



الجمهورية الجزائرية الديمقراطية الشعبية  
République Algérienne Démocratique et Populaire  
وزارة التعليم العالي والبحث العلمي  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة وهران 2 محمد بن أحمد  
Université d'Oran 2 Mohamed Ben Ahmed  
-----  
معهد الصيانة والأمن الصناعي  
Institut de Maintenance et de Sécurité Industrielle

Département de sécurité industrielle et environnement  
**MÉMOIRE**

Pour l'obtention du diplôme de Master

**Filière :** Hygiène et Sécurité industrielle  
**Spécialité :** sécurité prévention et intervention

**Thème**

**Détermination du sil dans un site de stockage  
des hydrocarbures :centre GPL**

Présenté et soutenu publiquement par :

**BENGHEZALA Mohamed**

**BEKAI Bouziane**

Devant le jury composé de :

Nom et Prénom	Grade	Etablissement	Qualité
ZOUARI Saim	MAA	IMSI	Président
AISSANI Nassima	MCA	IMSI	Encadreur
BENOMAR Fatima	MCA	IMSI	Examineur

Année 2022/2023

# REMERCIEMENT

Nous tenons à exprimer nos plus sincères remerciements à notre encadreur **Madame AISSANI Nassima**, maitre de conférences à l'institut de maintenance et de sécurité industriel, pour son soutien inconditionnel, son expertise et son engagement tout au long de la réalisation de ce mémoire. Sa précieuse guidance et ses conseils éclairés ont été d'une aide inestimable pour mener à bien cette recherche. Nous sommes reconnaissants pour sa disponibilité, sa patience, ainsi que pour sa contribution significative à notre développement académique et professionnel. Nous souhaitons également exprimer notre gratitude envers notre Co-encadreur, **MOURAD HENNINI**, ingénieur de renom, pour sa collaboration étroite et ses apports essentiels. Son expérience pratique et ses connaissances approfondies ont enrichi notre compréhension des enjeux techniques et ont contribué à la qualité globale de ce mémoire. Nous sommes reconnaissant(e)s pour son soutien constant et sa volonté de partager son expertise.

Un remerciement spécial est également adressé à Monsieur **GUETARNI Islam Hadj Mohamed**, Maître de Conférences à l'institut de maintenance et de sécurité industrielle, dont l'enseignement et les conseils nous ont été d'une grande valeur tout au long de notre parcours. Sa passion pour le sujet, sa rigueur académique et son dévouement à l'égard de ses étudiants ont été une source d'inspiration et de motivation pour nous. Nous lui sommes reconnaissant(e)s pour son soutien indéfectible et ses précieuses remarques.

Enfin, nous souhaitons exprimer notre profonde reconnaissance envers les deux jurés, le président et l'examineur, monsieur **ZOUARI Saim** et madame **BENOMAR Fatima**, Leur expertise et leur évaluation rigoureuse ont contribué à l'amélioration de ce mémoire. Nous les remercions pour leur temps et leurs commentaires constructifs, qui ont enrichi notre réflexion et ont permis de consolider nos connaissances.

Nous tenons à remercier chaleureusement toutes ces personnes qui ont joué un rôle essentiel dans la réalisation de ce mémoire. Leur soutien, leur expertise et leur engagement ont été d'une importance capitale, et nous sommes honorés d'avoir eu l'opportunité de travailler avec eux tout au long de ce projet.

## ***Résumé***

Une gestion des risques adéquate est essentielle dans toutes les activités industrielles pour prévenir les incidents et réduire les conséquences potentielles. Les méthodes d'analyse des risques, telles que HAZOP, l'analyse préliminaire des risques, l'arbre de défaillance et LOPA, sont utilisées pour une gestion systématique. Dans le cadre du mémoire de recherche sur les installations GPL de l'entreprise NAFTAL, la norme CEI 61508 est utilisée comme référence pour l'évaluation des niveaux de sécurité. Une étude de cas est réalisée pour évaluer les risques au sein de l'entreprise et déterminer le niveau SIL de la fonction instrumentée choisie. Le but principal de notre travail est de déterminer et évaluer le niveau d'intégrité de sécurité du « système détection G&F » du hall d'emplissage (situé au niveau du centre enfuteur CE141 NAFTAL). Par l'application de la méthode HAZOP intégrée avec un graphe de risque, le niveau SIL cible est déterminé et comparé au niveau SIL réel calculé par utilisation méthode d'arbre de défaillance à partir des données de défaillance réelles du système.

Les résultats obtenus permettent de recommander des mesures préventives visant à améliorer la sécurité des installations et à réduire les risques associés, assurant ainsi un environnement plus sûr pour les opérations industrielles.

**Mots clés :** SIL, SIF, SIS, HAZOP, système de détection F&G LOPA APR ADD

## ***Abstract:***

Adequate risk management is essential in all industrial activities to prevent incidents and mitigate potential consequences. Risk analysis methods, such as HAZOP, preliminary risk analysis, fault tree analysis, and LOPA, are employed for systematic risk management. In the context of the research thesis on GPL installations at NAFTAL company, the CEI 61508 standard is used as a reference for assessing safety levels. A case study is conducted to evaluate risks within the company and determine the SIL level of the chosen instrumented function. The main objective of our work is to determine and evaluate the safety integrity level of the "G&F detection system" in the filling hall (located at CE141 NAFTAL filling center). By applying the HAZOP method integrated with a risk graph, the target SIL level is determined and compared to the actual SIL level calculated using the fault tree analysis method with real system failure data. The obtained results enable the recommendation of preventive measures aimed at enhancing installation safety and reducing associated risks, thereby ensuring a safer environment for industrial operations.

**Keywords:** SIL, SIF, SIS, HAZOP, F&G detection, system, LOPA, PRA, FTA

## ***Dédicaces***

*A mon cher père A ma chère mère A ma famille A tous mes amis amine*

*Mohamed Halim Abed bassat Redha*

*A ceux que j'aime **CH***

***BENGHEZALA MOHAMED***

## ***Dédicaces***

***A mon cher père A ma chère mère A ma famille A tous mes amis A ceux qui  
m'aiment A ceux que j'aime A MA PETITE SŒUR SOUNDOUS RITADJE***

**BEKAI BOUAZIANE**

## Liste d'abréviation :

<b>AAD</b>	Analyse par arbre d'événements
<b>ADD</b>	Arbre de défaillance
<b>AMDE</b>	Analyse des modes de défaillance, de leurs effets
<b>AMDEC</b>	Analyse des modes de défaillance, de leurs effets et de leur criticité
<b>APD</b>	Analyse préliminaire des Dangers
<b>API</b>	Automates programmables industriel
<b>APP</b>	Analyse par Arbre de Panne
<b>APR</b>	Analyse préliminaire des risques
<b>ATEX</b>	Atmosphère explosive
<b>BLEVE</b>	Boiling liquide expanding vapour explosion
<b>BPCS</b>	Basic Process Control System
<b>CEI</b>	Commission électrotechnique internationale
<b>DCS</b>	Disturbed Control System
<b>EPC</b>	Equipements de protection collective
<b>EPI</b>	Equipement de protection individuelle
<b>ERDP</b>	Entreprise du Raffinage et de la Distribution des produits Pétroliers
<b>ESD</b>	Emergency shutdown system
<b>EUC</b>	Equipement Under Control
<b>GPL</b>	Gaz de pétrole liquéfié
<b>HAZOP</b>	Hazard and Operability
<b>HRA</b>	Human Reliability Analysis
<b>HSE</b>	Health safety environment
<b>ICI</b>	Imperial Chemical Industries
<b>IEC</b>	International Electrotechnical Commission
<b>IPL</b>	Independant Protection Layer

<b>ISO</b>	Organisation internationale de normalisation
<b>LOPA</b>	Layer of Protection Analysais
<b>MADS</b>	Méthodologie d'Analyse de Dysfonctionnement des Systèmes
<b>MCP</b>	Manual Call Point
<b>MOSAR</b>	Méthode organisée systémique d'analyse des risques
<b>PDF</b>	Probability of failure on demand
<b>PFH</b>	Probability of failure per hour
<b>PID</b>	Piping and Instrumentation Diagram
<b>PLC</b>	Programmable Logic Controller.
<b>RIA</b>	Robinets d'incendie armés
<b>SIF</b>	Safety Instrumented Function
<b>SIL</b>	Safety integrity level
<b>SIS</b>	Safety Instrumented System
<b>SNCC</b>	Les systèmes numériques de contrôle-commande
<b>UCVE</b>	Unconfined Vapour Cloud Explosion
<b>UIC</b>	Union des Industries Chimiques

## Liste de figures :

Figure 1: Caractérisation du risque .....	5
Figure 2: Approche d'analyse des risques .....	11
Figure 3: Typologie des méthodes d'analyse du risque .....	12
Figure 4: Typologie des types de méthode d'analyse .....	13
Figure 5: Déroulement de la méthode HAZOP .....	17
Figure 6: Démarche pour l'élaboration d'un arbre des défaillances .....	24
Figure 7: exemple d'arbre des défaillances (VILLEMEUR, 1988) .....	25
Figure 8: Les couches de protection de LOPA.....	29
Figure 9: CEI 61508 et ses déclinaisons par secteur d'application .....	38
Figure 10: Structure générale de la norme IEC 61508 [IEC61508, 2002].....	39
Figure 11: Schéma d'un SIS simple .....	41
Figure 12: Schéma d'un SIS effectuant plusieurs taches .....	43
Figure 13: Schéma d'un SIS recevant plusieurs informations .....	43
Figure 14: fonction instrumentée de sécurité .....	44
Figure 15: Classification des défaillances selon leurs causes .....	48
Figure 16: Typologie des défaillances selon la norme CEI 61508.....	49
Figure 17: Classification des défaillances selon SINTEF .....	50
Figure 18: Graphe de hiérarchisation du risque présenté dans la norme CEI 61511-3.....	51
Figure 19: localisation de centre d'emplissage (Google Earth) .....	58
Figure 20: Organigramme de l'organisation .....	59
Figure 21: réservoirs de stockage .....	62
Figure 22: les différentes activités de l'entreprise.....	64
Figure 23: Analyse fonctionnelle d'un système G&F.....	73
Figure 24: analyse fonctionnelle de hall d'emplissage des bouteilles de gaz .....	78
Figure 25: Schéma PID butane du hall d'emplissage des bouteilles de gaz .....	79
Figure 26: Configuration de système G&F étudié dans hall d'emplissage .....	80
Figure 27: les différentes phases de développement d'un UVCE .....	81
Figure 28: les évènements distingués dans l'HAZOP sont répertoriés dans la matrice des risques.....	84
Figure 29: Graphe nombre de conséquences en fonction de la gravité et de la probabilité ...	110
Figure 30 L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ DD - partie1 .....	112
Figure 32 : L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ DD - partie2.....	113
Figure 33 : L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ DD - partie3.....	114
Figure 34 : L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ DU - partie1 .....	115
Figure 35 : L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ DU- partie2.....	116



Figure 36 : L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ DU - partie3 .....	117
Figure 37 : L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ SD - partie1 .....	118
Figure 38 : L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ SD - partie2 .....	119
Figure 39 : L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ SD - partie3 .....	120
Figure 40 L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ SU - partie1 .....	121
Figure 41 L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ SU - partie2 .....	122
Figure 42 L'arbre des défaillances du système instrument de sécurité par utilisation $\lambda$ SU - partie3 .....	123

## Liste de tableau :

Tableau 1: Exemple d'interprétation des mots-clés .....	15
Tableau 2: Exemple de tableau HAZOP .....	17
Tableau 3: Exemple de tableau de type « APR » .....	20
Tableau 4: Symboles des évènements dans les arbres de défaillances.....	26
Tableau 5: Symboles des portes dans les arbres de défaillances.....	26
Tableau 6: Différentes couches dans les différentes catégories selon LOPA .....	30
Tableau 7: les niveaux de SIL .....	46
Tableau 8: Légende de la classification des paramètres de risques .....	52
Tableau 9: produits stockes .....	60
Tableau 10: Installations et Bâtiments principaux .....	61
Tableau 11: Tableau HAZOP.....	86

# Table des matières

Introduction générale .....	1
CHAPITRE I Présentation des méthodes d'analyses et leurs typologies .....	3
Introduction : .....	4
1. Notions générales : .....	4
1.1 Notion de danger.....	4
1.2 Notion de risque.....	4
1.3 Risque industriel majeur : .....	5
1.4 Notion de sécurité .....	5
1.5 Notion système : .....	6
1.6 Processus de gestion des risques : .....	6
1.6.1 Identification des risques : .....	6
1.6.2 Analyse des risques : .....	7
1.6.3 Evaluation des risques : .....	8
1.6.4 Traitement des risques : .....	9
1.6.4 Maîtrise des risques.....	10
1.7 Outils d'analyse des risques.....	11
1.7.1 Classification des méthodes et outils d'analyse des risques .....	11
1.8 Méthodes quantitatives vs qualitatives. ....	12
1.8.1 Méthodes quantitatives .....	12
1.8.2 Méthodes qualitatives .....	13
2. Les méthodes d'analyses les risques .....	14
2.1 La méthode HAZOP .....	14
2.1.1 Historique et domaine d'application .....	14
2.1.2 Déroulement.....	16
2.1.3 Limites et l'avantages .....	18
2.2 Analyse préliminaire des risques (APR).....	18
2.2.1 Historique et définition : .....	18

2.2.2 Les principes :	19
2.2.3 Déroulement	19
2.2.4 Limites et l'avantage	20
2.3 Arbre de défaillance	20
2.3.1 Historique et domaine d'application	21
2.3.2 Principe	21
2.3.3 Définition et l'événement redouté	23
2.3.4 Élaboration de l'arbre	23
2.3.5 Représentation graphique	26
2.3.6 Avantages et Limites :	27
2.4 LOPA	28
2.4.1 Définition	28
2.4.2 Domaine d'application	29
2.4.3 Les différentes couches de protection :	29
2.4.4 Processus de déroulement méthode LOPA	30
2.4.5 Les avantages de méthode LOPA	32
2.4.6 Les inconvénients de méthode LOPA	33
Conclusion	34
CHAPITRE 2 : Méthode d'analyse de niveau de SIL et définition des SIL	35
Introduction :	36
1. La norme CEI 61508	36
2. Norme CEI 61511	38
3. Sécurité fonctionnelle	39
3.1.1 Systèmes relatifs aux applications de sécurité	40
4. Les systèmes instrumentés de sécurité	40
4.1 Définition	40
4.2 La composition d'un système instrumenté de sécurité	41
4.2.1 Composition minimale d'un SIS	41
4.2.2 Composition d'un SIS en fonction des tâches à accomplir	42
5. Fonction instrumentée de sécurité :	43
6. Intégrité de sécurité	45
7. Niveau d'intégrité de sécurité	45

8. Mode de fonctionnement d'un SIS .....	45
8.1 Faible sollicitation .....	45
8.2 Forte sollicitation .....	45
9. Test relatif aux SIS .....	46
9.1 Rôle des tests .....	46
10. Classification retenue dans la norme CEI 61508 .....	46
10.1. Classification des défaillances selon leurs causes .....	46
10.2. Classification des défaillances selon leurs effets sur la fonction de sécurité : .....	48
10.3. Classification proposes par SINTEF .....	49
11. Méthodes qualitatives et quantitatives pour la détermination des SIL .....	50
11 .1 Méthodes qualitatives : .....	51
11.2. Les méthodes quantitatives .....	53
Conclusion.....	53
<b>CHAPITRE 3 Présentation du cas d'étude .....</b>	<b>54</b>
Introduction .....	55
1. L'entreprise NAFTAL.....	55
1.1. Historique .....	55
1.2. Présentation de l'entreprise.....	55
1.3. Présentation de la branche GPL.....	56
1.3.1. Services et produits : .....	56
2. Présentation de la branche GPL CE 141 TIARET .....	57
2.1. Description générale : .....	57
2.2. Situation Géographique : .....	58
2.3. Organigramme de l'organisation : .....	59
2.4. Les zones d'entreprise : .....	59
2.5. Produits stockés : .....	60
2.6. Installations et Bâtiments principaux : .....	61
2.7. Description des Réservoirs de Stockage : .....	62
2.8. Activités de l'entreprise .....	63
2.9. Les Moyens de Prévention au niveau du centre : .....	64
2.9.1. Réseau anti-incendie : .....	65
3. Système F&G .....	65

3.1. Fonction de base de système G&F .....	66
3.2. Détection.....	67
3.2.1 Emplacements concernés .....	67
3.2.2 Fonctions de base .....	67
3.2.3. Détection .....	67
3.2.4. Les types de détecteurs : .....	68
3.3. Unité centrale.....	70
3.3.1. Définition : .....	70
3.3.2. Les fonctions de système de traitement (détection) : .....	70
3.4. Action .....	70
3.4.1. Alarme.....	70
3.4.2. Electrovanne.....	71
3.4.3. Electrovanne gaz on/off .....	71
3.5. Description fonctionnement système G&F .....	72
3.6. Analyse fonctionnelle d'un système G&F.....	72
Conclusion : .....	74
<b>CHAPITRE 4 Analyse et recommandations .....</b>	<b>75</b>
Introduction .....	76
1. Description du hall d'emplissage.....	76
1.1. L'analyse fonctionnelle d'un hall d'emplissage des bouteilles .....	78
1.2. PID butane d'un hall d'emplissage.....	79
1.3. Configuration de système G&F étudié dans hall d'emplissage.....	80
1.4. Risques et dangers au niveau du centre emplisseur 141 GPL Tiaret.....	81
2. Analyse HAZOP .....	83
2.1. Matrice de risque.....	84
2.2. Tableau HAZOP .....	86
2.3. Interprétation des résultats .....	110
2.4. Résultats de l'allocation de niveau d'intégrité de sécurité « SIL » par graphe de risque .....	111
3. Arbre de défaillance : .....	111
3.1. Présentation arbre de défaillance .....	111
3.1.1. Calcule la probabilité de défaillance SIS par utilisation $\lambda_{DD}$ taux de défaillance aléatoire dangereuse du matériel détectable .....	112

3.1.2 Calcule la probabilité de défaillance SIS par utilisation $\lambda_{DU}$ taux de défaillance aléatoire dangereuse des matériels indétectables. ....	115
3.1.3. Calcule la probabilité de défaillance SIS par $\lambda_{SD}$ taux de défaillance aléatoire en sécurité du matériel défectable .....	118
3.1.4. Calcule la probabilité de défaillance SIS par $\lambda_{SU}$ taux de défaillance aléatoire en sécurité du matériel défectable indétectable : .....	121
3.2. Analyse résultats d'arbre de défaillance .....	124
4. Interprétation des résultats : .....	124
5. Recommandation.....	125
Conclusion générale : .....	127
Bibliographie .....	128
Annexe .....	131

## Introduction générale

Avec le développement industriel, les entreprises se préoccupent désormais non seulement des performances de leurs systèmes en termes de qualité et de rentabilité, mais également de leur sécurité. Il existe de nombreuses approches et mesures à prendre pour réduire les risques, qui sont diversifiées. La conception du procédé et la sélection des équipements jouent un rôle essentiel dans la diminution des risques.

Malheureusement, ces méthodes ne sont pas toujours adéquates. C'est pourquoi des systèmes spécialisés, connus sous le nom de Systèmes Instrumentés de Sécurité (SIS), sont utilisés pour réduire les risques d'événements dangereux et assurer automatiquement la protection des personnes, des équipements et de l'environnement.

Les normes IEC 61508 et IEC 61511 établissent une classification en quatre niveaux d'intégrité de sécurité (Safety Integrity Level) pour une fonction de sécurité, offrant ainsi quatre niveaux potentiels de SIL.

Pour mettre en place des SIS dans un système, il est nécessaire de déterminer préalablement le SIL (Safety Integrity Level) que la fonction instrumentée devrait atteindre. L'évaluation du niveau d'intégrité de sécurité se fait en utilisant à la fois des méthodes qualitatives et quantitatives.

Parmi les méthodes qualitatives les plus utilisées pour déterminer le niveau de SIL d'une SIF on trouve la méthode matrice de risque qui est décrite dans la norme IEC 61508. Lorsque cette méthode est mise en œuvre, divers paramètres de simplification sont introduits pour décrire la nature de la situation dangereuse en cas de défaillance ou d'indisponibilité des systèmes de sécurité. Parmi ces paramètres, un paramètre est sélectionné parmi quatre groupes caractéristiques de risque, puis les paramètres choisis sont combinés pour décider du niveau de SIL requis pour les systèmes de sécurité. Une autre méthode couramment utilisée est le graphe de risque, qui permet d'obtenir le niveau de SIL requis en fonction de quatre paramètres spécifiques.

L'architecture de la boucle SIF est généralement proposée par les experts en instrumentation, qui conçoivent des systèmes comprenant des équipements conformes au niveau SIL déterminé par l'étude d'allocation du SIL. Il est nécessaire de vérifier les niveaux de SIL des différentes architectures présentes sur site en utilisant des méthodes probabilistes telles que l'arbre de



défaillance. Ces méthodes permettent d'obtenir un niveau de SIL et de le comparer avec le niveau SIL cible obtenu à partir de l'allocation précédente.

La question qui se pose est de savoir quelle méthodologie adopter pour valider l'architecture du SIF installé dans le hall d'emplissage du centre CE141 de NAFTAL TIARET, et comment la comparer au niveau SIL cible.

Pour résoudre cette problématique, notre projet de fin d'études est organisé de la manière suivante :

Le premier chapitre concerne la définition de certains concepts utilisés dans le cadre de la sécurité industrielle et présentation des méthodes d'analyse et leur typologie.

Dans le deuxième chapitre, nous présenterons la sécurité fonctionnelle des systèmes de sécurité, définition de SIL et les méthodes qualitatives et quantitatives utilisées pour la détermination des SIL.

Le troisième chapitre présente une étude de cas portant sur l'entreprise NAFTAL et sa branche GPL. L'organisation de l'entreprise, les activités de la branche GPL et le système de détection et d'action (F&G) sont décrits en profondeur.

Le quatrième chapitre se concentre sur l'analyse fonctionnelle d'un hall d'emplissage des bouteilles dans l'entreprise, en mettant l'accent sur les risques et les dangers associés. Des méthodes telles que l'analyse HAZOP, l'arbre de défaillance et la matrice de risque sont utilisées pour évaluer et interpréter les résultats. SIL.

# CHAPITRE I

## Présentation des méthodes d'analyses et leurs typologies

## **Introduction :**

Chaque activité industrielle comporte des risques spécifiques qui nécessitent une gestion adéquate. La mise en place d'une gestion des risques appropriée permet d'identifier, évaluer et gérer ces risques de manière proactive, afin de prévenir les incidents et de réduire les conséquences potentielles.

Les méthodes d'analyse des risques sont des approches systématiques utilisées pour gérer ces risques. Le choix de la méthode ou des méthodes nécessaires pour réaliser l'analyse des risques est primordial.

Il existe donc des méthodes avec des objectifs différents, selon le besoin de l'entreprise dans la mise en place de son système dynamique de gestion des risques.

## **1. Notions générales :**

### **1.1 Notion de danger**

Selon Des Roches et la norme IEC 61508, les dangers définissent des problèmes qui peuvent nuire aux personnes, aux biens (endommagement ou destruction) ou à l'environnement.

Les dangers peuvent affecter les personnes directement, par des blessures ou des problèmes de santé, ou indirectement, par des dommages aux biens ou à l'environnement.

La norme OSHSAS 18001 définit un danger comme une source ou une condition qui peut causer des dommages par des blessures physiques ou des dommages à la santé, des dommages matériels à l'environnement de travail ou une combinaison de ces facteurs.

Il faut bien comprendre que de nombreux mots sont utilisés, tels que principes ou auteurs, autour de la notion de risque et la rendre claire. De plus, le dictionnaire combine le mot dangereux avec le mot peur. En fait, de nombreux dictionnaires recommandent le mot dangereux comme le même mot que dangereux, ce qui explique le fait qu'un grand nombre de personnes utilisent ces mots de manière interchangeable. Même les livres et les textes confondent risque et danger.

### **1.2 Notion de risque**

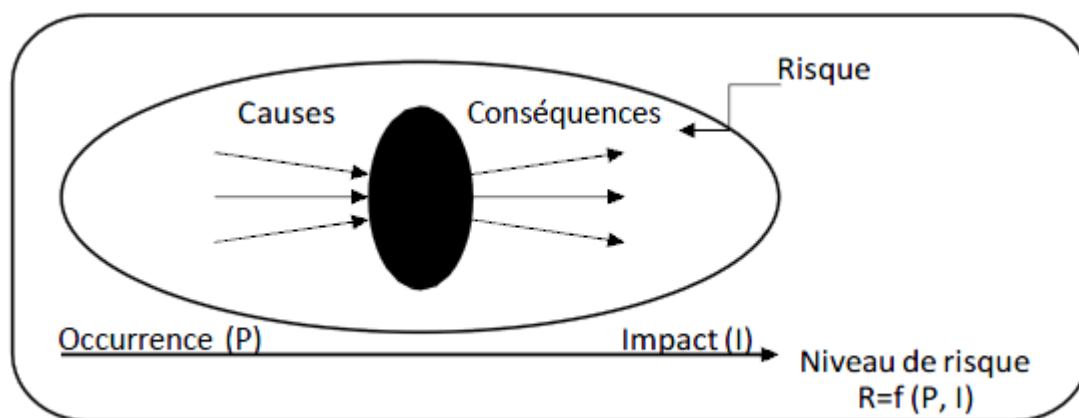
Le terme risque à plusieurs sens. De même, les facteurs de risque peuvent être de nature variable et plusieurs classifications ont été proposées. La définition du risque bidimensionnel est très proche.

Selon [Villemeur, 1998], le risque est un risque qui combine la mesure d'un événement négatif avec son effet ou résultat.

Et selon OHSAS 18001 [OHSAS18001, 1999], le risque est la combinaison de la probabilité et des conséquences.

Idéalement, le risque est :

- La gravité du dommage, suite à l'événement menaçant, selon la gravité (extrême, extrême, mineure, mineure, etc.). Ce processus prend en compte l'analyse des conséquences en termes de pertes humaines (blessures, décès) ou en termes économiques (paiements liés aux dommages, etc.).
- La nature de l'incertitude associée à la nature de la menace (fréquente, faible, impossible, etc.) cause des dommages à partir d'une situation dangereuse déterminée. Selon Gouri Veau, le risque peut être défini par la combinaison d'événements, de causes et de conséquences d'une situation donnée. Les événements peuvent être définis comme des causes par leur comportement (P) et des effets par leurs effets (I) (voir Figure 1). La combinaison de ces statistiques permet de créer un indicateur de risque  $R = f(\text{Occurrence}, \text{Impact})$ .



**Figure 1: Caractérisation du risque**

### 1.3 Risque industriel majeur :

Un risque industriel majeur est un événement accidentel se produisant sur un site industriel et entraînant des conséquences immédiates graves pour le personnel, les populations avoisinantes les biens et/ou l'environnement.

### 1.4 Notion de sécurité

La sécurité est souvent définie par son contraire : ce serait l'absence de danger, d'accident ou de catastrophe. La sécurité concerne la non occurrence d'événements pouvant diminuer ou porter

atteinte à l'intégrité du système, pendant toute la durée de l'activité du système, que celle-ci soit réussie, dégradée ou ait échoué.

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

### 1.5 Notion système :

La norme ISO/CEI 15288 :2008 définit un système comme « un ensemble d'éléments, en interaction dynamique, organisés en fonction d'un but ».

Cette description réunit en une phrase de quelque manière que ce soit toutes les parties importantes de ce qui sera utile, même si c'est nécessaire, et l'ingénieur dit au passage.

**Aspect fonctionnel** : le système sert, il en fait un but.

**Aspects structurels** : le système ne se réduit pas à un seul élément, ou à un agencement d'éléments interconnectés.

**Aspect comportemental** : composants du système qui fonctionnent ensemble pour produire un comportement (sortie) censé atteindre un objectif. Ce dernier point fait l'une des différences importantes entre l'approche systématique qui met l'accent sur la relation entre les éléments en considérant l'effet global de ces relations, et la recherche de processus qui réduit et considère ces choses individuellement, en se concentrant uniquement sur elle. Le type ou le type de relation entre ces choses.

### 1.6 Processus de gestion des risques :

#### 1.6.1 Identification des risques :

Le risque surgit lorsque le danger et la source d'exposition se rencontrent. Pour identifier les dangers, il est nécessaire de procéder à une cartographie des processus, qui clarifie les entrées et les sorties, ainsi que la contribution aux objectifs essentiels de l'organisation et les ressources utilisées.

Une fois ces processus identifiés, le diagnostic est réalisé en se concentrant sur deux aspects complémentaires : les processus d'un côté, et les installations de l'autre. Le premier permet de repérer les lacunes ou les dysfonctionnements de l'organisation, tandis que le second vise à détecter les failles dans la conception, l'adéquation, l'opération, l'entretien ou la maintenance des installations. L'objectif de cette identification des risques est d'établir une liste détaillée des

risques. Pendant cette phase, les principaux risques sont identifiés et décrits dans un catalogue des risques.

### 1.6.2 Analyse des risques :

Les risques identifiés à l'étape précédente sont évalués non seulement pour les hiérarchiser en termes de criticité mais aussi, pour comprendre la relation entre différents aspects des risques, tels que la vérification des interdépendances entre les risques.

Le processus d'analyse des risques comprend les étapes suivantes :

#### **Développement de réseaux de cause à effet pour les risques identifiés :**

Le but de la création de réseaux de cause à effet pour les risques identifiés est double : dans un premier temps, il permet l'exploration systématique et l'identification des causes profondes des risques identifiés au préalable, il permet aussi, dans un second temps, d'agrèger les risques identifiés dans une structure globale de causalité, ce qui permet la simplification et une amélioration de la transparence par l'agrégation d'un certain nombre de risques dans un réseau global de risques.

#### **Collecte de données :**

Dans l'étape de collecte de données pour la quantification des risques (probabilité et impact, ou distribution de probabilité), les données pertinentes pour quantifier les risques sont recueillies. Cela peut se faire de différentes façons et avec différents niveaux de précision et de détail. La compréhension qualitative du risque à l'étape précédente permet une prise de décision éclairée sur la précision qui est nécessaire à la quantification, et par conséquent la quantité et la précision des données nécessaires.

#### **Quantification et Qualification des risques**

Dans cette étape, les risques sont quantifiés selon les indications fournies par les parties prenantes et avec des méthodes appropriées selon le niveau de détail attendu et la fiabilité de l'évaluation. Il existe deux approches principales pour l'évaluation des risques. Une approche qualitative et une autre quantitative.

Dans l'approche qualitative, il y a lieu de tenir compte de différents facteurs tels que :

- Une description qualitative du risque ainsi que sa nature.
- Les conséquences de l'occurrence du risque (avec une description qualitative du potentiel des pertes ou des gains).

➤ La probabilité d'occurrence (il s'agit de donner un point de vue subjectif sur le fait de savoir si le risque se matérialise ou pas).

Les mesures n'ont généralement pas de valeur numérique et ne sont pas toujours pour la gestion des risques et ce, comparées à l'approche quantitative. Ce pendant et d'après les avis des experts, les méthodes qualitatives sont utilisées en cas d'absence de donnée quantitative.

Les approches quantitatives sont basées sur deux facteurs qui sont :

La probabilité d'occurrences de risque et l'impact du risque. Ainsi, par définition, Risque = Probabilité X impact

### **Compiler une liste des risques quantifiés**

Cette phase consiste en la tenue d'un catalogue des risques avec une mise à jour par des informations quantitatives. Les informations recueillies de la phase de quantification ajoutées au catalogue des risques devrait inclure :

- La quantification des risques
- Les méthodes par lesquelles ont été obtenues les quantifications
- Les données sur lesquelles la quantification a été basée
- La déclaration concernant la fiabilité de la précision de l'évaluation des risques (l'évaluation de

La précision doit dépendre de la sévérité du risque).

### **1.6.3 Evaluation des risques :**

L'évaluation des risques comprend les étapes suivantes :

#### **Comparaison quantitative des risques avec des seuils prédéfinis :**

Dans cette étape, le degré de risque déterminé lors de l'analyse des risques est comparé aux seuils d'acceptation. La décision sur l'acceptabilité des risques ne dépend pas seulement des nombres générés mais aussi, d'une évaluation attentive du contexte des risques et des facteurs qui n'ont pas été pris en compte par les modèles de quantification.

#### **Classement des risques :**

Les risques sont ensuite mis en rang selon la priorité qui leur a été assignée. Le classement des risques peut être divisé selon les zones de responsabilité.

Sélection des risques pour le traitement et la ré- analyse :

La sélection des risques pour le traitement doit impliquer les parties prenantes ainsi que, les personnes pour qui la responsabilité du traitement sera probablement affectée. Les décideurs peuvent également découvrir lors de cette étape, que les informations actuelles sur les risques sont insuffisantes.

### **Compilation de la liste des risques pour le traitement**

Dans cette étape, le catalogue des risques est mis à jour avec des informations sur les

Risques qui ont été sélectionnés pour le traitement. Ces informations devraient inclure :

- L'identification des risques pour le traitement.
- La réduction prévue des risques.
- Le coût prévu ou l'effort de réduction des risques.

#### **1.6.4 Traitement des risques :**

Cette phase englobe toutes les activités qui sont concernées par, la sélection et l'exécution

De mesures de traitement des risques supérieurs aux seuils. Elle comporte les étapes suivantes:

#### **Analyse du niveau de gestion et les actions possibles :**

Dans cette étape, des options de traitement alternatives pour réduire les risques sont identifiées.

Cette étape peut être éclairée par une analyse de la cause fondamentale du risque afin

De démontrer les points d'intervention possibles, en cas d'occurrence du risque, ou par la

Description de son impact, afin de déterminer les possibilités de minimisation de ses dommages.

Quelques stratégies de gestion des risques sont énumérées ci- dessous : **[25]**

- ✓ Stratégie d'évitement.
- ✓ Stratégie de contournement.
- ✓ Stratégie d'acceptation.
- ✓ Stratégie d'élimination.
- ✓ Stratégie d'acceptation avec réduction.
- ✓ Stratégie de transfert.



#### 1.6.4 Maîtrise des risques

Les risques étant identifiés, puis quantifiés et qualifiés, il reste à envisager de les maîtriser.

Maîtriser un risque, ce n'est pas l'éliminer à tout prix, mais le ramener économiquement à un niveau, qui soit accepté par l'ensemble des parties prenantes et des parties intéressées.

C'est prendre si nécessaire, des dispositions permettant de le réduire, en agissant sur sa probabilité d'occurrence (prévention) ou, sur une ou plusieurs composantes de sa gravité (protection). [24].

La première question que l'on doit se poser est de savoir si le risque est acceptable en l'état, compte tenu de sa criticité ou des efforts à engager pour le maîtriser davantage. Pour cela, le management de l'organisation définira une matrice d'acceptabilité.

Cette grille doit être validée au plus haut niveau de l'organisation, car elle décide des priorités dans le programme de maîtrise des risques donc, des coûts qui y sont associés, puisqu'à chaque zone de la matrice, correspond une stratégie de maîtrise.

Il sera prudent d'attendre la fin du recensement et de la hiérarchisation des risques pour construire la matrice d'acceptabilité, afin d'éviter que le nombre de risques inacceptables ne soit pas compatible avec les moyens financiers de l'organisation. On adoptera avec sagesse une démarche de progrès faisant croître graduellement la zone de risques inacceptables.

Pour traiter ses risques, l'organisation dispose d'une boîte à outils contenant des instruments de quatre types :

**•Outils d'organisation et de management :**

De prévention, par exemple des procédures opératoires, des consignes de sécurité, l'externalisation de certaines fonctions, la formation redondante,

De protection, tels que des plans de sauvegarde ou de survie, des fournisseurs redondants ;

**•Outils techniques :**

De prévention, tels que des détecteurs, des équipements de sécurité, des contrôles d'accès,

De protection, tels que des murs coupe-feu, des stockages cloisonnés, des équipements de protection individuels, des sauvegardes informatiques, des stocks de pièces détachées ou de produits finis, la partition des moyens, voire leur duplication (exemple : back-up informatique)

;

**•Outils juridiques :**

Des clauses contractuelles de limitation de responsabilités.

Des contrats de travail.

**•Financement :**

Des provisions pour risques,

Un crédit conditionnel,

Des rétentions,

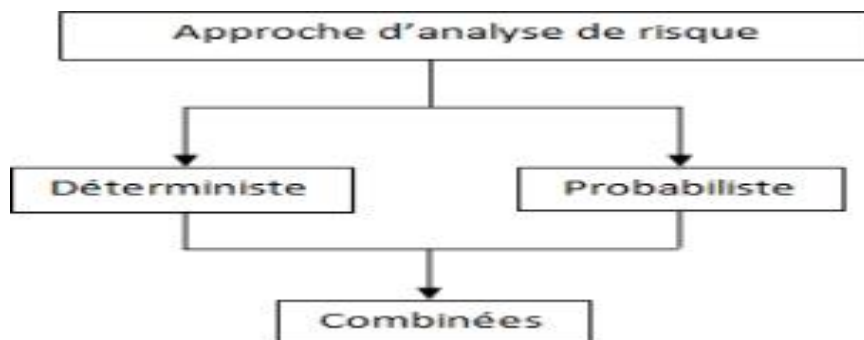
Des assurances.

**1.7 Outils d'analyse des risques**

Aujourd'hui les méthodes d'analyse des risques connaissent un fort développement en nombre, ainsi qu'une spécialisation en fonction de leurs domaines d'application. Cette partie se veut illustrative des méthodes à employer en matière de gestion des risques décrits précédemment.

**1.7.1 Classification des méthodes et outils d'analyse des risques**

D'une manière générale, l'évaluation du risque est probabiliste. Toute analyse de risques qui se veut aussi exhaustive que possible ne peut se priver d'éléments d'incertitude. Toutefois, s'agissant de la sûreté de fonctionnement d'une installation ou d'un système présentant des risques industriels, l'approche déterministe reste l'approche privilégiée.



**Figure 2: Approche d'analyse des risques**

**Approche déterministe**

L'approche déterministe a généralement été adoptée dans les domaines à haut risque tels que nucléaire, militaire, transports guidés, où le moindre risque significatif est traqué et réduit à la source. Elle consiste à recenser les événements pouvant conduire à un scénario d'accident en

recherchant le pire cas possible et en affectant une gravité extrême à ses conséquences potentielles.

Dans le domaine de la gestion des risques, les approches déterministes se concentrent sur l'évaluation des conséquences d'un accident. La maîtrise des risques consiste alors à s'assurer de la maîtrise des conséquences à l'aide de techniques de modélisation (modèle physique, modèle de contrainte) et de calcul déterministe à partir de scénarios d'accidents.

### **Approche probabiliste**

L'approche probabiliste repose sur le calcul de probabilités relatives à l'occurrence d'événements faisant partie du processus de matérialisation d'un scénario d'accident donné. Dans ce sens, la maîtrise des risques consiste alors à démontrer que la probabilité de survenue du risque est maintenue à des valeurs acceptables, si besoin est par la mise en place de mesures destinées à les réduire. L'évaluation des risques repose alors sur une analyse probabiliste des indices de probabilité et de conséquence.

Il s'agit d'une approche complémentaire qui permet d'analyser le dispositif de défense en profondeur décidé à l'issue d'une approche purement déterministe, ceci a été le cas dans le domaine nucléaire ou les techniques probabilistes viennent appuyer l'approche déterminé.

## **1.8 Méthodes quantitatives vs qualitatives.**



**Figure 3: Typologie des méthodes d'analyse du risque**

### **1.8.1 Méthodes quantitatives**

Les analyses quantitatives sont supportées par des outils mathématiques ayant pour but d'évaluer la sûreté de fonctionnement et entre autres la sécurité. Cette évaluation peut se faire par des calculs de probabilités ou bien par recours aux modèles différentiels probabilistes tels que les Chaines de Markov, les réseaux de Pétri, les automates d'états finis, etc.

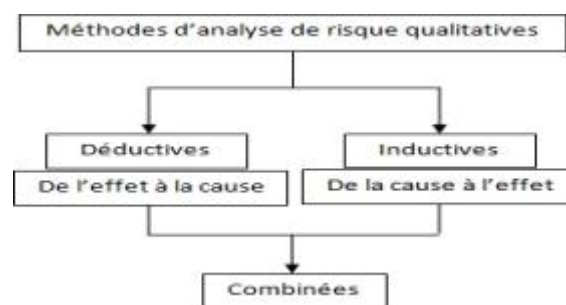
Quoique l'utilité des méthodes quantitatives soit indiscutable, ces dernières présentent tout de même un certain investissement en temps, en efforts et également en moyens (logiciels, matériels, financiers, etc.). Cet investissement peut être disproportionné par rapport à l'utilité des résultats attendus, ce qui va pousser au court-circuit de l'analyse pour laisser la place aux approximations qualitatives (statistiques, retour d'expérience, jugement d'expert, etc.).

### 1.8.2 Méthodes qualitatives

Il existe des méthodes qualitatives même si certaines mènent parfois aux estimations de fréquences d'occurrence avant la classification des risques, on cite : l'APR, l'AMDEC, l'arbre de Défaillances ou l'arbre d'événements.

L'application de ces méthodes fait systématiquement appel aux raisonnements par induction et par déduction comme l'ont très bien expliqué Montceau & Avaro, dans leurs ouvrages en 1990.

Les méthodes à caractère inductif ont une optique de recherche allant des causes aux conséquences éventuelles. En contrepartie, les méthodes déductives ont pour but de chercher les combinaisons de causes conduisant à des événements redoutés.



**Figure 4: Typologie des types de méthode d'analyse**

Il existe un grand nombre d'outils dédiés à l'identification des dangers et des risques associés à un procédé ou une installation, les suivants sont les plus fréquemment utilisés :

- L'analyse Préliminaire des Risques (APR).
- L'analyse des Modes de Défaillances, de leurs Effets et de leur Criticité (AMDEC).
- L'analyse des risques sur schémas type HAZOP ou « Wat-if ? ».
- L'analyse par arbre des défaillances.
- L'analyse par arbre d'événements.
- Le Nœud Papillon.

Ces outils pris individuellement ou combinés permettent le plus souvent de répondre aux objectifs d'une analyse des risques portant sur un procédé ou une installation. Néanmoins, pour des problématiques particulières, il est nécessaire de faire appel à des méthodes possédant un domaine d'application spécifique. C'est le cas par exemple pour la prise en compte des effets dominos entre installations ou l'examen des erreurs humaines.

D'une manière générale, le choix de retenir un outil particulier d'analyse des risques s'effectue à partir de son domaine d'application et de ses caractéristiques, il n'y a pas de bons ou mauvais outils d'analyse des risques. Ces outils ne sont que des aides guidant la réflexion et il convient donc de retenir les outils les mieux adaptés aux cas à traiter. D'ailleurs, ces outils peuvent être tout à fait complémentaires.

## **2. Les méthodes d'analyses les risques**

### **2.1 La méthode HAZOP**

La méthode HAZOP est une méthode d'analyse de risque inductive et très structurée dont l'objectif est l'identification exhaustive des risques à priori, c'est-à-dire avant que les incidents ne surviennent même si aucun historique d'incidents n'existe.

#### **2.1.1 Historique et domaine d'application**

La méthode HAZOP, pour Hazard Opérabilité, a été développée par la société Imperial Chemical Industries (ICI) au début des années 1970. Elle a depuis été adaptée dans différents secteurs d'activité. L'Union des Industries Chimiques (UIC) a publié en 1980 une version française de cette méthode dans son cahier de sécurité n°2 intitulés « Etude de sécurité sur schéma de circulation des fluides ». Considérant de manière systématique les dérives des paramètres d'une installation en vue d'en identifier les causes et les conséquences, cette méthode est particulièrement utile pour l'examen de systèmes thermo-hydrauliques, pour lesquels des paramètres comme le débit, la température, la pression, le niveau, la concentration... sont particulièrement importants pour la sécurité de l'installation. De par sa nature, cette méthode requiert notamment l'examen de schémas et plans de circulation des fluides ou schémas PID. [20].

La méthode HAZOP est un outil formalisé, systémique et semi-empirique utilisé et développé depuis quarante ans pour analyser les risques potentiels associés à l'exploitation d'une installation industrielle. Elle permet d'apprécier le niveau de dangerosité d'une installation.

Elle conduit à l'élimination ou la diminution des risques techniques à la source, en améliorant:

La protection du personnel d'exploitation.

La protection de l'environnement et des populations avoisinantes.

La sécurité, l'opérabilité, la maintenabilité, la fiabilité et l'intégrité physique de l'outil de protection.

La méthode **HAZOP** s'appuie sur la description détaillée des installations et des procédés. L'équipe de revue **HAZOP** examine chaque élément particulier (système par système, circuit par circuit, ligne par ligne, appareil par appareil, cet) afin de considérer d'une manière systématique les dérives possibles, grâce à la combinaison entre les mots-clés (Pas de, Plus de, Moins de, Trop de) et les paramètres définis au cours de la conception, en vue de décider si une situation dangereuse peut en résulter et d'en identifier les causes et les conséquences.

Mot-clé + Paramètre = Dérive

La norme CEI 61882 propose des exemples de mots-clés dont l'usage est particulièrement courant. Ces mots-clés sont repris dans le tableau ci-dessous, inspiré du Tableau 2 de la norme précitée.

**Tableau 1: Exemple d'interprétation des mots-clés**

Type de déviation	Mot-clé	Exemple d'interprétation
Négative	Ne pas faire	Aucune partie de l'intention n'est remplie
Modification quantitative	Plus	Augmentation quantitative
	Moins	Diminution quantitative
Modification qualitative	En plus de	Présence d'impuretés – Exécution simultanée d'une autre Opération / étape
	Partie de	Une partie seulement de l'intention est réalisée
Substitution	Inverse	S'applique à l'inversion de l'écoulement dans les canalisations ou à l'inversion des réactions chimiques
	Autre que	Un résultat différent de l'intention originale est obtenu

Temps	Plus tôt	Un événement se produit avant l'heure prévue
	Plus tard	Un événement se produit après l'heure prévue
Ordre séquence	Avant	Un événement se produit trop tôt dans une séquence
	Après	Un événement se produit tard tôt dans une séquence

Cette méthode est particulièrement utile pour l'examen de systèmes thermo- hydrauliques, pour lesquels des paramètres (débit, température, pression, niveau, concentration, etc.) sont particulièrement importants pour la sécurité de l'installation.

De par sa nature, cette méthode requiert notamment l'examen de schémas et plans de circulation des fluides ou schémas PID.

### 2.1.2 Déroulement

La méthode proprement dite comprend pour un procédé continu les étapes suivantes :

- 1) Dans un premier temps, choisir une ligne ou de la maille. Elle englobe généralement un équipement et ses connexions, l'ensemble réalisant une fonction dans le procédé identifiée au cours de la description fonctionnelle.
- 2) Choisir un paramètre de fonctionnement.
- 3) Retenir un mot-clé et générer une dérive.
- 4) Vérifier que la dérive est crédible. Si oui, passer au point 5, sinon revenir au point 3.
- 5) Identifier les causes et les conséquences potentielles de cette dérive.
- 6) Examiner les moyens visant à détecter cette dérive ainsi que ceux prévus pour en prévenir l'occurrence ou en limiter les effets.
- 7) Proposer, le cas échéant, des recommandations et améliorations.
- 8) Retenir un nouveau mot-clé pour le même paramètre et reprendre l'analyse au point 3.
- 9) Lorsque tous les mots-clés ont été considérés, retenir un nouveau paramètre et reprendre l'analyse au point 2.
- 10) Lorsque toutes les phases de fonctionnement ont été envisagées, retenir une nouvelle ligne et reprendre l'analyse au point.

Répéter les actions 4 à 10 pour tous les mots-clés.

Répéter les actions 3 à 11 pour toutes les déviations.

Répéter les actions 1 à 12 pour toutes les sections.

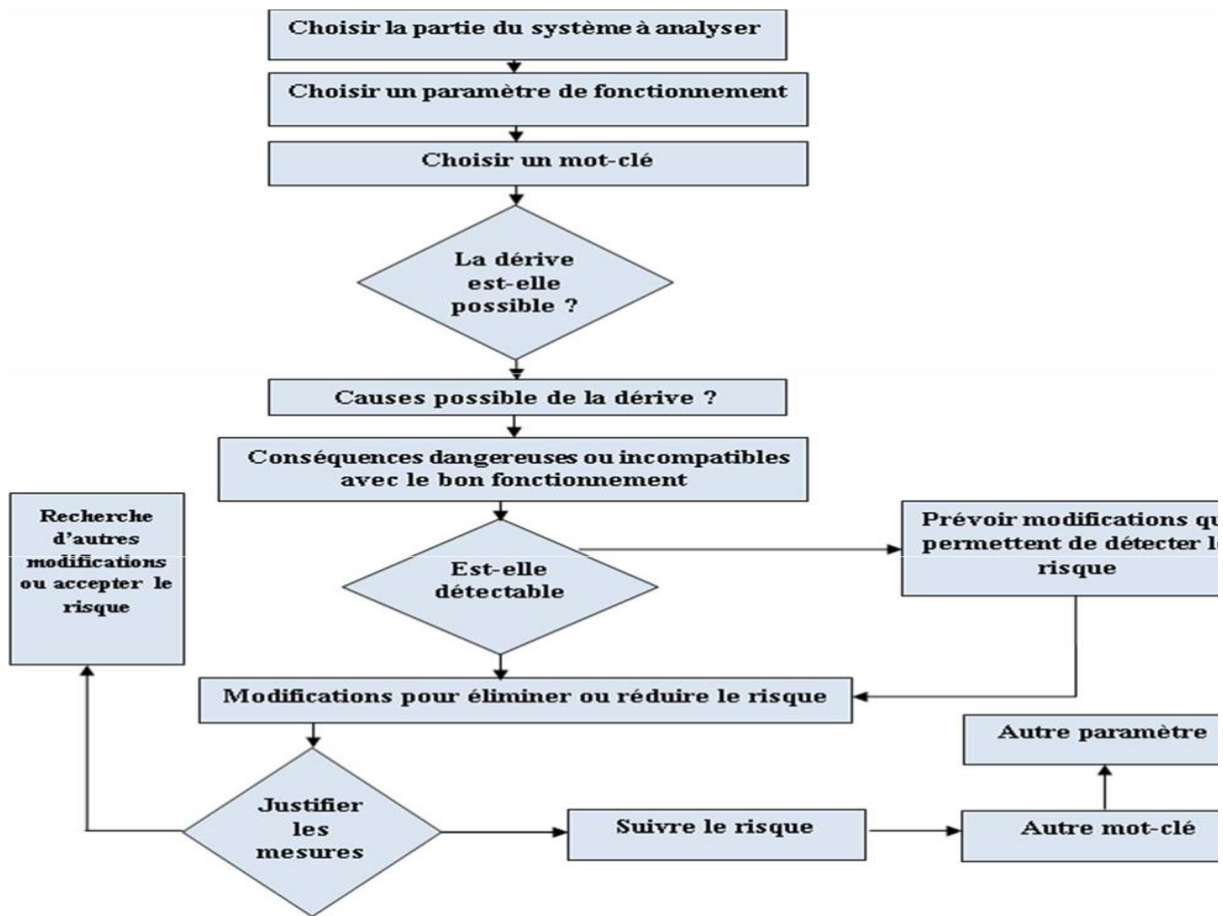


Figure 5: Déroulement de la méthode HAZOP

Tableau 2: Exemple de tableau HAZOP

Date:								
Ligne ou équipement :								
1	2	2	4	5	6	7	8	9
N°	Mot clé	Paramètre	Causes	Conséquences	Détection	Sécurités existantes	Propositions d'amélioration	Observations



### 2.1.3 Limites et l'avantages

#### Avantages

- Méthode simple à mettre en œuvre et efficace pour les systèmes thermo-hydrauliques ;
- Méthode qui favorise le caractère systématique de la recherche des déviations, elle est rigoureuse. Elle évite entre autres de considérer, tous les modes de défaillances possibles pour chacun des composants.
- Mise en commun des expériences. Réalisation de l'étude au sein d'un groupe de travail rassemblant différents métiers (sécurité, ingénierie, exploitation, maintenance, etc.).
- Détection précoce des erreurs de conception et mise en place d'actions correctives.

#### Limites

- Nécessité d'avoir une connaissance approfondie du système étudié et peut donc être plus difficilement réalisée sur un nouveau système.
- Méthode limitée aux fluides, ne fonctionne pas pour les systèmes mécaniques ou électroniques, ni pour les dérives liées aux facteurs humains.
- Groupe de travail compétent à constituer.
- Méthode d'analyse simple des dérives potentielles et trouvera ses limites dans la combinaison simultanée de plusieurs dérives.
- Méthode permet difficilement d'analyser les événements résultant de la combinaison simultanée de plusieurs défaillances.
- Difficile d'affecter un mot clé à une portion bien délimitée du système à étudier. Cela complique singulièrement l'identification des causes potentielles d'une dérive.

## 2.2 Analyse préliminaire des risques (APR)

### 2.2.1 Historique et définition :

L'Analyse Préliminaires des Risques (Dangers) a été développée au début des années 1960 dans les domaines aéronautiques et militaires. Elle est utilisée depuis dans de nombreuses autres industries.

L'Union des Industries Chimiques (UIC) recommande son utilisation en France depuis le début des années 1980.

L'analyse Préliminaire des Risques (APR) est une méthode d'évaluation systématique et préventive des risques potentiels associés à un processus, une installation, un système ou un

projet. Elle est généralement réalisée en début de projet, avant la mise en place effective du système, afin d'identifier les dangers et les risques associés à chaque étape du processus.

En conséquence, cette méthode ne nécessite généralement pas une connaissance approfondie et une description détaillée de l'installation étudiée. [28].

### 2.2.2 Les principes :

L'Analyse Préliminaire des Risques nécessite premièrement d'identifier les éléments dangereux de l'installation.

Ces éléments dangereux suivants font souvent référence à :

- Des matières ou préparations dangereuses, qu'elles soient sous forme de matières premières, de produits finis, d'outils, etc.
- Des matières dangereuses telles que le stockage, réception-expédition, réacteurs, infrastructures (foyers, etc.),
- Des opérations dangereuses liées au système.

-L'identification de ces éléments dangereux est fonction du type d'installation étudiée. L'APR peut être mise en œuvre sans ou avec l'aide de liste de risques types ou en appliquant les mots guides HAZOP.

- Il convient également de rappeler que l'identification de ces éléments est basée sur la description des travaux effectués avant la mise en place du système.

-A partir de ces facteurs de risque, l'APR cherche à identifier, pour les facteurs de risque, une ou plusieurs situations de danger. Aux fins du présent document, une situation dangereuse est définie comme une situation qui, si elle n'est pas maîtrisée, peut exposer les personnes concernées à une ou plusieurs situations dangereuses.

-Le groupe de travail déterminera également les causes et les effets des chaque situations dangereuses identifiées et déterminera les caractéristiques de sécurité du système étudié. Si ces dernières sont jugées insuffisantes vis-à-vis du niveau de risque identifié dans la grille de criticité, des propositions d'amélioration doivent alors être envisagées.

### 2.2.3 Déroulement :

L'utilisation d'un tableau de synthèse constitue un support pratique pour mener la réflexion et résumer les résultats de l'analyse. Pour autant, l'analyse des risques ne se limite pas à remplir

coûte que coûte un tableau. Par ailleurs, ce tableau doit parfois être adapté en fonction des objectifs fixés par le groupe de travail préalablement à l'analyse.

Le tableau 4 ci-dessous est donc donné à titre d'exemple.

**Tableau 3: Exemple de tableau de type « APR »**

Fonction ou système.						Date:	
1	2	3	4	5	6	7	8
N°	Produit ou équipement	Situation de danger	Causes	Conséquences	Sécurités existantes	Propositions d'amélioration	Observations

### 2.2.4 Limites et l'avantage

Le principal avantage de l'analyse préliminaire des risques est de permettre une évaluation rapide des situations dangereuses dans l'installation. Par rapport aux autres méthodes présentées ci-après, elle apparaît comme relativement économique en termes de temps passé et ne nécessite pas un niveau de description du système étudié très détaillé.

Cet avantage est bien entendu lié au fait qu'il est souvent mis en œuvre au la phase de conception de l'installation.

En revanche, l'APR ne permet pas de préciser l'enchaînement des événements pouvant conduire à un accident majeur pour les systèmes complexes.

Comme son nom l'indique, il s'agit à la base d'une méthode préliminaire d'analyse qui permet d'identifier des points critiques devant faire l'objet d'études plus détaillées. Ainsi, il permet de spécifier les équipements ou les installations qui peuvent nécessiter une analyse détaillée à l'aide d'outils tels que AMDEC, HAZOP ou l'analyse par arbre des défaillances. Toutefois, son utilisation seule peut être jugée suffisante dans le cas d'installations simples ou lorsque le groupe de travail possède une expérience significative de ce type d'approches.

### 2.3 Arbre de défaillance

L'arbre de défaillance (ADD) est une méthode déductive, qui fournit une démarche systématique pour identifier les causes d'un événement unique intitulé « événement redouté : ER ».

Il consiste en une représentation graphique des combinaisons possibles d'événements qui permettent la réalisation d'un événement indésirable prédéfini en mettant en évidence les relations de causes à effets. Il est complété par un traitement mathématique qui permet la combinaison de défaillances simples ainsi que de leur probabilité d'apparition et de quantifier la probabilité d'occurrence d'un événement indésirable. Il est nécessaire que les événements soient indépendants entre eux.

Leurs probabilité d'occurrence doit pouvoir être quantifiée (condition nécessaire seulement dans le cas où l'arbre est destiné à une analyse quantitative).

### 2.3.1 Historique et domaine d'application

L'analyse par arbre des défaillances fut historiquement la première méthode mise au point en vue de procéder à un examen systématique des risques. Elle a été élaborée au début des années 1960 par la compagnie américaine Bell Téléphone et fut expérimentée pour l'évaluation de la sécurité des systèmes de tir de missiles. Visant à déterminer l'enchaînement et les combinaisons d'événements pouvant conduire à un événement redouté pris comme référence, l'analyse par arbre des défaillances est maintenant appliquée dans de nombreux domaines tels que l'aéronautique, le nucléaire, l'industrie chimique.

Elle est aussi utilisée pour analyser a posteriori les causes d'accidents qui se sont produits. Dans ces cas, l'événement redouté final est généralement connu car observé. On parle alors d'analyse par arbre des causes, l'objectif principal étant de déterminer les causes réelles qui ont conduit à l'accident.

### 2.3.2 Principe

L'analyse par arbre de défaillances est une méthode déductive.

Elle appelée aussi :

- Arbre de dysfonctionnements
- Arbre des défauts
- "Fault Tree Analysis"

En effet, il s'agit, à partir d'un événement redouté défini a priori, de déterminer les séquences d'événements ou combinaisons d'événements peuvent finalement conduire à cet événement. Cette analyse permet de remonter de causes en causes jusqu'aux événements fondamentaux susceptibles d'être à l'origine de l'événement redouté.

Les événements fondamentaux correspondent en général à des :

- **Les événements élémentaires qui sont suffisamment connus et décrits pour qu'il ne soit pas nécessaire d'en rechercher les causes.** Ainsi, leur probabilité d'occurrence est également connue.
- **Évènements qui ne peuvent considérés comme élémentaires** mais dont les causes ne seront pas développées faute d'intérêt,
- **Évènements dont les causes seront développées ultérieurement** au gré d'une nouvelle analyse par exemple,
- **Évènements survenant normalement et de manière** récurrente dans le fonctionnement du procédé ou de l'installation.

Quelle que soit la nature des composants de base identifiés, l'analyse par arbre des défaillances est fondée sur les principes suivants :

- Ces évènements sont indépendants.
- Ils ne seront pas décomposés en éléments plus simples faute d'informations, d'intérêt ou parce que c'est impossible.
- Leur fréquence ou leur probabilité d'occurrence peut être évaluée.

Ainsi, l'analyse par arbre des défaillances permet de déterminer les successions et les combinaisons d'évènements qui conduisent des évènements de base jusqu'à l'évènement indésirable retenu

Les liens entre les différents événements identifiés sont réalisés grâce à des portes logiques (de type ET» et «OU par exemple). Cette méthode utilise un symbolisme graphique particulier qui rend possible la présentation des résultats dans une arborescence. Le lecteur peut, par exemple se reporter aux conventions de présentation proposées dans la norme CEI 61025:1990 Analyse par Arbre de Panne (APP)».

Avec l'aide de règles mathématiques et statistiques, il est alors théoriquement possible d'évaluer la probabilité d'occurrence de l'évènement final à partir des probabilités des événements de base identifiés,

L'analyse par arbre des défaillances d'un événement redouté peut être décomposée en trois étapes successives:

- définition de l'évènement redouté étudié.
- élaboration de l'arbre.

- exploitation de l'arbre.

Il convient d'ajouter à ces étapes, une étape préliminaire de connaissance du système. Nous verrons que cette dernière est primordiale pour mener l'analyse et qu'elle nécessite le plus souvent une connaissance préalable des risques.

### **2.3.3 Définition et l'événement redouté**

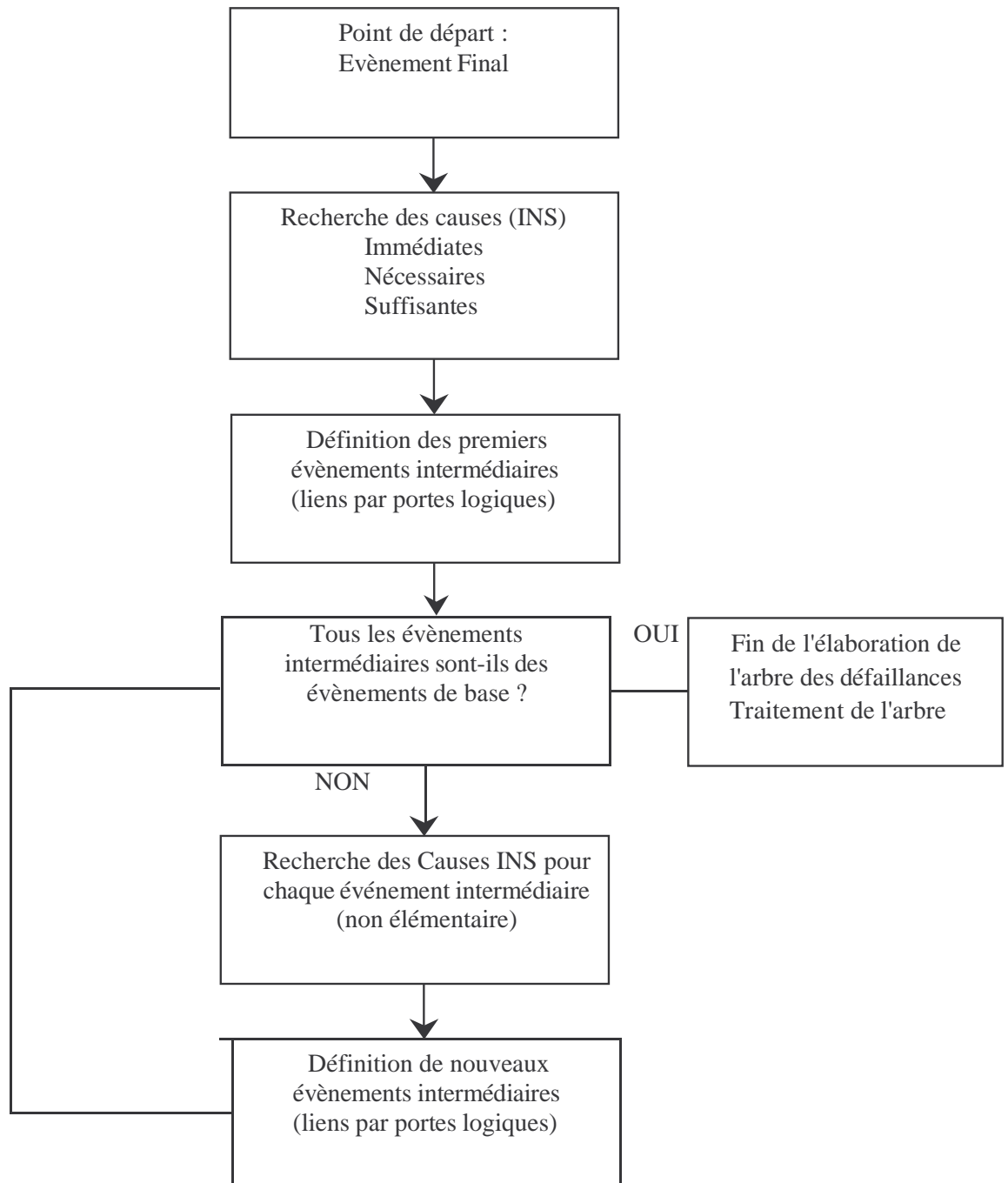
La définition du dernier événement, qui sera analysé, est une étape cruciale pour la construction de l'arbre. On conçoit que plus cet événement est défini de manière précise, plus simple sera l'élaboration de l'arbre des défaillances. De plus, puisqu'il s'agit d'une méthode qui peut se révéler rapidement lourde à appliquer, elle doit être réservée aux événements jugés particulièrement critiques.

De manière classique, les événements considérés peuvent concerner :

- l'émission de substances toxiques ou inflammables dans l'atmosphère.
- le risque d'incendie.
- le risque d'explosion.

### **2.3.4 Élaboration de l'arbre**

La construction de l'arbre des défaillances vise à déterminer les enchaînements d'événements pouvant conduire à l'événement final retenu. Cette analyse se termine lorsque toutes les causes possibles correspondent aux événements élémentaires. L'élaboration de l'arbre des défaillances suit le déroulement suivant :



**Figure 6: Démarche pour l'élaboration d'un arbre des défaillances [26].**

Cette démarche est facilitée par l'application préalable d'une méthode de type APR, HAZOP ou AMDEC.

- la recherche systématique des causes immédiates, nécessaires et suffisantes constitue donc la base de la construction de l'arbre.

- Il s'agit probablement de l'étape la plus délicate et il est souvent utile de procéder à cette construction au sein d'un groupe de travail pluridisciplinaire. De plus, la mise en œuvre préalable d'autres méthodes d'analyse des risques de type inductif facilite grandement la recherche des défaillances pour l'élaboration de l'arbre. Afin de sélectionner les événements intermédiaires, il est indispensable de procéder pas à pas en prenant garde à bien identifier les causes directes et immédiates de l'évènement considéré et se poser la question de savoir si ces causes sont bien nécessaires et suffisantes. Faute de quoi, l'arbre obtenu pourra être partiellement incomplet voire erroné.

Enfin, il est nécessaire de respecter certaines règles supplémentaires à observer durant la construction de l'arbre à savoir :

- vérifier que le système est cohérent, ça veut dire :
  - la défaillance de tous ses composants entraîne la défaillance du système.
  - le bon fonctionnement de tous ses composants entraîne le bon fonctionnement du système.
- s'assurer que tous les événements d'entrée d'une porte logique ont bien été identifiés avant d'analyser leurs causes respectives.
- éviter de connecter directement deux portes logiques.
- ne sélectionner que les causes antérieures à l'existence de l'évènement considéré.

En définitive, l'application de ces règles aux réflexions menées au sein d'un groupe de travail conduit à la construction d'un arbre de la forme suivante :

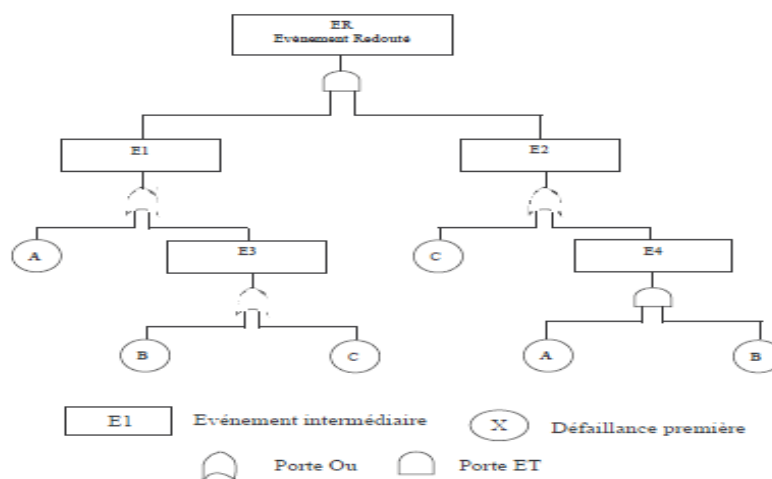


Figure 7: exemple d'arbre des défaillances [26].







### 2.3.5 Représentation graphique

La représentation graphique de l'arbre de défaillance se fait à travers une symbolisation graphique classée en deux types :

- Evènements.
- Portes logiques.

1° Evènements La symbolisation des évènements a pour but de faciliter la désignation entre les différents types d'évènements.




**Tableau 4: Symboles des évènements dans les arbres de défaillances**

Symbole	Nom	Description
	Evènement Intermédiaire ou final	<i>Evènement du plus haut niveau: sommet d'arbre « évènement redouté », ou évènement intermédiaire résultant d'un évènement redouté.</i>
	Evènement de base	<i>Evènement du plus bas niveau pour lequel la probabilité d'apparition ou d'information est disponible.</i>
	Evènement non développé	<i>Le développement de cet évènement n'est pas terminé, soit parce que ses conséquences sont négligeables, soit par manque d'information.</i>
	Evènement maison	<i>Evènement qui doit se produire avec certitude lors de la production ou de la maintenance. On peut aussi le définir comme un évènement non- probabilisé ou (P=1).</i>

2° Portes logiques Les portes logiques (ou connecteurs logiques) sont les liaisons entre les différents branches et/ou évènements. Les plus classiques sont ET et OU (Tableau 6). Les portes fonctionnent comme suit :

- OU : l'évènement en sortie/supérieur survient si, au moins, un des évènements en entrée/inférieur survient/est présent.
- ET : l'évènement en sortie/supérieur survient seulement si tous les évènements en entrée/inférieur surviennent/sont présents.

**Tableau 5: Symboles des portes dans les arbres de défaillances**

Symbole	Nom	Description	Nombre d'entrées
	<b>OU (OR)</b>	<i>L'évènement de sortie apparait si au moins un des évènements d'entrées apparait</i>	>1
	<b>ET (AND)</b>	<i>L'évènement de sortie apparait si tous les évènements apparaissent</i>	>1
	<b>SI (IF)</b>	<i>Sortie générée si l'évènement entrée est présent et si la condition X est réalisée</i>	=1

### 2.3.6 Avantages et Limites :

L'analyse par arbre de défaillances est le plus souvent utilisée dans les études de fiabilité, de disponibilité ou de sécurité des systèmes. Il présente un certain nombre d'avantages significatifs par rapport aux autres méthodes, à savoir :

- ✓ Une caractéristique particulièrement importante, l'aspect graphique, est un moyen efficace de montrer la logique des combinaisons d'erreurs. Il contribue grandement à la mise en œuvre aisée de la méthode et à la compréhension du modèle. C'est donc un excellent support de dialogue pour les équipes pluridisciplinaires.
- ✓ Un processus déductif de création d'arbres permet aux analystes de se concentrer uniquement sur les événements qui contribuent à l'apparition d'événements redoutés.
- ✓ Une fois la construction de l'arbre terminée, deux modes de fonctionnement sont possibles :
  - ❖ Évaluation qualitative pour identifier les combinaisons d'événements critiques dans le but d'identifier les faiblesses du système;
  - ❖ L'exploitation quantitative permettant de hiérarchiser ces combinaisons d'événements suivant leur probabilité d'apparition, et estimer la probabilité de l'événement sommet, l'objectif in fine étant de disposer de critères pour déterminer les priorités pour la prévention de l'événement redouté.
- ✓ L'approche analytique offerte par les arbres de défaillances présente des avantages par rapport aux méthodes de simulation dans la mesure où elle permet d'effectuer des calculs rapides (un avantage très relatif compte tenu du développement constant de l'informatique) et des calculs précis.
- ✓ Cette méthode permet d'estimer non seulement la probabilité de l'événement redouté à partir de l'événement de base, mais aussi la probabilité des portes intermédiaires. Il est également possible de faire de la propagation d'incertitudes sur les données d'entrée, et du calcul de facteurs d'importance.
- ✓ La taille de l'arbre de défaillances est proportionnée à la taille du système étudié, et pas exponentielle en fonction de cette taille.

L'utilisation de l'arbre de défaillances devient inefficace ou Impraticable lorsque les caractéristiques suivantes se présentent:

### 1. Dépendance entre les événements

Les calculs de probabilité d'occurrence effectués par l'arbre de défaillances sont basés sur l'hypothèse que les événements fondamentaux sont indépendants les uns des autres. Par exemple, la probabilité qu'un événement de base se produise ne peut pas dépendre de l'occurrence d'autres événements de base.

### 2. Notion d'événements temporisés

L'arbre de défaillances ne rend pas compte de l'aspect temporel des événements. Il ne peut donc considérer ni les dépendances fonctionnelles, ni les états passés. De plus, il ne permet pas de prendre en compte un ordre imposé dans lequel des événements doivent se produire pour induire une défaillance.

### 3. Système dégradé

L'arbre de défaillances est binaire. Un événement peut ou non se produire, mais aucun concept de capacité ou d'efficacité ne peut intervenir. Par exemple, les vannes sont considérées comme ouvertes ou fermées, mais les états intermédiaires ne peuvent pas être déterminés.

### 4. Taille de l'arbre

La taille n'est pas une limite en soi. Cependant, une croissance exponentielle nécessite de diviser l'arbre en sous-arbres, ce qui rend le modèle plus difficile à lire et à comprendre.

## 2.4 LOPA

### 2.4.1 Définition

L'analyse des couches de protection est une méthode semi-quantitative orientée barrières, qui est destinée à la maîtrise des risques d'accidents majeurs. [28].

Généralement, le principe de cette méthode consiste en premier lieu à identifier les différents scénarios d'accidents d'une installation.

Elle est souvent utilisée dans les industries à haut risque, telles que les industries chimiques, pétrolières, gazières, pharmaceutiques et nucléaires.

La méthode LOPA repose sur l'idée que les barrières de protection, qu'elles soient physiques, opérationnelles ou de gestion, peuvent être organisées en plusieurs couches ou niveaux, et que chaque couche a une probabilité de défaillance et une efficacité associées. En évaluant ces probabilités de défaillance et ces efficacités, la méthode LOPA permet de quantifier le niveau de protection global d'un processus industriel.

### 2.4.2 Domaine d'application

La méthode LOPA trouve plusieurs applications :

- Compléter l'analyse menée dans l'HAZOP si le groupe de travail considère le scénario trop complexe ou que les conséquences sont trop importantes.
- Déterminer les niveaux de SIL requis pour les fonctions instrumentées de sécurité (SIF).
- Elle permet de déterminer le nombre de barrières de sécurité indépendantes (IPL) à mettre en œuvre dans le but de pouvoir justifier d'un niveau de risque acceptable.
- La finalité de la méthode est d'estimer le niveau de risque résiduel en considérant l'effet des IPL. Pour ce faire, il est nécessaire
- Calculer la fréquence d'occurrence du scénario d'accident (par an), ce qui nécessite d'évaluer la fréquence d'occurrence des événements initiateurs et les probabilités de défaillances de chaque IPL.
- Evaluer la gravité associée à la conséquence en cas de survenue de l'accident.

### 2.4.3 Les différentes couches de protection :



**Figure 8: Les couches de protection de LOPA**

La méthode LOPA introduit le concept de « couches de protection » présenté en figure 8 et ceci dans une optique de réduction des risques car les industriels sont amenés à mettre en place différentes barrières prévues, soit pour prévenir l'apparition d'un accident (barrière de prévention), soit pour en limiter les conséquences (barrière de mitigation et de protection). Ces

moyens sont nombreux et diversifiés et ils sont mis en œuvre pour intervenir de manière graduelle dans le temps.

En d'autres termes, ces différentes couches vont être « sollicitées » tour à tour avec pour objectif de « stopper » le déroulement du scénario d'accident ou d'en réduire les effets.

Ces huit couches peuvent être réparties en trois catégories :

Les couches dites de prévention prévues pour « stopper » le déroulement de la séquence accidentelle avant l'apparition d'un événement redouté.

Les couches dites de mitigation prévues pour limiter les conséquences dans le cas où la survenue de l'événement redouté ne pourrait être évitée.

Les couches dites de protection prévues pour « limiter » l'exposition des « cibles » vis-à-vis des phénomènes dangereux liés à la réalisation de l'événement redouté.

La répartition des différentes couches dans l'une des catégories précédentes est présentée dans le tableau qui suit :

**Tableau 6: Différentes couches dans les différentes catégories selon LOPA**

Catégorie	Couches de protection
<b>Couches de prévention</b>	Conception du procédé Conduite du procédé  Alarmes et interventions humaines
<b>Couches de mitigation/protection</b>	Systèmes instrumentés de sécurité  Sécurités physiques (organes de décharge, etc.) Protections post-décharge (cuvette de rétention, etc.) Plans d'urgence site  Plans d'intervention

#### 2.4.4 Processus de déroulement méthode LOPA

Le processus de déroulement d'une méthode LOPA (Layer of Protection Analysis) est une approche utilisée dans l'industrie pour évaluer les risques associés à un système ou à un

processus et pour déterminer les couches de protection nécessaires pour prévenir ou atténuer les conséquences des accidents potentiels.

Voici les étapes générales du processus de déroulement d'une méthode LOPA :

- **Définir l'objectif de l'analyse** : Il est important de clarifier l'objectif de l'analyse LOPA dès le début du processus. Cela peut inclure la définition des scénarios d'accidents à analyser, les limites du système ou du processus à étudier, les conséquences potentielles des accidents, et les critères de tolérable des risques.
- **Identifier les scénarios d'accidents** : Les scénarios d'accidents sont les événements indésirables qui peuvent se produire dans le système ou le processus étudié. Ils peuvent être identifiés à partir d'une analyse des modes de défaillance, d'une étude de sécurité existante, ou d'autres méthodes d'identification des risques.
- **Estimer les fréquences d'occurrence des scénarios d'accidents** : Pour chaque scénario d'accident identifié, il est nécessaire d'estimer la fréquence d'occurrence, c'est-à-dire la probabilité que l'événement se produise sur une période donnée. Cela peut être basé sur des données historiques, des informations opérationnelles, ou des jugements d'experts.
- **Estimer les conséquences des scénarios d'accidents** : Pour chaque scénario d'accident, il faut évaluer les conséquences potentielles, y compris les conséquences sur la sécurité des personnes, l'environnement, la production, la réputation de l'entreprise, etc. Cela peut nécessiter la modélisation des scénarios d'accidents pour déterminer les conséquences probables.
- **Identifier les couches de protection existantes** : Les couches de protection sont les barrières ou les mesures de sécurité déjà en place pour prévenir ou atténuer les conséquences des scénarios d'accidents. Il est important d'identifier toutes les couches de protection existantes, y compris les dispositifs de sécurité, les procédures opérationnelles, les formations, les équipements de sécurité, etc.
- **Évaluer l'efficacité des couches de protection existantes** : Pour chaque couche de protection identifiée, il faut évaluer son efficacité pour prévenir ou atténuer les conséquences des scénarios d'accidents. Cela peut être basé sur des données de performance, des essais, des études de fiabilité, ou des jugements d'experts.
- **Déterminer les couches de protection nécessaires** : En comparant l'estimation des fréquences d'occurrence des scénarios d'accidents et l'efficacité des couches de protection existantes, il est possible de déterminer si des couches de protection

supplémentaires sont nécessaires pour atteindre les critères d'opérabilité des risques. Cela peut inclure l'identification de nouvelles couches de protection à mettre en place, ou l'amélioration des couches de protection existantes.

#### 2.4.5 Les avantages de méthode LOPA

La méthode LOPA (Layer of Protection Analysis) présente plusieurs avantages dans l'évaluation des risques et la détermination des mesures de protection nécessaires pour les prévenir ou les atténuer.

Voici quelques avantages clés de la méthode LOPA :

**Approche systématique :** La méthode LOPA est une approche structurée et systématique pour évaluer les risques en identifiant les scénarios d'accidents, en estimant leurs fréquences d'occurrence et leurs conséquences, et en évaluant l'efficacité des couches de protection existantes. Cela permet une analyse complète et approfondie des risques associés à un système ou à un processus.

**Prise en compte des couches de protection :** La méthode LOPA met l'accent sur l'évaluation des couches de protection existantes, c'est-à-dire les barrières ou les mesures de sécurité déjà en place pour prévenir ou atténuer les conséquences des accidents potentiels. Cela permet de reconnaître et de valoriser les mesures de sécurité déjà en place, et d'identifier les lacunes éventuelles dans les couches de protection existantes.

**Flexibilité :** La méthode LOPA est une approche flexible qui peut être adaptée aux besoins spécifiques d'un système ou d'un processus particulier. Elle permet de sélectionner les scénarios d'accidents à analyser en fonction de leur importance et de se concentrer sur les couches de protection les plus critiques. Elle peut également être utilisée conjointement avec d'autres méthodes d'évaluation des risques pour obtenir une analyse plus complète.

**Prise en compte des données existantes :** La méthode LOPA permet d'utiliser les données existantes, telles que les données historiques, les informations opérationnelles, les études de fiabilité, etc., pour estimer les fréquences d'occurrence des scénarios d'accidents et évaluer l'efficacité des couches de protection existantes. Cela peut permettre une analyse plus basée sur les faits et moins dépendante des jugements d'experts.

**Aide à la prise de décision :** La méthode LOPA fournit des informations claires sur les risques associés à un système ou à un processus, ainsi que sur l'efficacité des couches de protection existantes. Cela peut aider les décideurs à prendre des décisions éclairées sur les mesures de

protection nécessaires pour prévenir ou atténuer les risques identifiés, et à allouer les ressources de manière appropriée.

Amélioration continue : La méthode LOPA encourage l'amélioration continue en identifiant les lacunes dans les couches de protection existantes et en recommandant des mesures de protection supplémentaires si nécessaire. Cela permet de maintenir un niveau de sécurité approprié et de s'adapter aux changements dans l'environnement opérationnel ou dans les exigences réglementaires.

En résumé, la méthode LOPA offre une approche structurée, flexible et basée sur les données pour évaluer les risques et déterminer les mesures de protection nécessaires, ce qui peut aider à améliorer la sécurité des systèmes et des processus industriels.

#### 2.4.6 Les inconvénients de méthode LOPA

Bien que la méthode LOPA présente de nombreux avantages, elle comporte également quelques inconvénients potentiels. Voici quelques points à prendre en compte :

- **Subjectivité** : La méthode LOPA repose souvent sur l'expertise et les jugements d'experts pour estimer les fréquences d'occurrence des scénarios d'accidents, évaluer l'efficacité des couches de protection existantes et déterminer les valeurs des paramètres clés utilisés dans l'analyse. Cela peut introduire une certaine subjectivité dans les résultats, ce qui peut être source d'incertitude et de variabilité.
- **Simplifications** : La méthode LOPA simplifie souvent la complexité des systèmes et des processus en utilisant des modèles ou des approximations pour estimer les fréquences d'occurrence des scénarios d'accidents et les conséquences associées. Cela peut entraîner des approximations et des simplifications excessives, ce qui peut affecter la précision des résultats obtenus.
- **Dépendance des données existantes** : Bien que la méthode LOPA utilise les données existantes pour estimer les fréquences d'occurrence des scénarios d'accidents, cela peut être un inconvénient si les données sont limitées, non fiables ou inappropriées pour le système ou le processus en question. Cela peut entraîner des estimations de risques inexacts et des décisions erronées.
- **Limitations dans la détermination des couches de protection** : La méthode LOPA peut être limitée dans la détermination des couches de protection nécessaires. Elle peut sous-estimer ou surestimer l'efficacité des mesures de protection existantes, en fonction des



informations disponibles et des hypothèses utilisées. Cela peut entraîner une mauvaise évaluation des risques et des mesures de protection inadéquates.

- Limitations dans l'évaluation des interactions entre les couches de protection : La méthode LOPA ne tient généralement pas compte des interactions potentielles entre les différentes couches de protection, ce qui peut entraîner une évaluation inexacte de l'efficacité globale des mesures de protection. Les interactions entre les couches de protection peuvent être complexes et difficiles à évaluer, ce qui peut limiter la précision de l'analyse.
- Temps et ressources nécessaires : L'application de la méthode LOPA peut nécessiter du temps et des ressources pour collecter et analyser les données nécessaires, estimer les fréquences d'occurrence, évaluer l'efficacité des couches de protection et prendre des décisions appropriées. Cela peut être un inconvénient en termes de coûts et de temps, surtout pour les systèmes ou les processus complexes.
- Il est important de noter que malgré ces inconvénients potentiels, la méthode LOPA reste une approche largement utilisée et reconnue pour évaluer les risques et déterminer les mesures de protection nécessaires dans de nombreux domaines industriels. Il est essentiel d'utiliser la méthode LOPA avec prudence, en prenant en compte ses limites et en utilisant d'autres sources d'information et d'évaluation pour obtenir une analyse complète et fiable des risques.

## Conclusion

Ce chapitre a présenté différentes méthodes d'analyse des risques industrielles, ainsi que leurs typologies. Nous avons abordé les notions générales telles que le danger, le risque, la sécurité et le système. De plus, nous avons examiné en détail le processus de gestion des risques, comprenant l'identification, l'analyse, l'évaluation et le traitement des risques.

Une partie importante de ce chapitre a été consacrée à la classification des outils d'analyse des risques. Nous avons distingué entre les méthodes quantitatives et qualitatives, en mettant en évidence leurs différences et leurs avantages respectifs.

En ce qui concerne les méthodes d'analyse spécifiques, nous avons étudié la méthode HAZOP, l'analyse préliminaire des risques (APR), l'arbre de défaillance et la méthode LOPA. Chacune de ces méthodes a été examinée dans ses détails, y compris son historique, son domaine d'application, ses principes, son déroulement et ses avantages et limites.

Il est important de noter que chaque méthode d'analyse des risques a ses propres caractéristiques et peut être utilisée dans des contextes spécifiques. Certaines méthodes mettent davantage l'accent sur l'identification des défaillances potentielles, tandis que d'autres se concentrent sur l'évaluation quantitative des risques.

## **CHAPITRE 2 :**

# Méthode d'analyse de niveau de SIL et définition des SIL

## Introduction :

Le niveau SIL d'une installation est une mesure de la fiabilité et de la sécurité du système de contrôle de sécurité. Il est déterminé en fonction des risques associés à l'installation et des mesures de sécurité mises en place pour les atténuer.

Voici quelques méthodes pour la détermination du niveau SIL d'une installation :

**Analyse des risques :** Cette méthode consiste à identifier et à évaluer les risques associés à l'installation, puis à déterminer les mesures de sécurité nécessaires pour les atténuer. Les résultats de l'analyse des risques sont utilisés pour déterminer le niveau SIL approprié.

**Normes et directives :** Il existe des normes et des directives internationales qui définissent les exigences de sécurité pour les systèmes de contrôle de sécurité. Par exemple, l'IEC 61508 est une norme internationale pour les systèmes de contrôle de sécurité et définit quatre niveaux SIL.

Les niveaux SIL appropriés peuvent être déterminés en fonction des exigences de la norme.

**Approche hybride :** Cette méthode combine les deux méthodes précédentes en utilisant à la fois une analyse des risques et les exigences des normes et directives pour déterminer le niveau SIL approprié.

**Consultation d'experts :** Il est également possible de consulter des experts en sécurité fonctionnelle pour déterminer le niveau SIL approprié en fonction des risques associés à l'installation et des mesures de sécurité mises en place.

Il est important de noter que la détermination du niveau SIL d'une installation est une tâche complexe qui nécessite une compréhension approfondie des risques et des mesures de sécurité associées. Il est donc recommandé de faire appel à des professionnels qualifiés en sécurité fonctionnelle pour mener à bien cette tâche.

### 1. La norme CEI 61508

La norme internationale CEI 61508 définit les exigences de sécurité fonctionnelle pour les systèmes électriques, électroniques et électroniques programmables utilisés dans divers secteurs industriels, de transport, énergétiques et de défense. Elle fournit un cadre pour la conception, la validation, la certification et la validation des systèmes E/E/EP afin d'assurer leur sécurité fonctionnelle. Cette norme définit les exigences de sécurité à chaque étape du cycle de vie du système, allant de la spécification au débogage, en passant par le développement, la

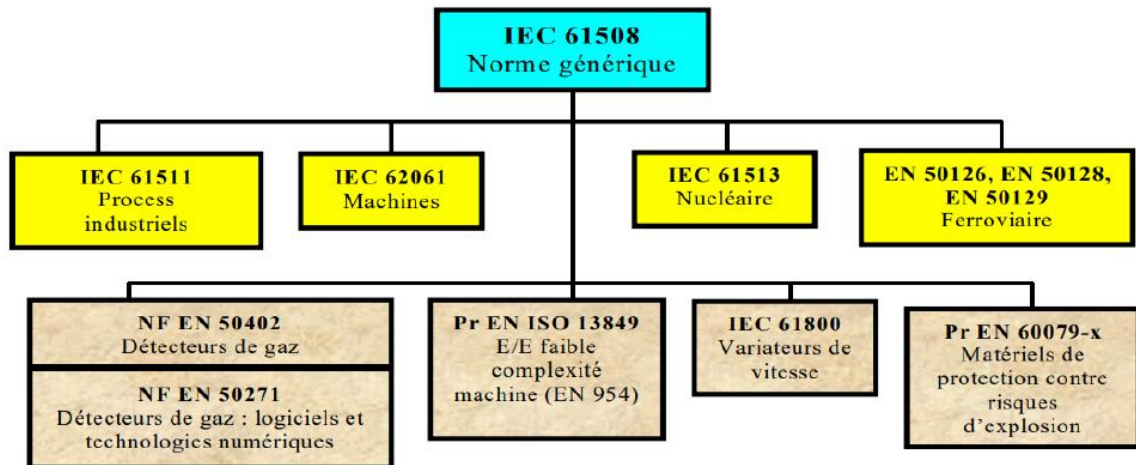
validation et la certification. De plus, elle établit les niveaux d'intégrité de la sécurité (SIL) à atteindre en fonction des risques associés à l'utilisation des systèmes E/E/EP, allant du SIL 1 (niveau le plus bas) au SIL 4 (niveau le plus élevé). La conformité à la norme CEI 61508 est souvent exigée dans des domaines critiques pour la sécurité tels que l'industrie chimique, le pétrole et le gaz, le transport ferroviaire et aérien, ainsi que la défense.

L'IEC 61508 s'articule autour de sept chapitres :

1. prescriptions générales.
2. Prescriptions pour les systèmes électriques/électroniques/Électroniques programmables relatifs à la sécurité.
3. prescriptions concernant les logiciels.
4. définitions et abréviations.
5. exemples de méthodes de détermination des niveaux d'intégrité de sécurité.
6. lignes directrices pour l'application de la IEC 61508-2 et de la IEC 61508-3.
7. présentation des techniques et des mesures.

Les points importants de la norme IEC 61508 [IEC61508 02] :

- Elle concerne toutes les phases du cycle de vie des matériels et du logiciel (depuis la conceptualisation, en passant par la conception, l'installation, l'exploitation, la maintenance, jusqu'à la mise hors service).
- Elle repose sur deux concepts qui sont fondamentaux vis-à-vis de son application : le cycle de vie en sécurité et les niveaux d'intégrité de sécurité.
- Elle présente une approche générique de toutes les activités liées au cycle de vie de sécurité de systèmes électriques/électroniques/électroniques programmables (E/E/PES) qui sont utilisés pour réaliser des fonctions de sécurité.
- Fournir les moyens aux utilisateurs et aux autorités de réglementation d'acquiescer la confiance dans les technologies basées sur l'électronique programmable.
- Il est indispensable de fournir à tous les responsables suffisamment d'éléments liés à la sécurité pour les guider dans leurs prises de décisions.



**Figure 9: CEI 61508 et ses déclinaisons par secteur d'application**

## 2. Norme CEI 61511

La norme internationale CEI 61511 définit les exigences de sécurité fonctionnelle des systèmes de sécurité des instruments (SIS) utilisés dans les processus industriels. Elle guide la conception, l'installation, la maintenance et la validation des SIS pour assurer leur sécurité fonctionnelle. Cette norme établit également un niveau de sécurité intégré (SIL) similaire à celui défini dans la norme CEI 61508, permettant d'évaluer les performances de sécurité du SIS. Elle est applicable à divers secteurs industriels tels que l'industrie chimique, pétrolière, gazière, pharmaceutique et alimentaire, où la sécurité est cruciale pour la protection des travailleurs, de l'environnement et des actifs.

Cette norme comprend trois parties :

- 1- Cadre, définitions, exigences pour le système, le matériel et le logiciel.
- 2- Lignes directrices pour l'application de la CEI 61511-1.
- 3- Conseils pour la détermination des niveaux exigés d'intégrité de sécurité.

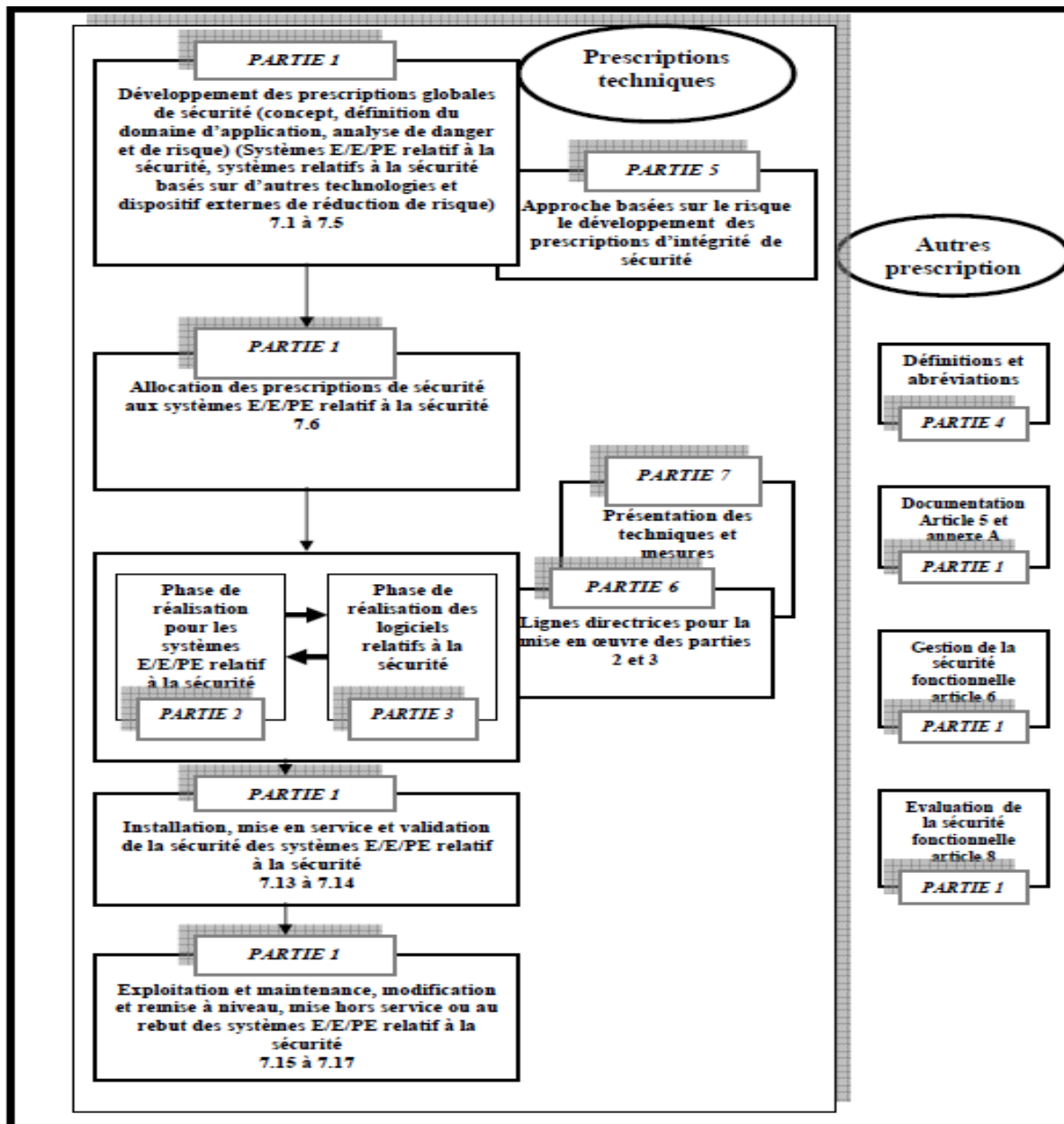


Figure 10: Structure générale de la norme IEC 61508 [IEC61508, 2002]

### 3. Sécurité fonctionnelle

La norme IEC 61508-4 définit la sécurité fonctionnelle comme un sous-ensemble de la sécurité globale qui se rapporte au système commandé Equipement Under Control (EUC) et qui dépend du fonctionnement correct du système E/E/EP relatif à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque.

La norme IEC 61511-1 définit la sécurité fonctionnelle comme un sous-ensemble de la sécurité globale qui se rapporte au processus et au système de commande de processus et au BPCS, qui

dépend du fonctionnement correct du système instrumenté de sécurité (SIS) et d'autres couches de protection.

### 3.1.1 Systèmes relatifs aux applications de sécurité

Un système E/E/PE (électrique/électronique/électronique programmable de sécurité) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité. C'est-à-dire, depuis le capteur, en passant par la logique de contrôle et les systèmes de communication, jusqu'à l'actionneur final, tout en incluant les actions critiques de l'opérateur.

Les systèmes de sécurité sont définis en termes d'absence de risque inacceptable de blessure ou de préjudice à la santé des personnes. Les dommages aux personnes peuvent être directs ou indirects, comme des dommages aux biens ou à l'environnement par exemple. Certains systèmes peuvent être principalement conçus pour se prémunir contre des pannes ayant des implications économiques majeures. Ceci signifie que dans l'esprit, à objectifs techniques comparables ou identiques, il n'y a pas de différence entre un système de sécurité et un système de contrôle commande. L'IEC 61508 [IEC61508, 1998] et l'IEC 61511 [IEC61511, 2000] peuvent donc être utilisées pour développer n'importe quel système E/E/PE comportant des fonctions critiques, telles que la protection des équipements, des biens ou de la productivité.

## 4. Les systèmes instrumentés de sécurité

### 4.1 Définition

La norme CEI 61511 (CEI\_61511 2003) définit les systèmes instrumentés de sécurité de la façon suivante : système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux).

La norme CEI 61508(CEI\_61508 2010) définit quant à elle les systèmes relatifs aux applications de sécurité par : un système E/E/PE (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.

Un système instrumenté de sécurité (SIS) est un système visant à mettre un procédé en position de replis de sécurité (c'est-à-dire un état stable ne présentant pas de risque pour l'environnement et les personnes), lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu).

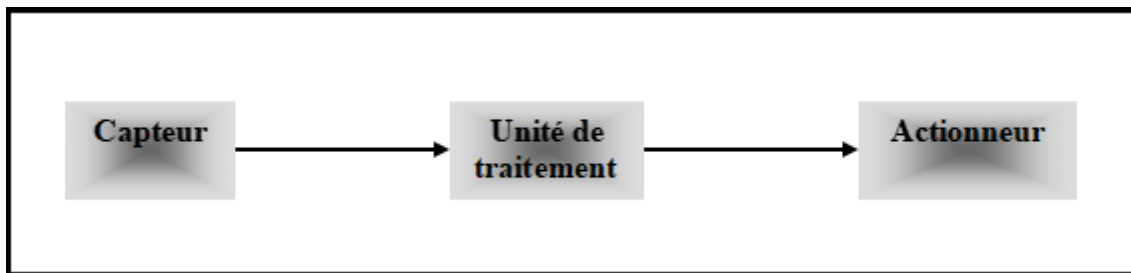
Les SIS sont utilisés pour exécuter des fonctions de sécurité ou sous fonction de sécurité, ils sont aussi appelés boucles de sécurité. Ils comprennent les matériels et logiciels nécessaires pour obtenir la fonction de sécurité désirée.

Ces systèmes peuvent atteindre un niveau d'intégrité de sécurité important en conformité avec les normes en vigueur telles que la norme IEC 61508 et la norme IEC 61511 qui traitent de la sécurité fonctionnelle des systèmes.

## 4.2 La composition d'un système instrumenté de sécurité

### 4.2.1 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.



**Figure 11: Schéma d'un SIS simple**

#### **Capteur :**

Est un dispositif qui convertit une grandeur physique en une autre grandeur, souvent électrique (tension, courant, résistance), qui est directement utilisable pour la mesure ou le contrôle. La grandeur physique d'origine peut être la température, la pression, le niveau, le débit ou la concentration d'un gaz.

#### **Unité de traitement :**

Selon Ayault (2005), l'unité de traitement peut varier en termes de complexité. Elle peut avoir pour fonction principale d'acquies et d'afficher une mesure provenant d'un capteur. Elle peut également jouer un rôle plus avancé en activant les commandes d'un ou plusieurs actionneurs en fonction de combinaisons d'informations fournies par différents capteurs. Les unités de traitement peuvent être classées en deux catégories en fonction de leur technologie. D'un côté, il y a les technologies câblées qui utilisent des composants logiques élémentaires (tels que des



relais) interconnectés électriquement (ou pneumatiquement). De l'autre côté, il y a les technologies programmées qui se basent sur des dispositifs tels que les centrales d'acquisition, les alarmes, les automates programmables (API), les systèmes numériques de contrôle-commande (SNCC), les calculateurs industriels ou les cartes électroniques équipées de microprocesseurs.

### **Actionneurs :**

Un actionneur peut être (vanne, moteur, servo-moteur...) transformer 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.

Enfin, l'unité de traitement est connectée aux capteurs et aux actionneurs par divers moyens de transmission. Ces moyens peuvent inclure des câbles électriques, des lignes téléphoniques, des ondes hertziennes (comme la transmission par talkie-walkie) ou des tuyauteries (pour la transmission pneumatique ou hydraulique).

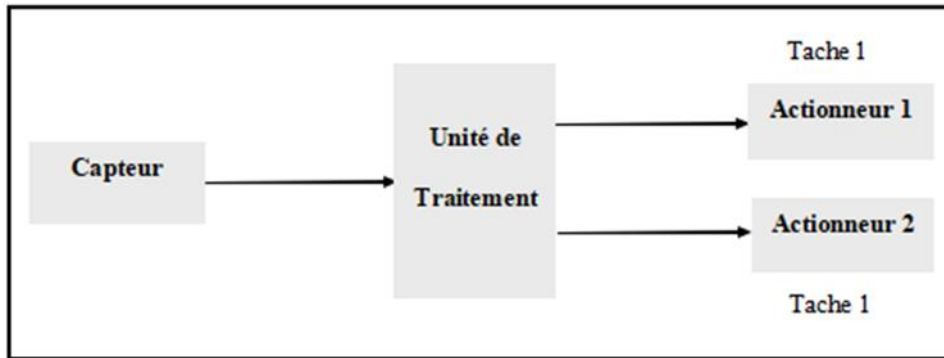
Les capteurs, l'automate et les actionneurs font partie des équipements de sécurité. Un équipement de sécurité est un élément d'un système instrumenté de sécurité (SIS) qui remplit une sous-fonction de sécurité.

En combinaison avec le traitement, l'ensemble de ces sous-fonctions permet la réalisation de la fonction instrumentée de sécurité "maîtriser une fuite".

### **4.2.2 Composition d'un SIS en fonction des tâches à 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 tâches que l'on trouve fréquemment au sein des SIS le montage en parallèle de plusieurs actionneurs.

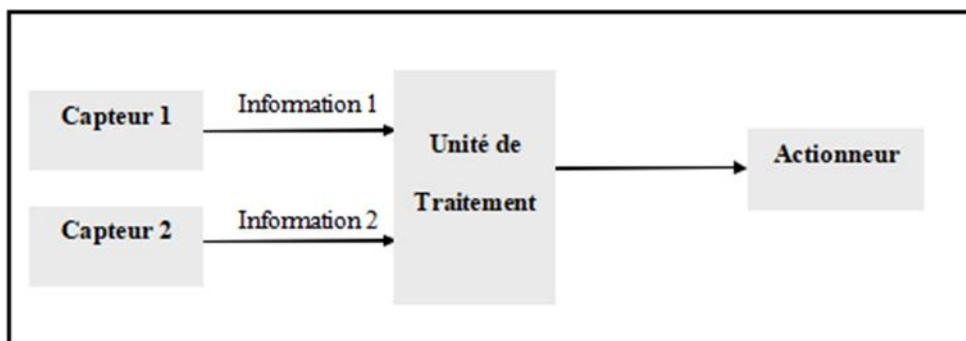
A noter qu'un unique actionneur peut commander plusieurs actionneurs. Par exemple, une électrovanne trois voies située sur un réseau d'air instrumenté peut, par mise à l'atmosphère de ce réseau, commander la fermeture de toutes les vannes pneumatiques alimentées par le réseau.



**Figure 12: Schéma d'un SIS effectuant plusieurs tâches**

Beaucoup moins fréquemment, on trouve le montage en parallèle de plusieurs capteurs afin de répondre à 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.

L'unité de traitement gère alors l'arrivée de différentes informations soit par un opérateur logique (par exemple, le déclenchement des actions de sécurité est réalisé si la température est supérieure à 100°C ou si la pression est supérieure à 10 bars), soit par calcul (par exemple, correction de l'information principale reçue par la deuxième information reçue).



**Figure 13: Schéma d'un SIS recevant plusieurs informations**

## 5. Fonction instrumentée de sécurité :

Les principales étapes de la norme IEC 61508 [IEC61508 98] et ses normes filles sont déclinées dans ce qu'on appelle le cycle de vie, c'est-à-dire que ces normes traitent depuis l'analyse des risques jusqu'à l'exploitation des fonctions de sécurité instrumentées SIF.

Une fonction instrumentée de sécurité 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.

Selon la norme CEI 61511 : Une fonction instrumentée de sécurité est une fonction de sécurité avec un niveau d'intégrité de sécurité spécifique qui est nécessaire pour assurer et maintenir la sécurité fonctionnelle et qui peut être soit une fonction instrumentée de protection ou une fonction instrumentée de contrôle.

La fonction instrumentée de contrôle est une fonction instrumentée de sécurité avec un niveau d'intégrité de sécurité spécifique fonctionnant en mode continu qui est nécessaire pour prévoir la survenance des événements dangereux et/ou limiter ces conséquences.

Un système instrumenté de sécurité contient habituellement plusieurs fonctions instrumentées de sécurité. Si les exigences d'intégrité de la sécurité pour ces fonctions instrumentées de sécurité diffèrent, alors les exigences applicables au niveau d'intégrité de la sécurité le plus élevé s'appliquent à l'intégralité du système instrumenté de sécurité, sauf si l'implémentation garantit une indépendance suffisante entre les fonctions de sécurité. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à réduire la fréquence d'occurrence du danger. Les probabilités de défaillance des différentes fonctions de sécurité ne peuvent s'additionner que si les fonctions sont indépendantes entre elles. Dans ce mémoire, nous prenons comme hypothèse que chaque SIS ne peut réaliser qu'une seule SIF.

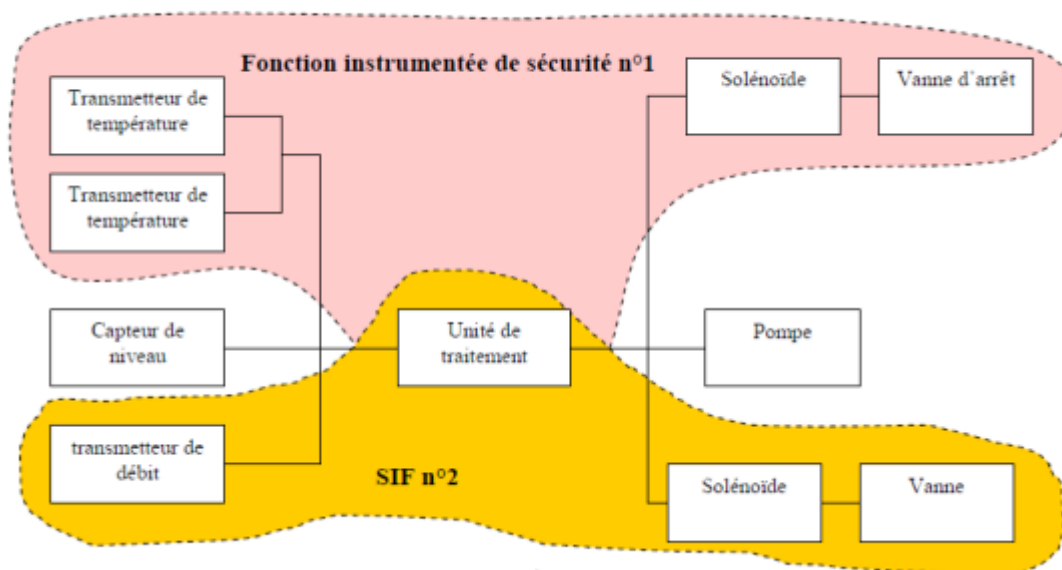


Figure 14: fonction instrumentée de sécurité

## 6. Intégrité de sécurité

Intégrité de sécurité est définie selon la norme CEI 61508 comme étant probabilité pour qu'un système relatif à la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps spécifiée.

Selon la norme CEI 61511 : l'intégrité de sécurité est la probabilité moyenne pour qu'un système instrumenté de sécurité mette en œuvre de manière satisfaisante une fonction instrumenté de sécurité dans toutes les conditions spécifiques et dans une période de temps spécifique.

## 7. Niveau d'intégrité de sécurité

Niveau d'intégrité de sécurité (SIL) : niveau discret (parmi quatre possibles) permettant de spécifier les prescriptions concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux systèmes E/E/PE relatifs à la sécurité. Le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité, le niveau 1 possède le plus bas.

Selon la norme CEI 61511 le niveau d'intégrité de sécurité est défini comme étant un niveau discret (parmi quatre possibles) permettant de spécifier les prescriptions concernant l'intégrité de sécurité des fonctions instrumentées de sécurité à allouer aux systèmes instrumentés de sécurité.

Les normes CEI 61508 et CEI 61511 définissent le niveau d'intégrité de sécurité SIL pour définir le niveau de réduction du risque, c'est-à-dire le niveau d'intégrité de sécurité que doit avoir le système de protection. Plus le SIL à une valeur élevée, plus la réduction du risque est importante.

## 8. Mode de fonctionnement d'un SIS

### 8.1 Faible sollicitation

La fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et la fréquence des sollicitations n'est pas supérieure à une par an.

### 8.2 Forte sollicitation

La fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et la fréquence des sollicitations est supérieure à une par an.

Dans la plupart des cas, le mode de sollicitation est de forte demande.

**Tableau 7: les niveaux de SIL**

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

## 9. Test relatif aux SIS

Les systèmes instrumentés de sécurité (SIS) agissent comme des dispositifs de sécurité essentiels. Afin de garantir leur performance continue, il est nécessaire de les soumettre à des tests. Ces tests impliquent la simulation de situations dangereuses pour vérifier si la fonction de sécurité pour laquelle ils ont été conçus est correctement mise en œuvre.

### 9.1 Rôle des tests

Ces tests permettent :

- d'avoir un retour sur la dérive des équipements et donc sur la maintenance à mettre en place,
- de détecter les défaillances non automatiquement détectables en temps réel.

Ils peuvent être considérés comme complets ou partiels (détection d'une partie uniquement des défaillances).

## 10. Classification retenue dans la norme CEI 61508

### 10.1. Classification des défaillances selon leurs causes

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

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

- ❖ Vieillessement du matériel. Les défaillances dues au vieillissement sont appelées défaillances naturelles ou primaires.
- ❖ Exposition aux contraintes excessives : ces contraintes peuvent être induites par des facteurs externes ou par des erreurs humaines. Ces défaillances sont appelées défaillances secondaires.

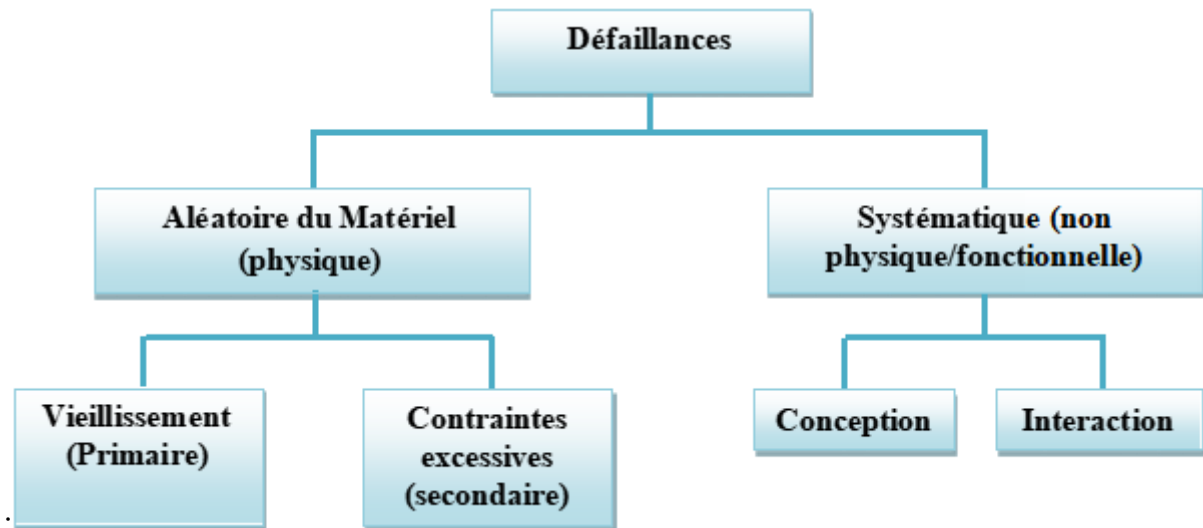
Les défaillances aléatoires du matériel sont relativement bien comprises. Les données relatives à cette catégorie de défaillances sont, dans la plupart du temps, disponibles.

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

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

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

Cette classification de défaillances est :



**Figure 15: Classification des défaillances selon leurs causes**

### 10.2. Classification des défaillances selon leurs effets sur la fonction de sécurité :

Toutes les défaillances, qu'elles soient aléatoires ou systématiques, peuvent être classées dans l'une des deux catégories suivantes : défaillances en sécurité ou défaillances dangereuses.

Dans cette classification, seules les défaillances aléatoires du matériel sont prises en compte. Selon la norme CEI 61508, les définitions des deux catégories sont les suivantes :

- Défaillance dangereuse : "une défaillance qui a le potentiel de mettre le système relatif à la sécurité dans un état dangereux ou l'empêcher d'exécuter sa fonction".
- Défaillance en sécurité : "une défaillance qui n'a pas le potentiel de mettre le système relatif à la sécurité dans un état dangereux ou l'empêcher d'exécuter sa fonction".

Dans le contexte de la norme CEI 61508, une défaillance dangereuse peut être définie comme une défaillance qui a tendance à compromettre la fonction de sécurité lorsqu'une demande émane de l'Équipement Sous Contrôle (EUC), le plaçant ainsi dans un état dangereux. En revanche, une défaillance sûre est une défaillance qui a tendance à prévenir l'activation de la fonction de sécurité en l'absence de toute demande, maintenant ainsi l'EUC dans un état sûr. Autrement dit, cela signifie que la survenue de tout événement préjudiciable devient impossible.

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

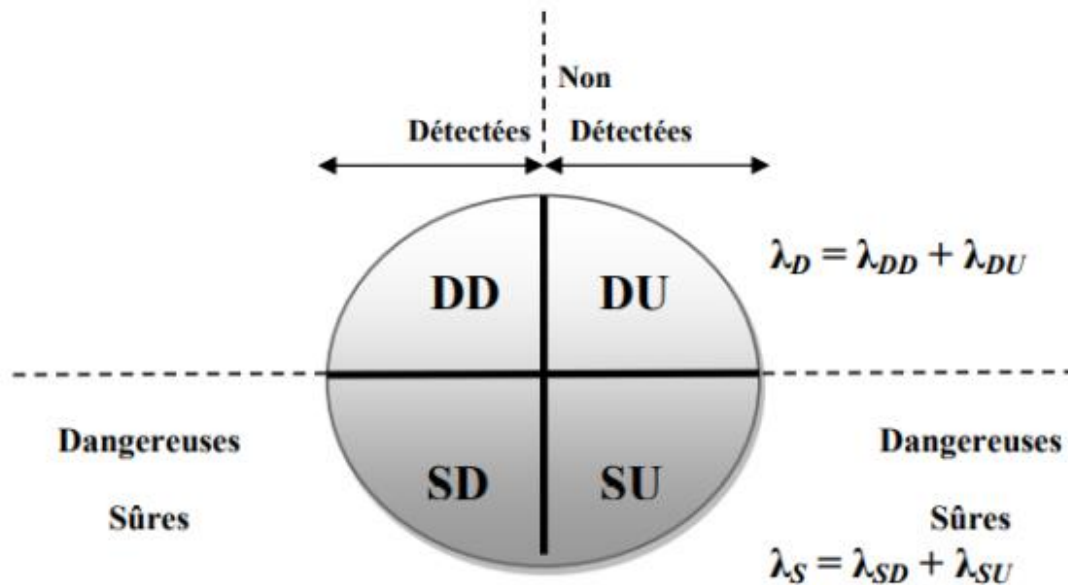
$$\lambda = \lambda_S + \lambda_D$$

Avec :

$\lambda_S$ : taux de défaillance aléatoire en sécurité du matériel,

$\lambda_D$ : taux de défaillance aléatoire dangereuse du matériel.

Une autre distinction se fait en fonction de savoir si ces défaillances peuvent être détectées par des tests en ligne ou non. Les défaillances qui peuvent être détectées sont appelées "défaillances détectées", tandis que celles qui ne peuvent être révélées que lors de tests périodiques hors ligne ou lors de l'utilisation du SIS par le système surveillé sont appelées "défaillances non détectées". Le schéma suivant est couramment utilisé pour résumer cette double distinction.



**Figure 16: Typologie des défaillances selon la norme CEI 61508**

### 10.3. Classification proposées par SINTEF

Cet organisme propose SINTEF [34], 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 :



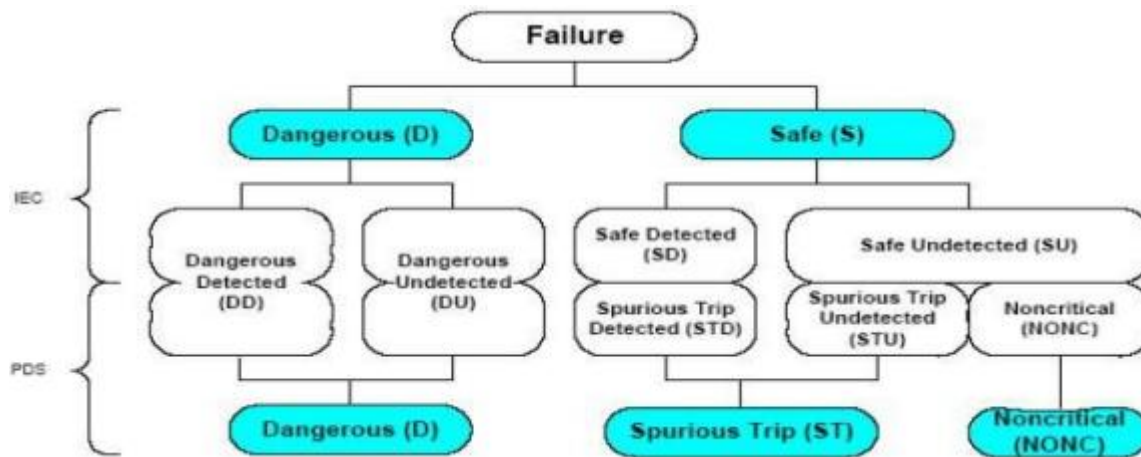


Figure 17: Classification des défaillances selon SINTEF . [34]

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

- Les défaillances dangereuses sont celles de la norme et se divisent donc en défaillances détectées ( $\lambda_{DD}$ ) et non-détectées ( $\lambda_{DU}$ ).
- Les défaillances intempestives sont un sous-ensemble des défaillances sûres et se divisent également en défaillances détectées ( $\lambda_{STD}$ ) et non-détectées ( $\lambda_{STU}$ ).
- Les défaillances non-critiques ( $\lambda_{NONC}$ ) sont celles qui n'ont aucune incidence sur les deux fonctions principales du système EUC, c'est-à-dire son aptitude à produire (disponibilité de production) et son aptitude à ne pas engendrer d'événements redoutés (sécurité).

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

- $\lambda_{DD}$  et  $\lambda_{DU}$  sont ceux définis dans la norme.
- $\lambda_{STD}$  est le taux de défaillance intempestive détectée. Il correspond au  $\lambda_{SD}$  de la norme.
- La somme ( $\lambda_{STD} + \lambda_{NONC}$ ) correspond au  $\lambda_{SU}$  de la norme.
- La somme ( $\lambda_D + \lambda_{STD} + \lambda_{STU}$ ) est appelée  $\lambda_{crit}$ .

## 11. Méthodes qualitatives et quantitatives pour la détermination des SIL

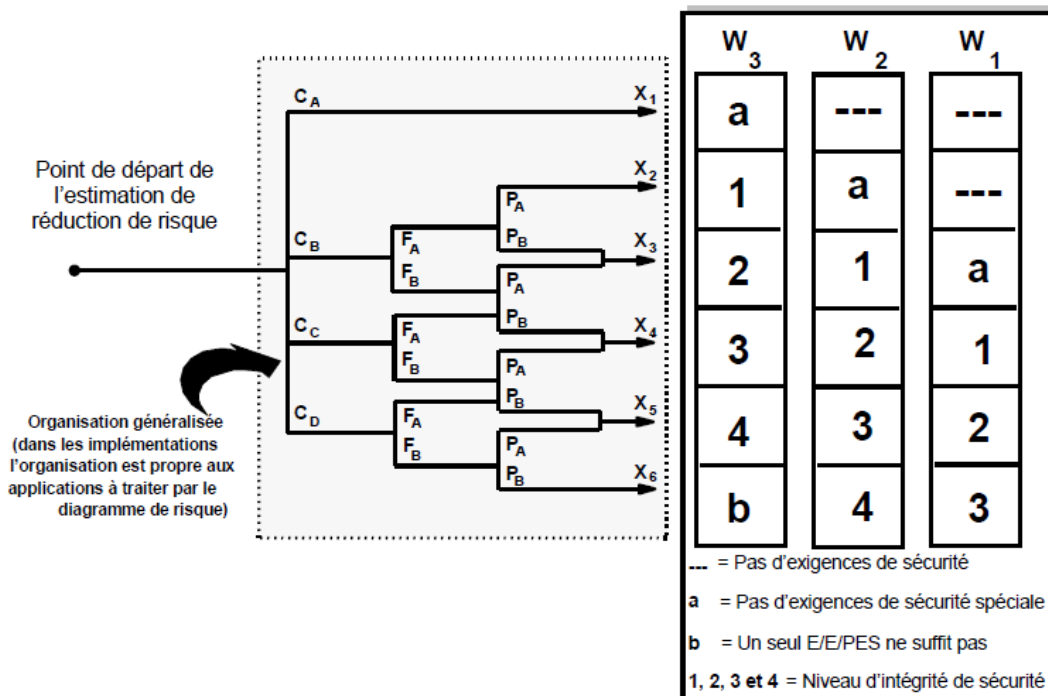
La norme IEC 61508 fixe le niveau d'intégrité de sécurité (SIL) qui doit être atteint par un SIS qui réalise la Fonction Instrumentée de Sécurité (SIF). Elle donne le SIL en fonction de sa probabilité de défaillance moyenne (PFD<sub>avg</sub>) sur demande pour les SIS faiblement sollicités

(moins d'une sollicitation par an) ou en fonction de probabilité de défaillance par heure (PFH) pour les SIS fortement sollicités où agissant en mode continu.

**11.1. Méthodes qualitatives :**

Il s'agit de méthodes qui permettent de déterminer et allouer le niveau de SIL à partir de la connaissance des risques associés au procédé.

Le graphe de risque consiste à hiérarchiser les niveaux de sécurité à partir de quatre paramètres liés à la conséquence du risque sur le personnel ou l'environnement (C), à la fréquence d'exposition au risque (F), à la possibilité d'éviter le danger (P) et à la probabilité d'occurrence du danger (W) tels que présenté sur la figure 18



**Figure 18: Graphe de hiérarchisation du risque présenté dans la norme CEI 61511-3**

La classification repose sur une hiérarchisation en 6 classes d'exigences graduées de "a" à "b" en passant par SIL1 à SIL 4. La catégorie "a" correspond alors à "aucune exigence particulière de sécurité" tandis que la catégorie "b" correspond à une situation inacceptable (le système instrumenté est insuffisant).

Ce graphe s'explique de la manière suivante. L'utilisation des paramètres de risque C, F et P aboutit à un certain nombre de sorties (X1, X2, ..., Xn). Chaque sortie est consignée dans une des trois échelles (W1, W2 et W3). Chaque échelle indique le niveau de SIL nécessaire auquel doit satisfaire le système relatif à la sécurité pris en considération. La mise en correspondance

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

Un exemple de classification des paramètres du graphe de risques est montré au tableau 9.

**Tableau 8: Légende de la classification des paramètres de risques**

Paramètres de risque		Classification
Conséquences	CA	Incident mineur
	CB	Effets réversibles
	CC	Effets létaux limités au site
	CD	Effets létaux en dehors du site
Exposition	FA	Exposition rare dans la zone considérée
	FB	Exposition fréquente dans la zone considérée
Possibilité d'éviter le danger	PA	Possible sous certaines conditions
	PB	Impossible
Taux de sollicitations	W1	Faible probabilité (Accident pouvant se produire)
	W2	Probabilité moyenne (Accident, déjà observé)
	W3	Probabilité élevée (Accident fréquent, observé plus d'une fois)

### 11.2. Les méthodes quantitatives

Il s'agit des méthodes qui permettent de calculer la probabilité de défaillance moyenne des SIS à partir des paramètres de fiabilité de leurs composants.

Les méthodes les plus répandues sont :

- Les équations simplifiées proposées par la norme.
- Les arbres de défaillances.
- Les approches Markoviennes.

### Conclusion

.En conclusion, ce chapitre a présenté les principaux éléments relatifs à l'analyse du niveau de SIL et à la définition des SIL dans les systèmes instrumentés de sécurité (SIS). Nous avons examiné les normes pertinentes, telles que la norme CEI 61508 et la norme CEI 61511, qui fournissent des directives et des méthodes pour évaluer la sécurité fonctionnelle des systèmes. Nous avons également examiné la composition d'un SIS, en soulignant l'importance des fonctions instrumentées de sécurité et de l'intégrité de sécurité. Les différents modes de fonctionnement d'un SIS, tels que la faible sollicitation et la forte sollicitation, ont été abordés, mettant en évidence les tests nécessaires pour garantir le bon fonctionnement du système.

La classification des défaillances selon leurs causes et leurs effets a été discutée, soulignant l'importance de comprendre les différentes sources de défaillances et leur impact sur la sécurité. Nous avons également examiné les méthodes qualitatives et quantitatives utilisées pour déterminer les SIL, en mettant l'accent sur les avantages et les limitations de chaque méthode.

# CHAPITRE 3

## Présentation du cas d'étude

## Introduction

L'Algérie a acquis ces dernières 20 années, une expérience dans le domaine de GPL, devenu un produit de large consommation (2,4 millions tonnes/an), répondant aux exigences de la politique énergétique nationale. L'Algérie dispose d'un potentiel en GPL, qui peut atteindre 9.7 millions tonnes/an, capable d'alimenter des programmes d'exportation. Le centre vrac 165 est l'un des centres les plus importants en Algérie et en Afrique, depuis sa construction en 1984.

De ce fait, Ce chapitre présente une étude de cas basée sur l'entreprise NAFTAL et plus spécifiquement sur sa branche GPL (Gaz de Pétrole Liquéfié). Nous examinerons en détail cette entreprise, sa branche GPL située à Tiaret, ainsi que le système F&G (Fire and Gas) utilisé dans ses installations. Cette présentation vise à fournir une compréhension approfondie du contexte dans lequel se déroule notre étude. [6].

## 1. L'entreprise NAFTAL

### 1.1. Historique

Issue de SONATRACH, l'entreprise du Raffinage et de la Distribution des produits Pétroliers en Algérie (ERDP) a été créée par le décret N°80-101 du 06 avril 1980.

L'entreprise ERDP, est entrée en activité le 01 janvier 1982, sous le signe NAFTAL qui est titre de deux syllabes :

**NAFT** : Pétrole en arabe ;

**AL** : Algérie.

En 1987 par décret N° 87/189 du 25 /08/1987 l'activité du raffinage est séparée de l'activité distribution par la création de la société appelée NAFTEC.

A partir de 1998, elle change de statut et devient filiale à 100% du groupe SONATRACH.

NAFTAL a pour mission principale, la distribution et la commercialisation des produits pétroliers sur le marché national. [6].

### 1.2. Présentation de l'entreprise

**NAFTAL** est une société nationale composée de trois grandes Branches qui sont :

La branche GPL (Gaz du Pétrole Liquéfié).

La branche carburants (terre, AVM).

La branche Commercialisation (Bitumes, pneumatique, lubrifiants et stations de services.

Les branches ont pour mission de définir avec la direction générale, la stratégie de distribution et de commercialisation des produits pétroliers en veillant à assurer toutes les conditions nécessaires à la bonne gestion des centres opérationnels de la société .[6].

### 1.3. Présentation de la branche GPL

Créé le 15 octobre 1998, la Branche GPL a été chargée des activités liées au transport, stockage, enfûtage, distribution, promotion et développement des GPL de l'entreprise NAFTAL surtout le territoire national.

Les principaux objectifs de la branche sont :

Gérer, organiser, promouvoir et développer l'activité d'enfûtage et de distribution des GPL (transport du GPL vrac par cabotage, canalisation et camion, stockage primaire et secondaire, transport par route des GPL conditionnés) ;

Commercialiser les GPL vrac et conditionner leurs emballages et accessoires ;

Veiller au respect des normes et consignes de sécurité de toute la chaîne des GPL (transport, installations d'enfûtage et de stockage, bouteilles, citernes, accessoires, etc.).

#### 1.3.1. Services et produits :

Les GPL sont des mélanges de Butane (C4) et de Propane (C3), qui peuvent être obtenus à partir de diverses sources de traitement des hydrocarbures telles que :

- Le traitement du gaz naturel ou gaz associés.
- Le raffinage du pétrole.
- La liquéfaction du gaz naturel.

Dans la gamme des produits GPL, **NAFTAL** commercialise deux produits essentiels :

##### ➤ **Le Butane Commercial :**

Mélange d'hydrocarbures composé essentiellement de butanes et de butènes et en faible proportion de propane et de propène (moins de 19 % du volume). Le butane est commercialisé sous deux formes de conditionnement :

- Bouteille de 13 Kg (B13).

- Bouteille de 06 Kg (B6).

### **Généralités**

- Bouteille de 03 Kg (B3).

#### ➤ **Le Propane Commercial :**

Mélange d'hydrocarbures composé d'au moins 93% de propane et de propène et pour le surplus d'éthane, d'éthylène, de butane et de butènes.

Le propane conditionné est commercialisé en bouteille de 35 kg exclusivement.

➤ **GPL Carburant :** « SIRGHAZ » est intervenue en 1983 avec l'adoption de la bicarburation et la mise en place de la réglementation liée aux conditions d'utilisation et de distribution du GPL/C.

➤ **Lubrifiants :** Naftal commercialise une gamme complète de lubrifiants qui couvre toutes les applications du secteur automobile et industriel.

➤ **Pneumatiques :** Naftal commercialise des pneumatiques de grandes marques dans les catégories de véhicules les plus divers.

#### ➤ **Bitume**

➤ **Produits Spéciaux :** Naftal commercialise dans sa gamme de produits spéciaux quatre 04 familles de produits (Les Paraffines, Les Cires, Les Essences spéciales, Les Solvants)

## **2. Présentation de la branche GPL CE 141 TIARET**

Créé le 15 octobre 1998, la Branche GPL a été chargée des activités liées au transport stockage, enfûtage, distribution, promotion et développement des GPL de l'entreprise

NAFTAL surtout le territoire national.

### **2.1. Description générale :**

Le Centre Emplisseur « CE 141 Tiaret », est un centre parmi plusieurs centres d'emplissage de gaz de pétrole liquéfié (GPL) de l'exploitant **NAFTAL BRANCHE GPL**, mis en service en 1985.

Dans lequel se déroulent les opérations de stockage, conditionnement et la distribution des bouteilles de 13kg de butane et de propane P35, destinées à être utilisées dans divers domaines.



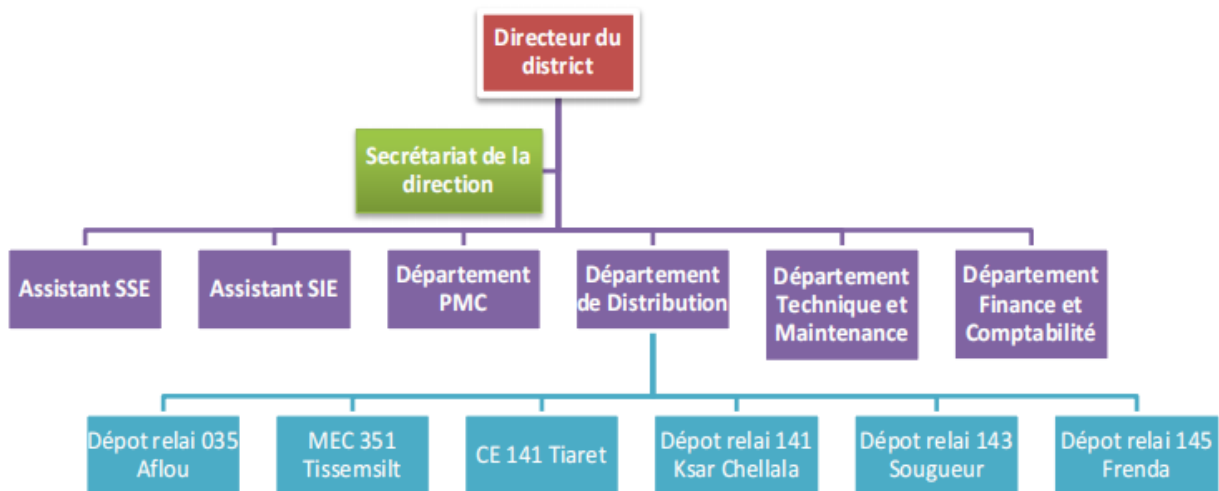
## 2.2. Situation Géographique :

Le centre s'étend sur une superficie de **43 001m<sup>2</sup>** dans la zone industrielle Zaaroura, au Sud-ouest de la wilaya de Tiaret. Avec une surface bâtie de **3 387,90m<sup>2</sup>** sans le hall d'emplissage.



Figure 19: localisation de centre d'emplissage (Google Earth)

### 2.3. Organigramme de l'organisation :



**Figure 20: Organigramme de l'organisation**

### 2.4. Les zones d'entreprise :

#### ❖ Zone classée

- ✓ Hall d'emplissage.
- ✓ Stock des bouteilles.
- ✓ Poste chargement /déchargement contient deux Bras (dans chacun des deux on a un bras pour phase liquide et un autre pour phase gazeuse).
- ✓ Pompier GPL dont il y a 04 pompes GPL et 03 compresseurs GPL.
- ✓ Un bac d'eau anti-incendie.

Deux cigares pour le stockage du propane  $C_3H_8$  chacune avec une capacité de  $150m^3$  (75T) et une sphère de  $2000m^3$  (1000T) pour le butane  $C_4H_{10}$

#### ❖ Zone non-classé

- ✓ Vestiaires.
- ✓ Ateliers.
- ✓ Magasins.
- ✓ Bloc administration.

Le district GPL Tiaret est approvisionné en butane et propane vrac à partir d'Arzew (GP1Z et GP2Z) ou l'on transporte le produit dans des citernes spéciales.

Arrivés au niveau des centres on procède au dépotage du produit et son stock :

-pour le centre 141 de Tiaret, dans une sphère pour le butane et deux cignes pour le propane.

### 2.5. Produits stockés :

**Tableau 9: produits stockes**

Nature des produits stockés	Capacité de stockage	Condition de stockage
Butane	2000 m <sup>3</sup>	Une (01) Sphère
Propane	300 m <sup>3</sup>	02 Cignes d'une capacité unitaire 150 m <sup>3</sup>
Gasoil	3000 Litres	Cuve enterrée
Principaux produits mis en Œuvre	Le Propane Le Butane	
Principaux produits dangereux mis en œuvre	<ul style="list-style-type: none"> <li>- Le Propane</li> <li>- Le Butane</li> </ul>	

**Butane** : Le butane est un gaz issu du raffinage de pétrole, dont la formule chimique est (C<sub>4</sub>H<sub>10</sub>), il a comme tous les GPL, un pouvoir calorifique plus élevé que le gaz naturel et il est moins toxique. Il est naturellement incolore et inodore, mais a été rendu odorant pour raisons de sécurité.

**Le Propane** : C'est un gaz également dérivé du pétrole dont la formule chimique est (C<sub>3</sub>H<sub>8</sub>). C'est le plus léger des GPL commercialisés par NAFTAL, il a donc le pouvoir calorifique le plus élevé.

Le GPL/carburant ou le SIRGHAZ : Le sirghaz est un mélange de butane et de propane (en hiver c'est 100% de propane, en été – il est composé de 80% de butane). Il est stocké dans la station de service à bord des véhicules sous forme de liquide, sous une pression de 5 à 8 bars.

## 2.6. Installations et Bâtiments principaux :

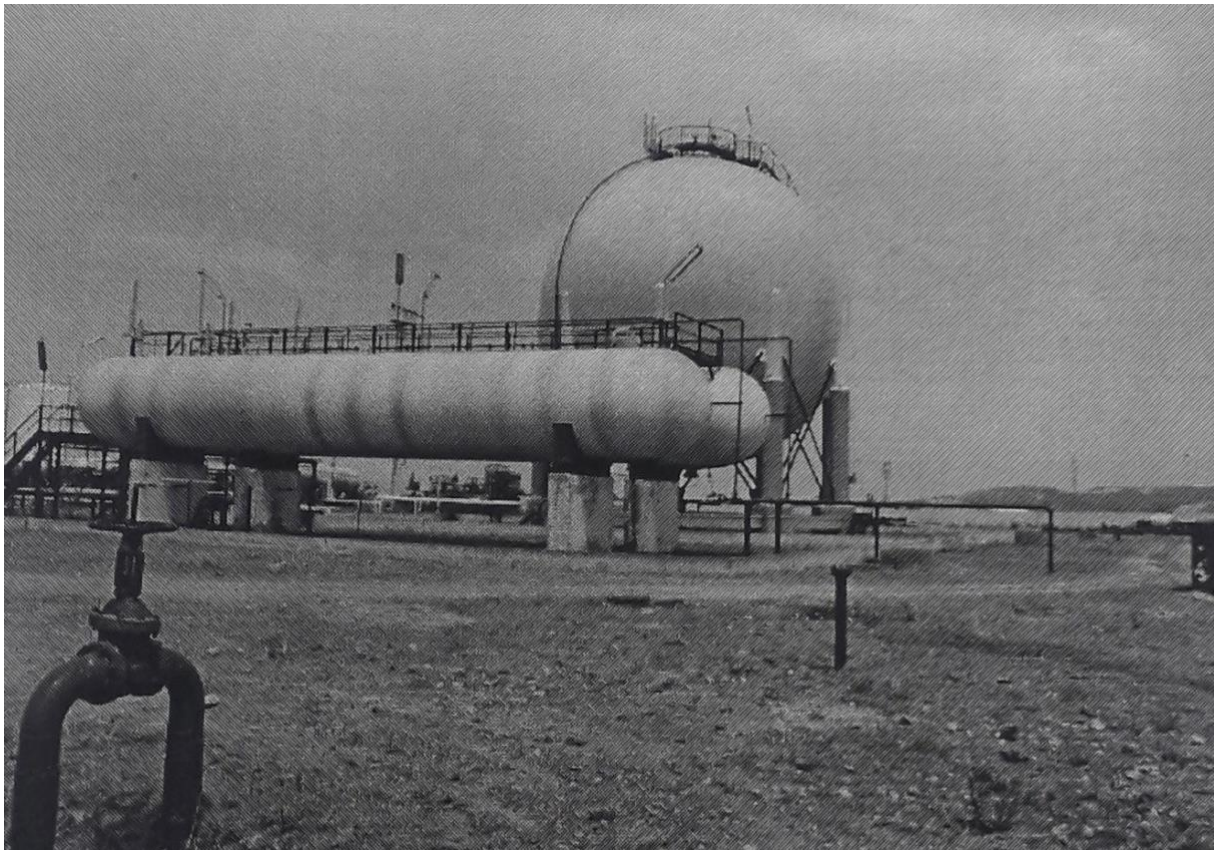
**Tableau 10: Installations et Bâtiments principaux**

<p><b>Installations principales</b></p>	<ul style="list-style-type: none"> <li>- Bloc administratif.</li> <li>- Hangar magasin.</li> <li>- Atelier mécanique.</li> <li>- Un hall d'enfûtage (bouteilles propane et butane).</li> <li>- Sphère Butane 2000m<sup>3</sup>.</li> <li>- Deux cigares Propane 150m<sup>3</sup>/unité.</li> <li>- Pomperie GPL.</li> <li>- Bâtiment utilités (Station d'air comprimé et groupe électrogène).</li> <li>- Aire de chargement/déchargement des camions.</li> <li>- Réserve eau incendie.</li> <li>- Transformateur.</li> <li>- Deux postes de garde et 02 guérites pour agents de sécurité.</li> </ul>
<p><b>Points dangereux</b></p>	<ul style="list-style-type: none"> <li>- Sphère Butane.</li> <li>- Cigares Propane.</li> <li>- Hall d'emplissage.</li> <li>- Pomperie.</li> <li>- Aire de Chargement/déchargement des Camions.</li> <li>- Circuit interne de GPL.</li> </ul>

### 2.7. Description des Réservoirs de Stockage :

Le Butane est stocké dans une (01) sphère d'une capacité de 2000m<sup>3</sup> à température ambiante sous sa pression de vapeur saturante. Cependant, le Propane est stocké dans deux (02) cigares d'une capacité unitaire de 150m<sup>3</sup>.

Les stockages sont mis en rétention. Un dispositif d'arrosage fixe permet d'arroser les réservoirs en cas de nécessité pour les refroidir lorsqu'ils sont soumis à un feu ou au rayonnement d'un feu voisin.



**Figure 21: réservoirs de stockage**

#### Caractéristiques des Bâtiments :

Le Hall d'emplissage se compose de :

- Deux carrousels de vingt-quatre (24) bascules (butane).
- Quatre bascules de remplissage propane sur convoyeur P35 (bouteilles de 35kg Propane).
- Une bascule de remplissage propane P11 (bouteille 11kg propane).
- Une bascule de remplissage butane B3 (bouteille 3kg butane).

- Deux palettiseuses.
- Un convoyeur entrée vide.
- Convoyeur sortie plein.

La Zone de stockage bouteilles :

- Une aire de stockage est dédiée aux bouteilles de gaz pleines, en attente d'expédition.
- Les bouteilles de gaz sont stockées par type de gaz, par capacité et par marque commerciale.
- Les bouteilles de gaz sont palettisées dans des casiers métalliques.

### **2.8. Activités de l'entreprise**

NAFTAL a pour mission principale, la distribution et la commercialisation des produits pétroliers sur le marché national. Elle intervient dans les domaines :

- De l'enfûtage GPL.
- De la formulation de bitumes.
- De la distribution, stockage et commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux.
- Du transport des produits pétroliers.

Pour assurer la disponibilité des produits sur tout le territoire, NAFTAL met à contribution plusieurs modes de transport :

- Le rail pour le ravitaillement des dépôts à partir des entrepôts.
- Le cabotage et les pipes, pour l'approvisionnement des entrepôts à partir des raffineries.
- La route pour livraison des clients et le ravitaillement des dépôts non desservis par le rail.





**Figure 22: les différentes activités de l'entreprise**

Le ravitaillement du GPL vrac s'effectue par des attelages (tracteurs + citernes) d'ARZEW comme une source (SONATRACH GP1/z et GP2/z) et de stocker ce produit vrac dans des capacités comme suite :

- Une sphère de  $2000m^3$  1000TM pour le butane.
- Deux cigares de  $150m^3$  75TM dans chacune pour le stockage du propane vrac.
- Le chargement et le déchargement de ces réservoirs s'effectuent à l'aide des bras de chargement/déchargement.
- Une pomperies GPL contient des pompes et des compresseurs GPL.
- Un bloc pour les utilités où se trouve pomperies du réseau anti-incendie, compresseurs d'air, armoires pour l'alimentation en courant du CE et un groupe électrogène pour maintenir le courant électrique en cas de coupure ou rupture électrique.

Un réseau anti-incendie pour sécuriser le personnels et les installations de l'établissement se réseau alimenté par un bac de stockage de  $150m^3$  d'autonomie de 3heures d'intervention, de deux motopompes une de  $500m^3/h$  et une autre de  $300m^3/h$ , de quatre.

### **2.9. Les Moyens de Prévention au niveau du centre :**

A travers sa politique HSE, NAFTAL – Branche GPL vise à réduire la probabilité de la survenance de situation d'urgences pendant le déroulement des opérations du Centre.

Formation, Information et Sensibilisation : Le personnel est formé sur les bases de la sûreté et sécurité individuelle et collective, et suit les informations provenant de leur chef, et font ainsi

partie de plusieurs exercices de sensibilisation qu'ils refassent au sein du centre quelques fois chaque année.

EPI/EPC : Le port des EPI (équipement de protection individuelle) est obligatoire, et la présence des EPC (équipements de protection collective) l'est également.

Détection gaz et flammes : Le centre est muni d'un grand réseau de détecteurs de gaz/fumée répartis dans les zones ATEX et les zones où le gaz est présent en permanence.

Audit Interne et Externe et Inspection ; des inspections régulières sont faites de la part du personnel

HSE de NAFTAL, et visent le bon état des machines, outils, accessoires, ...Etc. Et vérifie aussi le comportement du personnel envers les exigences de sécurité demandées

### 2.9.1. Réseau anti-incendie :

Le réseau anti incendie au CE 141 Tiaret se compose de :

- Réserve d'eau de 1500 m<sup>3</sup> située dans la cour.
- 03 électropompes d'une capacité de 108 m<sup>3</sup> /h et une (01) de 150 m<sup>3</sup> /h.
- 02 motopompes de 500-300 m<sup>3</sup> /h.
- Des Armoires et poteaux anti incendie réparties dans la cour et le hall d'emplissage et 03 **RIA** (robinets d'incendie armés) au niveau du hall.

La détection et déclenchement du réseau dépend de l'efficacité des 41 détecteurs de fumée et de gaz répartis dans les zones où la concentration du gaz ou le danger d'incendie sont présents.

## 3. Système F&G

Le système gaz et flamme (ou système G&F) est un système de détection et de contrôle de flamme utilisé dans diverses applications industrielles pour la sécurité et la régulation des processus.

Le système G&F est conçu pour détecter les flammes produites par des combustibles tels que le gaz, le pétrole, le charbon, le bois, etc., et pour activer des dispositifs de sécurité tels que des vannes d'arrêt ou des systèmes d'extinction automatique en cas de détection d'une flamme non contrôlée.



Le système G&F peut utiliser diverses méthodes de détection de flamme, telles que la détection UV, la détection IR, la détection de rayonnement visible, etc. Les capteurs de flamme sont généralement placés à proximité des zones où les flammes sont susceptibles de se produire, telles que les brûleurs de gaz, les cheminées, les fours, etc.

### 3.1. Fonction de base de système G&F

Système conçu pour prévenir aussi tôt que possible des incidents suivants et en indiquer l'emplacement :

- Fuite de gaz inflammable.
- Fuite de gaz toxique ou faible niveau d'oxygène.
- Feu ou combustion.

Et pour déclencher la mise en œuvre d'un moyen d'extinction et mettre l'établissement en configuration de sécurité, avec l'interfaçage (et l'assistance ...) du système ESD.

Le fonctionnement de base du système de gaz et de flamme peut être résumé en quatre étapes principales :

**Détection** : le système est équipé de détecteurs de fumée, de chaleur ou de flammes qui surveillent en permanence les zones à risque d'incendie. Lorsqu'un feu est détecté, le système déclenche une alarme pour avertir les occupants de l'immeuble et des mesures d'urgence peuvent être prises.

**Alarme** : Lorsqu'un incendie est détecté, le système déclenche une alarme sonore et visuelle pour avertir les occupants de l'immeuble. Cette étape est cruciale pour permettre une évacuation rapide et sûre des personnes et faciliter l'intervention des équipes de secours.

**Extinction** : En fonction du type de système de gaz et de flamme, des agents d'extinction peuvent être automatiquement déployés pour éteindre l'incendie ou contenir sa propagation. Les agents d'extinction les plus couramment utilisés sont les gaz ininflammables comme l'azote, l'argon, le dioxyde de carbone ou les gaz halogénés.

**Arrêt du système** : une fois l'incendie éteint, le système est réarmé pour être prêt à détecter et répondre à d'autres incendies éventuels.

Le système de gaz et de flamme est essentiel pour protéger les personnes, les biens et les actifs des risques d'incendie. Il est important de noter que la conception, l'installation et l'entretien du

système doivent être effectués par des professionnels qualifiés pour garantir leur fiabilité et leur efficacité en cas d'urgence

### 3.2. Détection

Un détecteur est un dispositif ou un instrument qui est conçu pour détecter, mesurer ou surveiller un signal ou un phénomène spécifique. Les détecteurs sont utilisés pour identifier la présence de quelque chose, tels que des particules, fumée, chaleur, flamme, gaz toxiques et inflammables, MCP (déclencheur manuel d'alarme).

#### 3.2.1 Emplacements concernés

Tous les lieux d'un site sont concernés par le système. La protection est différente (ou « adaptée ») selon l'emplacement ou la zone spécifique :

- Bureau : risque d'incendie « classique ».
- Local technique : risque d'incendie d'origine électrique.
- Procédé : feu et fuites de gaz. Lieu confiné : feu, gaz toxique et faible niveau d'oxygène.

#### 3.2.2 Fonctions de base

Les équipements de détection, de commande (traitement) et d'action constituent les trois caractéristiques principales du système F&G.

Les signaux des capteurs sont centralisés (dirigés) vers le système logique qui identifie, analyse et active les équipements afin que les actions spécifiques opportunes soient mises en œuvre.

Afin d'augmenter la fiabilité, toutes les alimentations électriques doivent être connectées à des sources disponibles en permanence (batteries, alimentations non interruptibles), toute la logique doit être assurée par des processeurs redondants. Toutefois, dans certaines configurations de détection spécifiques, toutes les alimentations, y compris les batteries et les alimentations non interruptibles, doivent être à l'arrêt et isolées.

#### 3.2.3. Détection

Fumée, chaleur, flamme, gaz toxiques et inflammables, MCP (déclencheur manuel d'alarme),  
...

**Détection rapide :** Un « instant » est suffisant pour qu'un incendie (ou une explosion) causant d'importants dégâts se produise. Par conséquent, la détection doit se faire aussi rapidement que possible.

**Gaz inflammables ou explosifs :** La présence d'un gaz inflammable doit être détectée immédiatement, ceci afin de sécuriser le(les) zone(s) concernée(s) et de lancer l'action qui s'impose pour éliminer le risque d'explosion. Des points de détection déterminés (avec plusieurs niveaux d'alarme) sont fixés bien en dessous de la limite d'explosivité, ceci afin de permettre un temps de « réaction » et d'éviter le point critique.

**Gaz toxiques :** Il s'agit là d'une détection critique. La sécurité du personnel est la priorité numéro un, mais de toutes façons, la présence d'un gaz toxique signifie qu'il y a un « problème » du type fuite, obturation, fonctionnement défectueux, pièces endommagées, etc...

### 3.2.4. Les types de détecteurs :

#### 3.2.4.1. Le détecteur optique de flamme :

Plus communément appelé détecteur de flamme réagit aux rayonnements émis par tous types de flammes. Elaboré pour prévenir très rapidement un départ de feu en quelques dizaines de millisecondes,

#### Fonctionnement des détecteurs de flammes :

Les détecteurs optiques de flammes sont composés de capteurs travaillant dans les rayonnements invisibles à savoir l'ultraviolet (UV) ou l'infrarouge (IR). Les plus performants des détecteurs de flammes possèdent généralement plusieurs capteurs (UV, UV/IR, IR3 ou IR4). À l'instar d'un détecteur gaz fixe, un détecteur de flammes fonctionne généralement connectés à une centrale de détection gaz.

#### 3.2.4.2. Les différents types de détecteurs optiques de flamme :

**Détecteur de flamme UV :** Composé d'un capteur sensible à la radiation UV. Génère un signal de sortie, fonction du rayonnement, comparé à une référence minutieusement calculée.

**Détecteur de flamme IR :** Composé d'un capteur sensible à la radiation IR émise par le CO<sub>2</sub> issue de la combustion du produit en flamme.

**Détecteur de flamme UV-IR :** Ce détecteur combine un capteur UV et un capteur IR pour la détection de feux d'hydrocarbures, d'hydrogène et de métaux avec temps de réponse très rapide (<150 msec). Requier une réponse simultanée des deux éléments sensibles.

**Détecteur de flamme IR3 :** Trois capteurs pyroélectriques détectent les radiations IR relatives à différents pics d'émission. Le capteur IR3 pour la détection de flammes d'hydrocarbures n'est pas sensible au rayonnement solaire.

**Détecteur de flamme IR4 :** Combinaison de 4 capteurs infrarouges pour la détection de flammes d'hydrocarbures et d'hydrogène sur des distances de 5 à 65 mètres maximum, tout en assurant une haute immunité aux alarmes intempestives.

#### **Détecteur de gaz fixe :**

Les détecteurs gaz fixes sont des capteurs gaz destinés à la détection et la mesure des concentrations de gaz :

Gaz explosifs (gaz naturel, GPL, hydrocarbures, solvants, alcools), gaz toxiques, composés organiques volatils (COV), gaz asphyxiants (manque d'oxygène) ou fréons (fluides frig La plupart des détecteurs de gaz fixes disposent d'une sortie linéaire 4-20 mA permettant de les relier à une centrale de détection gaz et sont certifiés ATEX. Certains modèles plus évolués disposent en plus d'un afficheur numérique, de relais d'alarme ou de là de communication numérique. Pour chaque type de fluide, il existe une technologie spécifique de cellule, garantissant la précision et la répétitivité des mesures. (En savoir plus sur les technologies de cellules) origines).

#### **3.2.4.3 Bris de glace**

Le bris de glace est un dispositif de sécurité qui se présente sous la forme d'une boîte en verre contenant un marteau ou une clé spéciale. En cas d'urgence, une personne peut briser la vitre de la boîte pour accéder à la clé ou au marteau, et ainsi déclencher une alarme incendie où fermer une vanne d'isolement pour arrêter l'écoulement d'eau dans le système de sprinklers.

Le bris de glace est un moyen simple mais efficace pour assurer la rapidité d'intervention en cas d'incendie et éviter des dommages plus importants. Il est souvent utilisé dans les lieux publics, les immeubles de grande hauteur, les entrepôts, les usines, etc.

### 3.3. Unité centrale

#### 3.3.1. Définition :

La centrale de détection est une unité fixe de contrôle de présence de gaz en liaison permanente avec un ou plusieurs détecteurs de Gaz fixes.

#### 3.3.2. Les fonctions de système de traitement (détection) :

- Contrôler l'intégrité des lignes de détection (détection d'un circuit ouvert, de fils rompus)
- Déclencher les alarmes (sonores, visuelles), l'évacuation. Interconnexion avec le PAGA (Public (Adresse and General Alarme : annonce vocale et alarme générale) (si nécessaire).
- Déterminer au sein de leur logique les actions à mettre en œuvre Interfacier avec les autres processeurs (système ESD, DCS, PLC de traitement,).
- Autoriser le blocage et la dérivation pour les tests et la maintenance

### 3.4. Action

La détection et la commande logique doivent déclencher un démarrage automatique (pompes à incendie) et/ou une activation automatique (vannes, électrovannes) des équipements de lutte contre l'incendie. Les actions peuvent être résumées ainsi :

- Alarmes sonores, visuelles
- Message par annonce vocale (PAGA) – ordre d'évacuation ou autres messages
- Equipements d'extinction/de lutte contre l'incendie automatiquement connectés
- Signaux au DCS, à l'ESD et automatismes de traitement pour des initiatives de conditions de sécurité.
- Informations à l'équipe de lutte contre l'incendie

Sur ce, les fonctions de « sortie » (même chose que pour la détection et la commande) et, pour augmenter la fiabilité, toutes les alimentations, doivent être connectées à des sources disponibles en permanence (batteries, alimentations non interruptibles)

#### 3.4.1. Alarme

Alarme est un dispositif de sécurité visant à avertir le propriétaire de la mise en danger du lieu où est installée l'alarme. Une alarme est définie comme étant un système de sécurité composé

d'un ensemble d'éléments permettant de détecter un danger potentiel et, de cette manière, d'en prévenir les conséquences. Ces éléments sont généralement constitués de pièces de détection, d'un module de contrôle, d'un clavier et d'un avertisseur. Le but d'un système d'alarme est donc d'envoyer une information grâce à un signal afin de provoquer une réaction (telle qu'une intervention des services de secours, de sécurité, des propriétaires...). Pour cela, une reconnaissance d'une certaine situation comme étant un danger doit pouvoir être effectuée par le système.

### **3.4.2. Electrovanne**

Une électrovanne est un dispositif électromécanique utilisé pour contrôler le débit de fluides tels que l'eau, l'air, le gaz, l'huile et autres fluides dans les systèmes industriels, les machines et les équipements. Elle est composée d'un corps de vanne, d'un actionneur électromagnétique et d'un système de commande électronique.

L'électrovanne fonctionne en utilisant une bobine électromagnétique pour activer un mécanisme de commande qui ouvre ou ferme le passage du fluide à travers la vanne. Lorsque l'électricité est appliquée à la bobine, elle crée un champ magnétique qui déplace un noyau métallique à l'intérieur de l'actionneur, qui est connecté à la tige de la vanne. La tige de la vanne est alors déplacée pour ouvrir ou fermer le passage du fluide à travers la vanne.

Les électrovannes sont couramment utilisées dans les applications industrielles, telles que la régulation de la pression, la régulation du débit, le contrôle du niveau de liquide et la commande de vannes d'arrêt automatiques. Elles sont également utilisées dans les équipements domestiques, tels que les lave-linges et les lave-vaisselles, pour contrôler le débit de l'eau.

Les électrovannes peuvent être commandées manuellement ou automatiquement à l'aide de signaux électriques provenant de capteurs de pression, de débit, de niveau et d'autres types de capteurs.

Elles peuvent également être intégrées à des systèmes de contrôle automatisés pour une régulation précise et efficace du débit de fluide dans les processus industriels.

### **3.4.3. Electrovanne gaz on/off**

L'électrovanne gaz ON/OFF est conçue pour être commandée manuellement ou automatiquement, en fonction des besoins de l'application. Elle est équipée d'une bobine électromagnétique qui, lorsqu'elle est activée, déplace un piston ou un diaphragme à l'intérieur

de la vanne pour ouvrir ou fermer le passage du gaz. Lorsque l'électrovanne est activée, elle permet au gaz de circuler dans le système, et lorsqu'elle est désactivée, elle ferme l'accès au gaz. Ce contrôle précis et rapide permet de maintenir une sécurité élevée en cas de fuite de gaz ou d'autres situations d'urgence.

### **3.5. Description fonctionnement système G&F**

En cas détection d'incendie dans hall d'emplissage par détecteur flamme or par bris de glace

Détection de flamme : Cette fonction est réalisée par un détecteur de flamme qui détecte la présence de flammes ou de chaleur élevée.

Détection de bris de glace : Cette fonction est réalisée par un détecteur de bris de glace qui détecte le bris de vitres par operateur.

Communication de l'alarme : Cette fonction est réalisée par un système d'alarme qui est activé par les détecteurs de flamme et de bris de glace. Le système d'alarme utilise des haut-parleurs et des lumières clignotantes pour avertir les occupants du bâtiment qu'il y a une situation d'urgence.

Le capteur d'incendie détecte la flamme et transmis un message à la centrale de détection G&F (gaz flamme).

Déclenchement des mesures de sécurité : Cette fonction est réalisée par un système de sécurité qui est activé par les détecteurs de flamme et de bris de glace. Le système de sécurité peut inclure des mesures de sécurité telles que fermeture de la vanne gaz et l'ouverture les électrovannes de réseau anti incendie et l'envoi un signal à électropompe pour démarrage et d'une alerte à un service de sécurité ou à un centre de contrôle.

3.6. Analyse fonctionnelle d'un système G&F

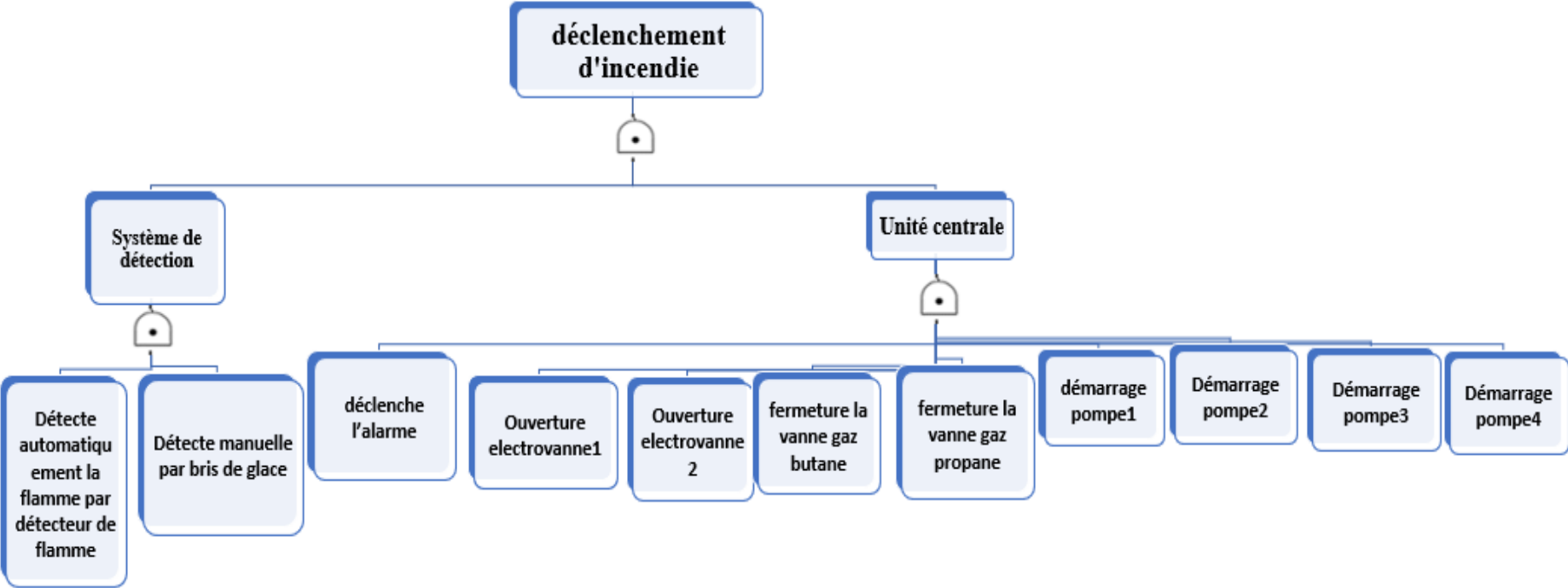


Figure 23: Analyse fonctionnelle d'un système G&F



**Conclusion :**

En conclusion, le système de détection de feu et de gaz est d'une importance cruciale pour la sécurité dans de nombreuses industries et environnements. Il permet de détecter rapidement les départs de feu et les fuites de gaz potentiellement dangereuses, ce qui permet une réaction rapide et efficace pour minimiser les risques et les dommages.

Grâce à des capteurs avancés, des alarmes et des systèmes de contrôle sophistiqués, le système feu & gaz offre une surveillance continue des zones à risque, permettant une détection précoce des situations dangereuses. Cela permet aux opérateurs de prendre des mesures appropriées telles que l'évacuation, l'extinction du feu, la ventilation ou la mise en place de mesures de confinement.

# CHAPITRE 4

## Analyse et recommandations

## Introduction

Dans ce chapitre, une limitation du système étudié est fixe, nous nous intéresserons au hall d'emplissage, nous commencerons par une analyse fonctionnelle puis une identification des risques, ensuite une analyse approfondie en commençant par une HAZOP puis une ADD avec identification du niveau de SIL et intégration des recommandations pour améliorer son niveau.

### 1. Description du hall d'emplissage

Le hall d'emplissage est une zone clé d'un centre emplisseur de bouteilles de gaz. C'est là que les bouteilles sont remplies, contrôlées et préparées pour la distribution.

Voici une description des éléments typiques que l'on peut trouver dans un hall d'emplissage (comme montre dans l'analyse fonctionnelle de la figure 24) :

1. Carrousels de bascules pour l'enfutage des bouteilles butane B13 : Les carrousels sont des structures rotatives comprenant des bascules spécialement conçues pour l'enfutage des bouteilles de gaz butane B13. Ces bascules permettent de transférer le gaz depuis la source d'alimentation vers les bouteilles en toute sécurité.
2. Bascules de remplissage propane sur convoyeur (bouteille P35Kg) : Les bascules de remplissage propane sont utilisées pour remplir les bouteilles de gaz propane de 35 kg. Elles sont généralement situées sur des convoyeurs qui acheminent les bouteilles vers les bascules et les déplacent ensuite vers d'autres zones du hall.
3. Bascule de remplissage propane P11 (bouteille 11Kg propane) : Cette bascule est spécifiquement conçue pour le remplissage des bouteilles de gaz propane de 11 kg. Elle permet de mesurer précisément la quantité de gaz transférée dans chaque bouteille.
4. Bascule pour l'enfutage des bouteilles B03 et B06 à valve : Cette bascule est utilisée pour l'enfutage des bouteilles de gaz butane de 3 kg et 6 kg équipées d'une valve. Elle garantit un remplissage précis et sécurisé de ces bouteilles.
5. Palettiseuses : Les palettiseuses sont des machines automatiques qui empilent les bouteilles remplies sur des palettes de manière ordonnée. Elles permettent de faciliter le stockage et le transport des bouteilles.

6. Convoyeurs d'entrée vide : Ces convoyeurs sont utilisés pour acheminer les bouteilles vides vers les différentes bascules de remplissage. Ils assurent un flux régulier des bouteilles vides vers le processus d'emplissage.

7. Convoyeur de sortie plein : Ce convoyeur transporte les bouteilles remplies depuis les bascules de remplissage vers d'autres zones du hall, telles que la zone de palettisation ou le stockage temporaire avant la distribution.

8. Détecteur de fuite : Un détecteur de fuite est installé dans le hall d'emplissage pour détecter toute fuite de gaz qui pourrait survenir pendant le processus de remplissage. Il déclenche des alarmes en cas de détection de fuite, ce qui permet de prendre rapidement des mesures pour éviter les risques potentiels.

9. Bascule de pré-pesée et de contrôle de poids : Ces bascules sont utilisées pour mesurer le poids des bouteilles avant et après le remplissage afin de garantir le respect des normes de remplissage et d'assurer la qualité des produits.

10. Cabine de peinture : Cette cabine est utilisée pour appliquer des revêtements de peinture protecteurs sur les bouteilles, notamment pour les identifier visuellement et les protéger contre la corrosion.

11. Bons d'essai pour le test hydrostatique des bouteilles B13 et un autre pour le P35 et le robinet : Ces bons d'essai sont utilisés pour enregistrer les résultats des tests hydrostatiques effectués sur les bouteilles de gaz butane B13, les bouteilles de propane P35 et les robinets, afin de s'assurer de leur conformité aux normes de sécurité.

Ces différents éléments du hall d'emplissage travaillent ensemble pour assurer un processus de remplissage sûr, précis et efficace des bouteilles de gaz, en veillant à la qualité des produits et à la sécurité des opérateurs et de l'environnement.

1.1. L'analyse fonctionnelle d'un hall d'emplissage des bouteilles

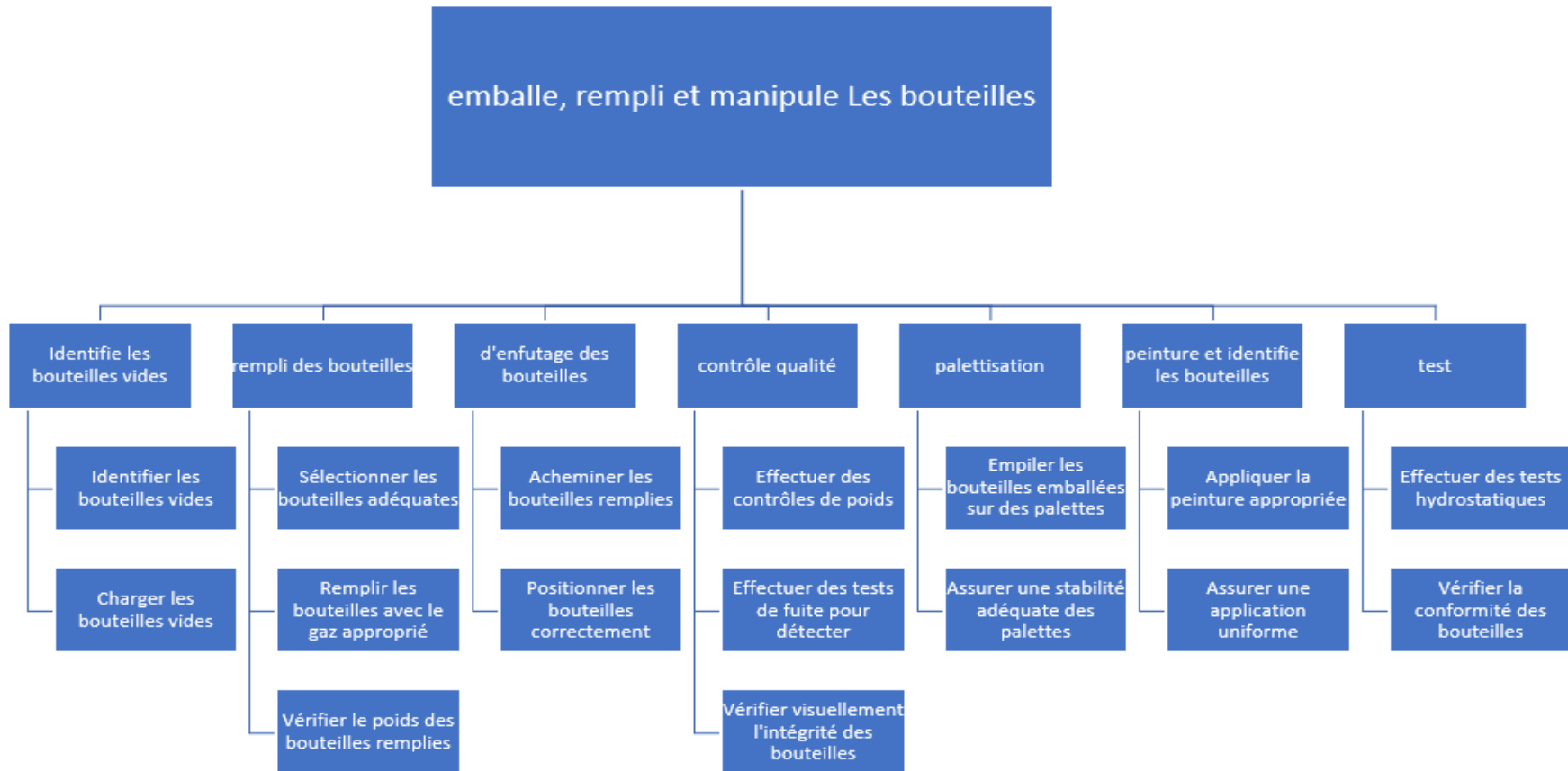


Figure 24: analyse fonctionnelle de hall d'emplissage des bouteilles de gaz

1.2. PID butane d'un hall d'emplissage

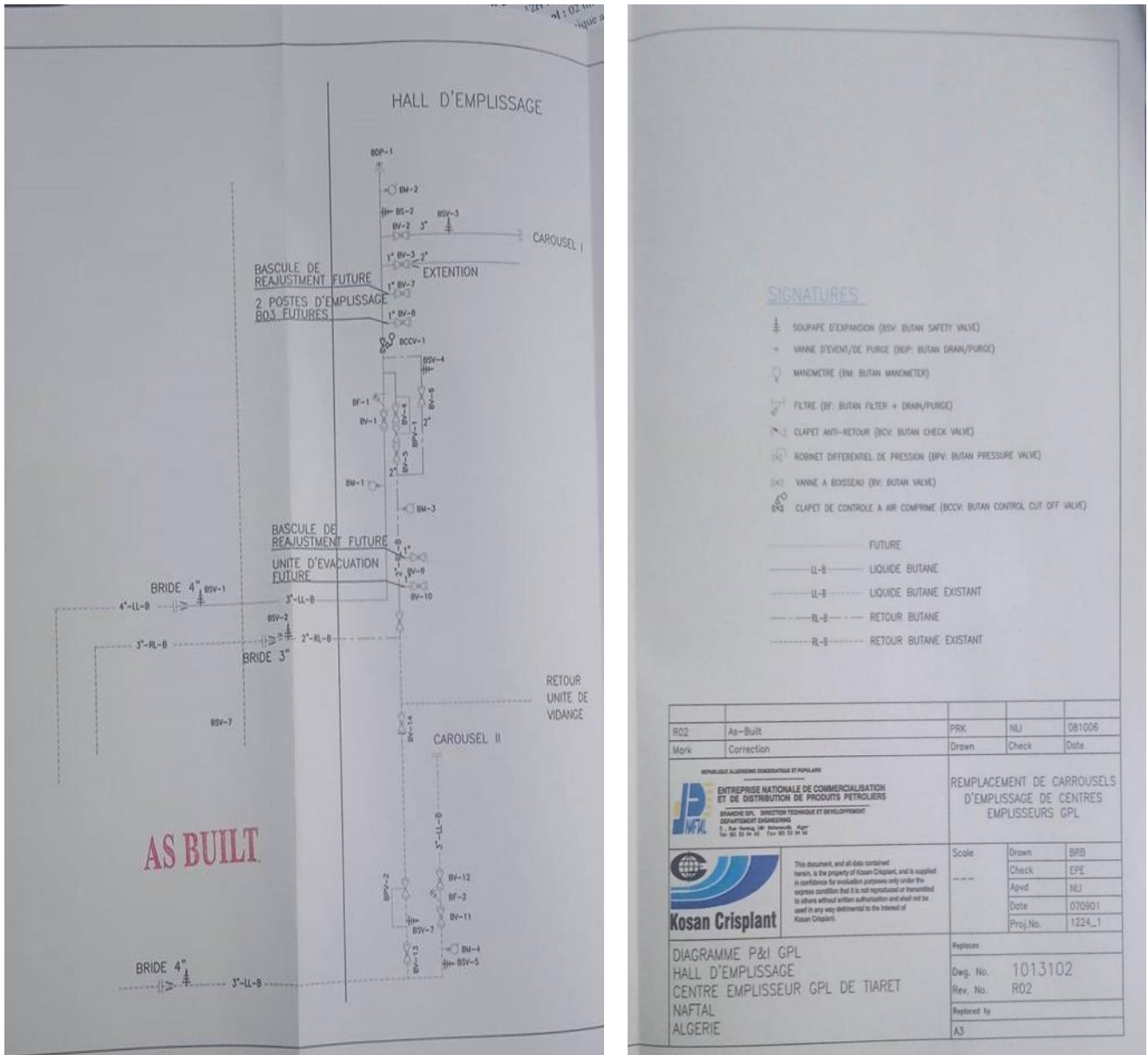


Figure 25: Schéma PID butane du hall d'emplissage des bouteilles de gaz

1.3. Configuration de système G&F étudié dans hall d’emplissage

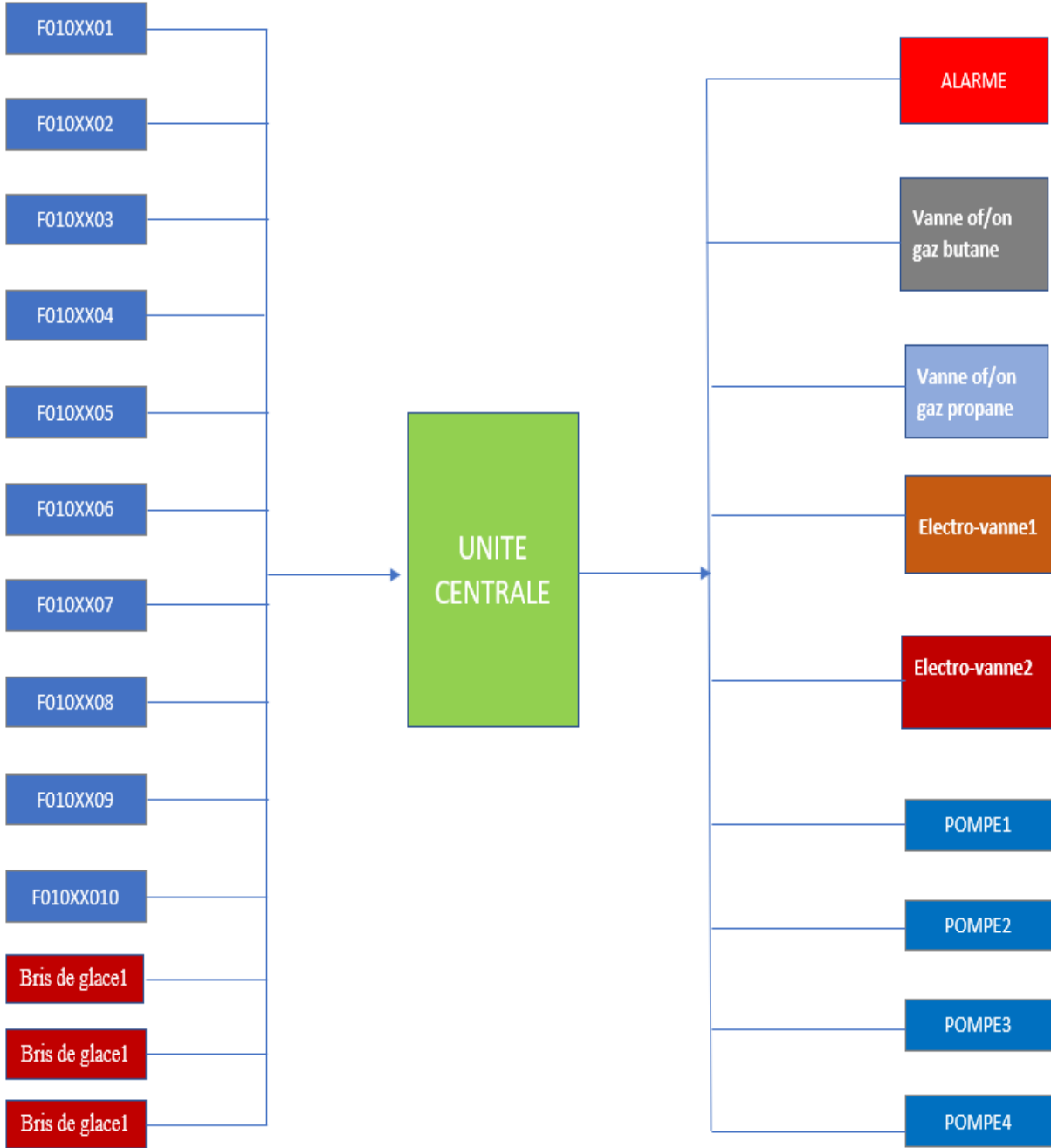


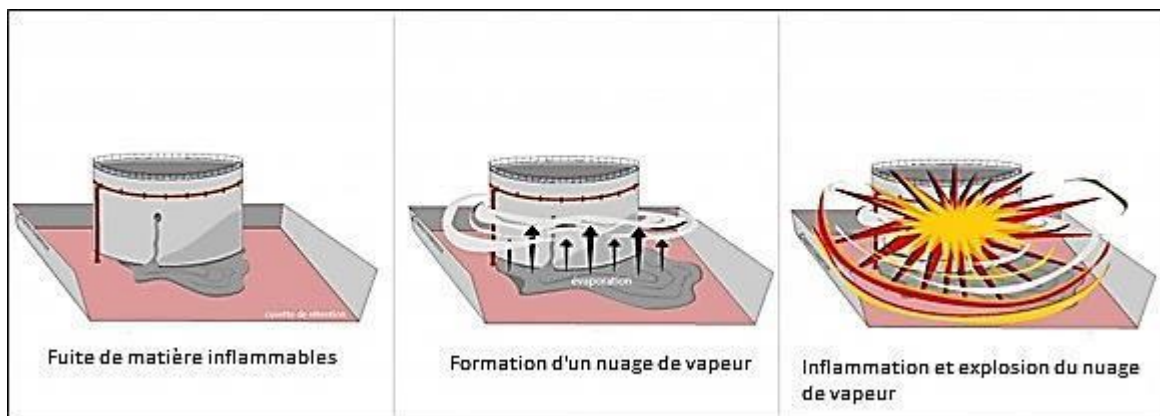
Figure 26: Configuration de système G&F étudié dans hall d emplissage

#### 1.4. Risques et dangers au niveau du centre emplisseur 141 GPL Tiaret

**Risque d'explosion et d'incendie :** Les bouteilles de gaz contiennent des substances inflammables et peuvent provoquer des explosions ou des incendies en cas de fuite, d'étincelle ou d'ignition accidentelle.

**UCVE :** c'est l'explosion d'un nuage de gaz en milieu non confiné (cas de l'accident de Flixborough, en 1947, 28 morts).

Suite à une fuite de gaz inflammable, le mélange du gaz et de l'air forme un nuage qui, en rencontrant une source d'inflammation, peut exploser. Les effets sont essentiellement des effets de pression.



**Figure 27: les différentes phases de développement d'un UVCE**

**BLEVE :** est un type d'explosion provoqué par une augmentation brutale de la pression à l'intérieur d'un réservoir, à la suite d'un dégagement de vapeur par un liquide en ébullition (vaporisation non contrôlée). Le gaz cherche alors à s'échapper rapidement du réservoir, mais n'y parvient pas, ce qui conduit au phénomène d'ébullition-explosion. Ce phénomène particulièrement dangereux dépasse ordinairement les effets d'une déflagration. L'augmentation brutale de la pression à l'intérieur du réservoir peut être causée soit par l'exposition du réservoir à une source de chaleur externe, comme un incendie (BLEVE à chaud), soit par une défaillance du réservoir (BLEVE à froid). Le BLEVE à froid peut avoir plusieurs origines :

- Une soupape de sécurité défectueuse empêchant le surplus de pression de sortir ;
- Une fragilisation de la structure du réservoir : des fissures peuvent se former à la suite de l'apparition de corrosion ou d'une déformation causée par un choc.



**Fuites de gaz :** Les fuites de gaz peuvent entraîner une accumulation de gaz dans l'air, augmentant ainsi le risque d'incendie, d'explosion ou d'asphyxie pour le personnel travaillant dans la zone.

**Manipulation incorrecte des bouteilles :** Une manipulation incorrecte des bouteilles de gaz, notamment lors du chargement, du déchargement ou du déplacement, peut provoquer des chutes, des renversements ou des collisions, entraînant des blessures pour les travailleurs ou des dommages matériels.

**Poids excessif des bouteilles :** Les bouteilles de gaz peuvent être lourdes lorsqu'elles sont remplies, ce qui peut entraîner des blessures musculaires ou des troubles musculosquelettiques si elles sont soulevées ou manipulées de manière incorrecte.

**Risques chimiques :** Les gaz comprimés ou liquéfiés utilisés dans le processus de remplissage des bouteilles peuvent cause

**1. Effets sur la santé :** L'inhalation de propane ou de butane en concentrations élevées peut provoquer des effets nocifs sur la santé. Ces effets peuvent inclure des irritations des voies respiratoires, des étourdissements, des maux de tête, des nausées, voire des pertes de conscience dans les cas graves.

**2. Asphyxie :** Les gaz propane et butane peuvent remplacer l'oxygène dans un espace clos, créant un risque d'asphyxie si la concentration d'oxygène devient trop basse pour maintenir la respiration normale.

**Ventilation inadéquate :** Une mauvaise ventilation dans le hall d'emballage peut entraîner une accumulation de gaz, de vapeurs ou de poussières potentiellement dangereuses, augmentant ainsi le risque d'incendie, d'explosion ou de problèmes respiratoires.

**Défaillance des équipements :** Les défaillances des équipements tels que les carrousels, les bascules, les convoyeurs ou les détecteurs de fuite peuvent entraîner des accidents ou des dysfonctionnements qui compromettent la sécurité des travailleurs et la qualité du processus de remplissage.

**Risques électriques :** La présence d'équipements électriques dans le hall d'emballage accroît le risque d'électrocution ou de court-circuit, notamment en cas de contact avec l'humidité ou les liquides.

## 2. Analyse HAZOP

L'analyse HAZOP (Hazard and Operability Study) est une méthode systématique utilisée pour identifier, évaluer et gérer les risques potentiels associés à un système, un processus ou une installation. Dans le cas du hall d'emballage d'un centre emplisseur de bouteilles de gaz, l'application de la méthode HAZOP permettrait de passer en revue de manière approfondie chaque élément et chaque étape du processus pour identifier les dangers potentiels, les défaillances opérationnelles et les situations anormales qui pourraient causer des accidents ou des incidents.

Voici comment une analyse HAZOP pourrait être appliquée au hall d'emplissage (HAZOP - A Systematic Approach to Identify and Assess Process Hazard):

1. Établissement de l'équipe HAZOP : Une équipe multidisciplinaire composée d'experts en sécurité, en ingénierie, en opérations et en maintenance serait formée pour mener l'analyse HAZOP.
2. Identification des nœuds : Chaque équipement et chaque étape du processus du hall d'emballage serait identifié et défini comme un nœud dans l'analyse HAZOP. Cela inclurait les carrousels de bascules, les bascules de remplissage, les palettiseuses, les convoyeurs, les détecteurs de fuite, les bascules de pré-pesée, etc.
3. Définition des paramètres : Pour chaque nœud, les paramètres pertinents seraient identifiés, tels que la pression, la température, le débit, le niveau, le poids, la vitesse, etc. Ces paramètres décrivent les conditions normales de fonctionnement du système.
4. Création des mot clé : Des mots clés standardisés seraient utilisés pour guider l'équipe HAZOP dans la recherche de déviations potentielles par rapport aux conditions normales. Les mot clé comprennent des termes tels que "plus", "moins", "pas de", "trop", "partiel", "dévié", "en retard", etc.
5. Exploration des déviations potentielles : Pour chaque nœud et chaque paramètre, l'équipe HAZOP examinerait les combinaisons de mots clés pour identifier les déviations potentielles. Par exemple, "plus de pression", "moins de débit", "pas de contrôle de poids", "trop de remplissage", etc.
6. Évaluation des conséquences : Pour chaque déviation identifiée, les conséquences potentielles seraient évaluées en termes de sécurité, d'environnement, de santé et de production.

Cela comprendrait l'identification des risques d'incendie, d'explosion, de fuite de gaz, de blessures, de dommages matériels, etc.

7. Proposition de mesures de prévention et de protection : Pour chaque déviation et ses conséquences, des mesures de prévention, de protection ou de réduction des risques seraient proposés. Cela pourrait inclure des modifications de conception, l'ajout de systèmes de sécurité, l'amélioration des procédures opérationnelles, l'utilisation d'EPI, la formation du personnel, etc.

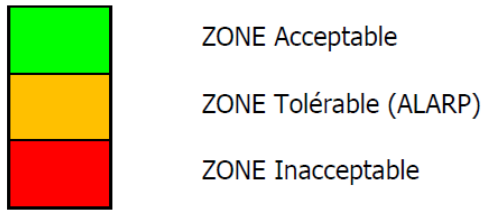
8. Documentation des résultats : Les résultats de l'analyse HAZOP, y compris les déviations identifiées.

### 2.1. Matrice de risque

Suite à cette analyse, la matrice des risques est définie :

<b>Severity</b>	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	10
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		<b>Likelihood</b>				

Figure 28: les événements distingués dans l'HAZOP sont répertoriés dans la matrice des risques



### **Zone acceptable**

La signification de "acceptable" dans ce contexte est que l'on considère la probabilité de décès comme raisonnable et que l'on n'entreprend pas d'efforts supplémentaires pour la réduire davantage. Cela implique que la probabilité de létalité est jugée acceptable et ne nécessite pas de mesures supplémentaires pour la diminuer.

### **Zone Tolérable (ALARP)**

Signifie accepter un niveau de risque spécifique tout en réévaluant les causes et les mesures préventives pour les réduire. Cela indique la conscience que le risque actuel peut être diminué. On accepte donc de vivre avec un certain niveau de risque, mais on s'engage à prendre des mesures pour le minimiser autant que possible. Cela nécessite une réflexion continue sur les facteurs de risque, l'identification de mesures supplémentaires et la mise en œuvre de solutions appropriées pour réduire les risques à un niveau jugé raisonnable et praticable.

### **Zone Inacceptable**

Signifie qu'on ne peut pas accepter le niveau de risque associé à une activité donnée. Cela implique qu'on refuse de participer à cette activité et qu'on n'autorise pas les autres personnes à poursuivre un processus qui présente un tel risque. Cette classification indique que le niveau de risque est jugé inacceptable, qu'il dépasse les seuils de tolérance ou les normes de sécurité établies. Par conséquent, des mesures doivent être prises pour réduire le risque à un niveau acceptable avant de poursuivre l'activité ou d'autoriser son fonctionnement.

2.2. Tableau HAZOP

Nous avons utilisé logiciel PHA-8-pro pour élaborer la méthode HAZOP

Tableau 11: Tableau HAZOP

Node: 1. hall d'emplissage

Déviations: 1. plus de débit

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination										
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. la vanne de gaz bloquée ouverte	1. Augmentation de pression	2	2	4	1. indication de pression	1. système de détection de débit anormal	2	1	2	1. système de détection de débit anormal	Rec	Minor	Low	1	c	Min	Low	1	c
	2. Fuite continue de gaz inflammable	2	4	8	2. plan d'urgence		2	2	4	2. système de détection de débit anormal	Rec	Serious	Medium	1	SIL 2	Min	Medium	2	c

Node: 1. hall d emplissage

Déviatiion: 1. plus de débit

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination										
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final				
												S	L	PLs	SIL	S	L	PLs	SIL	
	3. Risque d'incendie	4	3	12	3. rideau d'eau		4	2	8	3. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1	
	4. Risque d'explosion	4	3	12	4. réseau anti incendie	4	2	8												
	5. Risque d'asphyxie	3	3	9	5. 1. Système détection feu & gaz	3	2	6												
2. Une erreur de l'opérateur lors du processus remplissage	1. Impact sur l'environnement	2	2	4	1. 1. Système détection feu & gaz	2. formation du personnel	2	1	2	1.										
	2. Dommages matériels	3	3	9	2. réseau anti incendie		2	2	4	2.										

Node: 1. hall d emplissage

Déviatiion: 1. plus de débit

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination											
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final				
												S	L	PLs	SIL	S	L	PLs	SIL	
	3. Risque d'incendie	4	3	12			4	2	8	3. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1	
	4. Risque d'explosion	4	3	12			4	2	8	4. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1	
	5. Blessures corporelles	2	3	6			2	2	4	5.										
	6. Fuite de gaz	2	4	8			2	2	4	6. Système détection feu & gaz	Ext	Serious	Medium	2	SIL 1	Serious	Medium	2	SIL 1	

Node: 1. hall d emplissage

Déviatiion: 2. moins de débit

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination										
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. la vanne de gaz bloque ferme	1. Arrêt du processus de remplissage	3	2	6	1. Procédures d'inspection et d'entretien	3	1	3											
	2. Perturbations opérationnelles	3	2	6		4. surveillance continue	3	1	3										
						2. formation du personnel													
2. défaillance compresseur	1. Retards de production	3	2	6	1. Procédures d'inspection et d'entretien	3	1	3											
	2. Coûts de réparation	3	2	6		6. compresseurs de secours	3	1	3										



Node: 1. hall d emplissage

Déviatio: 2. moins de débit

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination											
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final				
												S	L	PLs	SIL	S	L	PLs	SIL	
3. défaillance de pompe	1. Retards de production	3	2	6	1. Procédures d'inspection et d'entretien	3	1	3												
	2. Coûts de réparation	3	2	6		7. pompes de secours	3	1	3											
4. Obstruction majeure du système (les tuyaux, les vannes ou les raccords)	1. Fuite de gaz	2	4	8	1. Procédures d'inspection et d'entretien	2	2	4	1. Système détection feu & gaz	Ext	Serious	Medium	2	SIL 1	Extensive	Medium	3	SIL 1		
	2. Risque d'explosion	4	3	12		8. plan d'urgence	4	2	8	2. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1	

Node: 1. hall d emplissage

Déviatiion: 2. moins de débit

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination										
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
	3. Risque d'incendie	4	3	12			4	2	8	3. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	4. Arrêt du processus de remplissage	3	2	6			3	1	3	4.									

Node: 1. hall d'emplissage

Déviatiion: 3. haute de température

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. Surcharge électrique	1. Risque d'incendie	4	3	12	1. Procédures d'inspection et d'entretien	9. protection contre les surcharges électriques	4	2	8	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	2. Risque d'explosion	4	3	12			5. maintenance préventive	2. Système détection feu & gaz	4	2	8	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2
	3. Perturbations opérationnelles	3	2	6	3	1			3										
	4. dommages aux installations	3	2	6	3	1	3												

Node: 1. hall d'emplissage

Déviaton: 3. haute de température

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	R R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
2. Activités de production intensives	1. Erreurs de remplissage ou de manipulation	3	2	6	1. système de refroidissement	10. ventilation et circulation de l'air	3	1	3										
	2. Pression sur les équipements	3	2	6		11. planification des activités	3	1	3										
	3. Augmentation du risque d'accidents incendie explosions	4	3	12				4	2	8									
	4. Augmentation des délais de production	2	4	8				2	2	4									

Node: 1. hall d'emplissage

Déviation: 3. haute de température

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
3. défaillance de système de refroidissement	1. Augmentation de la température	3	2	6	1. Procédures d'inspection et d'entretien	12. assistance technique	3	1	3										
	2. Détérioration des produits	3	2	6		13. arrêt d'urgence	3	2	6										
	3. Pannes d'équipements	3	3	9		3	2	6											
4. augmentation de la température ambiante	1. Risque accru d'incendie	4	3	12	1. système de refroidissement	10. ventilation et circulation de l'air	4	2	8	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	2. Risque d'explosion	4	3	12			4	2	8	2. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1

Node: 1. hall d emplissage

Déviatiion: 3. haute de température

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination													
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final						
												S	L	PLs	SIL	S	L	PLs	SIL			
	3. Détérioration des bouteilles de gaz	4	3	12			4	2	8	3.												
	4. Perturbation des opérations	3	2	6			3	2	6	4.												

Node: 1. hall d emplissage

Déviatiion: 4. basse de température

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	R R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. diminution température ambiante																			

Node: 1. hall d emplissage

Déviation: 5. haute de pression

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. Blocage ou restriction des tuyaux ou des conduites	1. Risque d'explosion	3	4	12	1. 1. Système de détection feu & gaz 2. système de pression	8. plan d'urgence	4	2	8	1. 1. Système de détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	2. Fuite de gaz	3	3	9			3	2	6										
	3. Impact sur la qualité des produits	3	2	6			3	2	6										
	4. Endommagement des équipements	3	3	9			3	2	6										
2. Problèmes liés aux compresseurs	1. Retards de production	3	2	6		5. maintenance préventive	3	2	6		Ext	Serious	Medium	2	SIL 1	Serious	Low	2	2



CHAPITRE 4

Analyse et recommandations

Node: 1. hall d emplissage

Déviation: 5. haute de pression

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination														
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final							
												S	L	PLs	SIL	S	L	PLs	SIL				
	2. Fuite de gaz	3	3	9	1. Procédures d'inspection et d'entretien	6. compresseurs de secours	3	2	6	1.1. Système détection feu & gaz													
3. Erreur de manipulation des vannes	1. Fuite de gaz	3	3	9		2. formation du personnel	3	2	6	1. Système détection feu & gaz	Ext	Serious	Medium	2	SIL 1	Serious	Low	2	c				
	2. Risque d'asphyxie	3	3	9			3	2	6	2. Système détection feu & gaz	Ext	Serious	Low	2	c	Serious	Low	2	c				
	3. Risque d'incendie	4	3	12			4	2	8	3. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1				

Node: 1. hall d emplissage

Déviatio: 5. haute de pression

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination										
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
	4. Risque d'explosion	4	3	12			4	2	8	4. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
4. défaillance de système de refroidissement	1. Risque accru d'incendie	3	4	12	1. Procédures d'inspection et d'entretien	5. maintenance préventive	4	2	8	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	2. Risque d'explosion	3	4	12		12. assistance technique	4	2	8	2. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	3. Impact sur la productivité	3	2	6		13. arrêt d'urgence	3	2	6	3.									

Node: 1. hall d'emplissage

Déviations: 5. haute de pression

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination												
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final					
												S	L	PLs	SIL	S	L	PLs	SIL		
	4. Risque de dommages matériels	3	2	6			3	2	6	4.											
5. augmentation de la température ambiante	1. Risque accru d'incendie	3	4	12	1. système de refroidissement	10. ventilation et circulation de l'air	4	2	8	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1		
	2. Risque d'explosion	3	4	12			14. maintenance préventive système de refroidissement	4	2	8	2. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1	
	3. Détérioration des bouteilles de gaz	3	4	12			ent	3	2	6	3.										

Node: 1. hall d emplissage

Déviatiion: 5. haute de pression

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
	4. Perturbation des opérations	3	2	6			3	2	6	4.									

Node: 1. hall d emplissage

Déviation: 6. basse de pression

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	R R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. Problème avec les compresseurs	1. Arrêt du processus de remplissage	3	3	9	1. Procédures d'inspection et d'entretien	6. compresseurs et de secours	3	2	6										
	2. Perte d'alimentation du carrousel et perte de production	4	2	8			3	2	6										
2. Obstruction dans le système (tuyaux filtres)	1. Risque d'incendie	4	3	12	1. Procédures d'inspection et d'entretien	8. plan d'urgence	4	2	8	1. 1. Système de détection feu & gaz	Ext	Extens ive	Medium	2	SIL 2	Ext ensi ve	Low	2	SIL 1

Node: 1. hall d emplissage

Déviati on: 6. basse de pression

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination										
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
	2. Risque d'explosion	4	3	12			4	2	8	2.1. Système de détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	3. Arrêt du processus de remplissage	3	3	9			3	2	6	3.									
	4. Fuite de gaz	3	4	12			3	2	6	4.1. Système de détection feu & gaz	Ext	Serious	Medium	2	SIL 1	Serious	Low	2	2
3. Problèmes liés aux compresseurs	1. Perte d'alimentation	3	3	9		6. compresseurs de secours	3	2	6										

Node: 1. hall d emplissage

Déviatiion: 6. basse de pression

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination										
		S	L	RR			S	L	R R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final				
												S	L	PLs	SIL	S	L	PLs	SIL	
	du carrousel et perte de production				1. Procédures d'inspection et d'entretien	5. maintenance préventive														
4. la vanne de gaz bloque semi fermée	1. Débit d'alimentation du carrousel insuffisant et baisse de production	3	3	9	1. Procédures d'inspection et d'entretien		3	2	6											

CHAPITRE 4

Analyse et recommandations

Node: 1. hall d emplissage

Déviatiion: 7. fuite

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. apparition de brèche due à l'effet de la corrosion	1. formation d'un nuage UVCE	4	2	8	1. réseau anti incendie	4	1	4	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1	
	2. Flash Fire	4	2	8	2. réseau anti incendie	4	1	4											
	3. Risque d'explosion	4	3	12	3. Système détection feu & gaz	4	2	8											
2. robinet, joint d'étanchéité défectueux	1. formation d'un nuage UVCE	4	2	8	1. réseau anti incendie	4	1	4	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1	
	2. Flash Fire	4	2	8	2. réseau anti incendie	4	1	4											
	3. Risque d'explosion	4	3	12	3. Système détection feu & gaz	4	2	8											



Node: 1. hall d emplissage

Déviatio: 8. chute d'une Platte

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination										
		S	L	RR			S	L	RR	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. erreur humain	1. Fuite de gaz	3	3	9		2. formation du personnel	3	2	6	1. Système détection feu & gaz	Ext	Seriou	Medium	2	SIL 1	Seriou	Low	2	c
	2. Risque d'explosion	3	4	12			4	2	8	2. Système détection feu & gaz	Ext	Extens	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	3. Risque d'incendie	3	4	12			4	2	8	3. Système détection feu & gaz	Ext	Extens	Medium	2	SIL 2	Extensive	Low	2	SIL 1
2. défaillance engin de levage	1. Fuite de gaz	3	3	9	1. Procédures d'inspection et d'entretien	5. maintenance préventive	4	2	8	1. Système détection feu & gaz	Ext	Seriou	Medium	2	SIL 1	Extensive	Low	2	SIL 1

Node: 1. hall d'emplissage

Déviations: 8. chute d'une Platte

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination										
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
	2. Risque d'incendie	4	3	12			4	2	8	2. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	3. Risque d'explosion	4	3	12			4	2	8	3. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1

Node: 1. hall d emplissage

Déviation: 9. rupture catastrophique d'une bouteille lors de l'emplissage

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction		SIL détermination										
		S	L	RR			S	L	R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
1. malveillance	1. Risque d'explosion (boule de feu)	4	2	8	1. rideau d'eau	2. formation du personnel	3	2	6	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	2. BLEVE froid	4	2	8	2. réseau anti incendie		3	2	6										
2. choc mécanique	1. Risque d'explosion (boule de feu)	4	2	8	1. rideau d'eau	8. plan d'urgence	3	2	6	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	2. BLEVE froid	4	2	8	2. réseau anti incendie		3	2	6										
3. forte source de chaleur	1. Risque d'explosion (boule de feu)	4	2	8	1. rideau d'eau	10. ventilation et circulation de l'air	3	2	6	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1

Node: 1. hall d emplissage

Déviatiion: 9. rupture catastrophique d'une bouteille lors de l'emplissage

Causes	Conséquences	Before Risk Reduction			Safeguards	Recommandations	After Risk Reduction			SIL détermination									
		S	L	RR			S	L	R R	SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
												S	L	PLs	SIL	S	L	PLs	SIL
	2. BLEVE froid	4	2	8	2. réseau anti incendie		3	2	6										
4. forte onde de choc	1. Risque d'explosion (boule de feu)	4	2	8	1. rideau d'eau	8. plan d'urgence	3	2	6	1. Système détection feu & gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Low	2	SIL 1
	2. BLEVE froid	4	2	8	2. réseau anti incendie		3	2	6										

### 2.3. Interprétation des résultats

D'après les résultats du tableau HAZOP on a obtenu :

- cinq évènements inacceptables
- dix-huit évènements en zone ALARP
- deux évènements acceptables

Les évènements inacceptables représentent des lacunes considérables pour notre système et ils sont en priorité pour réduire vers une échelle plus basse ou en constate que risque incendie ont une grande probabilité d'occurrence.

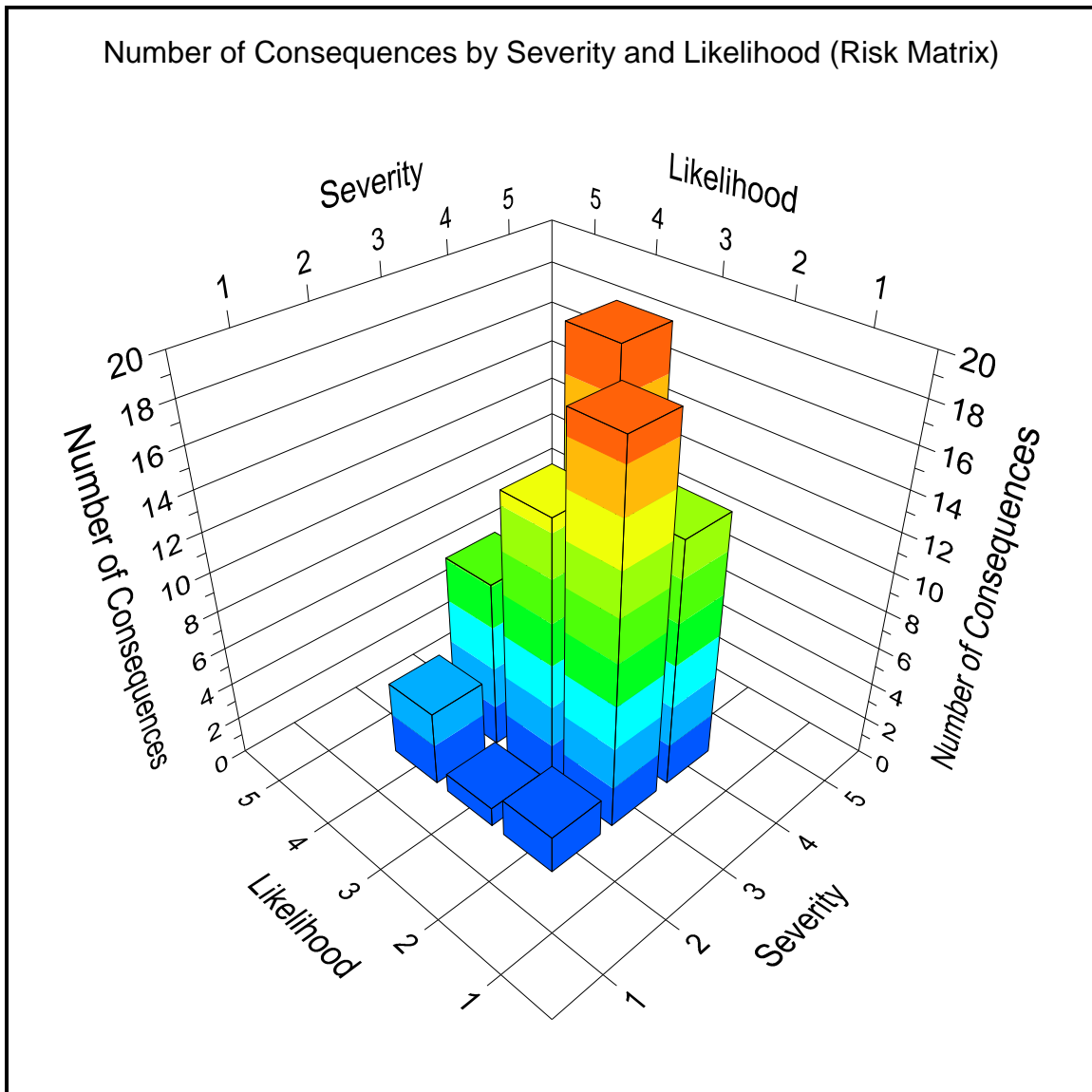


Figure 29: Graphe nombre de conséquences en fonction de la gravité et de la probabilité

## 2.4. Résultats de l'allocation de niveau d'intégrité de sécurité « SIL » par graphe de risque

Parmi les approches qualitatives nous avons utilisé le **graphe de risque** intégré avec la méthode d'analyse **HAZOP**. Cette méthode consiste évaluer les différents scénarios d'accidents selon le graphe de risque.

En prend par exemple le cas risque incendie au niveau du hall le SIF définie est système de détection de flamme comme résultat avant la mise en place des barrières est de **SIL 2**.

## 3. Arbre de défaillance :

### 3.1. Présentation arbre de défaillance

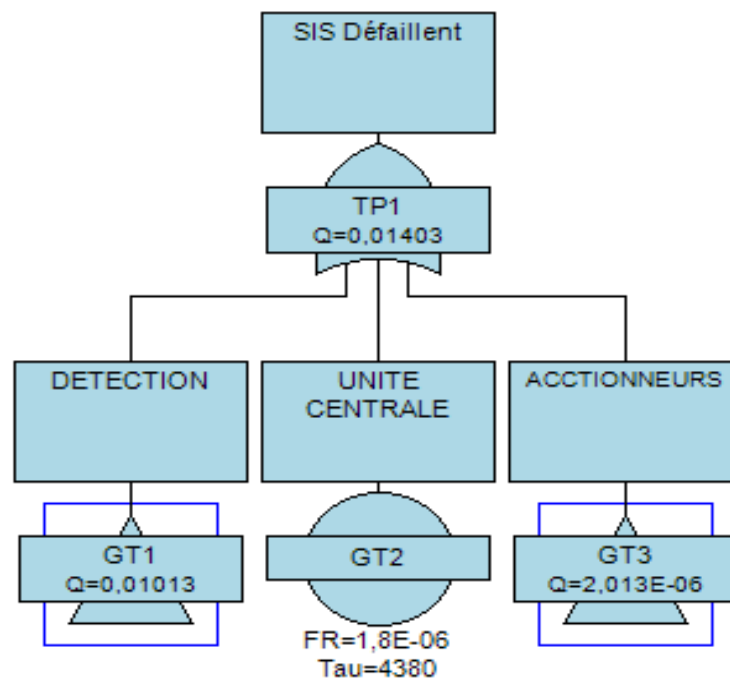
Un arbre de défaillance, également connu sous le nom de diagramme d'arbre de défaillance (FBD - Fault Tree Diagram), est un outil de modélisation utilisé pour analyser les causes potentielles d'une défaillance ou d'un accident. On utilise logiciel iso graph (reability workbench) pour trace arbre de défaillance

Pour créer un arbre de défaillance, On peut suivre les étapes suivantes :

1. Identifier l'événement de défaillance principal : Déterminer l'événement où le système d'instrument de sécurité défaille en cas d'incendie.
2. Identifier les causes principales.
3. Créer le diagramme : Dessiner un diagramme à partir de l'événement de défaillance principal en utilisant des portes logiques pour représenter les relations entre les causes. Les portes logiques couramment utilisées sont "ET" (pour représenter une conjonction de causes) et "OU" (pour représenter une disjonction de causes).
4. Ajouter des détails : Pour chaque cause principale, on peut continuer à décomposer les causes en causes secondaires, et ainsi de suite, pour obtenir une représentation plus détaillée des relations de cause à effet.
5. Analyser l'arbre de défaillance : Une fois que l'arbre de défaillance est construit, on peut l'analyser pour évaluer les probabilités de défaillance.
6. Tracer l'arbre de défaillance et calculer la probabilité de défaillance du système dans les 4 cas.on choisit durée de vie du système 15 ans (129600 heures),les sources des données utilisées

dans le calculs est la base de données SINTF( reability data safety instrumented systems ) et NRPD 2016 (Nonelectronic parts reliability data publication) ,voici les résultats :

### 3.1.1. Calcule la probabilité de défaillance SIS par utilisation $\lambda_{DD}$ taux de défaillance aléatoire dangereuse du matériel détectable .



**Figure 30 L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda_{DD}$  -partie1**

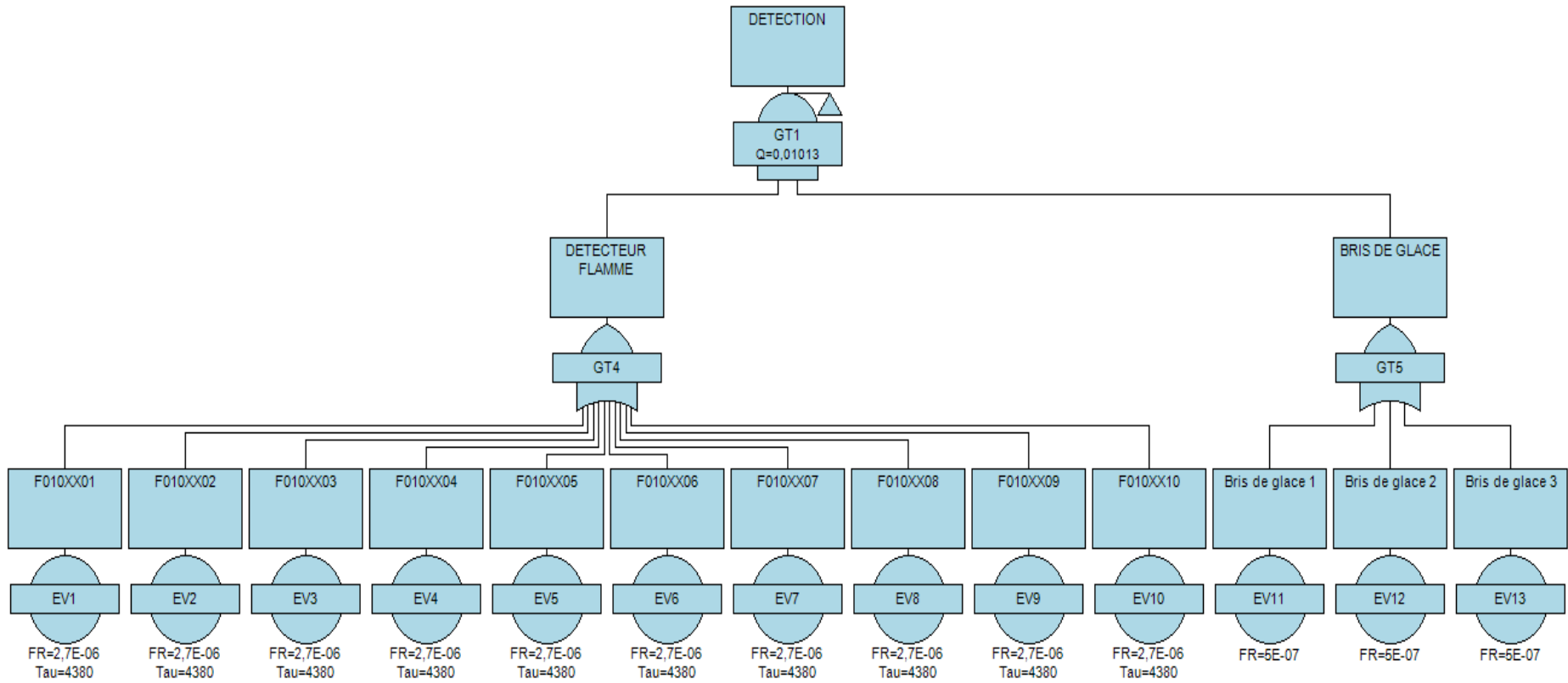


Figure 31 : L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda$ DD -partie2



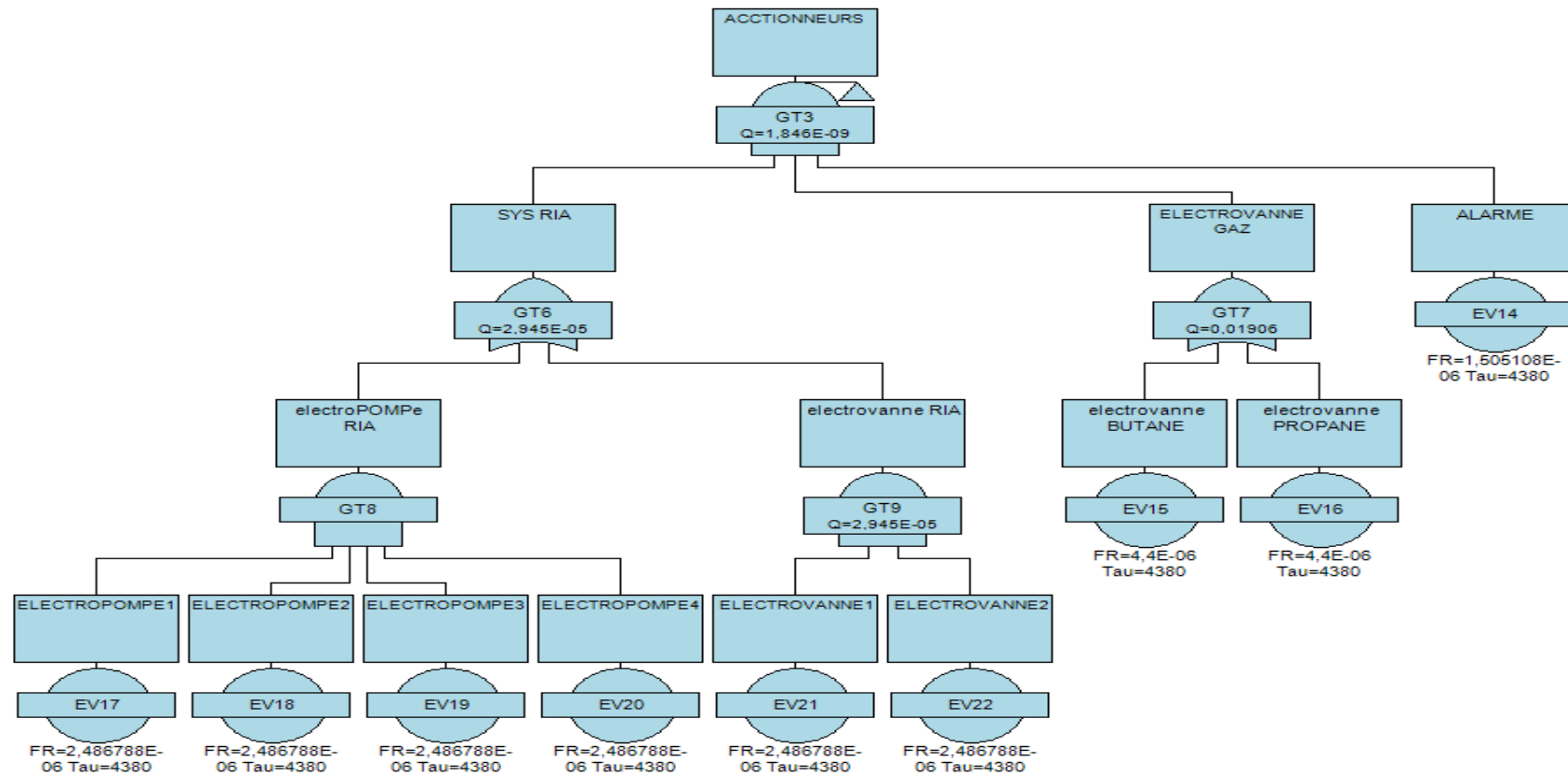
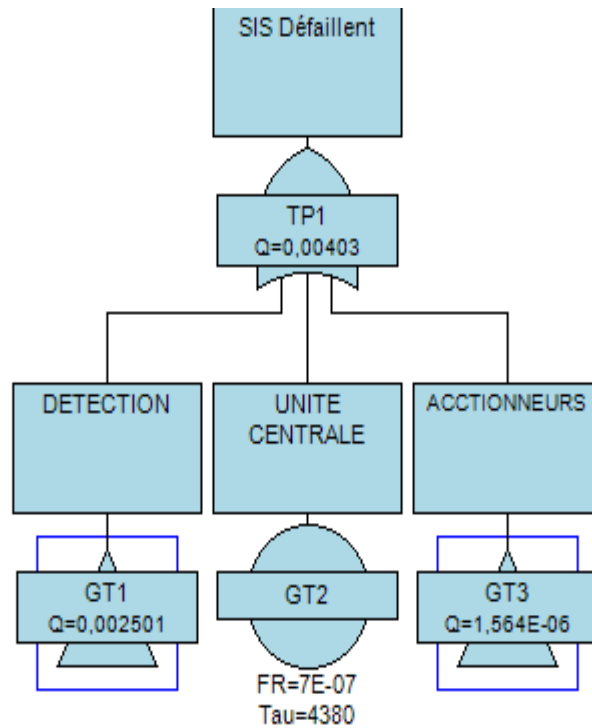


Figure 32 : L’arbre des défaillances du système instrument de sécurité par utilisation λDD -partie3

PFDmax=0,01403

D’après ces résultats on trouve que le niveau de SIL réel de ce système instrumenté de sécurité est le **SIL 2**.

**3.1.2 Calcule la probabilité de défaillance SIS par utilisation  $\lambda_{DU}$  taux de défaillance aléatoire dangereuse des matériels indétectables.**



**Figure 33 : L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda_{DU}$  -partie1**

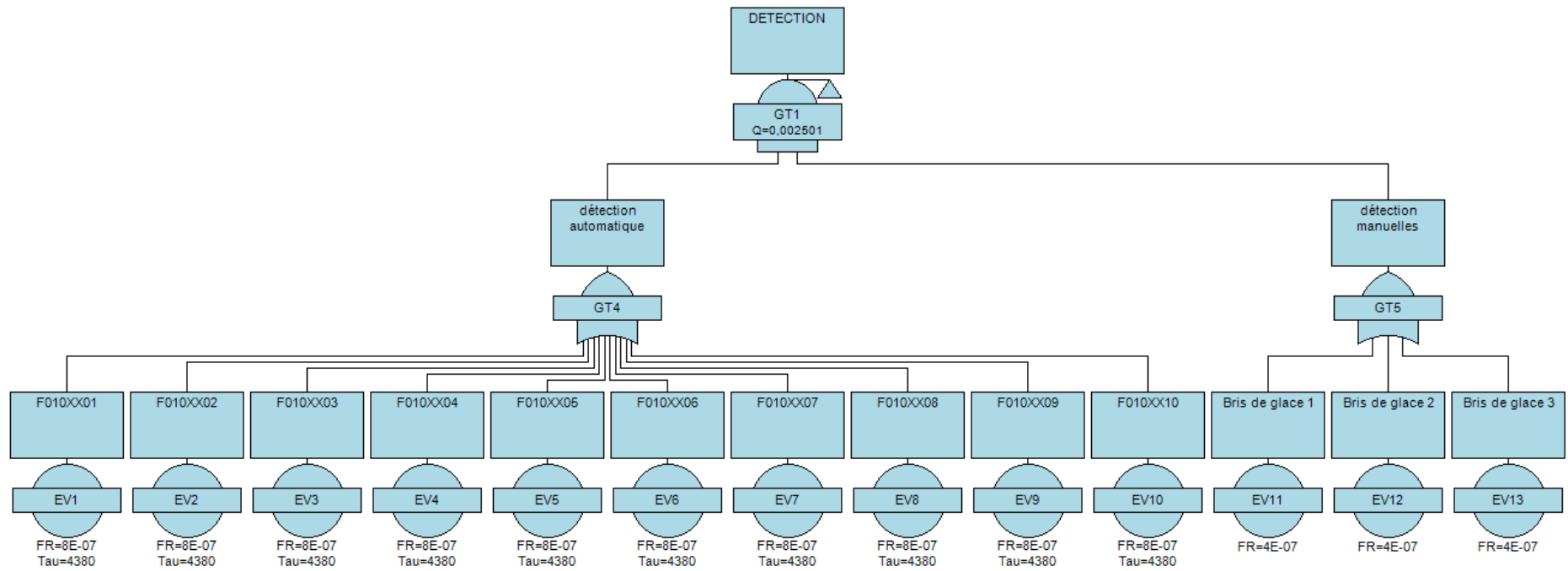


Figure 34 : L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda_{DU}$ - partie2

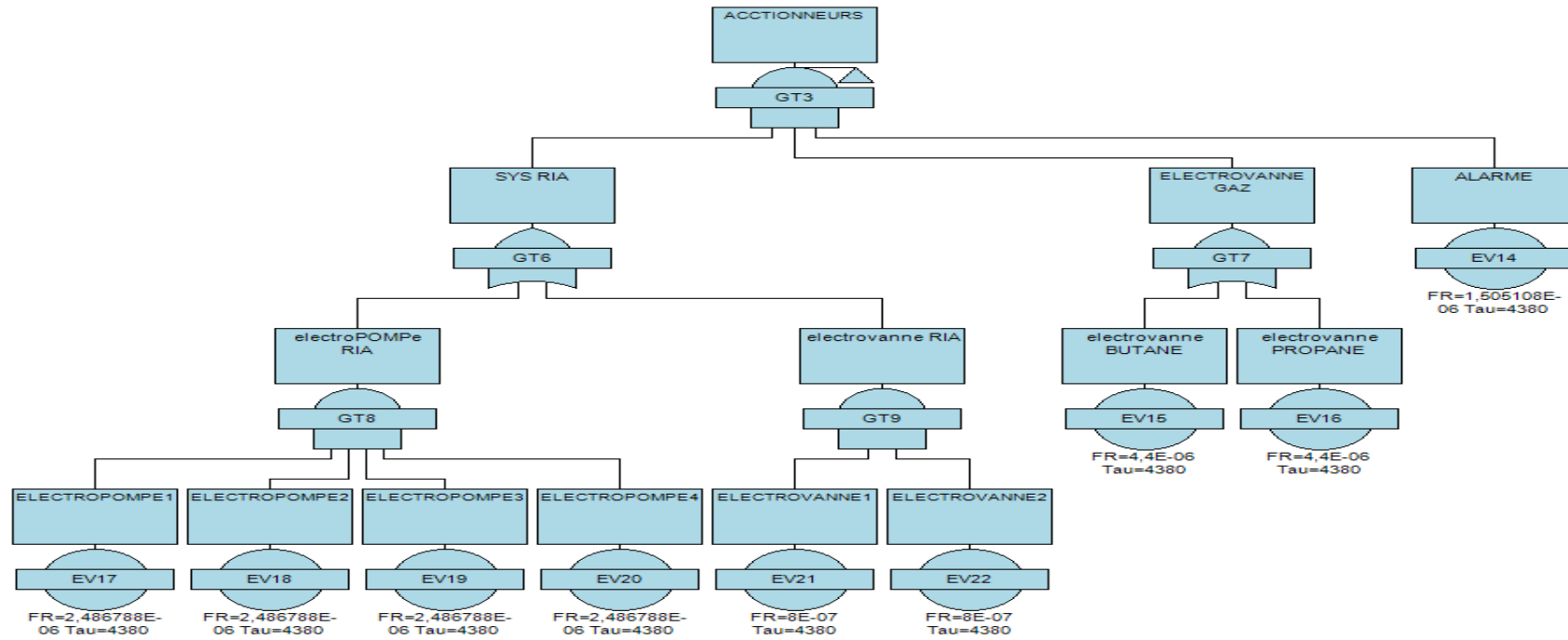


Figure 35 : L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda_{DU}$  - partie3

PFD<sub>max</sub>=0,00403

D'après ces résultats on trouve que le niveau de SIL réel de ce système instrumenté de sécurité est le **SIL 3**.

### 3.1.3. Calcule la probabilité de défaillance SIS par $\lambda_{SD}$ taux de défaillance aléatoire en sécurité du matériel défectable

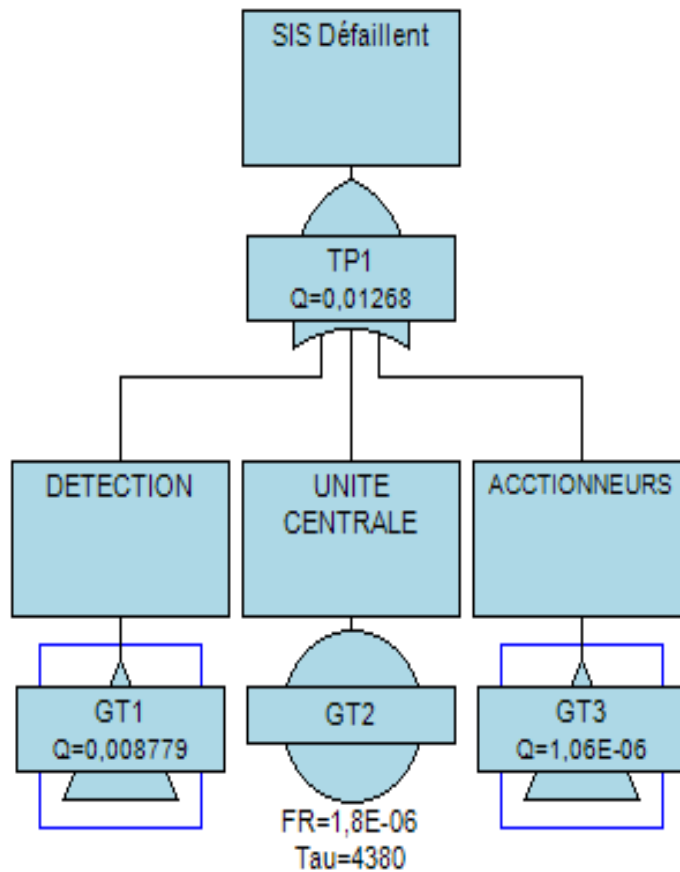


Figure 36 : L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda_{SD}$  - partie 1

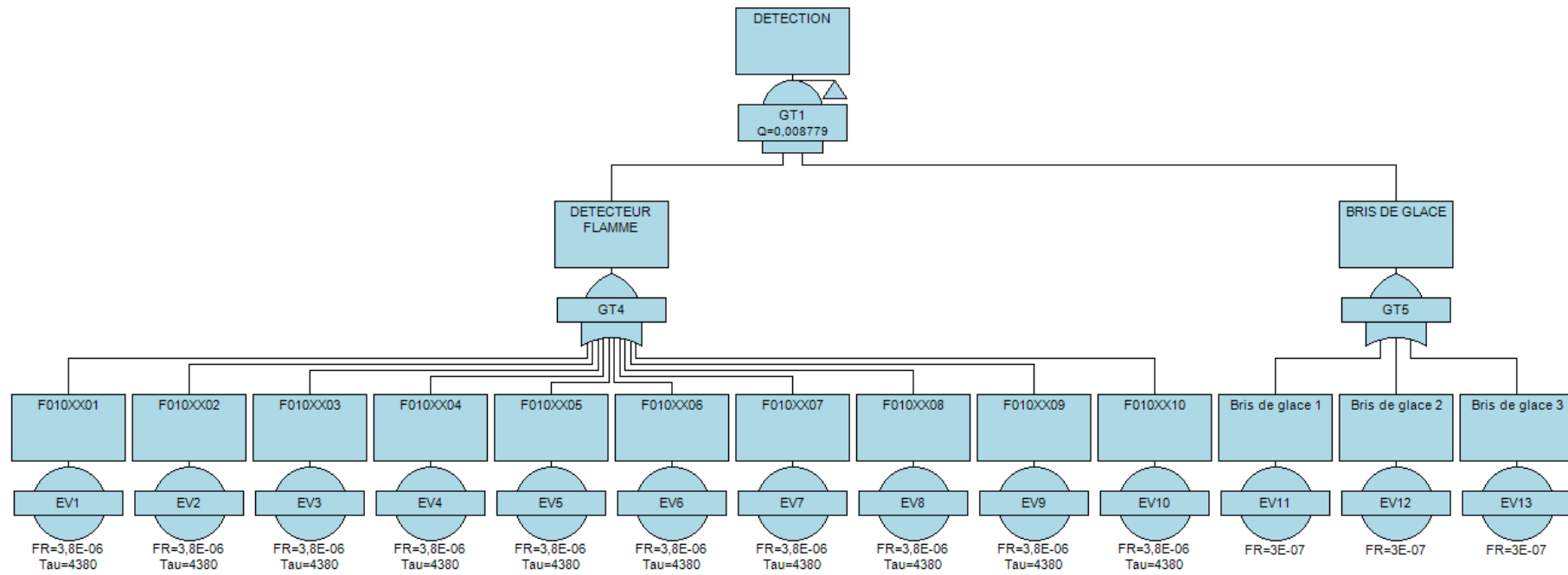


Figure 37 : L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda_{SD}$  - partie2

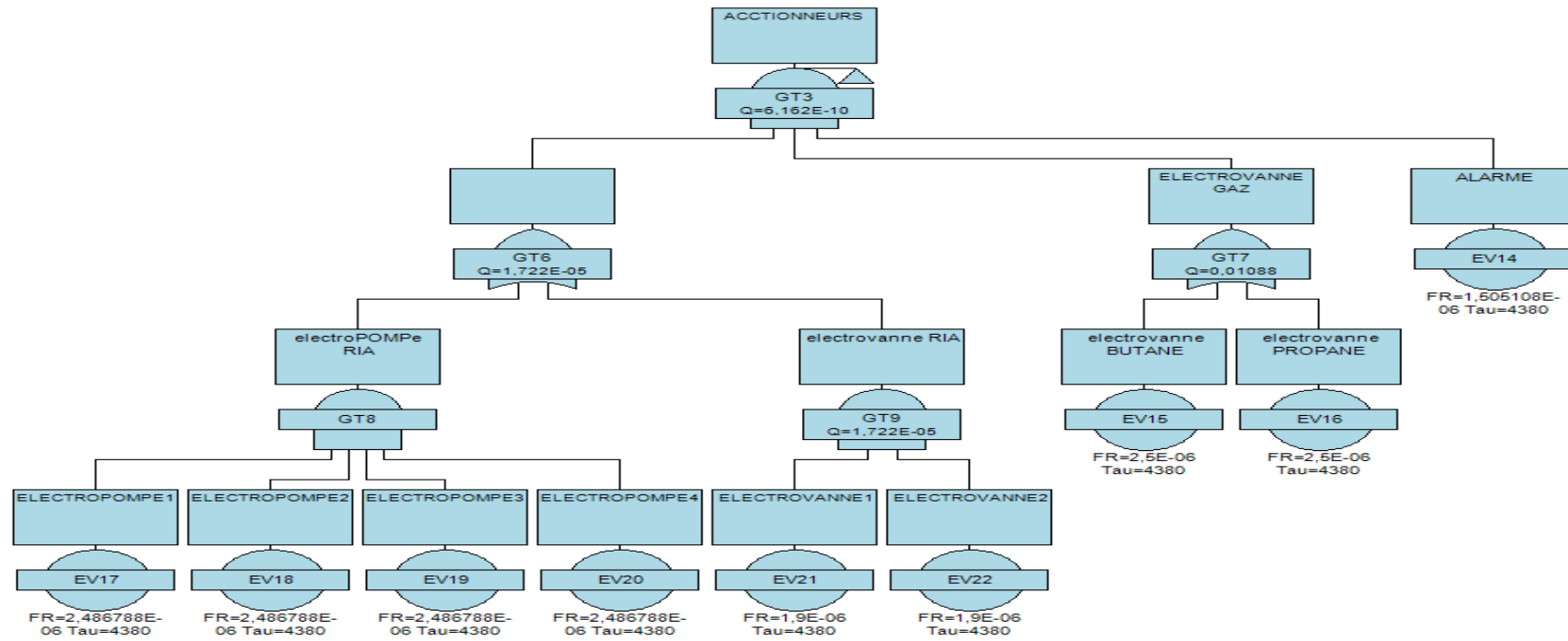
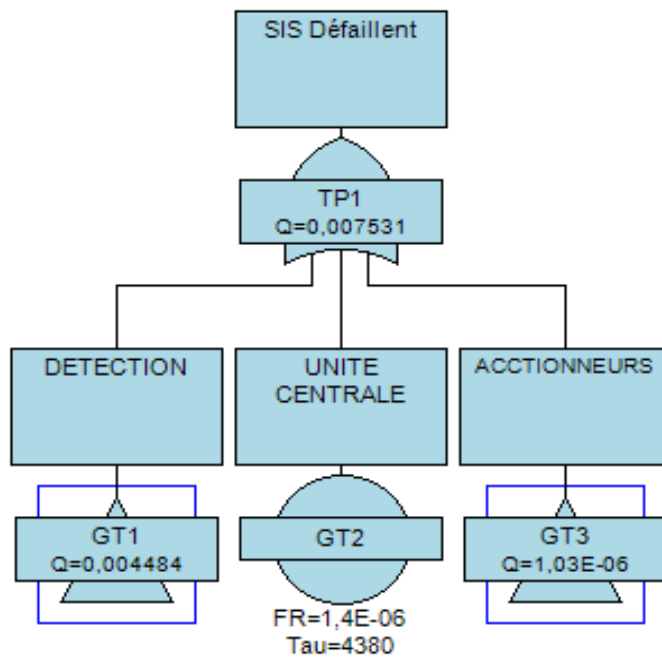


Figure 38 : L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda_{SD}$  - partie3

PFD<sub>max</sub>=0,01268

D'après ces résultats on trouve que le niveau de SIL réel de ce système instrumenté de sécurité est le **SIL 2**.

### 3.1.4. Calcule la probabilité de défaillance SIS par $\lambda_{SU}$ taux de défaillance aléatoire en sécurité du matériel défectable indétectable



**Figure 39** L'arbre des défaillances du système instrument de sécurité par utilisation  $\lambda_{SU}$  - partiel



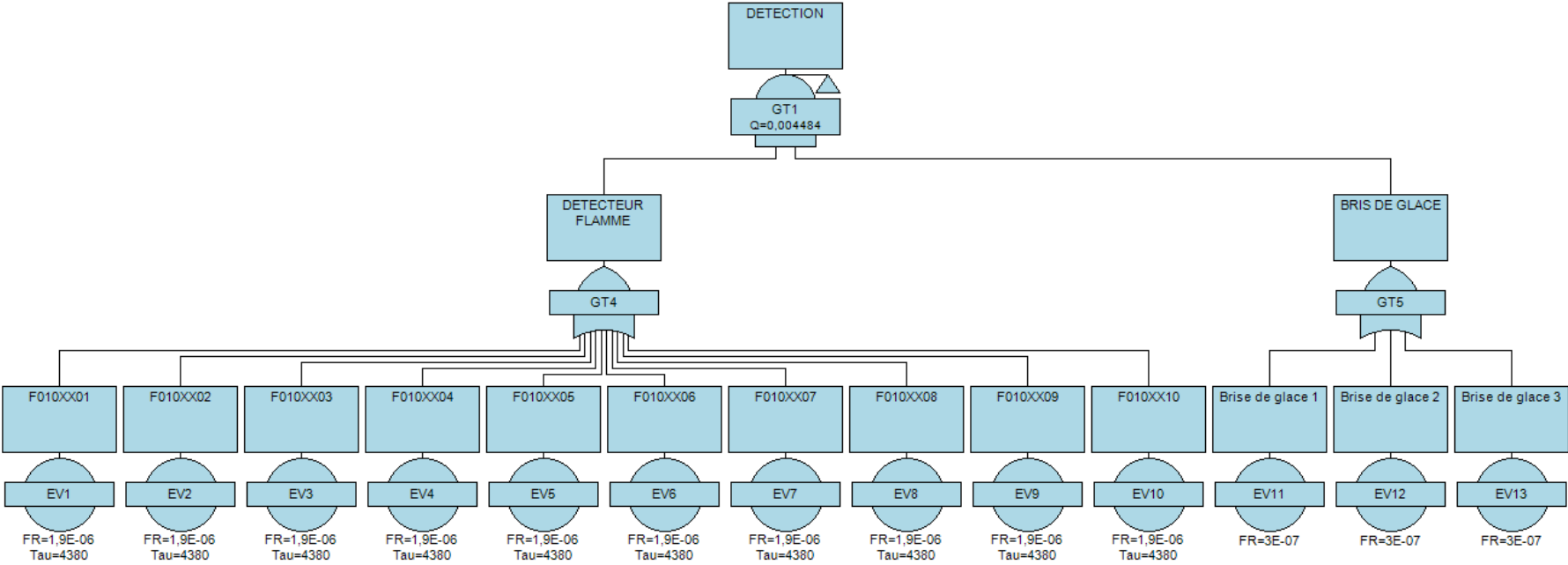


Figure 40 L'arbre des défaillances du système instrument de sécurité par utilisation λSU - partie2

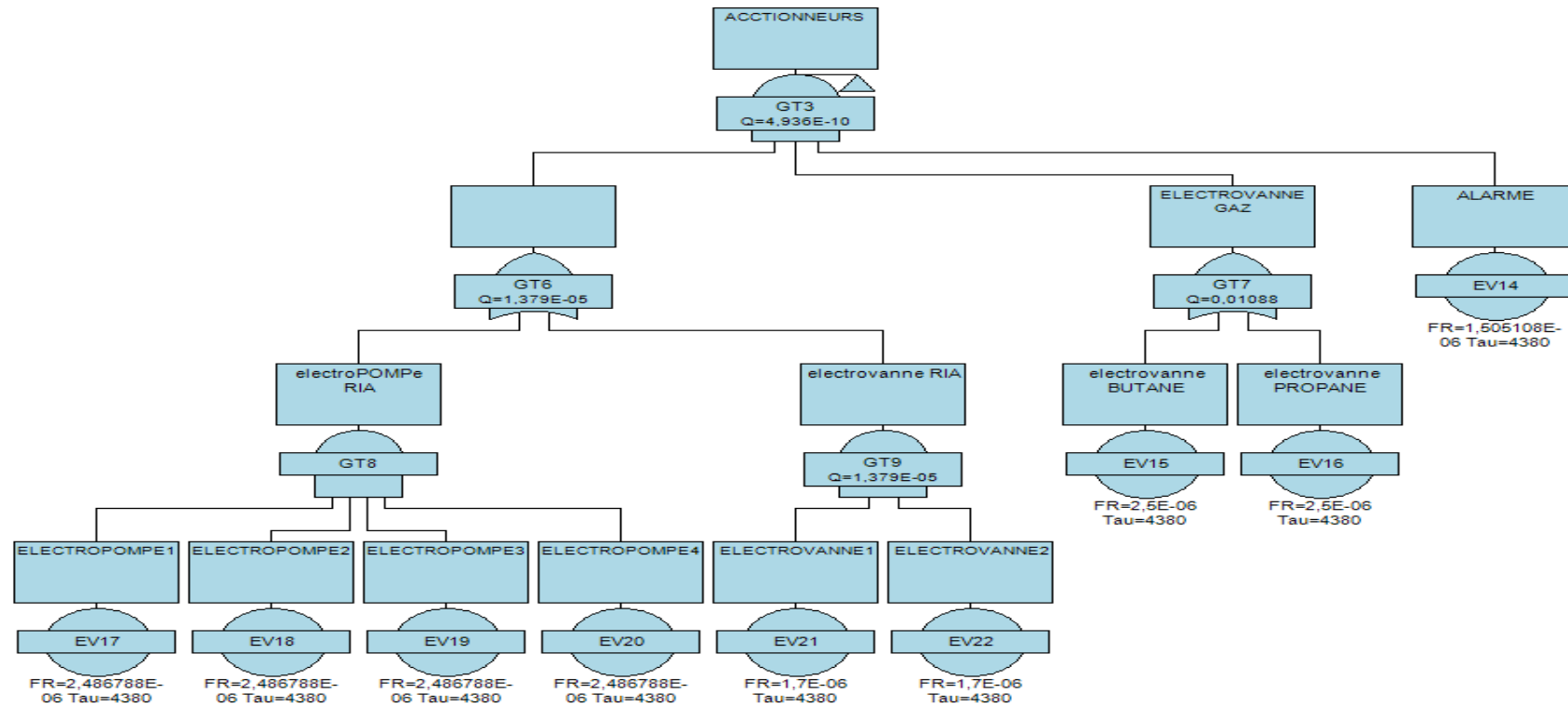


Figure 41 L'arbre des défaillances du système instrument de sécurité par utilisation λSU - partie3

PFDmax=0,007531

D'après ces résultats on trouve que le niveau de SIL réel de ce système instrumenté de sécurité est le **SIL 3**

### 3.2. Analyse résultats d'arbre de défaillance

Cas 1 : En utilisant un taux de défaillance aléatoire dangereuse du matériel détectable, nous avons obtenu un niveau d'intégration de sécurité 2. Cela indique que le système présente un niveau de sécurité moyen. Il est capable de détecter certaines défaillances dangereuses, mais il y a encore des possibilités d'amélioration pour réduire d'avantage les risques.

Cas 2 : En utilisant un taux de défaillance aléatoire dangereuse du matériel non détectable, nous avons obtenu un niveau d'intégration de sécurité 3. Cela suggère que le système présente un niveau de sécurité supérieur par rapport au cas précédent. Les défaillances dangereuses du matériel non détectables sont moins probables, ce qui contribue à réduire les risques.

Cas 3 : En utilisant un taux de défaillance aléatoire en sécurité du matériel détectable, nous avons obtenu un niveau d'intégration de sécurité 2. Cela indique que le système est capable de détecter les défaillances non dangereuses du matériel, ce qui améliore sa fiabilité globale. Cependant, des mesures supplémentaires pourraient être nécessaires pour réduire les défaillances dangereuses détectables.

Cas 4 : En utilisant un taux de défaillance aléatoire en sécurité du matériel non détectable, nous avons obtenu un niveau d'intégration de sécurité 3. Cela suggère que le système présente un niveau de sécurité supérieur par rapport au cas précédent. Les défaillances du matériel sont moins probables et il est plus fiable pour détecter les défaillances potentielles.

En résumé, les cas 2 et 4 semblent offrir un niveau de sécurité supérieur en comparaison aux cas 1 et 3. Il est important de prendre en compte ces résultats pour évaluer les risques associés au système d'instruments de sécurité dans le hall d'emballage des bouteilles de gaz inflammables et mettre en place les mesures appropriées pour garantir la sécurité des opérations.

### 4. Interprétation des résultats :

Après le calcul des niveaux SIL « Réel » dans le cas utilisation  $\lambda_{DD}$  taux de défaillance aléatoire dangereuse du matériel détectable et « Cible » nous constatons que ces deux derniers sont égaux pour l'élément d'entrée et l'élément final :

$$\text{SIL (cible)} = \text{SIL (réel)} = 2$$

## 5. Recommandation

Lorsque le niveau d'intégration de sécurité cible est égal au niveau d'intégration de sécurité réel (2), cela signifie que le système de sécurité atteint partiellement les objectifs de sécurité définis. Voici quelques recommandations pour améliorer le niveau d'intégration de sécurité dans cette situation :

- **Évaluation des risques** : Effectuez une évaluation approfondie des risques pour identifier les lacunes potentielles dans le système de sécurité. Identifiez les scénarios de défaillance critiques et évaluez les conséquences et les probabilités associées.
- **Mise en place de barrières de sécurité supplémentaires** : Identifiez les zones où des barrières de sécurité supplémentaires sont nécessaires et mettez-les en place. Cela peut inclure l'installation de systèmes de détection d'incendie et de gaz, de systèmes de suppression automatique d'incendie, de systèmes d'alarme et de surveillance, etc.
- **Formation et sensibilisation** : Assurez-vous que le personnel est correctement formé aux procédures de sécurité, aux équipements de sécurité et aux mesures d'urgence. Organisez régulièrement des sessions de sensibilisation à la sécurité pour rappeler aux employés les bonnes pratiques et les procédures de sécurité à suivre.
- **Maintenance préventive** : Mettez en place un programme de maintenance préventive pour assurer le bon fonctionnement et la fiabilité des équipements de sécurité. Cela comprend l'inspection régulière, le nettoyage, le remplacement des pièces défectueuses et la vérification des systèmes de sécurité.
- **Révision des procédures opérationnelles** : Revoyez et mettez à jour les procédures opérationnelles pour inclure les meilleures pratiques de sécurité. Assurez-vous que les procédures sont claires, facilement compréhensibles et suivies par le personnel.
- **Audit de conformité** : Effectuez régulièrement des audits de conformité pour vous assurer que les mesures de sécurité sont correctement mises en œuvre et respectées. Identifiez les écarts de conformité et prenez les mesures nécessaires pour y remédier.
- **Communication et participation des employés** : Encouragez la communication ouverte entre les employés et la direction concernant les problèmes de sécurité. Impliquez activement les employés dans l'identification des risques et la proposition de solutions pour améliorer le niveau d'intégration de sécurité.

- Suivi et mesure de la performance : Mettez en place des indicateurs clés de performance pour mesurer la performance du système de sécurité. Suivez régulièrement ces indicateurs et analysez les tendances pour identifier les domaines d'amélioration.
- Revue de direction : Effectuez régulièrement des revues de direction pour évaluer l'efficacité du système de sécurité et prendre des décisions d'amélioration. Utilisez les résultats des audits, des évaluations des risques et des indicateurs de performance pour guider les décisions et les actions.

## **Conclusion générale :**

Notre étude visait à évaluer l'intégrité d'une fonction de sécurité instrumentée dans un système de détection de feu et de gaz installé dans le hall d'emplissage.

L'objectif était d'apprécier son efficacité face aux dangers en déterminant son niveau d'intégrité.

Pour parvenir à cette détermination, nous avons suivi deux étapes principales. Tout d'abord, nous avons attribué un niveau SIL «cible» en utilisant la méthode HAZOP et le graphe de risque intégré. Ensuite, nous avons calculé le niveau SIL «réel » en utilisant un arbre de défaillance.

Grâce à l'application de la méthode HAZOP, nous avons obtenu des résultats nous permettant d'identifier les scénarios catastrophiques ainsi que les mesures mises en place pour maîtriser ces risques. En combinant le graphe de risque avec HAZOP, nous avons déterminé le niveau SIL en deux phases : un niveau SIL initial et un niveau SIL final. Le niveau SIL cible obtenu pour la fonction instrumentée de sécurité (SIF) étudiée est égal à « 2».

Le niveau SIL réel obtenu à l'aide du logiciel ISOGRAPHE "SIL vérification" est égal à «2».

Après avoir comparé les deux niveaux d'intégrité de sécurité, nous avons trouvé que le niveau SIL "Cible" correspond au niveau SIL "Réel".

## Bibliographie

[1] <https://www.naftal.dz/fr/>

[2] Guide HSE

[3] KHELIF Mohamed Amine, Etude SIL (Safety Integrity Level) Pour l'obtention du diplôme de Master, IMSI Université d'Oran 2 Mohamed Ben Ahmed, 2022.

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

[5] ABBAS Nazim, Approche analytique de la gestion globale des risques au sein de General Electric, Projet de fin d'étude pour l'obtention du diplôme d'ingénieur, Ecole Nationale Polytechnique Alger, 2015.

[6] DEROUAZ Djalal, Maîtrise des risques majeurs au niveau du "Centre Vrac GPL – CV 165" de NAFTAL à Sidi Arcine (Baraki), Projet de projet de fin d'études Pour l'obtention du Diplôme d'Ingénieur, Ecole Nationale Polytechnique Alger, 2016.

[7] BENIDA Rabah Abdelouahab, ARBRE DE DEFAILLANCES DES GARNITURES MECANIQUES POUR POMPES CENTRIFUGES MULTICELLULAIRES, Mémoire de fin d'étude Pour l'obtention du Diplôme de Master, Université Ibn Khaldoun de Tiaret, 2020.

[8] Kassas Bachir, Application de l'arbre de défaillance « Fault-tree » pour le système du ballon à vapeur au niveau de l'unité Production Ammoniac, Soutenance de Master 2 En Maintenance Industrielle et Fiabilité Mécanique, Université Badji Mokhtar Annaba, 2017.

[9] Mouloud BOURARECHE, Apport des techniques floues et possibilistes à l'analyse semi-quantitative des risques industriels, Mémoire magister en hygiène et sécurité industrielle, UNIVERSITÉ EL HADJ LAKHDAR – BATNA, 2009.

[10] Hafed TOUAHAR, Maintenance des Systèmes Instrumentés de Sécurité (SIS): Etude de cas, Université Hadj-Lakhdar Batna, 2015.

[11] SENOUCI Maroua, Etude d'allocation et de vérification de niveau SIL d'un système de détection F&G, MÉMOIRE Pour l'obtention du diplôme de Master, IMSI Université d'Oran 2 Mohamed Ben Ahmed, 2022.

[12] BOUBERAK Wissame, Maîtrise des risques d'incendie et d'explosion par l'application de la méthode Dow's Fire and Explosion Index, Projet de fin d'étude pour l'obtention du diplôme d'Ingénieur d'Etat, Ecole Nationale Polytechnique Alger, 2015.

- [13] CHERGUI Loubna, Diagnostic des Défaillances et Optimisation des Architectures des Systèmes Instrumentés de Sécurité: Apport de la Logique Floue, MEMOIRE Présenté pour l'obtention du diplôme de MAGISTERE, Université El-Hadj Lakhdar – Batna, 2010.
- [14] Shahinez Baitiche, La gestion des niveaux de sécurité intégrée « System Integrated Level » dans un procédé au niveau du GL2Z, Mémoire de magister, Université d'Oran 1 Ahmed Ben Bella, 2011.
- [15] OUKOUCHIH Sihem, Analyse et gestion des risques liés aux activités du stockage et de l'emplissage du Gaz Pétrole Liquéfié au niveau du projet Centre emplisseur de Bordj Menaiel Wilaya de Boumerdes, Université M'hamed Bougara- Boumerdes, 2017.
- [16] Saida BRAHIMI, Maitrise des risques liés à l'activité chargement /déchargement du carburant en respectant les bases d'hygiène, de la sécurité et de l'environnement Au sein de l'entreprise NAFTAL Carburant (EL Harrach), Université M'Hamed Bougara- Boumerdes, 2017.
- [17] IDDIR, O., Evaluation de la probabilité de défaillance d'un système instrumenté de sécurité (SIS). Techniques de l'ingénieur, 2009.
- [18] [Ayault, 2005] N.Ayault. Evaluation des barrières techniques de sécurité. INERIS, février 2005.
- [19] [Goble et Cheddie, 1998] W. Goble, H. Cheddie. Control system safety evaluation and reliability. US: ISA; 1998.
- [20] Méthode HAZOP et conduite des revues HAZOP ENSPM 2006.
- [21][IEC61508, 2002] IEC 61508. Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité, partie 6, mars 2002.
- [22] [IEC61511, 2003]IEC 61511. Functional safety – Safety instrumented systems for the process industry. International Electrotechnical Commission, Geneva, Switzerland, 2003.
- [23] [Coolen et Utkin, 2007] F. Coolen, L. Utkin. Imprecise reliability: A concise overview, in Risk, Reliability and Societal Safety, ESREL07, 2007.
- [24] BARTHELEMY, B .Gestion globale des risques. Techniques de l'ingénieur, Vol ag1100, (2013).
- [25] DARSA, D, J .La gestion des risques en entreprise : Identifier, comprendre maitriser. Gereso Edition. Le Mans. (2013).
- [26] Villemeur, A, Sûreté de fonctionnement des systèmes industriels. Number 2. Eyrolles, 1998.
- [27] [Ayault, 2005] N.Ayault. Evaluation des barrières techniques de sécurité. INERIS,



février 2005.

[28] Yueting Hu .2019 Open Journal of Safety Science and Technology, A Concise and Practical Barrier Model

[29] INERIS, Méthodes d'analyse des risques générés par une installation industrielle, Oméga 7, 2006, 119 pages.

[30] INERIS, Evaluation des performances des Barrières Techniques de Sécurité, Oméga 10, 2008, 87 pages.

[31] TOTAL, INSTRUMENTATION, MANUEL DE FORMATION Cours EXP-SI100, 2009.

[32] Stein Hauge, Reliability Prediction Method for Safety Instrumented Systems, 2013, édition par SINTEF Technology and Society.

[33] Stein Hauge, Reliability Prediction Method for Safety Instrumented Systems, 2010, édition par SINTEF Technology and Society.

[34] SINTEF. *Reliability Data for safety instrumented systems, PDS Data handbook*. 2006 édition ; 2006.

[35] OHSAS 18001, *Système de management de la santé et de la sécurité au travail – Spécification*. BSI, AFNOR; 2007.

[36] CEI 61508, sécurité fonctionnelle des systèmes E/ E/ EP relatifs à la sécurité, 2009.

[37] CEI 61511-3, Sécurité fonctionnelle–SIS pour le secteur des industries de transformation– Partie 3 : Conseils pour la détermination des niveaux exigés d'intégrité de sécurité, 2003.

[38] [www.inrs.fr](http://www.inrs.fr).

[39] [www.ineris.fr](http://www.ineris.fr).

[40] <http://www.qse-france.com/larbre-des-defaillances/>

[41] <https://www.gazdetect.com>

[42] <https://www.techniques-ingenieur.fr/base-documentaire>.

## Annexe

	Détecteur de flamme	Bris de glace	Unité centrale	Alarme	Electrovanne 1 et 2	Electro-pompe 1,2,3 et 4	Electrovanne gaz butane et propane
$\lambda_{DD}$	2,7E -6	0,5E -6	1,8E -6	2,4867E-06	1,1E -6	1,5051E-06	4,4E -6
$\lambda_{DU}$	0,8E -6	0,4E -6	0,7E -6	2,4867E-06	0,8E -6	1,5051E-06	4,4E -6
$\lambda_{SD}$	3,8E -6	0,3E -6	1,8E -6	2,4867E-06	1,9E -6	1,5051E-06	2,5E -6
$\lambda_{SU}$	1,9E -6	0,3E -6	1,4E -6	2,4867E-06	1,7E -6	1,5051E-06	2,5E -6

La base des données SINTF( reability data safety instrumented systems ) et NRPD 2016 (Nonelectronic parts reliability data publication)