REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'enseignement supérieur

Et de la recherche scientifique.

Université Yahia FARES Médéa.

Faculté de : science et technologie.

Département : Génie de procédure et environnement.

PROJET FIN D'ETUDE

Soumis pour obtention du diplôme en master HSI

Spécialité : Hygiène et sécurité industrielle.

THEME :

Mise en place d'un système instrumenté de sécurité pour une meilleure maitrise du risque industriel

Réalisé Par :

- **AMOURI M^ed Abdelghani**
- **CHIKER Abdessalem**

Encadré Par :

Dr : RAHMANI AHMED CHERIF

Année Scolaire: 2019 /2020

Abstract:

The security of the facilities gradually becomes the main problem of the companies and industries, because the errors are unforeseen and uncontrollable.

In order to avoid these errors and to ensure the safety of workers, facilities and continuity of production, material security appears to cover the most standards-related compliance to reduce errors and manipulate operations in an adequate way.

There must be a mentality with methods that complement the application of SIS, using a quality control method such as a control chart, using the data of the latter to improve the security of the facilities.

Equipment that depends on the proper functioning of the Safety Instrumented System (SIS), these safety-related systems based on other technologies and considered as an important means of risk reduction.

This project will demonstrate an example of the implementation of SIS for the control of hydraulic circuits.

Résumé :

La fiabilité humaine devenir de plus en plus la problématique principale des entreprises et industries, car les erreurs humaines sont imprévues et non contrôlables.

Dans le but d'éviter ces erreurs et pour assurer la sécurité des personnes, des installations et la continuité de la production, la fiabilité matérielle apparait afin de couvrir le maximum des erreurs et de manipuler les opérations d'une façon adéquate.

De plus, la fiabilité matérielle fait appelle à la sécurité fonctionnelle qui utilise les E/E/EP (Equipement électrique, électronique et électronique programmable) qui dépend du fonctionnement correct des SIS (Safety Instrumented System), ces systèmes relatifs à la sécurité basés sur d'autres technologies et des dispositifs externes de réduction de risque. Ce mémoire va démonter un exemple de l'implantation des SIS en vue de la surveillance des circuits hydraulique.

ملخص :

أصبح أمن المنشآت على مدى الوقت المشكلة الرئيسية للشركات والصناعات، لأن الحوادث غير متوقعة ولا يمكن السيطرة عليها.

لتجنب هذه الأخطاء ولضمان سلامة الأشخاص والمرافق واستمرارية الإنتاج، يبدو أن تأمين الآلات يغطي أكثر المتطلبات منها الالتزام بالمعايير للحد من الأخطاء لمعالجة العمليات وسيلة كافية للحماية.

يجب أن يكون هناك عقلية مع الأساليب التي تكمل تطبيق SIS وذلك باستخدام طريقة مراقبة الجودة مثل مخطط التحكم وذلك باستخدام بيانات هذا الأخير لتحسين أمن المنشآت.

المعدات التي تعتمد على حسن سير العمل في نظام السلامة الآلية، هذه الأنظمة المتعلقة بالسلامة تعتمد على تقنيات أخرى وتعتبر وسيلة هامة للحد من المخاطر،

ستوضح هذه المذكرة مثالا على تركيب نظام سلامة معد خصيصا لمراقبة الدوائر الهيدروليكية

Remercîment

Ce mémoire est le résultat d'un travail de recherche de près de six mois. En préambule, nous voulons adresser tous nos remerciements aux personnes avec lesquelles nous avons pu échanger et qui nous ont aidés pour la rédaction de ce mémoire.

En commençant par remercier très vivement tout d'abord Monsieur ***RAHMANI AHMED CHERIF****, « Maitre-Assistant- A à l'Univ de YAHIYA FARESS Médéa », Encadreur de ce mémoire, pour ses aides précieuses, conseils et pour le temps qu'il nous a consacré.*

Enfin, nous adressons nos plus sincères remerciements à nos familles : nos parents, nos sœurs, nos frères et tous nos proches et amis, qui nous ont accompagnés, aidés, soutenus et encouragés tout au long de la réalisation de ce mémoire.

Dédicace

Je dédie ce mémoire à :

A ma très chère mère et mon très cher père :

Affables, honorables, aimables : vous représentez pour moi le symbole de la bonté par

Excellence, la source de tendresse et l'exemple du dévouement qui n'a cessé de

M'encourager et de prier pour moi. Je vous dédie ce travail en témoignage de mon profond amour. Puisse Dieu,

le tout puissant, vous préserver et vous accorder santé, longue vie et bonheur.

A tous les membres de ma famille, petits et grands :

Veuillez trouver dans ce modeste travail l'expression de mon affection la plus sincère. Je

Vous dédie ce travail avec tous mes vœux de bonheur, de santé et de réussite.

A mon encadreur : Mr le docteur RAHMANI AHMAD CHERIF

Un remerciement particulier et sincère pour tous vos efforts fournis. Vous avez toujours

Été présents. Que ce travail soit un témoignage de ma gratitude et mon profond respect.

A mes chères amis (e) / collègues :

Je ne peux trouver les mots justes et sincères pour vous exprimer mon affection et mes

Pensées, vous êtes pour moi des frères, sœurs et des amis sur qui je peux compter. En

Témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passés ensemble, je

vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur.

POUR VOUS, mon binôme ABDELLSALEM





A. Abdelghani

Dédicace

Je dédie ce modeste travail à ***mes très chers parents*** *qui m'ont secoué et veillé le long de ma vie, qui m'ont soutenu depuis mes premières heures, jusqu'aux ultimes éclairs qu'ils trouvent dans ce travail un témoignage de grand amour et de respect, que* ***Allah*** *me les sauvegarde toujours en Bonne santé et que le paradis soit leurs logis.*

Ainsi à :

Ma sœur et mes frères que ***Allah*** *les protégé*

Toute la famille ***CHIKER.***

Tous mes amis.

A mon encadreur : Mr le docteur ***RAHMANI AHMAD CHERIF***

Merci Pour tous ceux qui m'ont appris une lettre

Et à tous ceux qui me sont chères et me portent dans leurs cœurs.

L'être qui m'a partagé ce travail, mon binôme ***Abdelghani.***

Merci ***Allah.***



C.Abdelslam



Table des matières

Remerciements.....4

Dédicaces.....5

Liste des figures.....11

Liste des tableaux.....13

Abréviations, acronymes.....14

Introduction générale.....16

1. Problématique..... 16

2. Objectifs..... 17

Chapitre 1 : La gestion des risques aux systèmes instrumentés de sécurité.

1.1 Introduction.....19

1.2 Concepts et définitions.....19

1.3 Notion de système.....20

1.4 Notion de sécurité 21

1.5 Notion de danger 21

1.6 Phénomènes dangereux et situations dangereuses.....22

1.7 Risque.....24

1.8 La gestion des risques.....26

1.18.1 Analyse des risques.....27

1.8.2 Evaluation des risques.....27

1.8.3 Réduction du risque.....28

1.9 Concept ALARP.....29

1.10 Sécurité fonctionnelle 30

1.11 Barrières de sécurité.....31

1.12 Conclusion.....33

Chapitre 2 : Les Systèmes Instrumentés De Sécurité

2.1 Introduction 35

2.2 Système E/E/EP relatifs aux applications de sécurité.....36

2.3 Normes relatives aux systèmes instrumentes de sécurité.....37

2.3.1 Norme IEC 61508 et ses normes filles **.....37**

2.3.2 La norme IEC 61511 **.....40**

2.3.3 La norme IEC 62061 **.....40**

2.3.4 La norme IEC 61513 **.....42**

2.3.5 La norme EN 50126 **.....43**

2.3.6 2.3.6 La norme ISA-84 **.....43**

2.4 Systèmes instrumentés de sécurité.....43

2.4 .1Définition d'un SIS 43

2.4.2 Constitution d'un SIS.....45

2.4.2.1 Sous-système S (Sensor)**.....45**

2.4.2.2 Sous-système LS (Logic Solver) **.....45**

2.4.2.3 Sous-système FE (Final Element) **.....45**

2.5 Fonction instrumentée de sécurité SIF.....46

2.6 Propriétés d'un SIS.....47

2.7 Redondance au sein d'un SIS.....48

2.8 Intégrité de sécurité d'un SIS.....49

2.9 Modes de fonctionnement des SIS et paramètres cibles de défaillances.....50

2.9.1 Fonctionnement en faible demande **.....50**

2.9.2 Fonctionnement en forte demande ou demande continue **.....50**

2.10 Classification des défaillances des SIS.....51

2.10.1 classifications retenues dans la norme 61508.....51

2.10.2 Classification proposée par SINTEF.....54

2.11 Définitions et classification des activations intempestives des SIS 56

2.11.1 Définitions 56

2.11.2 Classification des activations intempestives.....56

2.12 Causes des activations intempestives.....58

2.12.1 Causes des opérations intempestives.....60

2.12.2 Causes des déclenchements intempestifs 63

2.12.3 Causes des arrêts intempestifs.....63

2.13 Notion de niveau d'intégrité de sécurité (SIL).....64

2.13.1 Méthodes de détermination de SIL.....65

2.13.2 Comment choisir le SIS convenable à partir du SIL ?.....66

2.13.3 Prescriptions relatives à l'intégrité de sécurité 68

2.14 Conclusion.....70

Chapitre 3 : Les circuits hydrauliques industriels

3.1 Introduction 72

3.2 Définition 72

3.3 Les éléments de l'hydraulique 73

3.4L'introduction du SIS au circuit hydraulique 74

3.4.1 Que veut dire « proportionnel » ? 74

3.5 Rôle de l'hydraulique proportionnelle 76

3.5.1 Les principaux composants à commande proportionnelle 76

3.6 La presse hydraulique 78

3.6.1 Introduction 78

3.6.2 Présentation et fonctionnement 78

3.6.2.1 Fiche technique **.....79**

3.6.3 Exemple (la presse hydraulique SA500) **……..….....80**

3.6.3.1 le graphe de risque **…….…..…….82**

3.6.4 Application**.....86**

3.6.4.1 Recherche de l'architecture **.....87**

3.6.4.2 Application numérique **.....88**

3.6.5 vérification des résultats **……..…….....89**

3.7 Conclusion……...…….....90

Chapitre 4 : Proposition

4.1 Proposition de l'architecture du SIS 92

4.2 Concernant la presse SAM 500 93

Conclusion générale 95

Références bibliographique 96

Liste des figures

1.1 : Les attributs du mot système 20

1-2 Scénario d'accident 23

1.3 Diagramme état/transition du processus accidentel 24

1.4 Courbe de Farmer 25

1.5 : Relation entre les notions de danger et de risque 25

1.6 : Processus de gestion des risques 26

1.7 Risque tolérable et ALARP 30

1-8 Typologie des barrières techniques de sécurité 32

2.1 Structure générale de la norme IEC 61508 39

2.2 Norme CEI 61508 et normes dérivées 40

2.3 Structure générale de la norme IEC61511 41

2.4: Constitution d'un SIS 44

2.5 Schéma d'un SIS 45

2.6 Fonction instrumentée de sécurité 46

2.7 Exemple de fonction instrumentée de sécurité 47

2.8: Classification des défaillances selon leurs causes 52

2.9 : Typologie des défaillances selon la norme CEI 61508 54

2.10 : Classification des défaillances selon SINTEF 55

2.11 : les différents types des activations intempestives 57

2.12 : les décisions et les facteurs influençant les activations intempestives 59

3.1: cycle d'un circuit hydraulique 73

3.2: Exemple de la structure d'un SIS dans un circuit hydraulique 74

3.3: schématisation de la structure précédente 75

3.4: Distributeur 4/3 proportionnel 77

3.5 : limiteur de pression à action directe à commande proportionnelle 77

3.6: La presse SAM 500 **.....77**

3.7: schéma hydraulique de la presse **.....79**

3.8: Graphe de risque **.....81**

3.9: détermination du SIL d'après le graphe de risque **.....84**

3.10: L'architecture 1oo3 **.....87**

4.1: Schématisation de l'implantation du SIS **.....93**

4.2: Architecture finale **.....93**

Liste des tableaux

Table 2.1 : Les différents niveaux de SIL définis par la norme CEI 61508 **.....65**

Table 2.2: sous système de type A **.....67**

Table 2.3: sous système de type B **.....68**

Table 3.1: Descriptif des composants précédents **.....75**

Table 3.2: Les repères de la figure 4.2 **.....81**

Table 3.3 table de calibrage **.....85**

Table 3.4: Les intégrités de sécurité du graphe de risque **.....86**

Abréviations, acronymes

SIS: Safety Instrumented System.

EUC : Equipment Under Control (équipement à protéger).

SIL : Safety Integrity Level (niveau d'intégrité de sécurité.

PFD : Probability of Failure on Demand (probabilité de défaillance à la demande).

PFH : Probability of Failure per Hour (probabilité de défaillance par heure).

IEC : International Electrotechnical Comission.

CEI : Commission Electrotechnique Internationale (International Electrotechnical Commission).

SIF ; Safety Instrumented Function (fonction instrumentée de sécurité).

BPCS : Basic Process Control System.

HAZOP : Hazard and Operability study (Analyse de risque et d'exploitation)

SRS : système relatif à la sécurité

SD : situation dangereux

ANSI : American National Standards Institute.

DCC : Défaillance de Cause Commune

ISA: Instrument Society of America

KooN: K out of N (K parmi N)

MDT : Mean Down Time (durée moyenne d'indisponibilité après défaillance)

SO: Spurious Operation (Opération intempestive)

STR : Spurious Trip Rate (taux de déclenchement intempestif)

λ : Taux de défaillance aléatoire du matériel

λD : Taux de défaillance aléatoire dangereuse du matériel

λDD : Taux de défaillance aléatoire dangereuse du matériel détecté

λDU : Taux de défaillance aléatoire dangereuse du matériel non détecté

λS : Taux de défaillance aléatoire en sécurité du matériel

λSD : Taux de défaillance aléatoire en sécurité du matériel détectée,

λSU : Taux de défaillance aléatoire en sécurité du matériel non détectée

λSTD : Taux de défaillance intempestive du matériel détectée,

λSTU : Taux de défaillance intempestive du matériel non détectée,

λNONC : Taux de défaillance non critique du matériel,

λSO : Taux de défaillance d'une opération intempestive,

DC : Couverture de Diagnostic

Introduction générale

Les exigences sociétales actuelles imposent que les installations industrielles présentent les moins des risques possibles durant leur utilisation. C'est dans la phase de conception que l'on doit intégrer les éléments nécessaires à la sûreté de fonctionnement de ces installations. Deux approches permettent cette diminution du risque, la prévention en minimisant la probabilité d'apparition d'un risque, la protection en limitant les conséquences d'un dysfonctionnement.

Les moyens à mettre en œuvre pour réduire les risques sont nombreux et variés. Parmi les équipements utilisés pour réduire le risque, le système de contrôle de procédé connu sous le nom BPCS (Basic Process Controller System). Ce système est conçu pour surveiller, contrôler et maintenir le process dans un état de fonctionnement normale et sur. Cependant, la défaillance du BPCS peut être à l'origine d'un scénario d'un accident (événement initiateur).

Des systèmes d'arrêt d'urgence appelés Systèmes Instrumentés de Sécurité (SIS) interviennent dans le cas ou le process se trouve dans des conditions dangereuses de fonctionnement. Les SIS sont utilisés dans l'industrie de transformation pour réaliser une ou plusieurs fonctions instrumentées de sécurité SIF. Les normes IEC 61508 **[3]** et IEC 61511 **[4]** ont établi les prescriptions relatives à la spécification, l'exploitation et la maintenance de ces systèmes.

La réduction du risque apportée par la fonction instrumentée de sécurité est appelée réduction nécessaire du risque. Les normes IEC 61508 et IEC 61511 définissent quatre niveaux d'intégrité de sécurité (Safety integrity Level) pour une fonction de sécurité, quatre niveaux possibles de SIL. L'implémentation des SIS dans un système nécessite la détermination préalable du SIL qui devrait être atteint par la fonction instrumentée.

L'évaluation du niveau d'intégrité de sécurité est déterminée par des méthodes qualitatives et quantitatives.

Parmi les méthodes qualitatives les plus utilisées pour déterminer le niveau de SIL d'une SIF la méthode graphe de risque décrit dans le chapitre 3 de la norme IEC 61508 **[3]**. 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.

Bien que le graphe de risque est une méthode relativement facile à appliquer et permettant une évaluation rapide des SIL, il présente tout de même, des insuffisances quant à l'interprétation des termes linguistiques utilisés pour caractériser les paramètres C, F, P et W, laquelle peut différer d'un jugement à l'autre et d'un secteur industriel à l'autre en raison de la subjectivité liée à la définition qualitative des paramètres suscités. A ceci s'ajoute les déclarations fermes en termes de probabilités et taux exprimant les paramètres C, F, P, W et le SIL ; le problème de rigidité des intervalles utilisés pour la représentation quantitative des paramètres leur est imputable.

CHAPITRE 1 :

La Gestion des risques aux systèmes instrumentés de sécurité

1.1 Introduction

Généralement les systèmes industriels peuvent présenter des risques pour les personnes et l'environnement, diverses sécurités doivent être mises en œuvre. Ces types de sécurité utilisent des moyens contribuant soit à la prévention soit à la protection pour réduire les risques de dysfonctionnement. Les Systèmes Instrumentés de Sécurité (SIS) sont utilisés comme moyens de sécurité pour réaliser des Fonctions Instrumentées de Sécurité (SIF) afin de mettre le processus dans un état de repli de sécurité si le processus se trouve dans des conditions dangereuses de fonctionnement. La Commission Internationale d'Electronique (CEI), ou "International Electrotechnique Commission" (IEC), a normalisé les systèmes de sécurité ; Norme IEC 61508 en 1998 **[3]** et IEC 61511 en 2000 **[4]**. **[5].**

L'objet de ce chapitre est de donner dans un premier temps une définition de certains termes et concepts utilisés dans le cadre de la sécurité fonctionnelle des systèmes de sécurité.

1 .2 Concepts et définitions

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 plans ; humains et matériels. La fréquence de ces accidents conduit à des études de sécurité afin de mieux maîtriser les risques.

Dans les études de sécurité, l'utilisation d'une des méthodes conventionnelles est recommandée afin d'identifier les sources ou les situations dangereuses. Une analyse préliminaire des dangers (APD) permet de déterminer les risques qu'un système peut entraîner.

Elle conduit à une série de mesures d'analyse de risques mises en œuvre peut mener l'installation à un niveau de sécurité jugé acceptable par l'exploitant **[06].**

1.3 Notion du 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 » **[7].** Plusieurs définitions ont été proposées pour le mot système. Nous nous limitons cependant à celle proposée par J. L. Le Moigne **[8],** 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),
- 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).

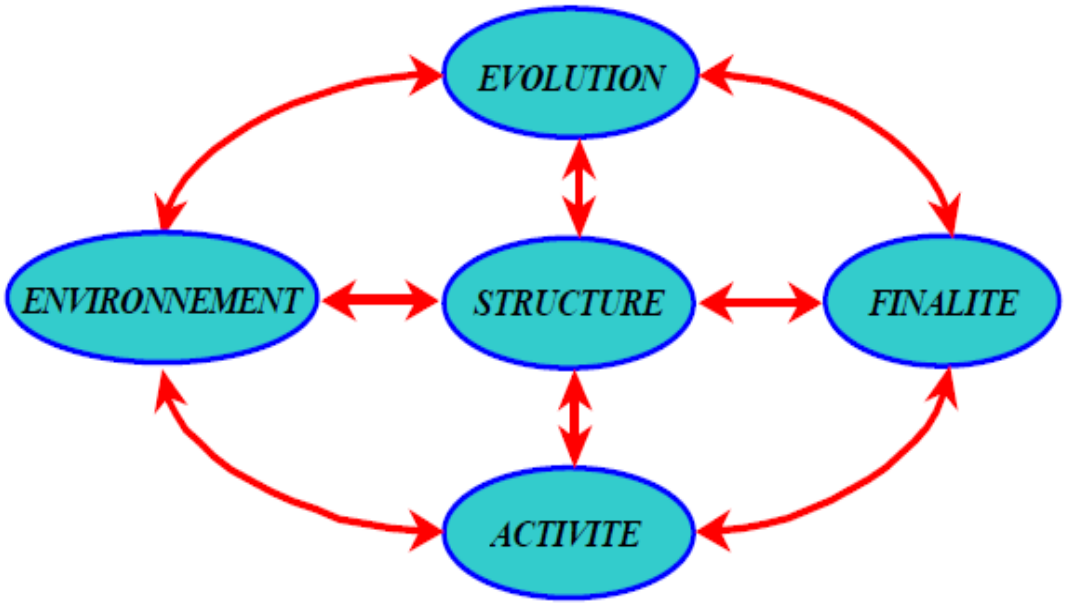


Figure 1-1 : Les Attributs du mot Système

1.4 Notion de sécurité

La sécurité est généralement définie par l'absence de phénomènes dangereux, de risque inacceptable, d'accident ou de situations catastrophiques **[9].**

Selon Villemeur **[10],** " la sécurité est l'aptitude d'une entité éviter de faire apparaitre dans des conditions données des l'évènement critiques ou catastrophiques ". D'après Desroches **[11],** la sécurité concerne la non occurrence d'événements pouvant diminuer ou porter atteinte à l'intégrité du système, pendant toute la durée de l'activité du système, que celle-ci soit réussie, dégradée ou ait échouée. 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 IEC 61508 **[3].**

1.5 Notion du danger

La norme IEC 61508 **[3**] définit le danger comme une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes.

Et selon le référentiel OHSAS 18001 **[12]**: "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 **[13]**, 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. Soulignons que de nombreux termes sont employés, selon les normes ou les auteurs, autour de la notion de danger et la rendent ambiguë. De plus, les dictionnaires associent souvent le terme danger au terme risque. En effet, plusieurs dictionnaires proposent le terme risque comme synonyme du terme danger, ce qui explique le fait qu'un grand nombre de personnes utilisent indifféremment ces termes. Même les documents et les textes officiels confondent danger et risque.

1.6 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 **[14]**, 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 **[1]**

$$\mathbf{SD = D \cap EC}$$

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

$$\mathbf{A = SD \cap EA = D \cap EC \cap EA}$$

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)**.

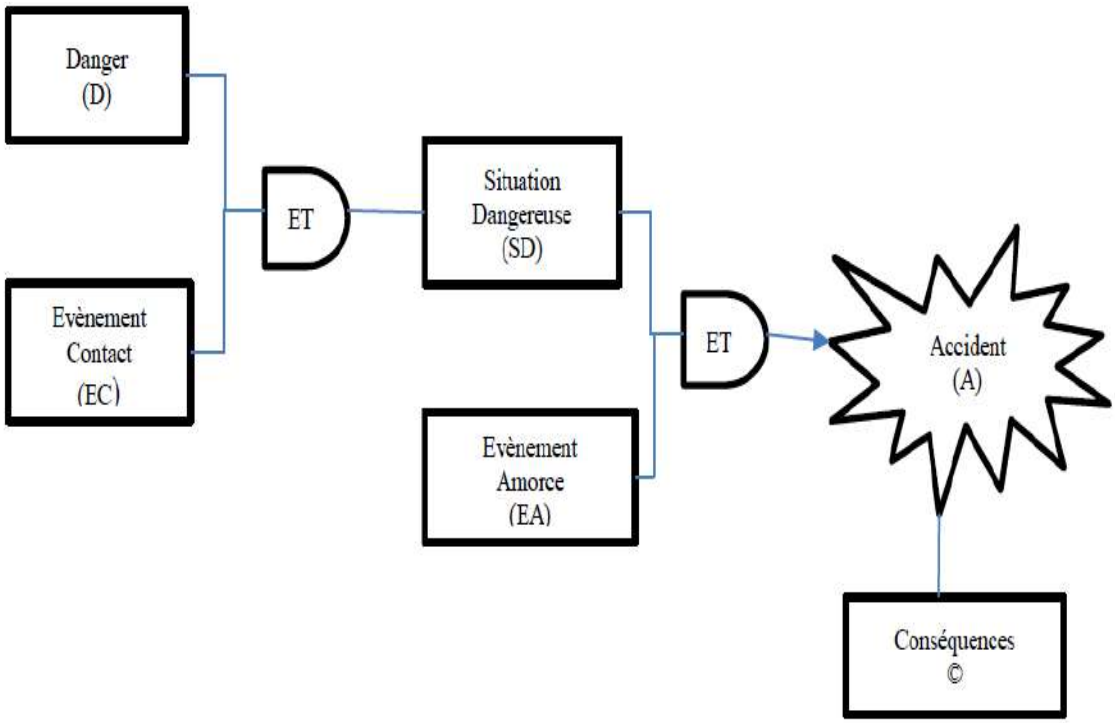


Figure 1-2 Scénario d'accident (adapté de Desroches 2005)

Selon Mazouni **[15]** 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).**

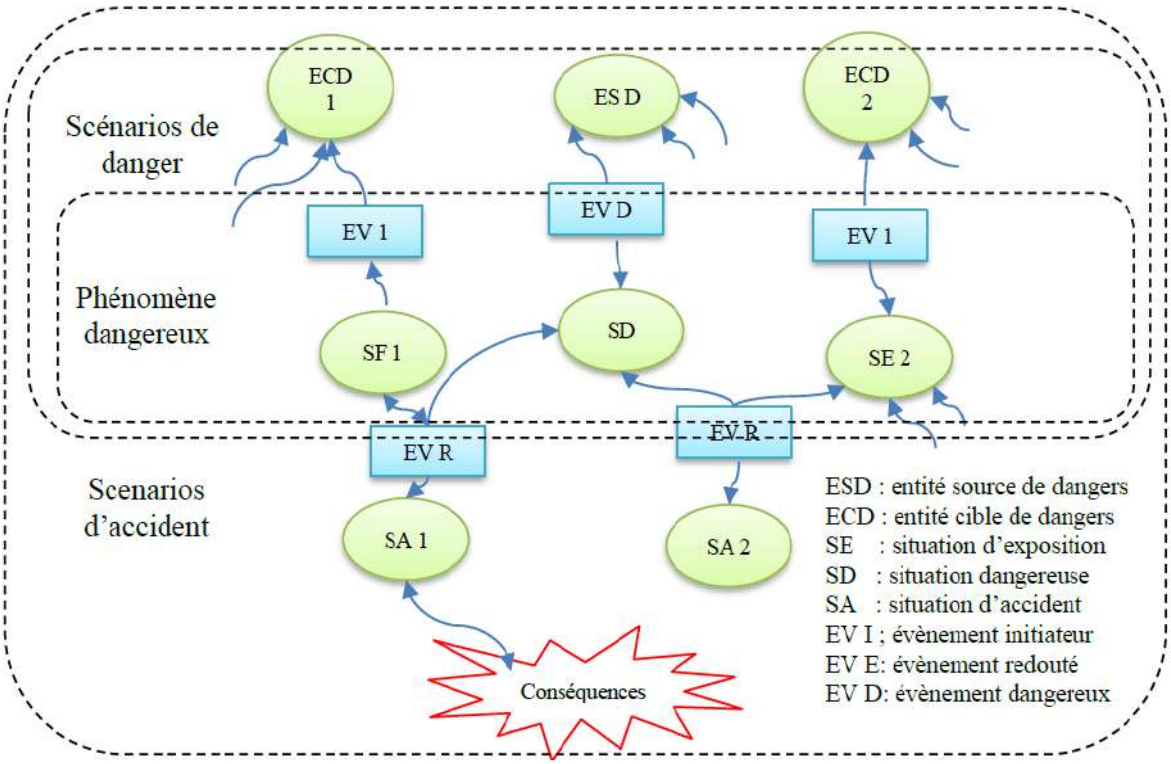


Figure 1-3 Diagramme état/transition du processus accidentel **[15]**

1.7 Risque

Le risque donne une mesure de la combinaison de deux facteurs qui sont la gravité d'un danger (ou sa conséquence) et la fréquence d'occurrence. Sa réduction peut être obtenue par la prévention (réduction de la fréquence d'occurrence) ou la protection (réduction de la gravité).

Selon **[16],** 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 **[12]**, un risque est la combinaison de la probabilité et de la (des) conséquence(s)de la survenue.

De manière plus formelle, un risque peut être mesuré par sa criticité, qui est fonction de sa probabilité et de sa gravité :

$$C = P \times G$$

Le critère de Farmer **[17]** permet de définir les notions de risque acceptable et inacceptables **(figure 1.4)**.

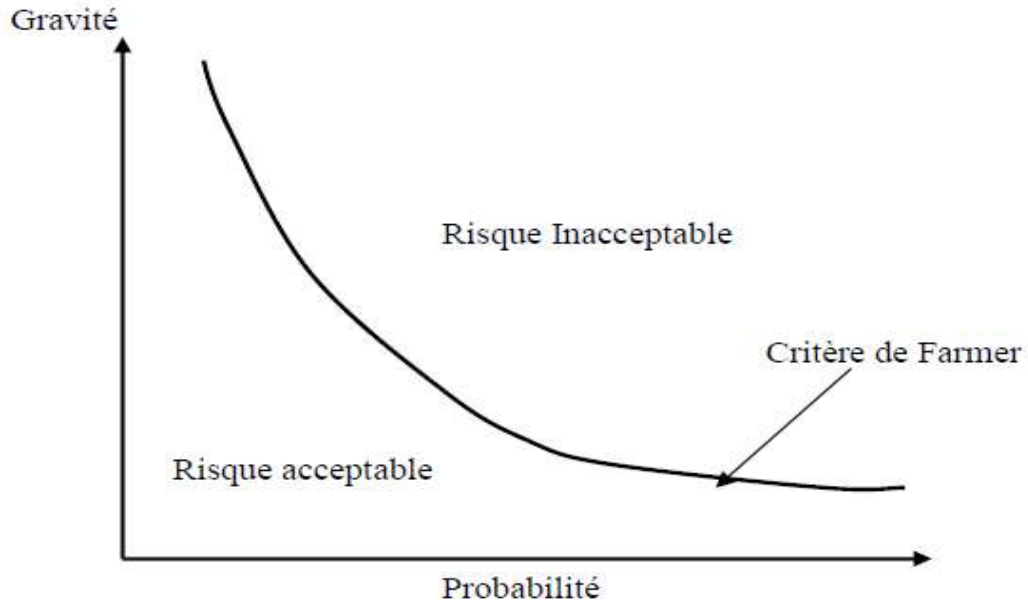


Figure 1-4 Courbe de Farmer [FAR 67]

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.

-La figure suivante permet de bien apprécier l´interaction entre les notions de danger et de risque (émergence de la notion de situation dangereuse).

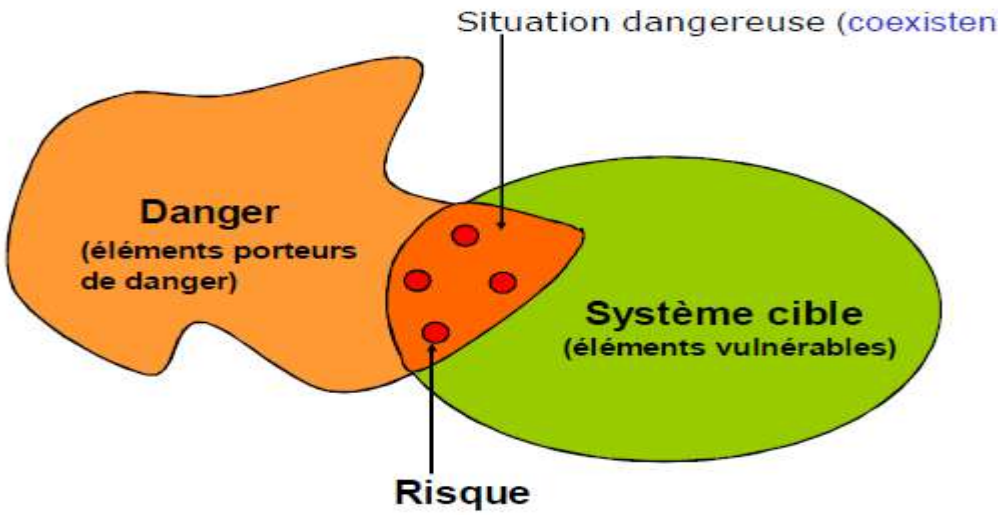


Figure 1-5 : Relation entre les notions de danger et de risque

1.8 La gestion des risques

La gestion des risques est l'un des enjeux majeurs de toute activité industrielle. Elle doit faire partie de la politique globale de l'entreprise et constitue par là l'une des composantes fondamentales de sa réussite. Aujourd'hui il incombe à tout exploitant de démontrer qu'il gère aux mieux les risques générés par son installation par la mise en place des mesures nécessaires permettant d'assurer la sécurité des personnes, des biens et de l'environnement. La gestion des risques peut être définie comme l'ensemble des activités coordonnées en vue de réduire le risque à un niveau jugé tolérable ou acceptable. Cette gestion constitue un processus itératif qui englobe de différentes phases dont l'enchaînement est décrit à la (**figure 1.6) [18].**

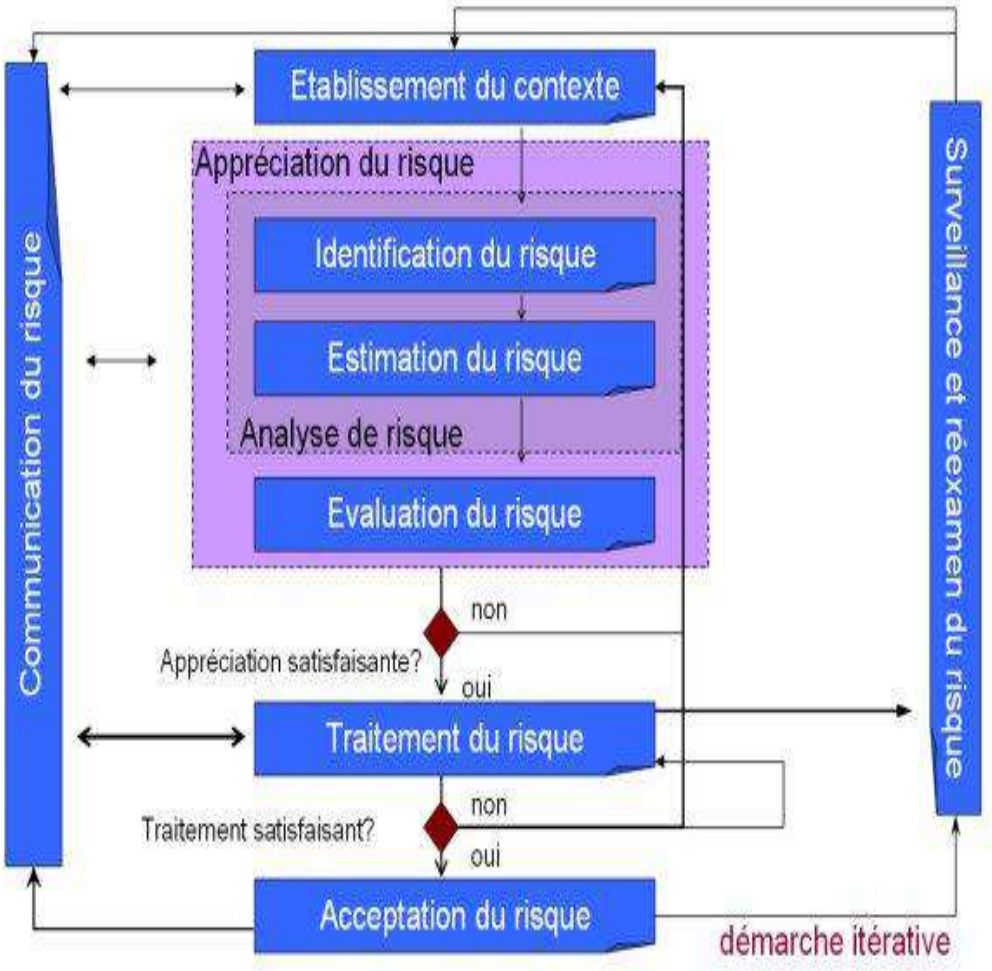


Figure 1-6 : Processus de gestion des risques

Ces différentes phases sont brièvement explicitées comme suit.

1.8.1 Analyse des risques

L'analyse des risques est définie dans le Guide ISO/CEI 51 **[19]** comme : « l'utilisation des informations disponibles pour identifier les phénomènes dangereux et estimer le risque ». Cette phase se compose des points suivants :

1/La première étape d'une démarche de gestion des risques consiste en l'identification, le plus exhaustivement possible, de l'ensemble des sources de dangers et des scénarios associés qui peuvent entraîner des dommages. Ceci est possible une fois que le système à étudié est identifié et le domaine de l'étude (surtout en termes d'objectif de sécurité) est déterminé sans ambiguïté.

2/Consécutivement à cette identification, l'estimation de chaque scénario d'accident doit considérer les deux composantes du risque :

- la probabilité (ou fréquence) d'occurrence.
- Les conséquences potentielles associées.

Cette estimation peut être réalisée à l'aide de méthodes telles que : APR, HAZOP, AMDEC, AdD, …) ; prises individuellement ou combinées. Notons également que cette phase, comme les autres phases, est conduite par un groupe de travail multidisciplinaire dont l'expertise conditionne considérablement la qualité et l'efficacité de la démarche de gestion des risques.

1.8.2 Evaluation des risques

Cette phase permet de situer le travail d'analyse par rapport aux objectifs fixés. Elle revient à comparer le niveau de risque estimé à celui jugé acceptable ou tolérable. L'acceptation du risque et une étape de négociation entre les différents partenaires impliqués dans la démarche de gestion des risques. Bien évidemment, les critères d'acceptabilité du risque doivent résulter d'un consensus entre ces partenaires.

1.8.3 Réduction du risque

La réduction du risque doit être considérée dès lors que le risque considéré est jugé inacceptable. Il s'agit d'identifier les barrières nécessaires pour ramener le niveau de risque des différents scénarios d'accidents, en agissant le plus en amont possible de leur développement (principe d'élimination à la source), à un niveau acceptable. Comme nous l'avons précisé, rappelons-le, le risque est une combinaison de la probabilité d'un événement dangereux et de sa gravité. Ceci étant, la réduction du risque peut être obtenue de deux manières différentes **(figure 1.4)** :

- **La protection :** elle regroupe les mesures prises pour limiter les conséquences de la survenue d'un accident en diminuant ainsi sa gravité. Par exemple : une cuvette de rétention assurant le non épandage d'un liquide, un système d'extinction automatique permettant de réduire les effets d'un incendie, les plans de secours et les procédures d'urgence pouvant réduire largement les dommages susceptibles d'être occasionnés, etc.

-La prévention : elle a pour but la réduction de sa probabilité (ou fréquence) d'occurrence. La prévention désigne donc les mesures préalables mises en place pour empêcher la survenue d'un accident. Cela peut être assuré par une conception sûre de l'installation ou par l'ajout de systèmes assurant la sécurité de l'installation en cas de dérive. Ainsi, pour protéger une installation contre les surpressions, les mesures de prévention peuvent consister en une soupape de sécurité, un disque de rupture ou encore en un système automatique d'arrêt d'urgence (SIS).

L'aptitude de réduction du risque des barrières proposées, ou même existantes, doit être évaluée et maintenu dans le temps, d'où l'intérêt de la CEI 61508 et ses normes filles dans le cadre des barrières basées sur une technologie instrumentée.

Par ailleurs, les risques assumés, résiduels, doivent être contrôlés et gérés notamment par :

- La sensibilisation et la communication sur ces risques. A ce titre, les exploitants sont tenus pour responsables et sont suspectés s'ils n'ont pas communiqué de manière suffisamment transparente sur les risques qui dépendent de leur autorité.

- Le maintien et le contrôle des mesures de réduction mises en place.

- La gestion financière et assurances.

Il convient de noter qu'il existe plusieurs cadres génériques définissant la structure générale d'un système de management des risques ou de sécurité. Nous citons, à titre d'exemple : OHSAS 18001 **[12],** ILO-OSH 2001 (développé par le Bureau International du Travail (BIT)) **[20]** et l'ISO 31000.

1.9 Concept ALARP

Le principe ALARP **[1] (**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] **[21]** 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.

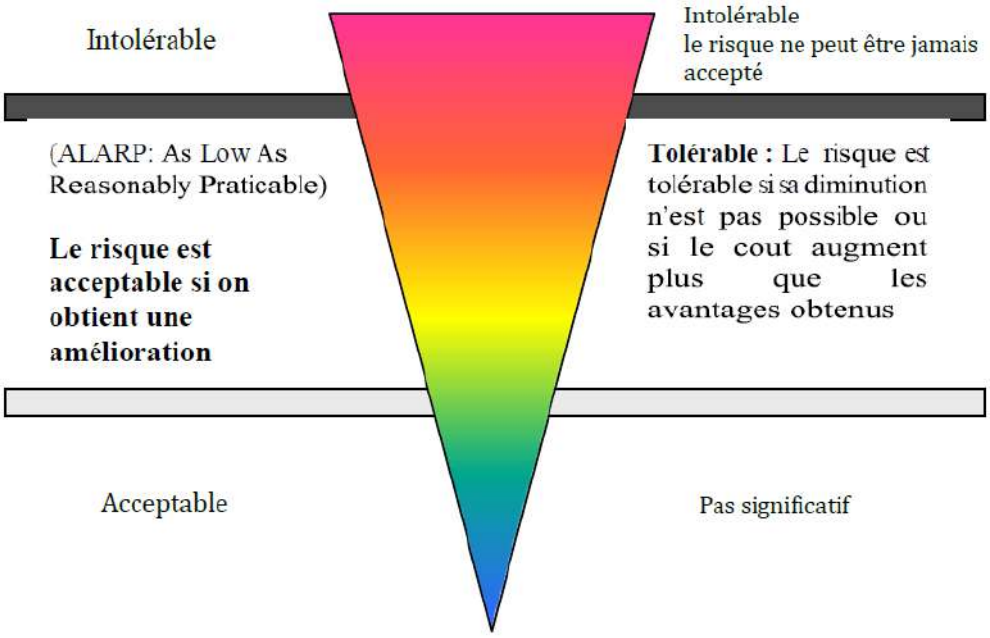


Figure 1-7 : Risque tolérable et ALARP [1]

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) **[21]**

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.

1.10 Sécurité fonctionnelle

La sécurité fonctionnelle a pour objet de contrôler les risques inacceptables qui pourraient provoquer des accidents dangereux. Elle couvre les systèmes mettant en œuvre des solutions de protection appliquées dans plusieurs domaines : mécanique, électrique, électronique,électronique

programmable, hydraulique, optique, **[5]** Selon la norme IEC 61508 **[3],** 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.

Selon la norme IEC 61511 **[4],** la sécurité fonctionnelle est un sous-ensemble de la sécurité globale qui se rapporte à un système de commande de processus de base (BPCS, Base Process Control System) et qui dépend du fonctionnement correct du système instrumenté de sécurité et d'autres couches de protection **[6]**.

1.11 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.

1.11.1 : Classification des barrières de sécurité techniques ou humaine

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

1-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).

2- 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)**.

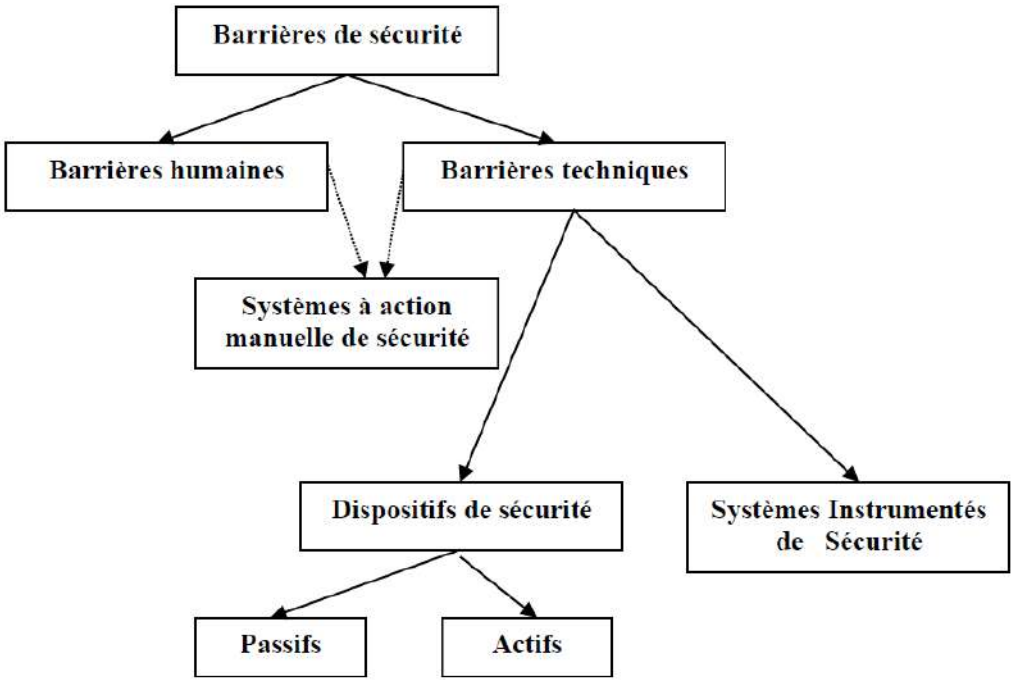


Figure 1-8 : Typologie des barrières techniques de sécurité

-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.

1.12 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 et l'identification / évaluation des risques inhérents au processus, ainsi 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 thème.

Chapitre 2 : Le Système Instrumenté de Sécurité

2.1 INTRODUCTION

Diverses sécurités sont mises en œuvre lorsque les systèmes automatisés présentent des risques pour l'homme, l'environnement ou les biens. Ces types de sécurités utilisent des moyens contribuant soit à la prévention soit à la protection pour limiter les conséquences d'un dysfonctionnement. Les systèmes instrumentés de sécurité (SIS) sont souvent utilisés comme moyens de protection pour réaliser des fonctions instrumentées de sécurité (SIF). Pour concevoir ces systèmes, deux normes sont utilisées : l'ANSI/ISA S84.01-1996 **[22]** et la CEI 61511 **[4]** qui est une déclinaison de la norme générique CEI 61508 **[1].**

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.

La première partie de ce chapitre porte sur la norme CEI 61508 qui est une norme générique et couvre plusieurs aspects tels que le cycle de vie, l'allocation de l'intégrité de sécurité en fonction d'un objectif, le choix de l'architecture matérielle ...

Pour être plus facilement mise en œuvre, des normes filles sectorielles ont été imaginées : c'est le cas notamment de la norme CEI 61511, spécialement pensée pour mettre en œuvre les systèmes instrumentés de sécurité, ou de la norme CEI 62061 qui est dédiée au secteur machine.

Les normes ANSI/ISA S84.01-1996 **[22]** et CEI 61511 **[4]** établissent les prescriptions relatives à la spécification, la conception, l'installation, l'exploitation et la maintenance du SIS, afin d'avoir toute confiance dans sa capacité à amener le procédé dans un état sûr. Les étapes de base pour se conformer à ces normes sont :

-Etablir une cible de sécurité (risque acceptable) du procédé et évaluer le risque existant.

-Identifier les fonctions de sécurité requises et les affecter aux niveaux de protection.

-Déterminer si la fonction instrumentée de sécurité est requise.

-Implémenter la fonction instrumentée de sécurité dans un SIS et déterminer le SIL du SIS.

-Vérifier que le SIS permet d'atteindre la cible de sécurité exigée au départ. Toute la difficulté est d'estimer le risque que présente le procédé et d'évaluer la diminution du risque que doit apporter le système instrumenté de sécurité. La norme formalise une démarche :

①d'analyse de risque qui identifie ce qui doit être fait pour éviter les événements dangereux associés au procédé.

② D'évaluation de risque permettant l'obtention de l'intégrité de la sécurité exigée du système pour que le risque devienne acceptable.

Cette intégrité de sécurité se matérialise par des niveaux SIL (Safety Integrity Level). Ces niveaux SILs sont d'autant plus importants lorsque la réduction du risque est importante et ils doivent concerner la boucle complète du SIS. Donner un niveau de SIL pour un instrument n'a en soi pas de sens.

2.2 Système E/E/EP relatifs aux applications de sécurité

Les systèmes de sécurité sont définis en termes d'absence de risque inacceptable de blessure ou de préjudice à la santé des personnes. Les dommages aux personnes peuvent être directs ou indirects, comme des dommages aux biens ou à l'environnement par exemple. **[23].**

Certains systèmes peuvent être principalement conçus pour se prémunir contre des pannes ayant des implications économiques majeures. Ceci signifie que dans l'esprit, à objectifs techniques comparables ou identiques, il n'y a pas de différence entre un système de sécurité et un système de contrôle.

Un système E/E/EP (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité, c'est-à-dire, depuis le capteur, en passant par l'unité logique de traitement, jusqu'à l'élément final (la partie actionneur), tout en tenant compte des actions de l'opérateur du système.

La norme IEC 61508 **[3]** peut être utilisée pour développer n'importe quel système E/E/EP comportant des fonctions critiques, telles que la protection des équipements, des biens ou de l'environnement.

2.3 Normes relatives aux systèmes instrumentes de sécurité

La norme internationale de sécurité IEC 61508 est une des dernières normes dédiées à la sécurité fonctionnelle. Elle est devenue avec ses normes filles les plus récentes et les plus connues des acteurs de la sécurité dans les secteurs industriels.

2.3.1 Norme IEC 61508 et ses normes filles

En 1984, le comité technique 65 de la CEI a commencé une tâche de définition d'une nouvelle norme internationale relative à la sécurité. Cette norme CEI 61508 **[1]** est la seule norme multisectorielle traitant de l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP ; relies à la sécurité elle traite à la fois le matériel et le logiciel. C'est également la seule norme très technique qui apporte des clés, auxquelles il suffit de se conformer pour atteindre un objectif. Cette norme est orientée performances en laissant à l'utilisateur le soin de réaliser son analyse de risque et elle lui propose des moyens pour réduire ce risque. Elle ne concerne pas les systèmes simples, pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Par exemple, un système comportant des fins de course et des relais électromécaniques reliés à un disjoncteur peut être étudié sans avoir

Recours à la CEI 61508. La norme CEI 61508 repose sur deux concepts qui sont fondamentaux vis-à-vis de son application : le cycle de vie en sécurité et les niveaux d’intégrité de sécurité.

Cette norme s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs électriques/électroniques/électroniques programmables. Elle comprend 7 parties **(figure 2.1),** afin de couvrir les multiples aspects des systèmes E/E/PE :

-61508 -1 : Prescriptions générales.

-61508 -2 : Prescriptions propres aux systèmes E/E/PE.

-61508 -3 : Prescriptions relatives au logiciel.

-61508 -4 : Définitions et abréviations.

-61508 -5 : Exemples de méthodes pour déterminer le niveau d'intégrité de la sécurité.

-61508 -6 : Guides pour l'application des parties 2 et 3 de la norme.

-61508 -7 : Tour d'horizon des techniques et des mesures.

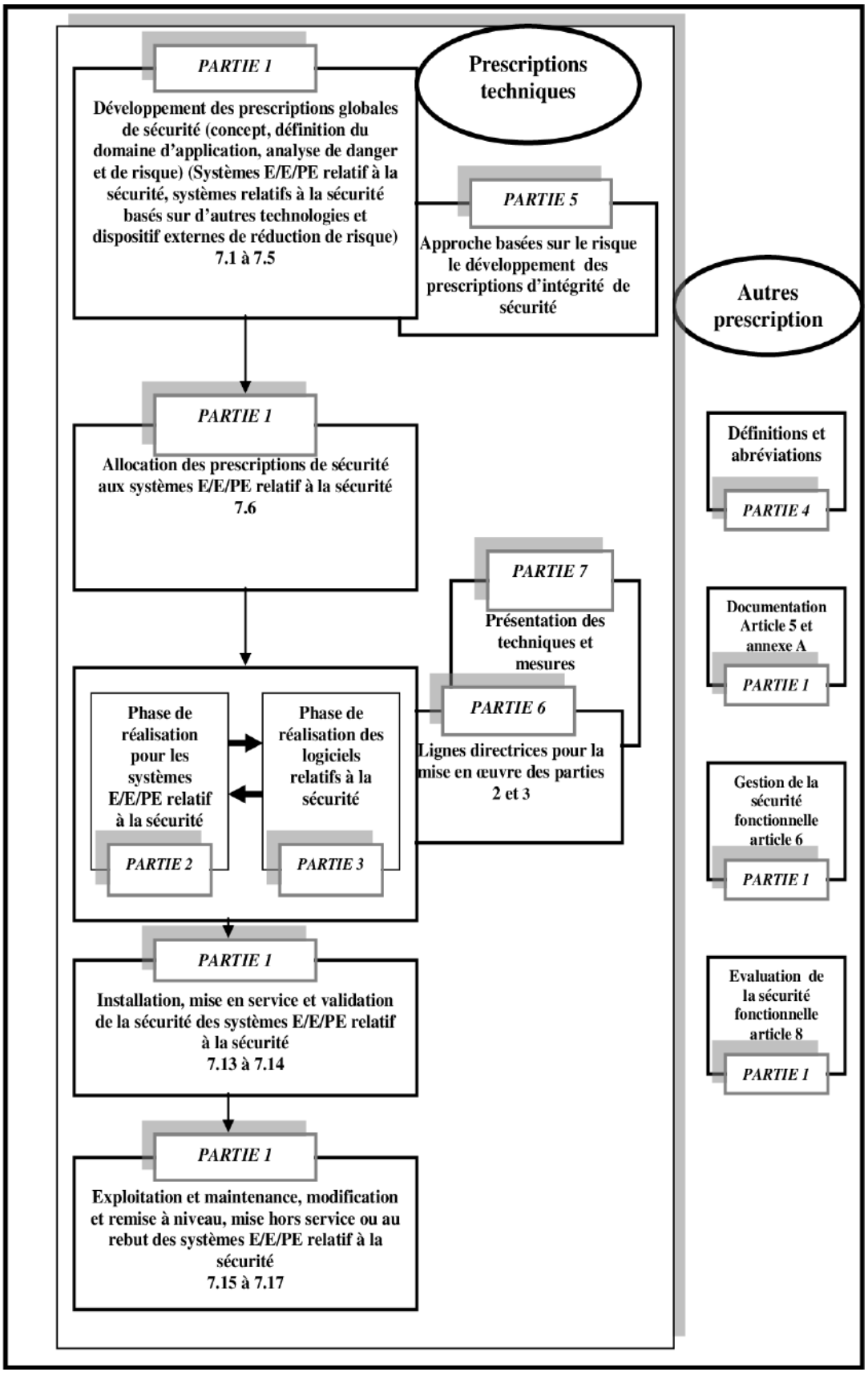


Figure 2-1 : Structure générale de la norme IEC 61508 [1]

La norme CEI 61508 est la base d'autres normes sectorielles (ex : machines, procédés continus, ferroviaire, nucléaire) ou de produits (ex : variateurs de vitesse). Elle influence donc le développement des systèmes E/E/PE et des produits concernés par la sécurité à travers tous les secteurs. La figure **(figure2.2) [24**] montre la norme CEI 61508 générique et ses normes filles par secteur d'activité.

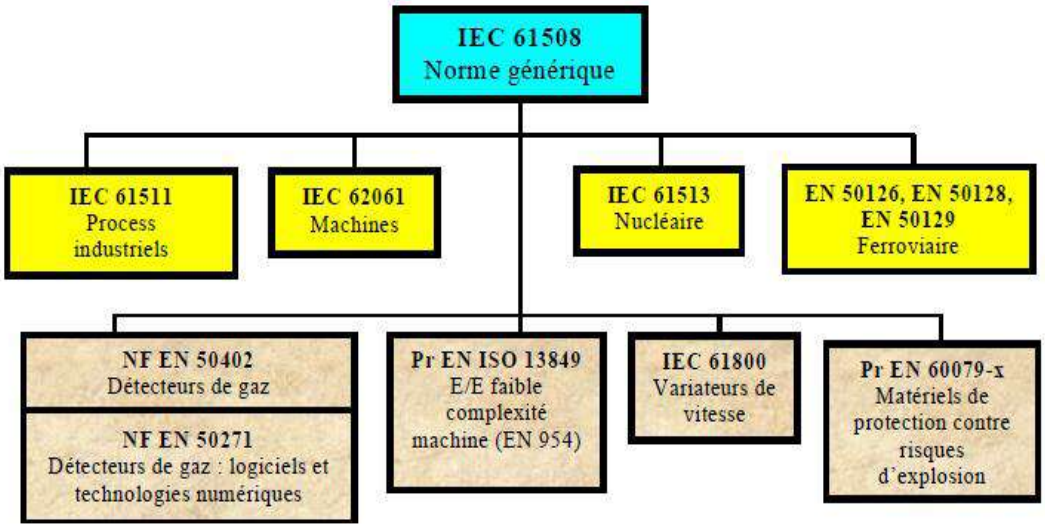


Figure 2-2 : Norme CEI 61508 et normes dérivées [24]

2.3.2 La norme IEC 61511

La norme sectorielle CEI 61511 concerne les systèmes instrumentés de sécurité pour le secteur les processus industriels. Cette norme présente une approche relative aux activités liées au cycle de vie de sécurité, pour satisfaire à ces normes minimales. Cette approche a été adoptée afin de développer une politique technique rationnelle et cohérente. Dans la plupart des cas, la meilleure sécurité est obtenue par une conception de processus de sécurité intrinsèques, chaque fois que cela est possible, combinée, au besoin, avec d'autres systèmes de protection, fondés sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable) et qui couvrent tous les risques résiduels identifiés. Elle comprend trois parties :

1. Cadre, définitions, exigences pour le système, le matériel et le logiciel,

2. Lignes directrices pour l'application de la CEI 61511-1,

3. Conseils pour la détermination des niveaux exigés d'intégrité de sécurité.

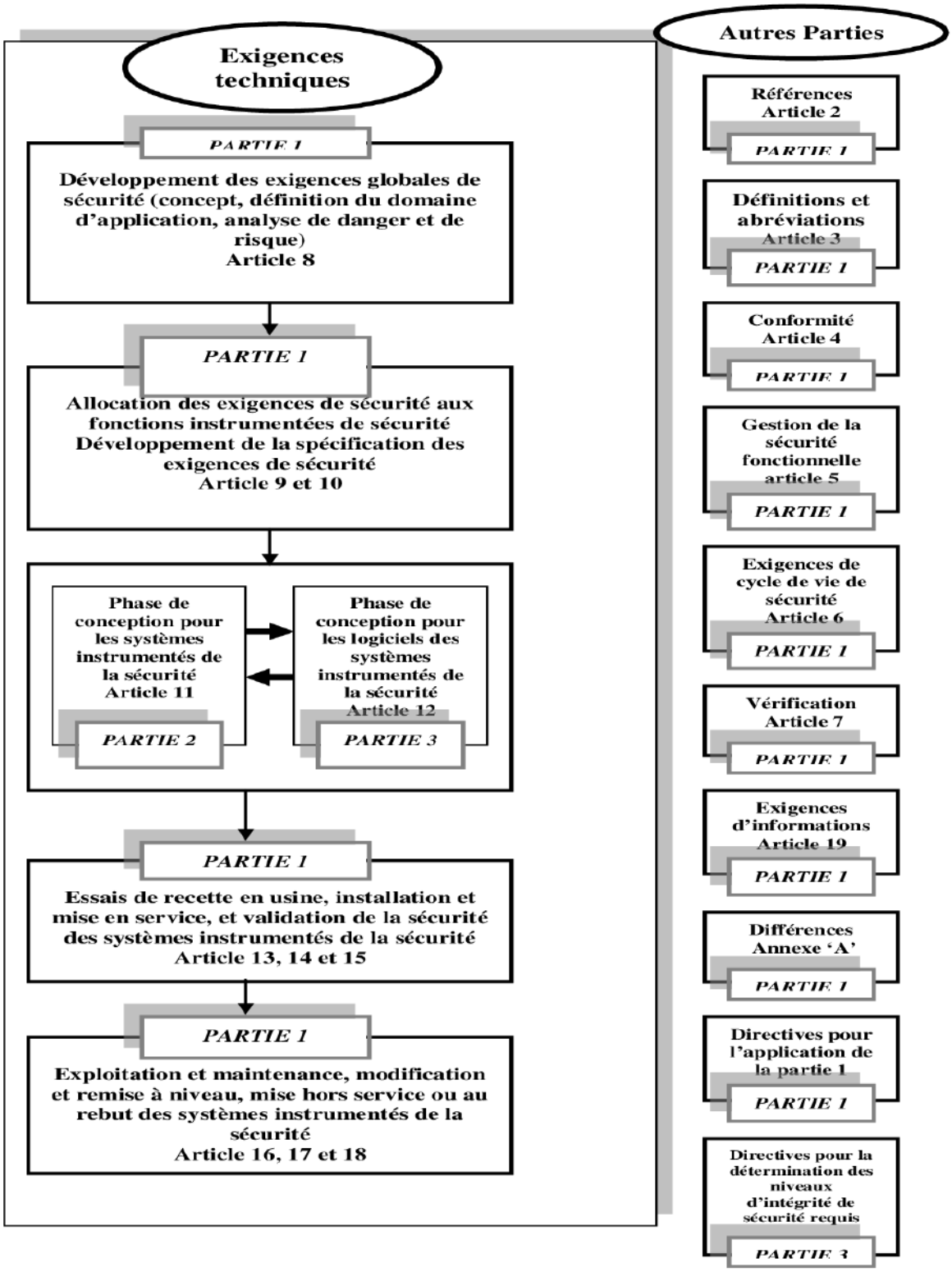


Figure 2-3 : Structure générale de la norme IEC61511 [4]

Cette norme permet de définir des exigences relatives aux spécifications, à la conception, à l'installation, à l'exploitation et à l'entretien d'un SIS, afin d'avoir toute confiance dans sa capacité à amener le procédé dans un état de sécurité.

La norme CEI 61511 restreint le périmètre aux systèmes pour des applications SIL 1 à 3 (les applications SIL 4 ne pouvant être traitées par un SIS seul). Les applications qui nécessitent l'utilisation d'une fonction instrumentée de sécurité de niveau d'intégrité de sécurité SIL 4 sont rares dans l'industrie de processus. Ces applications doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité **[4].**

2.3.3 La norme IEC 62061

L'IEC 62061 repose sur les mêmes concepts que ceux de l'IEC 61508 **[3]**. Elle est destinée à être utilisée par les concepteurs de machines et les fabricants de systèmes de commande électroniques relatifs à la sécurité de machines **[1].**

Elle concerne la spécification des prescriptions et fait des recommandations pour la conception, l'intégration et la validation de ces systèmes **[25].**

2.3.4 La norme IEC 61513

L'IEC 61513 concerne le secteur de la sûreté des centrales nucléaires. Elle présente les prescriptions relatives aux systèmes de contrôle commande utilisés pour accomplir les fonctions de sécurité des centrales nucléaires. La conception des systèmes de contrôle commande peuvent être réalisés à l'aide d'une combinaison de composants traditionnels câblés à des composants informatiques. La conformité à l'IEC 61513 facilite la compatibilité avec les exigences de l'IEC 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire.

2.3.5 La norme EN 50126

La norme EN 50126 **[26]** s'intéresse essentiellement aux applications ferroviaires. Elle permet de spécifier les principaux concepts de la sûreté de fonctionnement des systèmes tels que : la fiabilité, la disponibilité et la sécurité, . . . Cette norme est constituée de deux normes filles. L'EN 50128 **[27]** est destinée à la partie logicielle des systèmes de protection ferroviaire. L'EN 50129 **[28]** concerne les systèmes électroniques de sécurité pour la signalisation **[25].**

2.3.6 La norme ISA-84

La norme ISA-84 était acceptée par l'institut national américain des normes (American National Standards Institute, ANSI) en mars 1997. Elle spécifie les exigences pour la conception, l'installation, l'utilisation et la maintenance des systèmes instrumentés de sécurité **[29].**

La norme ISA-84 dispose uniquement de trois niveaux d'intégrité de sécurité, SIL1 à SIL3. C'est une norme nationale et incomplète par rapport à la norme CEI 61511 qui est une harmonisation de normes de plusieurs pays.

En 2004, le comité d'ISA SP84 a voté pour adopter le CEI 61511 comme nouvelle version d'ISA-84 (ANSI/ISA S84.00.01- 2004) **[30].** Il y a, cependant, une différence significative entre la norme ISA-84 et la norme CEI 61511. ISA-84 a ajouté une clause première génération dans la nouvelle (2004) version qui permet l'utilisation continue des systèmes instrumentés de sécurité qui suivent la version originale de la norme **[22**]. ISA est en cours de développement de directives et exemples d'implémentation basés sur le standard. Ceux-ci seront édités en tant que rapports techniques **[31].**

2.4 Systèmes instrumentés de sécurité

2.4.1 Définition d'un SIS

La norme CEI 61511 **[4]** 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 **[3]** 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 donc utilisés comme moyens de prévention et comportent une proportion grandissante de systèmes électriques, électroniques ou encore électroniques programmables (E/E/EP). Ces systèmes sont complexes ce qui rend difficile dans la pratique la connaissance de chaque mode de défaillance par l'examen des comportements possibles et la prévision des performances en terme de sécurité. 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…) **[25].**

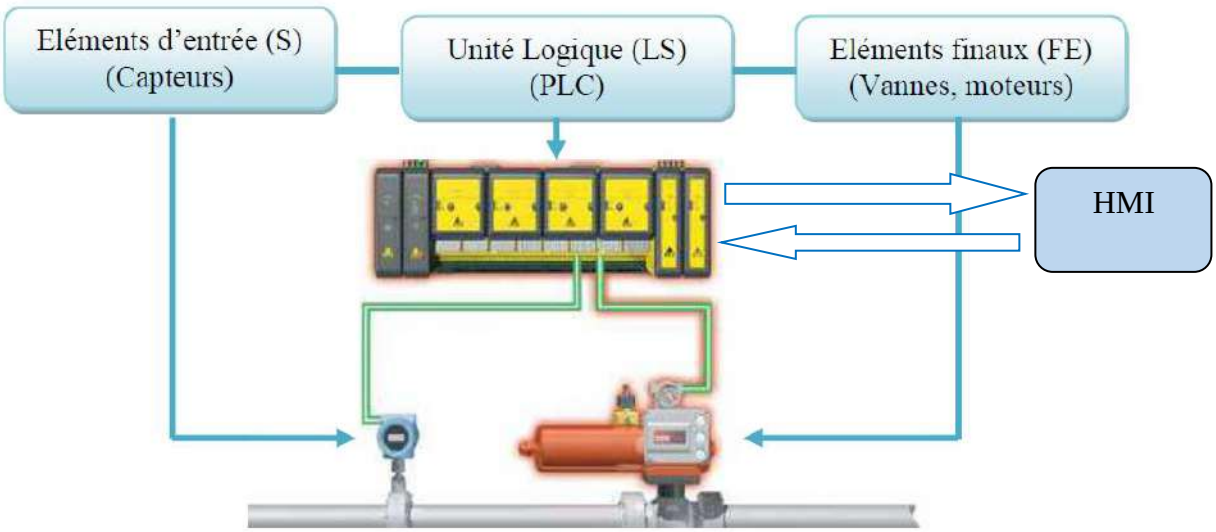


Figure 2.4 Exemple d'un SIS

2.4.2 Constitution d'un SIS

Les SIS sont constitués de différents éléments unitaires reliés entre eux par des moyens de transmissions. Au minimum, on retrouve en série un capteur, une unité de traitement et un actionneur.

•***2.4.2.1 Sous-système S (Sensor) :*** il est constitué d'un ensemble d'éléments d'entrée (capteurs, détecteurs) qui surveillent l'évolution des paramètres physico-chimiques représentatifs du comportement du procédé (température, pression, débit, niveau…). Si au moins un de ces paramètres dévie au-delà d'une valeur de consigne et s'y maintient, cette déviation constitue ce qui a été appelé demande ou sollicitation émanant du procédé, de l'EUC. Elle est détectée par les capteurs concernés qui envoient un signal au sous-système LS.

•**2.4.2.2 *Sous-système LS (Logic Solver)* :** ce sous-ensemble d'éléments logiques réalise le processus de prise de décision qui s'achève par l'activation du troisième sous-système FE. Le sous-système LS peut être un automate programmable ou un microordinateur doté de logiciels spécifiques.

•**2.4.2.3 *Sous-système FE (Final Element) :*** ces éléments agissent directement (vannes d'arrêt d'urgence) ou indirectement (vannes solénoïdes) sur le procédé pour neutraliser sa dérive en mettant, en général, le système à l'arrêt (état sûr) au terme d'un délai qui doit être spécifié pour chaque fonction de sécurité **[1]**.

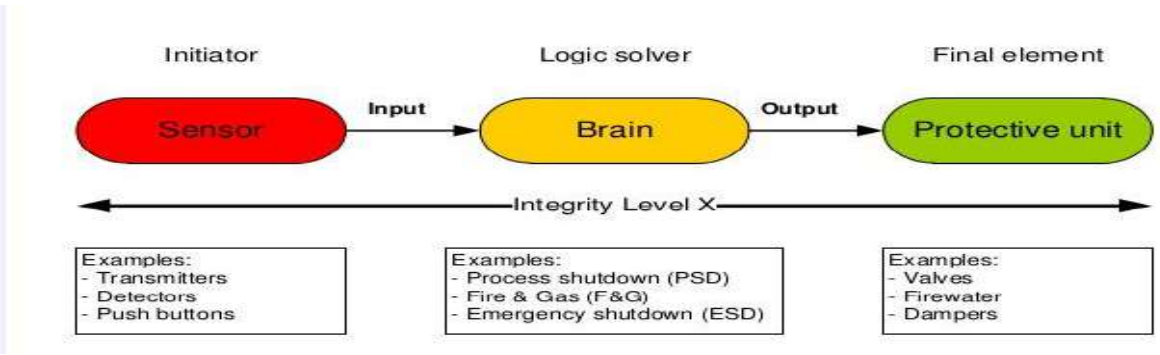


Figure 2-5 : Constitution d'un SIS

2. 5 Fonction instrumentée de sécurité SIF

Les principales étapes de la norme IEC 61508 **[3]** 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 de sécurité instrumentées 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 **[6], [32].**

Une fonction instrumentée de sécurité est spécifiée pour s'assurer que les risques sont maintenus à un niveau acceptable par rapport à un événement dangereux spécifique.

Une fonction instrumentée de sécurité est à réaliser par un système instrumenté de sécurité (ou par une combinaison des composantes de ce système), par un système relatif à la sécurité basé sur une autre technologie ou par un dispositif externe de réduction de risque. **[6].**

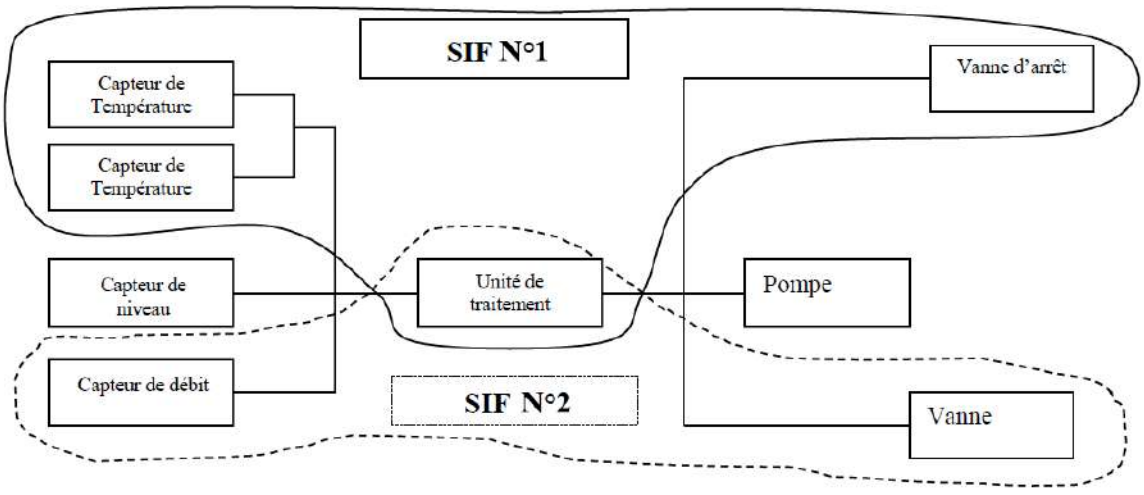


Figure 2-6 : Fonction instrumentée de sécurité [6]

Pour illustrer et rendre plus claire cette définition, nous proposons l'exemple d'un équipement utilisé dans la fonction instrumentée de sécurité **(Figure 2.7).**

Cette dernière est conçue pour protéger un réservoir sous pression contenant un liquide inflammable lorsqu'une haute pression a lieu à l'intérieur du réservoir, cette fonction de sécurité agira selon deux procédures :

• Fermeture de la vanne pour arrêter l'alimentation du liquide.

• Arrêt de la pompe qui injecte le liquide dans le réservoir.

Il est indispensable de lister tous les composants intervenant à la réalisation de cette fonction instrumentée de sécurité, ces composants sont : Transmetteur de pression, solver, vanne, pompe.

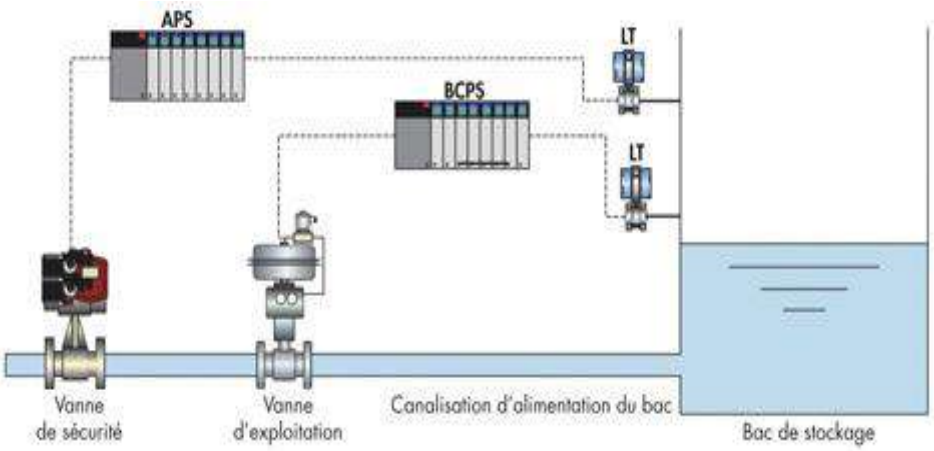


Figure 2-7 : Exemple de fonction instrumentée de sécurité

2.6 Propriétés d'un SIS

Un certain nombre de propriétés caractérisent les systèmes instrumentés de sécurité :

• Les systèmes instrumentés de sécurité nécessitent une source d'énergie extérieure pour remplir leur fonction de sécurité.

• On retrouve tout ou partie de ces différents éléments pour constituer des chaînes de sécurité.

• Plusieurs capteurs ou actionneurs peuvent être reliés à une même unité de traitement.

• Toutes les combinaisons de capteurs, d'unité de traitement et d'actionneurs qui sont exigées pour accomplir des fonctions de sécurité sont considérées comme une partie de systèmes instrumentés de sécurité.

• Les capteurs, l'unité de traitement, les éléments finaux sont des équipements de sécurité et réalisent des sous-fonctions de sécurité. L'ensemble des sous-fonctions réalise la fonction de sécurité.

2.7 Redondance au sein d'un S.I.S :

Pour améliorer le niveau de confiance d'un système instrumenté de sécurité, il est possible, entre autres, de la doubler totalement (redondance totale), ou de doubler une partie de ses composants (redondance partielle de la barrière de sécurité). A noter que la redondance peut être réalisée avec du matériel identique ou avec du matériel de technologie différente, ce dernier type de redondance permet de limiter les modes communs de défaillance.

Tous les éléments constituant un système instrumenté de sécurité peuvent être redondés : capteurs, unité de traitement, actionneurs et même les moyens de transmission.

A noter que l'on peut distinguer plusieurs types de redondance :

- **la redondance active** qui est une redondance telle que tous les moyens d'accomplir une fonction requise fonctionnent simultanément.
- **la redondance passive** qui est une redondance telle qu'une partie seulement des moyens d'accomplir une fonction requise est en fonctionnement, le reste n'étant utilisé sur sollicitation qu'en cas de défaillance de la partie en fonctionnement.
- **la redondance majoritaire m/n** qui est une redondance telle qu'une fonction n'est assurée que si au moins m des n moyens existants sont en état de fonctionner ou en fonctionnement.

Les architectures les plus souvent rencontrées relatives à ce dernier type de redondance sont les suivantes :

- **1oo1** (m=n=1) : Cette architecture comprend un seul élément, et toute défaillance dangereuse de cet élément empêche le traitement correct de tout signal d'alarme valide.
- **1oo2** (m = 1 et n = 2) : Cette architecture comprend deux éléments connectés en parallèle de façon que chacun puisse traiter la fonction de sécurité. Ainsi, il faudrait la défaillance dangereuse des deux éléments pour qu'un signal d'alarme valide ne soit pas traité correctement.
- **1oo3 (**m=1 et n=3) Cette architecture est composée de trois canaux connectés en parallèle, fonctionnant en redondance active. C'est-à-dire que ce système restera opérationnel, vis-à-vis des défaillances dangereuses, tant qu'au moins un de ces canaux le sera. Cela dit, une opération intempestive de l'un des trois canaux provoque l'activation de la fonction de sécurité.

2.8 Intégrité de sécurité d'un SIS

La référence **[1]** la définit comme suit : "probabilité pour qu'un système relatif à la sécurité (SRS) exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et pour une période de temps spécifiée". Elle indique également que cette définition est centrée sur la fiabilité des SRS dans l'exécution de leurs fonctions de sécurité.

Cette même référence, précise que l'intégrité de sécurité comprend l'intégrité de sécurité du matériel ainsi que l'intégrité de sécurité systématique. Elles sont définies ci-après.

- **Intégrité de sécurité du matériel** *:* partie de l'intégrité de sécurité des systèmes relatifs à la sécurité liée aux défaillances aléatoires du matériel en mode de défaillance dangereux.
- **Intégrité de sécurité systématique** *:* partie de l'intégrité de sécurité des systèmes relatifs à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux, en précisant que l'intégrité systématique ne peut normalement, ou précisément, être quantifiée, mais simplement considérée d'un point de vue qualitatif.

Les prescriptions concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux SIS sont spécifiées en termes de niveau d'intégrité de sécurité (SIL) : niveau discret parmi quatre possibles, le SIL 4 possède le plus haut degré d'intégrité de sécurité. Sa détermination dépend du mode de fonctionnement du SIS. Ce point est évoqué dans ce qui suit.

2.9 Modes de fonctionnement des SIS et paramètres cibles de défaillances:

2.9.1. Fonctionnement en faible demande : Un SIS est en mode de fonctionnement à faible demande lorsque la fréquence de sollicitation est inférieure à une fois par an (1/an) ou inférieure au double de la fréquence des tests périodiques auxquels il est soumis. **[1]**.

-Probabilité moyenne de défaillance à la demande : notée *PFDavg* (*Average Probability of Failure on Demand*). Elle 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. **[2].**

2.9.2 Fonctionnement en forte demande ou demande continue : Un SIS en mode de fonctionnement continu ou à forte demande implique une forte sollicitation du SIS. Il est considéré lorsque la fréquence de sollicitation est élevée ou continue, c'est-à- dire qu'elle est supérieure à une fois par an (1*/an*) ou supérieure à deux fois la fréquence des tests périodiques. **[33].**

-Probabilité de défaillance dangereuse par heure : notée 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 à demande élevée. **[34].**

2.10 Classification des défaillances des SIS

2.10.1 Classification retenue dans la norme CEI 61508

- **Classification des défaillances selon leurs causes**

La norme CEI 61508 **[1]** adopte une classification qui contient deux catégories de défaillances : les défaillances physiques (aléatoires du matériel) et les défaillances fonctionnelles (systématiques).

La définition des défaillances aléatoires : du matériel donné par cette norme est la suivante : « défaillances survenant de manière aléatoire et résultant de divers mécanismes de dégradations au sein du matériel ». Une telle défaillance rend donc le système incapable de remplir sa fonction suite à sa dégradation physique. Il est important de noter que la dégradation physique du système à deux causes principales :

Vieillissement du matériel. Les défaillances dues au vieillissement sont appelées défaillances naturelles ou primaires.

Exposition aux contraintes excessives : ces contraintes peuvent être induites par des facteurs externes ou par des erreurs humaines. Ces défaillances sont appelées défaillances secondaires.

Les défaillances aléatoires du matériel sont relativement bien comprises. Les données relatives à cette catégorie de défaillances sont, dans la plupart du temps, disponibles.

La défaillance systématique est définie par la même norme comme étant « défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés ». Lors de l'occurrence d'une telle défaillance, le système ne remplit plus la fonction qui lui est demandée, mais il ne présente aucune dégradation physique. C'est la

raison pour laquelle ces défaillances sont qualifiées de non physiques ou de fonctionnelles (par exemple : l'opérateur ferme une vanne par erreur, la vanne dans ce cas n'est pas dégradée physiquement). Les défaillances systématiques peuvent être divisées en deux catégories :

Défaillances de conception : ces défaillances sont introduites lors de l'une des phases du cycle de vie du système. Elles existent à l'état latent, se révèlent lors du fonctionnement du système et ne peuvent généralement être éliminées que par une modification de la conception ou du processus de fabrication. Des exemples typiques de ces défaillances sont les défauts de conception du logiciel et du matériel.

Défaillances d'interactions : ces défaillances sont initiées par les erreurs humaines lors de l'exploitation, la maintenance, …

La norme CEI 61508 considère que les défaillances du logiciel sont toutes systématiques. Par opposition aux défaillances aléatoires du matériel, les défaillances systématiques sont difficiles à modéliser et de ce fait moins compréhensibles.

Cette classification de défaillances est résumée à la **(figure 2.8)**

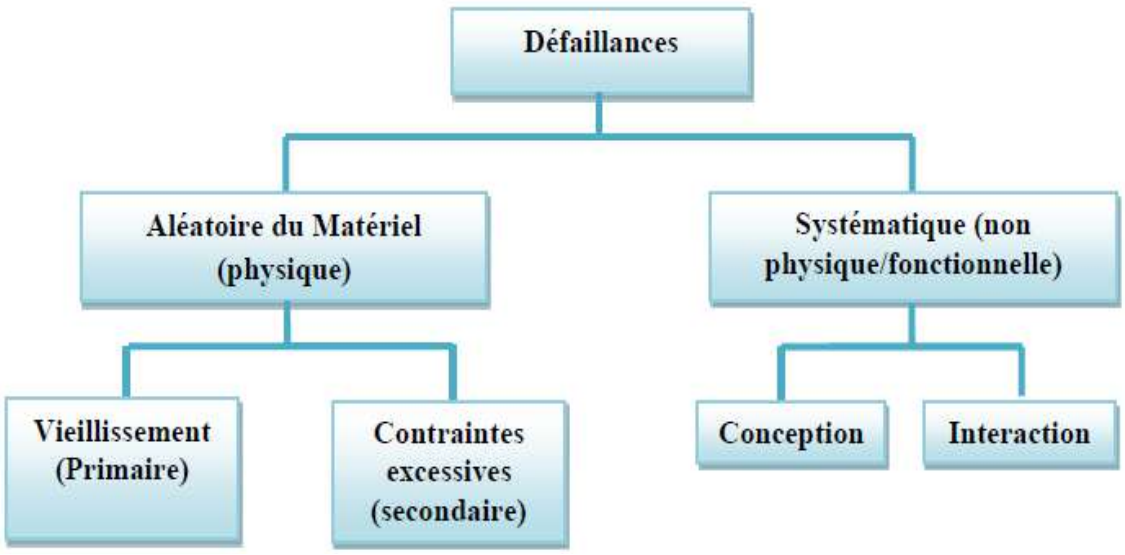


Figure 2.8 : Classification des défaillances selon leurs causes. [33]

- **Classification des défaillances selon leurs effets sur la fonction de sécurité**

Toutes les défaillances (aléatoires du matériel et systématiques), selon leurs effets, peuvent être classées dans l'une des deux catégories suivantes : défaillances en sécurité (safe failures) ou défaillances dangereuses (Dangerous failures).

Suivant cette dernière classification, seules les défaillances aléatoires du matériel sont prises en compte dans ce qui suit. Dans ces conditions, les définitions de ces deux catégories selon la norme CEI 61508S**. [1]** sont données ci-après :

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 ».

En nous situant donc dans le contexte de la CEI 61508, une défaillance dangereuse est une défaillance qui tend à inhiber la fonction de sécurité en cas de demande émanant de

L'EUC qui sera alors dans un état dangereux. Une défaillance sûre est une défaillance 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 dommageable n'y est plus possible.

Compte tenu de cette décomposition, le taux de défaillance aléatoire du matériel de chaque canal (λ) comporte deux composantes :

$\lambda = \lambda S + \lambda D$

Avec :

λS : taux de défaillance aléatoire en sécurité du matériel,

λD: taux de défaillance aléatoire dangereuse du matériel.

Une autre partition résulte du fait que ces défaillances peuvent être ou non détectées par des tests en ligne (tests de diagnostic). Les premières sont dénommées défaillances détectées (detected Failures) et les secondes, qui ne peuvent être révélées que lors des tests périodiques hors ligne ou lors de la sollicitation du SIS par le système surveillé, sont dénommées défaillances non détectées (undetected failures). Le schéma suivant est classiquement présenté pour résumer cette double partition **[2].**

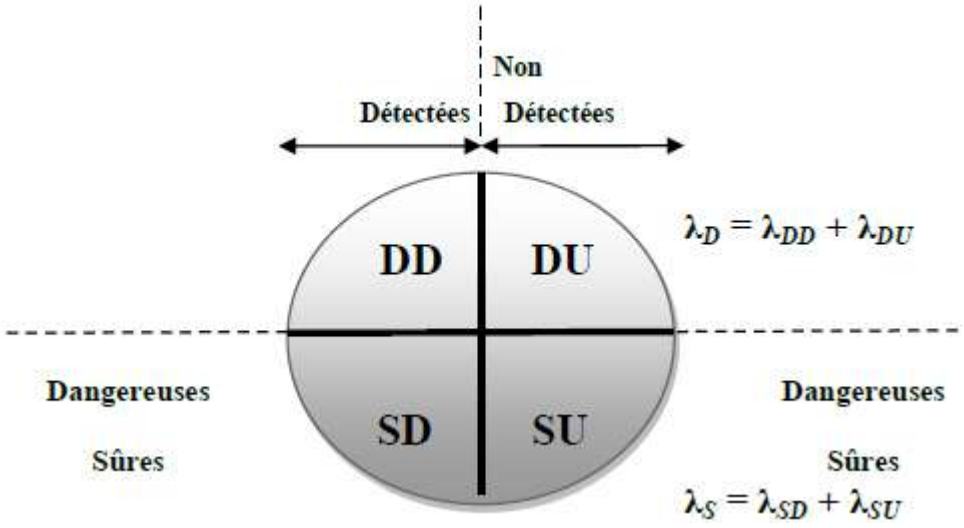


Figure 2-9 : Typologie des défaillances selon la norme CEI 61508.

2.10.2 Classification proposée par SINTEF

Cet organisme propose, dans son manuel **[35]**, une classification plus fine et plus réaliste que la précédente, puisqu'elle prend en compte les défaillances intempestives et les défaillances non-critiques qui sont définies ci-après. Cette classification est résumée par l'arborescence suivante :

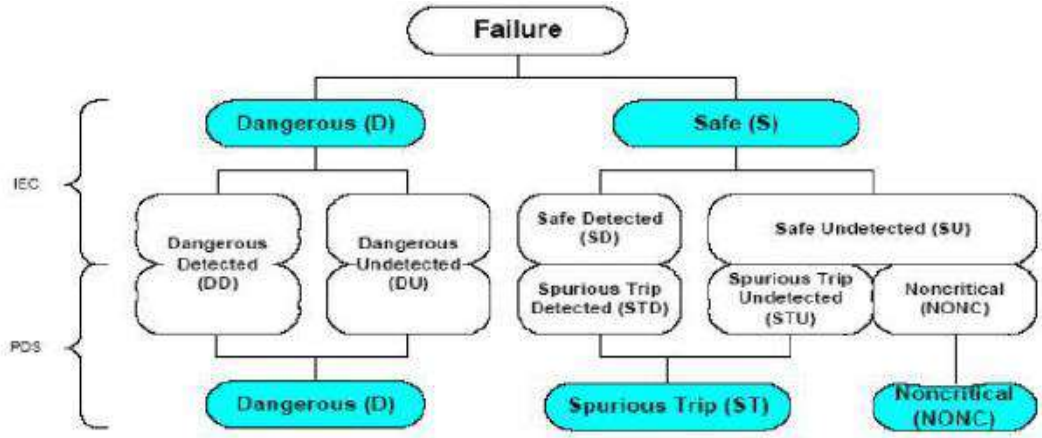


Figure 2-10 : Classification des défaillances selon SINTEF. [37]

Pour résumer, la méthode PDS de SINTEF considère, au niveau des composants, trois types de défaillances : dangereuses, intempestives et non-critiques.

Les défaillances dangereuses sont celles de la norme et se divisent donc en défaillances détectées (λDD) et non-détectées (λDU).

Les défaillances intempestives sont un sous-ensemble des défaillances sûres et se divisent également en défaillances détectées (λSTD) et non-détectées (λSTU).

Les défaillances non-critiques (λNONC) sont celles qui n'ont aucune incidence sur les deux fonctions principales du système EUC, c'est-à-dire son aptitude à produire (disponibilité de production) et son aptitude à ne pas engendrer d'événements redoutés (sécurité).

A partir de cette classification, il a été déduit une classification des taux de défaillance résumée ci-dessous **[2]** :

- λDD et λDU sont ceux définis dans la norme.
- λSTD est le taux de défaillance intempestive détectée. Il correspond au λSD de la norme.
- La somme (λSTD + λNONC) correspond au λSU de la norme.
- La somme (λD + λSTD + λSTU) est appelée λcrit.

2.11 Définitions et classification des activations intempestives des SIS

2.11.1 Définitions

La première étude monothématique qui traite le sujet des défaillances intempestives des SIS est celle présentée par M.A. Lundteigen et M. Rausand **[36].** Dans cet article, les auteurs utilisent le terme collectif : activation intempestive (spurious activation). Dans ce qui suit de ce mémoire, nous utilisons le même terme comme générique. Le terme ‘activation’ indique qu’il y a une certaine transition d’un état vers un autre et le terme ‘intempestive’ indique que les causes du déclenchement sont fausses, incorrects et non-réels **[36]**. Dans un processus industriel, les activations intempestives des SIS peuvent provoquer des arrêts partiels ou complets des installations, donc il est nécessaire de réduire son nombre d’apparition pour :

(1) éviter les pertes de production suite aux arrêts,

(2) éviter les risques qui peuvent apparaitre durant la phase de redémarrage.

2.11.2 Classification des activations intempestives

Selon la référence **[36]**, il existe trois différents types des activations intempestives des systèmes instrumentés de sécurité qui sont :

- **L’opération intempestive (Spurious operation)** : une opération intempestive SO est une activation d’un élément du SIS individuellement en absence d'un processus spécifié la demande d’activation (des déviations réelles).

Exemples :

(1) Un faux signal sur un niveau élevé émet par un détecteur du niveau dû à une défaillance interne du détecteur.

(2) Une alarme est émet à partir d'un transmetteur de niveau sans que le niveau de liquide ait dépassé la limite supérieure, en raison de l'échec à distinguer la mousse par rapport au niveau réel du liquide dans un séparateur.

-Le déclenchement intempestif (*Spurious trip*) : un déclenchement intempestif est une activation d'un ou plus d'éléments du SIS sachant que la fonction instrumentée de sécurité (SIF) est effectuée en absence d'un processus spécifié la demande d'activation (des déviations réelles)

Exemples :

(1) deux détecteurs de flamme dans une configuration 2oo3 (le système fonctionne si au moins 2 composants fonctionnent parmi les 3) donnent un faux signal sur le feu ce qui provoque le déclenchement des éléments finaux et l'activation de la fonction instrumentée de sécurité (SIF).

(2) La fermeture d'une vanne d'arrêt d'urgence (ESV) dans une configuration 1oo2 (le système fonctionne si au moins 1 composant fonctionne parmi les 2) des éléments finaux suite à une défaillance interne.

- L'arrêt intempestif (Spurious shutdown) : un arrêt intempestif est un arrêt partiel ou complet des systèmes en absence d'un processus spécifié la demande d'activation (des déviations réelles).

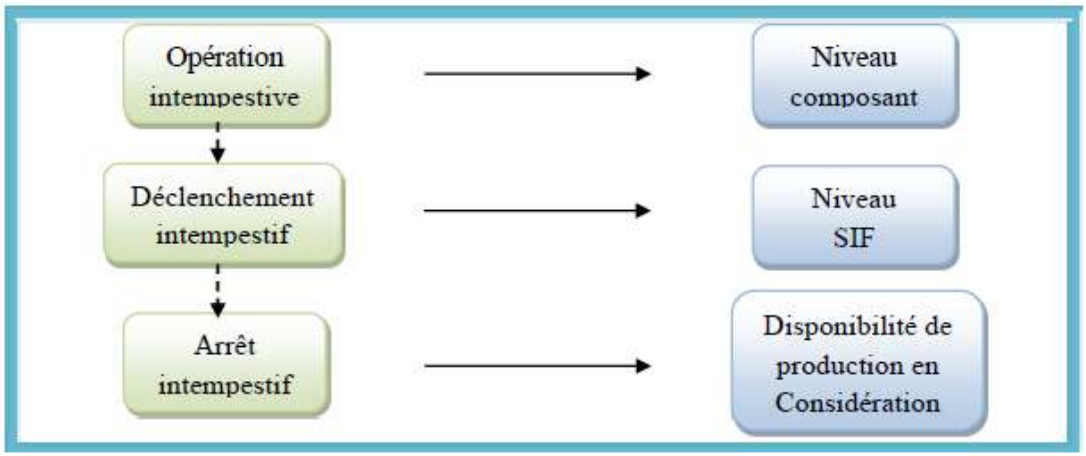


Figure 2-11 : les différents types des activations intempestives

Selon les définitions précédentes, les différents types des activations intempestives se réalisent 'en absence d'un processus spécifié la demande d'activation ' ce qui nous permet de penser que ces activations des SIS ne concernent que le mode de fonctionnement faible demande. Cette restriction n'a pas de justification, si ce n'est le fait que le domaine de la demande continue, et là

PFH qui lui est associée, ont été moins largement étudiés que celui de la faible demande et de son indicateur caractéristique, la PFDmoy. **[2]**

La définition suivante est plus étendue que les précédentes : « Une défaillance intempestive ne peut se définir que par rapport à une fonction de sécurité spécifiée. Elle a pour résultat, soit de déclencher la réalisation de cette fonction de sécurité en l'absence de toute demande, soit d'annihiler l'effet protecteur de cette fonction après son déclenchement réussi ». **[2]** On remarque que le premier volet de cette définition concerne le mode de fonctionnement faible demande des SIS qui assurent la fonction de sécurité, et que le second concerne le mode de fonctionnement continu.

Autre point à souligner : l'activation intempestive des SIS peut être considérée comme sûre (peut être temporairement), tandis qu'elle est dangereuse. Autrement dit, cela nous conduit à nouveau à affirmer que les activations intempestives ne constituent pas un sous-ensemble des défaillances sûres, ni d'ailleurs des défaillances dangereuses. **[2]**

2.12 Causes des activations intempestives

Des relations de causalité peuvent liées les différents types des activations intempestives des systèmes instrumentés de sécurité tel que :

- Une opération intempestive peut être l'une des nombreuses causes d'un déclenchement intempestif.

-Un déclenchement intempestif peut-être l'une des causes d'un arrêt intempestif. Ces relations sont illustrées dans la **(Figure 2.12)** par des flèches en pointillés.

La **(figure 2 12)** illustre les causes principales des activations intempestives représentées dans un diagramme de fluence (influence diagramme).

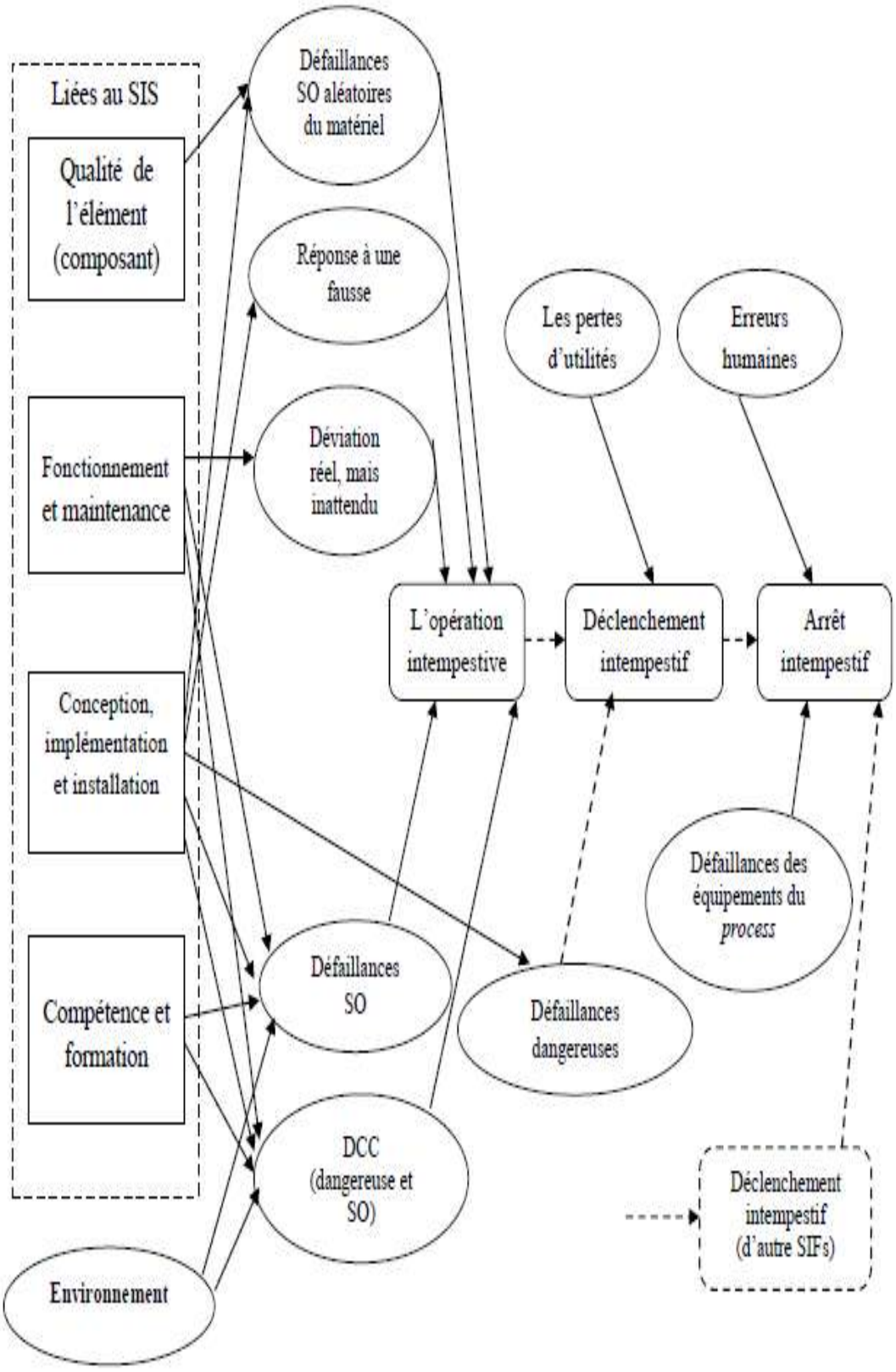


Figure 2.12 : les décisions et les facteurs influençant les activations intempestives. [36]

Discussion :

L'opération intempestive SO, le déclenchement intempestif, et l'arrêt intempestif sont présentés comme nœuds de performance (rectangles arrondis), puisque leurs taux d'occurrence sont des mesures de performance qui nous voulons de les minimiser afin de réduire les pertes de production. **[37]**

Les nœuds de chance (cercles) représentent les facteurs qui influencent les taux des activations intempestives. Nous ne sommes pas en mesure de contrôler ces facteurs directement, mais nous pouvons les influencer indirectement par un ensemble de décisions.

Une décision peut être de choisir un élément avec une fiabilité supérieure à celle spécifiée. Autre décision peut être d'investir davantage dans la formation et la compétence du personnel, afin de réduire les erreurs humaines en cours de fonctionnement et d'entretien. Les décisions pertinentes sont illustrées dans la figure comme des nœuds de décision (rectangles).

Les flèches indiquent les relations entre les décisions, les facteurs influençant, et les mesures de performance. Les flèches en pointillés sur la (**figure 2.12)** indiquent que la liaison est présente, sous certaines conditions, par exemple, pour une configuration matérielle donnée. Plus de détaille dans ce qui suit.

2.12.1 Causes des opérations intempestives

Pour les opérations intempestives SO, on trouve deux causes principales d'activation des éléments du SIS tel que :

(1) Une défaillance interne de l'élément (ou son support) conduit à une Opération Intempestive.

(2) L'élément d'entrée répond à une fausse déviation.

Les défaillances SO dues à des défaillances internes sont souvent considérées comme défaillances en sécurité car ils ne gênent pas le SIS á l'exécution en demande. Cependant, toutes les défaillances en sécurité ne conduit pas forcément à des défaillances SO, et il est donc

nécessaire d'étudier les modes de défaillance en sécurité pour chaque élément pour déterminer quelles ceux qui sont pertinents pour les défaillances SO.

Les défaillances SO **(figure 2.12)** sont distinguées en :

-Défaillances SO aléatoires du matériel dus principalement aux dégradations normales des éléments du SIS et,

-Des défaillances SO systématique dus aux erreurs de conception, l'insuffisance des procédures,

La qualité des éléments du SIS influence sur le taux des défaillances SO aléatoires du matériel (illustré par une flèche en **(figure 2.12).** Une matière bien définie peut, par exemple, supporter des hautes températures et des pressions élevées plus qu'une autre matière. Ou bien un principe de détection utilisé pour un capteur de niveau peut être plus vulnérable à une condition de fonctionnement spécifique qu'un autre. Les procédures d'exploitation et d'entretien, les outils, et les méthodes de travail, la conception, l'implémentation et l'installation des procédures, les compétences et la formation, ainsi que l'exposition á l'environnement peuvent influer sur la probabilité de défaillances systématiques **(figure 2.12).**

La vérification, la validation et les tests peuvent réduire le taux d'apparition des défaillances systématiques. Des moyens de vérification (par exemple, des essais ou des révisions) pour vérifier et confirmer que la conception mis en œuvre est conforme aux spécifications, bien que des moyens de validation pour évaluer également la pertinence du modèle choisi. Dans la phase d'exploitation, le taux des défaillances systématiques peut être réduit par la vérification et la validation des tests par exemple, des procédures d'inspection visuelles, … La compétence et la formation sont aussi importantes pour réduire les erreurs humaines lors des fonctions de tests. Les conditions environnementales influencent sur l'apparition des défaillances systématiques si ces conditions ne conforment pas aux conditions de conception. Cependant, dans la plupart des cas, il n'est pas possible d'influer sur les conditions environnementales. La contribution de l'environnement est donc illustrée par un nœud de chance dans la **(figure 2.12).**

Les défaillances de causes communes (DCC) peuvent être aussi l'une des causes des opérations intempestives **(figure 2.12).** Non seulement les DCC dangereuses qui conduit á des opérations intempestives, mais il est également nécessaire de tenir compte les défaillances SO de causes communes DCC-SO. Ces derniers n'ont pas les mêmes causes que les DCC dangereuses. La norme CEI 61508 **[1]** recommande que les DCC dangereuses soient modélisés par un modèle de facteur beta β, et la partie 6 de la norme inclut une procédure pour estimer une valeur spécifique du paramètre β pour les DCC dangereuses. Comme ces derniers ont une nature différente des DCC-SO intempestives, la procédure présentée dans la partie 6 de la norme CEI 61508 n'est pas adapté pour estimer le paramètre βSO pour les DCCSO intempestives.

Les fausses déviations sont des causes importantes qui conduisent aux opérations intempestives des éléments du SIS. Une fausse déviation partage souvent certaines caractéristiques (par exemple, l'aspect visuel et composition) avec une déviation réelle, alors il peut être difficile pour l'élément d'entrée du SIS de distinguer les deux. Un rayon de la lumière du soleil peut être, par exemple, vue comme une petite flamme sur certains angles, et un détecteur de flamme peut donc le lire comme une flamme.

Il n'est pas possible de réduire l'apparition des fausses déviations, mais nous pouvons influencer la façon de réponse de l'élément d'entrée du SIS. On ne peut pas, par exemple, de supprimer la lumière du soleil ou de modifier la densité de la mousse, mais nous pouvons sélectionner les éléments qui visent à mieux distinguer entre faux et vrai exigences du processus, ou nous pouvons déplacer les éléments pour les rendre moins vulnérables aux fausses déviations.

Quelques fausses déviations sont provoquées par l'homme, ce qui signifie que nous sommes en mesure d'influencer la façon dont ils se produisent souvent en améliorant les procédures d'exploitation et de maintenance et les processus des travaux.

Si nous voulons, par exemple, éviter la réponse du détecteur de flamme á la soudure, nous devons assurer que le détecteur ne voit pas ces flammes par des couverts ou d'autres barrières.

Ceci est illustré par une flèche de « fonctionnement et maintenance » au nœud de chance « Déviation réel, mais inattendu » sur la **(figure 2.12).**

2.12.2 Causes des déclenchements intempestifs

L'un des principaux contributeurs aux déclenchements intempestifs est évidemment les opérations intempestives SO des éléments du SIS. SO peut conduire à un déclenchement intempestif si le nombre d'éléments activés correspond au nombre d'éléments nécessaires à l'exécution de la fonction de sécurité. La configuration matérielle choisie détermine donc si les opérations intempestives SO peuvent conduire à un déclenchement intempestif ou non. Cette « condition » est illustrée par des flèches en pointillés sur la **(figure 2.12).**

Il existe plusieurs d'autres causes des déclenchements intempestifs, par exemple :

Les pertes d'utilités ; comme pneumatique, hydraulique ou l'alimentation électrique : ces pertes d'utilités peuvent directement conduire á des déclenchements intempestifs.

Défaillances dangereuses détectées (DD) : Dans certains cas, les systèmes instrumentés de sécurité peuvent intempestivement réaliser la fonction de sécurité (SIF) attendue même en présence des défaillances dangereuses détectées (DD) qui arrêtent la réalisation du SIF en présence de demande. Dans une configuration 2oo3, la fonction de sécurité peut réaliser en présence d'une seule défaillance DD, mais ce n'est pas le cas en présence de deux défaillances DD.

2.12.3 Causes des arrêts intempestifs

Un déclenchement intempestif peut généralement, mais pas toujours, conduire à un arrêt intempestif du processus. Si la fonction instrumentée de sécurité (SIF) du SIS n'a pas un effet direct sur le processus (par exemple, activer d'autres SIFs), le processus peut être en dépit de l'arrêt suite au déclenchement intempestif. Une flèche en pointillé est donc utilisé pour indiquer qu'un déclenchement intempestif peut (mais pas toujours) conduire à un faux arrêt.

La **(figure 2.12)** indique également (par des flèches en pointillés et nœud) que les différents types de SIFs peuvent conduire à des arrêts intempestifs.

Un arrêt intempestif peut aussi être causé par des défaillances (arrêts) des équipements du processus (équipements ne sont pas des éléments du SIS) comme des vannes de commande ou des pompes…. Une fermeture intempestive d'une vanne de régulation ou un arrêt intempestif d'une pompe peut être dû aux défaillances internes d'éléments, d'erreurs humaines ou les erreurs du système de contrôle automatique.

Dans la **(figure 2.12)**, les défaillances des équipements du processus (non SIS) et les défaillances du système de contrôle automatique sont illustrées par un nœud de chance « défaillances des équipements de processus », et les erreurs humaines en tant que nœud de chance "erreurs humaines".

2.13 Notion de niveau d'intégrité de sécurité (SIL)

Les normes de sécurité fonctionnelle CEI 61508 et CEI 61511 définissent une démarche d'analyse du niveau d'intégrité de sécurité (SIL) d'un système. Elles permettent de définir le niveau SIL qui doit être atteint par un SIS qui réalise la fonction de sécurité suite à une analyse de risque. Plus le SIL a une valeur élevée plus la réduction du risque est importante.

Les SIS sont classés en quatre niveaux SIL qui se caractérisent par des indicateurs discrets positionnés sur une échelle d'un à quatre niveaux **(Tableau 2.1).** Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisées par des systèmes E/E/EP relatifs à la sécurité selon la norme CEI 61508. Le SIL "4" désigne le degré de sécurité le plus élevé du fait de l'exigence forte de sécurité imposée et le niveau SIL "1" désigne l'exigence la plus faible.

Solicitation	Demande faible	Demande élevée
SIL	PFD_{avg}	PFH
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$10^{-6} \leq PFH < 10^{-5}$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$10^{-7} \leq PFH < 10^{-6}$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10^{-8} \leq PFH < 10^{-7}$
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$10^{-9} \leq PFH < 10^{-8}$

Table 2.1 Les différents niveaux de SIL définis par la norme CEI 61508.

L'utilisation des niveaux SIL permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel, menant aux événements dangereux identifiés pendant l'analyse de risque. Les SIL sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances.

La norme CEI 61508 détaille les prescriptions nécessaires pour répondre aux exigences de chaque niveau d'intégrité de sécurité. Ces prescriptions deviennent plus rigoureuses à mesure que le niveau de SIL s'élève en vue d'obtenir la probabilité d'une défaillance dangereuse de plus en plus faible.

2.13.1 Méthodes de détermination de SIL

La détermination du SIL d'un SIS peut s'obtenir par différentes méthodes :

Méthodes qualitatives : Il s'agit de méthodes qui permettent de déterminer le niveau de SIL à partir de la connaissance des risques associés au procédé, la méthode graphe de risque par exemple.

Méthodes semi quantitatives : La méthode la plus répandue est la matrice de risque. Cette matrice donne le niveau de SIL en fonction de la gravité de risque et de sa fréquence d'occurrence.

Méthodes quantitatives : Il s'agit des méthodes qui permettent de calculer le PFD des SIS à partir des probabilités de défaillances de leurs composants. Les méthodes les plus répandues sont :

- Les équations simplifiées **[22].**

- Les arbres de défaillances **[38].**

- Les chaînes de Markov **[39]** : Cette technique est souvent utilisée en sûreté de fonctionnement lorsque l'on souhaite modéliser un système avec des composants à taux de défaillance constant et réparable. Il permet ainsi de faire une analyse dynamique du système.

2.13.2 Comment choisir le SIS convenable à partir du SIL ?

Dans le contexte de l'intégrité de sécurité du matériel le niveau d'intégrité (SIL) le plus élevé qui peut être annoncé pour la fonction de sécurité donnée est limité par la tolérance aux anomalies du matériel et la proportion de défaillances en sécurité (SFF) des sous-systèmes qui réalisent la fonction de sécurité. La norme 61508-2

Une tolérance aux anomalies du matériel d'indice M signifie que (M+1) anomalies sont susceptibles de provoquer la perte de la fonction de sécurité : pour une architecture KooN,

$$\mathbf{M + 1 = N - K + 1} \qquad \mathbf{2.1}$$

La proportion de défaillances en sécurité d'un sous-système (Safe Failure Fraction ou SFF)

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda} \qquad \mathbf{2.2}$$

Les tableaux suivants de la CEI 61508-2 spécifient le SIL le plus élevé qui peut être annoncé pour la fonction de sécurité étudiée et pour des canaux identiques :

SFF	Tolérances aux anomalies Matérielles (M)		
	0	1	2
≤60%	SIL1	SIL2	SIL3
60% - 90%	SIL2	SIL3	SIL4
90% - 99%	SIL3	SIL4	SIL4
≥90%	SIL3	SIL4	SIL4
Un SIS peut être considéré du type A si son comportement en présence d'anomalies est bien déterminé, si les modes de défaillance de ses constituants sont bien définis et si les données concernant leurs défaillances, issues du retour d'expérience, sont connues avec une bonne fiabilité.			

Table 2.2: sous système de type A [40]

Afin de préciser le SIL convenable on va chercher dans le tableau le point d'intersection entre la valeur du SFF et la valeur de tolérance aux anomalies matérielles (M).

Si notre installation comporte plus d'un SIL, on peut aller à la combinaison des SIL comme suit :

F Pour une configuration série (NooN) :

$$\textbf{SIL (sous fonction) = MIN (SIL (canal ; i = 1……, N)}$$

F Pour une configuration KooN :

$$\textbf{SIL (sous fonction) = MIN(MAX(SIL(canal)) + N - K ; SIL}_4\textbf{)}$$

SFF	Tolérances aux anomalies Matérielles (M)		
	0	1	2
≤60%	non autorisé	SIL1	SIL2
60% - 90%	SIL1	SIL2	SIL3
90% - 99%	SIL2	SIL3	SIL4
≥90%	SIL3	SIL4	SIL4
Un SIS peut être considéré du type B si une des trois conditions régissant le type A n'est pas satisfaite.			

Table 2.3: sous système de type B [40]

2.13.3 Prescriptions relatives à l'intégrité de sécurité (aléatoire) du matériel : PFD ou PFH :

Formules de calcul :

PFD_{KooN} = indisponibilité moyenne de l'architecture KooN

$$PFD_{KooN} = PFD_{KooN}^{Ind} + PFD_{KooN}^{DCC}$$

$$MDT_{1ooi} = \frac{\lambda_{DU}}{\lambda_{DD} + \lambda_{DU}}.(\frac{T_i}{i+1} + MTTR) + \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}.MTTR$$

$$PFD_{KooN}^{DCC} = \lambda_{DUDCC}.(\frac{Ti}{2} + MTTR) + \lambda_{DDDCC}.MTTR$$

$$PFD_{KooN}^{Ind} = A_N^{N-K+1}.\lambda_{Dind}^{N-K+1}.\prod_{i=1}^{N-K+1} MDT_{1ooi}$$

Remarque : MDT :(Mean Down Time) : durée moyenne d'indisponibilité.

λDind = λDUind + λDDind:

T1 : durée entre deux tests périodiques.

$A_p^n = \frac{n!}{(n-p)!}$

$$PFH_{KooN} = PFH_{Ind}^{KooN} + PFH_{DCC}^{KooN}$$

$$PFH_{Ind}^{KooN} = A_N^{N-K+1}.\lambda_{Dind}^{N-K+1}$$

$$PFH_{DCC}^{KooN} = \lambda_{DUDCC} + \lambda_{DDDCC}$$

Pour un SIS complet, composé de trois sous-systèmes (A, B, C), les quantités PFDSIS et PFHSIS s'obtiennent en sommant celles relatives à ses sous-systèmes, chacun ayant une architecture KooN :

$$PFD_{SIS} \approx PFD_A + PFD_B + PFD_C \quad \textbf{2.3}$$

$$PFH_{SIS} \approx PFH_A + PFH_B + PFH_C \quad \textbf{2.4}$$

$\textbf{Remarque :} MDT_{1ooi} = \frac{MTTR}{i}$.

En calculant le PFD et le PFH de chaque système nous pouvons alors estimer le SIL comme suit:

Le PFD_{moy}^{sis} doit être certainement inférieure à la relation Ft/Fnp pour que le système sera bien protéger.

$$PFD_{moy}^{sis} \leq \frac{Ft}{Fnp} \quad \textbf{2.5}$$

Tel que :

Ft : la fréquence tolérable que l'on peut accepter

Fnp : la fréquence de l'évènement dangereux

Par comparaison entre $PFD_{moy}^{sis} \leq \frac{Ft}{Fnp}$ et le tableau des SIL nous définissons alors le SIL convenable.

2.16 CONCLUSION

Au cours du deuxième chapitre nous avons, présenté l'ensemble des normes qui discutent les systèmes instrumentés de sécurité (norme CEI 61508 et ses normes sectorielles). Il convient à cet effet de rappeler que la CEI 61508 de même que ses normes filles sont actuellement devenues la référence par excellence pour la mise en œuvre de ce type de systèmes.

Outre cela, nous abordé à une exposition de la typologie des défaillances liée aux systèmes instrumentées de sécurité selon deux approches différentes (norme CEI 61508 et SINTEF) ; puis nous avons présenté les concepts de base relatifs aux activations intempestives des SIS et discuté ses causes.

CHAPITRE 3 : Les circuits hydrauliques industriels

3.1 Introduction

L'hydraulique est la science qui traite des problèmes posés par l'emploi des fluides en mouvement ou au repos. Ses bases scientifiques, établies par Blaise Pascal et par Isaac Newton, remontent au 17eme siècle. C'est d'ailleurs à cette époque que le mot « hydraulique » apparaît dans la langue française.

Autrefois, une machine hydraulique était toujours mue par l'eau, aujourd'hui, le terme désigne tout engin dont le fonctionnement fait intervenir un liquide.

Les 25 dernières années ont vu l'hydraulique s'imposer graduellement au cœur des grandes industries. Aujourd'hui, l'hydraulique se révèle aussi essentielle pour les grandes machines de fabrication et de production que peut l'être le système artériel pour le corps humain. Car, en plus d'acquérir ses lettres de noblesse auprès des chercheurs, l'hydraulique est devenu indispensable à tous ceux qui en réalisent les applications dans l'industrie moderne.

L'automatisation ainsi que la nouvelle génération de produits de grande qualité confirment de plus en plus le rôle primordial que joue l'hydraulique. Or, son utilisation dans plusieurs secteurs de la mécanique appliquée nécessite avant tout de bonnes connaissances de base en mécanique des fluides et sur les systèmes qui l'emploient. **[41]**

3.2 Définition

On entend par « hydraulique » : la transmission de forces et de mouvements au moyen d'un fluide. **[42]**

Un système hydraulique, en hydromécanique, est un assemblage de composants fonctionnant de manière unitaire et souvent en interaction afin d'utiliser un fluide sous pression pour effectuer un travail mécanique. Un tel système peut aussi être appelé installation hydraulique. Son principal élément est une centrale hydraulique.

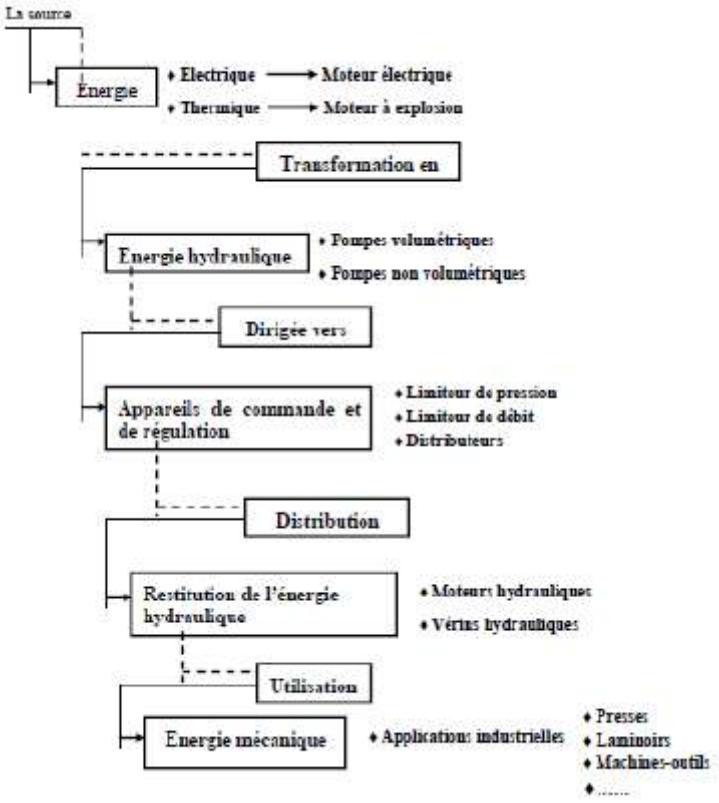


Figure 3.1: cycle d'un circuit hydraulique [42]

3. 3 Les éléments de l'hydraulique

Les principaux éléments que nous rencontrons dans tout circuit hydraulique sont :

Réservoir : Stocker le fluide.

Pompe hydraulique : Générer la puissance hydraulique.

Moteur électrique : Actionner la pompe.

Distributeur : Distribuer la puissance hydraulique au vérin.

Vérin : Transformer la puissance hydraulique en puissance mécanique.

Accumulateur : Stocker l'énergie hydraulique et la restituer en cas de besoin.

Régulateur de débit : Régler le débit et la vitesse du fluide.

Vanne : Distribuer ou interrompre le passage du fluide.

Limiteur de pression : Protéger l'installation contre les surpressions.

Filtre : Empêcher les impuretés de s'infiltrer dans les organes sensibles.

Manomètre : Indiquer la valeur de la pression.

Débitmètre : Indiquer la valeur de débit.

Clapet anti-retour : Autoriser le passage du fluide dans un seul sens.

3.4 L'introduction du SIS au circuit hydraulique

Les systèmes hydrauliques se retrouvent partout dans les installations industrielles qui requièrent de la force, de la flexibilité et de la fiabilité.

De nos jours, l'avènement de l'électronique et de l'informatique a permis de perfectionner les circuits hydrauliques. Ceux et celles qui œuvrent dans ce domaine doivent donc se tenir à l'avant-garde de ce qu'il est convenu d'appeler aujourd'hui l'électrohydraulique.

Pour ce faire, il leur faut bien connaître les principaux facteurs qui conditionnent les systèmes hydrauliques et être en mesure d'utiliser les formules mathématiques qui les déterminent. **[41]**

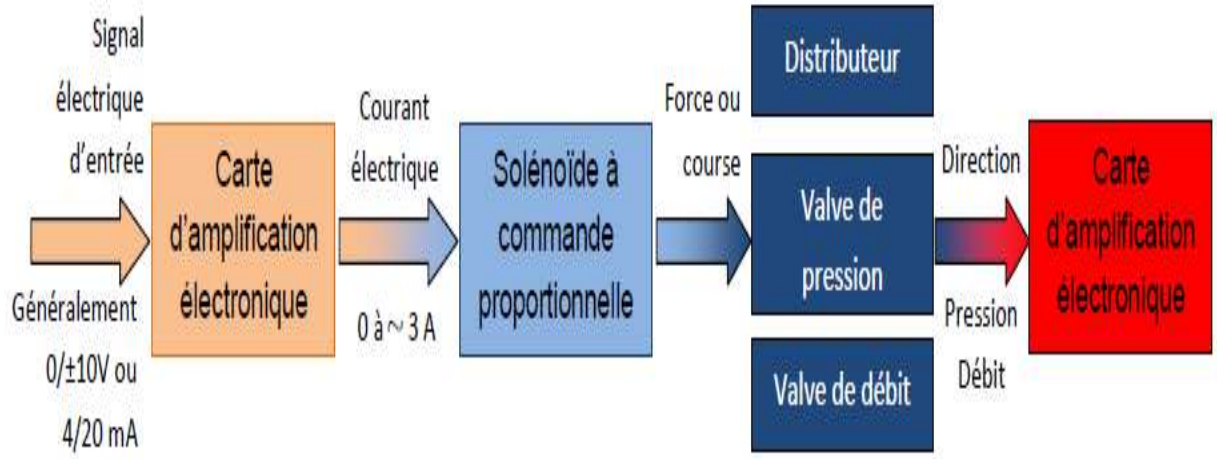


Figure 3.2: Exemple de la structure d'un SIS dans un circuit hydraulique [43]

3.4.1 Que veut dire “proportionnel” ?

Un composant proportionnel est un composant dont la grandeur de sortie (pression ou débit) varie proportionnellement à une grandeur d'entrée électrique : en général, une consigne

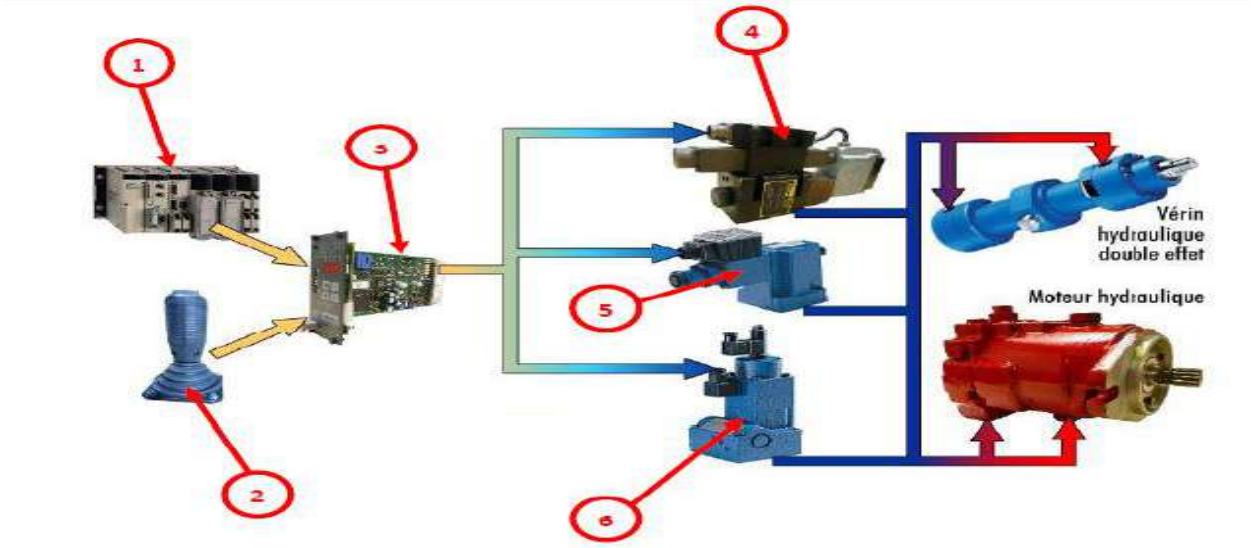


Figure 3.3: schématisation de la structure précédente [43]

Référence	Nom	Fonction
1	Automate industriel programmable	Un signal électrique d'entrée provenant d'un automate programmable envoie une consigne (généralement 0/± 10Vou4/20mA) à un amplificateur électronique
2	Manipulateur électrique	Un signal électrique d'entrée provenant d'un manipulateur électrique envoie une consigne (généralement 0/ ± 10Vou4/20mA) à un amplificateur électronique
3	Carte d'amplificateur électronique	La carte électronique transforme la consigne d'entrée en un courant de sortie amplifié 0/ 3A.
4	Distributeur à commande proportionnelle	Le distributeur proportionnel produit un signal de sortie Hydraulique proportionnel au signal électrique d'entrée. La grandeur hydraulique de sortie est contrôlée en direction et en débit et est transmise à l'actionneur.
5	Limiteur de pression à commande proportionnelle	Le limiteur de pression à commande proportionnelle produit un signal de sortie hydraulique proportionnel au signal électrique d'entrée. La grandeur hydraulique de sortie est contrôlée en pression et est transmise à l'actionneur
6	Régulateur de débit commande proportionnelle	Le régulateur de débit à commande proportionnelle produit un signal de sortie hydraulique proportionnel au signal électrique d'entrée. La grandeur hydraulique de sortie est contrôlée en pression et est transmise à l'actionneur

Table 3.1: Descriptif des composants précédents [43]

3.5 Rôle de l'hydraulique proportionnelle

Les exigences industrielles toujours plus importantes en termes de production, de rentabilité et de maintenance des équipements ont favorisées l'essor de l'hydraulique proportionnelle.

Celle-ci, bien qu'onéreuse, offre de nombreux avantages.

Les avantages

- La commande à distance.
- Les transitions progressives, qui, en évitant les coups de bélier et les chocs mécaniques permettent une augmentation de la durée de vie des équipements.
- La simplification des schémas puisqu'un seul appareil permet d'obtenir de nombreuses valeurs de débit ou de pression.
- Le pilotage du système hydraulique par un ordinateur ou un automate programmable muni de cartes analogiques permettant de fixer des valeurs de consignes à la carte électronique qui commande le composant hydraulique.
- La possibilité de réaliser un asservissement de pression-force-position-vitesse. **[44]**

Les appareils :

Les premiers composants utilisés en hydraulique proportionnelle étaient les servovalves, ces composants, bien que performant, ont l'inconvénient d'exiger une grande propreté du fluide, ils ont donc été remplacés par d'autres composants :

- Les distributeurs hydrauliques proportionnels.
- Les limiteurs de débits hydrauliques proportionnels.
- Les limiteurs de pressions hydrauliques proportionnelles. **[44]**

3.5.1 Les principaux composants à commande proportionnelle

1. Distributeur (Voir la figure3.4).

2. limiteurs de pression. (Voir la figure 3.5)

3. régulateurs de pression. (Voir la figure 3.6)

4. limiteurs de débit (Voir la figure 3.7)

5. régulateurs de débit (Voir la figure 3.8)

6. Les pompes à cylindrée variable (Voir la figure 3.9)

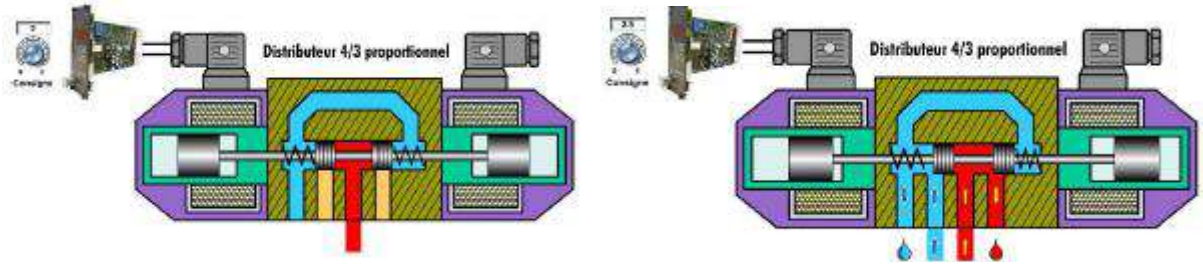


Figure 3.4: Distributeur 4/3 proportionnel [45]



Figure 3.5: limiteur de pression à action directe à commande proportionnelle [43]



Figure 3.6: Régulateur de pression à commande proportionnelle [43]

3.6 : La presse hydraulique SAM 500

3.6.1 Introduction

Dans le domaine industriel, toute machine est concernée de la sécurité et le bon fonctionnement pour que l'utilisateur être toujours sécurisé pendant la manipulation et que la production être sûr.

Les machines hydrauliques ou les machines qui fonctionnent avec le système hydraulique sont les plus connues dans les industries.

Dans ce chapitre nous allons prendre l'exemple d'une presse hydraulique de compactage de carton pour appliquer le principe des SIS afin de traiter les problèmes de haut pression.

3.6.2 Présentation et fonctionnement

Les Machines ont été conçues et fabriqués conformément à la directive machine 2006=42=CE et la Norme EN16500 en respectant le rapprochement des législations relatives aux machines ainsi qu'à d'autres spécifications techniques. Elles sont donc conformes à l'état actuel de la technique et garantissent une sécurité optimale pendant le fonctionnement.

Nos presses verticales répondent au niveau de sécurité Plrd. Niveau de performance requis (Plr)

Dans la pratique, la sécurité de la machine peut seulement être concrétisée si les mesures nécessaires sont prises, il incombe à l'exploitant de la machine dans le cadre de son devoir de vigilance de planifier ces mesures et d'en assurer l'exécution.

La presse semi-automatique SAM 500 allie une grande capacité de chargement à un faible encombrement.

Son groupe hydraulique lui assure puissance et fiabilité. Son faible encombrement lui permet dans un espace restreint, la réduction de déchets toutes sortes (papiers, cartons, plastiques), en balles compactes.

Sa simplicité d'utilisation à laquelle s'ajoute une grande facilité de chargement, l'éjection semi-automatique des balles, la possibilité de transfert par trans-palette en font un appareil des plus performants. **[46]**

3.6.2.1 Fiche technique

Déclaration de conformité CE relative aux matériels soumis à l'auto certification Le constructeur soussigné



Figure 3.7 : La presse SAM 500 [47]

SAS SACRIA Industries 4 rue de la Taye BP 40133 28113 LUCE Cedex(France). Déclarons que la presse à balle.

Marque : SACARIA Industrie.

Type : SAM 500.

Description : Compacter de la matière (recyclage de déchets).

Numéro de série : 17 - 51 – 4017.

Année de construction : 2017.

Est conforme aux directives :

-Directive Machine2006=42=CE en sa dernière version modifiée en vigueur

-Directive de comptabilité électromagnétique 2014=30=UE

-Directive Basse Tension 2014=35=UE

Correspond à la conformité aux normes harmonisées ou autres documents suivants :

EN60204 : 1997 EN ISO13849 / 12008 EN ISO12100 : 2010 sécurité machines. Notions fondamentales des principes généraux de conception et principes d'appréciation du risque EN16500 : 2014 presse verticales (Norme de type C）.

Personne autorisée à constituer le dossier technique (pour la directive 2006=42=CE)

Nom : GOFFE

Prénom : Documentaliste

Adresse : SACRIA Industries

4, rue de la Taye BP 40133

28113 LCE Cedex(France)

Fait à LUCE, le 19=12=2017

Mr. Jean François BEDOS

3.6.3 Exemple (la presse hydraulique SAM500)

Nous avons choisi cette machine pour faire notre exemple grâce à son simple schéma hydraulique où nous avons pu faire l'évaluation des dangers (ou bien la détermination du niveau de SIL requis pour couvrir ces dangers).

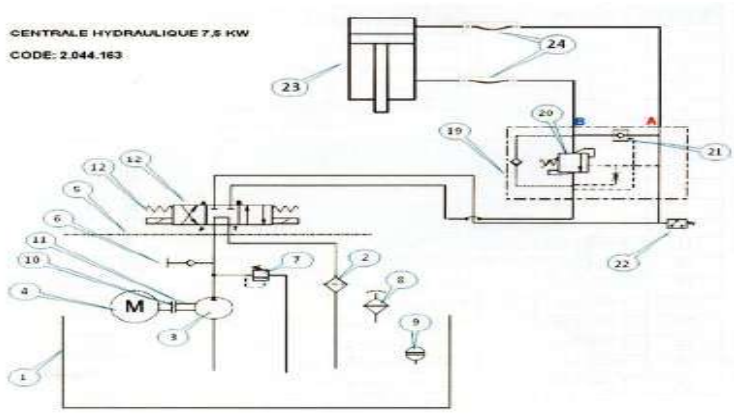


Figure 3.8 : schéma hydraulique de la presse [46]

Repère	Désignation
01	*Réservoir*
02	*Filtre par le retour complet*
02	*Cartouche pour filtre par retour*
03	*Pompe hydraulique*
04	*Moteur électrique*
05	*Embase avec Limiteur de pression*
06	*Prise de pression*
07	*Limiteur de pression*
08	*Bouchon reniflard*
09	*Niveau visuel*
10	*Lanterne pompe*
11	*Accouplement complet*
12	*Distributeur*
19	*Bloc valve génératrice avec clapet*
20	*Valve génératrice*
21	*Clapet anti retour*
22	*Capteur de pression analogique vérin*
23	*Vérin*
24	*Flexible hydraulique*

Table 3.2: Les repères de la Figure3.2 [46]

-dus à cette presse en utilisant le graphe de risque (il a d'autres méthodes pour la détermination du SIL **[46].**

3.6.3.1 le graphe de risque

Des systèmes différents entraînent des risques différents. Par conséquent, les exigences relatives aux défauts de sécurité des systèmes instrumentés de sécurité (SIS) deviennent plus strictes à mesure que le risque s'accroît.

Les normes CEI/EN 61508 et CEI/EN 61511 définissent quatre niveaux de sécurité différents qui décrivent les mesures de contrôle du risque dans ces composants. Il s'agit des quatre niveaux d'intégrité de sécurité, ou SIL.

Plus la valeur numérique du niveau d'intégrité de sécurité (SIL) est élevée, plus la réduction du risque est importante.

Cela signifie que le SIL représente la dimension correspondant à la probabilité que le système de sécurité puisse remplir correctement les fonctions de sécurité requises pendant un laps de temps précis. La probabilité de défaillance moyenne (PFD ou PFH) baisse selon un facteur de 10 par niveau de sécurité. **[48].**

Il n'y a pas de recette toute faite. Les normes proposent des méthodes différentes pour l'allocation du SIL mais n'imposent pas de règle. Le choix dépend essentiellement de la nature des données d'entrée. Il est préférable de bien utiliser une méthode qualitative (graphe de risque ou matrice de criticité) que d'utiliser une méthode quantitative lorsque les données d'entrée (fréquences d'occurrence d'événements initiateurs, probabilités de défaillance des barrières de sécurité) sont insuffisantes.

En revanche, ces dernières s'appliqueront mieux lorsqu'il y a des données de retour d'expérience quantifiées et lorsque l'organisation du site autorise une analyse en couches fonctionnelles indépendantes. **[49]**

Le graphe de risque consiste à hiérarchiser les niveaux de sécurité à partir de quatre paramètres liés à la conséquence du risque sur le personnel ou l'environnement (C), à la fréquence d'exposition au risque (F), à la possibilité d'éviter le danger (P) et à la probabilité d'occurrence du danger (W).

Les niveaux affectés aux paramètres du graphe constituent la base de l'évaluation du risque.

Une phase de calibrage ou d'étalonnage du diagramme de risque est nécessaire. Elle permet d'adapter les paramètres en prenant en compte les spécificités de l'entreprise et la réglementation.

La difficulté est alors de calibrer le graphe. L'étalonnage des paramètres doit prendre en compte toutes les situations.

Un compromis doit être trouvé entre une échelle trop large et une précision suffisante. En effet, selon les choix de l'analyste, les résultats peuvent rapidement passer d'un niveau d'intégrité à un autre. La classification repose sur une hiérarchisation en six classes d'exigences graduées de « a » à « b » en passant par SIL 1 à SIL 4. La catégorie « a » correspond alors à « aucune exigence particulière de sécurité » tandis que la catégorie « b » correspond à « une situation inacceptable » (le système instrumenté est insuffisant).

Le graphe de risque consiste à hiérarchiser les niveaux de sécurité à partir de quatre paramètres liés à la conséquence du risque sur le personnel ou l'environnement (C), à la fréquence d'exposition au risque (F), à la possibilité d'éviter le danger (P) et à la probabilité d'occurrence du danger (W).

Les niveaux affectés aux paramètres du graphe constituent la base de l'évaluation du risque. **[49]**

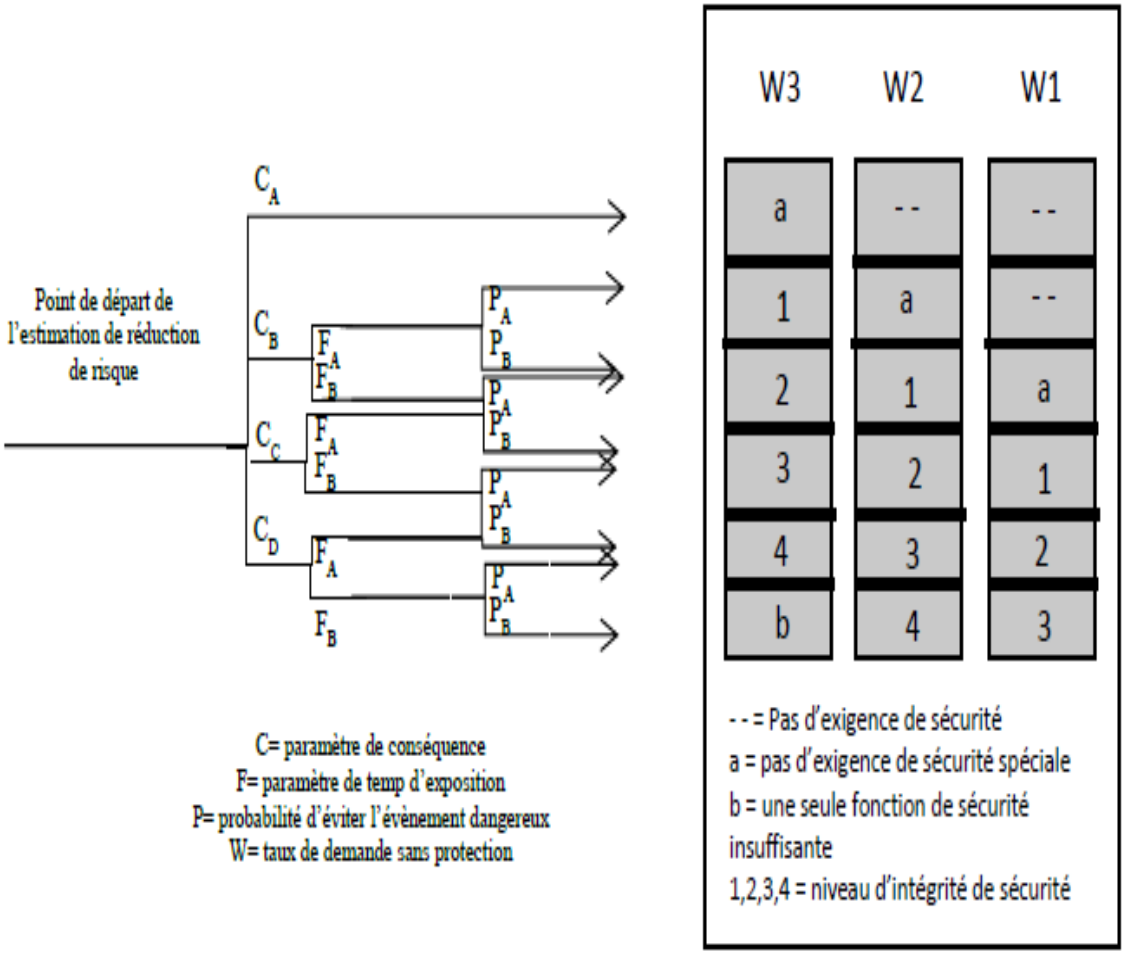


Figure 3.9 : Graphe de risque [49]

Paramètre de risque	niveau	classification	commentaires
Conséquence (C) Nombre d'accidents mortels Ce paramètre peut être calculé en déterminant le nombre des personnes présentes lorsque la zone exposée au danger est occupée. La vulnérabilité est : **V = 0 .01** faible déversement ou dégagement de matériaux inflammables ou toxiques **V = 0.1** important déversement ou dégagement des matériaux inflammables ou toxiques. **V = 0.5** comme ci-dessus, mais aussi une haute probabilité d'incendie ou matériaux très toxiques **V = 1** rupture ou explosion	**CA** **CB** **CC** **CD**	Lésion mineure Plage de 0.01 à 0.1 Plage de ≥ 0.1 à1.0 Plage ≥ 1.0	**1 :** le système de classification a été établi pour traiter les blessures infligées aux personnes ou les décès. **2 :** pour l'interprétation de CA, CB, CC, et CD, il convient de tenir compte des conséquences de l'accident et du rétablissement normal
Occupation (F) Ce paramètre est calculé en déterminant la durée proportionnelle pendant les périodes normales de travail.	**FA** **FB**	Exposition rare à plus fréquente dans la zone dangereuse. L'occupation est inférieure à 0.1. Exposition fréquente à permanente dans la zone dangereuse	**3 :** voir commentaire 1 ci-dessus
Probabilité (P) pour que l'événement dangereux Soit évité en cas de défaillance du système de protection	**PA** **PB**	***A**doptée si toutes les conditions de la colonne 4 sont remplies. ***A**doptée si toutes les conditions ne sont pas remplies	**4** :il convient de choisir PA uniquement si toutes les conditions suivantes sont variées : des moyens sont prévus pour l'avertissement de la défaillance du SIS ; des moyens indépendants sont prévus pour arrêter le procédé. Le temps entre le moment d'avertissement et le moment de l'accident dépasse 1h ou est finalement suffisant pour entreprendre les actions nécessaires
Taux de sollicitation (W) le nombre de fois par an où l'événement dangereux est susceptible de se produire en l'absence d'un SIS. Pour le déterminer, il est nécessaire de considérer toutes les sources de défaillance susceptibles de provoquer un événement dangereux. Il faut accorder une confiance limitée aux performances et à l'intervention du système de commande. Les performances qui peuvent être revendiquées si le système de commande n'est pas conçus et entretenu conformément à la CEI 61511 sont limitées à des valeurs inférieures aux plages de performances SIL 1	**W1** **W2** **W3**	Taux de sollicitation inférieur à 0.1D par an Taux de sollicitation entre 0.1D et D par an. Taux de sollicitation entre D et 10D par an. Pour des taux de sollicitation supérieure à 10D par an une intégrité plus élevée est nécessaire	**5** : le but du facteur W est d'estimer la fréquence du danger qui apparaît sans l'ajout du SIS. Si W est très élevé, Le SIL doit être déterminé par une autre méthode ou le graphe de risque doit être étalonné une nouvelle fois. Il convient de noter qu'il est possible que les méthodes utilisant des graphes de risque ne constituent pas la meilleure approche dans le cas d'application fonctionnant en mode continu. Se reporter au paragraphe 3.2.4.3 de la CEI 61511 - 1. **6** : il convient de déterminer la valeur de C à partir de critères propres à la société concernant de risque tolérable en tenant compte d'autres risques auxquels des personnes peuvent être exposées.

Table 3.3 table de calibrage

Paramètre	Niveau	Classification
Gravité des conséquences	CA	Blessure mineure
	CB	Blessure sérieuse ou victime
	CC	Plusieurs victimes
	CD	Grand nombre de victimes
Fréquence et temps d'exposition au phénomène dangereux	FA	Rare
	FB	Fréquent
Possibilité d'éviter le phénomène dangereux	PA	Possible
	PB	Invraisemblable
Probabilité d'apparition d'un accident	W1	Très faible probabilité
	W2	Faible probabilité
	W3	Forte probabilité

Table 3.4: Les intégrités de sécurité du graphe de risque [49]

3.6.4 Application

Vu notre installation les niveaux de calibrage sont :

Conséquence (C) :

Rupture ou explosion c'est à dire la vulnérabilité est : V = 1 $\Longrightarrow$ C_D

Occupation (F) :

Exposition fréquente à permanente dans la zone dangereuse $\Longrightarrow$ F_B

Probabilité(P) :

On considère que l'explosion est soudaine. On suppose donc que les gens n'ont pas la possibilité de détecter ce phénomène et ne sont pas bien préparés pour se mettre dans un endroit sûr. Toutes les conditions ne sont pas remplies $\Longrightarrow$ P_B.

Taux de sollicitation(W) :

Taux de sollicitation entre 0.1D et D par an $\Longrightarrow$ W_2

Commentaire :

D'après le graphe de risque le niveau de SIL requis pour diminuer la probabilité d'explosion de la presse hydraulique SAM 500 est **SIL4**.

3.6.4.1 Recherche de l'architecture

Comme il est présenté dans le 2éme chapitre (2.2 comment choisir le SIS convenable à partir du SIL ?) nous allons utiliser le même principe pour déterminer l'architecture de notre SIS en commençant par le calcul des λ_D et λ_S arrivant à calculer λ_{DD} et **SFF**. Nous allons utiliser le tableau du système A (voir tableau 2.2). Selon la banque des données spécifique à notre presse hydraulique SAM 500 nous avons :

λ=0.376.10^{-3}h$^{-1.}$

Fr=10^{-5}

DC = 0.6

(Voir la référence **[50]**)

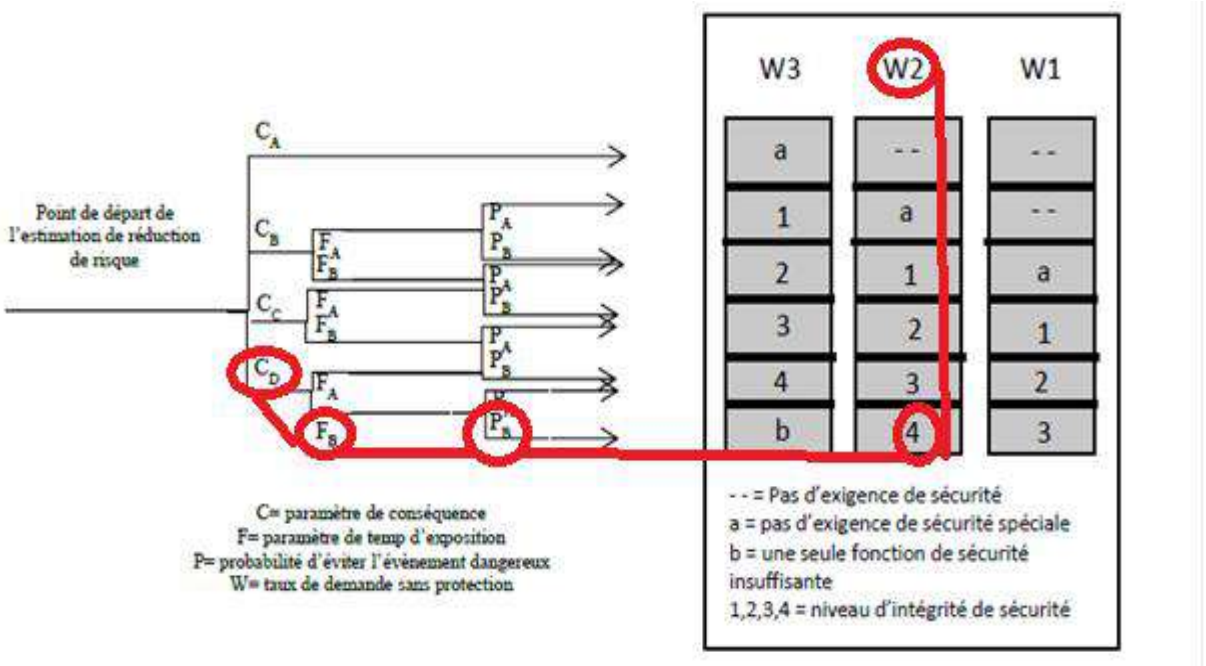


Figure 3.10 : détermination du SIL d'après le graphe de risque [48]

3.6.4.2 Application numérique

$$\lambda = \lambda_S + \lambda_D \quad \textbf{4.1}$$

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \quad \textbf{4.2}$$

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \quad \textbf{4.3}$$

$$\lambda_{DU} = (1 - DC) \cdot \lambda_D \quad \textbf{4.7}$$

Rappelons l'équation (**4.1**) et supposons que $\lambda_S = \lambda_D$ on obtient

$$\lambda_S = \lambda_D = \frac{\lambda}{2} = 0.188.10^{-3}h^{-1} \quad \textbf{4.4}$$

Utilisons les équations **($\lambda_{DD} = DC.\ \lambda_D$)** et (**4.4**) ; Alors on obtient

: $\lambda_{DD} = 0.1128.10^{-3}h^{-1}$ **4.5**

Donc à l'aide de l'équation (**2.2**) la SFF sera alors :

$$SFF = \frac{0.188.10^{-3} + 0.1128.10^{-3}}{0.376.10^{-3}} = 0.8 \quad \textbf{4.6}$$

Donc : SFF = 80% sans oublions que nous avant trouver **SIL = 4.**

Selon le tableau du système A et en utilisons les équations (**2.1**) et (**4.6**) on résulte que :

M = 2 $\Longrightarrow$ N - K = 1 avec K = 1 $\Longrightarrow$ **N = 3**

L'architecture sera donc :1oo3.

Commentaire :

L'architecture 1oo3 veut dire que notre circuit hydraulique de la presse hydraulique SAM 500 nécessite trois canaux de détection (trois capteurs de pression) afin d'assurer la couverture du danger qui est la rupture ou l'explosion des conduites de cette machine.

Il suffit qu'un seul de ces trois capteurs fonctionne pour que la probabilité de la survenance de l'accident sera diminuée. C'est la redondance matérielle.

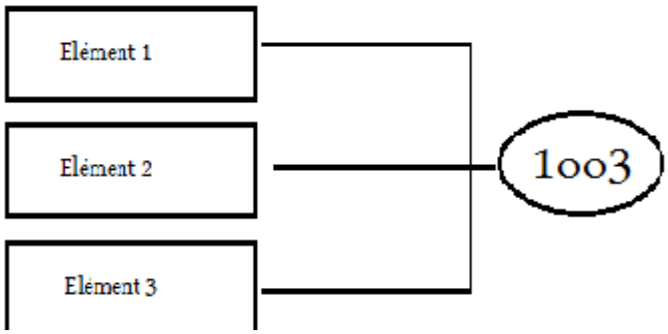


Figure 3.11 : L'architecture 1oo3

3.6.5 vérification des résultats

Le SIS est considéré comme une couche de protection globale où les capteurs de notre SIS jouent le rôle d'un surveillant électronique qui veille et contrôle la pression d'huile dans les conduites, mais rien est parfait, ce SIS est exposé aux défaillances qui peuvent provoquer la non détection des anomalies.

Cette probabilité de défaillance connue par la PFD et la PFH.

D'après les équations (**2.3**) et (**2.4**), la probabilité de défaillance du SIS est la même des capteurs (la non détection) présent dans notre SIS. C'est à dire la connaissance des λDU des capteurs c'est à peu près la connaissance des PFDSIS.

Dans cette partie nous allons calculer la PFDSIS de mon SIS et la comparer avec la probabilité de la survenance du danger initiale (avant l'implantation du SIS) afin d'éclairer le rôle et l'importance de notre SIS.

Calcul de laPFDSIS **:**

Rappelons la formule (**2.3**) et (**4.7**), le PFDSIS dans ce cas est :

DONC $$PFD_{SIS} = \prod PFD_{capteur}$$ **4.8**

AVEC $$PFD_{SIS} = \lambda_{DU}^{1}.\lambda_{DU}^{2}$$ **4.9**

ALORS $$\lambda_{DU} = (1-0.6).0.188.10^{-3} = 0.0752.10^{-3}h^{-1}$$ **4.10**

$$PFD_{SIS} = 0.225.10^{-3}h^{-1}$$ **4.11**

Calcul du nouveau SIL

Utilisons la formule (**2.5**) et (**4.7**), la nouvelle PFDSIS sera

$$PFD_{SIS}^{nouveau} = \frac{10^{-5}}{0.225.10^{-3}} = 4.43.10^{-2} \qquad \textbf{4.12}$$

A l'aide du tableau des niveaux de SIL (voir tableau **2.1**), le résultat de l'équation (**4.12**) veut dire que le SIL requis dans ce cas est **SIL2**.

3.7 Conclusion

L'étude est appliquée sur la presse hydraulique SAM 500, presse à balle semi-automatique où nous avons expliqué le rôle principal de cette machine et son principe de fonctionnement sélectionnant les risques qui peuvent être présentés par cette presse. Basant sur le risque le plus grave (explosion ou rupture des conduites) nous avons étudié la situation par la méthode graphe de risque pour définir le niveau de SIL requis afin de diminuer ce danger.

Nous avons trouvé que le SIL requis après l'implantation du SIS est inférieur à celui d'avant, qui veut dire que la probabilité pour que le circuit soit exposé à l'explosion est diminuer presque à sa moitié.

Chapitre 4 : Proposition

4.1 Proposition de l'architecture du SIS

D'après l'étude de notre circuit nous allons proposer une schématisation possible de l'installation qui se compose des trois capteurs de pression (DC = 0.6), amplificateur, une unité logique et une électrovanne.

Le principe de fonctionnement est le suivant :

Le capteur de pression mesure la pression d'une façon permanente. L'amplificateur transforme les mesures de la grandeur « Bar » à un signal électrique ; l'unité logique reçoit ces signaux et les analyser en les comparant par un seuil maximum de pression. Dans le cas où la pression atteint sa valeur maximale, L'unité logique envoie un signal électrique spécifique à l'électrovanne pour qu'elle s'ouvre.

Les trois canaux identiques fonctionnant en parallèle. Il est donc nécessaire que chacun des canaux subisse une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande émanant de l'EUC. Selon l'hypothèse de mise en état de sécurité, le SIS conduit l'EUC vers un état sûr dans le cas de détection de défaillances dangereuses dans les trois canaux.

Le schéma ci-dessous présente une proposition de L'implantation du SIS (voir figure 5.1)

1. Sous-système « Eléments d'entrée (S) » : constitué d'un ensemble d'éléments d'entrée (Capteurs, détecteurs) qui surveillent l'évolution des paramètres représentatifs du comportement de l'EUC (température, pression, débit, niveau...).

2. Sous-système « Unité Logique (LS) » : comprend un ensemble d'éléments logiques (PLC, API) qui récoltent l'information en provenance du sous-système S et réalisent le processus de prise de décision qui s'achève éventuellement, si l'un des paramètres dévie au-delà d'une valeur-seuil, par l'activation du sous-système FE.

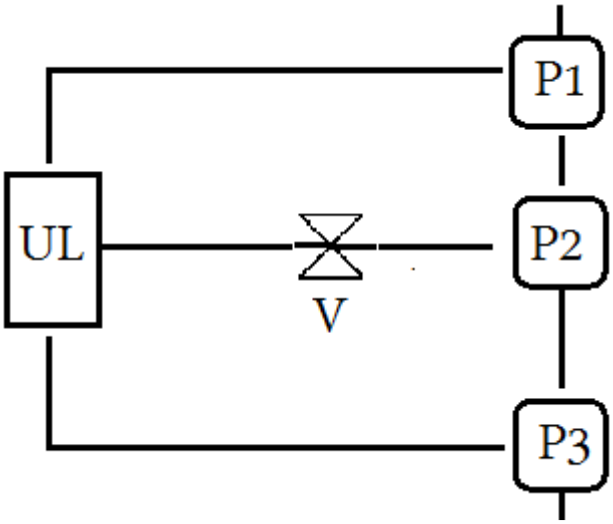


Figure 4.1 : Schématisation de l'implantation du SIS

3. Sous-système « Eléments Finaux (FE) » : agit directement (vanne d'arrêt d'urgence) ou indirectement (vanne solénoïdes, alarme) sur le procédé pour neutraliser sa dérive en le mettant, en général, dans un état sûr.

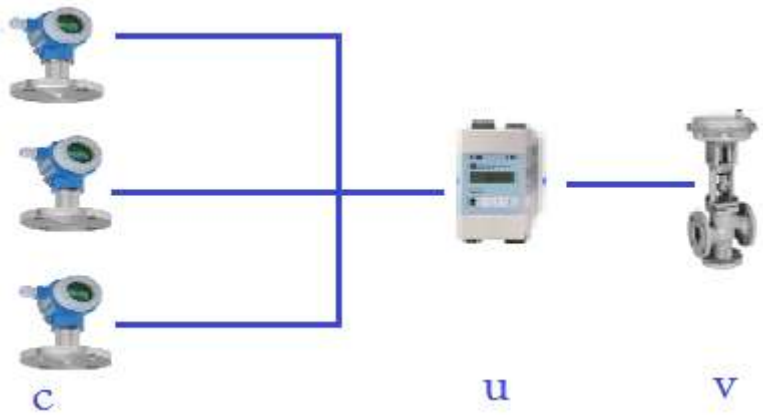


Figure 5.2: Architecture finale

4.2Concernant la presse SAM 500

Mesures de sécurités fondamentales pour la maintenance et la remise en état : Observer les intervalles d'inspection et de maintenances stipulées dans les instructions de service.

Respecter les consignes de maintenance, de nettoyage et de réparation des différents composants stipulées dans les présentes instructions de service.

Avant d'exécuter tout travail de maintenance, de nettoyage ou de réparation interdite à toute personne non habilitée l'accès à la zone de travail de la machine.

Installer un panneau pour signaler les travaux de maintenance, de nettoyage ou de réparation.

Avant d'exécuter tout travail de maintenance, de nettoyage ou de réparation mettre la machine hors circuits placer le sectionneur sur « **0** »et le cadenassé. Avant d'exécuter tout travail de maintenance, de nettoyage ou de réparation s'assurer que les pièces de la machine à manipuler sont refroidies (température ambiante) et sont immobilisées.

Éliminer dans les règles de l'art les lubrifiants Les liquides de refroidissement et les produits de nettoyage dangereux pour l'environnement

Conclusion générale

Arrivant à conclure notre travail, les SIS peuvent remplacer l'être humain dans la matière de contrôle et surveillance pour l'objectif de compléter la fiabilité humaine. Mais le SIS reste toujours un élément qui admet les modifications, les améliorations et les mis à jours. Rien n'est parfait, la machine reste un objet que l'homme la manipule soit d'une façon directe ou indirecte.

Dans ce mémoire nous avons traité le phénomène de contrôler un simple circuit hydraulique par un SIS afin de diminuer la probabilité de la survenance d'une explosion ou rupture des conduites .

.

Références Bibliographiques

[1] Norme CEI 61508, nouvelle version. Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité. Parties 1 à 7,. Commission Electrotechnique Internationale, Genève, Suisse. 2009

[2] FARES INNAL. 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 Docteur de L'Université BORDEAUX 1.

[3] IEC61508, Functional safety of electrical/electronic/programmable electronic (e/e/pe) safety related systems. International Electro Technical Commission (IEC), 1998.

[4] IEC61511, Functional safety: Safety instrumented systems for the process industry sector. International Electrotechnical Commission (IEC), 2000.

[5] Mechri.W, Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis. Doctorat thesis, Tunis université, Ecole Nationale d'Ingénieurs de Tunis,2011

[6] Mkhida, A, Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'Intelligence. PhD thesis, Nancy Université, Institut National Polytechnique de Lorraine, France, 2008.

[7] Commissariat à l'Energie Atomique (CEA). *Méthode Organisée et Systémique d'Analyse des Risques.* CEA, France.

[8] J. L. Le Moigne. La théorie du système général – Théorie de la modélisation. PUF, Paris, France.7.

[09] Exida. Safety Equipment Reliability Handbook. Second Edition.

[10] Villemeur, A, Evaluation de la fiabilité, disponibilité et maintenabilité des systèmes réparables : la méthode de l'Espace des Etats. Number 2. Eyrolles, 1987

[11] Desroches, A., Leroy, A., and Vallée, F. La gestion des risques : principes et pratiques, volume 1.Lavoisier Franc 2003.

[12] OHSAS18001, Système de management de la santé et de la sécurité au travailSpécification - BSI, Afnor, 1999.

[13] Mazouni, M.-H, Pour une Meilleure Approche du Management des Risques : De la modélisation Ontologique du Processus Accidentel au Système Interactif d'Aide à la Décision

[**14**] Les invariants de l'analyse préliminaire des risques, Qualita. 685-694. EN_954-1. Safety of machinery. Safety 1997

[**15**] Mazouni, M. H., D. B. Charreton, et al. Proposal of a generic methodology to harmonize Preliminary Hazard Analyses for guided transport. IEEE International Conférence. 2007.

[16] Villemeur, A, Sûreté de fonctionnement des systèmes industriels. Number 2. Eyrolles, 1998.

[17] Farmer., F. R., Siting criteria: a new approach. Atom, chapter 128, page 152166, 1967.

[18] INERIS-DRA35. Outils d'analyse des risques générés par une installation industrielle. INERIS, Direction des Risques Accidentels. France

[19] ISO/CEI Guide 51. Aspects liés à la sécurité : Principes directeurs pour les inclure dans les normes. Organization International de normalization (ISO).

[20] ILO-OSH 2001. Guidelines on occupational safety and health management systems. BIT.

. PhD thesis, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France, 2008.

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

[22] ISA, Application of Safety Instrumented Systems for the process Industries, ANSI / ISA-S84.01, 1996.

[23] Innal, F, Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances Analyse critique de la norme CEI 61508. PhD thesis, Université Bordeaux I, France, 2008.

[24] Rauzy, A., Dutuit, Y., and Signoret, J.-P, Assessment of safety integrity levels with fault trees. In ESREL Estoril, Portugal, 2006.

[25] Sallak, M, Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité. PhD thesis, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France, 2007.

[26] EN50126, Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS), 1999.

[27] EN50128, Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems, 2001.

[28] EN50129, Safety related electronic systems for signalling, 1998.

[29] A. E. Summers, Setting a new standard of the safety instrumented systems, Chemical Engineering, 2000.

[30] ISA 84.00.01–2004, Functional Safety Instrumented Systems for the Process Industries, Parts 1–3, 2004.

[31] ARC Advisory Group, Siemens Process Safety Systems Deliver Modern Features on a Proven Platform, October 2005.

[32] Charpentier, P. Artchitecture d'automatisme en sécurité des machines : Etude des conditions de conception liées aux défaillances de mode commun. PhD thesis, Nancy Université, Institut Nationnal Polytechnique de Lorraine, France. 2002.

[33] S.HADDAD, Evaluation et Optimisation des Performances des Systèmes Instrumentés de Sécurité pour une Meilleure Maîtrise des Risques. Mémoire de Magister de l'université Hadj Lakhdar de Batna ; 2012.

[34]. Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis, Thèse de Docteur de L'Université de Tunis El Manar ; 2011

[**35**] SINTEF. Reliability prediction methods for safety instrumented systems, PDS method handbook. 2006 edition; 2006.

[**36**] M.A. Lundteigen, et M. Rausand, Spurious activation of safety instrumented systems in the oil and gas industry: basic concepts and formulas. Reliability Engineering and System Safety, 93:1208–1217; 2008.

[**37**] M.A Lundteigen, Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation. PHD-theses at NTNU; 2008.

[38] L. Beckman, Easily assess complex safety loops. Chem Eng Progr 2001.

[39] W. Goble, H. Cheddie. Control system safety evaluation and reliability. US: ISA; 1998.

[40] La norme CEI 61508 [CEI 00]. 2014.

[41] Sami Rekik. Formater. Circuits hydrauliques. Conception et maintenance. Page 99, 2015.

[42] A. Schmitt Ing.dipl.Chef des Cours d'Hydraulique G.L. Rexroth GmbH. Lohr am Main. Le cours d'Hydraulique. Ouvrage d'enseignement et d'informations sur l'Hydraulique .1991.

[43] L. CUVELIER. D'après à le guide des automatismes à la puissance de l'hydraulique contrôlée par l'électronique. 2013.

[44] L. CUVELIER. Rôle de l'hydraulique proportionnelle. Hydraulique proportionnelle. 2012.

[45] L. CUVELIER. Hydraulique proportionnelle. Distributeurs à commande proportionnelle. D'après ? Le guide des automatismes. 2013.

[46] SCARIA industrie. Notice d'instruction originale. Manuel d'utilisation SAM 500, 2017.

[47] SCARIA industrie. PRESSE A BALLE VERTICALE type SAM 500, 2017.

[48] Endress and Hauser people for process automation. Sécurité fonctionnelle. Sil les systèmes instrumentés de sécurité dans l'industrie des process. 2014.

[49] MESURES 813. Dossier sécurité fonctionnelle. Trois méthodes pour déterminer le niveau de sécurité sil. 2014.

[50] OREDA participants. OREDA Project Manager. OREDA. Offsher reliability Data HandBook, 2002