الجمهـــوريـــــة الجزائـــريـــــة الديمقـــراطيـــــة الشـعبيـــة
République Algérienne Démocratique et Populaire
وزارة التـــعلـــيـــــم العـــــالـــــي والبـــحـــــث العـلمـــي
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

جامعة وهران 2 محمد بن أ حمد
Universitéd'Oran 2 Mohamed Ben Ahmed

معهد الصيانة و الأمن الصناعي
Institut de Maintenance et de Sécurité Industrielle

Département : Sécurité Industrielle et Environnement

MÉMOIRE

Pour l'obtention du diplôme de Master

Filière : Hygiène et Sécurité Industrielle
Spécialité : Sécurité Industrielle et Environnement

Thème

Etude d'allocation et de vérification de niveau SIL d'un système de détection F&G

Présenté et soutenu publiquement par :

SENOUCI Maroua

Devant le jury composé de :

Nom et Prénom	Grade	Etablissement	Qualité
AISSANI Nassima	MCA	IMSI	**Président**
GUETARNI Islam Hadj Mohamed	MCB	IMSI	**Encadreur**
BENOMAR Fatima	MAA	IMSI	**Examinateur**

Année 2021/2022

Etude d'allocation et de vérification de niveau SIL d'un système de détection F&G

Résumé

La norme CEI 61511 s'intéresse à la sécurité fonctionnelle dans l'installation des systèmes instrumentés de sécurité au niveau des industries de production par procédé. Elle exige dans ce cadre de conduire une évaluation de risque des processus pour permettre d'en déduire des spécifications et le cycle de vie pour les SIS. Cette étude s'intéresse plus particulièrement au niveau d'intégrité de sécurité et à leur allocation en fonction du SIS à évaluer. Le but principal de notre travail est de déterminer et évaluer le niveau d'intégrité de sécurité du « système détection de flamme » du hall d'emplissage (situé au niveau du centre enfuteur CE141 NAFTAL). Pour cela, nous allons passer par trois principales étapes soit « identification de la boucle SIF existante une Allocation du sil et vers la fin une vérification du niveau de SIL est établi par des modèle numériques. Pour déterminer le niveau SIL de la fonction instrumentée choisie, nous avons procédé à la détermination, en premier lieu, du niveau SIL dit « Cible » et cela par l'application de la méthode qualitative Hazop intégrer avec Matrice et « graphe de risque ». Ce niveau SIL « Cible » sera ensuite comparé au niveau SIL « Réel » calculé à partir des données de défaillance réelles du système. Tous ces calculs sont obtenus par l'exploitation du logiciel GRIF-SIL.

Mots clés : SIL, SIF, SIS, HAZOP, système de détection F&G

SIL Allocation and Verification Study of Fire and gas detection system

Abstract :

The standard IEC 61511 focuses on functional safety in the installation of the safety instrumented systems to process production industries. In this context, it's requiring that a risk assessment of the processes be carried out in order to deduce specifications for SIS. This study focuses on the level of security integrity and their allocation according to the SIS to be assessed.

The main purpose of our work is to determine and evaluate the safety integrity level of the "flame detection system" installed in the filling hall (located at the CE141 NAFTAL smoke). For this reason, we will start through three main steps: "identification of the existing SIF, an allocation of the SIL and at last a verification of the SIL level is established by numerical models.we have divided this brief into 03 chapters in order to structure our work. To determine the SIL level of the chosen instrumented function, we proceeded to the determination, in the first place, of the so-called "Target" SIL level and this by applying the qualitative method "risk graph". This "Target" SIL level will then be compared to the "Real" SIL level calculated from the actual system failure data. All these calculations are obtained by using the GRIF software.

Keywords : SIL, SIF, SIS, HAZOP, F&G detection system

REMERCIMENT

Je remercie avant tout, Dieu le tout Puissant de nous avoir donné tous les moyens et nous a dirigé vers ce qui est le meilleur pour nous, ELHAMDOULI'ALLAH.

J'adresse toute ma gratitude à mon encadrant Monsieur GUETARNI Islam Hadj Mohamed, Maître de Conférences à l'institut de maintenance et de sécurité industrielle de m'avoir proposé ce sujet de mémoire et de m'avoir encadré. Pour sa collaboration inestimable, sa disponibilité et pour tous les conseils judicieux, pour ces critiques pertinentes, pour ça souplesse de travail. Je voudrais le remercier aussi pour sa patience et son soutien. J'exprime mes profonds remerciements à Madame SERAT Fatima Zohra, Maître de conférences à l'institut de maintenance et de sécurité industrielle pour son aide et ses encouragements tout au long de ce travail.

Mes remerciements iront naturellement vers tous ceux qui ont accepté avec bienveillance de participer au jury de mémoire :

Je remercie Madame AISSANI Nassima, maitre de conférences à l'institut de maintenance et de sécurité industriel pour avoir présidé le jury. Et également Madame BENOMAR Fatima, Maître de Conférences à l'institut de maintenance et de sécurité industriel, d'avoir accepté d'examiner ce mémoire.

J'exprime, également, ma profonde gratitude à tous les personnels de l'entreprise NAFTAL, centre enfuteur CE141 TIARET, pour leur aide et fourniture des données.

Enfin un grand merci à toutes les personnes qui m'ont encouragé de près ou de loin pendant la fin de mon mémoire.

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

Liste d'abréviation :

BLEVE: Boiling Liquid Expanding Vapor Explosion.

BPCS: Basic Process Control System

CPF: Central Processing Facilities

DCS: Distributed Control System

FAL: Flow Alarm Low

FALL: Flow Alarm Low Low

FT: Flow Transmitter

FV: Flow Valve

GPL : Gaz de pétrole liquéfié

H : Heater

HAZOP: Hazard and Operability Study

IEC: International Electrotechnical Commission

OHSAS: Occupational Health and Safety Assessment Series

PAH: Pressure Alarm High

PAHH: Pressure Alarm High High

PAL: Pressure Alarm Low

PALL: Pressure Alarm Low Low

PCV: Pressure Controller Valve

P&ID: Piping and Instrumentation Diagram

PFD: Probability of Failure on Demand

PFH: Probability of Failure per Hour

PHA: Process Hazard analysis

PLC: Programmable Logic Controller

PT: Pressure Transmitte

SDV: Shutdown Valve

SIF: Safety Instrumented Function

SIL: Safety Integrity Level

SIS: Safety Instrumented System

TAH: Temperature Alarm High

TAHH: Temperature Alarm High High

TI: Temperature Indicator

TV: Temperature Valve

UVCE: Unconfined Vapour Cloud Explosion

Sommaire

Liste de figures

Liste de tableaux :

INTRODUCTION :

Le développement industriel a fait que Les industries s'occupent non seulement des performances des systèmes en termes de qualité et de rentabilité mais aussi en termes de sécurité. Les moyens à mettre en œuvre pour réduire les risques sont nombreux et variés. La conception du procédé, le choix des équipements participent à la réduction du risque.

Ces approches ne sont pas toujours suffisantes. Des systèmes spécifiques appelés Systèmes Instrumentés de sécurité (SIS) sont utilisés ayant pour objectif de réduire les risques d'occurrence d'´évènements dangereux tout en garantissant la protection ; des personnes, des équipements matériels et de l'environnement d'une manière automatique.

La réduction du risque apportée par la fonction instrumentée de sécurité est appelée réduction nécessaire du risque.

Les normes IEC 61508 et IEC 61511 définissent quatre niveaux d'intégrité de sécurité (Safety integrity Level) pour une fonction de sécurité, quatre niveaux possibles de SIL.

L'implémentation des SIS dans un système nécessite la détermination préalable du SIL qui devrait être atteint par la fonction instrumentée. L'évaluation du niveau d'intégrité de sécurité est déterminée par des méthodes qualitatives et quantitatives [SAL 06b], [SAL 08].

Parmi les méthodes qualitatives les plus utilisées pour déterminer le niveau de SIL d'une SIF la méthode matrice de risque décrit dans la partie 5 de la norme IEC 61508. Quand cette méthode est adoptée, un certain nombre de paramètres de simplification sont introduits pour décrire la nature de la situation dangereuse lorsque les systèmes relatifs à la sécurité sont défaillants ou non disponibles. Un paramètre est choisi parmi quatre groupes caractéristiques du risque et les paramètres sélectionnés sont alors associés pour décider du niveau de SIL des systèmes relatifs à la sécurité. On peut citer aussi la méthode la plus utilisée soit Graphe de risque qui permet d'obtenir le niveau de SIL requis selon 4 paramètres.

La boucle SIF est souvent proposée selon une architecture établie par les instrumentistes se composant d'équipements conformément au SIL déterminer par l'étude d'allocation du SIL.

Une vérification des niveaux de sil selon les architectures présentes in site est requise par l'utilisation des méthodes probabilistes tel que « arbre de défaillance, les chaines de Markov…. ».

Ces méthodes permettre d'obtenir un niveau de SIL et le vérifie avec le SIL cible obtenu à partir de l'allocation.

A cet effet La problématique qui se pose quelle est la meilleure méthodologie a adopté pour permettre la validation de l'architecture SIF installer au niveau du hall d'emplissage de centre enfuteur CE141 NAFTAL ainsi que de la comparer avec le SIL cible.

Afin de répondre a cette problématique notre projet de fin d'étude s'organise comme suite :

Le premier chapitre concerne la définition de certains concepts utilisés dans le cadre de la sécurité fonctionnelle des systèmes de sécurité. Une brève description des normes relatives aux systèmes de sécurité est donnée, suivie d'une description des différentes méthodes utilisées pour déterminer le SIL d'un SIS

Dans le deuxième chapitre, nous présenterons d'abord le système fire & gaz et ses fonctions ainsi que ses composants essentiels (détecteur, unité logique et l'actionneur) et on présentera par la suite les différentes architectures KooN usuelles d'un système F&G.

Le troisième chapitre est consacré à l'allocation de SIL d'un système instrumenté de sécurité (système de détection de flame) au niveau du centre emplisseur CE 141 TIARET de l'entreprise NAFTAl par l'application du modèle graphe de risque et à la fin une vérification du niveau de SIL est élaborer par le biais de ce SIS sur le logiciel GRIF.

CHAPITRE I

Système instrumenté de sécurité et les méthodes de détermination de SIL

1. Notions générales :

1.1. Système :

La norme ISO/CEI 15288 :2008 définit un système comme « un ensemble d'éléments, en interaction dynamique, organisés en fonction des buts ». Cette définition condense en une seule phrase pratiquement tous les aspects essentiels de ce qui sera utile, voire nécessaire pour faire l'ingénierie dudit système :

- **Aspect fonctionnel** : le système sert à quelque chose, il tend vers un but ;
- **Aspect structurel :** le système n'est pas réduit à un seul élément, mais est un ensemble d'éléments reliés entre eux ;
- **Aspect comportemental** : les éléments constitutifs d'un système interagissent entre eux pour produire un(des) comportement(s) (émergence) censé(s) tendre vers le but.

Ce dernier point cristallise une des différences fondamentales entre l'approche systémique qui met l'accent sur les interactions entre les éléments en considérant les effets globaux de ces interactions, et l'approche analytique qui est réductionniste et ne considère les éléments qu'un à un, en ne s'intéressant qu'aux types ou catégories d'interactions entre ces éléments. [1]

1.2. Danger :

Source potentielle de dommage [2]

« La propriété intrinsèque d'une substance dangereuse ou d'une situation physique de pouvoir provoquer des dommages pour la santé humaine et/ou l'environnement. » [3]

1.3. Identification du danger :

Processus visant à reconnaître qu'un danger existe et à définir ses caractéristiques.

1.4. Situation dangereuse :

Une situation dangereuse selon la norme (ISO 12100-1) est une situation dans laquelle une personne est exposée à au moins un phénomène dangereux. L'exposition peut entraîner un dommage, immédiatement ou à plus long terme.

1.5. Risque :

« Combinaison de la probabilité d'un dommage et de sa gravité » [3]

Et Selon Iso31000 « effet de l'incertitude sur l'atteinte des objectifs »Selon Farmer, le risque est classé en deux catégories risque acceptable (maitrisé) et risque inacceptable en se basant sur la fonction G = f(P), comme le montre la courbe ci-dessous appelée « Courbe de Farmer »[18]

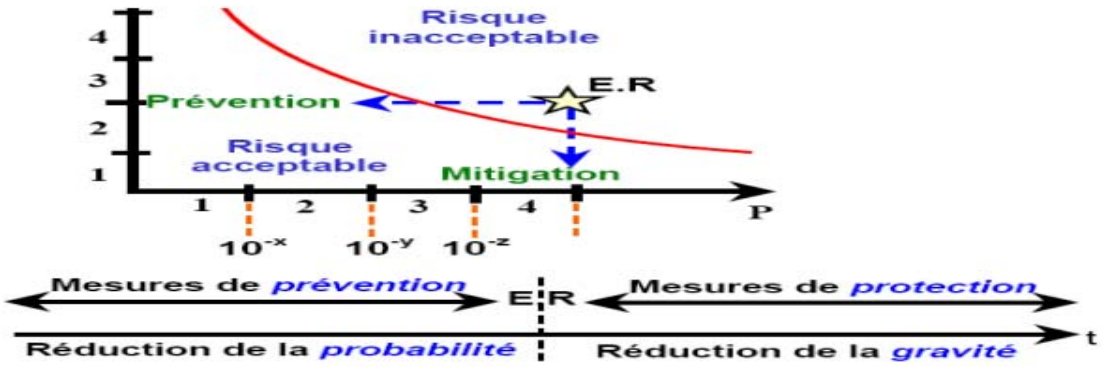


Figure 1 Courbe de Farmer

1.4.1. Risque tolérable :

Risque tolérable risque accepté dans un certain contexte et fondé sur les valeurs admises par la société [4]

1.4.2. Risque résiduel :

Risque subsistant après que des mesures de prévention ont été prises [5]

1.4.3. Evaluation des risques :

Processus général d'estimation de l'ampleur du risque et de prise de décision concernant l'acceptabilité du risque.

a. La matrice des risques :

La matrice des risques est un outil d'analyse qui permet d'évaluer en amont la probabilité et la gravité des risques liés à un projet, une fois ces deux éléments évalués, vous pouvez alors représenter chaque risque de manière visuelle dans votre matrice afin d'en calculer les éventuelles répercussions.

1.4.4. Réduction du risque :

La réduction du risque doit être considérée dès lors que le risque considéré est jugé inacceptable. Il s'agit d'identifier les barrières nécessaires pour ramener le niveau de risque des différents scénarios d'accidents, en agissant le plus en amont possible de leur développement (principe d'élimination à la source), à un niveau acceptable. La réduction du risque peut être obtenue de deux manières différentes (figure1.1).

La protection : elle regroupe les mesures prises pour limiter les conséquences de la survenue d'un accident en diminuant ainsi sa gravité. Par exemple : une cuvette de rétention assurant le non épandage d'un liquide, un système d'extinction automatique permettant de réduire les effets d'un

incendie, les plans de secours et les procédures d'urgence pouvant réduire largement les dommages susceptibles d'être occasionnés, etc.

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

Couches de protection indépendantes (IPL) :

Une couche de protection qui empêche un scénario à risque de progresser quel que soit l'évènement initiateur ou l'exécution d'une autre couche de protection.

Les critères de qualification d'une couche de protection (PL) en tant qu'IPL sont les suivants : la protection fournie réduit le risque identifié dans une large mesure, à savoir une réduction d'au moins 10 fois ;

La fonction de protection présente un haut degré de disponibilité (au moins 0,9);

Elle présente les caractéristiques importantes suivantes :

- Spécificité : une IPL est uniquement conçue pour éviter ou atténuer les conséquences d'un événement potentiellement dangereux (par exemple : réaction d'emballement, dégagement de matériau toxique, perte de confinement ou incendie). De nombreuses causes peuvent conduire au même événement dangereux ; et, par conséquent, de nombreux scénarios d'événements peuvent déclencher une action de la part d'une IPL ;
- Indépendance : une IPL est indépendante des autres couches de protection associées au danger identifié ;
- Sûreté de fonctionnement : une grande confiance peut lui être apportée pour qu'elle remplisse la fonction qui lui est assignée. Les deux modes de défaillances aléatoires et systématiques sont inclus lors de la conception ;
- Aptitude aux contrôles : elle est conçue pour faciliter la validation périodique des fonctions de protection. Des essais périodiques et la maintenance du système de sécurité sont nécessaires.

Seules les couches de protection satisfaisant aux essais de disponibilité, de spécificité, d'indépendance, de sûreté de fonctionnement et d'aptitude aux contrôles sont classées comme des couches de protection indépendantes (IPL).[6]

1.5. Sécurité :

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 suivant le guide ISO/CEI 73 [7].

1.5.1. Sécurité fonctionnelle :

Sous-ensemble de la sécurité globale se rapportant à l'EUC et au système de commande de l'EUC qui dépend du fonctionnement correct des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque) [8]

1.5.2. Évaluation de la sécurité fonctionnelle FSA :

Recherche, à partir de preuves, destinée à juger de l'état de sécurité fonctionnelle atteint par un ou plusieurs SIS et/ou d'autres couches de protection Note 1 à l'article : L'abréviation « FSA » est dérivée du terme anglais développé correspondant « functional safety assessment».

1.5.3. Cycle de vie de sécurité :

Activités nécessaires à la mise en œuvre des systèmes relatifs à la sécurité, se déroulant au cours d'une période allant de la phase de conception d'un projet jusqu'au moment où aucun des systèmes E/E/PE relatifs à la sécurité et des dispositifs externes de réduction de risque ne sont plus disponibles pour une utilisation [9]

1.6. Système électronique programmable (système PE) :

Système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électroniques programmables. Ce terme recouvre tous les éléments du système, tels que l'alimentation, les capteurs et les autres dispositifs d'entrée, les autoroutes de données et les autres voies de communication, ainsi que les actionneurs et les autres dispositifs de sortie (voir la Figure 2)[10]

1.7. Système E/E/PE :

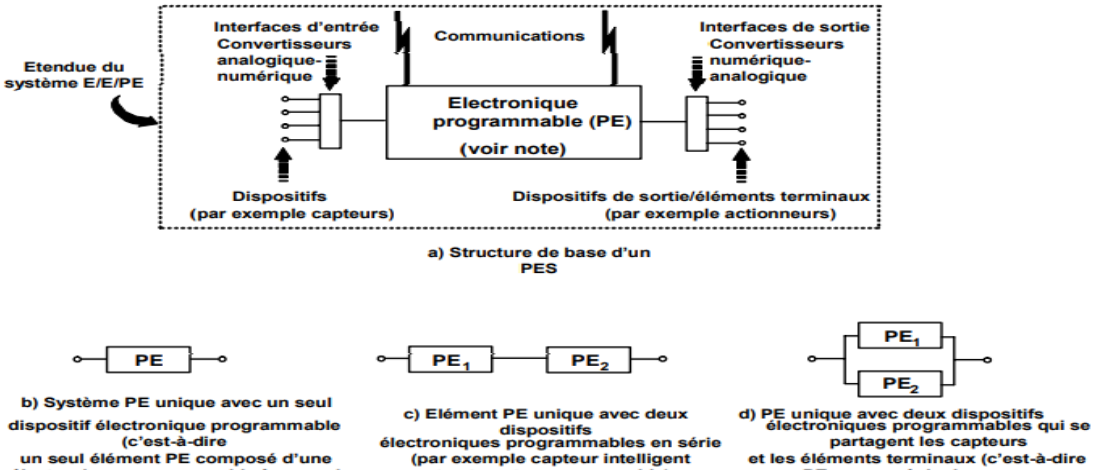


Figure 2 système électronique programmable

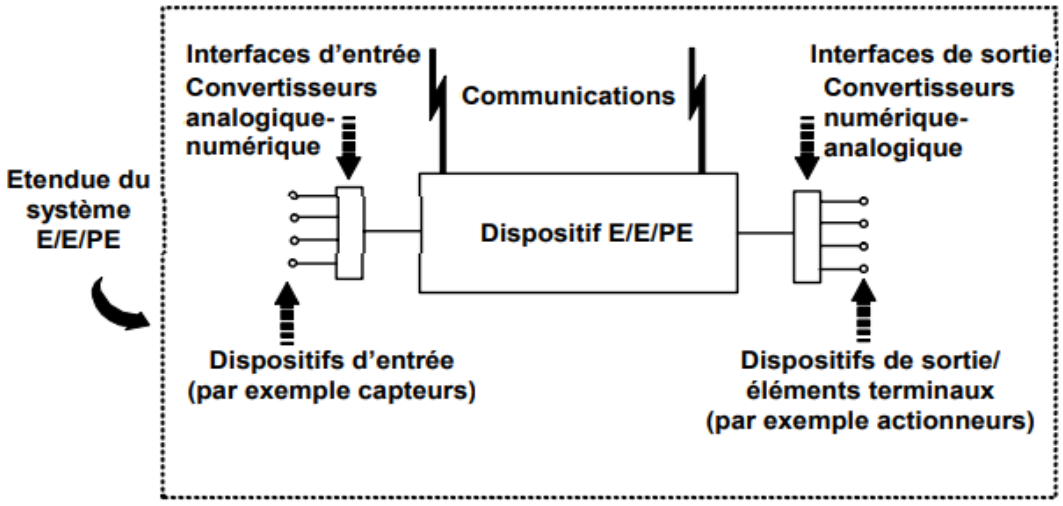


Figure 3 Système E/E/PE structure et terminologie

Système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électriques/électroniques/électroniques programmables (E/E/PE). Ce terme recouvre tous les éléments du système, tels que l'alimentation, les capteurs, et les autres dispositifs d'entrée, les autoroutes de données et les autres voies de communication, ainsi que les actionneurs et les autres dispositifs de sortie (voir la Figure 3) [11]

2. Normes relatives aux systèmes instrumenté de sécurité :

2.1. Norme CEI 61508 :

La norme CEI 61508, constituée de sept parties est développée comme norme générique qui contient un ensemble d'informations et lignes directives concernant l'amélioration de la sécurité à travers l'utilisation des systèmes de sécurités instrumentés (SIS). Elle s'inscrive dans une approche globalisée de la sécurité que l'on pourrait comparer au système ISO 9000 pour la qualité, et au système ISO 14000 pour l'environnement. L'un des principaux objectifs de la CEI 61508 est d'être utilisé par les organisations internationales de normalisation comme une base pour le développement des normes spécifiques à chaque secteur d'application (voir figure 4). Elle permet donc d'avoir des principes et langages communs.

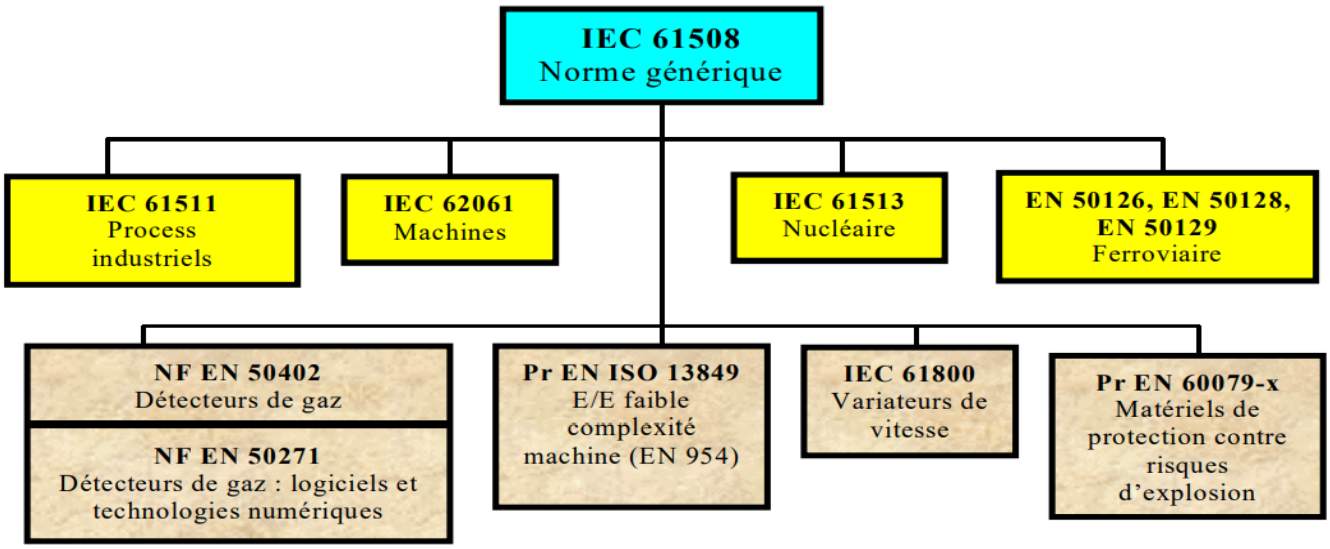


Figure 4 CEI 61508 et ses déclinaisons par secteur d'application

Le principe fédérateur de cette norme est fondé sur le modèle de cycle de vie globale de sécurité, depuis la spécification, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service des SIS, comme montré à la figure 5. Le cycle de vie fournit un guide complet pour l'établissement des caractéristiques et spécifications relatives aux fonctions de sécurité allouées aux SIS.

Globalement, trois grandes parties dans le cycle de vie global de sécurité peuvent être distinguées :

1. Les premières étapes se basent sur une analyse de risques pendant laquelle l'ensemble des situations dangereuses (scénarios d'accident) est établi, en termes de gravité et de probabilité (fréquence) d'occurrence, afin d'en comparer la criticité à une valeur limite constituant l'objectif de sécurité à atteindre. Si cette criticité excède la valeur-seuil précitée, il sera alors nécessaire de la réduire. L'ampleur de cette réduction donne lieu à la définition de prescriptions globales de sécurité (phase 4) en termes de fonctions de sécurité et de prescriptions d'intégrité de sécurité (voir la définition de cette notion plus basse dans ce document) qui sont ensuite déclinées en prescriptions particulières de sécurité (phase 5) allouées aux différents moyens de réduction de risques (voir figure 6). Pour les SIS, ces prescriptions sont établies en termes de niveaux d'intégrité de sécurité (SIL requis) (voir figure 7). Plus la réduction de risque à réaliser est importante, plus le SIL est élevé. Ce constat souligne l'importance et le rôle capital que joue l'analyse de risques dans l'ensemble du cycle de vie. Nous allons plus loin donner quelques méthodes de détermination du SIL requis, telles décrites dans les références [CEI 61508-5, 2000] et [CEI 61511-1, 2003]. [12] [13]

2. Puis vient le cycle de vie inhérent au développement des moyens de réduction de risques (SIS, systèmes relatifs à la sécurité basés sur d'autres technologies, moyens externes de réduction de risques) : phases 9, 10 et 11. Comme nous l'avons déjà noté, la CEI 61508 ne considère que les spécifications relatives au développement des systèmes instrumentés de sécurité (phase 9).

3. Ces deux premières parties sont complétées par les phases d'installation et de validation globale de la sécurité, de fonctionnement et de modifications éventuelles, avec, le cas échéant, un retour à la phase adéquate du cycle de vie. Il convient de noter que CEI 61508 recommande l'adoption et la mise en application du cycle de vie de sécurité dans le système de management de la sécurité (SMS) de l'établissement concerné.

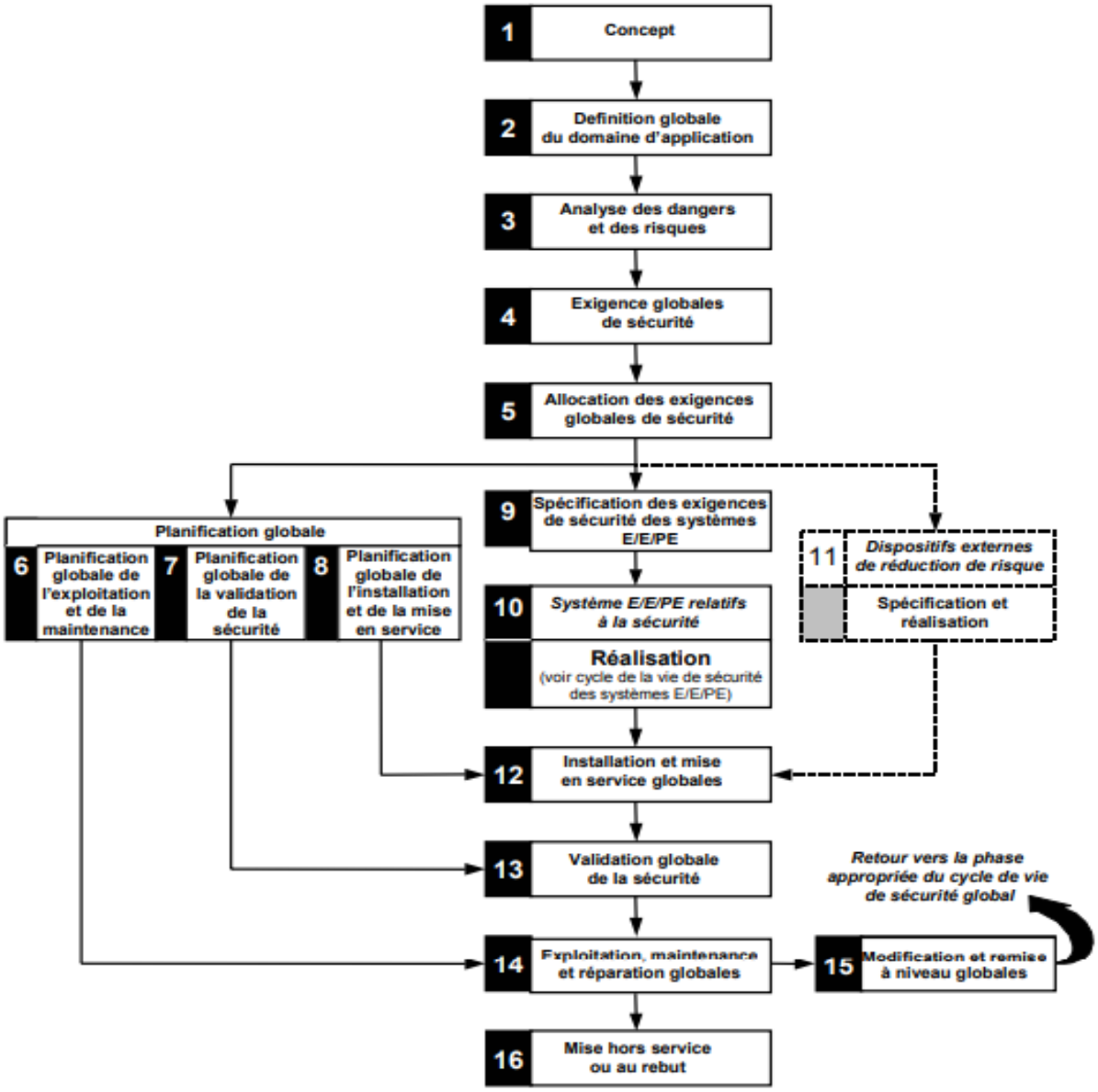


Figure 5 Cycle de vie de sécurité globale [IEC 61508-1]

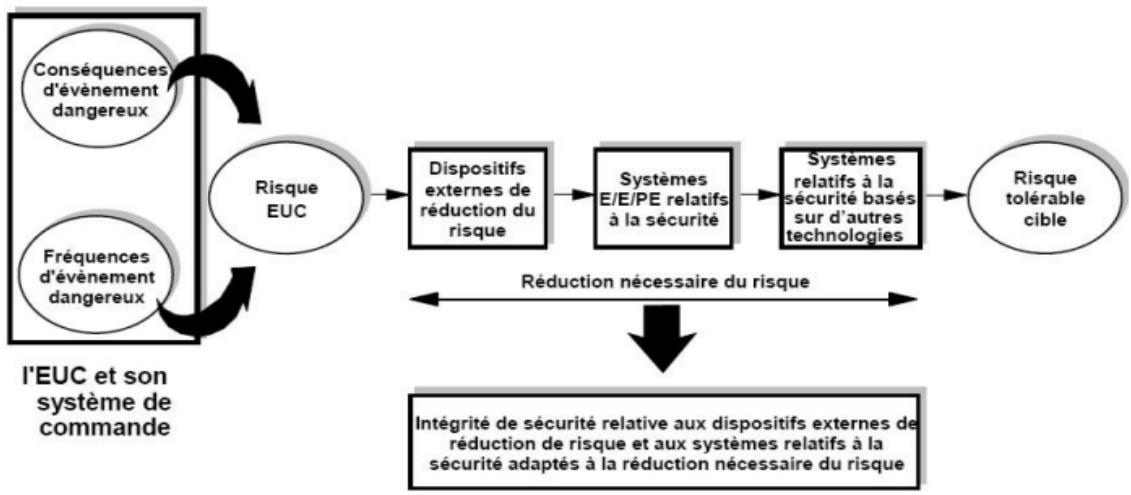


Figure 7 Concept de risque et d'intégrité de sécurité

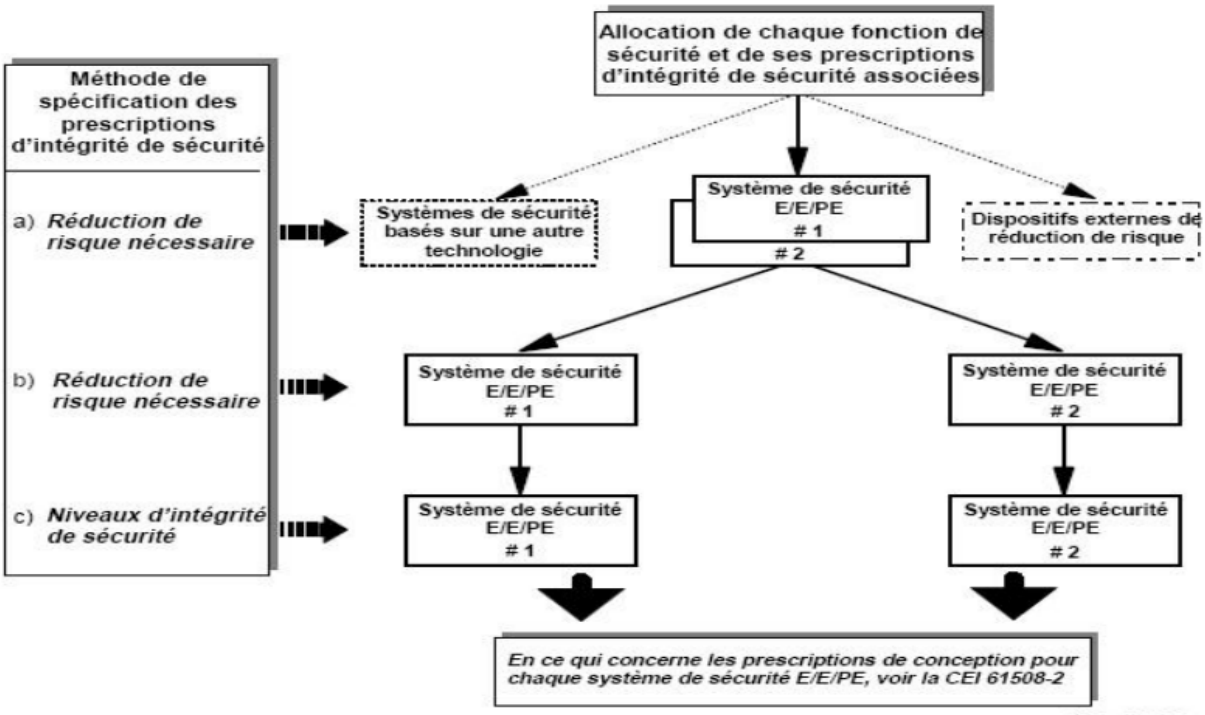


Figure 6 Allocation des prescriptions de sécurité aux systèmes de sécurité E/E/PE (SIS),

3. Système instrumenté de sécurité (SIS) :

3.1. Définition d'un SIS :

Un SIS, aussi appelé boucle de sécurité, est un ensemble d'éléments (matériel et logiciel) assurant la mise en état de sécurité des procèdes lorsque des conditions prédéterminées sont atteintes.

Pour la norme CEI 61508 [IEC 61508-4, 2002] définit les SIS comme suit : « un système E/E/PE (électrique/électronique/électronique programmable) relatifs aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité ».

La norme CEI 61511 [CEI 61511, 2003] définit, quant à elle, les systèmes instrumentés de sécurité comme « 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'unité loriquet(s) et d'élément(s) terminal (aux) ».

L'architecture type d'un SIS est donnée à la figure 4. Voici un descriptif succinct de chacune de ses parties :

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

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

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

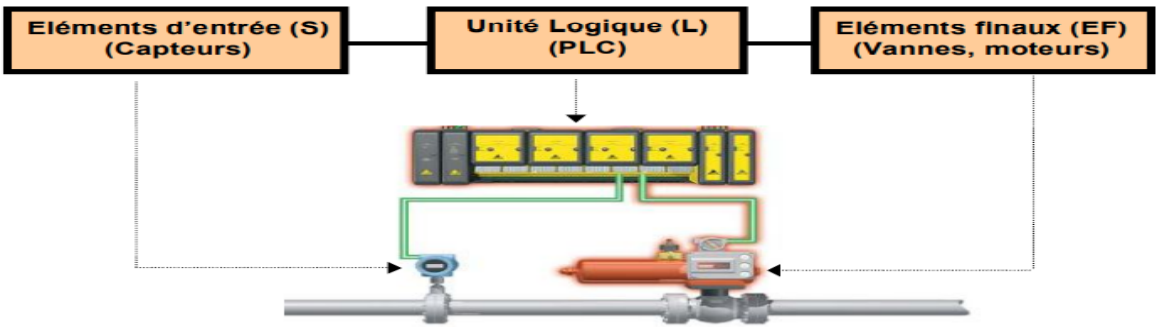


Figure 8 Système instrumenté de sécurité (SIS ou SRS E/E/PE)

3.2. Propriétés d'un SIS

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

- Les systèmes instrumentés de sécurité nécessitent une source d'énergie extérieure pour remplir leur fonction de sécurité.
- On retrouve tout ou partie de ces différents éléments pour constituer des chaînes de sécurité.
- Plusieurs capteurs ou actionneurs peuvent être reliés à une même unité de traitement.
- Toutes les combinaisons de capteurs, d'unité de traitement et d'actionneurs qui sont exigées pour accomplir des fonctions de sécurité sont considérées comme une partie de systèmes instrumentés de sécurité.
- Les capteurs, l'unité de traitement, les éléments finaux sont des équipements de sécurité et réalisent des sous-fonctions de sécurité. L'ensemble des sous-fonctions réalise la fonction de sécurité. [14]

3.3. Rôle des systèmes instrumentés de sécurité

Un système instrumenté de sécurité (SIS) met en œuvre les fonctions instrumentées de sécurité (SIF) exigées pour atteindre ou maintenir un état de sécurité du processus et, en tant que tel, contribue à la réduction de risque nécessaire afin de satisfaire au risque tolérable. Par exemple, la spécification des exigences de sécurité (SRS) peut stipuler que, lorsque la température atteint une valeur x, la vanne y s'ouvre pour laisser de l'eau pénétrer dans le récipient

3.4. Les modes de fonctionnement d'un SIS :

Le mode de fonctionnement concerne la façon dont une fonction de sécurité est prévue d'être utilisée par rapport à la fréquence des sollicitations dont elle fait l'objet et qui peut être :

– mode 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 où la fréquence des sollicitations n'est pas supérieure à une par an, (voir 7.4.6 de la CEI 61508-2).

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

– mode continu : la fonction de sécurité maintient l'EUC dans un état de sécurité en fonctionnement normal.

3.5. Fonction instrumentée de sécurité SIF :

Une SIF est définie pour obtenir un facteur de réduction du risque mise en œuvre pour un SIS. Lorsque le SIS est considéré comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une fonction de sécurité [15], [16].

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

Une fonction instrumentée de sécurité est à réaliser par un système instrumenté de sécurité (ou par une combinaison des composantes de ce système), par un système relatif à la sécurité basé sur une autre technologie ou par un dispositif externe de réduction de risque. [15]

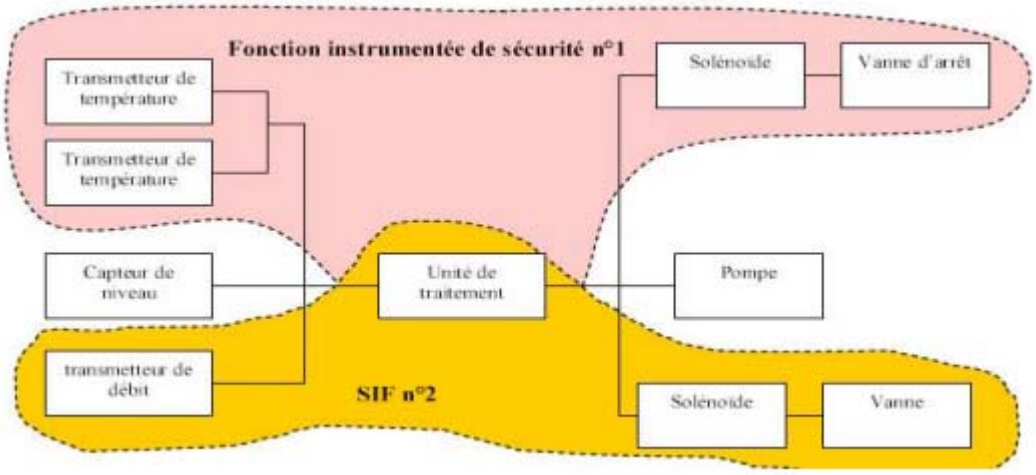


Figure 9 fonction instrumentée de sécurité

Pour illustrer et rendre plus claire cette définition, nous proposons l'exemple d'un équipement utilisé dans la fonction instrumentée de sécurité (Figure 9).

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

- Fermeture de la vanne pour arrêter l'alimentation du liquide.
- Arrêt de la pompe qui injecte le liquide dans le réservoir.

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

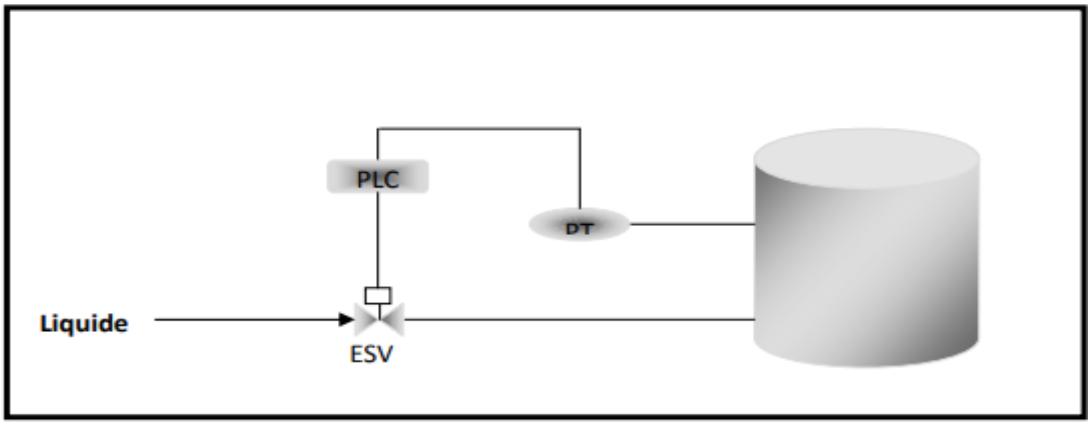


Figure 10 Exemple de fonction instrumentée de sécurité

3.6. Niveau d'intégrité de sécurité SIL :

Le SIL ou Safety Integrity Level est le niveau d'intégrité de sécurité. La notion de SIL découle directement de la norme IEC 61508. Le SIL peut se définir comme une mesure de la sûreté de fonctionnement qui permet de déterminer les recommandations concernant l'intégrité des fonctions de sécurité à assigner aux systèmes E/E/PE concernant la sécurité

Les normes de sécurité fonctionnelle IEC 61508 et IEC 61511 définissent une démarche d'analyse du niveau d'intégrité de sécurité (SIL) d'un système. Elles permettent de définir le niveau SIL qui doit être atteint par un SIS qui réalise la fonction de sécurité suite à une analyse de risque. Plus le SIL à une valeur élevée plus la réduction du risque est importante. Les SIS sont classés en quatre niveaux SIL qui se caractérisent par des indicateurs positionnés sur une échelle de un (01) à quatre (04) niveaux. Les niveaux SIL sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisées par des systèmes E/E/EP relatifs à la sécurité. Le SIL "quatre" désigne le degré de sécurité le plus élevé du fait de l'exigence forte de sécurité imposée et le niveau SIL "un" désigne l'exigence la plus faible.[17]

Classification retenue dans la norme CEI 61508

3.7. 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).
- 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 :

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

La défaillance systématique est définie par la même norme comme étant « défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés ». Lors de l'occurrence d'une telle défaillance, le système ne remplit plus la fonction qui lui est demandée, mais il ne présente aucune dégradation physique. C'est la raison pour laquelle ces défaillances sont qualifiées de non physiques ou de fonctionnelles (par exemple : l'opérateur ferme une vanne par erreur, la vanne dans ce cas n'est pas dégradée physiquement). Les défaillances systématiques peuvent être divisées en deux catégories :

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

La norme CEI 61508 considère que les défaillances du logiciel sont toutes systématiques. Par opposition aux défaillances aléatoires du matériel, les défaillances systématiques sont difficiles à modéliser et de ce fait moins compréhensibles. Cette classification de défaillances est résumée à la figure 11 :

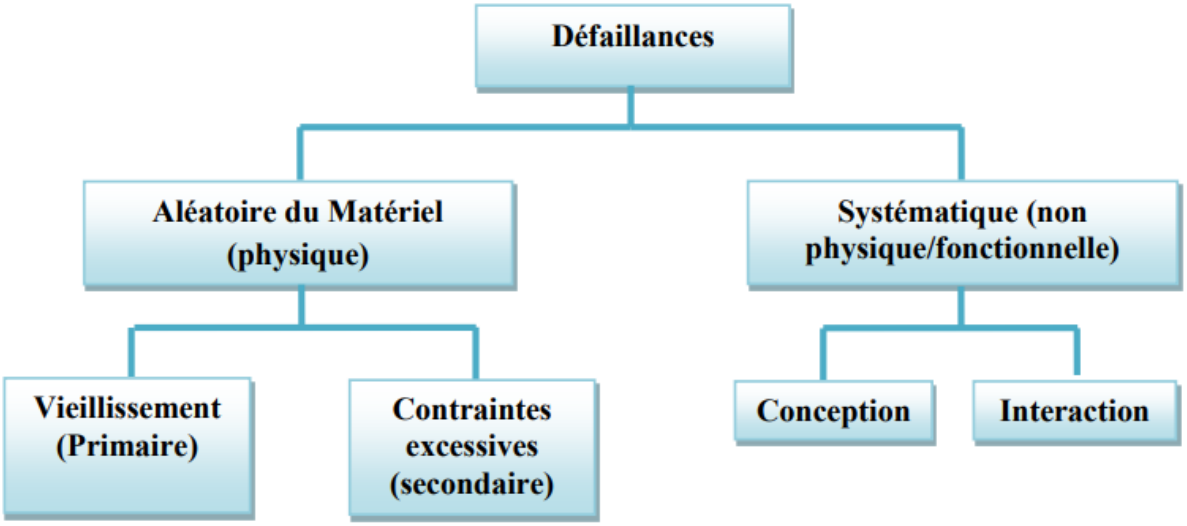


Figure 11 classification des défaillances selon leur causes

3.8. Classification des défaillances selon leurs effets sur la fonction de sécurité

Toutes les défaillances (aléatoires du matériel et systématiques), selon leurs effets, peuvent être classées dans l'une des deux catégories suivantes :

- Défaillances en sécurité (safe failures)
- Défaillances dangereuses (dangerous failures).

Suivant cette dernière classification, seules les défaillances aléatoires du matériel sont prises en compte dans ce qui suit. Dans ces conditions, les définitions de ces deux catégories selon la norme CEI 61508 [19] sont données ci-après :

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

En nous situant donc dans le contexte de la CEI 61508, une défaillance dangereuse est une défaillance qui tend à inhiber la fonction de sécurité en cas de demande émanant de l'EUC qui sera alors dans un état dangereux. Une défaillance sûre est une défaillance qui tend à anticiper le déclenchement de la fonction de sécurité, en l'absence de toute demande, en conduisant effectivement l'EUC dans un état sûr. C'est-à-dire tel que l'occurrence de tout événement dommageable n'y est plus possible.

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

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

Avec :

λ_S: taux de défaillance aléatoire en sécurité du matériel,

λ_D: taux de défaillance aléatoire dangereuse du matériel.

Une autre partition résulte du fait que ces défaillances peuvent être ou non détectées par des tests en ligne (tests de diagnostic). Les premières sont dénommées défaillances détectées (detected failures) et les secondes, qui ne peuvent être révélées que lors des tests périodiques hors ligne ou lors de la sollicitation du SIS par le système surveillé, sont dénommées défaillances non détectées (un-detected failures). Le schéma suivant est classiquement présenté pour résumer cette double partition [20].

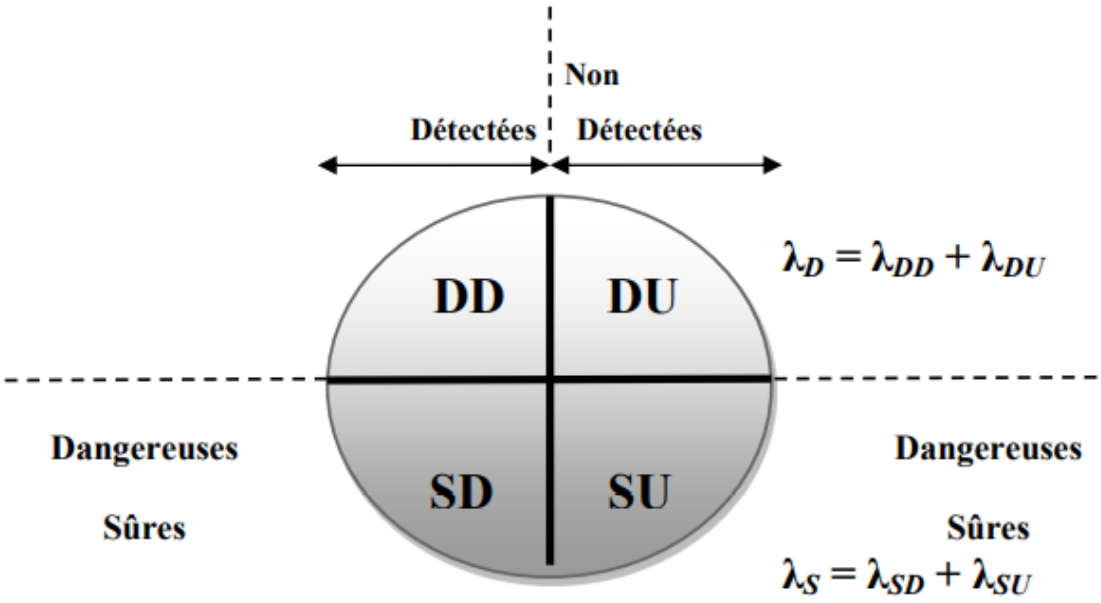


Figure 12 Typologie des défaillances selon la norme CEI 61508

4. Mesures cibles de défaillances :

Une fois le risque tolérable défini et la réduction nécessaire du risque estimée, les exigences d'intégrité de sécurité affectées au SIS, pour chaque fonction de sécurité, doivent être spécifiées (en termes de SIL) en fonction des mesures cibles de défaillances (voir tableau 1).

La notion de mesure cible de défaillances est désignée en matière de probabilité de défaillance dangereuse. Sa vocation diffère selon le mode de fonctionnement du système instrumenté de sécurité [21] :

4.1. Probabilité moyenne de défaillance :

Lors de l'exécution sur demande de la fonction spécifiée (PFDmoy), en mode demande faible. Ce mode de fonctionnement correspond à une fréquence de sollicitation du SIS inférieure ou égale à 1 an-1 et également inférieure ou égale au double de la fréquence des tests périodiques auxquels il est soumis [22].

4.2. Probabilité d'une défaillance dangereuse par heure (PFH) :

En mode demande élevée ou en mode continu. Ce second mode correspond à une fréquence de sollicitation du SIS supérieure à 1 an-1 ou supérieure au double de la fréquence des tests périodiques mentionnés précédemment [22]

Une analyse détaillée concernant les modes de fonctionnement d'un SIS est donnée dans la référence [23].

Les valeurs numériques des mesures cibles de défaillances, en fonction du mode d'opération du SIS, correspondantes aux niveaux d'intégrité de sécurité sont présentées au tableau 1.

Tableau 1 Niveaux d'intégrité de sécurité (SIL) en fonction des mesures cibles de défaillances

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

4.3. Taux de défaillance

Paramètre de fiabilité ($\lambda(t)$) d'une entité (composants ou systèmes simples) tel que $\lambda(t).dt$ est la probabilité de défaillance de cette entité comprise dans les limites [t, t+dt], à condition qu'aucune défaillance ne se soit produite pendant [0, t]

D'un point de vue mathématique, $\lambda(t)$ est la probabilité conditionnelle de défaillance par unité de temps pendant [t, t+dt]. Elle est en relation étroite avec la fonction de fiabilité (c'est-à-dire la probabilité d'aucune défaillance de 0 à t) par la formule générale

$R(t) = exp(-\int_0^1 \lambda(\tau)d\tau$. Inversement, elle est définie à partir de la fonction de fiabilité par

$$\lambda(t) = -\frac{dR(t)}{dt} \text{ x} \frac{1}{R(t)}$$

5. Réduction de risque nécessaire

La réduction de risque nécessaire) est la réduction du risque qui doit être réalisée pour atteindre l'objectif de risque tolérable dans une situation spécifique (qui peut être définie soit qualitativement soit quantitativement). Le concept de réduction de risque nécessaire est d'une importance fondamentale dans la réalisation de la spécification des exigences de sécurité pour les systèmes E/E/PE relatifs à la sécurité (en particulier, les exigences d'intégrité de sécurité qui font partie de la spécification des exigences de sécurité). La détermination du risque tolérable pour un événement dangereux spécifique a pour but d'établir ce qui est jugé raisonnable compte tenu de la fréquence (ou probabilité) de l'événement dangereux et de ses conséquences spécifiques. Les systèmes relatifs à la sécurité sont conçus pour réduire la fréquence (ou probabilité) de l'événement dangereux et/ou les conséquences de l'événement dangereux.

6. Les méthodes d'allocation et de vérification des SIL :

L'allocation des SIL est établi a partir de certaines méthodes permettant de définir le niveau d'intégrité de sécurité (SIL) requis pour une fonction de sécurité. C'est le SIL qui doit être atteint par un SIS afin de réaliser la réduction nécessaire du niveau de risque. La section suivante donne un aperçu des méthodes, telles que présentées dans les normes CEI 61508 et CEI 61511, de détermination du niveau d'intégrité de sécurité (SIL) correspondant à un phénomène dangereux spécifié (scénario d'accident) lors de la phase d'analyse des risques. Elles sont plus ou moins adaptées en fonction du niveau de détail des analyses de risques réalisées (type et détail des informations disponibles). La CEI 61508, dans sa partie 5, et la CEI 61511 décrivent deux types de méthodes : qualitatives et quantitatives.[24]

6.1. Méthodes qualitatives :

La norme CEI 61508 reconnaît qu'une approche quantitative pour déterminer le niveau d'intégrité de sécurité (SIL) d'une fonction instrumentée de sécurité (SIF) n'est pas toujours possible et qu'une approche alternative pourrait parfois être appropriée. Cette alternative consiste en un jugement qualitatif. Quand une méthode qualitative est adoptée, un certain nombre de paramètres de simplification doivent être introduits. Ils permettent de qualifier le phénomène dangereux (accident)

en fonction des connaissances disponibles. Les normes CEI 61508 et 61511 présentent deux méthodes qualitatives.

6.1.1. Le graphe de risque

Cette méthode a été introduite par la norme allemande DIN V 19250 [25], afin de pouvoir exprimer le risque sous forme de classes. La démarche est fondée sur l'équation caractérisant le risque (R) sans considérer les moyens instrumentés de sécurité : R= f. C, où f et C sont respectivement la fréquence et la conséquence de l'événement dangereux en l'absence de SIS. La fréquence de l'événement dangereux f est généralement composée de trois facteurs :

- F : la fréquence et la durée d'exposition aux dangers,
- P : la possibilité d'éviter l'événement dangereux,
- W : la probabilité de l'occurrence de l'événement dangereux sans moyen de protection (probabilité de l'occurrence non souhaitée). La combinaison des quatre paramètres précédents (C, F, P, W) peut ramener à une configuration comparable à celle présentée à la figure 13 [21]

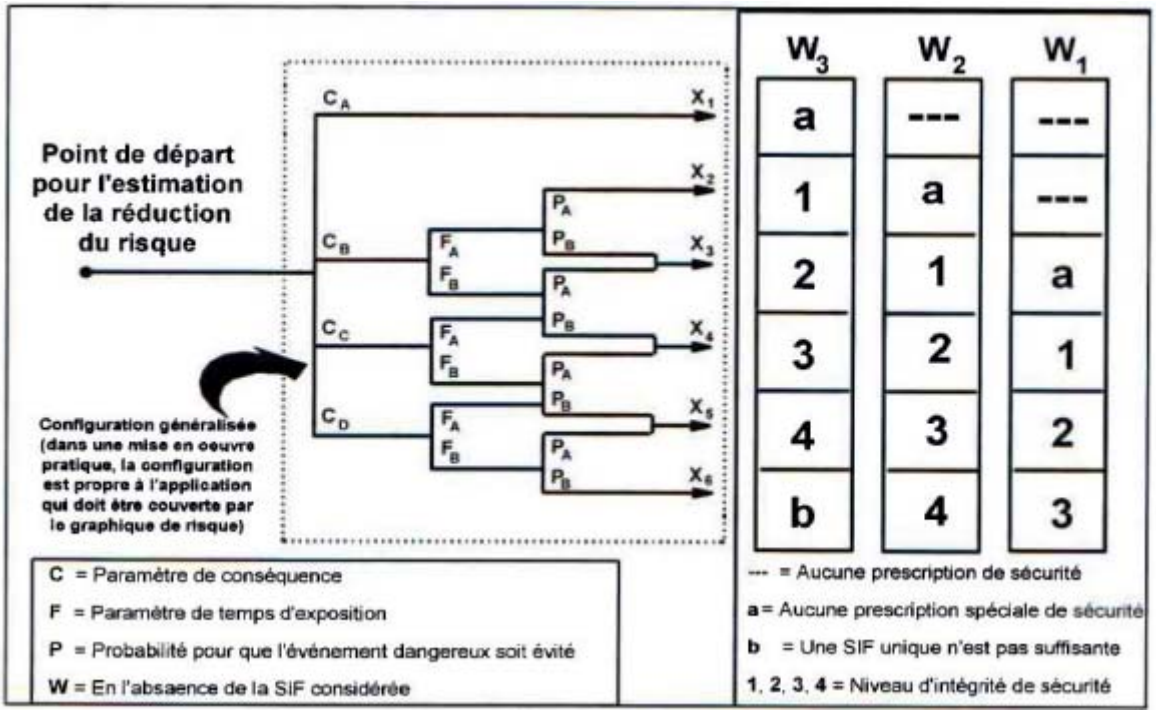


Figure 13 schéma général du graphe des risques

Le diagramme de risque associe des combinaisons particulières des paramètres de risque aux niveaux d'intégrité de sécurité requis pour la fonction de sécurité instrumentée en prenant en compte le risque tolérable associé au phénomènes dangereux. Les paramètres (C, F, P, W) et leur pondération doivent être précisément définis pour chaque situation dangereuse. Une phase de calibrage ou d'étalonnage du graphe de risque est nécessaire. Elle permet d'adapter les paramètres en prenant en compte les spécificités de l'entreprise, la réglementation et les normes du secteur d'application.

Tableau 3 description des paramètres du graphe de risque pour les industries de transformation

Paramètre		Description
Conséquence	C	Nombre d'accidents mortels et/ou de lésions graves susceptibles de se produire suite à l'occurrence de l'événement dangereux. Ce paramètre est déterminé en calculant les nombres dans la zone exposée lorsque la zone est occupée en tenant compte de la vulnérabilité à l'événement dangereux.
Occupation	F	Probabilité que la zone exposée soit occupée au moment où l'événement dangereux se produit. Ce paramètre est déterminé en calculant la fraction de temps durant laquelle la zone est occupée au moment où se produit l'événement dangereux. Cela peut tenir compte de la possibilité d'avoir une augmentation de la probabilité que des personnes soient présentes dans la zone exposée, afin de déterminer les situations anormales qui peuvent exister au moment de l'apparition de l'événement dangereux (vérifier aussi si cela modifie le paramètre C).
Probabilité que le danger soit évité	P	Probabilité que des personnes exposées puissent éviter la situation dangereuse qui existe en cas de défaillance de la fonction instrumentée de sécurité (SIF) sur sollicitation. Cela dépend de la présence de méthodes indépendantes utilisées pour avertir les personnes exposées au danger avant que le danger ne se produise, ainsi que de la présence de méthodes d'évacuation.
Taux de sollicitation	W	Nombre de fois par an où l'événement dangereux se produirait en l'absence de la SIF à l'étude. Ce paramètre peut être déterminé en tenant compte de toutes les défaillances pouvant provoquer l'événement dangereux et en évaluant le taux global d'occurrence. Il convient d'inclure d'autres couches de protection à l'étude.

6.1.2. Matrice de gravite (matrice de risque, matrice des couches de protection) :

Cette méthode est similaire à la précédente. Elle est utilisée lorsque la fréquence du risque ne peut être quantifiée d'une manière précise. L'analyse débute toujours par l'identification des dangers et leur estimation (fréquence et gravité). Après avoir identifié les différentes couches de protection (chaque couche de protection doit réaliser une réduction d'un ordre de grandeur de SIL (un facteur de 10)), la nécessité d'une couche de protection SIS supplémentaire peut être établie en comparent le risque résiduel au niveau de sécurité cible. Ainsi le niveau d'intégrité de sécurité du SIS peut être déterminé. Cette méthode suppose l'indépendance des couches de protection. Ces considérations conduisent à la matrice de gravité tridimensionnelle illustrée à la figure 14 [22].

Avec :

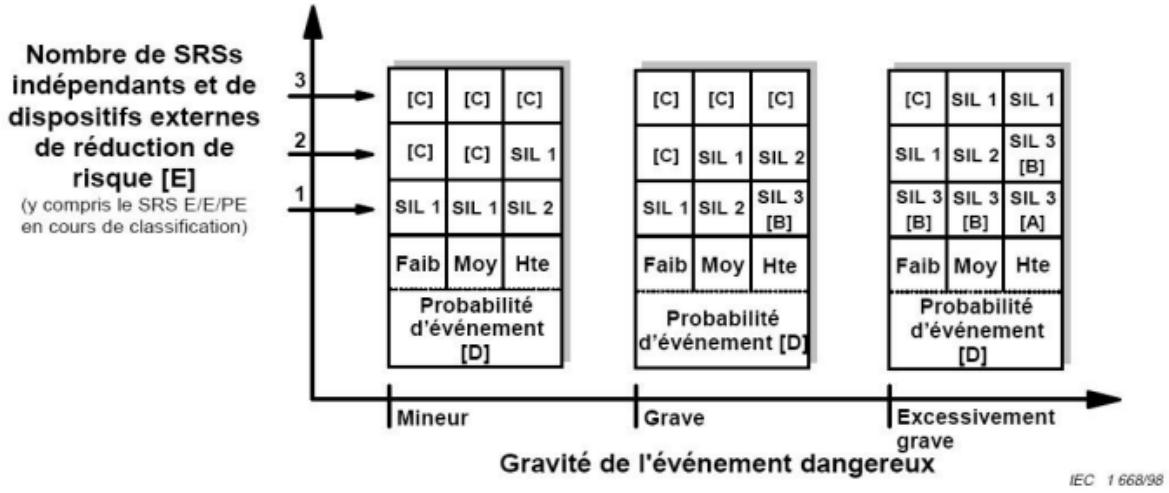


Figure 14 exemple de matrice de gravité

- **[A]** Un SRS E/E/PE SIL3 n'apporte pas une réduction suffisante de risque à ce niveau de risque. Des mesures supplémentaires de réduction de risque sont nécessaires.

- **[B]** Un SRS E/E/PE SIL3 peut ne pas apporter une réduction suffisante de risque à ce niveau de risque. L'analyse des risques et des dangers est requise pour déterminer si des mesures supplémentaires de réduction de risque sont Nécessaires.

- **[C]** Un SRS E/E/PE n'est probablement pas nécessaire.

- **[D]** La probabilité d'événement est la probabilité que l'événement dangereux survienne sans système relatif à la sécurité ou sans dispositif externe de réduction de risque.

- **[E]** La probabilité d'événement et le nombre total de couches de protection indépendantes sont définis en relation avec l'application spécifique.

6.1.3. L'analyse des risques par la méthode HAZOP :

- **Définition :**

La méthode d'analyse HAZOP « Hazard and Operability Studies » est parmi les approches les plus communes pour les analyses des risques, utilisée pour investiguer sur les déviations des paramètres des processus.

L'analyse HAZOP est particulièrement indiquée aux analyses des opérations et des processus qui sont réalisés dans les installations industrielles.

Un aspect particulier des analyses HAZOP est le fait qu'elle est développée par une équipe multidisciplinaire qui réunit ses propres connaissances avec un travail de « brainstorming ».

- **Objectif :**

L'objectif de l'étude HAZOP est de :

- Enquêter sur les dangers et sur les caractéristiques d'opérabilité qui peuvent créer un risque aux gens, aux biens et à l'environnement et garantir que les sauvegardes appropriées et les procédures soient exécutées pour prévenir ou atténuer les accidents ;

- Recherche systématique des causes possibles de dérive de tous les paramètres de fonctionnement d'une installation ;

- Mise en évidence des principaux problèmes d'exploitation et d'entretien ;

- Étude des conséquences et risques éventuels liés à ces dérives ;

- Proposition des mesures correctives appropriées.

Les lignes guide de l'application de l'HAZOP sont reportées et traitées aussi dans **la norme IEC 61882.**

5.1.2.2. MISE EN ŒUVRE DE LA METHODE

a) SELECTION DES NŒUDS

La sélection des Nœuds a été définie sur la base des (P&ID) plans d'instrumentation et diagramme et (PFD) plan de circulation de fluide sont représenté dans la partie pratique.

Le nœud sélectionné : Alimentation du hall d'emplissage en Propane

b) PARAMETRES ET MOTS-CLES

- **Paramètres :**

La méthode HAZOP fait appel à des paramètres spécifiques qui s'expriment par de simples mots (noms ou verbes) caractéristiques de l'intention de la conception et que l'on peut définir ainsi :

« Grandeur physiquement mesurable, action ou opération à réaliser ».

Les paramètres utilisés dans cette étude sont :

Pression, débit, température, niveau, fuite.

- **Mots-clés :**

Liste des mots-clés utilisés (keywords) :

- Débit : Plus de, Pas de
- Pression/Température : Haute, Basse
- Niveau : plus de, moins de

c) Etudes de déviation :

La combinaison de mots-clés et de paramètres va constituer une dérive, ou déviation, de ce paramètre :

MOT CLÉ + PARAMÈTRE = DÉVIATION

Par exemple :

- Plus/pas de débit
- Haute/basse pression
- Haute/basse Température

a) CAUSES DE LA DEVIATION

Les causes des déviations sont les raisons ou problèmes pour lesquels ces déviations ont lieu.

b) CONSEQUENCE DES DEVIATIONS

Les conséquences des déviations sont les résultats de ces déviations, mais peuvent aussi être les résultats de la cause elle-même.

c) ESTIMATION ET EVALUATION DES RISQUES

L'estimation du risque nécessite la quantification de la probabilité d'occurrence de l'événement redouté (l'accident), ainsi que celle de la gravité des effets engendrés par cet événement.

- **<u>Echelle de fréquence ou de probabilité :</u>**

Tableau 2 Echelle de fréquence ou de probabilité

	Fréquences/ Probabilité	**Explication**
1	**Possible mais extrêmement peu probable**	N'est pas impossible au vu des connaissances actuelles mais non rencontré au niveau mondial sur un très grand nombre d'années.

2	**Très improbable**	S'est déjà produit dans ce secteur d'activité mais a fait l'objet de mesures correctives réduisant significativement sa probabilité.
3	**Improbable**	S'est déjà produit dans secteur d'activité ou dans ce type d'organisation au niveau mondial, sans que les éventuelles corrections intervenues depuis apportent une garantie de réduction significative de sa probabilité.
4	**Probable**	S'est déjà produit et/ou peut se reproduire pendant la durée de vie de l'installation.
5	**Courant**	S'est produit sur site considéré et/ou peut se produire à plusieurs reprises pendant la durée de vie de l'installation malgré d'éventuelles mesures correctrices.

Gravité des conséquences

Tableau 3 Echelle de gravité

	Niveau de gravité	**Evaluation du nombre de personnes potentiellement impactées par les effets létaux**
1	**Modéré**	Aucune personne exposée.
2	**Sérieux**	Au plus 1 personne exposée.
3	**Important**	Entre 1 et 10 personnes exposées.
4	**Catastrophique**	Entre 10 et 100 personnes exposées.
5	**Désastreux**	Plus de 100 personnes exposées.

d) Grille de criticité (Matrice des Risques)

Lorsque le risque dépend de la probabilité de produire des dommages, et des effets indésirables, il peut être classé qualitativement par catégorie, utilisant une matrice de risque.

Une matrice de risque peut alors déterminer les critères d'acceptabilité du risque et identifier les événements acceptables et ceux non acceptables, ou ceux qui exigent des évaluations plus détaillées.

6.2. Méthodes quantitatives :

Ces méthodes sont les plus rigoureuses et les plus précises. L'estimation quantitative de la fréquence de l'événement dangereux (redouté) en constitue la base. La mise en œuvre d'une méthode quantitative nécessite les éléments suivants :

- La mesure cible de sécurité (fréquence tolérable d'accident : Ft) doit être spécifiée de façon numérique (par exemple, une conséquence donnée ne devrait pas se produire avec une fréquence supérieure à 1/10000 ans).

- La réduction du risque peut être définie numériquement. Ceci suppose la disponibilité des données numériques suivantes :

- La fréquence de l'événement initiateur : FEI. Elle peut être obtenue en utilisant le retour d'expérience, le jugement d'expert ou encore en utilisant des méthodes de prédiction appropriées (AdD, Chaînes de Markov, etc.).

- Les probabilités de défaillances des couches de protection : **PFD**

La méthode quantitative la plus utilisée pour l'allocation des niveaux d'intégrité de sécurité est celle fondée sur principe d'analyse par couches de protection (**LOPA** : Layers Of Protection Analysis),. [24] [26].

6.2.1. Arbres de défaillance :

La méthode des arbres de défaillance est l'une des méthodes les plus utilisées dans les analyses des performances des SIS [27], [28]. Elle a pour objectif le recensement des causes entrainant l'apparition de l'événement indésirable d'un système et le calcul de sa PFDavg. Elle constitue un moyen de représentation de la logique des défaillances, cette méthode est adaptée aussi pour l'étude des systèmes élémentaires présentant des défaillances de mode commun. L'arbre de défaillances est une méthode déductive, qui commence par l'événement indésirable et détermine ses causes. L'analyse par l'arbre de défaillances nécessite deux phases ; une qualitative, où on détermine la fonction logique du système en termes de l'ensemble de ses coupes minimales, et l'autre est dite quantitative, où on calcule la probabilité d'occurrence de l'événement indésirable (sommet). L'évaluation quantitative de la probabilité de l'événement sommet qui représente la non fiabilité du système lorsque cet évènement est la défaillance d'un système non réparable [29], [30]. La méthode de l'arbre de défaillances consiste µa rechercher toutes les combinaisons possibles d'événements entraînant la réalisation de l'évènement indésirable. On représente graphiquement ces combinaisons au moyen d'une structure arborescente dont l'évènement non désiré est le sommet (ou racine). Pour décrire la relation entre les événe-

ments et la logique d'un système, l'arbre de défaillances utilise des portes logiques. Ces portes indiquent les types des évènements et les types de relation qui sont impliquées. L'arbre de défaillances peut mener à des évaluations quantitatives de la probabilité d'occurrence de l'évènement indésirable qui représente la non fiabilité lorsque cet évènement est la défaillance d'un SIS non réparable [31], [32].

6.2.2. LOPA (Layers Of Protection Analysis)

Elle a été développée à la fin des années 1990 par le CCPS (Centre for Chemical Process Safety) [CCPS, 2001]. Cette méthode intègre toutes les couches de protection de l'installation, tant organisationnelles que techniques. Elle évalue la réduction du risque en analysant la contribution des différentes couches [LANTERNIER ET ADJADJ, 2008]. Son principe, rappelons-le, est d'estimer le risque résiduel, exprimé en fréquence d'accident, en quantifiant la fréquence de l'événement initiateur et les probabilités (moyennes) de défaillance sur demande de chaque couche. Ces couches peuvent être de prévention (diminution de la fréquence de l'occurrence de l'évènement dangereux) ou de protection (réduire les impacts de l'événement dangereux). Une condition majeure qui doit être satisfaite est l'indépendance des différentes couches de protection (IPL : Independant Protection Layers).

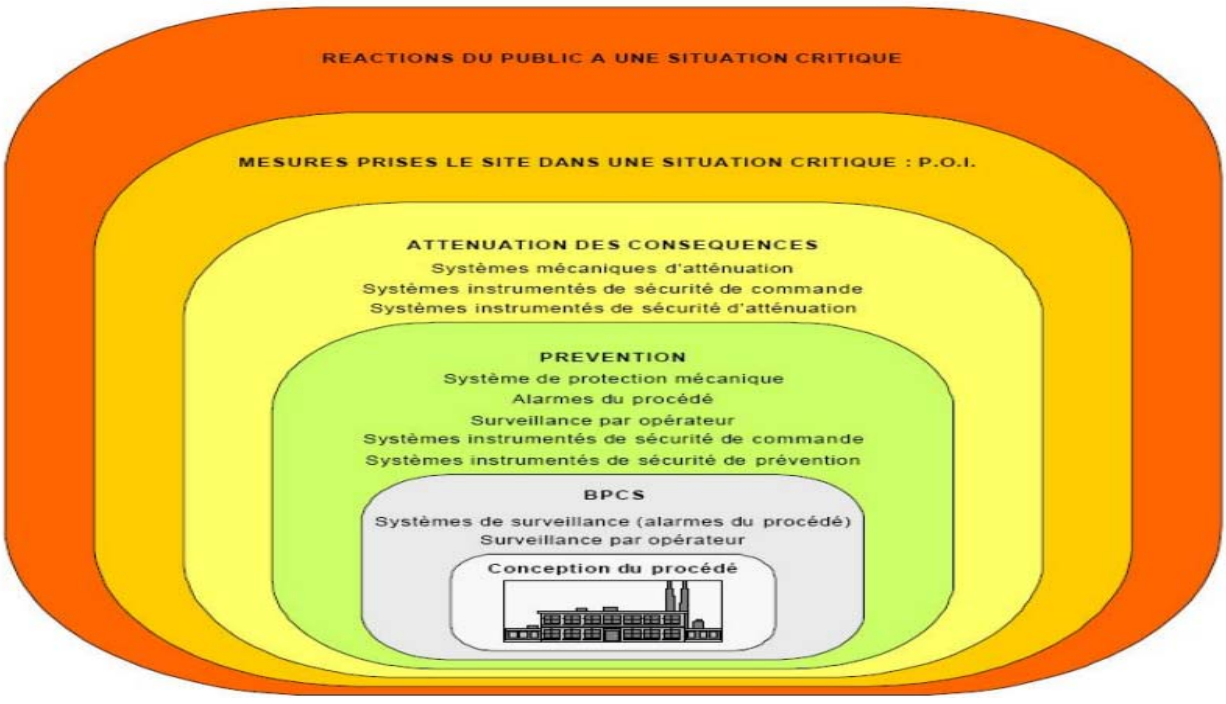


Figure 15 Concept d'analyse par couches de protection (LOPA)

6.2.3. Chaines de Markov :

Les chaines de Markov apportent une bonne formalisation de tous les états que peuvent prendre les systèmes en fonction des événements rencontrés (défaillance, réparation, . . .) et des paramètres étudiés (taux de défaillance, défaillance de cause commune,. . .) [33]. Les chaines de Markov apportent une finesse de modélisation pertinente au regard du comportement des SIS étudiés notamment les SIS faiblement sollicités et périodiquement testés [34]. Compte tenu de la relative complexité des SIS, l'explosion combinatoire du nombre des états est l'inconvénient majeur des chaines de Markov. Cet inconvénient est généralement surmontable. L'évaluation de la performance du SIS est obtenue grâce à une chaine de Markov synthétique représentant les différents états du SIS tout en tenant compte des différents types de défaillance. Elle permet de déterminer la probabilité de défaillance à la demande du SIS et de calculer sa valeur moyenne par intégration dans le temps. La détermination du niveau de sécurité du SIS est obtenue par référence aux données du tableau 1.1, [34], [35]. La méthode des chaines de Markov est souvent utilisée pour analyser et évaluer les per- formances des systèmes réparables et avec des composants à taux de défaillance constant. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et à chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une action de réparation. Elle permet ainsi de faire une analyse dynamique du système. Dans l'évaluation des performances des systèmes par les chaines de Markov on utilise le processus d'analyse constitué de trois parties. La première partie est consacrée au classement de tous les états du système en états de fonctionnement, états dégradés ou états de panne. La deuxième partie concerne la détermination de toutes les transitions possibles entre ces différents états, tout en tenant compte des actions de réparations. Enfin on calcule les probabilités de se trouver dans les différents états du système étudié. [M RABAH]

7. Choix de la méthode pour la détermination du niveau exigé d'intégrité de sécurité :

La méthode choisie pour une application spécifique dépendra de plusieurs facteurs, parmi lesquels :

- La complexité de l’application ;
- Les lignes directrices émanant des autorités compétentes ;
- La nature du risque et la réduction de risque exigée ;
- L’expérience et les compétences des personnes disponibles pour réaliser ce travail ;

- Les informations disponibles concernant les paramètres relatifs au risque (voir la Figure 14) ;
- Les informations disponibles sur les SIS actuellement utilisées dans les applications particulières, notamment celles décrites dans les normes et pratiques industrielles.

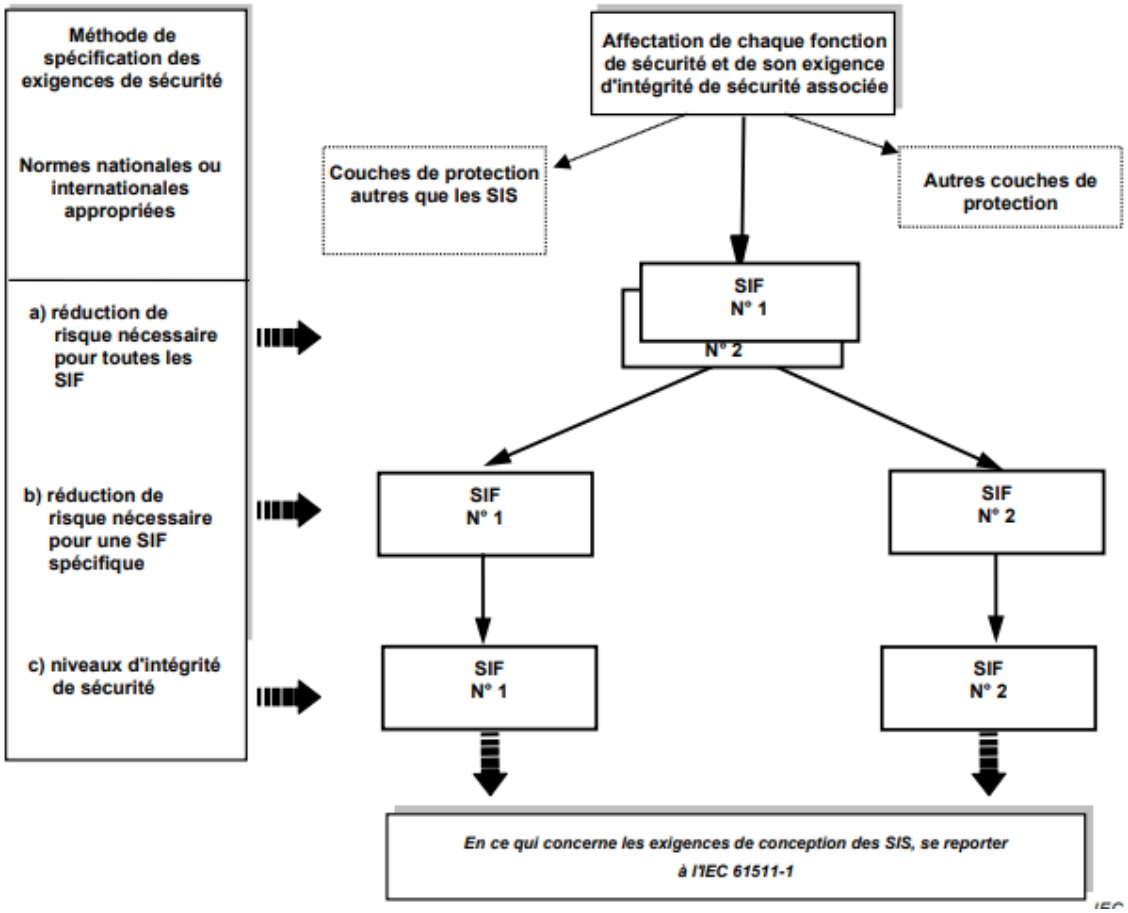


Figure 16 Affectation des exigences de sécurité aux couches de protection

8. Conclusion

Au cours du premier chapitre nous avons d'abord rappelé les définitions des termes fondamentaux du domaine de la sécurité afin de lever, si possible, toute ambiguïté quant à la signification que nous leur accordons dans la suite de ce PFE. Nous avons ensuite présenté l'ensemble des normes qui discutent les systèmes instrumentés de sécurité (norme CEI 61508 et ses normes sectorielles). Il convient à cet effet de rappeler que la CEI 61508 de même que ses normes filles sont actuellement devenues la référence par excellence pour la mise en œuvre de ce type de systèmes. Puis nous avons donné une synthèse sur les concepts et définitions relatifs aux SIS et nous avons cité les différentes méthodes d'allocation et de vérification de SIL. Ceci, est considéré comme une initiation pour passer

vers une généralité sur le système de détection gaz et flamme qui va être résumée au cours du prochain chapitre.

Chapitre II :

Système De détection feu & gaz

1. Introduction :

Les systèmes Feu & Gaz sont conçus pour surveiller les conditions environnementales et détecter les variations pouvant être associées à un début d'incendie ou à une fuite de gaz. La plupart du temps, le système F&G est formé d'un ou plusieurs panneaux de contrôle dont chacun est interconnecté avec des détecteurs de terrain, des unités de signalisation et des actionneurs. Les fonctions qu'un système F&G est normalement appelé à exécuter sont celles de surveillance, d'avertissement, de déclenchement et d'actionnement.

La fonction de surveillance a lieu entre le panneau et les détecteurs et vise à détecter toute variation environnementale pouvant être associée à une condition anormale. C'est le cas lors de la détection de la présence de fumée, de chaleur, de flamme ou de gaz combustible ou toxique dans la zone surveillée. Une autre fonction de surveillance est également présente entre le panneau et l'instrumentation distribuée dans la zone pour surveiller l'état des systèmes de lutte contre l'incendie tels que la pression d'eau ou de gaz, les positions des vannes, les activations du système, etc. La fonction d'avertissement est réalisée à l'intérieur du panneau et de l'unité de signalisation située dans la zone surveillée ainsi qu'à l'intérieur du panneau et de la salle principale d'incendie ou de contrôle. Cette fonction concerne la distribution de signaux d'avertissement dans la zone surveillée anticipant la formation d'une condition menaçante. La même chose est répétée dans la salle de contrôle où les opérateurs de l'usine surveillent le processus. [36]

Avant d'entamer les différents types de détecteur de feu et gaz il est nécessaire de commencer par un petit aperçu sur quelques accidents de propane parmi les plus désastreux afin de mettre en contexte le rôle des détecteurs

2. Accidentologie :

2.1. Accident N 01 : le 25/12/2000 aux ETATS-UNIS

Un réservoir de 2 m³ de propane explose dans une installation entreposant du gaz liquéfié. A priori, il s'agit d'un BLEVE qui n'a pas fait de blesser, la plupart du personnel étant en congé de fin d'année. Les secours se tiennent à bonne distance afin de prévenir de nouvelles explosions. Ils sont cependant rappelés sur place à 3 reprises pour éteindre des nouveaux départs de feu.

2.2. Accident N 02 : le 14/08/2008 en FRANCE

Dans un centre de distribution de combustibles gazeux, 2 soupapes de sécurité (tarage 5,4 bar) se déclenchent vers 9 h à la suite d'une surpression sur une sphère de butane de 1 000 m³ consécutive à un transfert de propane dans l'équipement à partir d'un camion-citerne contenant 21 t de gaz. Les soupapes évacuent ainsi à l'atmosphère un mélange gazeux de propane et butane. Le "soulèvement" simultané des 2 soupapes d'une durée de quelques secondes fait chuter la pression de la sphère en dessous de leur pression de tarage. Une des soupapes se referme correctement mais la seconde, mal repositionnée sur son siège en se refermant, maintient une fuite de mélange gazeux propane et butane durant environ 10 minutes, temps nécessaire à l'opérateur pour isoler la soupape défaillante. Le POI est déclenché vers 9h08. Les relevés d'atmosphère explosive effectués sur le site et à l'extérieur se révèlent négatifs. Aucune dégradation de l'installation n'est constatée. La soupape défaillante, qui avait été contrôlée en mai 2008, est remplacée. L'exploitant évalue la masse du mélange gazeux rejeté à 1 t maximum ; le coût de la perte de gaz est estimé à 1 500 euros. Une erreur humaine lors de l'ouverture des vannes (ligne butane au lieu de celle du propane), après raccordement du camion au poste mixte de déchargement (butane / propane), est à l'origine de la surpression. A la suite de l'accident, un contrôle des connaissances de l'opérateur qui est expérimenté (8 ans d'expérience) est réalisé. La procédure de dépotage est modifiée. Une réflexion est également menée pour identifier les mesures techniques et d'alerte à mettre en œuvre. L'exploitant envisage ainsi la mise en place de pressostats de pression haute sur stockage avec asservissement de la pomperie et alerte sonore.

3. Généralités :

3.1. Définition d'un système feu & gaz :

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

3.2. 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.

3.3. 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 assumée 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

4. 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 déterminé (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....

4.1. Les types de détecteurs :

4.1.1. Détecteur optique de flamme :

Les détecteurs optiques de flammes, réagissent aux rayonnements émis par tous types de flammes. Ils sont élaborés pour prévenir très rapidement (en quelques dizaines de millisecondes) tout départ de feu par le biais de signaux numériques.

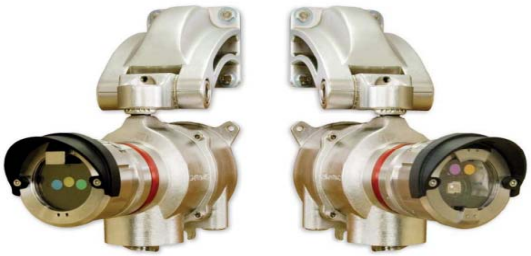


Figure 17 détecteur optique de flamme

1.1.1.1. 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)., un détecteur de flammes fonctionne généralement connecter à une centrale de détection gaz.

1.1.1.2. 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 CO2 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). Requiert 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.

4.2. 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 frigorigènes).

Figure 18 détecteur ponctuel infrarouge de gaz

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 la de communication numérique. Pour chaque type de gaz, il existe une technologie spécifique de cellule, garantissant la précision et la répétitivité des mesures …

5. Commande (Traitement) :

Cela est effectué par un système spécifique fourni par le fabricant **central de détection**.

5.1. Centrale de détection :

5.1.1. 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.

La centrale de détection constitue l'élément le plus important d'une installation fixe de détection de Gaz. Elle assure une surveillance continue est permanente et génèrent les actions en cas de détection de Gaz : signalisation, asservissements, télétransmission d'alarme.

Le système est équipé d'un afficheur graphique permettant de visualiser les informations sur les points de mesure.

Figure 19 centrale de détection (système MX62)

5.1.2. 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 Address and General Alarm : annonce vocale et alarme générale) (si nécessaire).
- Déterminer au sein de leur logique les actions à mettre en œuvre Interfacer avec les autres processeurs (système ESD, DCS, PLC de traitement,).
- Autoriser le blocage et la dérivation pour les tests et la maintenance.

6. 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)

7. Architecture d'un système F&G :

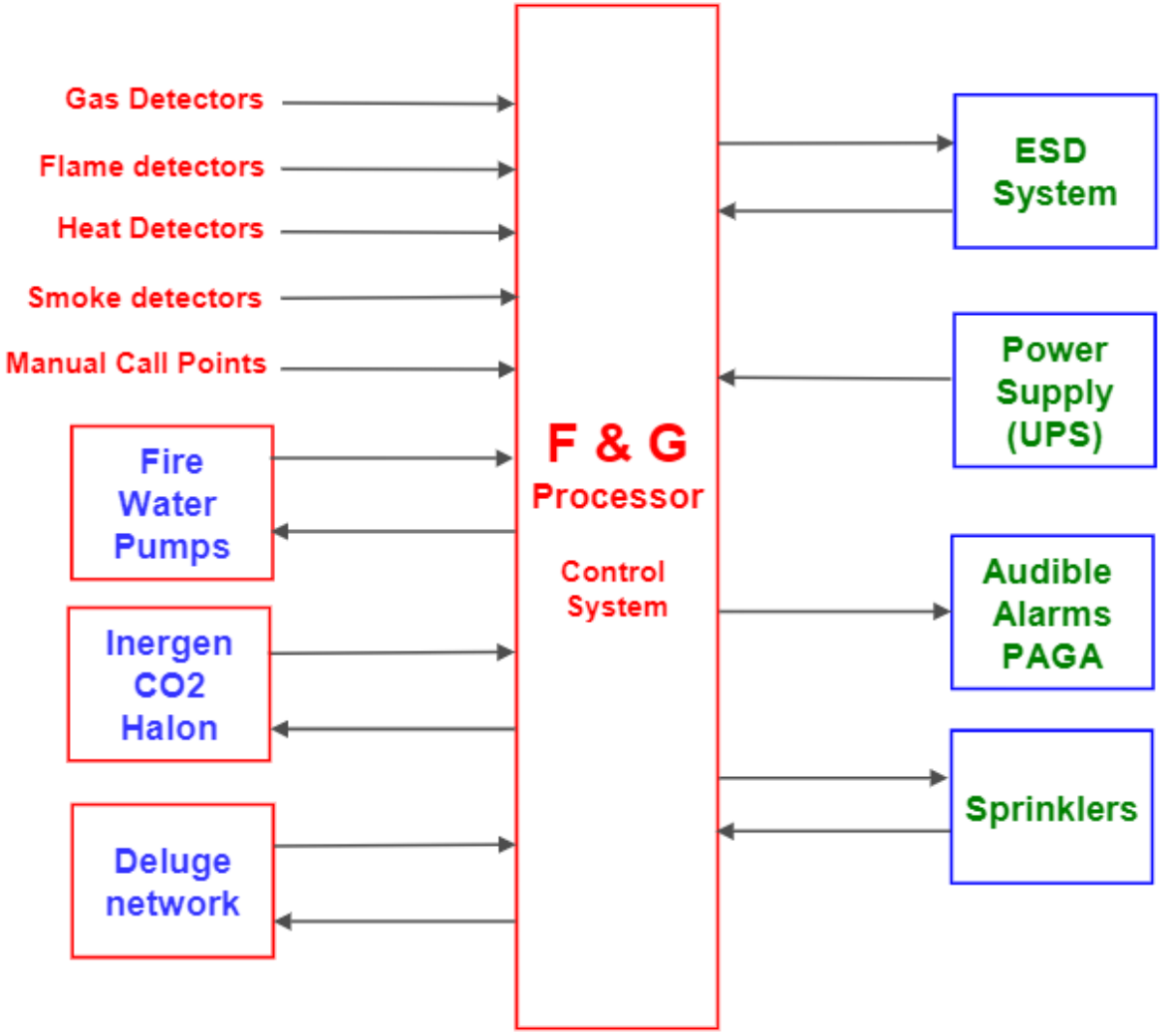


Figure 20 Architecture d'un système F&G

7.1. . Architectures KooN usuelles

7.1.1. Architecture 1oo1

Cette architecture de base est composée d'un seul canal et qu'en conséquence toute défaillance dangereuse induit la perte de la fonction de sécurité en cas de demande. De plus, toute défaillance sûre conduit à l'exécution de cette fonction en absence de demande. Cette architecture minimale, qui ne tolère pas de défaillance, ne peut être utilisée dans des applications de sécurité. Le bloc-diagramme physique ainsi que le schéma électrique de principe relatif à cette architecture sont donnés à la figure 21 [21] [38]. Les diagnostics y sont présents pour assurer la détection des défaillances (dangereuses et sûres) en vue de les réparer immédiatement.

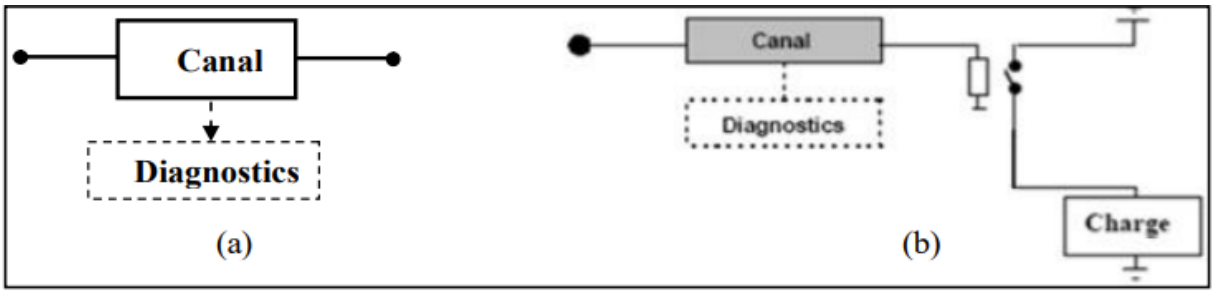


Figure 21 (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à l'architecture 1oo1

7.1.2. Architecture 1oo2

Cette architecture se compose de deux canaux identiques fonctionnant en redondance chaude : chaque canal peut réaliser la fonction de sécurité. Il faut donc que ces deux canaux subissent chacun une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande. A ce titre, la défaillance sûre de l'un ou l'autre des deux canaux conduit le système surveillé vers un état de repli sûr (activation de la fonction de sécurité). La figure 22 regroupe le bloc-diagramme physique et le schéma électrique relatif à cette seconde architecture.

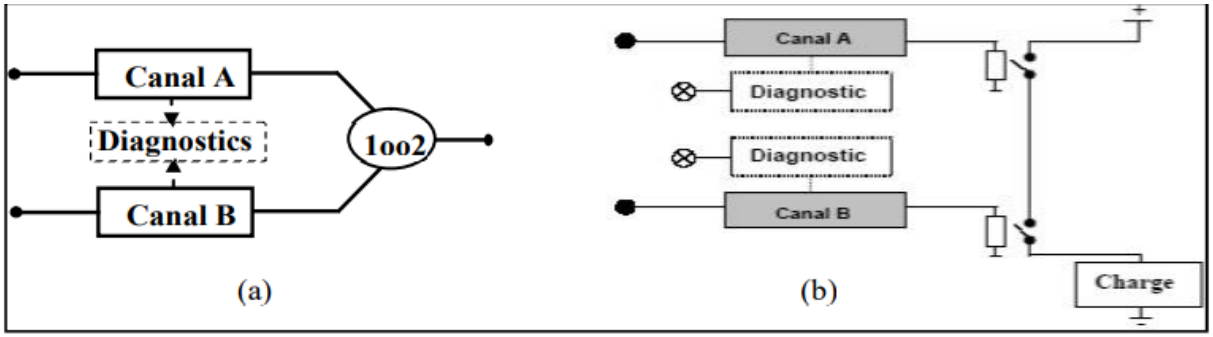


Figure 22 (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à l'architecture 1oo2

7.1.3. Architecture 2oo2

Cette architecture consiste en deux canaux en parallèle de sorte que les deux canaux doivent demander la fonction de sécurité pour que celle-ci soit activée : fonctionnement série au sens fiabiliste. Le système a donc un comportement dangereux dès qu'une défaillance dangereuse survient dans un des deux canaux. En revanche, le déclenchement intempestif (activation de la fonction de sécurité en absence de demande) ne se réalise que si les deux canaux observent des défaillances sûres. Le bloc-diagramme physique et le schéma électrique de principe de cette architecture sont donnés à la figure 23.

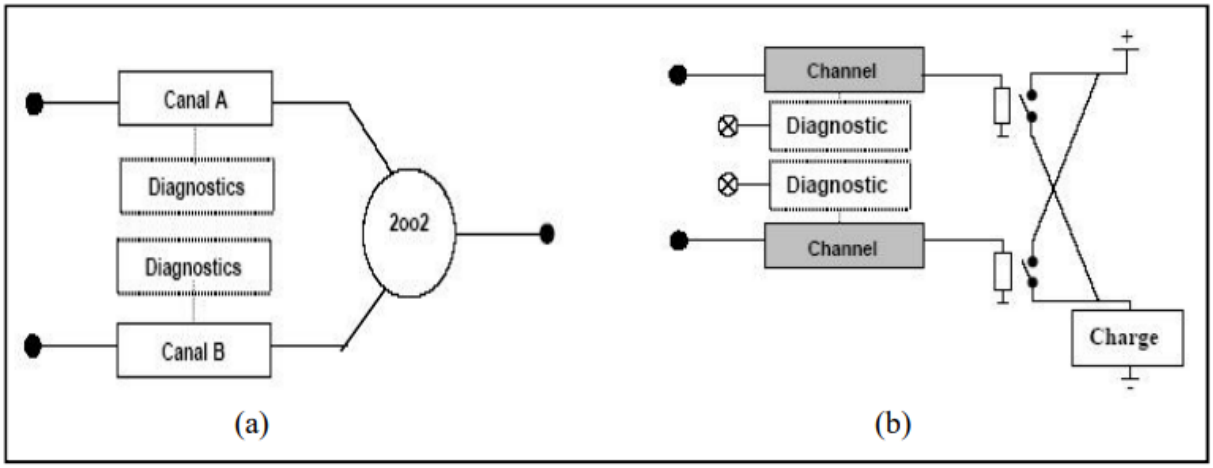


Figure 23 (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à 'architecture 2oo2

D'une manière générale, pour une architecture KooN ces deux nombres sont établis ainsi :

- N – K+1 représente le nombre de défaillances dangereuses dont l'occurrence induit la perte de la fonction de sécurité.
- K représente le nombre de défaillances sûres dont l'occurrence conduit à l'activation intempestive de cette même fonction.

7.2. Les différentes formules de la PFDmoy et de la PFH :

Les différentes formules concernant la PFDmoy sont regroupées au tableau 4 Celles relatives à la PFH diffèrent selon les deux versions de la norme CEI 61508.

Tableau 5 Formules analytiques relatives aux PFH des architectures KooN selon la CEI 61508-6

Architectures	***PFH* [CEI 61508-6, 2009]**
1oo1	λ_{DU}
1oo2	$2((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU}t_{CE}+\beta\lambda_{DU}$
1oo3	$6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^2(1-\beta)\lambda_{DU}t_{CE}t_{GE}+\beta\lambda_{DU}$
2oo2	$2\lambda_{DU}$
2oo3	$6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU}t_{CE}+\beta\lambda_{DU}$

Tableau 4 Formules analytiques relatives aux PFDmoy des architectures KooN selon la CEI 61508-6

Architectures	***PFD_{moy}* [CEI 61508-6, 2009]**
1oo1	$(\lambda_{DU}+\lambda_{DD})t_{CE}$
1oo2	$2((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^2 t_{CE}t_{GE}+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MRT\right)$
1oo3	$6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^3 t_{CE}t_{GE}t_{G2E}+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MRT\right)$
2oo2	$2\lambda_D t_{CE}$
2oo3	$6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^2 t_{CE}t_{GE}+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MRT\right)$

Avec :

$$t_{CE}=\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$t_{GE}=\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$t_{G2E}=\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

- ***MTTR*** *(mean time to restoration) : temps moyen de restauration d'une défaillance dangereuse détectée.*
- ***MRT*** *(mean repair time) : temps moyen de réparation d'une défaillance dangereuse non détectée.* La norme suppose que $MTTR \equiv MRT$.
- $\beta_{DU} = \beta$; $\beta_{DD} = \beta_D$.
- La norme ne tient pas compte des défaillances de cause commune pour les architectures série, en l'occurrence la configuration 2oo2.

Chapitre III :

Allocation et vérification du niveau de SIL

1. Introduction

NAFTAL est une société par actions (SPA) au capital social de 160 000 000 000 DA. Fondée en 1982 et filiale à 100% du Groupe Sonatrach, elle est rattachée à l'activité commercialisation. Elle a pour mission principale, la distribution et la commercialisation des produits pétroliers et dérivés sur le marché national. Elle intervient également dans le domaine de :

• L'enfûtage des GPL ;

• La formulation des bitumes ;

• La distribution, le stockage et la commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux ;

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

• Le cabotage et les pipes, pour l'approvisionnement des entrepôts à partir des raffineries.

• Le rail pour le ravitaillement des dépôts à partir des entrepôts.

• La route pour livraison des clients et le ravitaillement des dépôts non desservis par le rail.

A l'ère de la mondialisation, NAFTAL a jugé indispensable la mise en place d'une nouvelle organisation par ligne de produit (bitumes, lubrifiants, réseau, logistique, GPL, pneumatique, Aviation, Marine…).

NAFTAL fournit près de 13,3 millions de tonnes de produits pétroliers par an, un chiffre appelé à augmenter avec une demande en constante croissance.

Elle a également mis en place une nouvelle vision stratégique à moyen terme orientée client avec un plan de mise en œuvre.

2. Présentation générale du centre enfuteur CE 141 TIARET :

La branche GPL comporte 19 districts GPL au niveau national. Parmi eux on a celle de Tiaret qui ouvre la totalité des wilayas de Tiaret et TISSEMSILT ainsi que le nord de la wilaya de Laghouat représentant la région d'Aflou.

Elle dispose d'un centre emplisseur (CE) à Tiaret d'un Mini centre Enfuteur (MCE) à TISSEMSILT et de 4 dépôts relai (DR) à SOUGUEUR, Ksar CHELLALA, Frenda et à Aflou.

2.1. Identification de l'unité :

- **Nomination :** NAFTAL centre enfuteur 141 Tiaret
- **Raison sociale :** société par action (public)
- **Adresse :** zone industrielle de ZAAROURA/TIARET
- **Début d'activité :** 1983.
- **Activité principale :** EMPLISSAGE GPL (butane et propane) enfutage, Stockage et distribution du Butane et propane conditionné, du propane vrac et GPL Carburant (SIRGHAZ).
- **Capacité de production :** 120 tonnes/jour
- **Rythme de travail :** 1x8h, 3x8h et 2x12h.
- **Superficie totale :** 4.3ha

2.2. Prise de vue aérienne :

Figure 24 prise de vue aérienne du centre enfuteur CE141 NAFTAL TIARET

2.3. Missions du centre de TIARET :

- Le centre est exploité pour assurer le stockage et la distribution de différentes capacités de gaz de pétrole liquéfié (butane et propane).
- L'enfutage des bouteilles butane B13 et des bouteilles Propane P35.
- La distribution des bouteilles de gaz…

L'approvisionnement de l'entrepôt en produit GPL s'effectue par camion-citerne, vient principalement d'ARZEW. Sa distribution s'effectue principalement dans la wilaya Tiaret et TISSEMSILT et le nord de la wilaya de Laghouat.

2.4. Installations importantes :

- Réservoirs de stockage de propane et de butane (Sphère de stockage Butane, Cigares de stockage propane) ;
- Hall d'emplissage de GPL ;
- Station de pompage de GPL ;
- Poste de chargement / déchargement (dépotage) pour camions citernes ;
- Réservoir de stockage eau réseau incendie ;

- Local réseau incendie ;
- Local armoire électrique principale et groupe électrogène ;
- Bloc administratif ;
- Hangar magasin ;
- Atelier mécanique ;
- Vestiaires ;

2.5. Points dangereux :

- Sphère butane ;
- Cigares propane ;
- Bras de chargement / déchargement (dépotage)
- Pomperie GPL ;
- Circuit interne de GPL ;
- Hall d'emplissage ;
- Air de déchargement/chargement GPL conditionné des camions ;
- Station électrique poste TGBT

2.6. Description des grandes installations :

2.6.1. Description des réservoirs de stockage de propane et de butane :

Le butane est stocké dans une sphère d'une capacité de 2000 m^3 à température ambiante sous sa pression de vapeur saturante. Cependant, le propane est stocké dans deux cigares d'une capacité unitaire de 150 m^3.

Le stockage est mis sous 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 un rayonnement thermique d'un feu voisin.

Figure 25 sphère et cigares de stockage de propane et butane au niveau de CE141

2.6.2. Station de pompage GPL :

Au niveau de l'entrepôt, il existe 4 pompes, affectées comme suit :

- Deux (02) pompes GPL Butane 15 m^3/h

- Une (01) pompe GPL propane 30 m^3/h
- Une (01) pompe GPL mixte (butane et propane) 30 m^3/h

2. Description détaillée du process des installation :

a. Les camions GPL destiné à l'approvisionnement des autres centres de stockage du GPL se présentent au poste de dépotage vrac.

b. Connexion du bras articule de dépotage et la mise à la terre.

c. Le chargement des camions citernes à partir des installations de stockage par l'intermédiaire de compresseur à gaz.

d. Le GPL vrac en provenance du pipeline est stocké dans des réservoirs GPL vrac (2 cigares).

e. L'emplissage des bouteilles B13 commence par la vérification par le poste de surveillance de la qualité des bouteilles.

f. Le GPL est soutiré des cigares par pompes vers le hall d'enfutage.

g. Les bouteilles vides déchapeautées et transportées par la chaine automatique (convoyeur), subissent le remplissage lors de la rotation du carrousel.

h. Mise en place des écrous d'inviolabilité.

i. Les bouteilles subissent un test d'étanchéité après remplissage.

j. Les bouteilles fuyardes sont retirées du circuit et celles qui ne présentent pas d'anomalies sont chapeautées et transmises par la palettiseuse au stockage de palettes de 35 bouteilles.

k. Chargement des bouteilles par chariot automoteur (ADF) au niveau de l'aire de stockage.

l. Chargement des camions de conditionnement par palette unitaire de 35 bouteilles butan13kg.

3. Détermination des SIL :

3.1. Champ d'application :

Comme étant le site comporte plusieurs installations Notre étude a été réalisée au niveau de hall d'emplissage la ou la probabilité des fuites et plus élevée

3.2. Recueil des données :

Afin de sélectionner les données d'entrée nécessaires à la réalisation de notre étude, une étape de recueil des données a été menée. Le recueil de données a été réalisé comme suit :

- Une partie pour « l'Initiateur » (élément d'entrée) à savoir les détecteurs de flamme ;
- Une partie pour L'autre partie pour « le Solveur logique » (unité de traitement) à savoir le DCS
- L'autre partie pour « l'Actionneur » (élément final) à savoir la vanne déluge et VCV ;

Cette étape a permis de définir les données nécessaires aux calculs, à savoir :

- Valider les architectures da la boucle de sécurité :
- Capteur, traitement de l'information, actionneur ;

Recueillir les principales caractéristiques du système détection- extinction du hall (marques, technologie, âge, …) ;

Prendre en compte le test et la maintenance mise en œuvre pour ce système (pannes et défaillances enregistrées pour ce système (tirées de la base de données PDS DATA HANDBOOK 2010 EDITION)).

3.3. Description du hall d'emplissage

Figure 26 location du hall d'emplissage dans le centre

Le hall d'emplissage se compose de :

- Deux carrousels de vingt-quatre 24 bascules pour l'enfutage des bouteilles butane B13 ;
- Quatre bascules de remplissage propane sur convoyeur (bouteille P35Kg) ;
- Une bascule de remplissage propane P11 (bouteille 11Kg propane) ;
- Une bascule pour l'enfutage des bouteilles B03 et B06 à valve ;
- Deux palettiseuses ;
- Deux (02) convoyeurs entrée vide ;
- Un (01) Convoyeur sortie plein ;
- Un détecteur de fuite ;
- Une bascule de pré pesée et une autre pour le contrôle de poids ;
- Une cabine peinture ;
- Un bon d'essai pour le teste hydrostatique des bouteilles B13 et un autre pour le P35 et le robinet,

- Un redresseur de pied « réparation à froid des pieds bouteilles » et une robineuse « serré le robinet sur la bouteille »

3.3.1. La répartition des détecteurs de flame au niveau du hall d'emplissage :

Ce présent plan représente la répartition des détecteur au niveau du hall d'emplissage plus de détail sur l'emplacement des détecteur et présenté par la figure qui suit

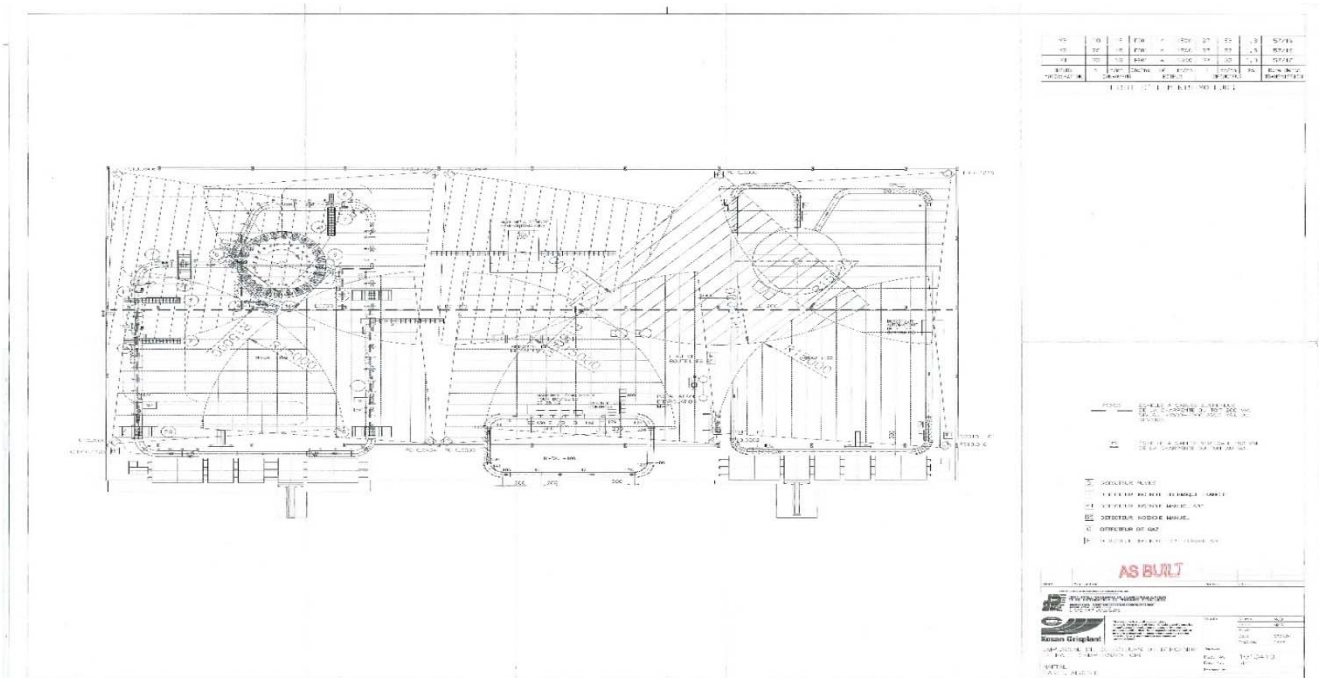


Figure 27 3 la répartition des détecteurs de flame au niveau du hall d'emplissage

3.4. Détermination du niveau SIL « Cible » :

3.4.1. Evaluation de risque par la méthode HAZOP :

- **La grille de criticité :**

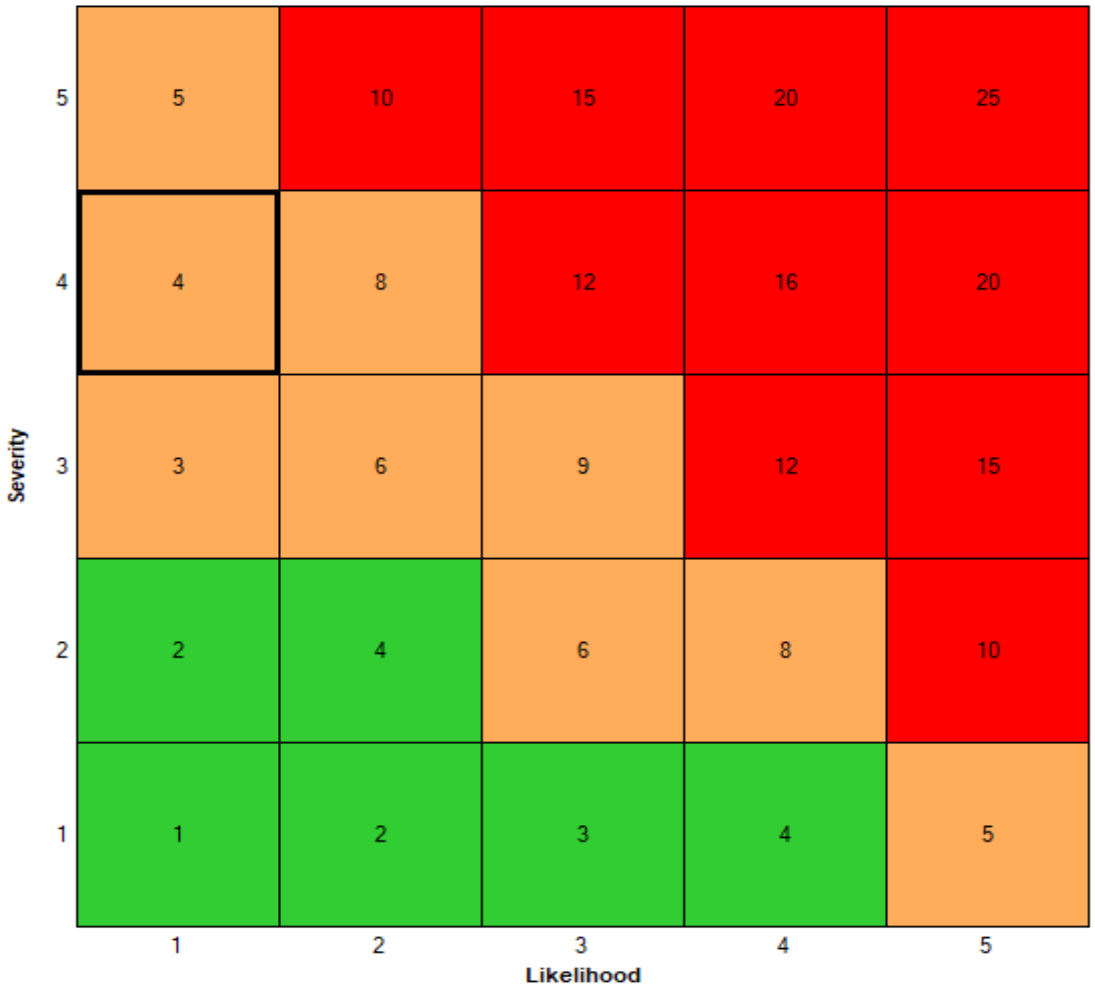
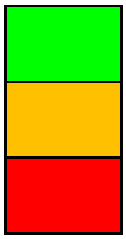


Figure 28 la grille de criticité



ZONE Acceptable

ZONE Tolérable (ALARP)

ZONE Inacceptable

Acceptable : Signifie, en général, qu'on accepte la probabilité de létalité comme raisonnable et qu'on ne cherche pas à faire des efforts pour la réduire davantage.

Tolérable (ALARP) : Implique qu'on accepte de vivre avec un niveau de risque particulier mais on reconsidère les causes de risques et les mesures préventives pour les réduire.

Inacceptable : Signifie qu'on n'accepte pas ce niveau de risque et qu'on ne participe pas à l'activité considérée et qu'on n'autorise pas les autres personnes à faire marcher un processus qui l'a exposé.

e) BARRIERES DE SECURITE (SAUVGARDES)

L'ensemble des dispositions adoptées en matière de conception, construction et modalités d'exploitation incluant les mesures d'urgence internes et externes afin de prévenir l'occurrence et limiter les effets d'un phénomène dangereux et les conséquences d'un accident potentiel associé.

3.4.2. Résultat HAZOP et graphe de risque intégré :

Tableau : HAZOP/Graphe de Risque

Node	Deviation	Causes	Consequences	Before Risk Reduction			Safeguards	SIL determination								
								SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
				S	L	RR				S	L	PLs	SIL	S	L	PLs	SIL
1. empllisage des bouteilles	1. plus de débit	1. la vanne FCV bloqué ouverte	1. Augmentation de pression vers les postes d'emplissage	2	2	4	1. Réseau anti-incendie	1. Système pression	Ext Systeme pression								
			2. débit de remplissage des bouteilles plus importante (déviation de débit importante de noued précédente)	2	2	4	2. Système détection feu & gaz	2. Système de detection gaz et feu	Ext	Extensive	Low	2	SIL 1	Minor	Low	3	---
			3. perturbation de l'emplissage des bouteilles(déversement de gaz)	2	3	6	3. PH										
			4. Risque de fuite aux postes d'emplissage	3	4	12	4. FSL										
							5. PI										
							6. rideau d'eau										
	2. pas de débit	1. la vanne FCV bloqué fermé	1. Débit d'alimentation du carroussel insuffisant et pas de production	3	2	6	1. PIT	1. Systeme pression	Ext								
							2. FSL										
							3. PCV										
		2. défaillance de pompe	1. Perte d'alimentation du carroussel et perte de production	3	2	6	1. PI										
		3. défaillance de compresseur	1. pas de production	3	2	6											
	3. haute pression	1. Fermeture de vanne manuelle sur le circuit vers le hall (erreur opérateur)	1. Montée en pression de la ligne vers hall à la pression maxi de la pompe à débit nul < pression de tenue de la ligne	2	2	4	1. Système détection feu & gaz	1. Systeme de détection Feu et gaz	Ext	Extensive	High	1	SIL 3 (a)	Serious	Medium	2	SIL 1
								2. Systeme pression	Ext								
			2. risque d'échauffement pompe transfert	2	2	4	2. PI										
			3. fuite GPL	3	4	12	3. PSV										
		2. flame à l'éxterieur	1. explosion	4	2	8	1. système anti-incendie										
		3. augmentation de la température ambiante	1. surpression	2	3	6	1. TRV										
							2. TI										
			1. augmentation de la température	3	2	6	1. PI										
							2. PCV										

Node	Deviation	Causes	Consequences	Before Risk Reduction			Safeguards	SIL determination								
								SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
				S	L	RR				S	L	PLs	SIL	S	L	PLs	SIL
		4. défaillance de système de refroidissement des installations					3. PH										
	4. basse pression	1. fuite dans la conduite	1. UVCE en cas d'éteincelle retardée	4	2	8	1. voir pas de débit	1. Systeme pression	Ext								
			2. incendie en cas d'éteincelle immédiate	4	2	8		2. Systeme Température	Rec								
			3. dommage environnementale	1	2	2											
		2. défaillance de pompe	1. Perte d'alimentation du carroussel et perte de production	3	2	6	1. PIT										
							2. PI										
							3. PCV										
							4. FSL										
		3. la vanne FCV bloqué semi fermée	1. Débit d'alimentation du carroussel insuffisant et baisse de production	3	2	6	1. PH										
							2. PI										
							3. PIT										
							4. PCV										
							5. TRV										
	5. haute température	1. Isolement prolongé de tronçon de ligne liquide et ensoleillement fort	1. Expansion thermique dans le tronçon et risque de fuite GPL en quantité limitée avec inflammation en cas de source d'ignition	3	2	6	1. voir haute pression	Systeme .Température 1. Systeme pression	Rec Ext								
		2. Explosion ou incendie à l'extérieur de l'installation	1. Augmentation de la pression	3	2	6	1. voir haute pression										
			2. Explosion -Jet Fier - BLEVE - UVCE	4	2	8											
		3. Température élevé en provenance des unités de traitement en amont	1. Augmentation de la pression dans la ligne	3	3	9	1. PI										
			2. Explosion -Incendie	4	2	8	2. PIT										
							3. PH										
							4. PCV										
							5. TRV										
		4. Défaillance des indicateurs de contrôle	1. Perte d'indication de la température	2	3	6											
		5. défaillance de système de refroidissement	1. augmentation de la pression	3	2	6											

Node	Deviation	Causes	Consequences	Before Risk Reduction			Safeguards	SIL determination									
								SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
				S	L	RR				S	L	PLs	SIL	S	L	PLs	SIL
			2. incendie - explosion	4	2	8											
		6. augmentation de la température ambiante	1. voir haute pression	1	2	2	1. voir haute pression										
	6. basse température	1. sans objet car température minimale = -10°C															
	7. plus de niveau (bouteille)	1. Défaillance de la bascule d'emplissage (mécanique, électrique et électronique)	1. Sur-remplissage de bouteilles et risque de fuite en cas d'expansion thermique (parc de stockage des bouteilles remplies exposées au soleil)	3	2	6	1. Système détection feu & gaz	1. Systeme de niveau	Rec								
							2. PI	2. Systeme de détection Feu et gaz	Ext	Minor	Medium	2	c	Minor	Medium	2	c
							3. PIT										
							4. LSHH										
							5. LI										
	8. moin de niveau (réservoir)	1. défaillance de capteur de niveau	1. Marche à sec et dégradation de la pompe vers hall	2	2	4	1. LI	1. Systeme de niveau	Rec Ext	Serious	Medium	1	SIL 2	Serious	Medium		
			2. - Fuite de GPL	3	3	9	2. LT	2. Systeme de détection Feu et gaz								2	SIL 1
			3. Risque de feu, UVCE, jet enflammé en cas de source d'ignition	4	2	8	3. système anti-incendie										
							4. Système détection feu & gaz										
	9. fuite ipmortante (pipe à l'exterieur)	1. Agression mécanique sur le pipe	1. Dispersion de GPL et UVCE	4	3	12	1. Système détection feu & gaz	1. Systeme de détection Feu et gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Medium	3	SIL 1
			2. jet enflammé en cas de source d'ignition	3	2	6	2. système anti-incendie										
							3. rideau d'eau										
		2. corrosion	1. Dispersion de GPL et UVCE	4	3	12	1. système anti-incendie										
							2. Système détection feu & gaz										
	10. fuite mineure(pipe à l'exterieur)	1. Fuite de bride	1. Dispersion de GPL et UVCE/jet enflammé en cas de source d'ignition	3	3	9	1. PI	1. Systeme de détection Feu et gaz	Ext	Serious	High	1	SIL 3 (b)	Serious	Medium	2	SIL 1
			2. débit faible	2	2	4	2. PDI										
							3. système anti-incendie										
							4. rideau d'eau										
	11. fuite mineure(pomperie)	1. Fuite de garniture	1. débit faible	2	3	6	1. voir fuite (pipe à l'exterieur)	1. Systeme de détection Feu et gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Medium	3	SIL 1
	12. fuite importante(hall)	1. Agression mécanique sur le pipe dans le hall ou contrainte mécanique (carroussel)	1. Dispersion de GPL et UVCE	3	3	9	1. voir fuite importante (pipe à l'exterieur)	Systeme de détection Feu et gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Medium	3	SIL 1
			2. jet enflammé en cas de source d'ignition (10 personnes présentes	3	2	6		2. Systeme de détection Feu et gaz						Serious			

Node	Deviation	Causes	Consequences	Before Risk Reduction			Safeguards	SIL determination								
								SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
				S	L	RR				S	L	PLs	SIL	S	L	PLs	SIL
			dans le hall en permanence)														
	13. fuite mineure(hall)	1. Fuite de brides sur le pipe dans le hall	1. Dispersion de GPL et flash/jet enflammé à proximité de la fuite	3	3	9	1. 1. voir fuite (pipe à l'exterieur)	1. Systeme de détection Feu et gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Medium	3	SIL 1
			2. risque faible d'accumulation dans le hall car volume important et hall aéré	2	2	4											

3.4.3. Interprétation des résultats

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

- Quatre évènements inacceptables
- Vingt-huit évènements en zone ALARP
- Neuf 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 les fuite mineurs ont une grande probabilité de Risque avec ceux de haute pression

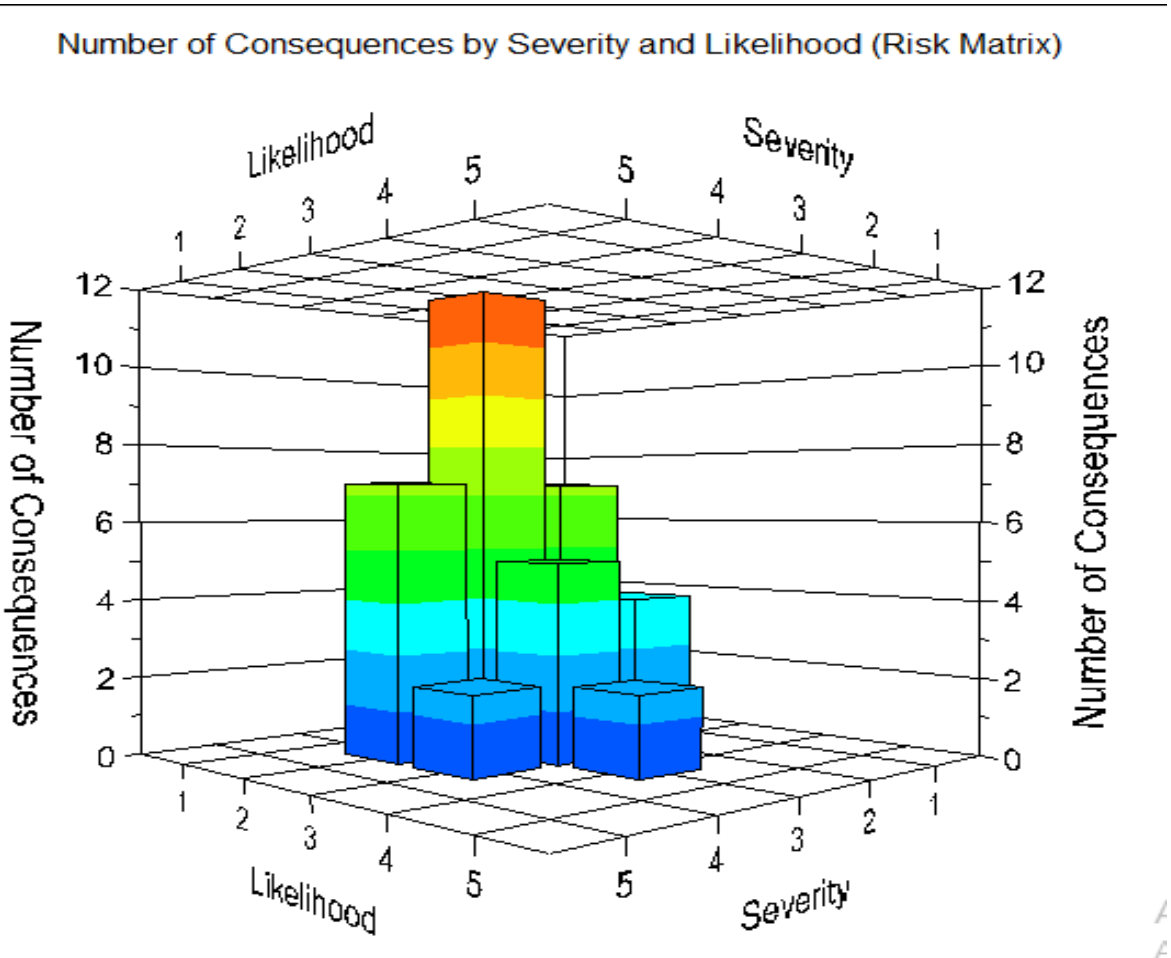


Figure 29 Graphe nombre de conséquences en fonction de la gravité et de la probabilité SIDE 1

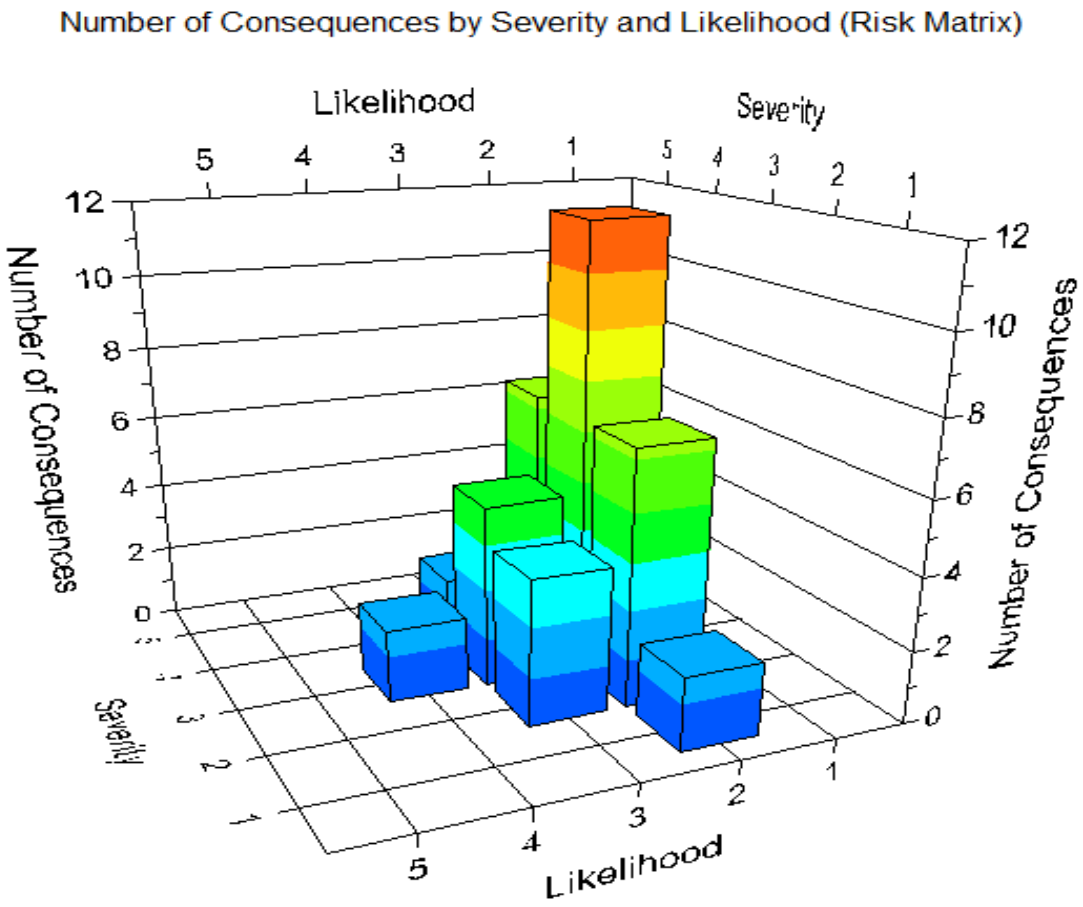


Figure 30 Graphe nombre de conséquences en fonction de la gravité et de la probabilité SIDE 2

3.5. 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 par 2 étapes détermination de SIL initiale sans barrière de sécurité et une nouvelle détermination avec les barrières de sécurité pour observer la diminution du niveau de sile.

En prend par exemple le cas de fuite mineure au niveau du hall le SIF définie est système de détection de flame comme résultat avant la mise en place des barrières est de **SIL 2** et après l'ajout des IPL ça devenu **SIL 1** voir extrait du tableau

SIL determination									
SIF	SIF Status	Safety Layer Matrix - Initial				Safety Layer Matrix - Final			
		S	L	PLs	SIL	S	L	PLs	SIL
1. Systeme de détection Feu et gaz	Ext	Extensive	Medium	2	SIL 2	Extensive	Medium	3	SIL 1

3.6. Détermination du niveau SIL « Réel » :

Le but principal de cette étape est de déterminer le niveau SIL en fonction des données réelles des taux de défaillance ($\lambda_S, \lambda_D, \lambda_{DD}, \lambda_{DU}$) de chaque élément de la SIF (initiateur / solveur logique / élément final) ainsi que de la périodicité des tests effectué sur ces 03 éléments et procéder par la suite à une comparaison entre le niveau SIL « Cible » et le niveau SIL « Réel »

3.6.1. L'architecture de SIS étudié :

Le SIS se compose de :

- Dix détecteurs de flammes optiques de flammes, réagissent aux rayonnements émis par tous types de flammes (1oo10) réparties dans le hall comme suit :

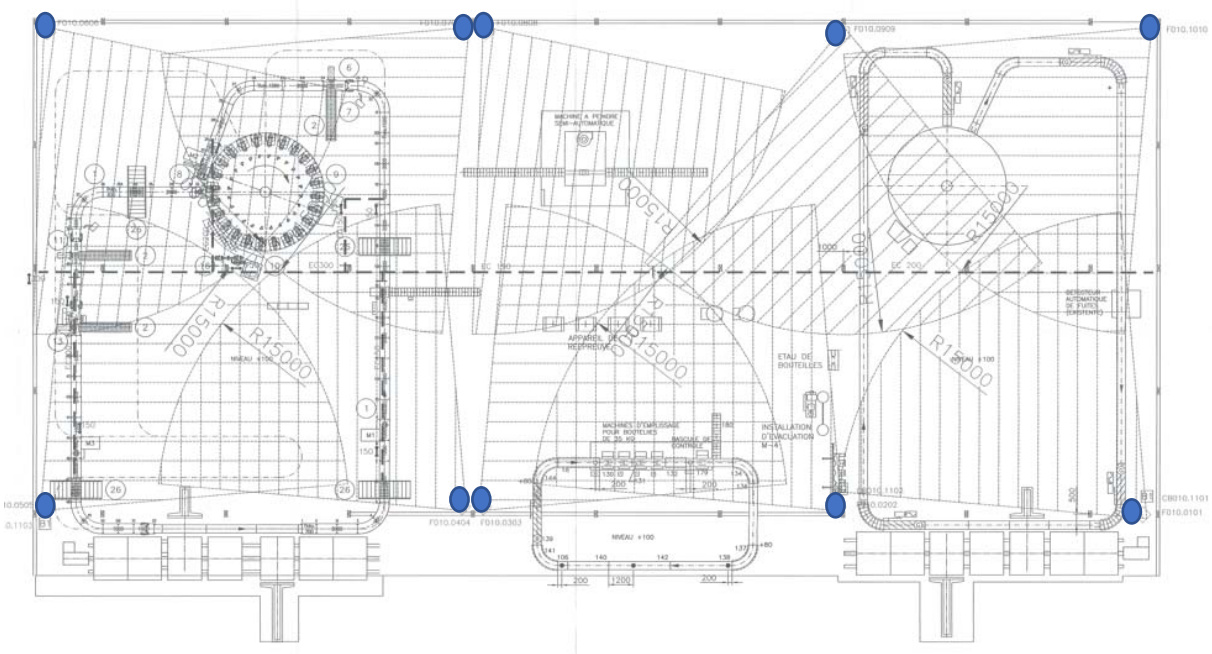


Figure 31 la répartition des détecteurs de flammes au niveau du hall d'emplissage

- Détecteur de flamme

- Une unité logique de type MX62 (1oo1) qui est une unité fixe de contrôle de présence de flamme en liaison permanente avec les détecteurs de flammes ;

- Deux actionneurs (2oo2) : la vanne de déluge et l'arret d'urgence par la vanne « ONOFF » ;

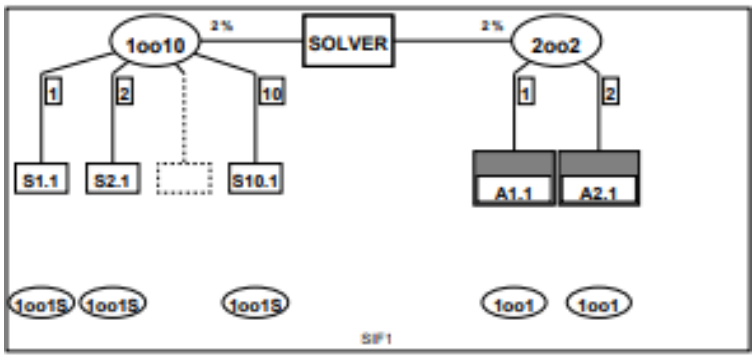


Figure 32 l'architecture de SIS étudié

3.6.2. Configuration des composants des 03 éléments de la SIF :

L'objectif est de spécifier les valeurs propres à chaque élément de la SIF étudiée.

Ceci s'effectue à travers différents onglets de la fenêtre de configuration :

- Un onglet **capteurs** contient le paramétrage des capteurs de la boucla de sécurité.
- Un onglet **solveur** contient le paramétrage du solveur.
- Un onglet **actionneur** contient le paramétrage des actionneurs.

3.5.1.1. La source des données :

La source des données utilisées dans les calculs est la base de données SINTEF (reability data for safety insrumented systems).

3.5.1.2. Paramétrage des capteurs :

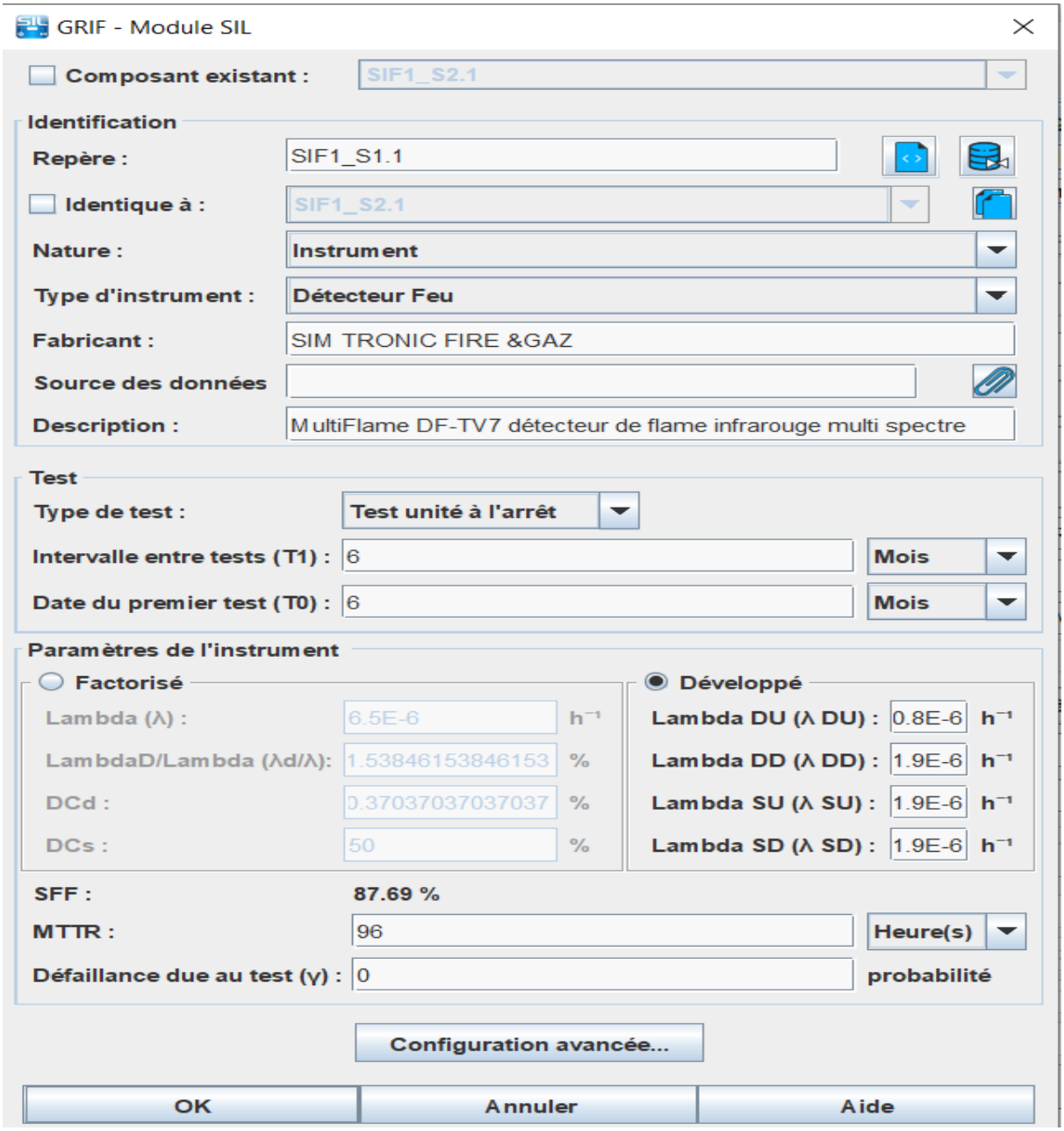


Figure 33 capture d'écran du fenêtre paramétrage des capteurs

3.5.1.3. Paramétrage du solveur :

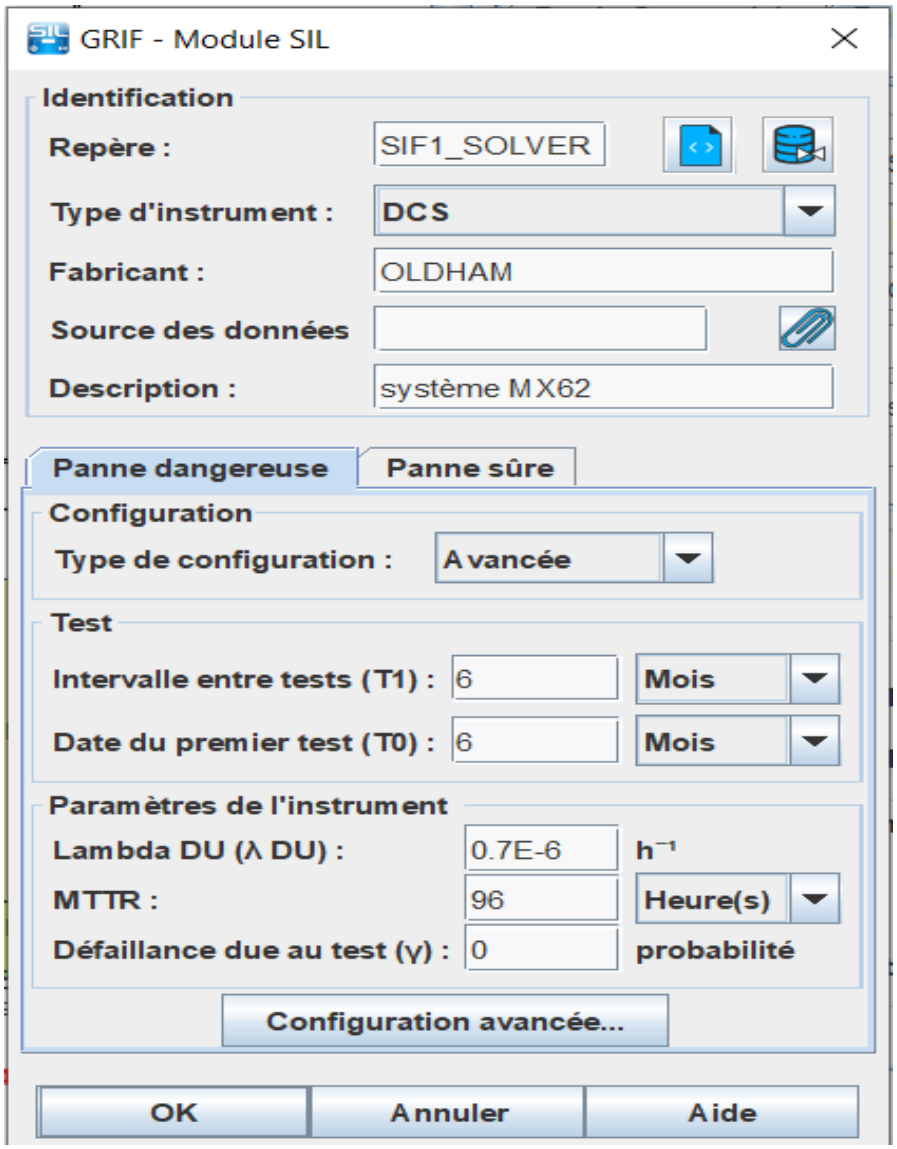


Figure 34 capture d'écran du fenêtre paramétrage du solveur

3.5.1.4. Paramétrage des actionneurs :

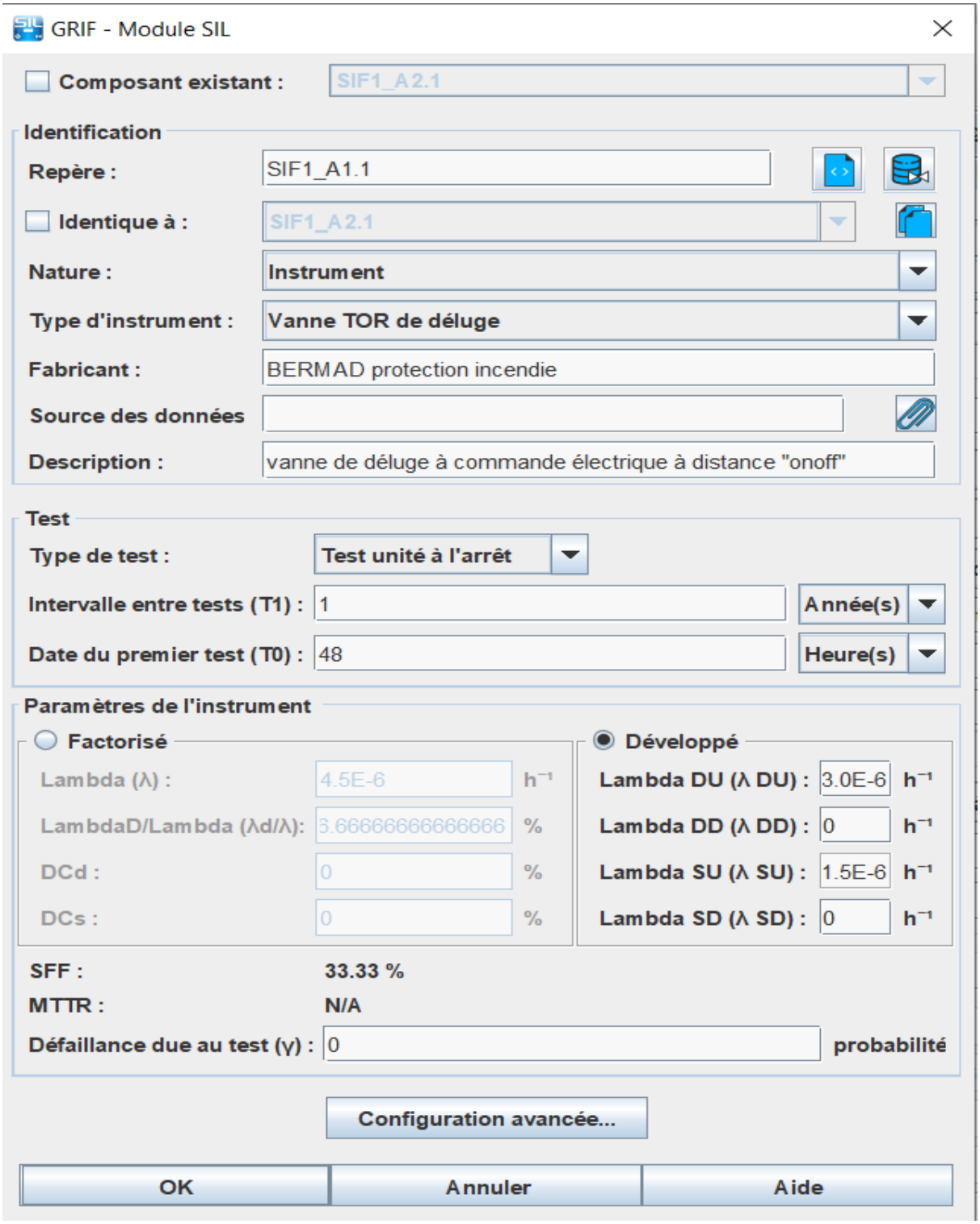


Figure 35 capture d'écran du fenêtre paramétrage d'actionneur vanne TOR de déluge

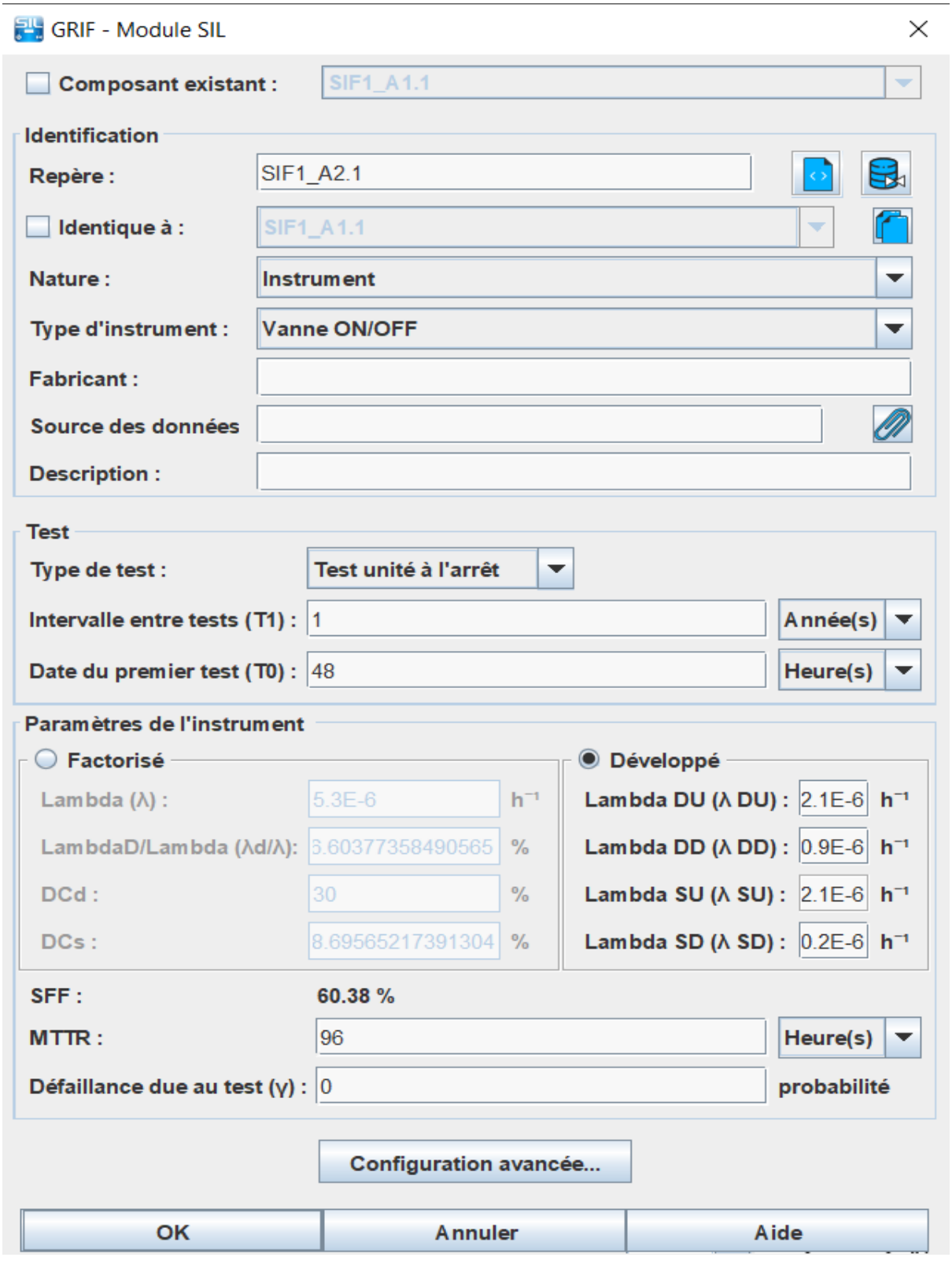


Figure 36 capture d'écran du fenêtre paramétrage d'actionneur (vanne ONOFF)

3.5.2. Les résultats :

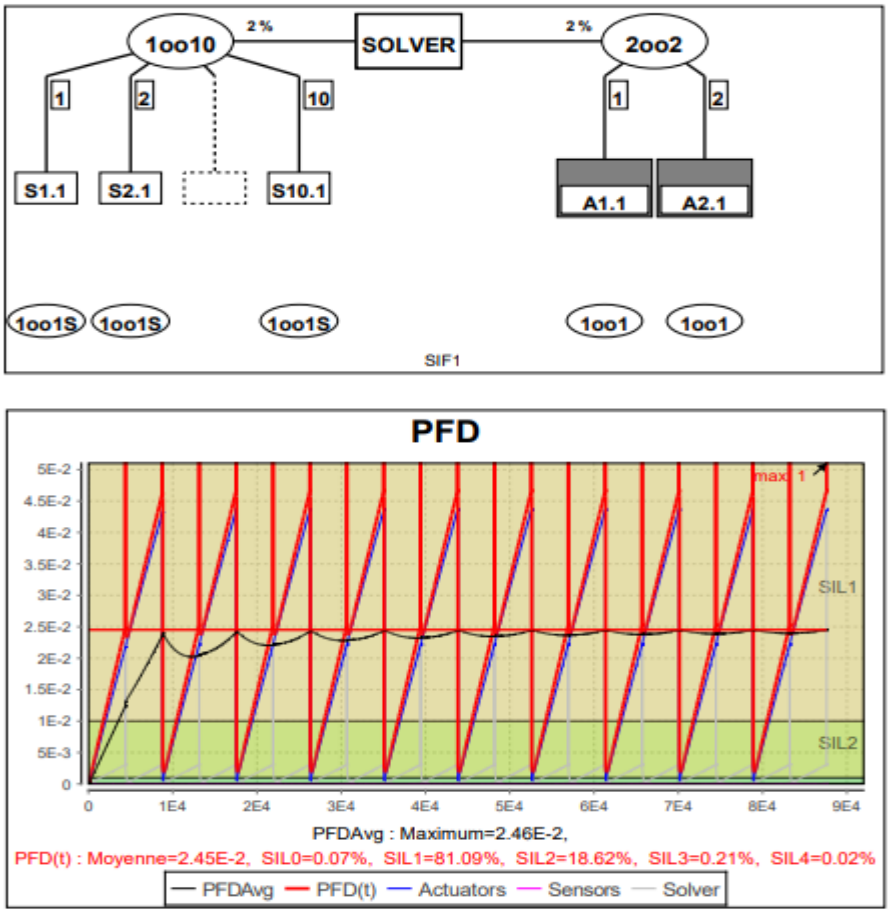


Figure 37 résultats généraux des calculs du PFD

Les graphes représentés par cette figure sont les résultats de l'architecture globale là où on voit clairement que la majorité des résultats sont de SIL1

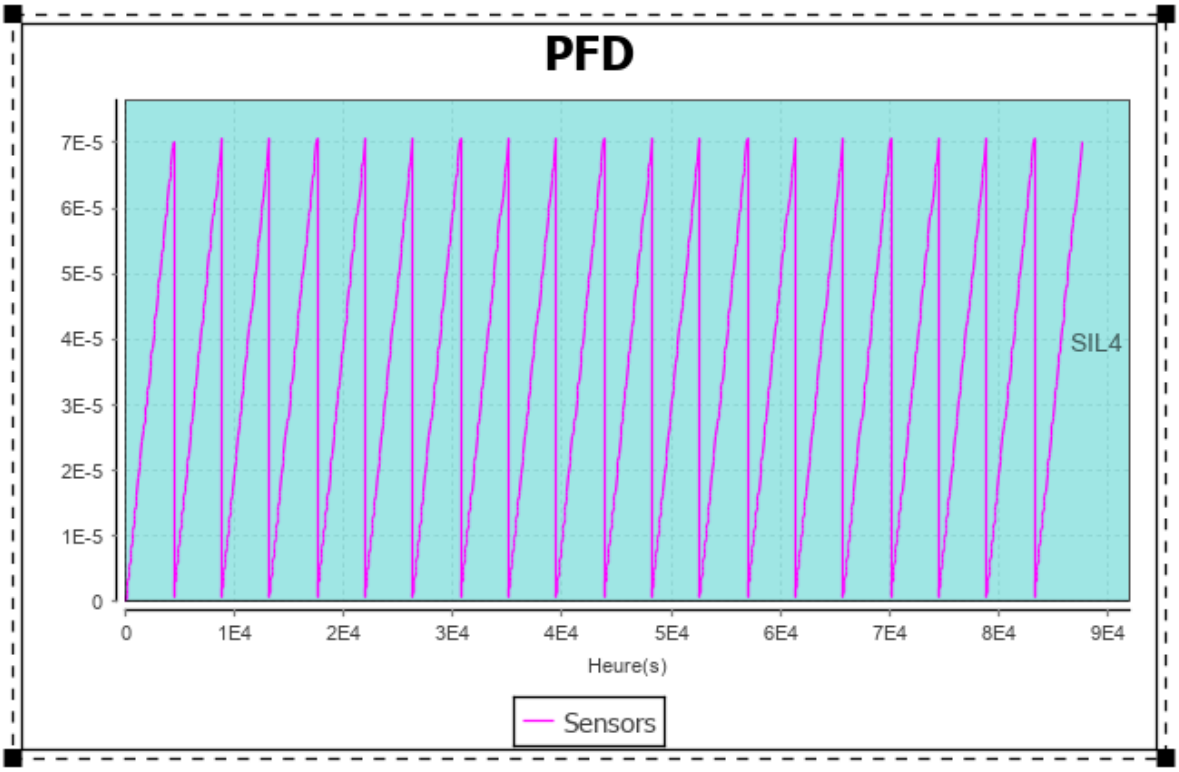


Figure 39 probabilité de défaillance de détecteurs de flamme

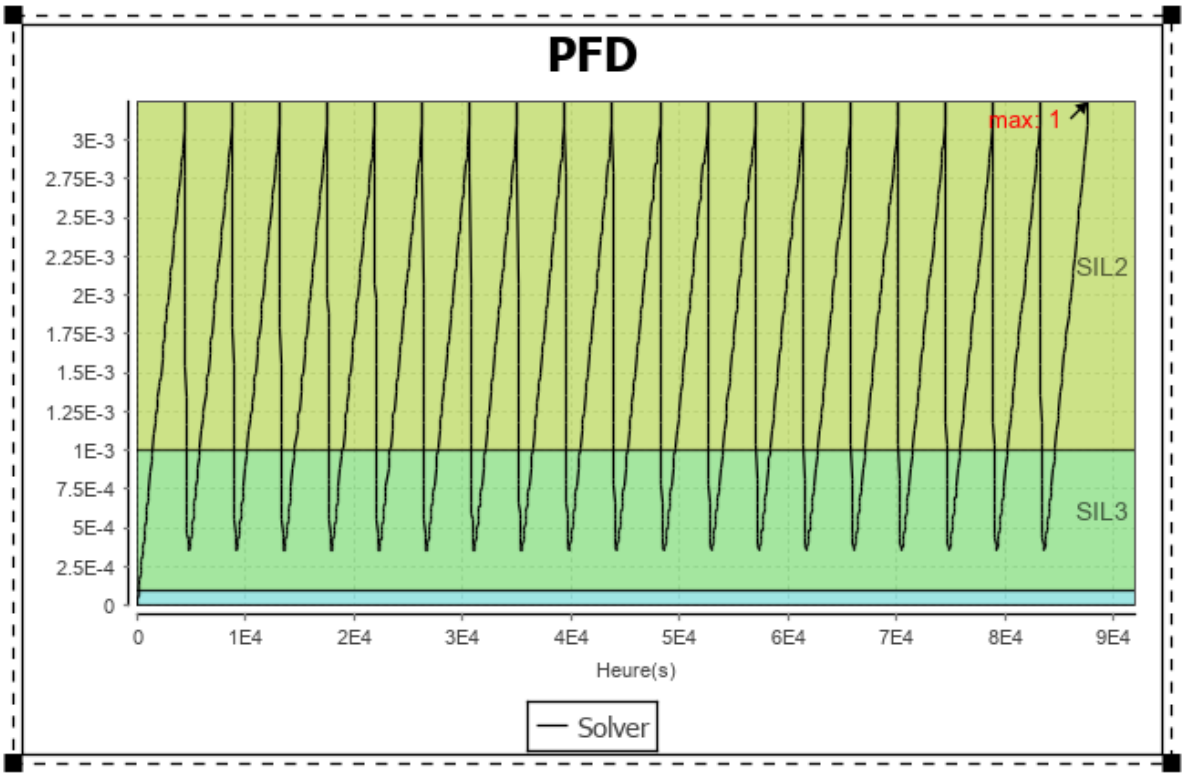


Figure 38 probabilité de défaillance de l'unité logique

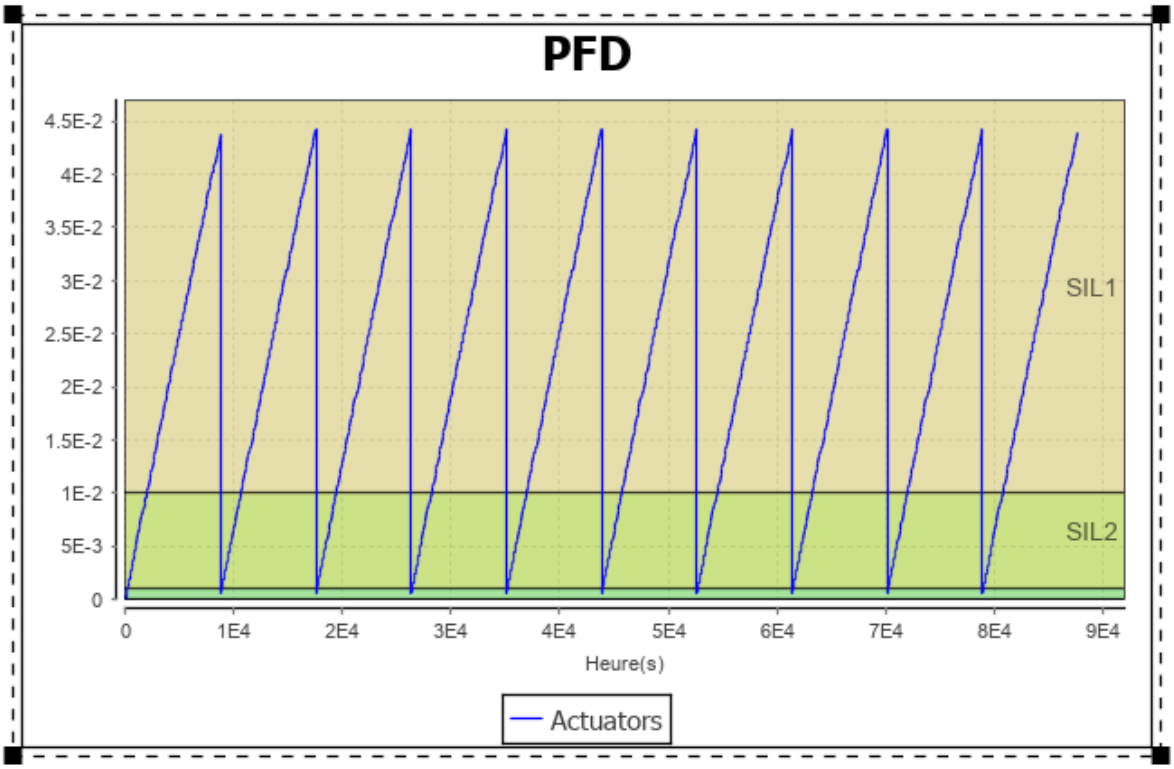


Figure 40 probabilité de défaillance des actionneurs

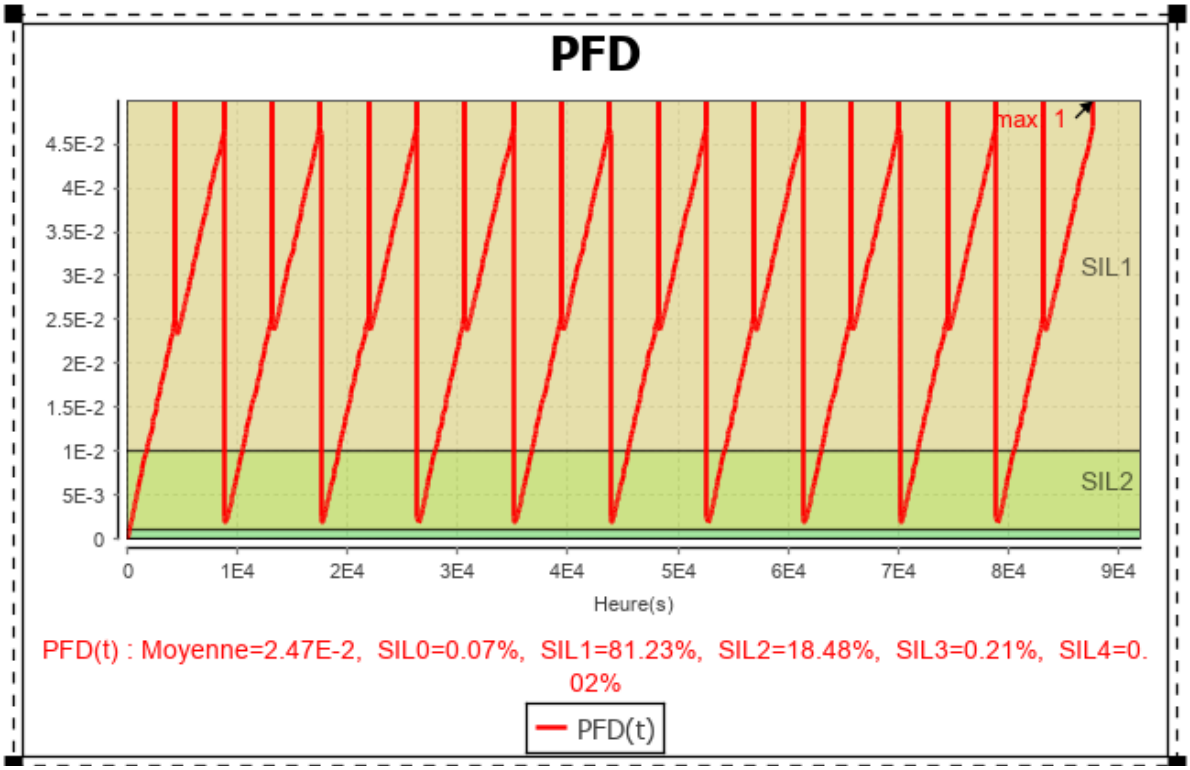


Figure 41 probabilité de défaillance de SIF

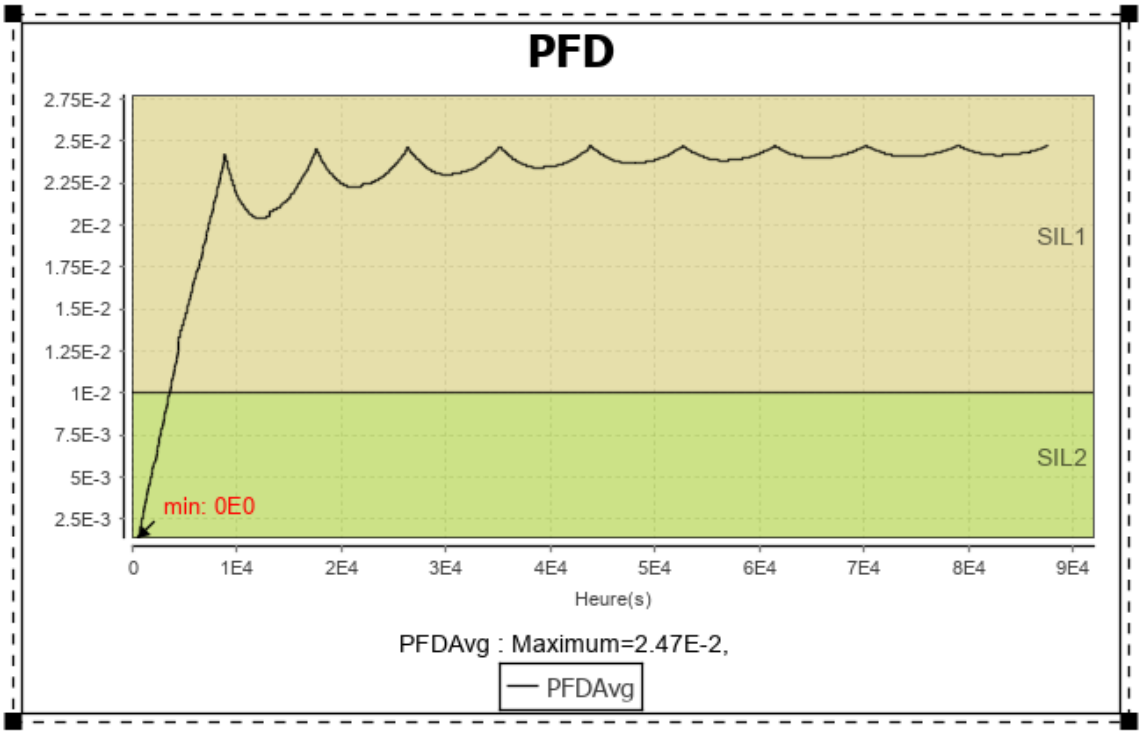


Figure 43 probabilité moyenne de défaillance de SIF

Synthèse

	PFD Avg	RRF	SIL Calculé	Contribution (%)
Partie Capteur(s)	3.57E-5	28032.41	4.00	0.14%
Partie Solveur	2.27E-3	439.91	2.00	9.18%
Partie Actionneur(s)	2.25E-2	44.52	1.00	90.68%
SIF	2.47E-2	40.47	1.00	100%

Figure 42 synthèse des résultats

3.6.3. Interprétation des résultats :

Après avoir établir la simulation de l'architecture du SIF sur le logiciel GRIF, le graphe obtenu représente des modèles qui suive une équation exponentielle présenté dans le deuxième chapitre avec une périodicité de test c'est-à-dire après chaque test l'équipement testé est considéré comme neuf et la probabilité de défaillance PFD revenu vers 0.

La probabilité de défaillance maximale pour chaque élément de la SIF :

- ✓ Détecteurs de flamme :

  PFDmax= 7E-5

- ✓ L'unité logique :

  PFDmax=3.25E-3

- ✓ L'actionneur :

  PFDmax=4.4 E-2

- ✓ SIF : PFDmax=2.47 E-2

D'après ces résultats on trouve que le niveau de SIL réel de ce système instrumenté de sécurité est le SIL 1

Après le calcul des niveaux SIL « Cible » et « Réel » nous constatons que ces deux derniers sont égaux pour l'élément d'entrée et l'élément final :

SIL (cible) = SIL (réel) =1

Conclusion

L'objectif de notre travail était de déterminer le niveau d'intégrité d'une fonction instrumentée de sécurité d'un système de détection de flame installer au niveau du hall d'emplissage afin d'apprécier son efficacité par rapport au danger.

Cette détermination a été élaborée par deux étapes principales à savoir l'allocation du niveau SIL dit « Cible », et cela par la méthode HAZOP et graphe de risque intégrée, ainsi que le calcul du niveau SIL dit « Réel » à partir des données de défaillance réelles du système et l'intervalle des tests effectués.

Les résultats de la méthode HAZOP nous ont permis d'identifier les scénarios catastrophiques ainsi que les mesures mise en place pour la maitrise de ce risque, par la combinaison du graphe de risque avec HAZOP le niveau de SIL a était déterminer en deux phase un niveau SIL initial ainsi qu'un niveau de SIL final après l'ajout des IPL. Le niveau SIL « Cible » obtenu pour la SIF étudiée, et cela par l'application de la méthode est égal à « 1 ».

L'architecture installer par les instrumentistes a la base des résultats obtenu par la première étape a été vérifie par l'utilisation des paramètres de défaillance ainsi que des périodes de test réels selon les modèles de fiabilité. Le niveau SIL « Réel » obtenu à l'aide de logiciel GRIF « SIL Verification » est égal à « 1 ».

Après la comparaison entre les deux niveaux d'intégrité de sécurité, nous avons constaté que le niveau SIL « Cible » est égal au niveau SIL « Réel ».

Comme perspective a notre travail une étude de cycle de vie complète présenté par un tableau de bord de notre SIF aura été souhaitable, par contrainte d'erreur d'exécution du logiciel EXIDA exSILentia sa n'a pas été achevé.

Bibliographie

[1] https://www.techniques-ingenieur.fr/base-documentaire.

[2] Guide 51 ISO/CEI:1999, définition 3.5

[3] Guide 51 ISO/CEI:1999, définition 3.2

[4] Guide 51 ISO/CEI:1999, définition 3.7

[5] Guide 51 ISO/CEI:1999, définition 3.9

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

[7] guide ISO/CEI 73 [ISO, 2002]

[8] Norme CEI 61508, Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le domaine de la production pour processus – Parties 4, janvier 2003-juillet 2003. Commission Electrotechnique Internationale, Genève, Suisse.,

[9] Norme CEI 61508, Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le domaine de la production pour processus – Parties 4, janvier 2003-juillet 2003. Commission Electrotechnique Internationale, Genève, Suisse.

[10] Norme CEI 61511, Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le domaine de la production pour processus – Parties 1 à 3, janvier 2010. Commission Electrotechnique Internationale, Genève, Suisse.

[11] **IEC 61808-4-210**, définition 3.3.2

[12] [CEI 61508-5, 2000]

[13] CEI 61511-1, 2003.

[14] Etude de l'implémentation des Systèmes Instrumentés de Sécurité par des méthodes semi-quantitatives dans un environnement de connaissances imparfaites,mémoire de magister,Université El-Hadj Lakhdar,Batna,2013

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

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

.[17] [Schonbeck, M., Rausand, M. et J « Human and organisational factors in the operational phase of safety instrumented systems : A new approach », 2010]

[18] F.R Farmer, Sitting criteria: a new approach. Atom,1967

[19] Norme CEI 61508, Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Parties 1 à 7, octobre 1998-2000. Commission Electrotechnique Internationale, Genève, Suisse.

[20] F. INNAL, Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances Analyse critique de la norme CEI 61508, Thèse de Docteur de L'Université BORDEAUX 1 ; 2008.

[21] Norme CEI 61508, Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Parties 1 à 7, octobre 1998-2000. Commission Electrotechnique Internationale, Genève, Suisse.

[22] Norme CEI 61508, Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Parties 4, octobre 2002. Commission Electrotechnique Internationale, Genève, Suisse.

[23] FARES INNAL. Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances Analyse critique de la norme CEI 61508, Thèse de Docteur de L'Université BORDEAUX 1.

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

[25] Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, Berlin, Deutsches Institut für Normung.

[26] Layer of protection analysis; simplified process assessment; center for chemical process safety of the American institute for chemical Engineers;New York;2001.

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

[28] Signoret, J.-P., Dutuit, Y., and Rauzy, A, High integrity protection systems (hips) : Methods and tools for efficient safety integrity levels (sil) analysis and calculations. In Risk, Reliability and Societal Safety Aven and Vinnem (eds), 2007.

[29] Rauzy, A, New algorithms for fault trees analysis. Reliability Engineering & System Safety, 59(5) :203-211, 1993.

[30] Signoret, J.-P, High integrity protection system (hips)overcoming sil calculation difficulties. Technical report, TOTAL document, Pau, 2004.

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

[32]Rauzy, A, New algorithms for fault trees analysis. Reliability Engineering & System Safety, 59(5) :203-211, 1993.

[33] Zhang, T., Long, W., and Sato, Y ,Availability of systems with self- diagnostic components-applying markov model to iec 61508-6. Reliability Engineering Systems Safety, 80 :133141, 2003

[34] Signoret, J.-P., Dutuit, Y., and Rauzy, A, High integrity protection systems (hips) : Methods and tools for efficient safety integrity levels (sil) analysis and calculations. In Risk, Reliability and Societal Safety Aven and Vinnem (eds),2007

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

[36] https://www-safireprotection-com

[37] http://www.aria.developpement-durable.gouv.fr

[38] Philippe charpentier. Architecture d'automatisme en securite des machines: Etudes des conditions de conception liées aux défaillances du mode commun – Thèse de DOCTEUR de l'Institut Nationale Polytechnique de LORRAINE – Spécialité Automatique.