmée. La redondance passive est également appelée redondance dynamique.

La redondance peut en outre être classée comme suit :

- La redondance matérielle peut être mise en œuvre en installant deux éléments ou plus pouvant exécuter la même fonction de sécurité ou une fonction de sécurité similaire. La redondance peut être implémentée au niveau de l'élément, au niveau du canal, au niveau du groupe voté, au niveau du sous-système et même au niveau du SIS.
- La redondance logicielle est parfois mise en œuvre en ayant au moins deux routines logicielles, chacune écrite par des équipes de codage indépendantes et développée pour donner la même sortie pour la même entrée. S'il n'y a pas d'erreur, les modules produisent des sorties identiques à tout moment, mais si l'une des sorties diffère, le logiciel présente un bogue non détecté ou le matériel sur lequel il est exécuté a échoué. Dans ce cas, la routine produisant la sortie divergente est ignorée et un signal d'erreur est envoyé.

Plusieurs autres types de redondance sont décrits et discutés par (Boulanger 2013).

Concernent les SISs chacun des trois sous-systèmes (capteurs, unité logique, élément final), est représenté par une architecture KooN. Par définition, la notion de redondance renvoie à l'existence, dans une entité, de plus d'un moyen pour accomplir une fonction requise. Ainsi, afin de diminuer la probabilité qu'un système ne remplisse pas sa fonction de sécurité au moment où il est sollicité, une solution consiste à redonder certains éléments constitutifs du système. Si l'amélioration de la sécurité est parfois nécessaire, il ne faut pas oublier que la disponibilité des installations se révèle dans la plupart des cas aussi importante que la sécurité (ou du moins elle constitue l'une des priorités des industriels). Afin de pouvoir réaliser un compromis entre la sécurité et la disponibilité des installations, un certain nombre d'architectures KooN sont disponibles(Rausand 2014).

Une redondance de type KooN est donc une redondance dite majoritaire telle qu'une fonction n'est assurée que si au moins K des N moyens existants sont en état de fonctionner ou en fonctionnement. La redondance Koon est également appelée groupe voté.

Les architectures les plus fréquemment rencontrées sont les suivantes :

- 1oo1 : architecture constituée par un seul élément, toute défaillance dangereuse de cet élément empêche le traitement correct de tout signal d'alarme valide figure 2.3;

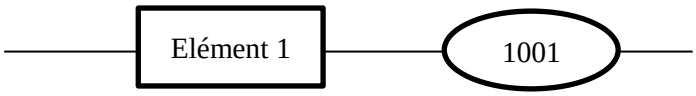


Figure 2.3 Architecture 1001

- 1oo2 : architecture constituée par deux éléments de façon à ce que chacun puisse traiter la fonction de sécurité figure 2.4;

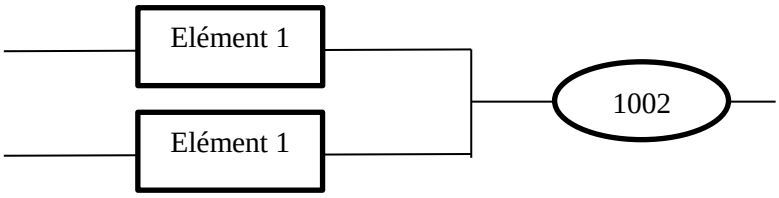


Figure 2.4 Architecture 1002

- 2oo2 : architecture constituée par deux éléments de sorte que la fonction de sécurité est activée uniquement si les deux éléments en font la demande. Dans ce schéma, la disponibilité de production est assurée au détriment de la sécurité figure 2.5;

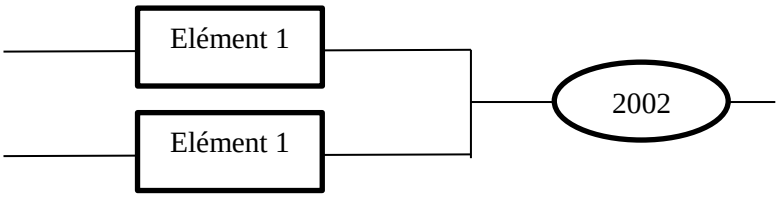


Figure 2.5 Architecture 2002

- 2oo3 : architecture constituée par trois éléments de sorte que la fonction de sécurité est activée uniquement si deux éléments parmi les trois en font la demande figure 2.3.d;

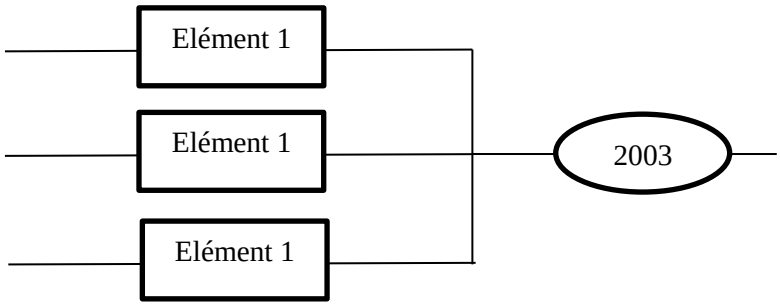


Figure 2.6 Architecture 2003

2.3.2 Fonction instrumentée de sécurité SIF

Les principales étapes de la norme CEI 61508 (CEI_61508 2010) et ses normes filles sont déclinées dans ce qu'on appelle le cycle de vie, c'est-à-dire que ces normes traitent depuis l'analyse des risques jusqu'à l'exploitation des fonctions instrumentées de sécurité SIF (Safety Instrumented Functions).

Une SIF est définie pour obtenir un facteur de réduction du risque mise en œuvre pour un SIS. Lorsque le SIS est considéré comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une fonction de sécurité (Mkhida 2008) (Charpentier 2002).

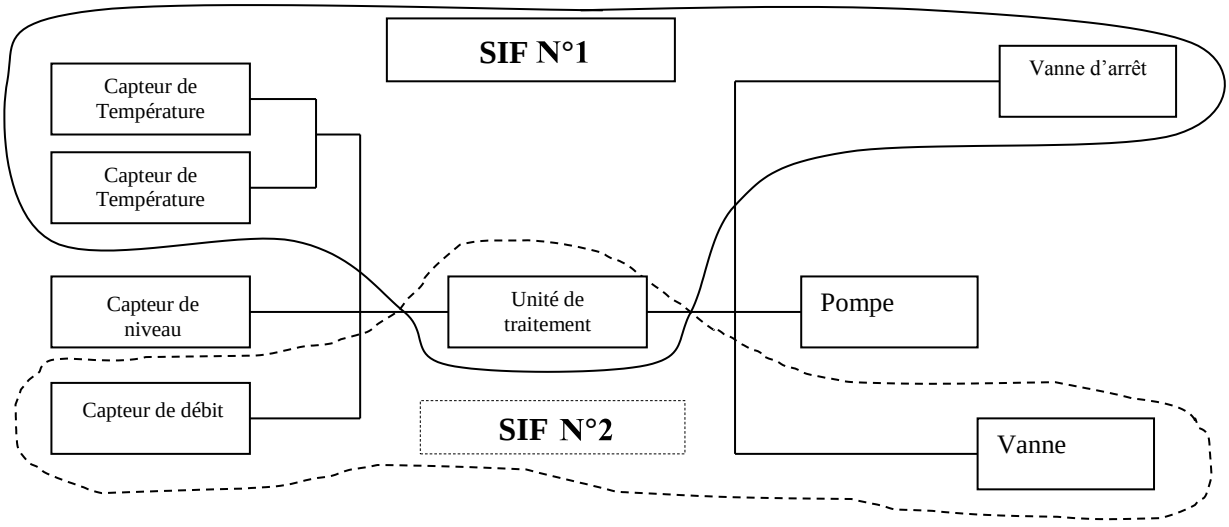


Figure 2.7 Fonction instrumentée de sécurité (adapté de Mkhida 2008)

Une fonction instrumentée de sécurité (SIF) est une fonction qui a été intentionnellement conçue pour protéger l'EUC contre une demande spécifique. Le SIF est mis en œuvre par un SIS et dispose d'un niveau d'intégrité de sécurité (SIL) spécifique. Un SIS peut effectuer un ou plusieurs SIF.

L'un des objectifs d'une fonction instrumentée de sécurité est de mettre l'EUC dans un état sûr ou de maintenir l'EUC dans un état sûr lorsqu'une demande survient afin de protéger les personnes, l'environnement et les biens matériels.

2.3.3 Modes de fonctionnement

Les modes de fonctionnement ont été présentés au chapitre 1. La norme CEI 61508 définit trois modes de fonctionnement : le mode à faible demande, le mode à forte demande et le mode continu, mais elle combine les deux derniers modes et les appelle le mode à forte demande/continu. La norme CEI 61511, quant à elle, distingue deux modes de fonctionnement :

- Le mode continu. : Il existe une différence importante entre une SIF qui fonctionne en mode demandé et un autre qui fonctionne en mode continu. Une SIF qui fonctionne en mode continu, par contre, joue un rôle actif dans le contrôle de l'EUC et un événement dangereux se produira presque immédiatement lorsqu'une défaillance dangereuse de la SIF survient.

- Le mode demandé : Une SIF en mode demandé est passive en ce sens qu'il n'exécute aucune fonction active pendant le fonctionnement normal, mais qu'il est un complément de l'EUC et n'est utilisé que lorsque quelque chose ne va pas bien ou commence à mal fonctionner.

La norme CEI 61508 divise le mode demandé en deux sous-modes :

- Mode à faible demande : Pour ce mode, la SIF n'est effectuée qu'en cas de demande, afin d'amener l'EUC dans un état sûr spécifié, et lorsque la demande (c.-à-d. la fréquence des demandes) n'est pas supérieure à une fois par année1. Est en fonctionnement continu, cela signifie que le taux de demande est λ_{de} < 1.15. 10^{-4} par heure. En mode à faible demande, l'EUC est généralement maintenue dans un état sûr par un EUC et la SIF n'est sollicité que lorsque la commande EUC tombe en panne, étant donné qu'illustrée par un simple arbre d'événements à la figure 2.5.
- Mode haute demande. Pour ce mode, la SIF n'est effectuée que sur demande, afin de transférer l'EUC dans un état sûr spécifié ou de maintenir l'EUC dans un état sûr, et lorsque le taux de demande est supérieur à une fois par an. Lorsque l'EUC est en fonctionnement continu, cela signifie que le taux de demande est λ_{de} > 1,15. 10^{-4} par heure. Le nombre moyen de demandes par an sera d'une ou plusieurs demandes.

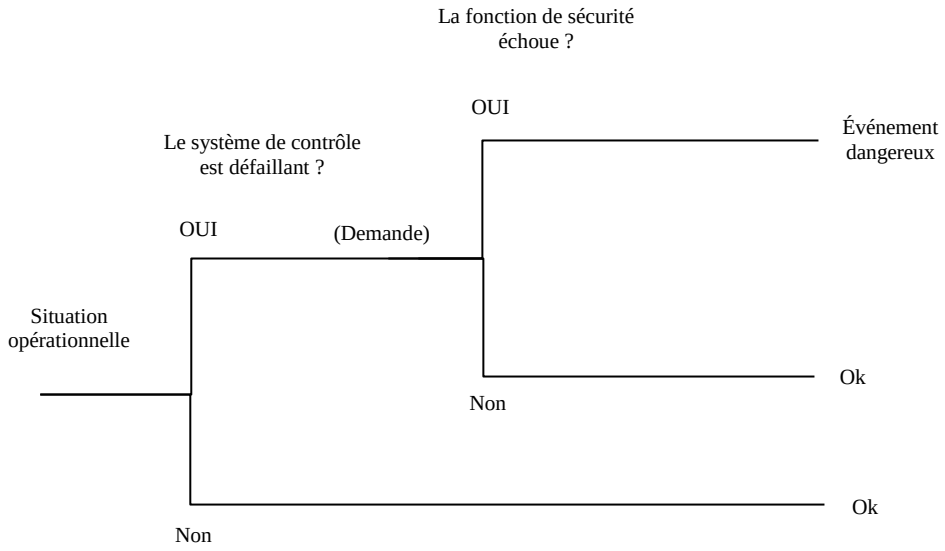


Figure 2.8 Arborescence des événements d'un SIS en mode faible demande.

2.3.4 Mesures des performances de sécurité des SIS

La norme CEI 61508 spécifié deux indicateurs de la sécurité relatifs aux systèmes électroniques programmables dédiés aux applications de sécurité. Ces deux paramètres utilisés

pour l'évaluation des performances des SIS suivant les deux modes de défaillance cités par les normes de sécurité. Ces modes sont le mode de défaillances dangereuses et le mode de défaillances par heure. Ces indicateurs sont donnés sous forme de probabilités de Probabilité moyenne de défaillance à la demande (PFD) et de Probabilité de défaillance dangereuse par heure (PFH).

2.3.4.1 Probabilité moyenne de défaillance à la demande

Il est utile de rappeler certains principes et hypothèses de base largement utilisés dans la norme CEI 61508 et ses normes filles.

La probabilité moyenne de défaillance à la demande, notée PFD_{avg} n'est pas définie dans le volume 4 de la norme CEI 61508, malgré son utilisation dans plusieurs définitions et abréviations. Cette probabilité représente tout simplement l'indisponibilité moyenne d'un système E/E/EP relatif à la sécurité, qui rend ce dernier incapable d'effectuer correctement sa fonction de sécurité, lorsqu'il est faiblement sollicité (Rausand 2014).

La dénomination PFD utilisée dans la norme est d'autant moins adéquate. Elle désigne la probabilité de défaillance dangereuse `a la sollicitation. La PFD_{avg} (Average Probability of Failure on Demand) est la mesure d'une indisponibilité moyenne sur une période spécifiée.

Cette probabilité se distingue formellement d'une indisponibilité asymptotique (quand elle existe) ou stationnaire. Cette distinction s'impose notamment pour les systèmes testés périodiquement et ne possédant pas de régime stationnaire. Elle est systématiquement ignorée, aussi bien dans la norme que par certains auteurs d'articles traitant du calcul des différentes architectures de base des SIS.

2.3.4.2 Probabilité de défaillance dangereuse par heure

La probabilité d'une défaillance dangereuse par heure (PFH) : Probability of a dangerous Failure per Hour, est parfois appelée « fréquence des défaillances dangereuses », ou « taux de défaillances dangereuses », ou « nombre de défaillances dangereuses par heure ».

La probabilité de défaillance par heure n'est pas aussi citée dans la partie 4 de la norme CEI 61508-4 destinée aux définitions. Elle est indiquée dans le tableau 2.1 pour le mode de fonctionnement continu ou `a demandé élevée.

2.3.5 Niveau d'intégrité de sécurité

La norme CEI 61508 utilise l'intégrité de sécurité comme mesure de performance pour une SIF.

Intégrité de sécurité. Probabilité qu'un SIS exécute de manière satisfaisante les SIF spécifiés dans toutes les conditions spécifiées dans un délai donné EIC 61508-4 (CEI_61508 2010).

La norme CEI 61508 ne spécifie pas de valeurs de probabilité détaillées mais définit les exigences en quatre niveaux d'intégrité de sécurité, SIL1, SIL2, SIL3 et SIL4. SIL4 étant le plus fiable et SIL 1 le moins fiable, Tableau 2.1.

Sollicitation	Demande faible	Demande élevée
SIL	PFD_{avg}	PFH
1	10^{-2} PFD_{avg} 10^{-1}	10^{-6} PFH 10^{-5}
2	10^{-3} PFD_{avg} 10^{-2}	10^{-7} PFH 10^{-6}
3	10^{-4} PFD_{avg} 10^{-3}	10^{-8} PFH 10^{-7}
4	10^{-5} PFD_{avg} 10^{-4}	10^{-9} PFH 10^{-8}

Tableau 2.1 Les différents niveaux de SIL (CEI_61508 2010)

L'utilisation des niveaux SILs permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel menant aux évènements dangereux identifiés pendant l'analyse de risque (Schönbeck et al. 2010). Les SILs sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances.

2.3.6 Classification des défaillances dans la norme CEI 61508

Généralement un système peut se trouver dans l'un des quatre états suivants :

- État normal : la fonction de sécurité du système est valide et il n'existe pas de défaillance.
- État normal dégradé : La fonction de sécurité est valide, des composants du système pouvant être défaillants. Le système peut réagir dès l'apparition d'un événement dangereux (Lamy 2002), (Signoret 2004).
- 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.
- 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.

D'après ces définitions, une défaillance dangereuse est une défaillance qui tend à empêcher le système à réaliser sa fonction de sécurité en cas de demande provenant de l'EUC qui sera alors dans un état dangereux. Une défaillance en sécurité, appelée aussi défaillance sûre qui tend à anticiper le déclenchement de la fonction de sécurité, en l'absence de toute demande, en conduisant effectivement l'EUC dans un état sûr. C'est-à-dire tel que l'occurrence de tout

événement indésirable n'y est plus possible. Le taux de défaillance aléatoire de chaque élément (λ) peut s'écrire alors (Rausand 2014) :

$$\lambda = \lambda_S + \lambda_D \tag{2.1}$$

La prise en compte de la détection ou non détection, par des tests en ligne (tests de diagnostic), de ces défaillances engendre une autre décomposition de celles-ci. Les premières sont appelées défaillances détectées et les secondes, qui ne peuvent être révélées que lors des proof tests hors ligne ou lors de la sollicitation du SIS par le système surveillé, sont dénommées défaillances non détectées. La figure 2.6 présente cette double décomposition.

La capacité d'un SIS à détecter ses défaillances en ligne se résume dans son taux de couverture ou sa couverture de diagnostic DC (Rausand 2014). En introduisant ce taux de couverture de diagnostic, on peut récrire les différents taux de défaillances, cités précédemment, comme suit

$$\lambda_{DD} = DC \,.\, \lambda_D \tag{2.2}$$

$$\lambda_{DU} = (1 - DC) \,.\, \lambda_D \tag{2.3}$$

$$\lambda_{SD} = DC_S \,.\, \lambda_S \tag{2.4}$$

$$\lambda_{SU} = (1 - DC_S) \,.\, \lambda_S \tag{2.5}$$

- Défaillances dangereuses non détectées (DU). Les défauts DU empêchent l'activation sur demande et ne sont révélés que par des proof tests ou lorsqu'une demande survient. Les défauts DU sont parfois appelés défauts dormants ou cachés. Les défauts DU sont d'une importance vitale pour le calcul de la fiabilité d'une SIF car ils sont un des principaux facteurs contribuant à l'indisponibilité de la SIF.
- Défaillances dangereuses détectées (DD). Les défauts de DD sont détectés peu de temps après leur apparition, par un test de diagnostic automatique. La période moyenne d'indisponibilité due à une panne de DD s'appelle le temps moyen de restauration (MTTR), le temps moyen qui s'écoule entre la panne de DD et la restauration de la fonction.
- Défaillances non détectées (SU) sûres. Défaillances non dangereuses qui ne sont pas détectées par l'autotest automatique.
- Défaillances détectées (SD) sûres. Défaillances non dangereuses qui sont détectées par autotest automatique. Dans certaines configurations, la détection précoce des défaillances peut empêcher un déclenchement intempestif du système.

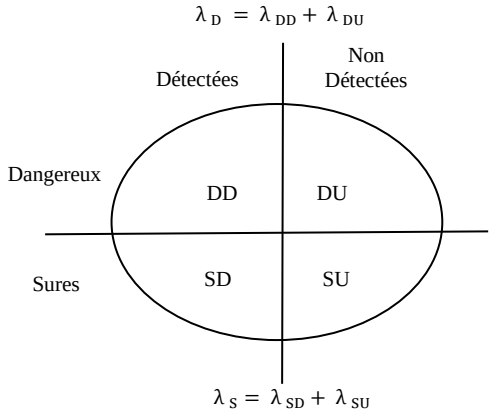


Figure 2.9 Classification des défaillances (CEI_61508 2010)

2.3.7 Tests et stratégies des tests des SIS

Un test peut être conçu pour confirmer les performances correctes et le comportement correct en réponse à des conditions de défaut spécifiques, telles qu'une perte de puissance. Dans la phase opérationnelle, les tests peuvent être divisés en deux grandes catégories : i) tests de diagnostic, ii) proof test.

i. Test de diagnostic est un test partiel automatique qui utilise des fonctions d'autotest intégrées pour détecter les défauts. Les défauts dangereux détectés par un test de diagnostic sont appelés défauts dangereux détectés (DD) et les défauts de sécurité détectés par un test de diagnostic sont appelés défauts de sécurité détectés (SD). Ils sont caractérisés par un taux de couverture DC, défini comme étant la probabilité qu'une défaillance soit détectée dès son apparition (Velten-Philipp and Houtermans 2006).

ii. Un proof test (test périodique) est un proof test soigneusement planifié, qui est conçu pour révéler tous les défauts DU de chaque canal d'une boucle de sécurité. Un proof test est en outre conçu pour révéler tous les défauts d'éléments qui peuvent influencer l'apparition de défauts DU et ainsi permettre la réparation de ces défauts. Après l'essai d'étanchéité et la réparation correspondante, la boucle de sécurité est présumée être aussi neuve que possible ou aussi proche que possible de cette condition. Pour indiquer clairement que le test est conçu pour révéler tous les défauts DU possibles et les défauts des éléments, le test est parfois appelé un proof test complet.

Le temps de mission noté Ti, est considéré comme égal au temps entre deux proof tests consécutifs (Bukowski 2001; Charpentier 2002; Lamy 2002).

Le proof test peut être mis en application en utilisant plusieurs stratégies de test différentes. Tores-Echeveria (Torres-Echeverria et al. 2009) énumère une classification des stratégies de test :

- Le test simultané ou tous les composants sont testés en même temps. Ceci exige d'avoir un nombre de réparateurs suffisant pour tester tous les composants du système.
- Le test séquentiel, où tous les composants redondants sont testés consécutivement l'un après l'autre. Juste après qu'un composant est testé et mis en service, le prochain composant est testé et ainsi de suite jusqu''a finir avec tous les composants du sous-système (Cepin 1995).
- Le test indépendant, dans cette stratégie, la durée de test, des composants testés, ne suit pas un programme spécifique, l'intervalle de temps de test entre deux composants est aléatoire (Torres-Echeverria et al. 2009).

Généralement, on considère un seul intervalle de test pour vérifier la fonction de sécurité de l'ensemble du système mais certaines applications exigent l'utilisation d'intervalles de test différents propres à chaque sous système du SIS voire à chaque composant (Lamy 2002; Signoret 2005).

2.3.8 Cycle de vie de la sécurité

Le cycle de vie SL de la sécurité est un concept important de la CEI 61508 et de ses normes sectorielles. Il est défini comme suit :

Cycle de vie de la sécurité. Un processus d'ingénierie conçu pour obtenir un SIS avec un niveau de sécurité basé sur le risque dans toutes les phases d'exploitation. Le cycle de vie est une séquence de phases fournissant un chemin logique allant de la spécification à la conception, au développement, à la mise en service, à l'exploitation, à la maintenance et enfin au déclassement du SIS, c'est-à-dire du « vie » au « mort »".

2.3.9 Taux caractéristiques des SIS

La norme CEI 61508 permet d'estimer la probabilité de défaillance de la fonction de sécurité due à des défaillances matérielles aléatoires. Les calculs font intervenir un grand nombre de paramètres : architecture, taux de défaillance des composants, intervalle des tests, taux de couverture de diagnostic DC et le facteur β qui caractérise les défaillances de cause commune) (Houtermans and Rouvroye ; Lamy 2002; Goble and Cheddie 2005).

2.3.9.1 Taux de couverture de diagnostic

Le taux de couverture de diagnostic DC peut être exprimé comme la probabilité conditionnelle qu'un défaut dangereux soit détecté (c'est-à-dire qu'il devienne un défaut DD) par le test de diagnostic. Ceci peut à nouveau être exprimé comme la fraction moyenne de tous les défauts D d'un article qui sont détectés par l'autotest de diagnostic.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dangereux}} \tag{2.6}$$

L'évaluation du taux de couverture DC se fait par une Analyse des Modes de Défaillances et de leurs Effets (AMDE) au niveau des différents composants d'un système

(Goble and Brombacher 1999; Torres-Echeverria and Thompson 2007). On cherche ainsi à déterminer les défaillances possibles et à savoir si elles peuvent être détectées (Jin et al. 2011).

Le taux de couverture DC intervient dans la détermination des taux de défaillances dangereuses ; détectées et non détectées.

2.3.9.2 Défaillances de causes communes

Une défaillance de cause commune (CCF : Common-Cause Failure) est une défaillance de deux éléments ou plus en raison d'un seul événement ou d'une seule cause et dans un intervalle de temps spécifié. Fleming (Fleming 1975) a introduit un modèle simple, appelé modèle à facteur bêta, pour incorporer les CCF dans les modèles de fiabilité, ce modèle il a était utilisé par la norme. L'idée du modèle à facteurs bêta est de diviser le taux d'échec λ d'un article en deux parties :

$\lambda^{(i)}$ Le taux de défaillances individuelles, c.-à-d. les défaillances qui n'affectent que l'élément spécifique et $\lambda^{(c)}$ le taux d'échecs qui affectent tous les éléments d'un groupe voté, c'est-à-dire le taux de CCF, de sorte que

$$\lambda = \lambda^{(i)} + \lambda^{(c)} \tag{2.7}$$

Le paramètre β est introduit comme la fraction de toutes les défaillances d'un élément qui sont CCFs.

$$\beta = \frac{\lambda^{(c)}}{\lambda} \tag{2.8}$$

Cela signifie que nous pouvons exprimer $\lambda^{(i)}$ et $\lambda^{(c)}$comme suit

$$\lambda^{(i)} = (1 - \beta)\lambda \tag{2.9}$$

$$\lambda^{(c)} = \beta\lambda \tag{2.10}$$

Le facteur bêta, β, peut également être interprété comme une probabilité conditionnelle : Lorsqu'une défaillance de l'élément est observée, β est la probabilité que cette défaillance soit en fait un CCF.

Une conséquence du modèle du facteur bêta est que toute défaillance est soit une défaillance individuelle affectant un seul élément, soit une défaillance CCF affectant tous les éléments du groupe voté. Lorsqu'une défaillance survient, par exemple, dans un groupe voté 2oo4, il s'agit soit d'une défaillance d'un seul élément, soit d'une défaillance affectant les quatre éléments. Un CCF affectant deux ou trois éléments n'est pas autorisé lorsqu'on utilise le modèle du facteur bêta.

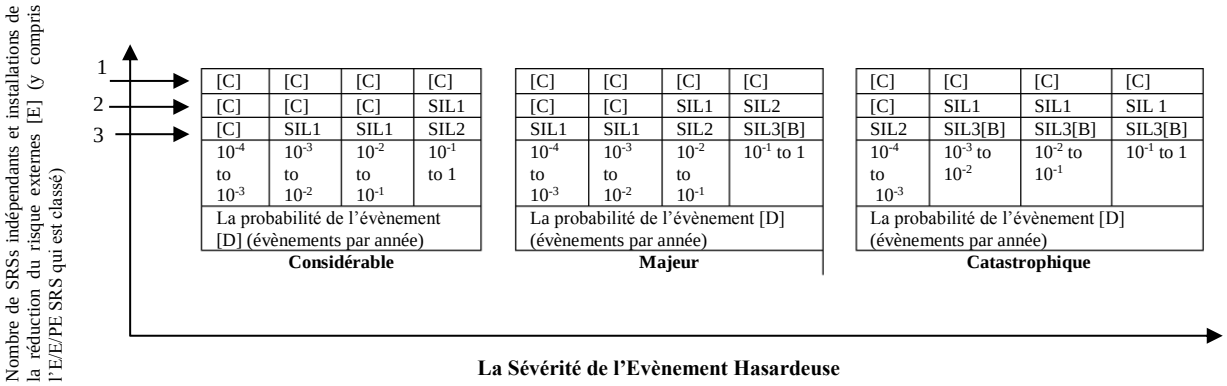
2.4 Allocation du niveau d'intégrité de sécurité

Cette allocation est conduite selon certaines méthodes permettant de définir le niveau d'intégrité de sécurité (SIL) requis pour une fonction de sécurité. C'est le SIL qui doit être atteint par un SIS afin de réaliser la réduction nécessaire du niveau de risque. La section suivante donne un aperçu des méthodes, telles que présentées dans les normes CEI 61508 et CEI 61511, de détermination du niveau d'intégrité de sécurité (SIL) correspondant à un phénomène dangereux spécifié (scénario d'accident) lors de la phase d'analyse des risques. Elles sont plus ou moins adaptées en fonction du niveau de détail des analyses de risques réalisées (type et détail des informations disponibles). La CEI 61508, dans sa partie 5, et la CEI 61511 décrivent deux types de méthodes : qualitatives et quantitatives.

2.4.1 Méthodes qualitatives

La norme CEI 61508 introduit des méthodes qualitatives qui permettent d'allouer le SIL à partir de la connaissance des risques associés au procédé. Les méthodes les plus utilisées sont la méthode du graphe de risque (Beugin et al. 2007; Sallak 2007) et la méthode de la matrice de gravité des évènements dangereux (Sallak et al. 2006). Le choix de la méthode du graphe des risques est justifié par la nature des données et principalement dans le cas où le retour d'expérience est insuffisant pour valider avec précision les taux de défaillance des SIS.

La matrice de risque intègre plusieurs fonctions de sécurité sous réserve de leur indépendance (CEI_61508 2010). La matrice possède trois dimensions : la gravité, la probabilité d'occurrence de l'accident potentiel et le nombre de dispositifs de sécurité qui sont déjà mis en place pour empêcher le développement du danger en un accident. La structure de la matrice de risque dépend du domaine spécifique d'activité (Beugin et al. 2007).



[A] Un SIL 3 E/E/PE le système sécurité apparente ne fournit pas réduction du risque suffisante à ce niveau du risque. Les mesures de la réduction du risque supplémentaires sont exigées
[B] Un SIL 3 E/E/PE le système sécurité apparente ne peut pas fournir réduction du risque suffisante à ce niveau du risque. Le hasard et risque l'analyse est exigée pour déterminer siles mesures de la réduction du risque supplémentaires sont nécessaires
[C] Un E/E/PE indépendant que le système sécurité apparente n'est pas exigé probablement
[D] La probabilité de l'évènement est la probabilité que l'évènement hasardeux se produit sans toute sécurité systèmes apparentes ou installations de la réduction du risque externes
[E] SRS = système sécurité apparente. Probabilité de l'évènement et le nombre totale de couches de protection indépendantes sont définis par rapport à la candidature spécifique.

Figure 2.10 Matrice de gravite des évènements dangereux (CEI_61508 2010)

2.4.1.1 Méthode du graphe de risque

La méthode qualitative la plus utilisée pour déterminer le niveau de SIL est la méthode dite du « graphe de risque » (CEI_61508 2010). Quand cette méthode est adoptée, un certain nombre de paramètres de simplification sont introduits pour décrire la nature de la situation dangereuse lorsque les systèmes relatifs à la sécurité sont défaillants ou non disponibles. Un paramètre est choisi parmi quatre groupes caractéristiques du risque et les paramètres sélectionnés sont alors associés pour décider du niveau de SIL des systèmes relatifs à la sécurité. Ces quatre paramètres permettent de faire une gradation significative des risques et contiennent les facteurs clés d'appréciation du risque.

2.4.1.2 Synthèse du graphe de risque

La procédure simplifiée s'appuie sur l'équation suivante : R = f x C

Où : R est le risque en l'absence de systèmes relatifs à la sécurité, f est la fréquence de l'événement dangereux en l'absence de systèmes relatifs à la sécurité et C'est la conséquence de l'événement dangereux.

La fréquence de l'événement dangereux f est supposée être le résultat de trois facteurs exerçant une influence :

- Fréquence et durée d'exposition dans une zone dangereuse ;
- La possibilité d'éviter l'événement dangereux ;

La probabilité que l'événement dangereux se produise en l'absence de systèmes relatifs à la sécurité. C'est ce qu'on appelle la probabilité d'occurrence non souhaitée.

On obtient les quatre paramètres de risque suivants :

- Conséquence de l'événement dangereux (C) ;
- Fréquence et durée d'exposition au danger (F) ;
- Possibilité d'éviter l'événement dangereux (P) ;
- Probabilité de l'occurrence non souhaitée (W).

Paramètre		**Description**
Conséquence	**C**	Nombre d'accidents mortels et/ou de blessures graves pouvant résulter de l'occurrence de l'événement dangereux. Déterminé en calculant les nombres d'accidents clans la zone exposée lorsque celle-ci est occupée en tenant compte de la vulnérabilité à l'événement dangereux
Occupation	**F**	Probabilité que la zone exposée soit occupée. Déterminée en calculant la fraction de temps d'occupation de la zone. Il convient de prendre en compte la possibilité d'une probabilité accrue de personnes se trouvant dans la zone exposée afin de rechercher les situations anormales pouvant exister lors de la progression vers l'événement dangereux
Probabilité d'éviter le phénomène dangereux	**P**	Probabilité que des personnes" exposées peuvent éviter la situation de phénomène dangereux qui existe si la fonction instrumentée de sécurité échoue à la sollicitation. Dépend s'il existe des méthodes indépendantes d'alerte des personnes exposées au phénomène dangereux et s'il existe des moyens pour y échapper
Taux de demande	**W**	Nombre de fois par an que l'événement dangereux se produit si aucun système instrumenté de sécurité n'a été adapté. Peut être déterminé en considérant toutes les défaillances pouvant générer l'événement dangereux et en estimant le taux global d'occurrence

Tableau 2.2 Descriptions des paramètres du graphe de risque (CEI_61508 2010)

2.4.1.3 Mise en œuvre du graphe de risque

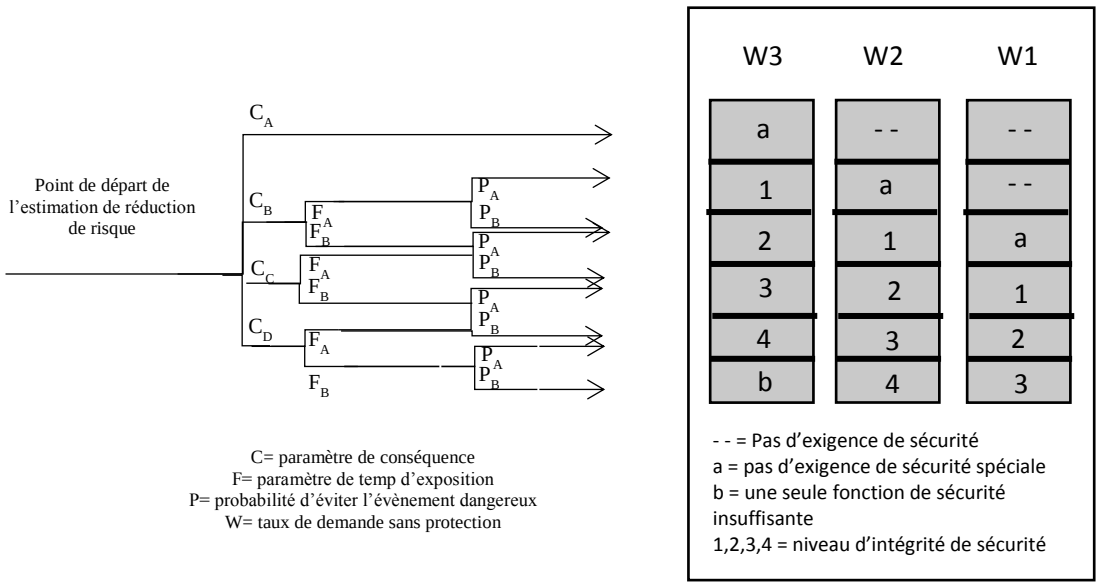


Figure 2.11 Schéma général de graphe de risque

Le graphe de risque s'explique de la manière suivante. L'utilisation des paramètres de risque C, F et P aboutit à un certain nombre de sorties, à savoir X1, X2, X3…Xn. La Figure 2.8 prend pour exemple une situation dans laquelle aucune pondération n'est appliquée aux pires conséquences. Chaque sortie est consignée dans une des trois échelles (W1, W2 et W3).

Chaque échelon indique le niveau de SIL nécessaire auquel doit satisfaire le système relatif à la sécurité pris en considération.

La mise en correspondance avec W1, W2 ou W3 permet de réaliser la contribution d'autres mesures de réduction du risque. Le décalage dans les échelles W1, W2 et W3 est nécessaire pour avoir trois niveaux différents de réduction des risques à partir d'autres mesures. Cette échelle est composée de l'échelle W1, qui fournit la réduction minimale du risque grâce à d'autres mesures (c'est-à-dire la plus forte probabilité de l'apparition d'un événement non désiré), l'échelle W2 une contribution moyenne et l'échelle W3 une contribution maximale. Pour une sortie spécifique du graphe de risque (c'est-à-dire X1, X2…ou X6) et, pour une échelle W spécifique (c'est-à-dire W1, W2 et W3) (Simon et al. 2007), la sortie finale du graphe de risque donne le niveau de SIL du SIS (c'est-à-dire 1, 2, 3 ou 4) et correspond à une mesure de la réduction nécessaire du risque pour le système.

A l'aide de ce graphe de risque, la fonction de sécurité à implanter pour prévenir un danger de faible probabilité sera réalisée en tenant compte des exigences relatives au SIL1.

Dans cet exemple les conséquences portent uniquement sur l'atteinte à la vie de personnes. La prise en compte des dégâts matériels et de dommages causés à l'environnement

nécessite l'utilisation de graphes additionnels.

Un exemple de classification des paramètres du graphe de risques est montré au tableau 2.3 (Sallak 2007)**.**

Paramètres de risque		**Classification**
Conséquence	C_A C_B C_C C_D	Incident mineur Effets réversibles Effet létaux limités au site Effets létaux en dehors du site
Exposition	F_A F_B	Exposition rare dans la zone considérée Exposition fréquente dans la zone considérée
Possibilité	P_A P_B	Possible sous certaines conditions Impossible
Taux de sollicitations	W_1 W_2 W_3	Faible probabilité (Accident pouvant se produire) Probabilité moyenne (Accident déjà observé) Probabilité élevée (Accident fréquent, observé plus d'une fois)

Tableau 2.3 Paramètres du graphe de risque

2.4.1.4 Etalonnage du graphe de risque

Les objectifs de la procédure d'étalonnage sont les suivants :

- Décrire tous les paramètres afin de permettre à l'équipe chargée d'établir le niveau d'intégrité de sécurité (SIL) de porter des jugements objectifs fondés sur les caractéristiques de l'application.
- Garantir que le SIL choisi pour une application répond aux critères de risque définis par la société et qu'il tient compte de risques provenant d'autres sources.
- Permettre de vérifier la procédure de sélection des paramètres.

L'étalonnage du graphe de risque est une procédure qui consiste à attribuer des valeurs numériques aux paramètres du graphe de risque. Ceci constitue la base pour l'évaluation du risque lié au procédé et permet de déterminer l'intégrité requise de la fonction instrumentée de sécurité faisant l'objet de l'étude. A chacun des paramètres est attribuée une plage de valeurs de sorte que, lorsque ces paramètres sont combinés, ils permettent d'effectuer une évaluation nuancée du risque qui existe en l'absence de la fonction particulière de sécurité.

De ce fait, on détermine une mesure du degré de confiance à attribuer à la fonction instrumentée de sécurité. Le graphe de risque se rapporte à des combinaisons particulières de paramètres de risque et de niveaux d'intégrité de sécurité. La relation entre les combinaisons de paramètres de risque et de niveaux d'intégrité de sécurité est établie en considérant le risque

tolérable associé aux dangers spécifiques.

2.4.2 Méthodes quantitatives

Les normes de sécurité fonctionnelle, l'CEI 61508 et l'CEI 61511, introduisent une approche probabiliste pour l'évaluation quantitative de la performance du SIS et la qualification de cette performance par des niveaux de sécurité référencés (Signoret 2005). L'introduction de probabilité dans la mesure du niveau d'intégrité a entrainé la mise en place de concepts tels que les notions de calcul de probabilité de défaillance a la sollicitation ou de défaillance par unité de temps (Signoret et al. 2007).

L'évaluation de la performance des SIS doit être réalisée par l'utilisation de modèles adaptés. Différentes techniques sont néanmoins préconisées dans les annexes de la norme CEI 61508. Parmi les méthodes quantitatives citées, on trouve les équations simplifiées, les arbres de défaillances (Signoret 2005), les blocs diagramme fiabilité, les réseaux de Petri ainsi que les chaines de Markov (Torres-Echeverría et al. 2011; Innal et al. 2015; Mechri et al. 2015). La performance ainsi calculée permet de qualifier le niveau SIL du SIS selon les niveaux définis dans la norme (Tableau 2.1).

2.4.2.1 Équations simplifiées

Les normes de sécurité fonctionnelle n'imposent cependant pas l'utilisation de modèles particuliers mais fournissent des formules approchées pour les architectures courantes. En effet, la communauté des fiabilistes s'est rendue compte que certaines équations citées dans la norme CEI 61508-6 ne sont valables que sous plusieurs hypothèses qui ne sont pas citées dans la norme (Rausand 2014). En outre, ces formules ne sont valables que pour certains types d'architecture *k* parmi *n*. D'après Rausand (Rausand 2014), les équations simplifiées sont utilisées pour l'étude d'architectures de SIS dont les canaux sont mutuellement indépendants et homogènes.

Les équations simplifiées donnent la PFD_{avg} du SIS en fonction de l'architecture des composants (1*oo*1 : un parmi un, 1*oo*2 : au moins un parmi deux, . . .) et des paramètres de fiabilité utilisés (taux de défaillances des composants ¸, taux de couverture de diagnostic *DC* et le facteur qui caractérise les défaillances des causes communes).

Comme mentionné par plusieurs chercheurs dans le domaine de la fiabilité des systèmes (Mechri 2011; Rausand 2014; Innal et al. 2015), il est nécessaire d'utiliser des méthodes de sureté de fonctionnement classiques telles que les diagrammes de fiabilité (Rausand and Høyland 2004), les arbres de défaillances, ou les approches markoviennes pour évaluer les performances des SIS (la PFD_{avg} et le SIL), plutôt que d'utiliser les équations simplifiées données dans la partie six de la norme CEI 61508.

2.4.2.2 Blocs diagramme de fiabilité

La méthode de diagramme de fiabilité est une représentation de la logique de fonctionnement des systèmes. Cette méthode est basée sur l'utilisation de blocs pour représenter les composants, les sous-systèmes ou les fonctions. La modélisation consiste à rechercher les liens existants entre ces blocs (Rausand and Høyland 2004). Elle permet une analyse quantitative qui a pour objectif en particulier de définir la probabilité de bon fonctionnement d'un système. Les calculs reposent sur les probabilités de réussite des missions des éléments constituants le système. Cette méthode est utilisée dans l'évaluation des performances des SIS par le calcul de la PFD_{avg} résultante et la détermination du son niveau SIL (Guo and Yang 2007).

La méthode de bloc diagramme de fiabilité a ses limites d'application : il faut s'assurer de l'indépendance entre les différents états de fonctionnement, elle ne permet pas de modéliser des systèmes dynamiques, sauf sous certaines conditions.

2.4.2.3 Arbres de défaillance

La méthode des arbres de défaillance est l'une des méthodes les plus utilisées dans les analyses des performances des SIS. Elle a pour objectif le recensement des causes entrainant l'apparition de l'événement indésirable d'un système et le calcul de sa PFD_{avg}. Elle constitue un moyen de représentation de la logique des défaillances, cette méthode est adaptée aussi pour l'étude des systèmes élémentaires présentant des défaillances de mode commun (Rausand 2014).

L'arbre de défaillances est une méthode déductive, qui commence par l'événement indésirable et détermine ses causes. L'analyse par l'arbre de défaillances nécessite deux phases

- Une qualitative, où on détermine la fonction logique du système en termes de l'ensemble de ses coupes minimales, et l'autre est dite quantitative, où on calcule la probabilité d'occurrence de l'événement indésirable (sommet).
- L'évaluation quantitative de la probabilité de l'événement sommet qui représente la défiabilité du système lorsque cet évènement est la défaillance d'un système non réparable. La méthode de l'arbre de défaillances consiste µa rechercher toutes les combinaisons possibles d'événements entraînant la réalisation de l'évènement indésirable.

On représente graphiquement ces combinaisons au moyen d'une structure arborescente dont l'évènement non désiré est le sommet (ou racine).

Pour décrire la relation entre les événements et la logique d'un système, l'arbre de

défaillances utilise des portes logiques. Ces portes indiquent les types des évènements et les types de relation qui sont impliquées.

L'arbre de défaillances peut mener à des évaluations quantitatives de la probabilité d'occurrence de l'évènement indésirable qui représente la défiabilité lorsque cet évènement est la défaillance d'un SIS non réparable (Villemeur 1987).

2.4.2.4 Chaines de Markov

Les chaines de Markov apportent une bonne formalisation de tous les états que peuvent prendre les systèmes en fonction des événements rencontrés (défaillance, réparation…) et des paramètres étudiés (taux de défaillance, défaillance de cause commune …) (Mechri et al. 2015).

Les chaines de Markov apportent une finesse de modélisation pertinente au regard du comportement des SIS étudiés notamment les SIS faiblement sollicités et périodiquement testés. Compte tenu de la relative complexité des SIS, l'explosion combinatoire du nombre des états est l'inconvénient majeur des chaines de Markov. Cet inconvénient est généralement surmontable (Rausand 2014).

L'évaluation de la performance du SIS est obtenue grâce à une chaine de Markov synthétique représentant les différents états du SIS tout en tenant compte des différents types de défaillance. Elle permet de déterminer la probabilité de défaillance à la demande du SIS et de calculer sa valeur moyenne par intégration dans le temps. La détermination du niveau de sécurité du SIS est obtenue par référence aux données du tableau 2.1.

La méthode des chaines de Markov est souvent utilisée pour analyser et évaluer les performances des systèmes réparables et avec des composants à taux de défaillance constant. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et à chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une action de réparation. Elle permet ainsi de faire une analyse dynamique du système.

Dans l'évaluation des performances des systèmes par les chaines de Markov on utilise le processus d'analyse constitué de trois parties. La première partie est consacrée au classement de tous les états du système en états de fonctionnement, états dégradés ou états de panne. La deuxième partie concerne la détermination de toutes les transitions possibles entre ces différents états, tout en tenant compte des actions de réparations. Enfin on calcule les probabilités de se trouver dans les différents états du système étudié.

2.4.2.5 Autres travaux

Il existe dans la littérature plusieurs formules analytiques qui traitent des performances des systèmes instrumentés de sécurité, les plus utilisées sont les formules données par la norme

CEI 61508 (CEI_61508 2010). Il y'a aussi les formules développées dans l'organisme norvégien SINTEF (SINTEF 2013b), qui met en œuvre un facteur β généralisé, moins pessimiste que celui utilisé par la CEI 61508. Dans la norme américaine ISA (ISA-84.00.01–2004 2004), les formules données représentent des approximations optimistes de celles de la norme CEI 61508. Les formulations analytiques PFD_{avg} et PFH de Innal (Innal 2008) ont été développée par la méthode markovienne approchée, ainsi que par la méthode binominale pour PFD_{avg}, PFH, PFS, et STR. Jin (Jin et al. 2016) tient en compte des défaillances dangereuses détectées et néglige β pour le calcul de PFH, Goble (Goble 1998) calcule PFD_{avg} et PFS par des modèles Markovien. Dans (Smith 2005) une revue générale des formules PFD_{avg} est proposée par Smith. Dans ses travaux, Oliveira (Oliveira 2008) utilise les formules de la norme CEI 61508 pour le calcul de PFD_{avg}.

Il existe d'autres recherches qui traitent de l'intervalle de temps des proof tests (Jin et al. 2015; Mechri et al. 2015; Asklou and Noureddine 2017a). Jin (Jin et al, 2015) considère qu'il existe un λDU qui ne peut pas être détecté par le proof test mais, qui peut être trouvé seulement quand le SIS est en marche. Tandis que Mechri (Mechri et al, 2015) a traité les SIS en utilisant la chaine de Markov notamment en introduisant deux paramètre : le paramètre d'efficacité « ξ » et le paramètre d'innocuité « γ ». Dans (Asklou et Noureddine, 2017a), on a proposé l'introduction des corrections de Jin (Jin et al, 2015) dans les équations analytiques découlant de la norme CEI 61508.

2.5 Conclusion

Dans ce chapitre nous avons étudié les méthodes de conception et d'évaluation des systèmes instrumentés de sécurité. On a d'abord détaillé la constitution et les modes de fonctionnement d'un SIS. Ensuite on a montré comment effectué leur évaluation à travers les niveaux d'intégrité de sécurité (SIL : safety integrity level). L'allocation du niveau d'intégrité SIL peut se faire par des méthodes qualitatives ou quantitatives.

Les méthodes qualitatives permettent d'allouer le SIL à partir de la connaissance des risques associés au procédé. La méthode la plus utilisée est basée sur le graphe de risque qui repose sur la détermination de paramètres liés à la conséquence et la fréquence de l'événement dangereux ainsi qu'à la possibilité de son évitement.

Les méthodes quantitatives permettent de calculer la probabilité de défaillance moyenne des SIS à partir des paramètres de fiabilité de leurs composants. Les méthodes les plus répandues sont les équations simplifiées qui donnent le PFD_{avg} et le PFH du SIS en fonction de l'architecture des composants et des paramètres de fiabilité utilisés.

Dans le chapitre suivant, on s’est intéressé aux équations simplifies que nous avons étudié et développé en détails.

3

Evaluation analytique des performances des systèmes instrumentés de sécurité

3.1 Introduction

Ce chapitre traite les systèmes instrumentés de sécurité (SIS) qui sont exploités en mode faiblement demandé et fortement demandé et où la probabilité moyenne de défaillance dangereuse à la demande (PFD_{avg}) et la probabilité de défaillance dangereuse par heure (PFH), sont utilisée pour quantifier leur fiabilité.

Le SIS est indépendant du système de commande de l'équipement sous contrôle (EUC) et constitue une couche de protection distincte et dormante qui n'est activée que lorsqu'un événement dangereux se produit dans l'EUC. Certains défauts peuvent donc ne pas être détectés jusqu'à ce que le SIS soit demandé ou testé.

Un SIS qui met en œuvre une fonction instrumenté de sécurité (SIF) à deux rôles distincts :

- Exécuter-la SIF : C'est la fonction essentielle du SIS, c'est-à-dire la raison pour laquelle il a été installé. Lorsqu'une demande survient, le SIS doit être en mesure d'effectuer la SIF conformément aux critères de performance spécifiés dans le SRS (Safety requirements specification) (Rausand 2014).
- Ne pas activer la SIF sans la présence d'une demande : Une défaillance de cette fonction peut entraîner une perte de production ou de service, mais peut également avoir des conséquences sur la sécurité. Une telle défaillance est considérée comme une défaillance sûre et elle est souvent appelée fausse alarme ou déclenchement intempestif.

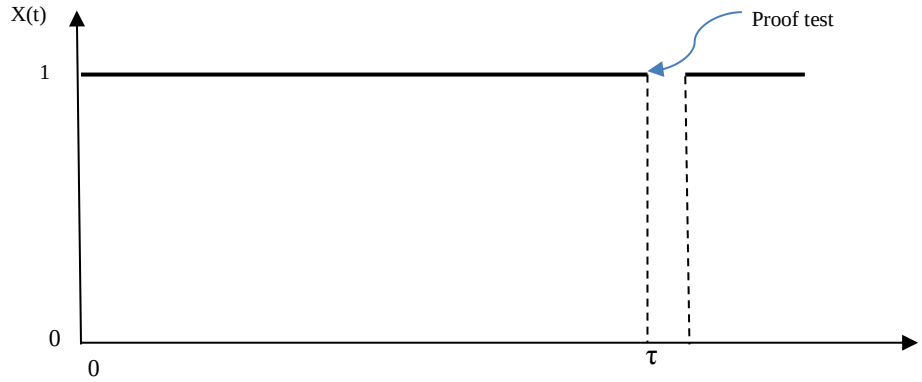
3.2 Sécurité par rapport à la production

3.2.1 Performances typiques

Trois états de performances typiques (Rausand 2014) d'un élément du SIS peuvent être énumérés. L'élément peut être un canal, un groupe de vote, un sous-système ou une boucle de sécurité entière. Les défaillances sûres ne sont pas prises en compte. L'élément du SIS est observé à partir du temps t = 0, juste après un proof test (test périodique) seras effectué. L'élément est comme neuf et l'état est $X(O) = 1$. Les trois êtas de performance typiques, de l'élément, dans un intervalle de proof test $(0, \tau)$ sont :

i. Pas de défaillance dangereuse dans l'intervalle de proof test : Cette performance est illustrée à la figure 3.1 et constitue la performance la plus typique pour les éléments à haute fiabilité. L'appareil est en mesure d'exécuter sa fonction de sécurité pendant toute

la durée de l'intervalle de proof test. A l'instant τ, le proof test est lancé. Le temps moyen requis pour effectuer le proof test s'appelle le temps moyen du test de périodique et il est souvent assez court (typiquement 1-2 heures), mais peut dans



certains cas être beaucoup plus long. Une fois le proof test terminé, l'appareil est remis en service et fonctionne à plein régime.

Figure 3.1 Pas de défaillance dangereuse dans l'intervalle de proof test.

ii. Une défaillance DD (dangereuse-détectée) dans l'intervalle de proof test : Cette performance est illustrée à la figure 3.2. Une défaillance DD se produit au moment t de l'intervalle et l'élément "saute" à l'état $X(t) = 0$, ce qui signifie qu'il a perdu la capacité d'exécuter sa fonction de sécurité. Une équipe de réparation est appelée à ramener l'article à l'état neuf (c.-à-d. à $X(t) = 1$). Le temps moyen total de rétablissement ($MTTR$) du défaut de DD est de deux parties :

- (a) Le temps moyen entre le moment où la défaillance dangereuse se produit et le moment où la défaillance dangereuse est détectée. Il s'agit d'une fraction de τ_D, l'intervalle de temps entre deux proof tests consécutifs. La fraction dépend de l'architecture de l'élément SIS.
- (b) Le temps moyen entre le moment où la défaillance dangereuse est détectée et celui où la fonction a été complètement rétablie.

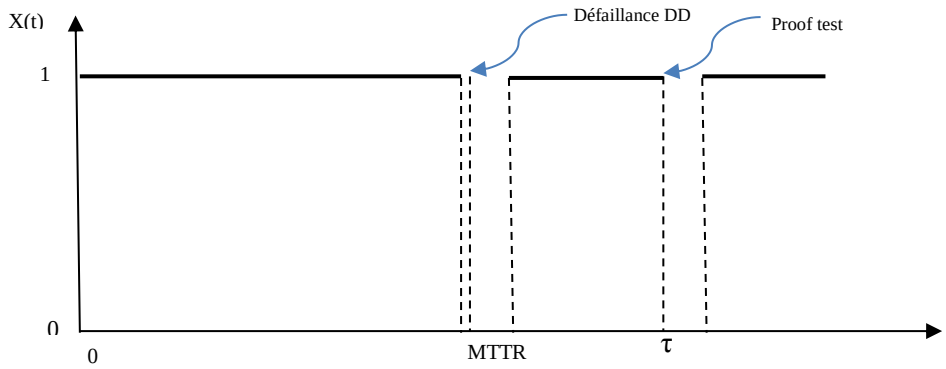


Figure 3.2 Défaillance DD dans l'intervalle de proof test

Une valeur typique pour le $MTTR$ est de 5 à 10 heures. Dans de nombreuses applications, le temps entre les tests de diagnostic est si court que le temps avant la détection peut être négligé.

iii. Une défaillance DU (dangereuse non détectée) dans l'intervalle de proof test : Cette performance est illustrée à la figure 3.3 où une défaillance DU se produit à l'instant t de l'intervalle de proof test et amène l'élément à l'état $X(t) = 0$. Comme la défaillance dangereuse n'est pas détecté (c'est-à-dire caché), le défaut n'est révélé qu'au moment $t = \tau$. L'arrêt associé (entre le moment où la défaillance se produit et celui où l'épreuve est lancée) est marqué D_1 à la figure 3.3. La durée moyenne du test est la même que pour les deux premières représentations. Lorsqu'un défaut DU est révélé lors du proof test, une action de réparation est entreprise pour ramener l'élément à l'état neuf, et le temps moyen de réparation est indiqué par MRT(MTTR).

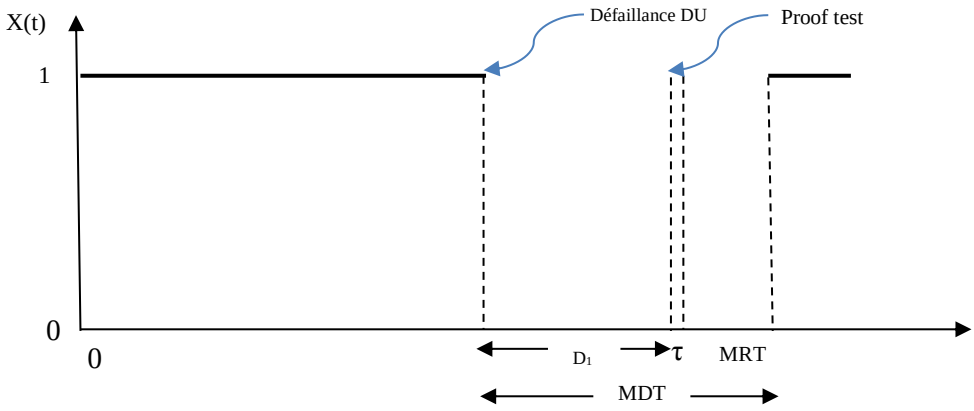


Figure 3.3 Défaillance DU dans l'intervalle de proof test

La probabilité de deux ou plusieurs défaillances dangereuses d'un même élément dans l'intervalle périodique est généralement si faible qu'elle peut être négligée.

3.2.2 Indisponibilité typique

Deux types d'indisponibilité typiques (Rausand 2014) d'un élément du SIS peuvent être énumérés :

i. Indisponibilité de sécurité inconnue : Dans ce cas, la fonction de sécurité est perdue lorsque nous croyons que nous sommes protégés. Cette situation peut se produire (a) dans la fraction de l'intervalle de diagnostic lorsqu'une défaillance DD survient, et (b) dans le temps d'arrêt inconnu D_1 après une défaillance de DU. Pour certaines architectures, nous pouvons aussi, sans le savoir, ne pas être protégés pendant le proof test lorsqu'une défaillance DU est présent.

ii. Indisponibilité de sécurité connue : Dans ce cas, nous savons que la fonction de sécurité n'est pas disponible en raison des essais, des réparations et de l'entretien préventif planifié, et nous pouvons prendre des précautions, introduire d'autres

barrières de sécurité ou éviter des opérations dangereuses.

Ces deux catégories sont distinguées dans la méthode PDS ou « Reliability of Computer Based Safety Systems » de la norme SINTEF (SINTEF 2013b) mais pas dans la norme CEI 61508.

3.3 PFD_{avg} - PFH d'un SIS

Comme mentionné au chapitre 2, la boucle de sécurité qui effectue une SIF comporte habituellement trois sous-systèmes principaux : (a) un sous-système de capteur, (b) un sous-système de solveur logique, et (c) un sous-système d'élément final. Les trois sous-systèmes sont configurés comme un système en série, figure 3.4.

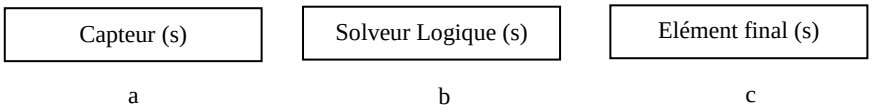


Figure 3.4 Trois sous-systèmes d'un SIS.

Soit E_i le cas où le sous-système i tombe en panne (i = a, b, c). Les trois sous-systèmes doivent fonctionner pour que la SIF puisse fonctionner, la SIF n'ai pas réalisé si l'un des sous-systèmes tombe en panne. Soit $\mathrm{PFD}_{\mathrm{avg}}^{(S)}$ désigne la PFD_{avg} du sous-système capteur, $\mathrm{PFD}_{\mathrm{avg}}^{(LS)}$ désigne la PFD_{avg} du sous-système solveur logique et $\mathrm{PFD}_{\mathrm{avg}}^{(FE)}$ désigne la PFD_{avg} du sous-système élément final.

Lorsque les trois sous-systèmes sont indépendants et ils ont une grande fiabilité, la probabilité que deux ou trois sous-systèmes tombent en panne en même temps est négligeable, de sorte que le PFD_{avg} pour une SIF peut donc être déterminé en ajoutant les PFD_{avg} pour les trois sous-systèmes.

$$PFD_{avg}^{(FIS)} = \Pr(E_1) + Pr(E_2) + P\,r(E_3) = PFD_{avg}^{(S)} + PFD_{avg}^{(LS)} + PFD_{avg}^{(FE)} \qquad (3.1)$$

De la même manière, la probabilité de défaillance dangereuse par heure (PFH) s'écrit :

$$PFH^{(FIS)} = \Pr(E_a) + Pr(E_b) + P\,r(E_c) = PFH^{(S)} + PFH^{(LS)} + PFH^{(FE)} \qquad (3.2)$$

- Remarque : Dans de nombreux cas, les trois sous-systèmes de la figure 3.4 dépendent d'une alimentation électrique et ne peuvent fonctionner que lorsque l'alimentation électrique fonctionne. Ceci peut être modélisé en incluant un sous-système d'alimentation en série avec les trois autres sous-systèmes. La probabilité que le sous-système d'alimentation soit en panne lorsqu'une demande survient peut alors être ajoutée à l'équation (3.1).

3.4 Expressions analytiques des PFD_{avg}

La norme CEI 61508-6 fournit des formules d'approximation pour la PFD_{avg} pour des configurations simples avec un maximum de trois canaux. Nous appelons ces formules les formules CEI. Les formules de la CEI sont présentées dans la norme CEI 61508-6 sans aucune justification et par conséquent difficilement assimilable. Dans cette section nous démontrons les formules PFD_{avg} similaires pour différentes configurations de SIS afin de les rendre compréhensibles.

L'idée principale des formules de la CEI est de calculer le PFD_{avg} d'un groupe voté (G) de canaux comme si le groupe était un élément unique. Le calcul est basé sur le taux moyen de défaillance d'un groupe dangereux ($\lambda_{D,G}$), et le temps d'arrêt moyen équivalent au groupe (t_{GE}). Le PFD_{avg} pour ce groupe est calculé comme suit :

$$PFD_{avg}^{(G)} = \lambda_{D,G} t_{GE} \tag{3.3}$$

Dans le calcul du PFD_{avg}, il est nécessaire de prendre en compte le temps d'arrêt moyen t_{GE} d'un canal qui a une défaillance dangereuse. Le temps d'arrêt moyen t_{GE} est appelé le temps d'arrêt moyen équivalent au canal.

Les formules de la CEI tiennent compte des défaillances DU et DD pour le calcul de la PFD_{avg}, mais les défaillances sûres ne sont pas prises en compte.

3.4.1 PFD_{avg} pour les canaux indépendants

Pour déterminer le PFD_{avg} d'un groupe voté, il est nécessaire de trouver :

- Le taux moyen de défaillances de groupes dangereux (DGF : Dangerous group failure).
- Le temps d'arrêt moyen du groupe voté lorsqu'une DGF se produit.

3.4.1.1 Fréquence des défaillances de groupes dangereux

Cette première tâche consiste à formuler le taux moyen de défaillances de groupes dangereux. Nous commençons par développer le taux moyen de défaillance pour les deux architecture s loo2 et 2oo3.

- Taux moyen de défaillance du système pour un groupe voté de 1oo2 : Considérons un groupe loo2 voté de canaux indépendants et identiques avec un taux de défaillance D λ_D. Parce que les canaux sont indépendants, ils ne tomberont pas en panne exactement

en même temps. Une défaillance dangereuse d'un groupe doit donc commencer par une défaillance D de l'un des deux canaux. Le taux de cet événement est de $2\lambda_D$, car les deux canaux peuvent tomber en panne. Lorsqu'un canal a une défaillance, il sera en panne pendant un certain temps t_{GE}. Pour qu'il y ait une défaillance de groupe dangereuse, le canal restant doit être défaillant pendant le temps d'arrêt du canal déjà défaillant, et cette défaillance se produit avec la probabilité Pr ($T_D < t_{GE}$). Où T_D est le temps avant la défaillance dangereuse d'un canal. Le taux moyen de défaillance du système pour le groupe voté par rapport aux défaillances D est donc le suivant

$$\lambda_{D,G} = 2\lambda_D\left(1 - e^{-\lambda_D t_{CE}}\right) = 2\lambda_D\lambda_D t_{CE} = 2(\lambda_D)^2 t_{CE} \quad (3.4)$$

- Taux moyen de défaillance du système pour un groupe voté 2oo3 : Considérons un groupe voté 2oo3 de trois canaux indépendants et identiques avec un taux de défaillance D λ_D. Parce que les canaux sont indépendants, ils ne tomberont pas en panne exactement au même moment. Comme pour le groupe loo2 voté, une défaillance dangereuse du groupe doit commencer par une défaillance D de l'un des trois canaux. Le taux de cet événement est en $3\lambda_D$, car les trois canaux peuvent tomber en panne. Lorsqu'un canal est en panne, il sera en panne pendant un certain temps t_{CE}. Pour avoir une panne de groupe dangereuse, au moins l'un des deux autres canaux doit être en panne pendant le temps d'arrêt du canal déjà en panne. Le taux moyen de défaillance du système pour le groupe voté par rapport aux défaillances D est donc le suivant

$$\lambda_{D,G} = 3\lambda_D\left(1 - e^{-2\lambda_D t_{CE}}\right) = 3\lambda_D 2\lambda_D t_{CE} = 6(\lambda_D)^2 t_{CE} \quad (3.5)$$

3.4.1.2 Temps d'arrêt moyen équivalent.

La tâche principale suivante consiste à déterminer le temps d'arrêt moyen du groupe lorsqu'un DGF se produit. Dans la mesure où le temps d'arrêt après une panne de DD est différent du temps d'arrêt après une panne de DU, nous devons peser les deux temps d'arrêt. Le processus de pesage est d'abord illustré pour un seul canal. Par la suite, le temps d'arrêt moyen pour un groupe de deux canaux indépendants et identiques votés loo2 est déterminé.

- Temps d'arrêt moyen équivalent pour un seul canal : Considérons un canal unique qui peut avoir des défaillances DU et DD. Le canal peut être considéré comme une architecture en série de deux éléments virtuels, un élément qui ne peut avoir que des défaillances DU et un élément qui ne peut avoir que des défaillances DD, comme le montre la figure 3.5.

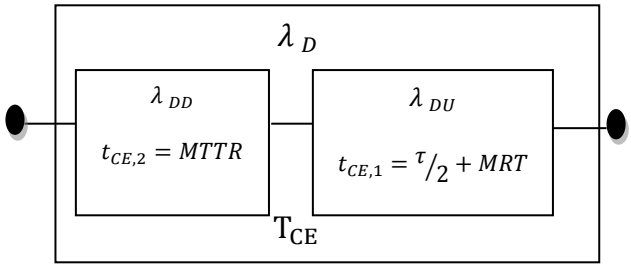


Figure 3.5 Schéma fonctionnel de fiabilité d'un canal unique considéré comme un système en série de deux éléments virtuels.

Si une défaillance D se produit, la probabilité que cette défaillance soit une défaillance DU est la suivante :

$$\Pr(DU/D) = \frac{\lambda_{DU}}{\lambda_{DD} + \lambda_{DU}} = \frac{\lambda_{DU}}{\lambda_D} \tag{3.6}$$

Et la probabilité qu'il s'agisse d'une défaillance de DD est la suivante :

$$\Pr(DD/D) = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} = \frac{\lambda_{DD}}{\lambda_D} \tag{3.7}$$

Si la défaillance D est une défaillance DU, le temps d'arrêt moyen associé à cette défaillance est de :

$$E(D_{DU}) = \frac{\tau}{2} + MRT \tag{3.8}$$

Une défaillance DU n'est révélé que lors d'un proof test et elle est en moyenne présent depuis un certain temps τ/2 (CEI_61508 2010; Rausand 2014). Lorsque la défaillance DU a été révélée lors d'un proof test, le canal doit être réparé/restauré et le temps d'arrêt associé est le temps moyen de réparation (MRT).

Si la défaillance D est une défaillance DD, le défaut est révélé par le système de diagnostic et le temps d'arrêt moyen jusqu'à ce que le canal soit restauré est le $MTTR$, qui comprend deux parties :

- Le temps entre la défaillance et sa détection
- Le temps nécessaire pour réparer ou restaurer le canal.

Le temps entre la défaillance et sa détection est égale à la moitié de l'intervalle du test de diagnostic (habituellement moins de quelques minutes).

Le temps d'arrêt moyen équivalent au canal (t_{CE}) pour le canal est donc le suivant :

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}\ MTTR \tag{3.9}$$

- Temps d'arrêt moyen équivalent pour un groupe voté de 1oo2 : Considérons un groupe voté de 1oo2 avec deux canaux indépendants et identiques qui peuvent avoir des défaillances DU et DD. Parce que les canaux sont indépendants, ils ne peuvent pas tomber en panne en même temps. Pour qu'il y ait une défaillance dangereuse d'un groupe, l'un des canaux doit d'abord avoir une défaillance D, et lorsque ce canal est en panne avec une défaillance D, l'autre canal doit avoir aussi une défaillance D. Si la deuxième défaillance est une défaillance DU, le temps d'arrêt du groupe loo2, sera approximativement $\tau/3 + MRT$(CEI_61508 2010; Rausand 2014). Si la deuxième panne est une panne DD, le temps d'arrêt sera $MTTR$.

Le temps d'indisponibilité moyen équivalent au groupe loo2 voté est donc de

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}\ MTTR \tag{3.10}$$

3.4.2 PFD_{avg} avec défaillances de causes communes

Cette section montre comment le modèle du facteur bêta peut être utilisé avec les formules de la CEI. La norme CEI 61508 applique deux facteurs bêta, β pour les défaillances DU et β_D pour les défaillances DD. Il est généralement admis que le β_D < ß. La justification de cette différence est examinée dans la référence (Rausand 2014). Dans la section 3.4.1.2 montre qu'un canal peut être divisé en une partie virtuelle qui n'est exposée qu'aux défaillances du DU et une autre partie virtuelle qui est uniquement exposée aux défaillances du DD. A partir de cette approche, un canal peut être divisé en quatre parties virtuelles :

- Une pièce indépendante qui n'est exposée qu'aux défaillances DU
- Une pièce indépendante qui n'est exposée qu'aux défaillances DD
- Un élément de cause commune pour les défaillances DU (DU-CCFs)
- Un élément de cause commune pour les défaillances DD (DD-CCFs)

Le canal peut être représenté sous la forme d'une architecture en série de ces quatre parties, comme l'illustre la figure 3.6 le groupe de canaux votés peut être représenté sous la forme d'une architecture en série de trois parties :

- (a) une partie "indépendante" comprenant un certain nombre de canaux indépendants et identiques avec des taux de défaillance (1 - β_D) λ_{DU} et (1 -

β) λ_{DD}, respectivement pour les défaillances DU et DD ;

- (b) un élément CCF virtuel représentant les défaillances DU, avec taux de défaillance $\beta\lambda_{DU}$;
- (c) un élément CCF virtuel représentant les défaillances DD avec taux de défaillance $\beta_D\beta\lambda_{DD}$.

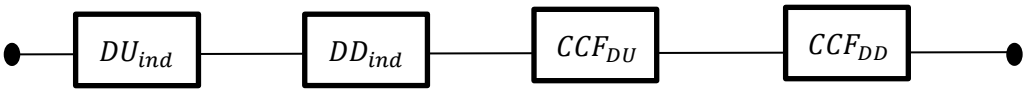


Figure 3.6 Canal intégrant les défaillances indépendantes de de cause commune

Le schéma bloc fiabilité pour un groupe voté 2oo3 est montré à la figure 3.7

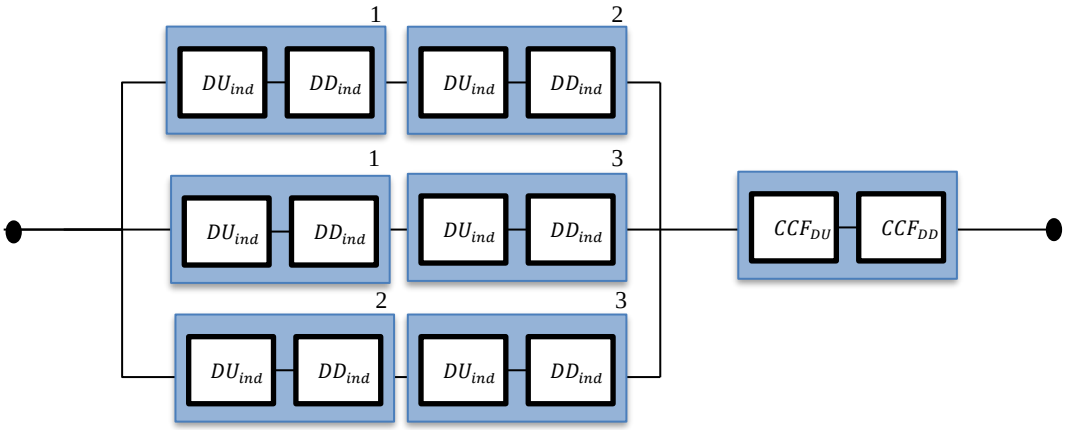


Figure 3.7 Schéma fonctionnel de fiabilité d'un groupe 2oo3 voté avec DU et DD-CCF modélisés avec le modèle du facteur bêta.

Nous avons montré en (3.3) que le PFD_{avg} pour une architecture de série est approximativement égal à la somme des PFD_{avg} des éléments de l'architecture de série. Le PFD_{avg} d'un groupe voté modéliser avec le modèle du facteur bêta peut donc s'écrire ainsi

$$PFD_{avg}^{(G)} = PFD_{avg}^{(i)} + PFD_{avg}^{(DU-CCF)} + PFD_{avg}^{(DD-CCF)} \quad (3.11)$$

Où,

- $PFD_{avg}^{(i)}$ est le PFD_{avg} du groupe voté des chaînes indépendantes.
- $PFD_{avg}^{(DU-CCF)}$ est le PFD_{avg} de l'élément CCF virtuel pour les défaillances DU.
- $PFD_{avg}^{(DD-CCF)}$ est le $PFDavg$ de l'élément CCF virtuel pour les défaillances DD.

Et,

$$PFD_{avg}^{(DU-CCF)} = \beta\lambda_{DU}(\frac{\tau}{2} + MRT) \tag{3.12}$$

Où $\beta\lambda_{DU}$ est le taux de DU-CCF et $(\frac{\tau}{2} + MRT)$est le temps d'arrêt moyen pour chaque DU-CCF.

$$PFD_{avg}^{(DD-CCF)} = \beta_D\lambda_{DU}MTTR \tag{3.13}$$

Où $\beta_D\lambda_{DU}$ est le taux de DD-CCF et $MTTR$ est le temps d'arrêt moyen pour chaque DD-CCF.

3.4.3 PFD_{avg} selon l'architecture KooN

Finalement on synthétisant les expressions analytiques, on obtient les formules présenter dans le tableau 3.1 pour différente architecture KooN.

Architectures	**PFD_{avg}**
1oo1	$(\lambda_{DU} + \lambda_{DD}) \times t_{CE}$
1oo2	$2 \times \left[(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}\right]^2 \times t_{CE}$ $\times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \times \left(\frac{Ti}{2} + MTTR\right)$
1oo3	$6 \times \left[(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}\right]^3 \times t_{CE}$ $\times t_{GE} \times t_{G2E} + \beta_D \times \lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \times \left(\frac{Ti}{2} + MTTR\right)$
2oo2	$2\lambda_D t_{CE}$
2oo3	$6 \times \left[(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}\right]^2 \times t_{CE}$ $\times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \times \left(\frac{Ti}{2} + MTTR\right)$

Tableau 3.1 Formules Analytiques Relatives Aux PFD_{avg} Des Architectures Koon Selon La CEI 61508-6

Sachant que :

$$T_{GE} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T_I}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR \tag{3.14}$$

$$T_{CE} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T_I}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR \tag{3.15}$$

$$T_{G2E} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T_I}{4} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR \tag{3.16}$$

$$\beta = 2 \times \beta_D \tag{3.17}$$

3.5 Expressions analytiques des PFH

La norme CEI 61508-6 fournit des formules d'approximation pour les PFH pour certains groupes votés avec un maximum de trois canaux. Les formules sont basées sur les mêmes idées qui sont utilisées pour les PFD_{avg} par les formules de la CEI a la section 3.4.1.

Le temps de rétablissement pour les défaillances DD n'est pas couvert dans les formules PFH de la CEI parce que la contribution des événements dangereux dans le temps de rétablissement moyen, MTTR, est considérée comme négligeable.

3.5.1 PFH selon l'architecture KooN

- Groupe voté 1oo1. Une défaillance DD d'un groupe avec un seul canal est une défaillance de groupe et l'EUC est immédiatement ramenée à un état sûr. Une défaillance de groupe dangereuse (DGF) ne se produit donc que lorsqu'une défaillance DU se produit et que le PFH est par conséquent

$$PFD_G^{(1001)} = \lambda_{DU} \tag{3.18}$$

- Groupe voté 1oo2. Une FDG d'un groupe voté de 1oo2 peut se produire de deux façons différentes, défaillances indépendantes et défaillances de cause commune :
  - Défaillance D indépendante : Il peut s'agir d'une défaillance DU ou d'une défaillance DD. Le temps d'arrêt équivalent au canal est $t_{CE.}$ Si la deuxième défaillance est une défaillance de DD, cette défaillance est détectée et la fonction est restaurée dans $MTTR$, de sorte que la probabilité d'un DGF dans ce court intervalle est négligeable. La seule option pour un DGF est donc que la deuxième défaillance est une défaillance DU. La contribution au PFH à partir de cette option s'élève à :

$$PFD_{G(a)}^{(1002)} = 2\lambda_D^{(i)}\left(1 - e^{-(1-\beta)t_{CE}\lambda_{DU}}\right) = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}](1-\beta)\lambda_{DU}t_{CE} \tag{3.19}$$

  - Défaillance de cause commune DU-CCF : La contribution au PFH à partir de cette option s'élève à :

$$PFD_{G(b)}^{(1002)} = \beta\lambda_{DU} \tag{3.20}$$

Le PFH total du groupe loo2 voté est donc de

$$PFD_G^{(1002)} = 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}](1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU} \quad (3.21)$$

- 2002 Groupe voté. Un groupe voté 2oooo2 se trouve dans une situation dangereuse lorsqu'un de ses canaux subit une défaillance dangereuse, mais de la même manière que pour un seul canal, l'EUC est immédiatement mis dans un état sûr lorsqu'une défaillance de DD survient. Seules les défaillances DU sont donc dangereuses pour l'EUC. Le PFH d'un groupe 2oo2 voté est donc

$$PFD_G^{(2002)} = 2\lambda_{DU} \quad (3.22)$$

- 2003 Groupe voté. Considérons un groupe de 2oo3 chaînes votées identiques. Comme pour le groupe de vote loo2, le groupe de vote 2oo3 peut avoir deux types de défaillances dangereuses.
  - Défaillances indépendantes : Supposons que l'un des trois canaux ait une défaillance D indépendante. Le taux de cet événement est de 3λ. Pour qu'il y ait une défaillance dangereuse d'un groupe, l'un des deux canaux restants doit avoir une défaillance DU indépendante (avec le taux $2(1-\beta) \times \lambda_{DU}$ avant que la première défaillance D est restaurée.
  - Défaillance de cause commune : Une défaillance de groupe dangereuse se produit lorsqu'un DU-CCF se produit. Si une DD-CCF se produit, l'EUC est immédiatement amenée à un état sûr et le DD-CCF n'est donc pas une défaillance de groupe dangereuse pour l'EUC.

La formule de la CEI pour le groupe 2oo3 voté est donc la suivante :

$$\begin{aligned} PFD_G^{(2003)} &= 3\lambda_D^{(i)}\left(1 - e^{-2(1-\beta)t_{CE}\lambda_{DU}}\right) + \beta\lambda_{DU} \\ &= 3[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]2(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU} \\ &= 3\lambda_D^{(i)}\left(1 - e^{-2(1-\beta)t_{CE}\lambda_{DU}}\right) + \beta\lambda_{DU} \\ &= 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}](1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU} \end{aligned} \quad (3.23)$$

Finalement on obtient les formules PFH présentées dans le tableau 3.2 pour differente architecteur KooN.

Architectures	PFH
1oo1	λ_{DU}
1oo2	$2 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}](1-\beta) \times \lambda_{DU} \times t_{CE} + \beta \times \lambda_{DU}$
1oo3	$6 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}]^2 (1-\beta) \times \lambda_{DU} \times t_{CE} \times t_{GE} + \beta \times \lambda_{DU}$
2oo2	$2\lambda_{DU}$
2oo3	$6 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}](1-\beta) \times \lambda_{DU} \times t_{CE} + \beta \times \lambda_{DU}$

Tableau 3.2 Formules analytiques relatives aux PFH des architectures KooN selon la CEI 61508-6

3.6 Conclusion

L'évaluation des performances des système instrumentés de sécurité passe impérativement par la détermination des PFD_{avg} et / ou PFH comme mesure de fiabilité. Lorsque le taux de demande est respectivement moins d'une fois par an ou plus d'une fois par an on peut revendiquer la conformité à la norme CEI 61508 en utilisant respectivement PFD_{avg} et PFH.

Dans ce chapitre on a synthétisé et présenté les expressions analytiques des PFD_{avg} et PFH permettant l'évaluations des performances des SIS selon la CEI pour différentes architectures KooN.

Pour déterminer le PFD_{avg} et le PFH d'un groupe voté, il est nécessaire de déterminer le taux moyen de défaillances et le temps d'arrêt moyen lorsqu'une DGF (Dangerous group failure) se produit, tout en intégrant le facteur β des défaillances de cause commune à travers les formules de la norme CEI 61508.

Il est a noté que lorsque le taux de demande est proche d'une fois par an, on devrait aussi pouvoir revendiquer la conformité à la norme CEI 61508 en utilisant soit PFD_{avg} soit PFH. Le problème est toutefois que les deux mesures de fiabilité peuvent mener à des conclusions différentes. Trois causes possibles de cette incohérence sont identifiées :

- Les intervalles dans les tableaux SIL pour les différents SIL ne sont pas calibrés correctement.
- Les formules de la CEI pour les modes de fonctionnement à faible et à forte demande reposent sur des hypothèses différentes.
- Les approximations sur lesquelles se fondent les formules de la CEI ne sont pas entièrement adéquates lorsque le taux de demande est d'environ une fois par an.

Dans la suite de ce travail, le chapitre 4 est consacré à l'évaluation des SIS, sollicités à

faible demande, par la mesure du PFD_{avg} conformément à la CEI 61508, et tente en partie l'amélioration des approximations sur lesquelles elles se fondent.

4

Contribution à l'amélioration de l'évaluation des performances des SIS

4.1 Introduction

Dans ce chapitre on traite l'imperfection des valeurs de la probabilité moyenne de défaillance à la demande (PFD_{avg}) qui crée une incertitude en ce qui concerne l'efficacité du système instrumenté de sécurité (SIS). Pour surmonter ce problème, de nombreux paramètres tels que les défaillances dangereuses, les défaillances de cause commune, le taux de couverture de diagnostic et les proof tests sont pris en compte. L'impact et l'importance de ces proof tests sur l'attribution du niveau d'intégrité de sécurité (SIL) du SIS est montré à travers les résultats obtenus dans quatre études de cas réalisées. La dernière étude de cas est consacrée à nos propositions et développements de deux nouvelles formules analytiques permettant l'amélioration de l'évaluation des performances de sécurité des SIS.

- Dans la première étude on définit le niveau d'intégrité de sécurité (SIL) lié à une fonction instrumentée de sécurité (SIF), en l'occurrence la « LAHH-1507 », en utilisant la méthode de graphe des risques. Cette fonction instrumentée de sécurité est une boucle de sécurisation de la ligne d'aspiration du GPL au sein du complexe gazier.
- Dans la deuxième étude le problème d'imprécision dans l'évaluation de niveaux d'intégrité des systèmes instrumentés de sécurité (SIS) est traité. Deux méthodes d'évaluation sont appliquées. La première méthode d'évaluation utilise l'approche analytique découlant de la norme CEI 61508 et la seconde utilise un automate de simulation qui se base sur l'amélioration de ces équations.
- La troisième étude est consacrée à une comparaison entre différentes formulations analytiques relatives aux indicateurs de performance des SIS : PFD_{avg}, PFH, formules découlant de la norme CEI 61508 (IEC61508 1998) et (CEI_61508 2010), aux formules proposées par Innal (Innal 2008) et celles exposées dans l'organisme norvégien SINTEF (SINTEF 2013b).
- Dans la quatrième étude on propose deux modèles analytiques permettant d'analyser l'effet des proof tests dans l'évaluation de la performance de ces SIS. A la base de nombreux paramètres tels que les défaillances dangereuses, les défaillances de causes communes, le taux de couverture de diagnostic et les proof tests sont pris en considération. On a accordé une attention particulière aux taux de défaillance non détectée par le proof test. L'influence de ce taux de défaillance, sur la précision du PFD_{avg} d'un SIS est montré à travers les résultats obtenus dans l'étude quantitative réalisée.

4.2 Etude de cas 1 – Evaluation à partir du Graphe des risques

Le SIS étudié est situé dans un complexe industriel du groupe Sonatrach, localisé à Hassi R'mel, (Benamar 2010/2011) in (Asklou and Noureddine. 2016a) qui fait le stockage et le transfert du GPL (Gaz Pétrolier Liquéfié) et du condensat. Ce complexe est constitué d'un ensemble d'équipements industriels (Pompes, compresseurs, turbines, ballons, sphère, échangeurs, turbo-expander)

4.2.1 Analyse de la fonction instrumentée de sécurité « LAHH-1507 »

La fonction de sécurité instrumentée (SIF) « LAHH-1507 » figure 4.1, du SIS étudié, a pour rôle d'assurer la protection contre le dépassement du niveau de GPL dans la sphère. Le signal de haute pression capté au niveau du capteur LT1507 est utilisé comme signal d'entrée à l'unité logique qui va générer un signal d'alarme sur DCS (Distributed Control System) et permettre à la vanne HV1528 de s'ouvrir. Ceci assurera la dépressurisation du niveau de GPL dans la sphère.

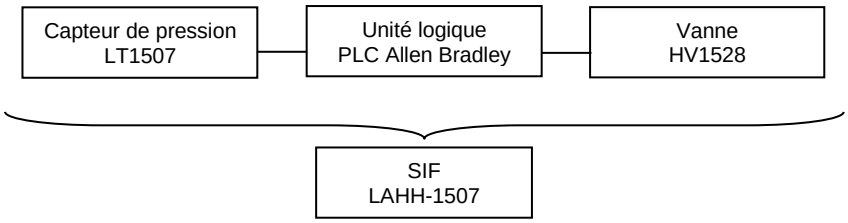


Figure 4.1 Structure de la fonction instrumentée de sécurité « LAHH-1507 »

4.2.2 Allocation du niveau d'intégrité de sécurité de la SIF « LAHH-1507 »

Les données découlant de l'analyse préliminaire des risques associées aux paramètres de risque liés à la norme CEI 61511, permettent d'identifier les paramètres du graphe des risques, figure 4.2, ont été utilisées pour allouer le niveau d'intégrité de sécurité (SIL) à la SIF « LAHH-1507 » :

- Paramètre C : La conséquence attendue en termes d'atteinte à la vie humaine ou de blessures, dans le cas où l'événement dangereux se produit est évalué à C_c (étendue du site assez importante), puisque l'analyse préliminaire des risques "APR" a évalué le niveau de gravité du scénario de sollicitation à un niveau C : Important {(externe) entre 1 et 10 personnes exposées ; (interne) entre 10 et 100 personnes exposées}
- Paramètre F : La fréquence d'exposition au risque a été évaluée au niveau F_B car une présence humaine permanente est envisagée dans la zone dangereuse considérée ;
- Paramètre P : La possibilité d'éviter le danger est considérée au niveau P_A puisqu'il

existe des moyens de protection (SV1503, Alarmes de détection gaz, Alarme de déclenchement, etc.)

- Paramètre W : Enfin en ce qui concerne la probabilité d'occurrence, le seuil W_2 est pris car ce risque de dépassement du niveau s'est produit récemment sur le site. La vanne de sécurité HV1528 a été sollicitée pour une dépressurisation d'urgence.

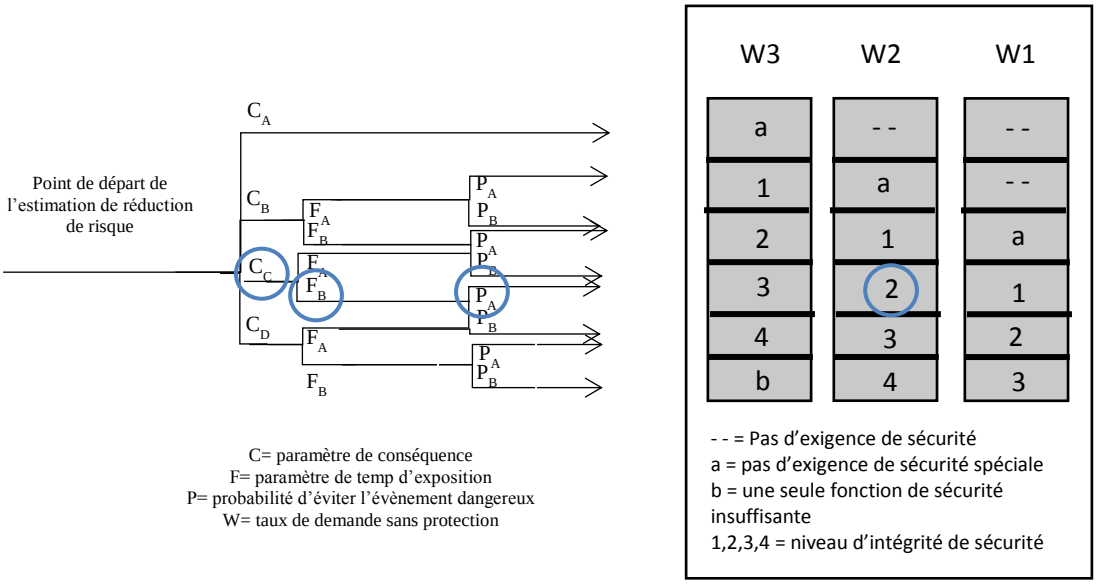


Figure 4.2 Allocation SIL sur graphe de risque présenté dans la CEI 61511

- *Résultat graphique* : Cette fonction instrumentée de sécurité « LAHH-1507 » est évaluée à un niveau d'intégrité de sécurité requis « SIL2 ». Le SIL2 correspond selon la norme CEI 61511, à une probabilité de défaillance moyenne PFD_{avg} comprise entre 10^{-2} et 10^{-3} (tableau 2.1).

4.2.3 Discussion et interprétation des résultats

Dans le cas du contexte du complexe gazier étudié, le choix de la méthode du graphe des risques adoptée pour l'évaluation du niveau d'intégrité de sécurité du SIS est justifié principalement par la nature des données. La fonction instrumentée de sécurité étudiée a été évaluée à un niveau d'intégrité de sécurité SIL2 qui correspond à un facteur de réduction de risques de 100 à 1000. La fréquence tolérable est réduite alors à un niveau entre 10^{-5} et10^{-7}, ce qui permet de faire chuter la fréquence d'occurrence à une fréquence extrêmement peu probable, c'est-à-dire de faire basculer le risque vers une zone moins dangereuse.

Cette contribution a permis d'une part de justifier l'utilisation de la méthode graphique, et d'autre part d'évoquer que des efforts restent à fournir pour la maîtrise des risques industriels

au niveau du complexe gazier étudié.

4.3 Etude de cas 2 – Evaluation à partir de la méthode analytique CEI 61508

Il s'agit d'un système de sécurité de torche. Deux méthodes d'évaluation sont appliquées (Asklou et al. 2016b). La première méthode d'évaluation utilise l'approche analytique découlant de la norme CEI 61508 et la seconde utilise un automate de simulation qui se base sur l'amélioration de ces équations.

La figure 4.3 présente de manière simplifiée la mise en place d'un SIS permettant de limiter la pression à l'intérieur d'un équipement sous pression. Ce dispositif est connu sous le nom de High Integrity Pressure Protection System (HIPPS). Ce type de système peut être mis en place lorsque le débit de gaz destiné à brûler au niveau d'une torche, suite à l'ouverture de soupapes, nécessiterait une torche dont les dimensions sont trop contraignantes en termes de dimensionnement.

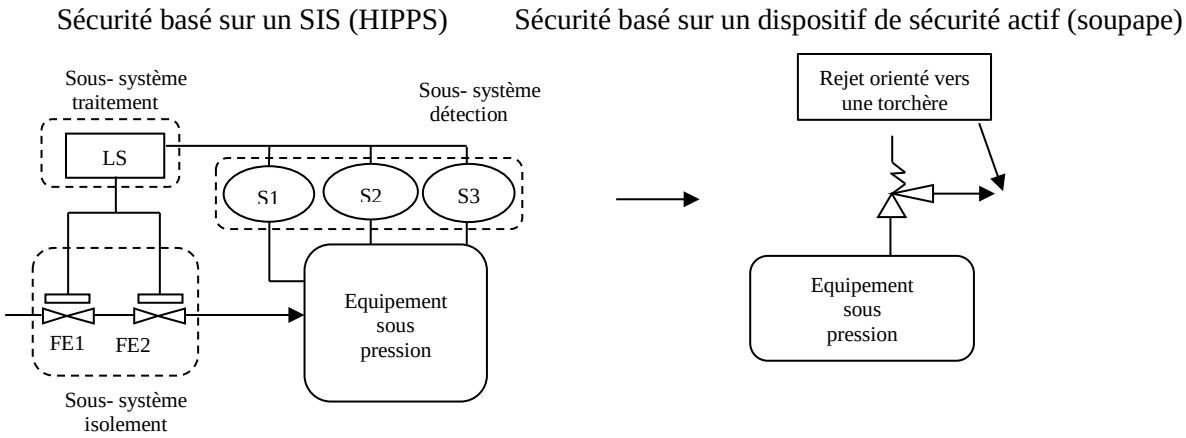


Figure 4.3 Schéma de principe du système de sécurité de torche

Ce cas d'étude peut être modélise par le schéma block présenté en figure 4.4.

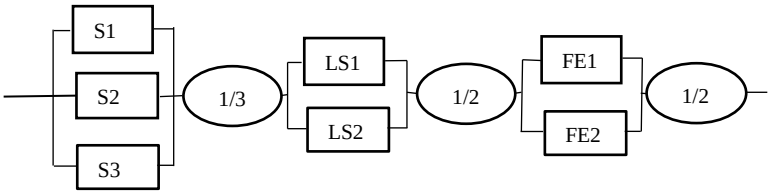


Figure 4.4 Schéma-bloc du SIS

Pour le calcul de la PFD_{avg} de ce SIS, les données de fiabilité du tableau 4.1 (Iddir 2009) in (Asklou et al. 2016b) sont retenues.

Dispositif	Taux de défaillance (10^{-6}/h)		Mode commun de défaillances (%)		MTTR (h)	TI (h)
	λ_D	λ_{DU}	B	β_D		
Transmetteurs analogique (S1, S2, S3)	0.8	0.3	3	1.5	8	4380
Logique (LS1, LS2)	1	0.1	2	1	8	4380
Vanne (FE1, FE2)	4	2.9	2	1	8	4380

Tableau 4.1 Données de fiabilité du SIS-HIPPS

4.3.1 Évaluation à l'aide des formules CEI 61508

Les équations utilisées pour déterminer la probabilité de défaillance moyenne sur demande sont celles présentées dans le tableau 3.1.

- Calcul de la PFD_{avg} du sous-système traitement (LS) :

$$PFD_{avg} = 4.46 \times 10^{-6} \text{ /sollicitation}$$

- Calcul de la PFD_{avg} du sous-système action (FE) :

$$\text{PFD}_{\text{avg}} = 1.27 \times 10^{-4} \text{/sollicitation}$$

- Calcul de la PFD_{avg} du sous-système détection (S) :

$$PFD_{avg} = 4.73 \times 10^{-5} \text{/sollicitation}$$

- Calcul de la PFD_{avg} total du SIS :

Le calcul de la PFD_{avg} total du SIS est donné par :

PFD_{avg} (SIS) = PFD_{avg} (bloc détection) + PFD_{avg} (bloc traitement) + PFD_{avg} (action).

On obtient :

$$PFD_{avg} \text{ (SIS)} = 1.78 \times 10^{-4} \text{ /sollicitation}$$

4.3.1.1 Présentation des résultats

Dans ce cas d'étude, la probabilité moyenne de défaillances à la sollicitation du SIS est évaluée à :

$$PFD_{avg} = 1.78 \times 10^{-4} \text{ /sollicitation}$$

Au regard de cette valeur de PFD_{avg} et des valeurs normatives, ce SIS est évalué un niveau d'intégrité SIL 3 (tableau 2.1).

4.3.2 Évaluation à l'aide d'un automate

Le logiciel utilisé dans ces simulations, dénommée « Système instrumenté de Sécurité », pour l'évaluation du SIL est téléchargeable gratuitement sur le site à l'adresse URL référencé (URL-2).

Les trois scénarios simulés prennent en compte les paramètres initiaux, minimaux et maximaux de λ_{sd} et λ_{su} (Asklou et al. 2016b) influant le calcul de l'intégrité SIL de la fonction instrumentée de sécurité étudiée.

4.3.2.1 Scénario 1 : Paramètres initiaux

On a introduit les paramètres initiaux, figure 4.5, du SIS-HIPPS. Le résultat du PFD_{avg} déterminé par simulation est le même que le résultat déterminé par calcul analytique. Cependant, l'allocation du niveau SIL à partir du logiciel est située à un niveau SIL 2 requis, alors qu'en application de la norme CEI61508 le niveau requis est un SIL 3.

Cette différence constatée, on peut l'attribuer à la prise en compté dans l'automate des paramètres de fiabilité λ_{sd} et λ_{su} par défaut.

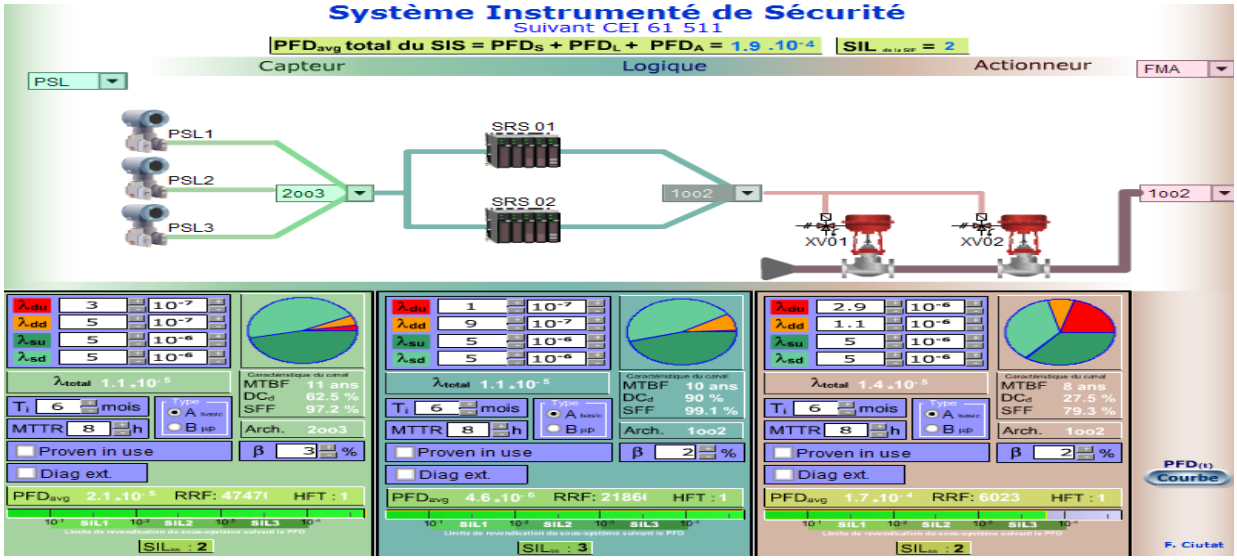


Figure 4.5 Visualisation du scénario 1

4.3.2.2 Scénario 2 : Paramètres maximaux

Dans ce scénario, figure 4.6, en plus des paramètres initiaux précédents, on a introduit les valeurs maximales des paramètres de fiabilité :

- Taux de défaillance sûre détecté : $\lambda_{SD} = 10^{-4}$
- Taux de défaillance sûre non détecté : $\lambda_{SU} = 10^{-4}$.

Dans ce cas, le résultat SIL alloué reste inchangé (SIL 2).

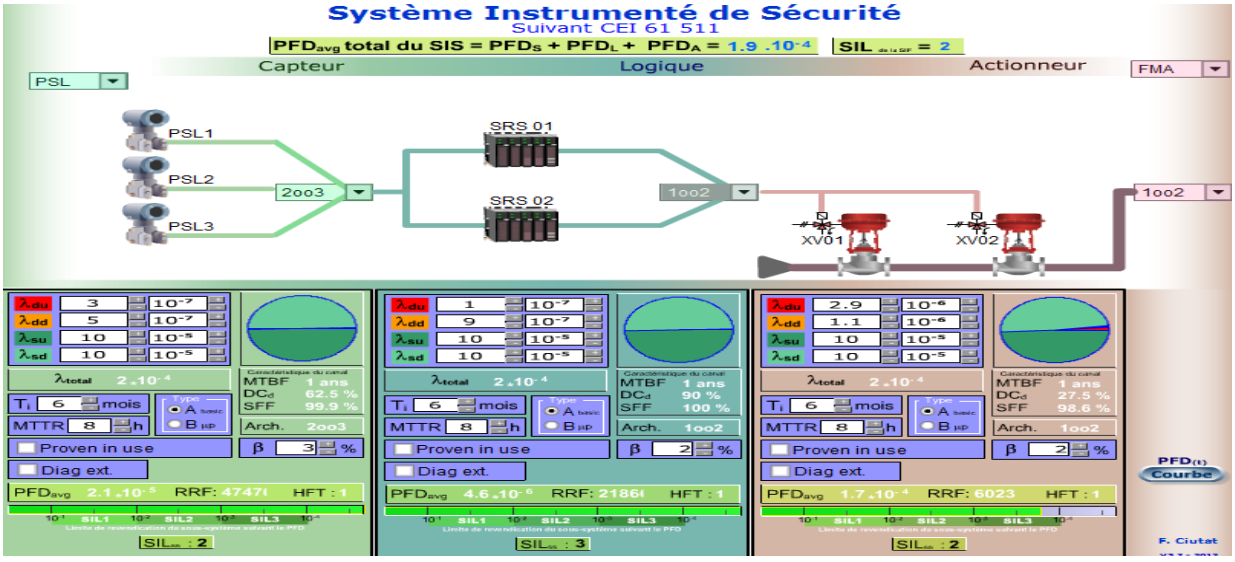


Figure 4.6 Visualisation du scénario 2

4.3.2.3 Scénario 3 : Paramètres minimaux

Dans ce 3ème scénario, figure 4.7, on a introduit les valeurs minimales des paramètres de fiabilité :

- Taux de défaillance sûre détecté : $\lambda_{SD} = 0$
- Taux de défaillance sûre non détecté : $\lambda_{SU} = 0$.

Malgré une valeur de PFD_{avg} inchangé, le SIL alloué dans ce cas par le simulateur est un SIL 1.

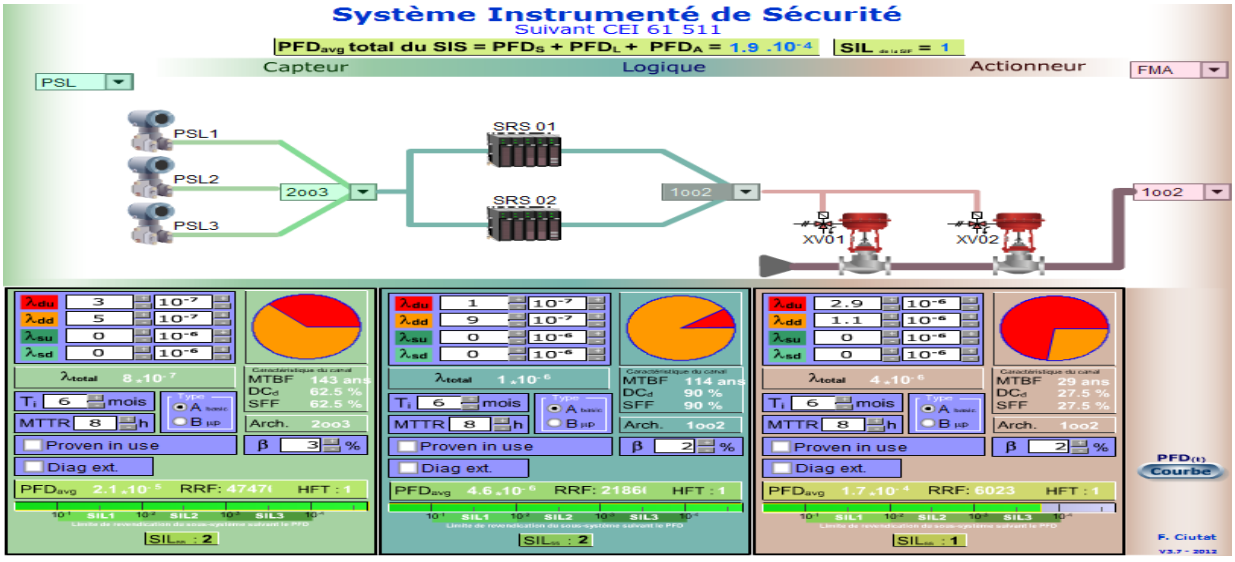


Figure 4.7 Visualisation du scénario 3

4.3.3 Discussion et interprétation des résultats

Dans cette étude de cas, le problème de l'imprécision dans l'évaluation du niveau d'intégrité dans les systèmes instrumentés de sécurité est montré, en appliquant deux méthodes.

A partir des résultats obtenus, on déduit qu'il existe une relation importante entre d'une part, le taux de défaillance sûre détecté et non détecté (λ_{sd}, λ_{su}) et d'autre part, le niveau d'intégrité SIL alloué. En effet, les taux de défaillance sûre ne sont pas pris en considération dans les équations analytiques simplifiées. Ce qui explique des SIL alloués différents malgré des valeurs de PFD_{avg} identiques dans les deux méthodes de calcul. De plus en l'absence de données spécifique à un matériel, l'analyse peut être amené à faire certaines hypothèses sur des paramètres, tels que le taux de défaillance sûre détecté et non détecté (λ_{sd} ;λ_{su}). La PFD_{avg} d'un SIS calculée et le SIL qui en découle ne saurait donc être une valeur exacte, et il est nécessaire que l'analyse précise les hypothèses et limites des calculs réalisés.

Enfin, le niveau SIL qui prend en compte les taux de défaillance sûre détecté et non détecté (λ_{sd} ;λ_{su}) est plus précis, mais la valeur PFD_{avg} est une exigence suffisante à satisfaire le niveau d'intégrité de sécurité par la norme CEI 61508. Pour la valeur (λ_{sd} ;λ_{su}) il n'existe pas actuellement de prescriptions dans le monde de la sécurité internationale, bien que les utilisateurs de système de sécurité exigent un niveau aussi bas que possible de cette valeur.

4.4 Etude de cas 3 - Comparaison approche analytique CEI 61508 - autres méthodes

Il existe dans la littérature plusieurs formules analytiques qui traitent des performances des systèmes instrumentés de sécurité. On s'intéresse plus en détails, dans cette étude de cas, aux formules découlant de la norme CEI 61508 (IEC61508 1998) et (CEI_61508 2010), aux formules proposées par Innal (Innal 2008) et celles exposées dans l'organisme norvégien SINTEF (SINTEF 2013b).

4.4.1 Formules Innal

Nous résumons dans ce qui suit les formulations analytiques développé par Innal (Innal 2008), fondées sur deux approches différentes : markovienne approchée et modèle binomial.

- Approche markovienne : elle a donné les formulations présentées dans les tableaux 4.2 et 4.3.

Architectures	**PFD_{avg}**
1oo1	$\lambda_{DU} \times \left(\frac{Ti}{2} + MTTR\right) + \lambda_{DD} \times MTTR$

1oo2	$2\lambda_D^2\left[\frac{(1-\beta)\lambda_{DU}}{\lambda_D}\left(\frac{Ti}{2}+MTTR\right)+\frac{(1-\beta_D)\lambda_{DD}}{\lambda_D}MTTR\right]\times\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{Ti}{3}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR\right]+\beta_D\times\lambda_{DD}\times MTTR+\beta\times\lambda_{DU}\times\left(\frac{Ti}{2}+MTTR\right)$
2oo2	$2[(1-\beta_D)\times\lambda_{DD}+(1-\beta)\times\lambda_{DU}]\times\left[\frac{(1-\beta)\lambda_{DU}}{(1-\beta_D)\times\lambda_{DD}+(1-\beta)\times\lambda_{DU}}\left(\frac{Ti}{2}+MTTR\right)+\frac{(1-\beta_D)\lambda_{DD}}{(1-\beta_D)\times\lambda_{DD}+(1-\beta)\times\lambda_{DU}}MTTR\right]+\beta_D\times\lambda_{DD}\times MTTR+\beta\times\lambda_{DU}\times\left(\frac{Ti}{2}+MTTR\right)$
2oo3	$3[(2-\beta_D)\times\lambda_{DD}+(2-\beta)\times\lambda_{DU}]\times\left[(1-\beta_D)\times\lambda_{DD}\times MTTR+(1-\beta)\times\lambda_{DU}\times\left(\frac{Ti}{2}+MTTR\right)\right]\times\left[\frac{(2-\beta)\lambda_{DU}}{(2-\beta_D)\times\lambda_{DD}+(2-\beta)\times\lambda_{DU}}\left(\frac{Ti}{3}+MTTR\right)+\frac{(2-\beta_D)\lambda_{DD}}{(2-\beta_D)\times\lambda_{DD}+(2-\beta)\times\lambda_{DU}}MTTR\right]+\beta_D\times\lambda_{DD}\times MTTR+\beta\times\lambda_{DU}\times\left(\frac{Ti}{2}+MTTR\right)$

Tableau 4.2 Formules analytiques relatives aux PFD_{avg} des architectures KooN obtenues via une approche markovienne approchée

Architectues	$\boldsymbol{PFH}$
1oo1	$\lambda_{DU}+\lambda_{DD}$
1oo2	$2\lambda_D^2\left[\frac{(1-\beta)\lambda_{DU}}{\lambda_D}\left(\frac{Ti}{2}+MTTR\right)+\frac{(1-\beta_D)\lambda_{DD}}{\lambda_D}MTTR\right]+\beta_D\times\lambda_{DD}+\beta\times\lambda_{DU}$
2oo2	$2[(1-\beta_D)\times\lambda_{DD}+(1-\beta)\times\lambda_{DU}]+\beta_D\times\lambda_{DD}+\beta\times\lambda_{DU}$
2oo3	$3[(2-\beta_D)\times\lambda_{DD}+(2-\beta)\times\lambda_{DU}]\times\left[(1-\beta_D)\times\lambda_{DD}\times MTTR+(1-\beta)\times\lambda_{DU}\times\left(\frac{Ti}{2}+MTTR\right)\right]+\beta_D\times\lambda_{DD}+\beta\times\lambda_{DU}$

Tableau 4.3 Formules analytiques relatives aux PFH des architectures KooN obtenues via une approche markovienne approchée

On peut facilement remarquer que les formules données dans la norme CEI 61508 ancienne et nouvelle version (tableau 3.1, 3.2) ne sont que des approximations optimistes des formules trouvées en suivant l'approche markovienne approchée.

- Approche binomiale : elle s'est appuyée sur les formules suivantes :

$$PFD_{MOY}(KooN) = A_N^{N-K+1}\lambda_{Dind}^{N-K+1}\prod_{i=1}^{N-K+1}MDT_{1ooi} + \beta_D \quad (4.1)$$

$$\lambda_{DD} \times MTTR + \beta \times \lambda_{DU} \left(\frac{Ti}{2} + MTTR\right)$$

$$PFH(KooN) = A_N^{N-K+1} \lambda_{Dind}^{N-K+1} \prod_{i=1}^{N-K} MDT_{1ooi} + \beta_D \times \lambda_{DD} + \beta \times \lambda_{DU} \quad (4.2)$$

$$A_N^{N-K+1} = \frac{N!}{(K-1)!} \quad (4.3)$$

$$MDT_{1ooi} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T_I}{i+1} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR \quad (4.4)$$

Pour une architecture 1*oo*1, au niveau de la formule 4.1, on doit supprimer la contribution de cause commune et mettre :

$$\lambda_{Dind} = \lambda_D = \lambda_{DD} + \lambda_{DU} \quad (4.5)$$

Dans ces conditions, les formules 4.1 et 4.2 généralisent les formules données dans la version précédente de la CEI 61508 (CEI_61508 2010), excepté l'architecture 2*oo*2 (car la norme ne considère pas les causes communes pour les architectures séries).

4.4.2 Approche SINTEF

Aux tableaux 4.4, et 4.5 sont présentées respectivement les différentes formules concernant les PFD_{avg} , PFH par l'approche SINTEF (SINTEF 2013b). Elles sont basées sur le fait de négliger, d'une part, les contributions des défaillances dangereuses détectées et, d'autre part, le facteur β devant l'unité.

Architectures	**PFD_{moy}**
1oo1	$\lambda_{DU} \times Ti/2 + \lambda_{DD} \times MTTR$
1oo2	$\frac{(1-\beta)^2 \lambda_{DU}{}^2 Ti^2}{2} + 2(1-\beta) \times \lambda_{DD}.\lambda_{DU} . MTTR.\frac{Ti}{2} + \beta(\lambda_{DU} \times Ti/2 + \lambda_{DD} \times MTTR)$
2oo2	$(2\text{-}\beta)\lambda_{DU} \times Ti/2 + \beta\lambda_{DD} \times MTTR$
2oo3	$2{,}4\beta\lambda_{DU} \times \frac{Ti}{2} + [(1-1.7\beta)\lambda_{DU} \times Ti]^2 + 3(1-1.7\beta)\lambda_{DD}. MTTR. \beta\lambda_{DU} \times Ti/2$

Tableau 4.4 Formules analytiques relatives aux PFD_{avg} des architectures KooN selon SINTEF

Architectures	**Formules de calcul de PFH**		
	Contribution de cause Commune		***Contribution de défaillance indépendants***
1oo1	/	+	λ_{DU}
1oo2	$B\lambda_{DU}$	+	$[\lambda_{DU} \times Ti]^2/Ti$

2oo2	/	+	$2\lambda_{DU}$
2oo3	$C_{2oo3}\ B\lambda_{DU}$	+	$3[\lambda_{DU} \times Ti]^2/Ti$

Tableau 4.5 Formules analytiques simplifiées relatives aux PFH des architectures KooN selon SINTEF

4.4.3 Confrontation des approches CEI 61508 – Innal - SINTEF

Dans le tableau suivant un ensemble de résultats numériques ont été obtenus (Asklou and Noureddine. 2017a) en utilisant les formules précédentes pour des architectures 1oo2, afin de donner des éléments de comparaison des différentes approches. Le jeu de données utilisé à cet effet est tiré de la référence (Haddad 2012) : T1 = 1 an (8760 h), λ= 5E-5h-1, ($\beta_{DD} = \beta_D$) = ($\beta_{DU} = \beta$) /2, MTTR = 8h.

Littérature	**DC (%)**	**B(%)**	**PFD_{avg}**	**PFH**
CEI 61508 (ancienne version)	0	10	2,40E-02	6,90E-06
		20	3,20E-02	8,50E-06
	60	10	6,00E-03	3,70E-06
		20	1,20E-02	5,10E-05
	90	10	1,30E-03	1,90E-06
		20	2,30E-03	3,20E-06
CEI 61508 (nouvelle version)	0	10	2,40E-02	6,94E-06
		20	3,20E-02	8,51E-06
	60	10	6,00E-03	1,74E-06
		20	1,20E-02	2,61E-06
	90	10	1,30E-03	2,97E-07
		20	2,30E-03	5,40E-07
Approche Markovienne	0	10	2,40E-02	6,94E-06
		20	3,22E-02	8,51E-06
	60	10	6,63E-03	3,65E-06
		20	1,07E-02	5,13E-06
	90	10	1,25E-03	1,87E-06
		20	2,33E-03	3,19E-06
Approche Binomiale	0	10	2,40E-02	6,90E-06
		20	3,20E-02	8,50E-06
	60	10	6,00E-03	3,70E-06
		20	1,20E-02	5,10E-05
	90	10	1,30E-03	1,90E-06
		20	2,30E-03	3,20E-06
SINTEF	0	10	2,39E-02	7,97E-06
		20	3,21E-02	10,47E-6
	60	10	6,47E-03	1,87E-06
		20	1,04E-02	2,87E-06
	90	10	1,24E-03	3,04E-07
		20	2,33E-03	5,54E-07

Tableau 4.6 Résultats numériques relatifs aux PFD_{avg} / PFH de l'architecture 1oo2

4.4.4 Discussion et interprétation des résultats

Dans cette étude un échantillon de résultats, pour les architectures 1oo2, a été fourni à des fins de comparaison entre les trois approches CEI 61508 – Innal - SINTEF.

- La lecture de tableau 4.6 nous permet de constater que les différentes approches donnent des résultats différents des valeurs PFD_{avg} et PFH. Ceci est imputable aux hypothèses utilisées par chacune d'elles.
- Un bon accord est toutefois constaté entre les résultats fournis par les approches markovienne et la norme CEI 61508 ancienne et nouvelle version.
- Toutefois, au regard des valeurs de PFD_{avg} et PFH par rapport aux valeurs normatives des SIL, ces résultats sont évalués au même niveau d'intégrité SIL 3.

Aux regards de ces considérations, les résultats présentés montrent que c'est l'évaluation par l'approche SINTEF qui fournit le plus de sûreté, alors que l'approche CEI 61508 (nouvelle version) donne un meilleur rapport Sûreté-Coût.

4.5 Étude de cas 4 – Approches proposées

Le diagnostic (tests en ligne) et les proof tests (tests hors ligne) sont des moyens très importants pour vérifier si un SIS est capable de remplir ses fonctions de sécurité et de révéler les défaillances qui empêchent le processus d'être sûr lorsqu'il y a une demande. Le diagnostic est un moyen de détection en ligne des déviations, des dégradations et des anomalies et est souvent réalisé par du matériel et des logiciels dédiés mis en œuvre dans les appareils. Habituellement, le proof test est considéré comme parfait, mais en réalité, ce n'est pas le cas, ce qui signifie qu'il ne couvre pas à 100% les défaillances non détectées par le test de diagnostic.

4.5.1 Corrections du proof test

Jusqu'à présent, on a supposé que les proof tests et les actions de réparation associées sont parfaits en ce sens que (Rausand 2014) :

- Le proof test est effectué dans des conditions identiques et couvre toutes les conditions de demande pertinentes ;
- Les défaillances DU et toutes celles qui augmentent le risque de défaillance DU sont mises en évidence grâce au proof test ;
- Les canaux avec un problème DU (révélé) sont réparés et les canaux sont toujours remis à zéro en tant que neufs.

Ce n'est évidemment pas toujours réaliste :

- Certaines demandes sont des événements dangereux et peuvent se produire de

nombreuses façons différentes ;

- La simulation d'une demande peut également être dangereuse et peut devoir être répétée plusieurs fois pour couvrir tous les aspects de la demande ;
- Les essais de proof test sont souvent effectués dans des conditions qui diffèrent des conditions réelles de la demande.

Parmi les recherches sur cette imperfection, (Jin et al 2015) considèrent qu'il y a λ_{DU} qui ne peut être détecté par le proof test mais ne peut être trouvé que lorsque le SIS fonctionne. Tandis que (Mechri et al 2015) ont traité le SIS à l'aide de la chaîne de Markov, notamment en introduisant deux paramètres : le paramètre d'efficacité ξ et le paramètre de sécurité γ.

Dans (Asklou and Noureddine 2017b), les corrections de Jin et al (2015) sont introduites dans les formules analytiques dérivées de la norme CEI 61508. Cette approche est désignée a la section 4.5.3 par l'approche IECξ. Dans (Asklou et Noureddine in press), les corrections de (mechri et al 2015) sont introduites dans les formules analytiques dérivées de la norme IEC 61508. Cette approche est désignée dans la section 4.5.4 par l'approche IEC$\xi\gamma$.

4.5.2 Approches existantes

Il est très difficile de trouver toutes les défaillances dangereuses potentielles par un proof test et certaines défaillances dangereuses existent encore pendant toute la durée de vie du système au lieu d'être trouvées. (Mechri et al 2015) et (Jin et al 2015) considèrent le proof test imparfait.

(Mechri et al 2015) définissent deux paramètres pour augmenter l'efficacité et la performance du proof tests en basant leur analyse sur des chaînes de Markov multiphases. Les paramètres sont considérés comme tels :

- Paramètre d'efficacité ξ : il s'agit de la probabilité conditionnelle qu'une défaillance non détectée ne soit pas détectée par le proof test puisque la défaillance survient lorsque le proof test est lancé. Ce paramètre représente la capacité du proof test à révéler les défaillances latentes. Par conséquent (1 - ξ) représente la capacité de proof test de révéler les défaillances latentes. Un proof test est parfait si $\xi = 0$ puisque toutes les défaillances non détectées sont révélées et un proof test est imparfait si $\xi > 0$. Le temps d'occurrence possible correspondant de la défaillance dangereuse non détectée par le proof test est la durée de vie système (SL). Certains analystes fournissent une estimation de ξ dans le manuel de sécurité. Cette estimation est obtenue par exemple en réalisant une AMDEC détaillée pour évaluer la capacité du proof test à révéler les défaillances latentes.

- Paramètre de sécurité γ : c'est la probabilité de défaillance due au test. Ce paramètre représente la sécurité du proof test. Par conséquent, un proof test est idéal si γ = 0 car aucun défaut n'est causé par le proof test.

(Jin et al 2015) ne prennent en compte que le paramètre d'efficacité ξ. En considération de la couverture du proof test ξ, le taux de défaillance dangereux d'un élément sera constitué de :

- λ_{DD} : taux de défaillance dangereux qui peut être détecté grâce à un test d'autodiagnostic.
- $\lambda_{DU1} = \xi \times \lambda_{DU}$: taux de défaillance dangereux qui peut être détecté par un proof test.
- $\lambda_{DU2} = (1 - \xi)\,\lambda_{DU}$: taux de défaillance dangereux qui ne peut pas être détecté par un proof test.

4.5.3 Approche IECξ proposée

Dans ce développement, on propose de combiner la correction de (Jin et al 2015), liées au taux de défaillance non détecté par le proof test , avec les équations de la norme CEI 61508 (CEI_61508 2010) afin d'amélioré l'évaluation des performances des systèmes instrumentés de sécurité, en faible demande. Cette proposition est appelée l'approche IECξ (Asklou and Noureddine 2017b).

En tenant compte de la considération de Jin dans les équations 3.14, 3.15 et 3.16, on obtient :

$$T_{GE} = \frac{\lambda_{DU1}}{\lambda_D} \times \left(\frac{T_I}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR + \frac{\lambda_{DU2}}{\lambda_D} \times \left(\frac{SL}{3} + MTTR\right) \quad (4.6)$$

$$T_{CE} = \frac{\lambda_{DU1}}{\lambda_D} \times \left(\frac{T_I}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR + \frac{\lambda_{DU2}}{\lambda_D} \times \left(\frac{SL}{2} + MTTR\right) \quad (4.7)$$

$$T_{G2E} = \frac{\lambda_{DU1}}{\lambda_D} \times \left(\frac{T_I}{4} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR + \frac{\lambda_{DU2}}{\lambda_D} \times \left(\frac{SL}{4} + MTTR\right) \quad (4.8)$$

$$\lambda_{DU2} = (1 - C_s)\lambda_{DU} \quad (4.9)$$

$$\lambda_{DU1} = C_s\lambda_{DU} \quad (4.10)$$

$$\lambda_{DU} = \lambda_{DU1} + \lambda_{DU2} \quad (4.11)$$

Et donc :

Architecture	$\mathbf{PFD_{avg}}$
1001	$(\lambda_{DU} + \lambda_{DD}) \times t_{CE}$

1002	$2 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}]^2 \times t_{CE} \times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta[\lambda_{DU1} \times \left(\frac{Ti}{2} + MTTR\right) + \lambda_{DU2} \times \left(\frac{SL}{2} + MTTR\right)]$
1003	$6 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}]^3 \times t_{CE} \times t_{GE} \times t_{G2E} + \beta_D \times \lambda_{DD} \times MTTR + \beta[\lambda_{DU1} \times \left(\frac{Ti}{2} + MTTR\right) + \lambda_{DU2} \times \left(\frac{SL}{2} + MTTR\right)]$
2002	$2\lambda_{DU1} \times \left(\frac{Ti}{2} + MTTR\right) + 2\lambda_{DD} \times MTTR + 2\lambda_{DU2} \times \left(\frac{SL}{2} + MTTR\right)$
2003	$6 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}]^2 \times t_{CE} \times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta[\lambda_{DU1} \times \left(\frac{Ti}{2} + MTTR\right) + \lambda_{DU2} \times \left(\frac{SL}{2} + MTTR\right)]$

Tableau 4.7 Formules de l'approche IECξ

4.5.4 Approche IECξγ proposée

Dans ce développement, nous proposons de combiner la prise en compte de (Mechri et al 2015), liée au taux de défaillance non détecté par le proof test, avec les formules de la norme IEC 61508 afin d'apporter une amélioration supplémentaire à l'évaluation des performances des systèmes de sécurité à faible demande. Cette proposition est désignée l'approche IECξγ (Asklou and Noureddine in press).

En tenant compte de la considération de Mechri en introduisant les deux paramètres ξ et γ dans les équations 3.14, 3.15 et 3.16, les formules ci-dessous peuvent être développées :

$$T_{CE} = \frac{\xi(1-\gamma)\lambda_{DU}}{\lambda_D} \times \left(\frac{T_I}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR + \frac{(1-\xi)\lambda_{DU}}{\lambda_D} \times \left(\frac{SL}{2} + MTTR\right) \quad (4.12)$$

$$T_{GE} = \frac{\xi(1-\gamma)\lambda_{DU}}{\lambda_D} \times \left(\frac{T_I}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR + \frac{(1-\xi)\lambda_{DU}}{\lambda_D} \times \left(\frac{SL}{3} + MTTR\right) \quad (4.13)$$

$$T_{G2E} = \frac{\xi(1-\gamma)\lambda_{DU}}{\lambda_D} \times \left(\frac{T_I}{4} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR + \frac{(1-\xi)\lambda_{DU}}{\lambda_D} \times \left(\frac{SL}{4} + MTTR\right) \quad (4.14)$$

Ces nouvelles équations sont utilisées pour générer les formules PFD_{avg} dans l'approche IECξγ, présentée au tableau 4.8.

Architecture	PFD_{avg}
1001	$(\lambda_{DU} + \lambda_{DD}) \times t_{CE}$

1002	$2 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}]^2 \times t_{CE} \times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta[\xi(1-\gamma)\lambda_{DU} \times \left(\frac{Ti}{2} + MTTR\right) + (1-\xi)\lambda_{DU} \times \left(\frac{SL}{2} + MTTR\right)]$
1003	$6 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}]^3 \times t_{CE} \times t_{GE} \times t_{G2E} + \beta_D \times \lambda_{DD} \times MTTR + \beta[\xi(1-\gamma)\lambda_{DU} \times \left(\frac{Ti}{2} + MTTR\right) + (1-\xi)\lambda_{DU} \times \left(\frac{SL}{2} + MTTR\right)]$
2002	$2(\lambda_{DU} + \lambda_{DD}) \times t_{CE}$
2003	$6 \times [(1-\beta_D) \times \lambda_{DD} + (1-\beta) \times \lambda_{DU}]^2 \times t_{CE} \times t_{GE} + \beta_D \times \lambda_{DD} \times MTTR + \beta[\xi(1-\gamma)\lambda_{DU} \times \left(\frac{Ti}{2} + MTTR\right) + (1-\xi)\lambda_{DU} \times \left(\frac{SL}{2} + MTTR\right)]$

Tableau 4.8 Formules de l'approche IECξγ

4.5.5 Application : étude d'un SIS de réacteur chimique

Il s'agit d'un système de sécurité qui permet de sécuriser un réacteur chimique, figure 4.8. Ce type de système peut être mis en place lors de la détection d'un dépassement de température ou de pression, le système de sécurité coupe l'alimentation du réacteur pour éviter une réaction d'emballement (Torres-Echeverria et al. 2011 ; Mechri et al. 2015) in (Asklou and Noureddine in press).

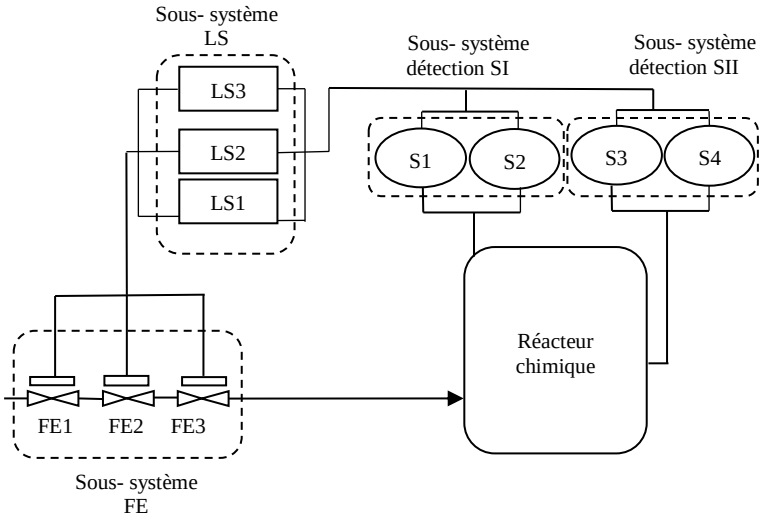


Figure 4.8 SIS du réacteur chimique

4.5.5.1 Diagramme de fiabilité

Les quatre sous-systèmes qui composent le SIS sont : 2 capteurs de température, 2 capteurs de pression, 3 unités logiques de traitement et 3 vannes.

L'architecture KooN des quatre sous-systèmes est comme suit :

- Sous-système SI (S1, S2 : capteurs de pression) : 1oo2.
- Sous-système SII (S3, S4 : capteurs de température) : 1oo2.
- Sous-système LS (LS1, LS2, LS3 : unités logiques) : 1oo3.
- Sous-système FE (FE1, FE2, FE3 : vannes) : 1oo3.

Le bloc-diagramme de fiabilité correspondant à ce SIS est donné à la figure 4.9

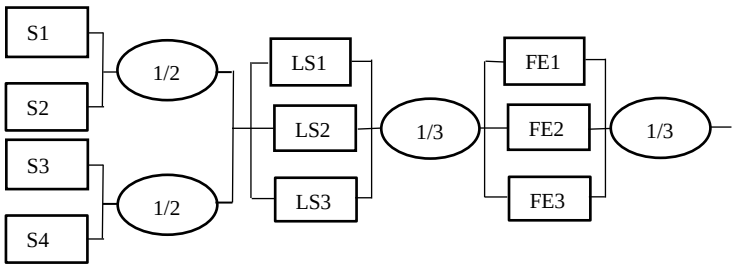


Figure 4.9 Diagramme de fiabilité du SIS

Les données de fiabilité, tableau 4.9, proviennent de (Mechri et al 2015) in (Asklou and Noureddine in press).

Sub-system Caractéristiques	pressure sensors (S1, S2)	temperature sensors (S3, S4)	Logic solvers (LS1, LS2, LS3)	Valves (FE1, FE2, FE3)
λ_D (10^{-6} /h)	1,5	1.5	1.1	2.7
DC	0,74	0,74	0,9	/0,3
β (%)	6	6	3	5
β_D (%)	3	3	1.5	2.5
$MTTR$ (h)	96	96	96	96
T (h)	4380	4380	8760	8760
ξ, C_S (%)	0.4	0.4	0.5	0.3
γ (%)	0.03	0.03	0.04	0.05
SL (h)	87600	87600	87600	87600

Tableau 4.9 Données du SIS du réacteur chimique

4.5.6 Présentation des résultats

Dans cette application on va évaluer les approches proposées CEIξ et CEIξγ respectivement développées aux section 4.5.3 et 4.5.4, en calculant la probabilité moyenne de

défaillances à la sollicitation (PFD_{avg}) du SIS et les confronter entre elles d'une part. et d'autre part de les comparer aux résultats découlant de la norme CEI 61508 (équations du tableau 3.1).

Les résultats sont synthétisés dans le tableau 4.10.

Approche	PFD_{avg}	SIL
IECξγ	3.4188×10^{-3}	2
IEC61508	2.3433×10^{-4}	3
IECξ	3.4236×10^{-3}	2

Tableau 4.10 Comparaison des résultats

4.5.7 Discussion et interprétation des résultats

- La détermination du PFD_{avg} du SIS à l'aide de l'approche proposée IECξ donne la valeur : $PFD_{avg} = 3.4236 . 10^{-3}$

  En ce qui concerne cette valeur PFD_{avg} et les valeurs normatives des niveaux d'intégrité de sécurité (SIL), ce SIS est évalué à un SIL 2.
- La détermination du PFD_{avg} du SIS à l'aide de l'approche proposée IECξγ donne la valeur : $PFD_{avg} = 3.4188 . 10^{-3}$

  En ce qui concerne cette valeur PFD_{avg} et les valeurs normatives des niveaux d'intégrité de sécurité (SIL), ce SIS est évalué à un SIL 2.
- La détermination du PFD_{avg} du SIS à l'aide de l'approche proposée CEI 61508 donne la valeur : $PFD_{avg} = 2.3433 . 10^{-4}$

  En ce qui concerne cette valeur PFD_{avg} et les valeurs normatives des niveaux d'intégrité de sécurité (SIL), ce SIS est évalué à un SIL 3.

Par rapport à la valeur PFD_{avg} obtenue par l'approche IEC 61508, les approches IECξ et IECξγ permettent une diminution du risque de l'ordre de 10.

La valeur PFD_{avg} obtenue par l'approche IECξ donne le même ordre de risque que l'approche IECξγ. Cependant l'approche IECξγ permet d'affiner la valeur calculée en tenant compte des défaillances causées par le test, ce qui pourrait également se traduire par un meilleur ratio de coût.

Il ressort de ces résultats que les approches proposées IECξ et IECξγ montrent l'influence de la précision apportée au niveau des proof test sur la valeur moyenne du PFD_{avg}

du SIS, alors que ces paramètres sont souvent négligés dans la pratique. Ces résultats confirment qu'il y a un impact sensible sur l'évaluation du niveau d'intégrité SIL.

Par conséquent, les effets des proof tests doivent être pris en compte lors du calcul quantitatif précis de la performance du système instrumenté de sécurité.

4.6 Conclusion

Les proof tests sont des moyens très importants pour vérifier si un SIS est capable d'exécuter ses fonctions de sécurité et pour détecter les défaillances qui empêchent le processus d'être sûr lorsqu'il y a une demande. Cependant, leur efficacité n'est pas totalement maîtrisée, ce qui a été démontré tout au long de ce chapitre à travers quatre études de cas.

Dans la première étude de cas, la contribution essentielle réside dans la justification du choix de la méthode du graphe des risques, adoptée pour l'évaluation du niveau d'intégrité de sécurité du SIS, qui est guidé principalement par la nature des données.

Dans les deux études de cas suivantes, on s'est intéressé aux différentes formules analytiques, qui traitent des performances des systèmes instrumentés de sécurité, découlant de la norme CEI 61508 (IEC61508 1998) et (CEI_61508 2010), de la référence (Innal 2008) et de l'organisme norvégien SINTEF (SINTEF 2013b). Après l'examen de ces différentes formules, le problème de l'imprécision dans l'évaluation du niveau d'intégrité dans les SIS est montré.

Afin de corriger ce problème, dans la dernière étude de cas, deux nouveaux modèles ont été proposé, en tenant compte de l'efficacité et de la performance des proof tests. Ces formules, désignées approches IECξ et IEC$\xi\gamma$ sont basée sur le modèle standard CEI 61508, dans lequel respectivement un paramètre (ξ) et deux paramètres (ξ et γ) ont été introduits. Le paramètre d'efficacité ξ représente la capacité du proof test à révéler les défaillances latentes et, le paramètre γ représente la sécurité du proof test.

Les modèles proposés ont été appliqué à un SIS de réacteur chimique et les résultats obtenus montrent que la modélisation proposée, utilisant l'approche IEC$\xi\gamma$, est plus précise que l'approche CEI 61508 et l'approche IECξ. En effet, l'impact de la précision apportée aux proof tests sur la valeur moyenne de PFD_{avg} du SIS peut être clairement observée en utilisant le modèle IEC$\xi\gamma$. La conséquence directe a un impact sur l'attribution du niveau d'intégrité SIL. Par rapport à la norme IEC 61508, l'approche IEC$\xi\gamma$ permet une meilleure sécurité avec un meilleur ratio de coût que l'approche IECξ.

Conclusion générale

Les systèmes instrumentés de sécurité (SIS) sont des barrières techniques qui ont pour rôle de détecter des situations dangereuses et diminuer leurs conséquences pour atteindre des niveaux de risques tolérables. La norme générique CEI 61508 et la norme CEI 61511 qui en découle, pour le secteur des process, sont les normes de référence pour la spécification et la conception de ce type de systèmes. La norme CEI 61508 utilise une approche basée sur le risque pour déterminer les exigences d'intégrité de la sécurité des systèmes. D'autre part, elle utilise un modèle global de cycle de vie qui définit les exigences nécessaires pour un SIS.

Dans la conception des SIS, il est nécessaire de fixer un niveau d'intégrité de sécurité (SIL) traduites en mesures cibles de défaillances. Ces dernières s'identifient à la probabilité moyenne de défaillance à la demande (PFD_{avg}) du SIS pour un SIS caractérisé par une faible demande, et à sa probabilité de défaillance dangereuse par heure (PFH) s'il est caractérisé par une demande élevée ou continue. La détermination du niveau d'intégrité SIL peut se faire par des méthodes qualitatives ou quantitatives. Les méthodes qualitatives permettent d'allouer le SIL à partir de la connaissance des risques associés au procédé. Les méthodes quantitatives permettent de calculer la probabilité de défaillance moyenne des SIS à partir des paramètres de fiabilité de leurs composants. Les équations simplifiées qui sont considérées parmi les méthodes les plus utilisé présente des imperfections.

La correction de ces imperfections peut passer par la correction des proof tests (tests périodiques). Les proof tests sont des moyens très importants pour vérifier si un SIS est capable d'exécuter ses fonctions de sécurité de manière sûre. Cependant, leur efficacité n'est pas totalement maîtrisée, ce qui engendre une incertitude en ce qui concerne l'efficacité du SIS.

Pour surmonter ce problème, nous avons proposées et développé deux nouveaux modèles :

- Le premier modèle désigné IECξ, est basé sur le modèle standard CEI 61508, dans lequel nous avons introduit :
  - Le paramètre d'éfficacité (ξ) qui représente la capacité du proof test à révéler les défaillances latentes.

- Le second modèle désigné IECξγ, est basé sur le modèle standard CEI 61508, dans lequel nous avons introduit deux paramètres :
  - Le paramètre d'efficacité (ξ).
  - Le paramètre γ qui représente la sécurité du proof test.

Les modèles proposés ont été appliqué à un SIS de réacteur chimique et les résultats obtenus montrent que :

- Les modèles IECξ et IECξγ permettent une diminution du risque de l'ordre de 10 par rapport à la valeur PFD_{avg} obtenue par le modèle CEI 61508.
- Le modèle IECξγ, donne meilleure précision que les modèles CEI 61508 et IECξ.
- Le modèle IECξ, donne plus de précision que le modèle CEI 61508.
- Le modèle IECξγ permet un meilleur ratio de coût que le modèle IECξ.

Ces résultats confirment l'influence de la précision apportée au niveau des proof tests sur l'attribution du niveau d'intégrité SIL du SIS, alors que ces paramètres sont souvent négligés dans la pratique. Par cette contribution, les effets des proof tests peuvent dorénavant être pris en compte lors du calcul quantitatif précis de la performance du système instrumenté de sécurité.

En perspective, d'une part il serait intéressant d'investiguer non seulement la capacité du SIS d'exécuter la fonction exigée, mais également à la capacité de fonctionner dans un état sûr lors de conditions de défaillances définies. D'autre part, d'aborder le problème d'optimisation de la conception des SIS sous contraintes définies.

Référence bibliographie

Asklou, N. and Noureddine, R., (2016a), Evaluation du niveau d'intégrité de sécurité d'un SIS, Colloque National Maintenance – Qualité (CNMQ16).

Asklou, N. and Noureddine, R., (2017b). Amélioration de l'évaluation des performances des systèmes instrumentés de sécurité par la correction des tests périodiques, 12ème Congrès International Pluridisciplinaire en Qualité, Sûreté de fonctionnement et Développement durable (QUALITA'2017), Bourges, France.

Asklou, N. and Noureddine, R., (in press), Effects of proof tests on the safety performance of safety-instrumented systems, International Journal of Industrial and Systems Engineering, Accepted 10 July 2018.ISSN online: 1748-5045.

Asklou, N. and Noureddine, R., et al., (2016b), Imprécision dans l'évaluation du niveau d'intégrité des systèmes instrumentés de sécurité, 3ème Colloque International sur le Monitoring des Systèmes industriels CIMSI2016, Fes, Maroc.

Asklou, N. Noureddine, R., (2017a), Etat de l'art et Comparaison des méthodes analytique d'évaluation des systèmes instrumente de sécurité, 3ème Conférence Internationale sur la Maintenance et la Sécurité Industrielle, CIMSI'17, Skikda, Algérie.

Benamar , M. I. (2010/2011). Etude des systèmes instruments de sécurité, mémoire de fin d'étude d'ingénieur, Filière Maintenance et Sécurité Industrielle, Université d'ORAN.

Beugin, J. (2006). Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé. 2006. Thèse de doctorat. Université de Valenciennes et du Hainaut-Cambresis.

Beugin, J., D. Renaux, et al. (2007). A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems. Reliability Engineering & System Safety **92**(12): 1686-1700.

Boulanger, J.-L. (2013). Safety of Computer Architectures, Edition John Wiley & Sons.

Bukowski, J. V. (2001). Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems. IEEE Transactions on Reliability **50**(3): 321-329.

CCPS (2007). Guidelines for safe and reliable instrumented protective systems. Editions John Wiley & Sons.

CEI_61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic

Safety-Related Systems. Part 1-7. Geneva: International Electrotechnical Commission. .

CEI_61511 (2003). Functional Safety - Safety Instrumented Systems for the Process Industry. Geneva: International Electrotechnical Commission. .

CEI_61513 (2004). Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems. Geneva: International Electrotechnical Commission. .

CEI_62061-1 (2010). Guidance on the application of ISO 13849-1 and IEC62061 in the design of safety-related control systems for machinery. Geneva: International Electrotechnical Commission. .

CENELEC–NF-EN-50126 (2000). Applications Ferroviaires. Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FMDS).

Cepin, M. (1995). Sequential versus staggered testing towards dynamic PSA. Nuclear Energy in Central Europe, 184-189.

Charpentier, P. (2002). Architecture d'automatisme en sécurité des machines: étude des conditions de conception liées aux défaillances de mode commun. Thèse pour le doctorat en automatique, INRS.

Desroches, A. (1995). Concepts et méthodes probabilistes de base de la sécurité, le management des risques des entreprises et de gestion de projet. Editions LAVOISIER.

Desroches, A. (2005). Les invariants de l'analyse préliminaire des risques, Qualita. 685-694.

EN_954-1 (1997). Safety of machinery. Safety related parts of control systems. General principles for design. European norm, CENELEC..

EU-2006/42/EC (2006). Council Directive 2006/42/EC of 17 May 2006 on machinery. Brussels: Official Journal of the European Union, L 157/24 (2006)..

Farmer, F. (1967). Siting criteria–a new approach. Containment and Siting of Nuclear Power Plants: 303-318.

Fleming, K. (1975). Reliability model for common mode failures in redundant safety systems. Modeling and simulation. Volume 6, Part 1.

Goble, W. M. and A. Brombacher (1999). Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems. Reliability Engineering & System Safety **66**(2): 145-148.

Goble, W. M. and H. Cheddie (2005). Safety instrumented systems verification:

practical probabilistic calculations, Editions ISA-The Instrumentation, Systems, and Automation Society.

Gouriveau, R. (2003). Analyse des risques: formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision. Thèse de doctorat. Toulouse, INPT

Guo, H. and X. Yang (2007). A simple reliability block diagram method for safety integrity verification. Reliability Engineering & System Safety **92**(9): 1267-1273.

Haddad, S. (2012). Evaluation et Optimisation des Performances des Systèmes Instrumentés de Sécurité pour une Meilleure Maîtrise des Risques.Thèse de doctorat. Université de Batna 2. 2012.

Houtermans, M. and J. Rouvroye. The influence of design parameters on the probability of failure on demand (PFD) performance of safety instrumented systems (SIS), 2005. Available on http://www. safetyusersgroup. com/documents/PN050005/EN/PN050005. pdf.

Iddir, O. (2009). Evaluation de la Probabilite de Defaillance D'Un Systeme Instrumente de Securite (SIS), Ed. Techniques Ingénieur.

IEC_62278 (2002). Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS). Geneva: International Electrotechnical Commission. .

IEC_62279 (2002). Railway applications - Communications, signalling, and processing systems - Software for railway control and protection systems. Geneva: International Electrotechnical Commission. .

IEC_62425 (2007). Railway applications - Communication signalling and processing systems - safety rleated electronic systems for signalling. Geneva: International Electrotechnical Commission. .

IEC61508 (1998). Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems, International Electrotechnical Commission (IEC).

Innal, F. (2008). Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances : analyse critique de la norme CEI 61508, Thèse de Doctorat, Université BORDEAUX 1.

Innal, F., Y. Dutuit, et al. (2015). Safety and operational integrity evaluation and design optimization of safety instrumented systems. Reliability Engineering & System Safety **134**: 32-50.

ISA-84.00.01–2004 (2004). Functional Safety Instrumented Systems for the Process Industries, Parts 1–3.

ISO (1999). Aspects liés à la sécurité : Principes directeurs pour les inclure dans les normes. Organisation internationale de normalisation..

ISO/CEI_Guide_73 (2002). Management du risque : Vocabulaire, Principes directeurs pour l'utilisation dans les normes. Organisation internationale de normalisation (ISO)..

ISO_12100 (2010). Safety of machinery - General principles for design - Risk assessment and risk reduction. Geneva: International Organization for Standardization. .

ISO_13849-1 (2006). Safety of Machinery - Safety-Related Parts of Control Systems - Part 1: General Principles for Design. Geneva: International Organization for Standardization.

ISO_26262 (2011). Road Vehicles - Functional Safety. Geneva: International Standardization Organization. .

Jin, H., M. A. Lundteigen, et al. (2011). Reliability performance of safety instrumented systems: A common approach for both low-and high-demand mode of operation. Reliability Engineering & System Safety **96**(3): 365-373.

Jin, J., L. Pang, et al. (2015). Quantitative assessment of probability of failing safely for the safety instrumented system using reliability block diagram method. Annals of Nuclear Energy **77**: 30-34.

Lamy, P. (2002). Probabilité de défaillance dangereuse d'un système: explications et exemple de calcul, Note scientifique et technique. Institut National de Recherche et de Sécurité (INRS).

Lamy, P., E. Levrat, et al. (2006). Méthodes d'estimation des risques machines: Analyse bibliographique. 15ème Congrès Lambda-Mu Maîtrise des risques et sureté de fonctionnement, Lille, France, Institut pour la Maitrise des Risques.

Le Moigne, J.-L. (1994). La théorie du système général: théorie de la modélisation, Editions jeanlouis le moigne.

Maslow, A. H. (2013). Toward a psychology of being, Editions Simon and Schuster.

Mazouni, M. H. (2008). Pour une meilleure approche du management des risques: de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision, Thèse de doctorat. Institut National Polytechnique de Lorraine-INPL.

Mazouni, M. H., D. B. Charreton, et al. (2007). Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport. IEEE International Conference

on System of Systems Engineering, SoSE'2007, IEEE.

Mechri, W. (2011). Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis. Thèse de doctorat. Université de Tunis El-Mana. 2011.

Mechri, W., C. Simon, et al. (2015). Prise en compte de la performance des proof tests sur celle des systèmes instrumentés de sécurité. 11ème Congrès International Pluridisciplinaire en Qualité, Sûreté de Fonctionnement et Développement Durable, QUALITA 2015.

Mkhida, A. (2008). Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence, Thèse de doctorat. Institut National Polytechnique de Lorraine-INPL.

mondiale de la Santé, O. (1998). Rapport sur la santé dans le monde 1998. La vie au 21ème siècle: une perspective pour tous, Genève.

NOG-070 (2004). Application of IEC 61508 and IEC61511 in the Norwegian Petroleum Industry. Stavanger, Norway: The Norwegian Oil and Gas Association. .

OHSAS18001 (1999). Système de management de la santé et de la sécurité au travail - Spécification -. BSI, Afnor..

PERILHON, P. (2003). MOSAR-Présentation de la méthode, Ed. Techniques de l'Ingénieur.2003.

Perilhon, P. (2004). Méthode Organisée et Systémique d'Analyse de Risques. Editions primarisk.

Rausand, M. (2011). Reliability of safety-critical systems: theory and applications, Editions John Wiley & Sons.

Rausand, M. (2014). Reliability of safety-critical systems: theory and applications, Editions John Wiley & Sons.

Rausand, M. and A. Høyland (2004). System reliability theory: models, statistical methods, and applications, Editions John Wiley & Sons.

Sallak, M. (2007). Évaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception: application aux Systèmes Instrumentés de Sécurité. Thèse de doctorat. Institut National Polytechnique de Lorraine. 2007.

Sallak, M., J.-F. Aubry, et al. (2006). Aide à la décision dans la réduction de l'incertitude des SIL: une approche floue/possibiliste. e-STA Sciences et Technologies de l'Automatique **3**: Revue électronique.

Schönbeck, M., M. Rausand, et al. (2010). Human and organisational factors in the

operational phase of safety instrumented systems: A new approach. Safety Science **48**(3): 310-318.

Signoret, J. (2004). High Integrity Protection System (HIPS)–Overcoming SIL calculation difficulties. TOTAL document, Pau.

Signoret, J. (2005). Methodology SIL evaluations related to HIPS–. Total Draft Memo, April: 27-2005.

Signoret, J. (2005). Methodology SIL evaluations related to HIPS–Total Draft Memo, April.

Signoret, J. P., Y. Dutuit, et al. (2007). High Integrity Protection Sytems (HIPPS): Methods and tools for efficient Safety Integrity Levels (SIL) analysis and calculations. In ESREL 2007 (Vol. 1, pp. 663-669).

Simon, C., M. Sallak, et al. (2007). SIL allocation of SIS by aggregation of experts' opinions. Safety and Reliability Conference, ESREL'2007, Taylor and Francis.

SINTEF (2013b). Reliability prediction methods for safety instrumented systems, PDS method handbook. Handbook STF A24442, SINTEF Safety Research, Trondheim, Norway. .

Tanzi, T. J. and P. Perrot (2009). Télécoms pour l'ingénierie du risque, Editions Hermes Science Publications.

Torres-Echeverria, A. and H. Thompson (2007). Multi-objective genetic algorithm for optimization of system safety and reliability based on IEC 61508 requirements: a practical approach. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability **221**(3): 193-205.

Torres-Echeverría, A. C., S. Martorell, et al. (2011). Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing. Reliability Engineering & System Safety **96**(5): 545-563.

Torres-Echeverria, A., S. Martorell, et al. (2009). Modelling and optimization of proof testing policies for safety instrumented systems. Reliability Engineering & System Safety **94**(4): 838-854.

Torres-Echeverria, A., S. Martorell, et al. (2011). Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing. Reliability Engineering & System Safety **96**(5): 545-563.

URL-1. Occupational Safety and Health Administration. Consulté sur https://www.osha.gov/.

URL-2. Automate de simulation. Consulté sur http://ics-safety-automation.cipen.fr/ressources-1/

Velten-Philipp, W. and M. J. Houtermans (2006). The effect of diagnostic and periodic testing on the reliability of safety systems. Conference Paper. Köln: TÜV.

Villemeur, A. (1987). Evaluation de la fiabilité, disponibilité et maintenabilité des systémes réparables: la méthode de l'Espace des Etats. EDF-DER HT/50/3-juillet.

Villemeur, A. (1988). Sureté de fonctionnement des systèmes industriels: fiabilité-facteurs humains, informatisation. Ed. Eyrolles. 1988.

Contribution à la maîtrise des Systèmes Instrumentés de Sécurité (SIS)

Résumé :

Les systèmes instrumentés de sécurité (SIS) sont des barrières techniques qui ont pour rôle de mettre un process dans une situation de sécurité fonctionnelle. L'allocation du niveau d'intégrité de sécurité (SIL), mesure cible d'évaluation, peut se faire par des méthodes qualitatives ou quantitatives. C'est cette dernière catégorie que nous avons privilégié dans cette thèse en utilisant les équations simplifiées pour déterminer la probabilité moyenne de défaillance à la demande (PFD_{avg}) du SIS. Les valeurs du PFD_{avg} présentent des imperfections qui crée une incertitude en ce qui concerne l'efficacité du SIS. Afin de corriger ce problème, dans ce travail, on a proposé deux nouveaux modèles, basés sur la norme CEI 61508, mais tenant compte de l'efficacité et de la performance des tests périodiques. Les résultats obtenus montrent que les modélisations proposées apportent une meilleure précision que le modèle standard CEI 61508.

***Mots clés** : Système instrumenté de sécurité, SIS, niveau d'intégrité de sécurité, SIL, probabilité moyenne de défaillance à la demande, PFDavg, probabilité de défaillance dangereuse par heure, PFH, proof test.*

Contribution to the mastery of Safety-Instrumented System (SIS)

Abstract:

Safety-instrumented systems (SIS) are technical barriers whose role is to put a process in a functional safety situation. The allocation of the safety integrity level (SIL), a target evaluation measure, can be done by qualitative or quantitative methods. It is the latter category that we have privileged in this thesis by using simplified equations to determine the average probability of failure on demand (PFD_{avg}) of the SIS. PFD_{avg} values present imperfections that create uncertainty about the effectiveness of the SIS. In order to correct this problem, in this work, two new models have been proposed, based on IEC 61508, but taking into account the efficiency and performance of proof tests. The results obtained show that the proposed models provide better accuracy than the standard IEC 61508 model.

***Key words**: Safety-instrumented system, SIS, safety integrity level, SIL, average probability of failure on demand, PFDavg, probability of failure per hour, PFH, proof test.*

المساهمة في التحكم في أنظمة الأمن المجهزة (SIS)

الملخص:

أنظمة الأمن المجهزة (SIS) هي حواجز تقنية يتمثل دورها في وضع عملي في حالة السلامة الوظيفية. يمكن أن يتم تخصيص مستوى سلامة الأمن (SIL)، وهو القياس المستهدف للتقييم، بطرق نوعية أو كمية .هذه الفئة الأخيرة هي التي فضلناها في هذه الأطروحة باستخدام المعادلات المبسطة لتحديد متوسط احتمال فشل الطلب (PFD_{avg}) الSIS. تحتوي قيم PFD_{avg} على عيوب تؤدي إلى عدم اليقين فيما يتعلق بفعالية ال SIS. لتصحيح هذه المشكلة ، تم اقتراح نموذجين جديدين على أساس IEC 61508 ، ولكن مع الأخذ في الاعتبار كفاءة وأداء الاختبارات الدورية .أظهرت النتائج التي تم الحصول عليها أن النماذج المقترحة تحقق دقة أفضل من النموذج القياسي IEC 61508.

مفتاحية كلمات: نظام الأمن المجهزة ، SIS، مستوى سلامة الأمن، SIL، متوسط احتمال الفشل عند الطلب، *PFDavg*، احتمال فشل خطير في الساعة، PFH، اختبار دورية .