*

République Algérienne Démocratique et Populaire

Ministère de l'enseignement et de la Recherche Scientifique



Université Yahia Fares De Médéa

Faculté de Technologie

Département de génie des procédés et environnement

Projet de Fin D'étude

Soumis Pour l'obtention du diplôme de Master HSI

Spécialité : Hygiène et sécurité industrielle

THEME

LES PARAMETRES D'ALLOCATIONS DE NIVEAU DE CONFIANCE DANS UN SYSTEME INSTRUMENTE DE SECURITE

PRESENTE PAR :

- ***BELHADJ Aymene***
- ***BENSALEM Hicham***

DIRIGE PAR

Dr . RAHMANI Ahmed Cherif

Promotion : 2024-2025

Remerciement

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui m'ont soutenu et accompagné durant la réalisation de ce projet de fin d'études.

Je remercie tout particulièrement Monsieur Ahmed Cherif Rahmani, mon encadrant, pour sa disponibilité, son accompagnement constant, ses conseils avisés et sa bienveillance tout au long de ce travail. Son expertise et ses orientations ont été d'une grande aide.

Je souhaite également adresser mes sincères remerciements à l'ensemble des enseignants et au personnel de nôtre université de MÉDÉA pour la qualité de la formation dispensée et leur contribution à mon parcours académique.

Enfin, je remercie mes camarades, amis et toutes les personnes qui, de près ou de loin, ont contribué à la réussite de ce projet.

dedicace

Un hommage particulier va à

mes parents, pour leur amour

inconditionnel, leur patience,

leur soutien moral et matériel,

ainsi que pour leur confiance en

moi tout au long de ces années.

Sans eux, rien de tout cela

n'aurait été possible.

Résume :

Ce projet de fin d'études est consacré à l'étude du Système Instrumenté de Sécurité (SIS), un ensemble de capteurs, de logique de traitement et d'actionneurs automatisés mis en œuvre pour détecter des conditions dangereuses et initier des actions correctives visant à ramener le système dans un état sûr.

Dans le cadre de ce travail, une attention particulière a été portée à l'allocation du niveau de confiance, aussi appelé Safety Integrity Level (SIL), qui permet de quantifier la fiabilité exigée des fonctions de sécurité. Par exemple, une fonction de coupure d'urgence d'un compresseur à haute pression, en cas de surpression détectée, ce qui signifie qu'elle doit réduire le risque avec un taux de défaillance acceptable dans une fourchette bien définie selon la norme IEC 61508.

L'analyse a permis d'identifier les fonctions critiques, de calculer le niveau de risque associé à chaque scénario dangereux et de recommander un SIL adapté en tenant compte de la gravité, de la fréquence et des moyens de protection existants.

Mots clés : systéme insteumenté de sécurité, niveau d'integrité de sécurité, analyse des risques, norme CEI 61508

Abstract :

This final year project is dedicated to the study of the Safety Instrumented System (SIS), a set of sensors, processing logic, and automated actuators implemented to detect hazardous conditions and initiate corrective actions to bring the system back to a safe state.

Particular attention was given to the allocation of the Safety Integrity Level (SIL), which quantifies the required reliability of safety functions. For example, an emergency shutdown function for a high-pressure compressor in the event of detected overpressure must reduce the risk to an acceptable level within a well-defined failure rate range, as specified by the IEC 61508 standard.

The analysis made it possible to identify critical functions, assess the risk level associated with each hazardous scenario, and recommend an appropriate SIL based on the severity, frequency, and existing protection measures.
Key word: safety insrumented system , safety integrity level , risk analysis , CEI 61508 standard

الملخص:

يُكرَّس هذا المشروع كجزء من مشروع التخرج لدراسة نظام السلامة الآلي (SIS)، وهو مجموعة من أجهزة الاستشعار، ومنطق المعالجة، والمشغلات الأوتوماتيكية التي تُستخدم لاكتشاف الحالات الخطرة واتخاذ الإجراءات التصحيحية لإعادة النظام إلى حالة آمنة.

تم التركيز بشكل خاص على تخصيص مستوى سلامة الأداء (Safety Integrity Level – SIL)، الذي يُستخدم لقياس مدى موثوقية وظائف السلامة المطلوبة. فعلى سبيل المثال، يجب أن تقوم وظيفة الإيقاف الطارئ لضاغط عالي الضغط في حالة اكتشاف ضغط زائد، بخفض مستوى الخطر إلى مستوى مقبول ضمن معدل أعطال محدد بدقة، وفقًا لمعيار IEC 61508.

لقد أتاح التحليل تحديد الوظائف الحرجة، وتقييم مستوى المخاطر المرتبطة بكل سيناريو خطِر، والتوصية بمستوى SIL مناسب بناءً على درجة الخطورة، وتكرار الحدوث، ووسائل الحماية الموجودة.
الكلمات المفتاحية :نضام السلامة المجهز بالادوات،مستوى سلامة الأداء ، تحليل المخاطر، المعيار CEI 61508

Sommaire

Remerciement
Dédicaces

Introduction.....- 1 -

Chapitre I: Notion de base et gestion des risques

1 Concepts et définition.....- 3 -
1-1 Notion de danger :.....- 3 -
1-2 Notion de risque.....- 3 -
1-3 Notion de sécurité.....- 5 -
1-4 Notion d'ALARP et de risque tolérable : .....- 5 -
1-5 Sécurité fonctionnelle .....- 7 -
2. La gestion des risques: .....- 7 -
2-1.analyse du risque :.....- 8 -
Étapes d analyse du risque :.....- 9 -
3- L'évaluation des risques:.....- 10 -
3.1. L'importance de l'évaluation des risques: .....- 10 -
3-2 L'évaluation des risques en 5 étapes: .....- 11 -
3 - 3 Méthodes d'analyse des risques : .....- 15 -
5. L'arbre des évènements (ADE) .....- 15 -
5-1 Présentation de la méthode ADE:.....- 15 -
5-2 Principe de la méthode ADE:.....- 15 -
5- 3- Déroulement:.....- 16 -

Chapitre II: Système instrumenté de sécurité

1-Normes relatives au système instrumenté de sécurité :.....- 21 -
1-1 Norme CEI 61508.....- 21 -
1-2 Norme CEI 61511.....- 23 -
1-3 La norme CEI 62061 :.....- 24 -
1-4 La norme ECI 61513 :.....- 24 -

1.5 Norme EN 50126 .....- 25 -
2. Définitions et concepts relatifs aux SIS : .....- 25 -
2-1 Définitions .....- 25 -
2-2 Exigences de sécurité des SIS en accord avec la norme CEI 61508.....- 27 -
2-3 Compositions d'un SIS : .....- 29 -
A. Capteur.....- 30 -
B. Unité de traitement .....- 30 -
C. Actionneurs .....- 30 -
Composition d'un SIS en fonction des taches a accomplir. .....- 31 -
2-4 Redondance au sein d'un S.I.S.....- 32 -
2-5 Fonction instrumente et de sécurité. .....- 34 -
2-5 Propriétés d'un SIS .....- 36 -
2-6 Intégrité de sécurité d'un SIS .....- 37 -
2-7 Modes de fonctionnement des SIS et paramètres cibles de défaillances .- 37 -
Notion de niveau d'intégrité de sécurité (SIL). .....- 38 -
2-8 Classification des défaillances des SIS :.....- 39 -
2.8.1- Classification retenue La norme CEI61508 .....- 39 -
3-8-2Classification proposée par SINTEF.....- 43 -
3-Définitions et classification des activations intempestives des SIS :.....- 44 -
2- Causes des activations intempestives : .....- 46 -
Chapitre III : Allocation De Niveau De Confiance des SIS
Niveau de confiance des SIS .....- 63 -
Exemple de Redondance appliqué sur des détecteurs.....- 65 -
4- Niveau intégrité de sécurité (SIL) : .....- 66 -
5- Comment choisir le SIS convenable à partir du SIL ? .....- 68 -
Chapitre IV: Recommaandation
Tests de fonctionnement :.....- 70 -
Exemples de configurations : .....- 71 -
3-la contribution de SIS dans la prévention et protection du risque .....- 71 -
Conclusion .....- 76 -

Liste des tableaux est des figures

N° :	Liste des Figures	Page
01	Figure 1. 1:Relation entre les notions de danger et de risque	04
02	Figure 1. 2: Courbe de Farmer [FARMER, 1967]	04
03	Figure 1. 3: Modèle ALARP	06
04	figure 1.4. les étapes d'analyses	09
05	Figure 1.5 les étapes d'analyses	11
06	Figure 1.6 : Schéma d'n AdE avec des barrières de sécurités	16
07	Figure 1.7 Arbre d'évènement défaillance du système de refroidissement.	20
08	Figure 2.1 montre la norme CEI 61508	23
09	Figure 2.2 relation entre la 61508et la 61511	24
10	Figure 2.3 exemple d'un SIS :	26
11	Figure 2-4 Schémas d'un sis simple	29
12	Figure 2.5 schéma d'un SIS effectuant plusieurs tâches	31
13	Figure2.6fonction instrumenté de sécurité	35
14	Figure2.7exemple de fonction instrumenté de sécurité	36
15	Figure2.8Classification des défaillances selon leurs causes	40
16	Figure 2.9 typologie des défaillances selon la norme CEI 61508	41
17	Figure 2.10 classification des défaillances selon SINTEF	43
18	Figure 2-11 les différents types des activations intempestives	46
19	Figure 2-12 Les décisions et les facteurs qui influencent les activations intempestives.	47
20	Figure 4.1 : Concept de couches de protection	71
21	Figure 4.2: Concept de couches de protection	72

N° :	Liste des Tableaux	Page
01	Tableau 1.1 identification des fonctions de sécurité	18
02	Tableau 2. 1 les différents niveaux de SIL définis par la normeCEI61508	39
03	Tableau2.2.sous système type A[7]	68
04	Tableau2.3.sous système type B	69

Introduction

Introduction :

Introduction :

Les établissements industriels deviennent techniquement de plus en plus complexes et le potentiel de danger s'accroit en conséquence si les flux de danger ne sont pas convenablement contrôlés . Lorsque les systèmes industriels présentent des risques potentiels pour les personnes, l'environnement ou les biens, la gestion de ces risques nécessite de mettre en place des mesures de maitrise des risques aussi communément appelées barrières de sécurité. Celles-ci participent soit a la prévention en minimisant la probabilité d'apparition du risque, soit a la protection pour limiter les conséquences d'un dysfonctionnement.

Les moyens a mettre en œuvre pour réduire les risques sont nombreux et varies.

Parmi les équipements s'utilises pour réduire le risque, le système de contrôle de procède connu sous le nom BPCS (Basic Procès Controller System). Ce système est conçu pour surveiller, contrôler et maintenir le procès dans un état de fonctionnement normale et sur. Cependant, la défaillance du BPCS peut être à l' origine d'un scenario d'un accident (événement initiateur).

Les Systèmes Instrumentes de Sécurité (SIS), décrits par les normes IEC 61508 et IEC 61511, jouent un rôle primordial dans la prévention des accidents pouvant survenir dans les systèmes industriels. Ils s'entrent en action lorsque le procès se trouve dans des conditions anormales et qu'une situation dangereuse risque de se développer.

Les SIS sont des associations de capteurs , d'unité de traitement et d'actionneurs , ayant pour objectif de remplir des fonctions de sécurité .

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

Introduction :

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.

Chapitre : I
Notion de base
et gestion des risques

1 Concepts et définition

1-1 Notion de danger :

Selon Desroches [DES 95] [1] et la norme IEC 61508 [IEC 98] [7] le danger désigne une nuisance potentielle pouvant porter atteinte aux personnes, aux biens (détérioration ou destruction) ou a l'environnement Les dangers peuvent avoir une incidence directe sur les personnes, par des blessures physiques ou des troubles de la santé, ou indirecte, au travers de dégâts subis par les biens ou l'environnement.

Le référentiel OHSAS 18001 [OHS 99] [3] définit le danger comme étant une source ou une situation pouvant nuire par blessure ou atteinte a`la santé, dommage a la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments. Soulignons que de nombreux termes sont employés, selon les normes ou les auteurs, autour de la notion de danger et la rendent ambigüe¨. 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.

1-2 Notion de risque

Selon VILLEMEUR [Villemeur, 1998], 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 [OHS18001, 1999] [3], le risque est la combinaison de la probabilité et de /des conséquence(s) de la survenue.

D'une manière générale, le risque peut être considéré comme la combinaison de deux facteurs : la fréquence de l'occurrence de l'évènement dangereux et la gravité de conséquences.

Risque (R) = Probabilité (P) × Gravité (G)

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

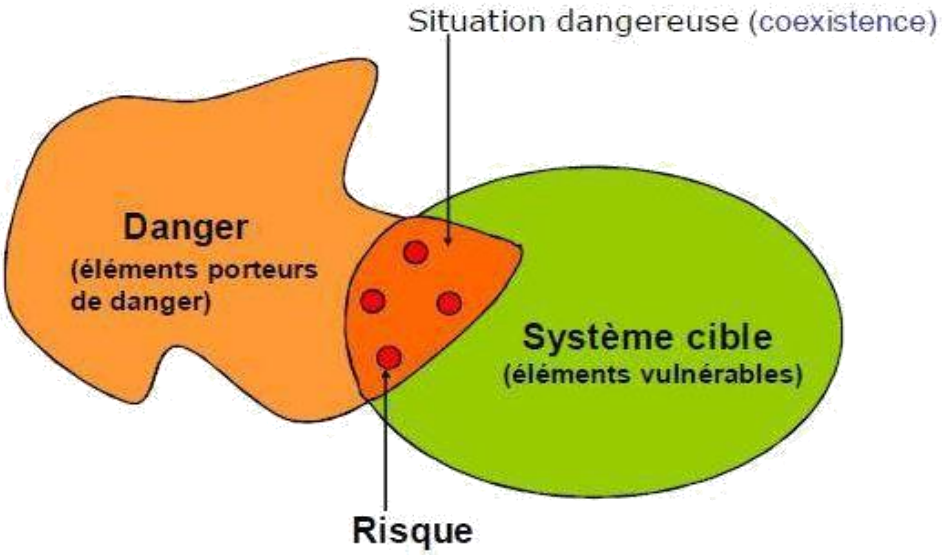


Figure 1. 1:Relation entre les notions de danger et de risque

Le critère de Farmer [Farmer, 1967] permet de définir les notions de risque acceptables et inacceptables (figure 1.2).

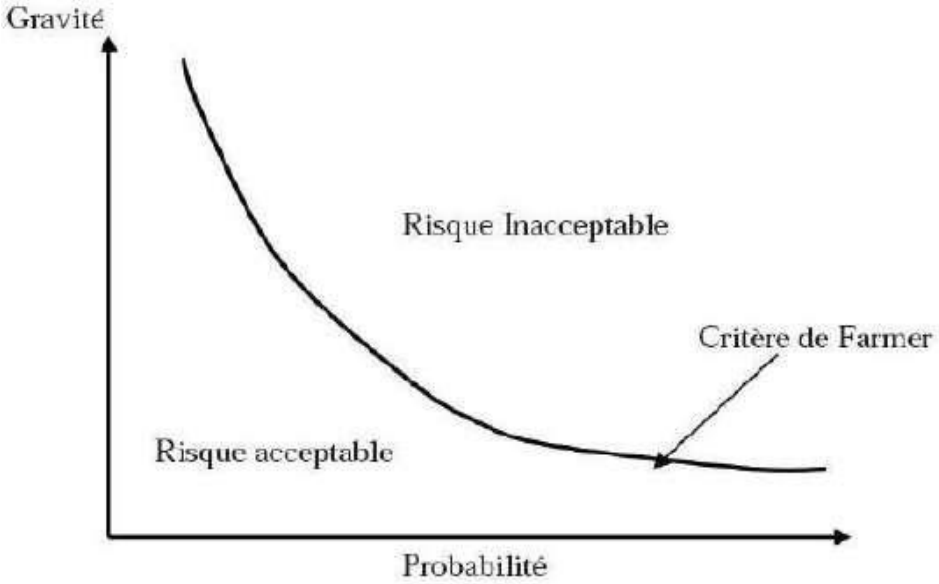


Figure 1. 2: Courbe de Farmer [FARMER, 1967]

1-3 Notion de sécurité

La sécurité est souvent définie par rapport a son contraire : elle serait L'absence de danger, d'accident ou de sinistre. Selon [DES 03], la se curite concerne la non occurrence d'événements pouvant diminuer ou porter atteinte a l'intégrité du système, pendant toute la durée de l'activité de ce dernier , que celle -ci soit reussie, dégradée ou ait échouée. Et suivant le guide ISO /CEI 73 [ISO 02] élaboré par l'ISO sur la terminologie du management du risque , la se curite est l'absence de risque inacceptable, de blessure ou d'atteinte a la sante des personnes , directement ou indirectement, résultant d'un dommage au matériel ou a l'environnement.

Chapitre : Systems instrumente de sécurité 6

1-4 Notion d'ALARP et de risque tolérable :

L'objectif primordial en matière de gestion des risques consiste à les réduire à leurs niveaux les plus bas réalisables tout au long de la durée de vie des installations. Les niveaux les plus bas réalisables sont définis par le principe ALARP (As Low as Reasonably Practicable) ou « aussi bas qu'il est raisonnablement possible de faire ») [Jean-Paul La coursière, 2012], Le modèle ALARP est illustré sur la Figure 1.3. [6]

Son principe est qu'il existe un niveau de risque qui est intolérable, au-delà du quel tout risque n'est justifiable d'aucune manière et est donc inacceptable. Cela correspond à la zone supérieure du schéma (zone I). En deçà de cette zone se situe la zone ALARP (zone II), pour laquelle tout risque peut être accepté si le bénéfice escompté est suffisant.

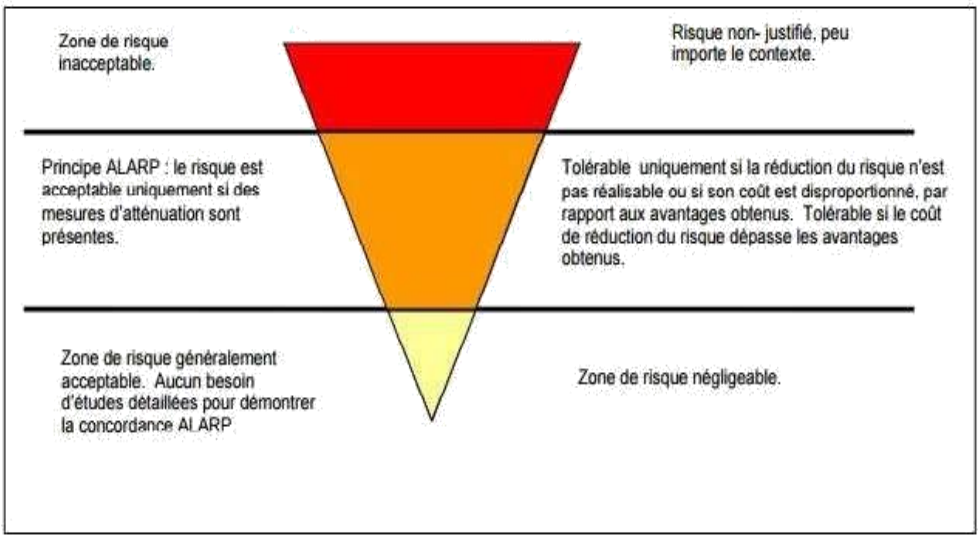


Figure 1. 3: Modèle ALARP

La zone inférieure (zone III) est celle du risque résiduel dont le niveau est considéré comme négligeable et, à ce titre, ne nécessite aucune réduction supplémentaire.

Et donc, le risque n'y est tolérable que :

- si toute réduction supplémentaire du risque est incompatible.
- si la société tire un avantage de l'activité, compte tenu du risque associé.

Pour prendre en compte les concepts ALARP, la mise à niveau d'une conséquence avec une fréquence tolérable peut se faire par l'intermédiaire des classes de risque.

Le tableau 1.1 représente quatre classes de risque pour un certain nombre de conséquences et de fréquences.

Avec :

La classe de risque I : Se situe dans la zone inacceptable ;

Les classes de risque II et III : Sont dans la zone ALARP ; la classe de risque II est juste à l'intérieur de la zone ALARP ;

La classe de risque IV : Se situe dans la zone globalement acceptable.

1-5 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, . . . La norme CEI 61508

[7] dans sa partie 4 définit la sécurité´ fonctionnelle comme un sous ensemble de la sécurité´ globale qui se rapporte au système commandé (EUC, Équipement Under Control) et qui de pend du fonctionnement correct du système électrique, électronique programmable E/E/EP relatif a la sécurité´, des systèmes relatifs a la sécurité´ basées sur une autre technologie et des dispositifs externes de réduction de risque. La norme CEI 61511 [8]

définit la sécurité fonctionnelle comme un sous -ensemble de la se curite ´globale qui se rapporte au processus et au système de commande de processus de base (BPCS, Base Process Control System) et qui de pend du fonctionnement correct du système instrumente de sécurité et d'autres couches de protection . Ce terme diffère de la de´finition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

2. La gestion des risques:

La gestion des risques vise a identifier et anticiper les événements, actions ou inactions susceptibles d'impacter la mise en œuvre de la stratégie dans un horizon donné , définir les options de traitements et s'assurer qu'une option optimale est choisie, mettre en œuvre cette option et contrôler l'efficacité ´de la solution retenue par rapport aux attentes. Plus généralement appliquée aux entreprises, la gestion des risques s'attache a identifier les risques qui pèsent sur les actifs (financiers ou non), les valeurs ainsi que sur le personnel de l'entreprise. La gestion des risques dans l'entreprise passe par

l'identification du risque résiduel, son évaluations, le choix d'une stratégie de maitrise et le contrôle de manière classique, la gestion du risque est un processus itératif qui inclut notamment les phases suivantes :

- -Appréciation du risque (analyse et évaluation du risque)
- Acceptation du risque
- Maitrise ou réduction du risque.

Chapitre : Systems instrumente de sécurité 8

2-1.analyse du risque :

L'analyse du risque est de´finie dans le guide ISO /CEI 51 [ISO 99] [5] comme : « l'utilisation des informations disponibles pour identifier les phénomènes dangereux et estimer le risque » . L'analyse des risques vise tout d'abord a identifier les sources de danger et les situations associe es qui peuvent conduire a des dommages sur les personnes, l'environnement ou les biens . Dans un second temps, l'analyse des risques permet de mettre en lumière les barrières de se curite existante en vue de prévenir l'apparition d'une situation dangereuse (barri ères de prévention) ou d'en limiter les conséquences (barrières de protection). Consécutivement à cette identification, il s'agit d'estimer les risques en vue de les hiérarchiser et de pouvoir les comparer ultérieurement à un niveau de risque juge acceptable .

Étapes d analyse du risque :

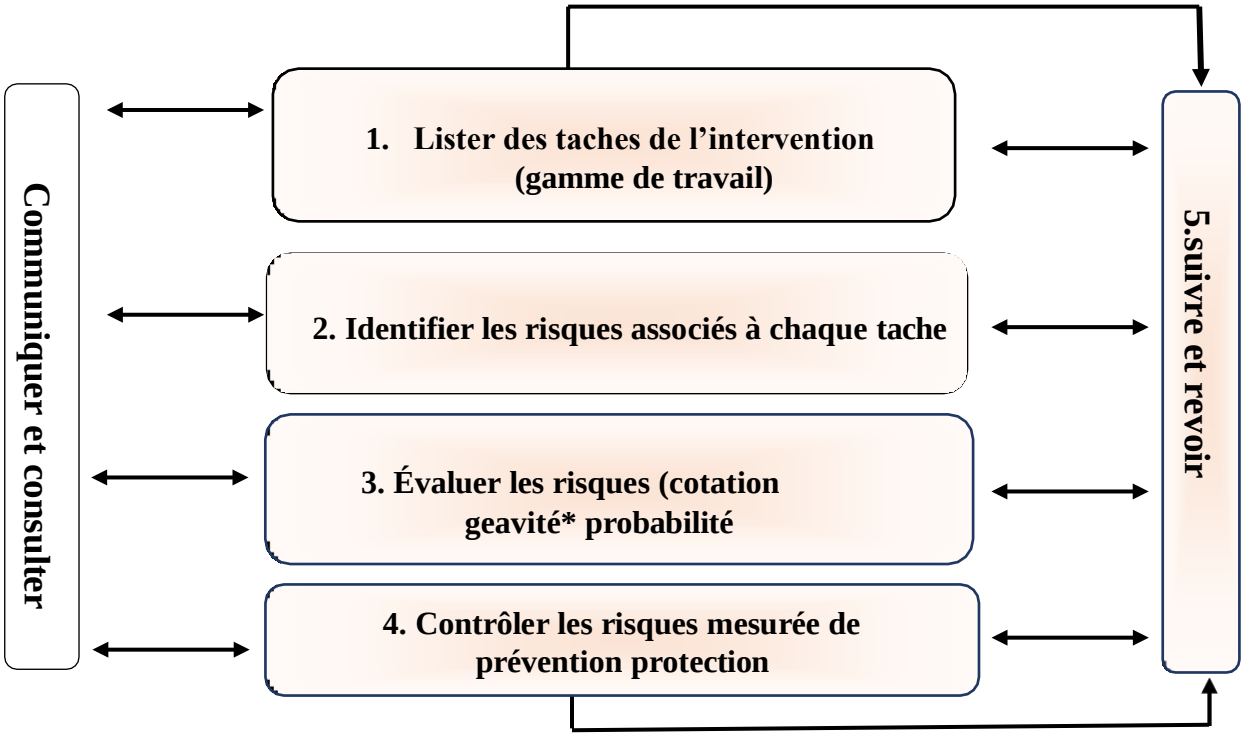


figure 1.4. les étapes d'analyses

Pour améliorer l'efficacité´ et l'objectivité´ d'une analyse de risques ainsi que pour faciliter la comparaison avec d'autres analyses de risque , il est souhaitable de suivre un certain nombre de règles générales . Il est également souhaitable d'effectuer le processus d'analyse de risque conformément a une séquence définie d'étape s.

Le processus détaille´ d'appréciation des risques est compose de 12 étapes distinctes :

1. Définir les objectifs et la portée de l'étude
2. Choisir la méthode d'analyse la plus appropriée
3. Constituer une équipe d'analyse multidisciplinaire
4. Récolter et préparer l'information requise
5. Définir les critères d'analyse

6. Identifier les activités
7. Identifier les risques lies aux activités
8. Évaluer les risques
9. Évaluer l'acceptabilité des risques
10. Maitrise des risques (plan d'action)
11. Documenter l'analyse
12. Mettre en œuvre les recommandations.

3- L'évaluation des risques:

Comme le nom l'indique, il s'agit d'un processus permettant d'évaluer les risques pour garantir la sécurité et la sante des salaries sur leur lieu de travail. Cependant, il faut faire la différence entre les termes "analyse des risques" , où il s'agit simplement de "dépister" les risques, et "évaluations des risques" , évaluation qui permet de classer les risques selon un degré d'importance . L'évaluation des risques est un examen systématique de tous les aspects du travail. Elle sert a établir:

• les causes potentielles d'accidents (et/ou de blessures) ou de maladies;

• les possibilités d'élimination de dangers;

• les mesures de prévention ou de protection à mettre en place pour maitriser les risques .

Lorsqu'un risque a peut-être être identifié, la première chose a` faire est de voir si ce risque peut être élimine. Si une élimination du risque s'avère impossible, le risque devra être maitrisé, c'est-à-dire réduit a un minimum et garde sous contrôle.

3.1. L'importance de l'évaluation des risques:

L'évaluation des risques est la première étape du processus de gestion des risques qui permet de faire comprendre aux personnes concernées, employeur et salaries, quelles sont les mesures a prendre afin d'améliorer la se curite et la sante sur le lieu de travail. Si une évaluation des risques n'a pas été réalisée, un

processus convenable de gestion des risques ne pourra être mis en place et les mesures appropries de prévention ne pourront être adoptées.

De plus, les mesures de prévention mises en place suite a une évaluation des risques peuvent servir à diminuer les couts engendres par les accidents et les maladies professionnelles.

L'évaluation des risques me ne donc aussi a une meilleure organisation de l'entreprise, ce qui signifie un gain de productivité et une augmentation de la qualité

3-2 L'évaluation des risques en 5 étapes:

Les cinq étapes d'évaluation des risques sont schématise dans la figure suivante:

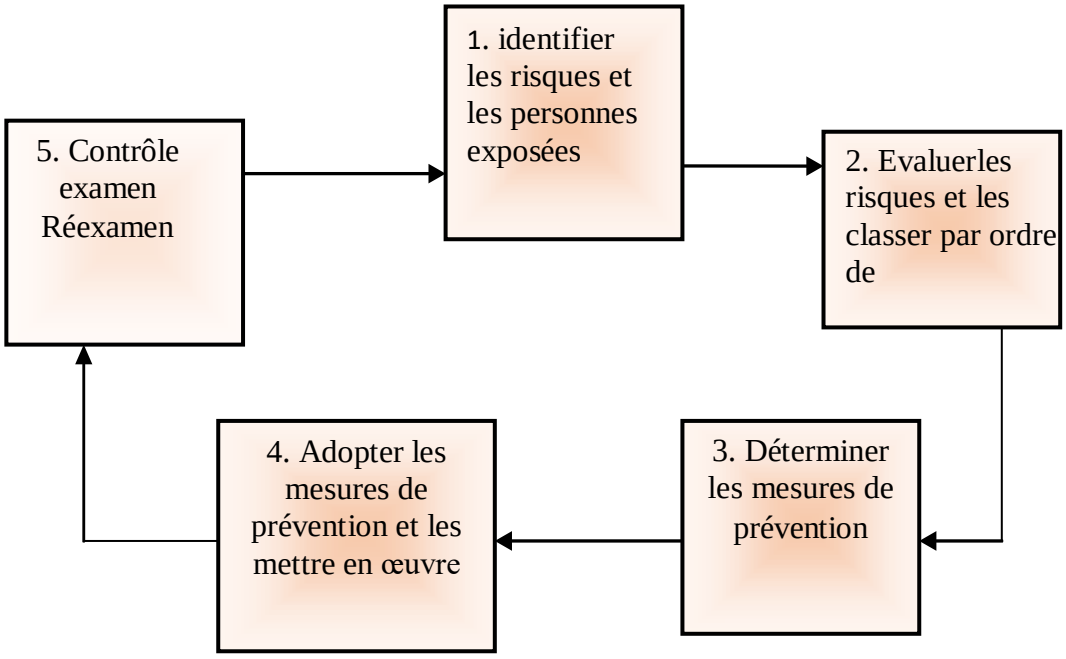


Figure 1.5 les étapes d'analyses

Étape 1 :

Identification des risques et des personnes exposées Cette étape consiste à dépister sur le lieu de travail les sources possibles d'accidents et a identifier les personnes qui peuvent y être exposées. Il faut donc se rendre sur le lieu de travail et y repérer les éléments pouvant engendrer un dommage, car aussi longtemps qu'un danger n'est pas repère, le risque y afférent ne pourra être ni analyse, ni gère. De plus, pour chacun des dangers, il faut identifier les personnes menacées. Il ne suffit pas d'identifier les personnes directement exposées au danger, mais également celles qui sont indirectement exposées. Outre les personnes actives sur un lieu de travail, il faut également considérer les groupes de personnes pouvant entrer en contact quelconque avec le danger, comme par exemple les salariés d'un autre secteur devant passer par ce lieu de travail ou encore les personnes faisant partie de l'équipe de nettoyage , etc. S'y ajoutent des groupes de personnes plus susceptibles d'être menacés, tels que les jeunes travailleurs, les travailleurs intérimaires sans formation spécifique, les travailleurs handicapes, les femmes enceintes et allaitantes , les salaries convalescents, etc.

Étape 2:

Évaluer les risques et les classer par ordre de priorité́ Dans cette deuxième étape, on évalue les risques lie s a chaque danger. On vérifie donc a quel niveau le salarie est expose au danger. Il faut évaluer dans quelle mesure le danger peut provoquer un accident ou une maladie, le niveau de gravite de cet accident ou de cette maladie et la fréquence à laquelle les salariés y sont exposés. Une évaluation des risques s'avérera toujours difficile car elle est toujours sujette a une interprétation subjective qui peut mener soit a une sur estimation, soit a une sous-estimation du risque. Pour remédier a la subjectivité d'une analyse individuelle, on peut recourir a différentes méthodes ou stratégies ou encore faire effectuer l'analyse par un travail en groupe.

Étape 3:

Déterminer les mesures de prévention La troisième étape consiste à déterminer les mesures a fin d'éliminer les risques ou, au moins, à les maitriser.

Il faut pouvoir déterminer si un risque peut être éliminé complètement ou dans le cas contraire mettre en place des mesures de façon à le contenir et s'assurer qu'il ne compromet pas la sécurité et la santé des salaries. Il faut également tenir compte du fait que les risques détectes peuvent s'additionner ou combiner leurs effets .Il est important de prendre en compte le résultat de l'évaluation des risques et de classer les mesures par ordre de priorité, de manière à appliquer en premier lieu les mesures de prévention qui sont les plus efficaces. Les principes géneuraux sont:

- éviter/écarter le risque;
- s'adapter au progrès technique;
- améliorer le niveau de protection.

Étape 4:

Adopter les mesures de prévention et les mettre en œuvre La quatrième étape consiste à mettre en œuvre les mesures de prévention déterminées auparavant.

Il va de soi que toutes les mesures ne pourront être mises en œuvre simultané ment : il faut donc établir un ordre de priorité en tenant compte de la gravité du risque et de ses conséquences. Il faut aussi déterminer les personnes pouvant s'occuper de la mise en œuvre, le temps que cela va prendre et déterminer un délai de mise en œuvre. Parmi les mesures a réalisé, on pourra ainsi distinguer:

- Les mesures applicables de suite et à moindres frais ;
- les mesures provisoires a mettre en place en attendant les
- Les mesures applicables a plus long terme et plus couteuses;

 Les mesures applicables a terme et représentant des frais plus élèves.

Étape 5:

Contrôle - Examen - Réexamen et Enregistrement Après que les mesures de Prévention aient été mises en œuvre, il faut contrôler si elles ont te exécutées et si les délais d'exécution des mesures ont été respectes. Il s'agit non seulement de vérifier si les risques ont pu être élimines ou écartes entièrement ou s'ils ont pu être diminues de façon a pouvoir les maitriser mais aussi si aucun nouveau risque n'a été crée suite a l'application des mesures.

De plus, il est recommande de réaliser régulièrement une nouvelle évaluation des risques, afin de déterminer si les risques ont bien pu être élimines définitivement ou si d'autres risques sont apparus depuis la dernière évaluation. Il est indispensable d'effectuer a nouveau une évaluation des risques chaque fois qu'il y a eu un changement dans l'entreprise. Ce changement peut se situer au niveau organisationnel, au niveau du personnel ou être de nature technique. Il peut s'agir, par exemple, de la création d'un nouveau poste de travail,

L'engagement de nouveaux salarie, l'installation d'une nouvelle machine, l'introduction d'un nouveau procède ou l "introduction d'un nouveau produit. Finalement, avoir enregistre l'évaluation des risques est toujours avantageux lors des contrôles et des examens. Un bon enregistrement peut servir en tant que: *base pour les réexamens et les évaluations des risques à venir ; * preuve destinée aux organismes de contrôle ; *information a transmettre aux personnes concernées.

Afin de bien servir de base pour des évaluations futures, il est recommande que l'enregistrement contienne:

1. les noms et fonctions des personnes effectuant les contrôles et examens.
2. la date du contrôle.
3. les risques qui ont pu être de pistes.
4. les groupes de personnes pouvant être menaces par les risques dépistes.

5. les mesures de prévention mises en œuvre.

6. les informations concernant des contrôlés et examens futurs.

7. les informations concernant la participation des travailleurs dans.

8. l'évaluation des risques.

3 - 3 Méthodes d'analyse des risques :

L"INERIS [INERIS DRA 35, 2006] [10] classe les méthodes d'analyse des risques selon deux catégories :

- Méthode classique d'analyse des risques : exp APR , HAZOP , ADE , ADD, AMDEC
- Méthode intégrées d'analyse des risques : exp LOPA , MODAR

Nous intéressons aux méthodes que nous allons utiliser dans notre travail.

5. L'arbre des évènements (ADE)

5-1 Présentation de la méthode ADE:

La quantification de risque s'associes aux installations industrielles nécessite l'identification et l'évaluation d'un très grand nombre de scenarios (ou séquences) envisageables .La complexité des systèmes (élémentaires) intervenant dans une installation industrielle, leurs nombreuses interactions et les redondances fonctionnelles existantes rendent difficiles ces tâches d'élaboration et dévaluation des séquences d'événements .L"ADE est l'outille plus a dé quat pour la caractérisation et la détermination de tels accidents potentiels.

5-2 Principe de la méthode ADE:

L'analyse par ADD vise, suivant une démarché déductive, à déterminer les Causes d'un événement indésirable retenu a priori.

A l'inverse, l'analyse par l'ADE suppose la défaillance d'un composant ou d'une partie du système et s'attache a déterminer les événements qui en découlent. A partir d'un événement initiateur ou d'une défaillance d'origine , l'analyse par ADE permet donc d'estimer la dérive du système en envisageant de manière systématique le fonctionnement ou la défaillance des dispositifs

de sécurité..

Chaque opé ration ou chaque système figurant dans l'ADE conduit a deux chemins (Succès Échecs). S'il y a une opé ration il y'aura 2 chemins ou séquences, chacun conduisant a une conséquence. Une séquence d'événements consiste en un premier événement (appelé événement initiateur) et une succession (ou combinaison) de défaillances et de fonctionnements des systèmes de sécurité . Lorsque cette succession d'événements conduit à:

*Des conséquences jugées inacceptables : «séquence inacceptable».

*Des conséquences jugées acceptables : «séquence acceptable».

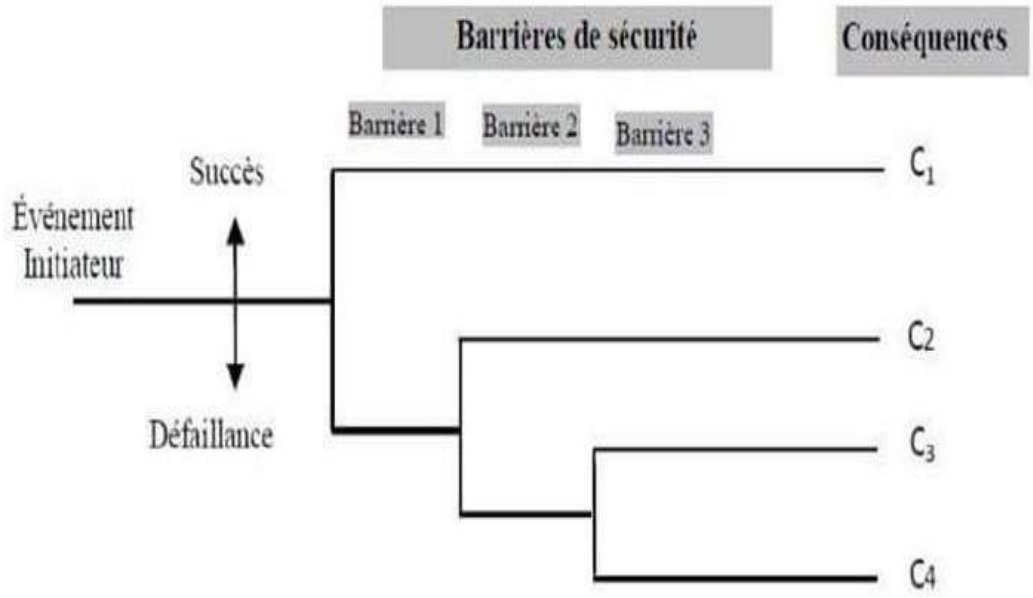


Figure 1.6 : Schéma d'n AdE avec des barrières de sécurités

5- 3- Déroulement:

La démarche déductive employée pour l'analyse des séquences accidentelles comporte quatre étapes principales:

* Première étape: définition des événements initiateurs

* Deuxième étape : identification des fonctions de sécurité

*Troisième étape: construction de l'arbre

* Quatrième étape: exploitation de l'arbre

*** Première étape :**

Définition des événements initiateurs Par définition un événement initiateur (EI) est le premier evénement d'une séquence d'événements.

Deux approches sont utilisées pour identifier les événements initiateurs:

*Le premier résulte d'une description du système , de l'expérience d'exploitation , des études des accidents déjà survenus…

*Le deuxième résulte d'une analyse préliminaire (APR) ou de la construction d'un ADD

*** Deuxième étape :**

Identification des fonctions de sécurité.

Les fonctions de sécurité doivent être assurées par des barrières en réponse a l'événement initiateur. Elles ont en général pour objectif d'empêcher, dans la mesure du possible , que l'evénement initiateur soit à l'origine d'un accident. Elles se déclinent le plus souvent en:

* Fonctions de détection de l'événement initiateur.

*Fonctions d'alarme signifiant l'occurrence de l'evénement initiateur.

* Fonctions de limitation visant en empêcher que l'evénement initiateur ne perdure dans le temps,

* Fonction d'atténuation s'attachant à réduire les effets de l'événement initiateur.

Cette liste n'est bien sûr pas exhaustive. De plus, ces fonctions peuvent être réalisées par des dispositifs automatiques ou bien des actions effectuées par des operateurs conformément à des procédures . Bien entendu, ces fonctions n'interviennent généralement pas simultanément. Il est particulièrement important de déterminer dans quel ordre elles vont intervenir suite à l'evénement initiateur et donc d'identifier les seuils commandant leur mise en œuvre. Ces informations permettent ainsi de donner des indications quant au temps nécessaire pour la mise en place de ces

mesures de sécurité. En conclusion de cette seconde étape, il est judicieux de dresser un tableau chronologique des fonctions de sécurité faisant figurer entre autres les systèmes ou équipements prévus pour assurer ces fonctions.

Tableau 1.1 identification des fonctions de sécurité

Fonction	Mesure de la températuredans la réaction	Alarme	Rétabilissement du système de réfrigérationpar un opérateur	Arrétla réaction
Dispositifs assurantla fonction	Sonde de températuredans le réacteur	Signaux sonores et lumineuxde travail	Opérateurselon une procédure	Introduction automatique d'uninhibiteur dala réaction
Paramètreou information déclanchant la fonction	Permanent	T ≥ T1	Alarme	T ≤ T2
Délai	Continu	1 mn	Si possible estiméà5mn	Estiméà10mn (De T_1 à T_2)

*** Quatrième étape :**

Construction de l'arbre La construction de l'arbre consiste alors à partir de l'evénement indésirable à envisager soit le bon fonctionnement soit la défaillance de la première fonction de sécurité . L'evénement initiateur est représenté schématiquement par un trait horizontal. Le moment où doit survenir la première fonction de sécurité est représentée par un nœud . La branche supérieure correspond généralement au suces de la fonction de sécurité , la branche inferieure à la défaillance de cette fonction. La suite de la méthode consiste alors à examiner le développement de chaque branche de manière itérative en considérant systématiquement le fonctionnement ou la défaillance de la fonction de sécurité suivante. Cette démarche temporelle permet d'identifier des séquences d'évènements susceptibles de conduire ou non à un accident potentiel . Elle n'est cependant généralement pas suffisante

en vue de construire un arbre . Il est ainsi indispensable durant la construction de l'arbre de prendre en considération l'ordre des événements génériques.

*** Quatrième étape :**

Exploitation de l'arbre.

*Approche qualitative : Un arbre qui présente des branches conduisant à l'échec et ne passant que par une branche inferieure (défaillance) d'une alternative révèle un système fragile (pas de défense en profondeur) à l'événement étudié (une seule défaillance ou condition défavorable suffit à provoquer l'échec). Une solide défense en profondeur (visà-vis de l'evénement étudie) se traduit par le fait que les seules branches conduisant aux conséquences non acceptées passent toutes par la branche inferieure de plusieurs alternatives (autrement dit qu'il faut la conjonction de plusieurs non-fonctionnements pour produire les conséquences redoutées). L "observation directe des extrémités de l'arbre qui présentent des conséquences négatives aux fréquences trop élevées permet en remontant ces branches d'identifier les points sur lesquels il faut agir pour améliorer cet aspect.

*Approche quantitative : Si on a pu attribuer une probabilité à chaque alternative (probabilité de succès et complément à 1 pour l'échec), on peut calculer, pour chacune des conséquences envisagées la probabilité qu'elle se produise , l'evénement initial étant advenu. Chaque extrémité (coté conséquence à droite) de l'arbre a une probabilité égale au produit des probabilités des branches d'alternatives empruntées pour y arriver .

Chaque conséquence possible a donc comme probabilité la somme des probabilités des extrémités où elle figure . On doit pouvoir vérifier que la somme des probabilités de toutes les conséquences est de 1. Ce résultat brut permet d'évaluer l'impact , donc l'intérêt d'une réduction de la probabilité de l'événement initiateur. On peut aussi évaluer l'importance réelle de

chaque dispositif en reprenant les calculs avec une autre valeur pour la probabilité de fonctionnement de ce dispositif (sensibilité du résultat final à la fiabilité de chaque dispositif). On peut découvrir ainsi qu'un dispositif auquel on accorde beaucoup d'importance n'en a guère, masqué.

L'analyse par l'ADE est une méthode qui permet d'examiner d'un evénement initiateur, l'enchainement des événements pouvant conduire ou non à un accident potentiel. Elle trouve ainsi une utilité toute particulière par l'étude de l'architecture des moyens de sécurité (Prévention, intervention, protection) existants ou pouvant être envisagés sur un site .

A ce titre, elle peut être utilisée pour l'analyse d'accidents posteriori.

Cette méthode peut s'avérer rapidement lourde à mettre en œuvre.

En conséquence, il faut définir avec discernement l'événement initiateur qui fera l'objet de cette analyse.

Exemple :

Arbre d'évènement défaillance du système de refroidissement.

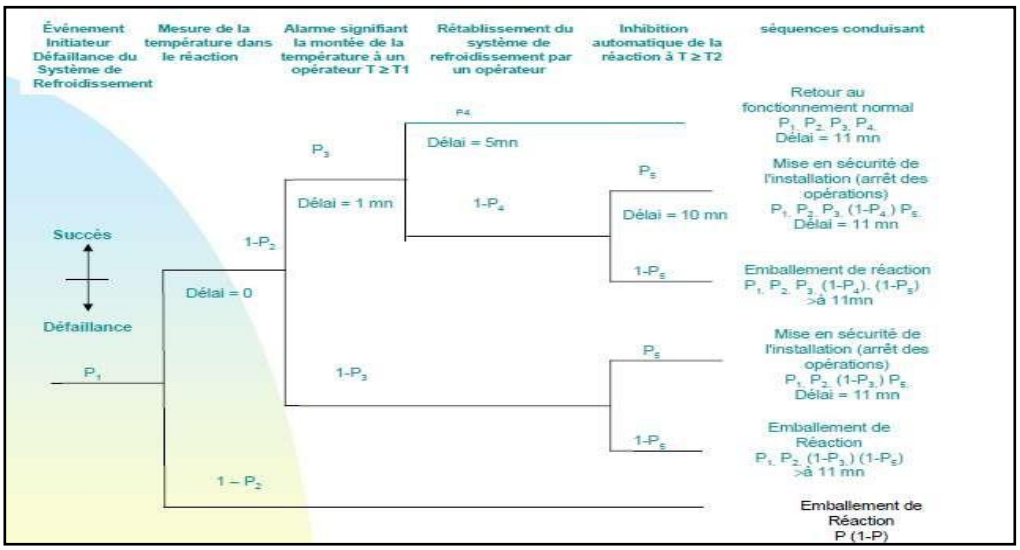


Figure 1.7 Arbre d'évènement défaillance du système de refroidissement.

Chapitre : II
Système instrumenté de sécurité

1-Normes relatives au système instrumenté de sécurité :

L'instrumentation doit réellement être utilisée pour réaliser des fonctions instrumentées de sécurité, donc il est essentiel qu'elle présente des niveaux minimums de qualité et de performance. En conséquence, un grand travail a été effectué mettant en question les performances des systèmes relatifs à la sécurité de type instrumenté, considérés comme complexes, par le développement des normes qui favorisent l'évaluation, la validation et la certification systématique de ces systèmes. Parmi ces différents documents normatifs, la norme CEI 61508[7] développée et publiée par la Commission d'Électrotechnique Internationale (CEI), cette dernière développe aussi des normes relatives à des secteurs bien précis, ce qui sera présenté dans la suite de cette section.

1-1 Norme CEI 61508

La CEI 61508[7] est une norme internationale qui a été conçue comme une norme générique contenant un ensemble d'informations et de lignes directrices visant à l'amélioration de la sécurité via l'utilisation des systèmes électriques, électroniques programmables E/E/PE que sont les SIS. Elle s'inscrit dans une approche globale de la sécurité que l'on peut comparer aux systèmes ISO 9000 et ISO 14000 qui concernent respectivement les domaines de la qualité et de l'environnement. Elle propose une démarche opérationnelle permettant de mettre en place un système E/E/PE à partir de l'étude des exigences de sécurité issues notamment d'une analyse et d'une évaluation des risques, et ce, en prenant en compte toutes les étapes de son cycle de vie. Un des objectifs visés lors de sa conception était (et est toujours) qu'elle serve de document de référence facilitant

L'élaboration de normes sectorielles qui devraient alors former un ensemble doté d'une certaine cohérence.

La CEI 61508 est un ensemble des règles et des recommandations permettant l'amélioration de la sécurité par l'utilisation des systèmes

E/E/EP. Cette norme orientée performances, propose une démarche opérationnelle permettant de mettre en place un système E/E/EP à partir de l'étude des exigences de sécurité issues notamment d'une analyse des risques. L'avantage de cette norme est qu'elle propose des moyens de justification sur l'ensemble du cycle de vie d'un produit en fonction du niveau de sécurité que l'on souhaite atteindre.

La norme CEI 61508 [7] se compose de sept volets comme suit :

*61508-1 présente les définitions des prescriptions générales.

*61508-2 traite les prescriptions spécifiques aspect matériel des systèmes E/E/EP

*61508-3 dédiée à la présentation des prescriptions spécifiques, aspect logiciel, des systèmes E/E/EP. Elle est développée dans la troisième partie de norme.

* 61508-4 présente les définitions et les abréviations utilisées.

*61508-5 donne des exemples de méthode pour la détermination des niveaux d'intégrité de sécurité.

*61508-6 fournit les guides d'application des parties 2 et 3 de la norme.

* 61508-7 présente les techniques et les mesures recommandées lors de la validation des systèmes E/E/EP.

La complexité de la norme CEI 61508 a conduit ses concepteurs à développer des normes relatives à des secteurs bien précis (ex : machines, processus industriels, ferroviaire, centrales nucléaires . . .). générique ainsi que ses normes filles selon le secteur d'activité concerné.

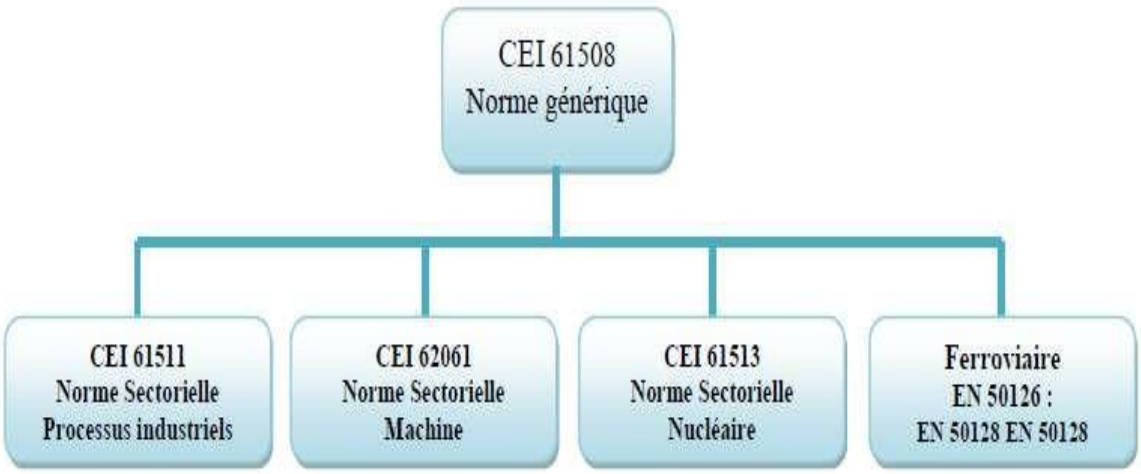


Figure 2.1 montre la norme CEI 61508

Elle influence le développement des systèmes E/E/EP et les produits concernés par la Sécurité dans tous les secteurs

1-2 Norme CEI 61511

La CEI 61511[8], s'intéresse à la sécurité fonctionnelle des SIS pour le secteur de l'industrie des procédés continus. Cette norme est composée de trois grandes parties :

- 61511-1 présente les définitions et les exigences des systèmes (matériel et logiciel).
- 61511-2 traite les lignes directrices pour l'application de la première partie de la norme.
- 61511-3 fournit des conseils pour la détermination des niveaux d'intégrité de sécurité.

La CEI 61511 [8] détaille les définitions et les prescriptions relatives au cycle de vie en sécurité contenant la spécification, la conception, l'exploitation et la maintenance d'un système instrumenté de sécurité, afin de maintenir le procédé dans une position de sécurité convenable.

La norme CEI 61511 est l'une des déclinaisons de la norme CEI 61508. Les SIS constituent l'objet principal de ces deux normes, mais ils y sont considérés différemment selon les métiers auxquels elles s'adressent(

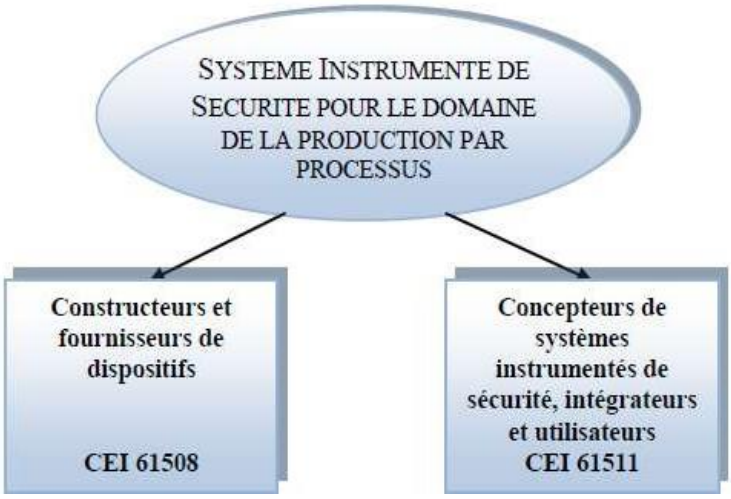


Figure 2.2 relation entre la 61508et la 61511

La CEI 61508 est une norme complexe, difficile à mettre en œuvre, elle est destinée surtout aux fabricants et fournisseurs de systèmes E/E/EP, alors que la norme CEI 61511 est plus facile à utiliser, elle présente une simplification de la CEI 61508, en se limitant aux éléments nécessaires pour l'industrie de process.

1-3 La norme CEI 62061 :

La CEI 62061[5] repose sur les mêmes concepts que ceux de la CEI 61508. 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. Elle concerne la spécification des prescriptions et fait des recommandations pour la conception, l'intégration et la validation de ces systèmes.

1-4 La norme ECI 61513 :

La CEI 61513 [13] concerne le secteur de la sureté 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 la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire .

1.5 Norme EN 50126

La norme EN 50126] s'intéresse essentiellement aux applications ferroviaires. Elle permet de spécifier les principaux concepts de la sureté de fonctionnement des systèmes tels que : la fiabilité, la disponibilité et la sécurité,...Cette norme est constituée de deux normes filles. L'EN 50128 est destinée à la partie logicielle des systèmes de protection ferroviaire.

L'EN 50129 concerne les systèmes électroniques de sécurité pour la signalisation.

2. Définitions et concepts relatifs aux SIS :

2-1 Définitions

La norme CEI 61508 [7] définit les systèmes relatifs aux applications de sécurité par:"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."La norme CEI 61511 [8] définit les systèmes instrumentés de sécurité de la façon suivante : " système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité(SIF). Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux)."

Les systèmes suivants sont des exemples des systèmes instrumentés de sécurité :

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

se compose de n'importe quelle combinaison de :

*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.

*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 micro- ordinateur doté de logiciels spécifiques.

Sous-système FE (Final Élément) : 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.

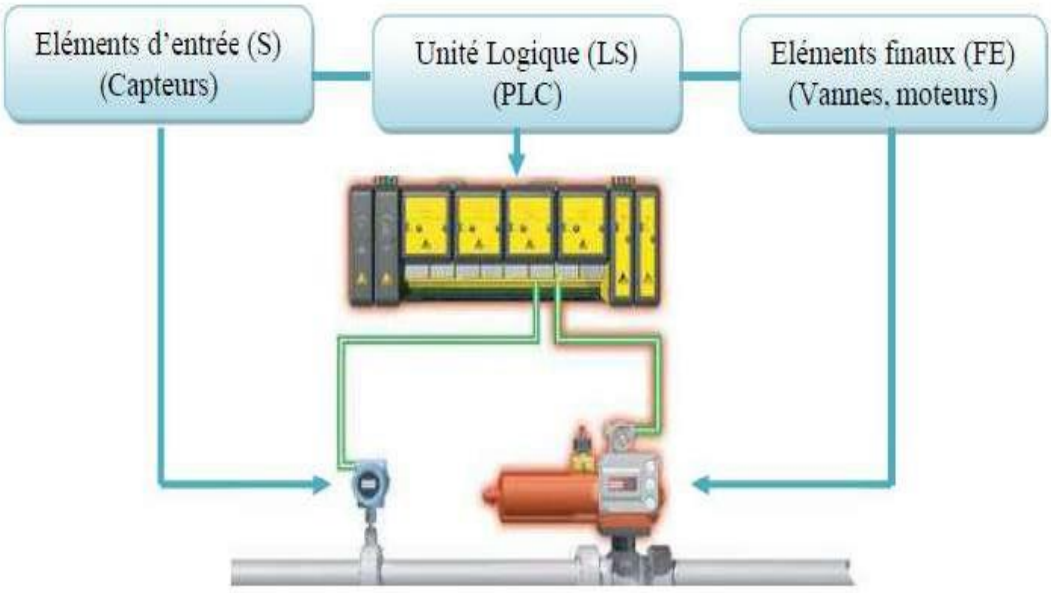


Figure 2.3 exemple d'un SIS :

Une fonction instrumentés de sécurité (SIF, Safety Instrumented Function)

est une fonction à réaliser par un SIS prévue pour assurer ou maintenir un état de sécurité de l'équipement à protéger (EUC) par rapport à un événement dangereux spécifique.

Une fonction instrumentée de sécurité (SIF) est utilisée pour décrire les fonctions de sécurité implémentées par un système instrumenté de sécurité. Une fonction instrumentée de sécurité peut être considérée comme une barrière de protection fonctionnelle lorsque le système instrumenté de sécurité est considéré comme un système réalisant cette barrière de sécurité .

Un SIS peut implémenter une ou plusieurs SIF. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à la réduction de la fréquence d'occurrence du danger.

L'architecture fonctionnelle d'un SIS est un ensemble de SIF qui comprend trois fonctionnalités de base, la détection (ou la mesure), le traitement (ou la décision) et l'actionnement.

2-2 Exigences de sécurité des SIS en accord avec la norme CEI 61508

En tant que notions fondamentales de la CEI 61508 se trouvent les exigences de sécurité des SIS. Celles-ci concernent les fonctions de sécurité et les niveaux d'intégrité de sécurité associés. La spécification des exigences des fonctions de sécurité des SIS consiste à décrire toutes les fonctions de sécurité qui leurs sont allouées (sur la base de l'analyse des dangers et des risques, et afin d'atteindre l'objectif de risque tolérable), qui sont nécessaires pour obtenir la sécurité fonctionnelle requise. De plus, doivent être spécifiés : le temps de réponse requis pour la réalisation des fonctions de sécurité ; les interfaces entre les SIS et les opérateurs ainsi que les autres systèmes ; les comportements requis des SIS en cas d'anomalies; les modes de fonctionnement de l'EUC; et toutes autres informations pertinentes susceptibles d'influencer la conception des SIS.

Une fonction de sécurité peut alors être sollicitée selon trois modes de fonctionnement [IEC61508,2010] : faible sollicitation, lorsqu'elle n'est réalisée que sur sollicitation (afin de faire passer l'EUC dans un état de sécurité

spécifié), et où la fréquence des sollicitations n'est pas supérieure à une par an ; Sollicitation élevée, lorsqu'elle n'est réalisée que sur sollicitation, et où la fréquence des sollicitations est supérieure à une par an ;Et continu, lorsqu'elle maintient l'EUC dans un état de sécurité en fonctionnement normal (à noter que cette classification diffère de celle de la précédente édition de la norme [IEC61508, 2002]).

La probabilité pour qu'un SIS accomplisse de manière satisfaisante les fonctions de sécurité spécifiées (dans toutes les conditions énoncées et dans une période de temps spécifiée) est l'intégrité de sécurité [IEC61508, 2010] (ce qui correspond en fait à la « disponibilité » du SIS. L'intégrité de sécurité comprend : l'intégrité de sécurité du matériel, qui est relative aux défaillances aléatoires du matériel, c'est-à-dire survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel ; et l'intégrité de sécurité systématique, qui est relative aux défaillances systématiques, c'est-à- dire liées 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 [IEC61508, 2010]. Pour chaque fonction de sécurité, une exigence relative à l'intégrité de sécurité cible est allouée (sur la base de l'analyse des dangers et des risques, et afin d'atteindre l'objectif de risque tolérable). Les intégrités de sécurité sont alors classées selon quatre niveaux discrets, nommés niveaux d'intégrité de sécurité (SIL, pour « safety integrity levels»), dont le niveau 4 possède le plus haut degré d'intégrité, et le niveau 1 le plus bas. Pour cela, un objectif chiffré de défaillance est spécifié selon le mode de sollicitation de la fonction de sécurité : probabilité moyenne d'une défaillance dangereuse lors de l'exécution sur sollicitation de la fonction de sécurité (PFDavg, pour « average proability of failure on demand»), définie comme une indisponibilité moyenne , pour un mode de faible sollicitation ; et fréquence moyenne d'une défaillance

dangereuse par heure (PFH, pour « probability of failure perhour»), exprimée par heure.

En plus du niveau d'intégrité requis pour chaque fonction de sécurité, avec l'objectif chiffré de défaillance correspondant, et du mode de fonctionnement (faible sollicitation, sollicitation élevée, continu) de chaque fonction de sécurité, la spécification des exigences sur l'intégrité de sécurité des SIS doit comprendre : le cycle de service et la durée de vie requis ; les contraintes sur les essais périodiques ; les valeurs extrêmes des conditions environnementales des SIS ; les limites d'immunité électromagnétique ; et les contraintes relatives aux possibilités de défaillances de causes communes.

2-3 Compositions d'un SIS :

Composition minimale 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 [Ayault ,2005] [18].

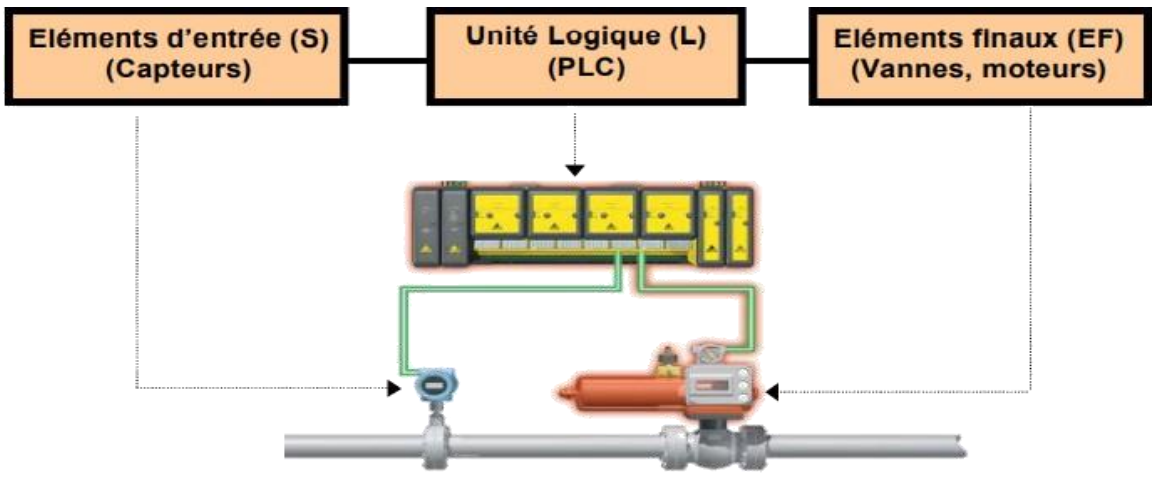


Figure 2-4 Schémas d'un sis simple

A. Capteur

Est un équipement qui délivre, à partir d'une grandeur physique, une autre grandeur, souvent électrique (tension, courant, résistance), fonction de la première et directement utilisable pour la mesure ou la commande [Ayault ,2005].Cette grandeur physique peut être la température, la pression, le niveau, le débit, la concentration d'un gaz.

B. Unité de traitement

La fonction "traitement" peut être plus ou moins complexe [Ayault ,2005]. Elle peut se résumer à acquérir une grandeur mesurée par un capteur et à l'indiquer. Elle peut également consister à activer la commande d'un ou plusieurs actionneurs à partir d'une fonction combinatoire des informations délivrées par différents capteurs. Les unités de traitement peuvent être classées en deux catégories selon leur technologie :

*Les technologies câble à base de composants logiques élémentaires (relais), liés entre eux électriquement (ou de manière pneumatique).

* Les technologies programmées, à base de centrales d'acquisition ou d'alarmes, d'automates programmables (API), de systèmes numériques de contrôle commande (SNCC), de calculateurs industriels ou de cartes électroniques à microprocesseurs.

C. Actionneurs

Un actionneur peut être (vanne, moteur, servo-moteur...) transforment un signal (électrique ou pneumatique) en phénomène physique qui permet de commander le démarrage d'une pompe, la fermeture ou l'ouverture d'une vanne... Selon l'énergie motrice, on parle d'actionneur pneumatique, hydraulique ou électrique [Ayault ,2005].

Enfin, l'unité de traitement est reliée aux capteurs et aux actionneurs par des moyens de transmission. Il peut s'agir de câbles électriques, de lignes téléphoniques, d'ondes hertziennes (transmission par talkie-walkie...), ou de tuyauteries (transmission pneumatique ou hydraulique).

Les capteurs, l'automate et les actionneurs sont des équipements de sécurité. Un

équipement de sécurité est un élément d'un SIS qui remplit une sous-fonction de sécurité.

Exemples

*un capteur remplit la sous -fonction "détecter du gaz", une vanne motorisée la sous-fonction "juguler une fuite".

* Associées au traitement, l'ensemble de ces sous -fonctions permet la réalisation de la fonction instrumentée de sécurité "maitriser une fuite "

Composition d'un SIS en fonction des taches a accomplir.

Un système instrumenté de sécurité a pour finalité, en cas de sollicitation, d'accomplir un certain nombre de fonctions (isoler une capacité, arrêter les flux de produits ,….) qui elles –mêmes peuvent se décomposer en tâches (fermeture de plusieurs vannes, arrêt de plusieurs machines,…).

C'est dans l'optique d'accomplir toutes les taches que l 'on trouve fréquemment au sein des SIS le montage en parallèle de plusieurs actionneurs . A noter qu'un unique actionneur peut commander plusieurs actionneurs. Par exemple, une électrovanne trois voies située sur un réseau d 'air instrumente peut , par mise a l 'atmosphère de ce réseau , commander la fermeture de toutes les vannes pneumatiques alimentées par le réseau .

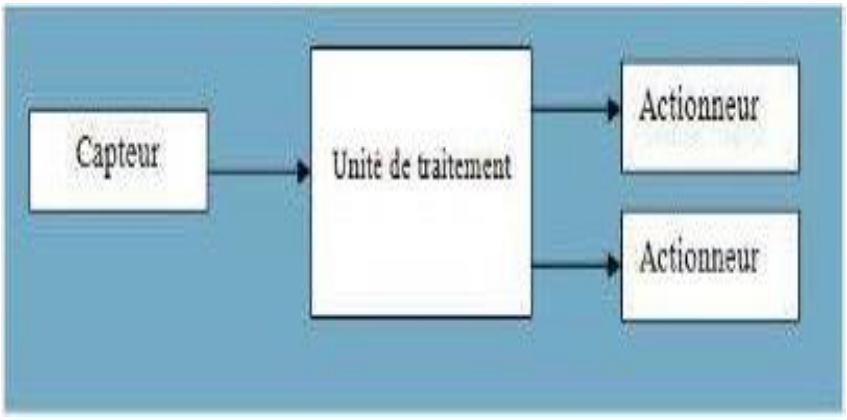


Figure 2.5 schéma d'un SIS effectuant plusieurs tâches

Beaucoup moins fréquemment, on trouve le montage en parallèle de plusieurs

capteurs afin de répondre a un besoin de réception d 'informations différentes (Pression et température d 'un fluide par exemple) par l 'unité de traitement pour décider le déclenchement des actions de sécurité (Figure1.6). L'unité de traitement gère alors l 'arrivée de différentes informations soit par un operateur logique (par exemple, le déclenchement des actions de sécurité est réalise si la tempé rature est supérieure a 100°C ou si la pression est supérieure a 10 bars), soit par calcul (par exemple, correction de l'information principale reçue par la deuxième information reçue).

2-4 Redondance au sein d'un S.I.S

Pour améliorer le niveau de confiance d'un système instrumente 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 été réalise 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 instrumente de sécurité peuvent être redondés: capteurs, unité de traitement, actionneurs et meˆme 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 utilise sur sollicitation qu'en cas de défaillance de la partie en fonctionnement. la redondance m /n qui est une redondance telle qu'une fonction n'est assure 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 traite ment correct de tout signal d'alarme valide.

1oo2 (m = 1 et n = 2) : Cette architecture comprend deux éléments connecte ́s en parallèle de fac ¸on 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 traite correctement.

2oo2 (m = 2 et n = 2) : Cette architecture comprend deux éléments connecte ́s en parallèle de sorte qu'il est nécessaire que les deux éléments demandent la fonction de sécurité avant que celle-ci ne survienne.

La défaillance dangereuse d'un seul élément empêche le traitement correct de tout signal d'alarme valide.

2oo3 (m = 2 et n = 3) : Cette architecture comprend trois éléments connecte s en par allèle avec un dispositif a logique majoritaire pour les signaux de sortie de telle sorte que l'état de sortie n'est pas modifie lorsqu' 'un seul élément donne un résultat différent des deux autres éléments. Il faudrait la défaillance dangereuse des deux éléments pour qu'un signal d'alarme valide ne soit pas traite correctement.

*Tests de système instrumente de sécurité.

Généralement ces tests sont établis pour vérifier et contrôler le bon fonctionnement

de SIS. Deux types de tests qui sont faits au niveau de SIS : 1.4.6.1 Test de diagnostic Test en ligne (en fonctionnement) pour détectera des défauts , les tests de diagnostic sont effectues périodiquement et automatiquement pour détecter les défauts latents caches qui empêchent le SIS (Safety Integrated System) de répondre a une demande [Lamy, 2002] [19].

Les tests de diagnostic agissent au niveau composant /interne (et non pas au niveau de la fonction de sécurité) et permettent de détecter les erreurs aléatoires (dues au matériel). 1.4.6.2 Proof T est T est périodique hors ligne réalise pour détecter des pannes dans un système de telle sorte que le système puisse être réparé afin de revenir dans un état équivalent à son état initial. Dans

le cas ou le diagnostic converge serait minimum ou insuffisant (si on ne peut pas ou ne sait pas réaliser un test de diagnostic satisfaisant), on pourra augmenter la fréquence du proof test . En augmentant la fréquence du proof test, on vérifier a plus souvent que la fonction de sécurité est bien disponible. Le proof test est exécute au niveau du système. C'est un test fonctionnel de la fonction de sécurité hors fonctionnement automatique sans perturbation de process (activité périodique devant être conduite selon une procédure afin de détecter les défauts latents qui empêchent le système de securit́de remplir sa fonction de sécurité ; le système de sécurité entier doit être testé) [Lamy, 2002]. En règle générale, un proof test a une périodicité beaucoup plut important (intervalle entre test plus grand) qu'un test de diagnostic. Alors que le test de diagnostic est plutôt une détection interne en fonctionnement. Le proof test permet de détecter les pannes latentes qui n'ont pas été vues par les tests de diagnostic.

2-5 Fonction instrumente et de sécurité.

La fonction instrumentée de sécurité́ est définie comme étant la fonction de sécurité avec niveau d'intégrité de sécurité́ (SIL) spécifique qui est nécessaire pour maintenir la fonction de sécurité́[FAL00] [21].La fonction de sécurité́ est définie comme la fonction qui doit être réalisée par un SIS, d'autres équipements de sécurité, cette fonction de sécurité́ a pour but de maintenir un état sécurisé du procès. Une fonction instrumentée de sécurité́ est spécifiée pour s'assurer que les risques sont maintenu sà un niveau acceptable par rapport à un événement dangereux spécifique.

Une fonction instrumentée de sécurité́ est à réaliser par un système instrumenté de sécurité́ (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.

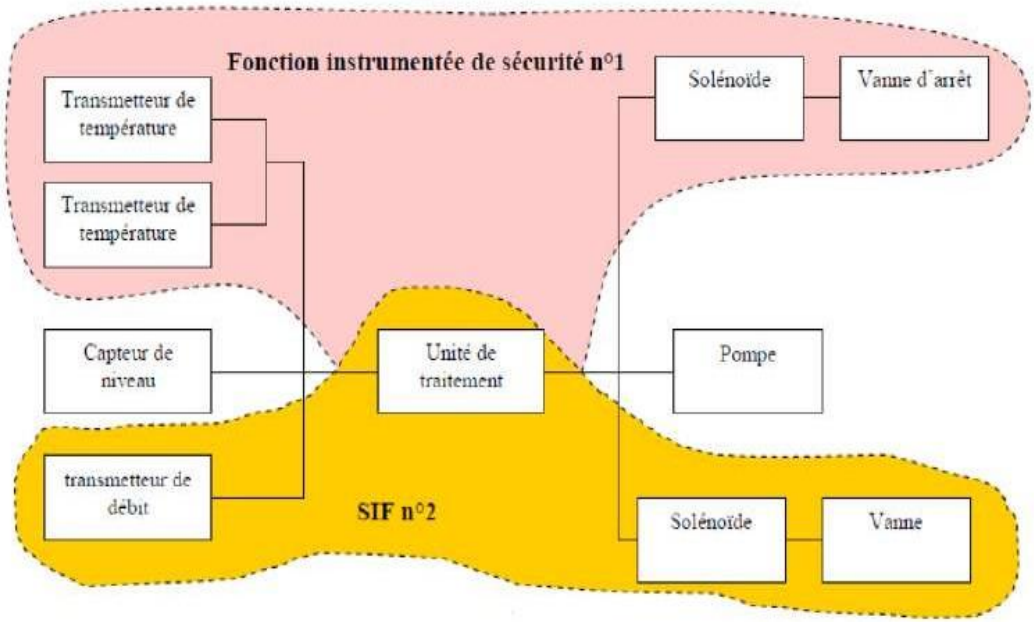


Figure2.6fonction instrumenté de sécurité

Pour illustrer et rendre plus claire cette définition, nous proposons l'exemple d'un équipement utilise dans la fonction instrumente de sécurité (Figure 2-6) .

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 a la réalisation de cette fonction instrumente e de sécurité, ces composants sont :Transmetteur de pression, solver, vanne, pompe.

Exemple de fonction instrumente de sécurité

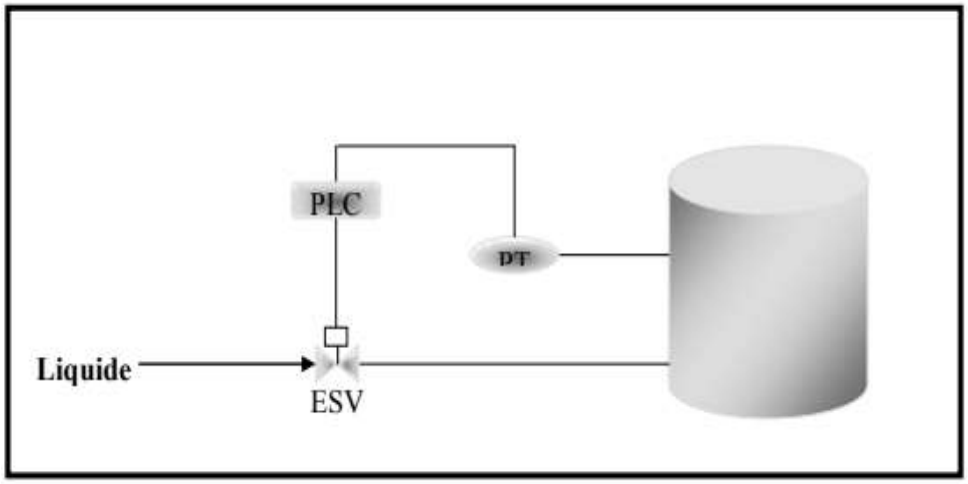


Figure2.7exemple de fonction instrumenté de sécurité

2-5 Propriétés d'un SIS

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

• Les systèmes instrumentent 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 chaines de sécurité.

• Plusieurs capteurs ou actionneurs peuvent être relies a 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.

2-6 Intégrité de sécurité d'un SIS

La référence 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 deux types de défaillances, aléatoires du matériel et systématiques, définis par la norme CEI 61508 seront explicités au début du prochain chapitre.

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 .

2-7 Modes de fonctionnement des SIS et paramètres cibles de défaillances

*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.

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. *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.

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 7.1 pour le mode de fonctionnement continu ou à demande élevée.

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 de un à quatre niveaux 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

Niveau d'intégrité de sécurité (SIL)	Mode de fonctionnement à faible sollicitation (PFD moy)	Mode de fonctionnement continu ou a forte sollicitation(PFH)
4	**$\geq 10^{-5}$à$<10^{-4}$**	**$\geq 10^{-9}$à $<10^{-8}$**
3	**$\geq 10^{-4}$à$<10^{-3}$**	**$\geq 10^{-8}$à $<10^{-7}$**
2	**$\geq 10^{-3}$à$<10^{-2}$**	**$\geq 10^{-7}$à $<10^{-6}$**
1	**$\geq 10^{-2}$à $< 10^{-1}$**	**$\geq 10^{-6}$à$< 10^{-5}$**

Tableau 2. 1 les différents niveaux de SIL définis par la normeCEI61508

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 SILs 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.

2-8 Classification des défaillances des SIS :

2.8.1- Classification retenue La norme CEI61508

La norme distingue les défaillances aléatoires du matériel et les défaillances Systématiques défaillances aléatoires du matériel : « défaillances survenant de manière aléatoires et résultant de divers mécanismes de dégradations au sein du matériel

» Défaillances systématiques : « 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 appropries » . Les défaillances aléatoires du matériel sont relativement bien comprises. Les données relatives a cette catégorie de défaillances sont, dans la plupart du temps, disponibles. Les défaillances systématiques sont difficiles à modéliser et de ce fait moins compréhensibles Défaillance dangereuse : défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité de remplir sa fonction.

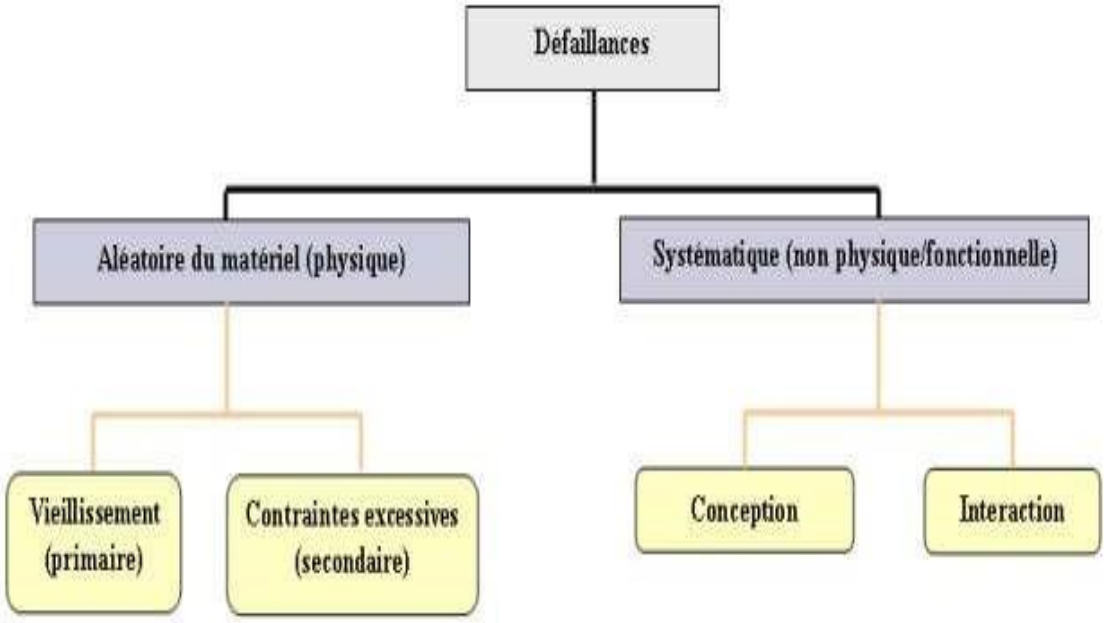


Figure2.8Classification des défaillances selon leurs causes

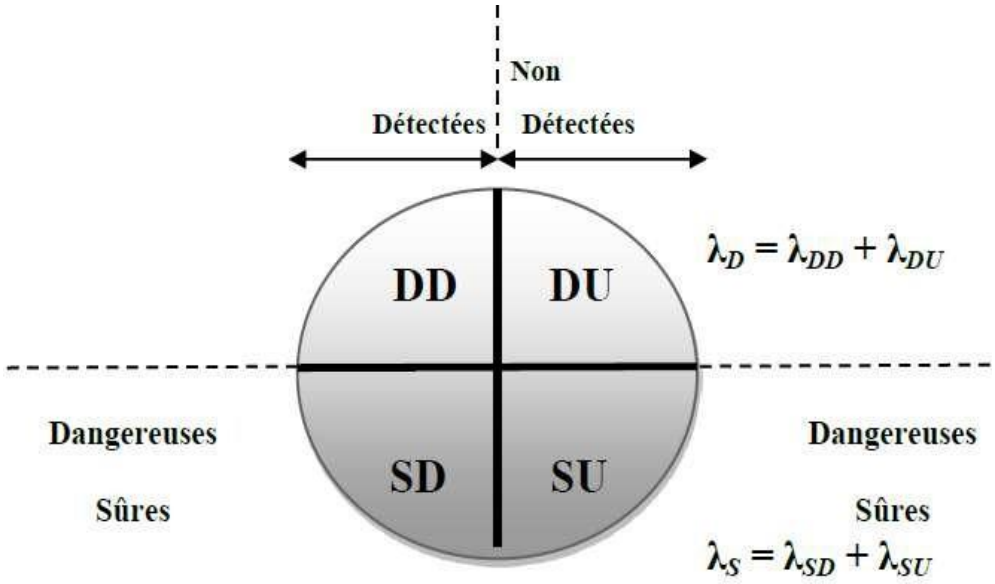


Figure 2.9 typologie des défaillances selon la norme CEI 61508

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 de remplir sa fonction . Une autre partition résulte du fait que ces défaillances peuvent être ou non détectées par des tests en ligne. Les premières sont de´nommées défaillances détectées (detectedfailures) et les secondes, qui ne peuvent être révélées que lors de tests périodiques hors ligne ou lors de la sollicitation du SIS par l'EUC , sont dénommées défaillances non détectées (undetectedfailures).

Le schéma suivant est classiquement présenté pour résumer cette double partition.

La simplicité de cette classification appelle trois commentaires :

• La première définition n'est pas auto -suffisante car elle est « a tiroirs » (défaillance dangereuse → état dangereux).

Il conviendrait donc de définir auparavant ce qu'est un état dangereux. Ce qui n'est pas fait explicitement dans la norme qui renvoie aux notions de situation dangereuse et d'événement dangereux. La notion d'événement

redouté serait plus appropriée , car ce type d'événement est plus facile a identifier comme résultant de la présence d'un état dangereux (le SIS est indisponible et donc dans l'impossibilité de remplir sa fonction) et de la survenue d'une demande émanant de l'EUC qui doit être protège

• Les défaillances en sécurité sont définies par opposition (ici aux défaillances dangereuses), c'est-à-dire par ce qu'elles n'entrainent pas .

Il aurait été plus simple de les définir « positivement » , ce qui aurait permis de mieux les situer par rapport aux défaillances intempestives (spurious trip ailures) qui ne sont me ˆ me pas citées dans la norme. Ces dernières défaillances correspondent, par exemple , à un déclenchement inopportun d'une action de sécurité.

Un exemple illustratif de ce type de défaillance est le cas d'un système de détection de surpression qui envoie un signal a l'unité de décision qui , à son tour commandera la fermeture de vannes de sécurité , alors qu'en réalité il n'y a pas de surpression.

• Cette classification des défaillances conduit à celle des taux de défaillance correspondants, qui est systématiquement utilisée dans la norme. Ceci est une source d'ambiguïté, car si l'on peut en général aisément qualifier de dangereux ou de sûr un taux de défaillance d'un composant, il n'en est pas de même dans le cas d'un système, même simple. C'est pourquoi l'option de définir avec précision les différents états dans lesquels peut se trouver un système est préférable à l'option de définir directement ses taux de défaillances dangereuses et sûrs.

La définition de ces derniers et des défaillances possibles du système résultera d'ailleurs de l'identification préalable de ses états potentiels, comme nous le verrons bientôt.

3-8-2Classification proposée par SINTEF

Cet organisme propose, dans son manuel, 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 :

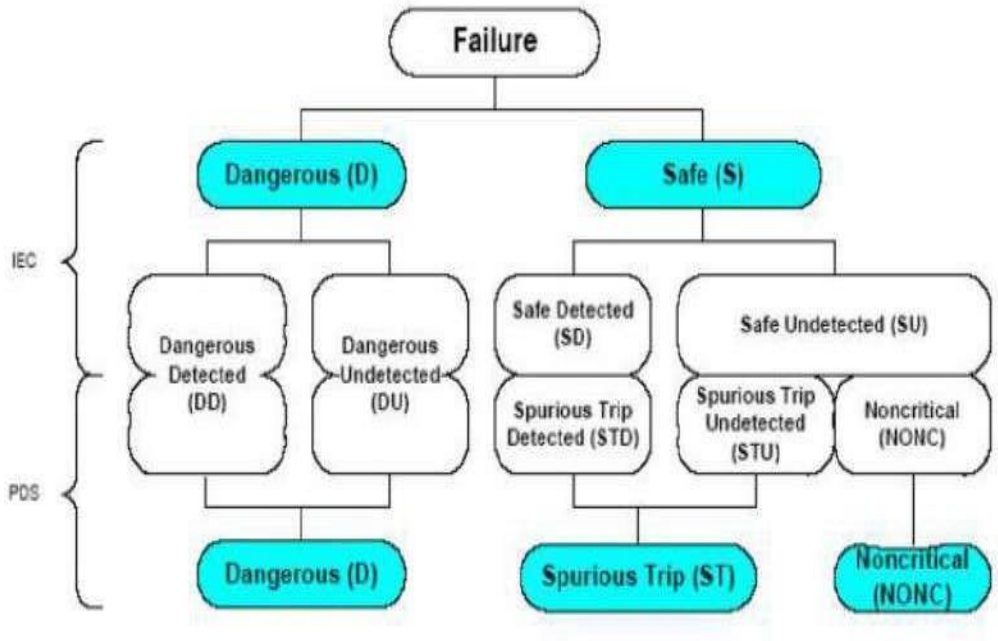


Figure 2.10 classification des défaillances selon SINTEF

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 s e divisent donc en défaillances détectées LDD et non détectées LDU .

• Les défaillances intempestives sont un sous -ensemble des défaillances sures et se divisent également en défaillances détectées LSTD) et non détectées LSTU.

• Les défaillances non critiques LNONC sont celles qui n'ont aucune incidence sur les deux fonctions principales du système EUC , c'est-à-dire son aptitude a produire (disponibilité de production) et son aptitude a ne pas

engendrer d'événements redoutes (sécurité).

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

- 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.

NB : Les défaillances intempestives ne sont même pas citées dans la classification retenue dans la norme CEI 61508, alors que la classification SINTEF considère ces défaillances comme une sous-classe des défaillances sûres. Les exemples, souvent évoqués, du déclenchement intempestif d'un airbag ou de l'inversion intempestive du flux de poussée d'un réacteur en plein vol suffisent à montrer que cette classification est pour le moins réductrice.

3-Définitions et classification des activations intempestives des SIS :

 Définitions : 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. Dans un processus industriel, les activations intempestives des SIS peuvent provoquer des arrêts partiel sou 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.

- Classification des activations intempestives :

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 instrumenté 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 fonctionnes 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 instrumenté de sécurité (SIF).

(2) La fermeture d'une vanne d'arrêt d'urgence (ESV) dans une configuration 1oo2 (le système fonctionnes 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).

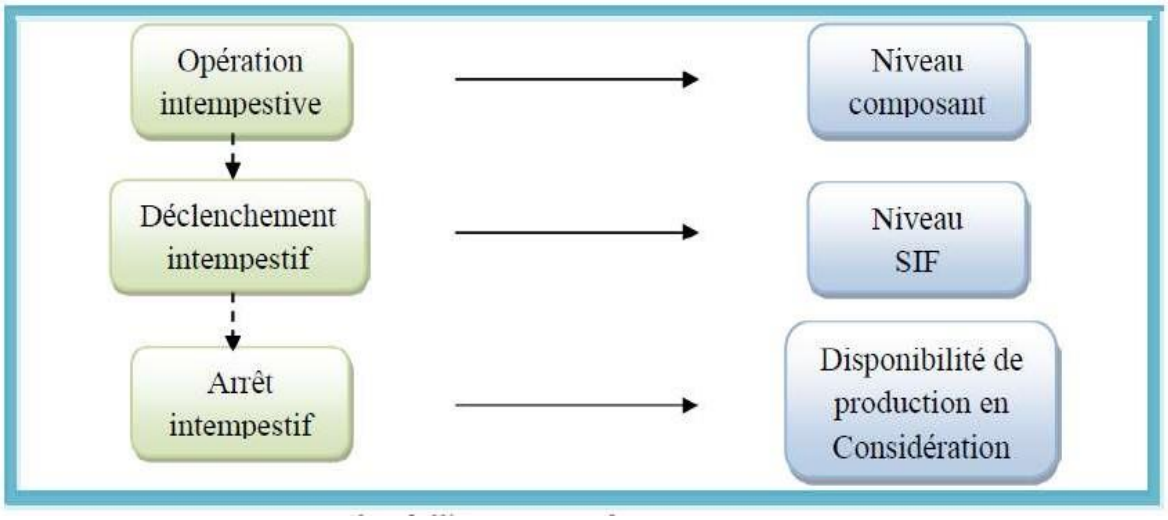


Figure 2-11 les différents types des activations intempestives

2- 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 suivante illustre les causes principales des activations intempestives représentées dans un diagramme de fluence (influence diagramme)

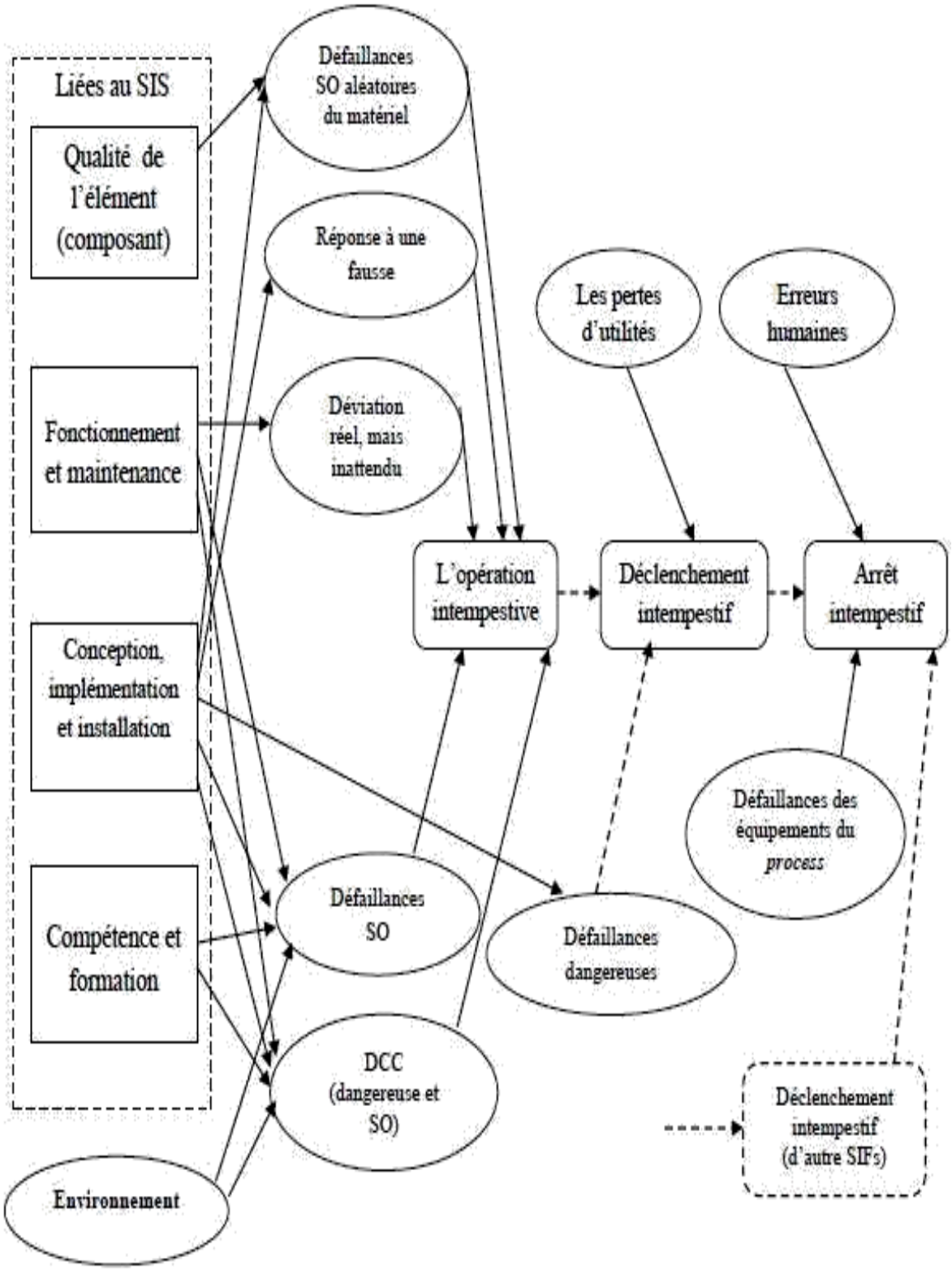


Figure 2-12 Les décisions et les facteurs qui influencent les activations intempestives.

Nous ne sommes pas en mesure de contrôler ces facteurs directement, mais nous pouvons les influencer indirectement par un ensemble de décisions. Les flèches indiquent les relations entre les décisions, les facteurs influençant, et les mesures de performance.

- **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 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 conforme 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.

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 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 DCC- SO 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.

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.

 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 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".

Chapitre III : Allocation De Niveau De Confiance des SIS

Niveau de confiance des SIS

Si le SIS était parfaitement fiable, le risque d'évolution du procédé vers une situation dangereuse serait totalement éliminé. Mais le SIS est un dispositif technique reposant sur des composants ayant une certaine probabilité d'être défaillants. Aussi le SIS n'élimine pas complètement le risque, mais le diminue seulement.

La norme NF-EN 61508 permet de définir un niveau de SIL (Safety Integrity Level) pour chaque composant.

Il y a deux modes de défaillances pour un élément ou une chaîne de commande:

- le déclenchement intempestif ou à tort, alors qu'aucun danger n'est présent; il ne conduit à aucune situation dangereuse, mais seulement à un coût opératoire injustifié consécutif à l'arrêt de production et éventuellement le déclassement d'une partie de la production. Il peut être dû à une détection erronée du capteur, une défaillance électronique de l'automate, d'un défaut d'air sur l'actionneur, ...
- la chaîne de commande devient incapable de fonctionner, et rien ne permet de le détecter tant qu'elle n'est pas sollicitée. Cela peut être dû à un capteur bouché ou bloqué et donc incapable de détecter correctement les variations du paramètre qu'il surveille, un actionneur ou une vanne grippés, ... En cas de situation anormale du procédé, l'action de sécurité prévue ne pourra pas être réalisée. Ce type de défaillance est parfois nommée "défaillance dangereuse". C'est elle qui est prise en compte dans la détermination du SIL de l'équipent. Le niveau de SIL correspond à une probabilité qu'a l'élément d'être défaillant lors de sa sollicitation (PFD : Probability of Failure on Demand).De même, le SIS qui est un assemblage d'éléments ayant chacun un certain niveau de confiance, peut être qualifié d'un SIL. La détermination du SIL d'un système répond à quelques règles :

- Le SIL d'un système comprenant des éléments en série est limité au SIL du maillon le plus faible ; le système ne fonctionne que si tous les éléments

fonctionnent.

- Le SIL d'un système comprenant des éléments en parallèle, correspond à la somme des SIL ; si chaque élément individuellement peut assurer la fonction, la probabilité que la fonction ne soit pas réalisée est plus faible que si l'élément le plus fiable était seul.

Exemple :

La pression d'un procédé est limitée par un système instrumenté composé de 2 capteurs de pression (SIL 1) traités en 1oo2 sur un automate de sécurité (SIL 2) et agissant sur une vanne (SIL 1).

La fonction de détection de pression sera qualifiée d'un SIL 2 puisqu'un seul capteur en état suffit pour détecter la pression et que l'automate est lui-même SIL 2, mais la fonction limitation de la pression qui implique le fonctionnement de la vanne n'est que SIL 1 à cause de l'élément « vanne ».
Le niveau de confiance d'un système ne dépend pas seulement de la qualité de ses éléments, mais aussi de la fréquence des tests réalisés pour vérifier leur bon fonctionnement. A noter que la plupart des détecteurs ou vannes sont maintenant fournis avec un certificat assurant du niveau de SIL de l'équipement, même s'il est destiné à la régulation de base du procédé. On pourrait conclure à tort, que ceci confère à l'installation un "certain niveau de sécurité". Il n'en est rien. Un SIS doit être totalement indépendant du système de conduite. Il est destiné à compenser des défaillances provenant du sytème de conduite, mais aussi d'erreurs opérateurs, d'un manque d'utilité, d'une matière première non conforme, ... Un SIS indépendant peut être nécessaire même si le système de conduite est très fiable.

Exemple de Redondance appliqué sur des détecteurs

Si le niveau de confiance d'un détecteur ne peut être augmenté, la multiplication des détecteurs peut augmenter le niveau de confiance du système. Les détecteurs redondants peuvent être de technologies différentes pour éviter les causes communes de défaillance.

La multiplication des détecteurs peut aussi augmenter la probabilité de détection à tort qui peut nuire à la disponibilité du procédé.

Différentes architectures sont possibles offrant différentes qualités de fiabilité et de disponibilité des installations:

Description	**Fiabilité**		**Dispo**
1oo1 (1 out of 1): un seul détecteur installé déclenchant systématiquement une action	SIL-1 SIL-2	-	+
1oo2 (1 out of 2) : deux détecteurs installés dont un seul suffit pour déclencher une action. Si l'un des deux est défaillant il provoquera un déclenchement à tort.	SIL-2 SIL-3	+	-
1oo2D (1 out of 2 avec diagnostic): deux détecteurs installés dont un seul suffit pour déclencher une action. Pour limiter les déclenchements à tort, une autosurveillance est prévue; par exemple, la différence entre les valeurs relevées par les deux capteurs est surveillée et initie une vérification si elle devient trop élevée.	SIL-2 SIL-3	+	+
2oo2 (2 out of 2) : deux détecteurs installés et les deux ensembles sont nécessaires pour déclencher une action , mais si l'un d'eux est défaillant, la chaîne de commande ne fonctionnera pas.	SIL-1	--	++
2oo3 (2 out of 3) : trois capteurs installés dont deux au moins sont nécessaires pour déclencher une action. Souvent nommé *système tripliqué*.	SIL-3	++	++

4- Niveau intégrité de sécurité (SIL) :

Les normes internationales de sécurité fonctionnelle CEI 61508 et CEI 61511 définissent une démarche d'analyse du niveau d'intégrité d'un systeme de sécurité. Elles permettent de dé finir le niveau d'intégrité de sécurité requis (SIL : Safety Integrity Level) pour une Fonction Instrumentée de sécurité par rapport a l'analyse de risque. Il n'y a pas de règle imposée par ces normes mais des méthodes d 'allocation du SIL , plus au moins adaptées en fonction du niveau de détail des analyses de risques réalisées au préalables ainsi que du type et du détail des informations disponibles .La réductions de risque ne cessaire apportée par les Fonctions Instrumentées de Sécurité, pour un objectif de risque résiduel défini, est de terminée en fonction de la contribution des autres systèmes de sécurité .

Les données nécessaires à la définition du SIL ne sont pas toujours disponibles ou n 'existent pas. Dans ce cas , il faut s 'appuyer sur le retour d 'expérience de l 'exploitant et l'expertise acquise dans des installations similaires. La norme CEI 61511 décrit plusieurs méthodes d'allocation de SIL. Certaines sont qualitatives (le graphe de risque ou la grille de criticité) et d'autres sont quantitatives (LOPA : Layer of Protection Analysais [30]

L'utilisation des niveaux SILs permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel menant aux évènements dangereux identifies pendant l'analyse de risque . Les SILs sont attribues aux fonctions de sécurité sur la base de l'étude des défaillances . Un SIS est en mode de fonctionnement a faible demande lorsque la fréquence de sollicitation est inférieure à une fois par an (1/an) ou inferieure au double de la fréquence des tests périodiques auxquels il est soumis. A partir de l'architecture du SIS réalisant la SIF faiblement sollicitée, la PFD avg est évaluée sur un intervalle [0, t]. Un SIS en mode de fonctionnement continu ou à forte demande implique une forte sollicitation du SIS. Il est considère lorsque l

a fréquence de sollicitation est élevée ou continue, c'est-à-dire qu'elle est supérieure à une fois par an (1/an) ou supérieure a deux fois la fréquence des tests périodiques. A partir de l 'architecture du système instrumente de sécurité réalisant la fonction instrumente e de sécurité fortement sollicitée , la PFH est évalue e sur un intervalle de temps [0, t]

La norme IEC 61508 relative a

l 'évaluation de performance des SIS établit la classification des systèmes étudies selon des niveaux de sécurité a partir du calcul de la PFDavg pour les SIS faiblement sollicites (moins d'une sollicitation par an) ou de la PFH dans le cas des SIS fortement sollicitées)

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 a partir d e la connaissance des risques associes au procède, 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 gravite de risque et de sa fréquence d'occurrence.

- Méthodes quantitatives: Il s'agit des méthodes qui permettent de calculer le PFD des SIS a partir des probabilités de défaillances de leurs composants . Les méthodes les plus rependues sont :
- Les équations simplifiées
- Les arbres de défaillances
- Les chaines de Markov: Cette technique est souvent utilise en sureté de fonctionnement lorsque l'on souhaite modéliser un système avec des composants a taux de défaillance constant et réparable . Il permet ainsi de faire une analyse dynamique du système .

5- 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 définit ces deux termes comme suit :

 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.

$$M+1 = N - K + 1$$

La proportion de défaillances en sécurité d"un sous-système (SafeFailure Fraction ou SFF)

$$SFF = \frac{\Lambda s + \lambda DD}{\lambda}$$

Les tableaux 2 et 3 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%	SIL 1	SIL 2	SIL 3
60% – 90%	SIL 2	SIL 3	SIL 4
90% – 99%	SIL 3	SIL 4	SIL 4
≥ 90%	SIL 3	SIL 4	SIL 4

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.

Tableau2.2.sous système type A[7]

SFF	Tolérances aux anomalies Matérielles (M)		
	0	1	2
$\leq 60\%$	non autorisé	SIL 1	SIL 2
$60\% - 90\%$	SIL 1	SIL2	SIL 3
$90\% - 99\%$	SIL 2	SIL 3	SIL 4
$\geq 90\%$	SIL 3	SIL 4	SIL 4

Un SIS peut être considéré du type Busine des trois conditions régissante type A n'est pas satisfaite.

Tableau2.3.sous système type B

Chapitre IV :

Recommandation

1- Tests de fonctionnement :

La fréquence des tests de fonctionnement est un élément important dans la détermination du niveau de SIL d'une chaîne de commande. Plus la fréquence des tests est élevée, plus grande sera le niveau de confiance accordé au système. Le test des SIS est obligatoire avant chaque démarrage d'une installation, pour s'assurer qu'aucune modification intempestive, désactivation temporaire oubliée, ne persiste au démarrage. Ces tests sont aisés à faire tant que l'installation est à l'arrêt.

Les tests des SIS au moins une fois par an est nécessaire pour assurer un niveau de SIL élevé (>1). C'est difficile à réaliser pour des unités fonctionnant en continu sur plusieurs années. Les équipements modernes basés sur des technologies numériques permettent de contourner cette difficulté:

- lorsque plusieurs capteurs sont employés pour mesurer un même paramètre, il est possible de mettre en place une détection de la différence de valeur relevée entre les deux capteurs; si une différence significative apparait entre les deux mesures, une alarme est déclenchée invitant à rechercher lequel est défaillant.
- les vannes peuvent être équipées de positionneurs numériques permettant des fermetures partielles des vannes, sans conséquence sur le fonctionnement de l'installation, mais permettant de s'assurer périodiquement du bon fonctionnement de la chaîne de commande. Ces tests peuvent être automatisés.

2- Exemples de configurations :

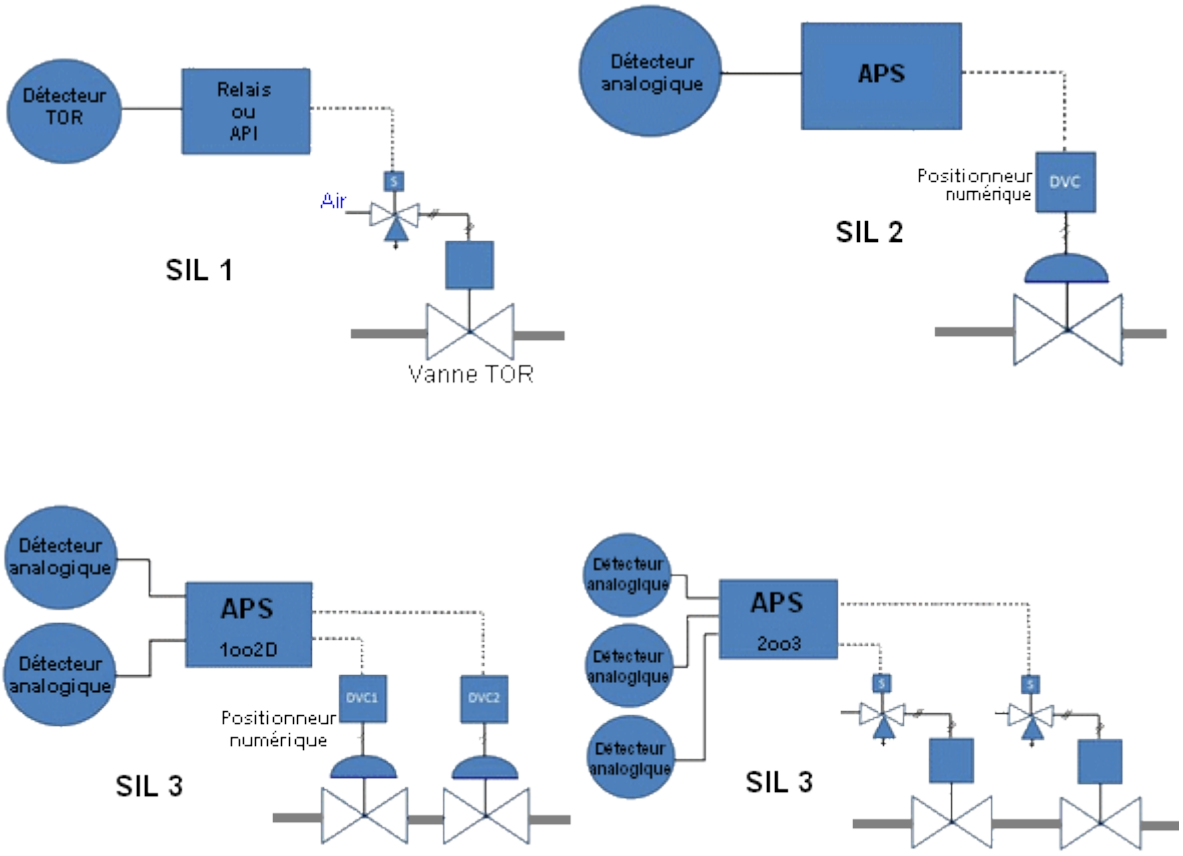


Figure 4.1 : Concept de couches de protection

3- la contribution de SIS dans la prévention et protection du risque

L'application de couches de protection multiples pour mettre le procédé en sécurité est souvent utilisée dans les industries de transformation [WIE 02]. Pour ce type d'industries, l'installation en sécurité peut être définie par une situation où tous les risques sont réduits à un risque tolérable [KNE 02]. Des critères clairs et non ambigus doivent être définis en regard des niveaux de risque tolérable. Des mesures pour la mise en sécurité du procédé doivent être dédiées à chaque spécificité de protection. Par exemple, pour protéger une unité particulière d'une installation contre une surpression, les dispositions de sécurité doivent se rapporter à la première couche comprenant un transmetteur de pression, une unité de traitement et un

actionneur et à la seconde couche de protection comportant une soupape de sécurité de surpression. Les deux couches de protection forment des systèmes relatifs à la sécurité (Safety related systems SRS). La première couche est composée par des systèmes à base de technologie E/E/EP (électrique, électronique et électronique programmable). Ce type de systèmes est appelé systèmes instrumentés de sécurité (SIS). La seconde couche désigne les SRS de type mécanique.

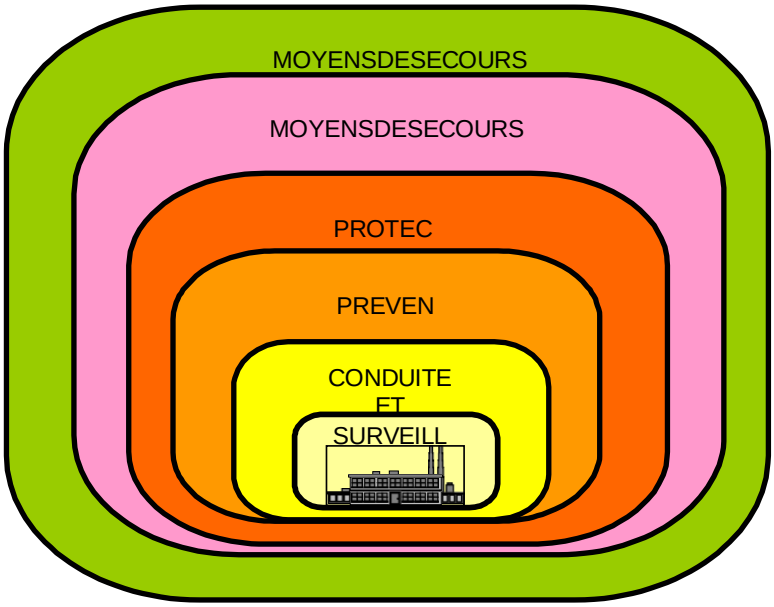


Figure 4.2: Concept de couches de protection

La figure 4.2 montre le concept des couches de protection et la composition des différents types de systèmes relatifs à la sécurité (SRS) comme définis dans la norme CEI 68511 -3. Il est à noter qu'il existe une distinction claire entre les BPCS et les SIS comme composantes des couches de protection. L'objectif primaire d'un BPCS est d'optimiser les conditions de conduite de procédé afin de maximiser la qualité et la production. Les systèmes instrumentés de sécurité s'appliquent pour prévenir des situations dangereuses (prévention) et réduire les conséquences d'événements dangereux (protection). La distinction est motivée par le fait que le BPCS n'est MOYENS DE SECOURS nécessairement pas utilisé pour contribuer à la réduction de risque et parfois il est lui-même source de risques potentiels.

Les méthodes de réduction sont de différents types et concernent tout d'abord le procédé dont la conception doit être plus au moins sûre. La conduite et la surveillance sont assurées par les systèmes de commande de procédés de base (BPCS), les systèmes de surveillance (alarmes du procédé) et par la surveillance des opérateurs.

La partie prévention des couches de protection est assurée par les dispositifs de sécurité mécaniques, par les alarmes suivies d'action et par les systèmes instrumentés de sécurité de prévention. La protection est assurée par des dispositifs de sécurité mécaniques, la supervision par l'opérateur et par les systèmes instrumentés de sécurité d'atténuation [KNE 02]. Les moyens de secours internes et externes concernent respectivement les procédures d'évacuation lors de l'occurrence d'une situation critique ainsi que la réaction du public après une radiodiffusion d'urgence.

Il faut noter qu'il existe un amalgame à propos de l'emplacement des systèmes instrumentés de sécurité comme couche de protection. Certains auteurs qualifient la couche allouée à ce type de systèmes comme une couche de prévention [KNE 02] (la norme aussi d'ailleurs) [CEI 03] alors que ce type de systèmes est voué uniquement à la protection par la réduction du risque nécessaire de telle sorte que ce risque devienne tolérable.

Il faut aussi différencier le BPCS qui est le système de commande de base du processus et le SIS qui est le système instrumenté de sécurité. En effet, le BPCS est aussi composé de capteurs, de régulateurs et d'éléments finaux. Bien que les architectures apparaissent similaires, les fonctions diffèrent beaucoup entre le BPCS et le SIS [GOB 05]. La fonction primaire d'une boucle de régulation est généralement de maintenir une variable de processus dans des limites prescrites. Le SIS surveille une variable de processus et ordonne l'action lorsque c'est exigé.

Les SIS sont rarement activés et durant les opérations normales du processus, ils demeurent statiques, dormants. La période moyenne entre

l'occurrence d'événements dangereux est souvent estimée à plus d'une dizaine d'années [GOB 05]. Avec le BPCS, les signaux de commande sont normalement dynamiques. Les modes de défaillances diffèrent aussi entre un BPCS et un SIS. Pour éviter qu'une cause unique ou cause commune affecte simultanément les fonctions de contrôle (BPCS) et de sécurité (SIS), la norme IEC 61508 recommande [SMI 04]:

- ✓ pour les fonctions à faible criticité (SIL1 à 2) : la distinction des fonctions de pilotage et de sécurité notamment du point de vue logiciel. A ce niveau, la norme autorise l'utilisation d'équipements (matériels) communs qui assurent simultanément des fonctions de pilotage et de sécurité, ils sont alors considérés comme des SRS et doivent êtres conçus comme tels, notamment du point de vue du SIL.
- ✓ pour les fonctions à criticité moyenne (SIL2 à 3) : distinction de la circuiterie, (électrique, ou autre : pneumatique par exemple), des capteurs et actionneurs.
- ✓ pour les fonctions à haute criticité (SIL4) : séparation intégrale physique, électrique et, dans la mesure du possible, géographique des systèmes.

Conclusion

Conclusion :

Conclusion

Ce projet de fin d'études a permis de mieux comprendre le rôle essentiel des Systèmes Instrumentés de Sécurité (SIS) dans la maîtrise des risques industriels. L'approche adoptée, fondée sur l'analyse des scénarios dangereux et l'évaluation des niveaux de risque, a mis en évidence l'importance d'une démarche rigoureuse pour la détermination du Safety Integrity Level (SIL) adapté à chaque fonction de sécurité.

L'étude a montré que le respect des exigences de la norme IEC 61508 est crucial pour garantir un niveau de sécurité fiable et proportionné aux dangers identifiés. En identifiant les fonctions critiques et en proposant des SIL appropriés, ce travail contribue à la conception de systèmes plus sûrs et plus performants dans les environnements à haut risque.

Ce projet constitue ainsi une base solide pour aborder des problématiques industrielles complexes liées à la sûreté de fonctionnement, tout en ouvrant la voie à de futures améliorations en matière de gestion des risques et d'automatisation sécurisée.

Référence Bibliographique

Référence bibliographique :

Référence bibliographique

[1][DES95] : A. Desroches, « Concepts et méthodes probabilistes de base de la sécurité », Lavoisier, France, 1995

[2][INERIS-DRA35] : outils d'analyse des risques générés par une installation industrielle.

[3] DEBRAY.B, CHAUMETTE.S, DESCOURIERE.S, TROMMETER.V, Méthode d'analyse des risques génèrés par une installation industrielle.

[4] http://gpp.oiq.qc.ca/analyse_par_arbre_d_evenements.htm ade

[5] Norme CEI 61513, Centrales nucléaires : Instrumentation et contrôle commande des systèmes importants pour la sureté, Prescriptions générales pour les systèmes. Commission Electrotechnique Internationale, Genève, Suisse; 2001.

[6] [IEC62061 05] IEC62061. Sécurité des machines : Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs a la sécurités. International Electrotechnique Commission (IEC), 2005.

[7] S. Sklet. Safety barriers: Definitions, classification and performance. Journal of Loss Prevention in the process industries, vol 19, pp 494-506; 2005.

[8] [IEC61508 02] IEC 61508. Sécurité fonctionnelle des systèmes électriques/électroniques électroniques programmables relatifs à la sécurité, partie 6, mars 2002.

[9] [IEC61508 10] IEC 61508 : Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - Partie 1 : exigences générales

[10][Ayault 05] : N.Ayault. Evaluation des barrières techniques de sécurité. INERIS, février 2005.

[11] [LAM 02] P.Lamy. Probabilité de défaillance dangereuse d"un système explications e t exemple de calcul. INRS, septembre 2002.

[12][OHS 99]: OHSAS 18001, Système de management de la sante

Référence bibliographique :

et de la securite au travail- Spécification -BSI, AFNOR, 1999.

Référence bibliographique

[13] [IEC 00] CEI 61508. Sécurité fonctionnelle des systèmes électriques/électroniques /électroniques programmables relatifs à la sécurité. Commissions Electrotechnique Internationale, Genève,Suisse, 2000.

[14] [FAL 00] E.Fal, J.Ldurka. Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de process industriels. INERIS, 2000

[15] F. 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 ; 2008.

[16] 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.

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

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

[19] M.A. Lundteigen, et M. Rausand, Spurious activation of safety instrumented systems in the oil

[20] 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.

[21] Circulaire du 29 septembre 2005 relatif aux critères d'appréciation de la démarche de maitrise des risques d'accidents susceptibles de survenir dans les établissements dits « SEVESO », vises par l'arrête

Référence bibliographique :

du 10 mai 2000 modifié, Ministère de l'Ecologie et du Développement Durable, France[29] Layer of Protection Analysis, simplified process risk assessment. CCPS of the AICHE, New York,2001.

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

Référence bibliographique

[23][OHS18001,1999] : système de management de la santé et de la sécurité au travail –spécification

[24] Article : ALLOCATION DE SIL REQUIS DES FONCTIONS INSTRUMENTEES DE SECURITE D'UNEINSTALLATION LORSQUE L'ANALYSE DE RISQUE EST IMCOMPLETEA djadj Ahmed, Charpentier Dominique

[25] Schonbeck, M., Rausand, M., and Rouvroye, J,Human and organisation alfactors in the operational phase of safety instrumented systems : A new approach. Safety Science, 48 :310-318, 2010.

[26]] Mkhida, A, Contribution à l‟ évaluation de la su ̂retede fonctionn ement desSystemes Instrumentes de Sécurité ́ intégrant de l‟Intelligence. PhD thesis,Nancy Université ́ , Institut National Polytechnique de Lorraine,France, 2008.

[27].] ISA-S84. Application of safety instrumented systems for process industries, 01.1996.

[28].A. Summers. Simplified methods and fault tree analysis- Viewpoint on ISA TR84.0.02. ISA Trans 2000;

[29]. T.Zhang, W. Long, Y.Sato. Availability of systems with selfdiagnostic components applying Markov model to IEC 61508-6. Reliab Eng System Saf, 2003.

[30]. J. Bukowski. A comparison of techniques for computing PFD average. In: Proceedings of the annual reliability and maintainability symposium, 2005.

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

Référence bibliographique :

[32] 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.

[33][DES 03] : A. Desroches, A. Leroy, and F. Vallée, « La gestion des risques :principes et pratiques », Lavoisier, France, 2003.

[34] Principes de science et de fonctionnement des réacteurs . Groupe de formation technique. Instrumentation fondamentale : Appareils de mesure et régulation. page 124, 2010.

[35]R RHODE ENSEMBLE SCOLAIRE PRADEAU LA SEDE. régulation analogique. 2005.

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

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

[38] SCARIA industrie. notice d'instruction originale. Manuel d'utilisation SAM 500, 2017.

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

[40] Endress and Hauser people for process automation. Sécurité´ fonctionnelle . sil les systèmes instrumentes de sécurité´ dans l'industrie des process. 2014.

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

[42] OREDA participants. OREDA Project Manager. OREDA. osher reliability Data HandBook, 2002.

[43][ISO 02]: ISO, « Management du risque : Vocabulaire, Principes directeurs pour l‟utilisation dans les normes », Organisation internationale de normalisation, 2002.

[44][Jean-Paul La coursière, 2012]

[45] Norme CEI 61508, Sécurité fonctionnelle des systèmes électriques /

Référence bibliographique :

électroniques / électroniques programmables relatifs à la sécurité – Parties 1 à 7, octobre 1998-2000. Commission Electrotechnique Internationale, Genève, Suisse.

[46] Norme CEI 61511, Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le domaine de la production pour processus – Parties 1 à 3, janvier 2003-juillet 2003. Commission Electrotechnique Internationale, Genève, Suisse.

[47][ISO] : ISO/CEI Guide 51, Aspects liés à la sécurité : Principes directeurs pour les inclure dans les normes. Organisation internationale de normalisation (ISO); 1999.and gas industry: basic concepts and formulas. Reliability Engineering and System Safety, 93:1208–1217; 2008 INERIS, Direction des risqué Accidentels. France