Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

ECOLE NATIONALE POLYTECHNIQUE

Projet de fin d'étude pour l'obtention du diplôme d'Ingénieur d'Etat en QHSE-GRI

Intitulé

EVALUATION DE LA PERFORMANCE DES SYSTEMES INSTRUMENTES DE SECURITE

Système d'Arrêt d'Urgence Automatique du Four Rebouilleur H201

Train 1, Module 1, SONATRACH-DP, Hassi R'Mel

Etudié par : **M^elle^ ASSADI Meriem et M FOUL Bilal**

Proposé par : **M Makhlouf CHATI, SONATRACH - DP, Hassi R'mel**

Encadré par : **Mme Karima Djouadi (ENP)**

M Makhlouf Chati (SH/DP/HR)

Promotion Juin 2015

10 ,Avenue des frères Ouadek. Hassen Badi. BP A82, 16200. Alger, ALGERIE.
www.enp.edu.dz

Remerciement

Nous tenons d'abord à remercier Madame ZEBOUDJ Saliha d'avoir accepté la présidence du jury, ainsi que, Messieurs, BENSARI Kamel, CHATI Makhlouf et mesdames DJOUADI Karima, OUSSEDIK Nassiba de nous avoir fait l'honneur de faire partie de notre jury et pour le temps qu'ils sont en train de nous consacrer.

Nous aimerions remercier également toute l'équipe de SONATRACH à Hassi R'mel pour leur accueil et leur esprit d'équipe, en particulier Monsieur ANOU pour nous avoir accueillis au sein de son équipe et pour la confiance qu'il nous a accordée en suivant ce stage, ses conseils avisés nous ont guidé tout au long de ce travail. Que ce travail soit le témoignage de nos respects.

Nous remercions nos encadreurs, monsieur CHATI Makhlouf et madame DJOUADI Karima pour le rôle crucial qu'ils ont joué en supervisant ce projet, principalement pour le savoir qu'ils nous ont transmis et pour le temps qu'ils nous ont consacré, nous les remercions également pour les conseils, le soutien et les directives qui furent d'une importance capitale à notre compréhension et ainsi à l'aboutissement de ce projet.

Nous souhaiterons remercier l'ensemble de nos professeurs de l'Ecole Nationale Polytechnique qui ont eu la politesse et la gentillesse de répondre à nos questions pendant nos études.

Un merci à tous nos amis, pour leur soutien constant et pour l'atmosphère chaleureuse et rassurante qu'ils ont su créer autour de nous, pendant le stage et notre séjour à Hassi R'mel.

Enfin nous remercions nos deux familles, pour leur soutien moral et financier que nous considérons être une indispensable contribution à l'achèvement ce projet.

ملخص

لأن هناك مستويات مختلفة من المخاطر في المنشآت الصناعية، هناك طرق مختلفة لتصميم انظمة السلامة المجهزة الخاصة بها. هذا ما يدفعنا للتساؤل حول قدرة هذه الأنظمة على تنفيذ وظائف سلامتها بشكل صحيح للتحكم في هذه المخاطر، بدءا بالنموذج رقم 61508 للجنة الكهرو تقنية الدولية كوثيقة مرجعية معيارية لتنفيذ هذه الانظمة.

تتألف منهجية تقييم أداء هذه الأنظمة من جزأين، الاولى نوعية؛ مبنية على التحليل الوظيفي والهيكلي ونظام تحليل المخاطر والاستغلال وتطبيق الرسم البياني المخاطر، والأخرى كمية تعتمد على أبحاث قام بها المعهد الوطني للبيئة الصناعية والمخاطر (تقييم متعدد المعايير)بشأن حواجز الأمن التقني.

هذا العمل يمثل منفعة للشركة المضيفة لمعرفة مستوى أداء نظامها للإغلاق التلقائي الخاص بالطوارئ، والذي يتمثل في **مستوى السلامة الامنية 2 والفعالية 100 بالمئة وزمن الاستجابة 75 ميلي ثانية**.

كلمات البحث: السيطرة على المخاطر، والأداء، انظمة السلامة المجهزة، النموذج رقم 61508 اللجنة الكهرو تقنية الدولية، مستوى
السلامة الامنية، والفعالية وزمن الاستجابة، نظام الاغلاق للطوارئ.

Résumé

Du fait qu'il y ait différents niveaux de risque dans les installations industrielles, il existe différentes façons de concevoir des Systèmes Instrumentés de Sécurité (SIS). La question derrière cette réflexion est l'aptitude de ces systèmes à exécuter correctement leurs fonctions de sécurité, avec le souci majeur de la maîtrise des risques, partant de la norme CEI 61508 comme document normatif de référence pour la mise en œuvre des SIS.

La méthodologie d'évaluation de la performance de ces systèmes est composée de deux parties, une qualitative ; basée sur une analyse fonctionnelle et structurelle du système, une étude HAZOP et une application du graphe de risque, et l'autre quantitative ; appuyée sur les recherches de l'INERIS sur les Barrières Techniques de Sécurité (BTS) (évaluation multicritères). Ce travail présente l'intérêt pour l'entreprise d'accueil de connaitre la performance de son système d'arrêt d'urgence automatique (ESD), qui se concrétise en un **SIL 2**, une **efficacité de 100%** et un **temps de réponse de 75ms**.

Mots clés : maitrise des risques, performance, SIS, CEI 61508, Niveau d'intégrité de sécurité, BTS, efficacité, temps de réponse, ESD.

Abstract

Just as there are many different levels of risk in many different process facilities, there are many different ways of designing safety instrumented systems. The question behind this reflection is the ability of these systems to successfully perform their safety functions.

With the major concern of risk control, starting from the IEC 61508 as a normative reference document for the implementation of the SIS. The methodology to evaluate the performance of these systems is composed of two parts, one qualitative; based on a functional and structural analysis of the system, a HAZOP study and a risk graph application, the other is quantitative; relied on the research of INERIS about Safety Technical Barriers (advanced evaluation). This work present the interest of the host company to know the performance of its automatic emergency shutdown system, it has a **SIL 2**, an **efficiency of 100%** and a **response time of 75 ms**.

Key words: risk control, performance, SIS, IEC 61508 Safety Integrity Level, BTS, efficiency, response time, ESD.

Liste des figures

Figure 2.1 : Complexité d'un système.

Figure 2.2 : Réduction du risque : Concept général.

Figure 2.3 : Processus de réduction du risque, du point de vue du concepteur.

Figure 2.4 : Cycle de vie de sécurité globale.

Figure 2.5 : Typologie des Barrières Techniques de Sécurité.

Figure 2.6 : Risque tolérable et ALARP.

Figure 2.7 : Méthodes habituelles de réduction de risque rencontrées dans les processus industriels.

Figure 3.1 : Système instrumenté de sécurité.

Figure 3.2 : Diagramme de fiabilité d'un élément soumis à des tests de révision complet et Partiel.

Figure 3.3 : Notion pour les problèmes de défaillance à la sollicitation (PFD) exemple n=4.

Figure 3.4 : Différents temps relatif aux SIS.

Figure 3.5 : Bloc diagramme physique pour l'architecture 1oo1.

Figure 3.6 : Diagramme de fiabilité pour l'architecture 1oo1.

Figure 3.7 : Bloc diagramme physique pour l'architecture 2oo3.

Figure 3.8 : Relation entre les éléments du SIS.

Figure 3.9 : Graphe de risque : schéma général.

Figure 4.1 : les zones d'exploitation à HRM.

Figure 4.2 : Représentation schématique du four H201 du train 1, Module 1.

Figure 4.3 : Fiche technique du four H201.

Figure 4.4 : Les transformateurs d'alimentation.

Figure 4.5 : Modèle du graphe de risque.

Figure 4.6 : Arbre de défaillance d'un SIS.

Figure 4.7 : Schématisation d'un SIS.

Figure 4.8 : Relais de sécurité relatifs au système d'arrêt des bruleurs.

Figure 4.9 : Configuration du système d'arrêt des brûleurs.

Figure 4.10 : Evolution de la PFD_{avg} en fonction de du temps (heures).

Figure 4.11 : Contribution de chaque composante du SIS au SIL calculé.

Figure 4.12 : Interpolation en utilisant la fonction « Polyfit » et la fonction « lsqcurvefit ».

Figure 4.13 : Effet des tests périodiques sur l'évolution de la PFD.

Figure 4.14 : Fiche technique des résultats trouvés par le module SIL.

Liste des tableaux

Tableau 1.1 : Incidents sur fours rebouilleurs – SONATRACH.

Tableau 2.1 : Causes de défaillance et mesures pour réduire le risque.

Tableau 2.2 : Cycle de vie de la sécurité : Systèmes E/E/EP.

Tableau 3.1 : Lien entre PFD et MOON.

Tableau 3.2 : Définition des niveaux SIL pour un mode de fonctionnement à faible Sollicitation.

Tableau 3.3 : Définition des niveaux SIL pour un mode de fonctionnement à forte Sollicitation.

Tableau 3.4 : Description des paramètres du graphe de risque.

Tableau 3.5 : Définition des paramètres du graphe de risque.

Tableau 4.1 : Situation géographique.

Tableau 4.2 : Les zones d'exploitation HRM.

Tableau 4.3 : Tableau local du four H201.

Tableau 4.4 : Principe de signalisation des composantes.

Tableau 4.5 : Alarmes et descriptions.

Tableau 4.6 : Analyse fonctionnelle et structurelle.

Tableau 4.7 : Scénarios critiques ressortis de l'étude HAZOP.

Tableau 4.8 : Caractérisation des paramètres C, P, F et W.

Tableau 4.9 : Données relatives aux éléments du sous-système des détecteurs.

Tableau 4.10 : Calcul de $\boldsymbol{\lambda_{éq}}$

Tableau 4.11 : Données sur les taux de défaillance équivalent aux BAL

Tableau 4.12 : Composition des branches du sous-système relais de sécurité

Tableau 4.13 : Calcul des $\lambda(B_{Ri})$ équivalant

Tableau 4.14 : Calcul de $\boldsymbol{\lambda}_{éq}$ au sous-système de relais de sécurité

Tableau 4.15 : Données relatives aux relais de sécurité

Tableau 4.16 : Données relatives aux éléments du sous-système des actionneurs

Tableau 4.17 : Caractère déterminé des éléments du notre système

Tableau 4.18 : Analogie entre les éléments du système d'arrêt des brûleurs et les éléments présentés dans la modélisation du système.

Tableau 4.19 : Valeurs de la PFDavg en fonction du temps d'exploitation (heures).

Tableau 4.20 : Réponse du SIS par rapport à chaque arrêt triennal, Train 1.

Tableau 4.21 : Réponse du SIS par rapport à chaque arrêt triennal, Train 2.

Tableau 4.22 : Réponse du SIS par rapport à chaque arrêt triennal, Train 3.

Tableau 4.23 : Réponse du SIS par rapport arrêt décennale, MPP1.

Tableau 4.24 : Moyenne des réponses du SIS.

Tableau 4.25 : Liste des Valeurs du TR des détecteurs.

Tableau 4.26 : Liste des Valeurs du TR d'une série donnant l'action du système.

Liste des annexes

Annexe 1 : Exemple de matrice de gravité.

Annexe 2 : Exemple d'un tableau de la méthode LOPA.

Annexe 3 : Cycle de vie de la sécurité : Système E/E/EP.

Annexe 4 : Notation générale relative au calcul des probabilités.

Annexe 5 : Processus de traitement de gaz Train 1, Module 1 (MPP1), DP, HRM, SH.

Annexe 6 : Etude HAZOP.

Annexe 7 : Fichier (.m file) interpolation polynomiale.

Annexe 8 : Fichier (.m file) calcul du maximum de la fonction F(x).

Abréviations et Acronymes

AdD	Arbre des Défaillances.
ALARP	As Low As Raisonably Practicable (aussi faible que raisonnablement possible).
BPCS	Basic Process Control System.
BTS	Barrières Techniques de Sécurité.
CEI / IEC	Commission Electrotechnique Internationale (International Electrotechnical Commission).
CTG	Centre de Traitement de Gaz.
CTH	Centre de Traitement d'huile.
DC	Diagnostic Coverage (Couverture du Diagnostic).
DNV	Det Norske Veritas.
E/E/EP	Electrique / Electronique / Electronique Programmable.
ESD	Emergency Shut Down (système d'arrêt d'urgence).
EUC	Equipment Under Control (équipement sous contrôle).
FAL	Flow Alarm Low (Alarm de Bas Débit).
FALL	Flow Alarm Low Low (Alarm de Trés Bas Debit).
FT	Flow Transmitter (Transmetteur de Débit).
FTF	Fail To Function on demand – Défaillance à la sollicitation
FV	Flow Valve (Vanne de Débit).
GPL	Gaz de Pétrole Liquéfié.
GRIF	Graphiques Interactifs pour la Fiabilité.
HAZOP	HAZard and Operability study (Analyse de risque et d'exploitation).
HRM	Hassi R'Mel.
INERIS	Institut National de l'Environnement Industrielles, et des RISques.
INRS	Institut National de la Recherche Scientifique.
ISA	Instrumentation, Systems and Automation Society
ISO	International Organisation for Standardization (Organisation International de normalisation).
LOPA	Layer Of Protection Analysis (Analyse des barrières (couches) de protection).
MDT	Mean Down Time (durée moyenne d'indisponibilité après défaillance).
MMR	Mesures de Maitrise des risques.
MMRI	Mesures de Maitrise des Risques Instrumentées.
MooN	M out of N (M parmi N).
MPP	Module Processing Plant (Module de traitement et de production).
MPP1	Module Processing Plante One.
MTBF	Mean Time Between Failure (durée moyenne entre défaillances consécutives).
MTTF	Mean Time To (first) Failure (durée moyenne de fonctionnement avant la première défaillance).
MTTR	Mean Time To Repair (durée moyenne de réparation).
MUT	Mean Up Time (durée moyenne de fonctionnement après réparation).
NC	Niveau de Confiance.
NF	Norme Française.
OREDA	Off-shore Relaibility Data base.

P&ID	Piping and Instrumentation Diagram.
PAH	Pressure Alarm High (Alarm de Haute Pression).
PAHH/LL	Pressure Alarm High High/Low Low (Alarm de Trés Haute /Trés Bas Pression).
PAL	Pressure Alarm Low (Alarm de Bas Pression).
PFD	Probability of Failure on Demand (probabilité de défaillance à la demande.
PFD_{avg}	Average Probability of Failure on Demand (Probabilité de Défaillance moyenne à la Demande).
PFD_i	Probability of Failure on Demand.
PFD_{max}	Probability of Failure on Demand-Max.
PFH	Probability of Failure per Hour (probabilité de défaillance par heure).
PFS	Probabilité de défaillance sûre (Intempestif).
PI	Pressure Indicator (Indicateur de pression).
PLC	Programmable Logic Controller.
PSH/L	Pressure Switch High/Low (switch de Haute/Bas Pression).
PT	Pressure Transmitter (Transmetteur de pression).
R(t)	Relaibility (Fiabilité).
RRF	Risk Reduction Factor (facteur de réduction du risque).
SCN/S	Station de réinjection des gaz Nord/Sud.
SDV	Shutdown Valve (Vanne d'arret).
SFF	Safe Failure Fraction (proportion des défaillances en sécurité).
SH	SONATRACH.
SIF	Safety Instrumented Function (fonction instrumentée de sécurité).
SIL	Safety Integrity Level (niveau d'intégrité de sécurité).
SIS	Safety Instrumented System (Système Instrumenté de Sécurité).
SRGA	Station de Récupération des Gaz Associés.
SRS	Safety Related Systems (Systèmes relatifs à la sécurité).
STR	Taux de défaillance sûr (Intempestif).
TAH	Temperature Alarm High (Alarm de Haute Temperature).
TAHH	Temperature Alarm High High (Alarm de Trés Haute Temperature).
TI	Temperature Indicator (Indicateur de Pression).
TV	Temperature Valve (Vanne de Température).
λ	Taux de défaillance d'un canal.
λ_D	Taux de défaillance dangereuse du canal.
λ_{DD}	Taux de défaillance dangereuse détectée du canal.
λ_{DU}	Taux de défaillance dangereuse non détectée du canal.

Table des matières

Introduction générale 1
Chapitre I : Cadrage de l'étude 3
Introduction 4
1. Problématique 4
2. Enjeux de la maitrise des barrières techniques de sécurité (BTS) 6
2.1. Enjeux Humains 6
2.2. Enjeux Environnementaux 6
2.3. Enjeux Réglementaires 7
2.4. Enjeux Economique 7
3. Objectifs 7
Conclusion 8
Chapitre II : De la sécurité fonctionnelle à la maitrise des risques 9
Introduction 10
1. Notions générales 10
1.1. Notion de système 10
1.2. Intégrité de Sécurité 11
1.3. Notion de réduction des risques 12
1.4. Notion de défaillance 16
2. Norme CEI 61508 18
2.1. Champ d'application 18
2.2. Chapitres de la norme 18
2.3. Objectif de la CEI 61508 20
2.4. Limites de la CEI 61508 20
2.5. Sécurité fonctionnelle 21
2.6. Cycle de vie de sécurité 21
3. Evaluation de la performance des barrières technique de sécurité (BTS) 23
3.1. Présentation générale 23
3.2. Types de BTS 23
3.3. Critères de performance des BTS 25
Conclusion 26
Chapitre III : Systèmes Instrumentés de Sécurité 27
Introduction 28

1. Concept de Systèmes Instrumentées de Sécurités 28
1.1. Définition d'un SIS 28
1.2. Constitution élémentaire d'un SIS 29
1.3. Fonction Instrumentée de Sécurité 29
1.4. Mode de fonctionnement 29
1.5. Test relatif aux SIS 30
2. Approche normative (CEI 61511) 32
3. Critères de performance des SIS 32
3.1. Taux de défaillance 32
3.2. Différents temps relatives aux SIS 37
3.3. Taux de Couverture - Diagnostic Coverage (DC) 39
3.4. Caractère déterminé du composant avec leur SIL équivalent 40
4. Configuration architecturelle d'un SIS 40
4.1. Architecture MooN 41
4.2. Architecture 1ooN 41
4.3. Architecture 2oo3 42
4.4. Lien entre les architectures et le PFD du système 42
5. Détermination du niveau d'intégrité de sécurité (SIL) 43
5.1. Description générale sur le SIL 43
5.2. Détermination du SIL requis 45
5.3. Allocation du SIL (réel) 48
Conclusion 48
Chapitre IV : Evaluation de la performance de système d'arrêt d'urgence automatique, du rebouilleur H201 50
Introduction 51
1. Présentation de l'entreprise 51
1.1. Situation géographique 51
1.2. Organisation du champ gazier 52
2. Description du four 53
2.1. Présentation générale 53
2.2. Analyse structurelle et fonctionnelle 60
3. Détermination des scénari critiques 62
4. Evaluation des critères de performance 64
4.1. Niveau d'Intégrité de sécurité (SIL) 64

4.2. Efficacité 82
4.3. Temps de réponse 85
Conclusion 86
Conclusion Générale 87
Bibliographie 88
Annexes 91

Introduction générale

Le risque est intimement lié à la vie. La reconnaissance du risque, de ses impacts sur l'environnement et des accidents qui en découlent reste récente. La société plaçait la maîtrise des risques entre les mains de la science et de la technologie, l'apparition de catastrophes technologiques importantes a conduit à remettre en cause la confiance qu'on accordait au progrès technique dans son aptitude à garantir la sécurité. Dans le domaine pétrolier, reconnu à haut risque, des accidents majeurs ont secoué les esprits à l'image de :

- Explosion dans une raffinerie à Amuay, Venezuela (48 morts et 151 blessés) en Août 2012.
- Explosion sur un site de conditionnement de gaz industriel liquéfié, Martigues, France (1 mort et 2 blessés) en Janvier 2011.
- Incendie des bacs de stockage de brut S105/ S106 Terminal RTE SH TRC Skikda, Algérie (2morts et 6 blessés) en Octobre 2005.
- Explosion de l'unité de liquéfaction GL1K- SH Aval, Skikda, Algérie (27 morts et 74 blessés) en Janvier 2004.

Progressivement, la société moderne a bien été forcée de reconnaître que le risque zéro n'existait pas. Ces catastrophes ont fait émerger une culture du risque, de la sécurité industrielle et une conscience de l'impact sur l'environnement des activités industrielles. Ainsi le risque est devenu un sujet de préoccupation majeure. Il engendre un sentiment croissant d'insécurité et nourrit à lui seul de nombreuses réflexions.

La démarche de maîtrise des risques vise essentiellement la réduction des risques existants. Celle-ci est souvent obtenue par l'interposition successive d'une ou plusieurs barrières de Sécurité. L'évolution de la règlementation internationale oblige à des mesures de maitrise des risques qui utilise des systèmes instrumentés de sécurité. L'utilisation de ces systèmes a pour objectif d'assurer la sécurité fonctionnelle des installations à travers la réduction des risques à un niveau inférieur ou égal au risque tolérable. La finalité assignée aux Systèmes Instrumentés de Sécurité est la détection des déviations pouvant mener à un accident, pour mettre en œuvre un ensemble de réponses nécessaires à la mise en sécurité des équipements critiques.

Vérifier l'aptitude d'un Système Instrumenté de Sécurité à exécuter correctement ses fonctions constitue une étape importante pour la validation de ce dernier. A ce titre plusieurs documents normatifs ont été élaborés afin de guider les fabricants et utilisateurs potentiels des SIS dans leur démarche de

validation. La norme Commission Electrotechnique Internationale (CEI) 61508 représente le document normatif central de la sécurité fonctionnelle des systèmes Electriques, Electroniques et Electroniques Programmables - E/E/EP - et la norme CEI 61511 représente un document normatif pour la conception et l'exploitation des SIS.

Notre travail, dont l'intitulé est « Evaluation de la performance des systèmes Instrumentés de Sécurité – cas du système d'arrêt d'urgence automatique d'un rebouilleur », s'inscrit dans ce contexte.

La démarche adoptée pour le traitement de ce sujet s'organise, logiquement en quatre chapitres qui sont :

Chapitre 1 : Il contient une introduction détaillée sur le sujet des SIS. Aussi nous présentons la problématique de notre étude et l'objectif assigné à notre démarche des d'évaluations de la performance des SIS.

Chapitre 2 : Un tour d'horizon est effectué décrivant la norme générique CEI 61508 disposant d'autres déclinaisons selon le secteur industriel. Cette norme formalise une démarche pour l'estimation du risque que présente le procédé et permet d'évaluer la diminution du risque que doit apporter le système instrumenté de sécurité. Ainsi qu'une vue d'ensemble sur les spécifications des critères de performance des barrières techniques de sécurité.

Chapitre 3 : Il a pour objectif de préparer une partie théorique sur les SIS basée sur la norme CEI 61511 et les notions de la sureté de fonctionnement, afin de faciliter la manipulation des paramètres au niveau de la méthodologie d'évaluation des performances.

Chapitre 4 : Il englobe la démarche adoptée pour l'évaluation de la performance du système d'arrêt d'urgence du four rebouilleur H201. Ainsi nous commençons par la définition du système, une analyse qualitative et en fin une analyse quantitative.

Chapitre I : Cadrage de l’étude

Introduction

L'industrie du process devient de plus en plus complexe, le potentiel de danger s'accroît en conséquence si les risques ne sont pas convenablement contrôlés. Ainsi, lorsque les installations industrielles présentent des risques potentiels pour les personnes, l'environnement ou les biens, diverses mesures de sécurité sont à mettre en œuvre [11]. Celles-ci s'inscrivent dans le cadre des mesures de maitrise des risques (MMR), elles participent à la prévention en minimisant la probabilité d'apparition du risque, ou à la protection pour limiter les conséquences d'un dysfonctionnement.

Les Systèmes Instrumentés de Sécurité (SIS) sont utilisés pour assurer la sécurité fonctionnelle des installations, autrement dit, réduire les risques à un niveau inférieur ou égal au risque tolérable. Pour concevoir les SIS, deux normes de sécurité sont utilisées : l'IEC 61508 [1] et l'IEC 61511 [6]. La mise en œuvre des prescriptions de ces deux normes n'est pas forcément triviale, et les méthodes proposées dans les annexes doivent être utilisées avec précaution [11].

La fiabilité est l'un des critères qui permet de juger la performance d'une Barrière Technique de Sécurité (BTS) , ce critère est souvent retranscrit à travers la probabilité de défaillance [12]. Cependant il existe d'autres critères de performance proposés par l'INERIS notamment dans l'article « Evaluation de la performance des barrières techniques de sécurité » qui nous permet d'évaluer explicitement la performance des SIS à l'aide d'une démarche multicritères.

1. Problématique

Les industries déploient beaucoup d'efforts pour éviter les accidents. Malgré ces efforts, de nombreux accidents se produisent dans le monde. Les conséquences des accidents se caractérisent par différents niveaux de gravité. L'analyse de leurs conséquences a permis l'évolution des études de sécurité afin de mieux maîtriser les risques.

Le groupe SONATRACH opère dans le secteur des hydrocarbures considéré à haut risque. Cette entreprise n'est pas à l'abri d'accidents majeurs qui peuvent engendrer des conséquences fatales sur le plan humain, environnemental ou économique. De ce fait, une analyse du retour d'expérience a classé les systèmes fours rebouilleurs comme points névralgiques, compte tenu de son mode de fonctionnement à chaud qui mérite une analyse approfondie de la sécurité fonctionnelle.

Au niveau de SONATRACH, le tableau suivant illustre les incidents les plus marquants survenus sur les fours et qui ont engendré la destruction totale de ces équipements. Le phénomène dangereux en cause, est un incendie qui a fait suite à la rupture des serpentins. Les impacts de ces incidents sont localisés et aucun dégât humain n'a été enregistré.

Tableau 1.1 : Incidents sur des fours rebouilleurs - SONATRACH

Date	Localisation	Equipement	Type d'accident	Dégâts
03/01/2013	Unité 100, Raffinerie RA1K, SH/ Aval, Skikda	Four	Incendie sur four rebouilleur (rénové par Samsung)	Four totalement détruit (1)
15/11/2003	GP2Z, SH/Aval, Arzew	Four	Incendie sur four rebouilleur	Four totalement détruit et un autre partiellement (2)
07/01/1989	MPP3, SH Amont, DP Hassi R'Mel	Four	Incendie sur four rebouilleur	Four totalement détruit (3)

L'analyse de ces incidents a révélé que les causes profondes sont des défaillances techniques, à savoir :

(1), suite à la rupture des serpentins au cours des tests de performance (augmentation de la charge).

(2) et (3), suite à la rupture du serpentin, la corrosion, les fissures ou les points chauds (cooking,..).

Sur la base de l'analyse du retour d'expérience, l'industrie et les compagnies d'assurance indiquent que 44 % des pertes des installations de procédés sont attribuables aux défaillances des fours [13].

La maîtrise des risques générés par les installations industrielles modernes ne pouvait être garantie sans l'utilisation d'un SIS. L'échec des SIS pour atteindre leurs fonctions assignées pourraient entraîner d'énormes conséquences, en ce qui concerne à la fois la sécurité du système surveillé, ainsi que la disponibilité de la production en raison des déclenchements intempestifs de ceux-ci.

Dans cette optique, nous avons jugé utile de développer un sujet traitant de la performance des SIS dans le cadre de la maitrise des risques industriels, pour faire, une question pertinente est posée, reformulée dans un contexte précis encadrant notre problématique, «**la performance des SIS, comment et quelle démarche à adopter ?** », qui peut être ainsi inscrite dans un contexte plus global c'est « **La maitrise des risques industriels par la maitrise des barrières techniques de sécurité** ».

Pour répondre à cette question, une approche basée sur les indicateurs de performance des barrières techniques de sécurité a été suivie, on fait appel aux attributs dits de : sûreté de fonctionnement (SdF), dont le choix a été porté sur la fiabilité, fondée sur le fait qu'elle est plus adaptée aux probabilités de défaillances et aux objectifs recherchés, notamment la détermination du niveau SIL. De plus, c'est une démarche qui possède une approche fiabiliste, et qui prend en considération l'évolution des systèmes dans le temps, cette composante est très importante lors de la conception des SIS.

L'approche globale de notre démarche est de déterminer les scénari dangereux avec les résultats de l'étude HAZOP du rebouilleur en question, ensuite nous évaluons le niveau SIL requis et nous déterminons le niveau SIL réel de la barrière technique de sécurité, pour notre étude, c'est le système d'arrêt d'urgence automatique. Ainsi nous comparons les deux niveaux SIL pour juger la performance du SIS envers ce critère, enfin nous évaluons l'efficacité et le temps de réponse en nous basant sur les résultats des recherches de l'INERIS.

2. Enjeux de la maitrise des barrières techniques de sécurité (BTS)

La notion d'enjeu regroupe l'ensemble des personnes, biens ou autres intérêts ; tels que l'environnement, susceptibles d'être affectés par un phénomène naturel ou technologique [14]. Ainsi la démarche de maitrise des BTS vise à concrétiser une grande partie des enjeux auxquels les entreprises sont confrontées, nous citons :

2.1. Enjeux Humains

Un accident grave a un coût important, particulièrement le nombre de victimes. Ainsi les enjeux humains se résument dans l'assistance de la sécurité des personnes, des travailleurs sur site, mais aussi les riverains et les citoyens. Ainsi les SIS visent à bloquer les déviations qui peuvent survenir dans les installations ou les unités de production, que ce soit une explosion, un incendie ou une dispersion de produit toxique.

2.2. Enjeux Environnementaux

Un accident industriel peut avoir des répercussions importantes sur les écosystèmes, notamment la destruction de la faune et la flore, mais les conséquences d'un accident peuvent également avoir un impact sanitaire (pollution de la nappe phréatique, albienne….). De ce fait, les BTS visent, aussi, la préservation de l'environnement face aux impacts réels ou potentiels en cas de dysfonctionnement ou accident.

2.3. Enjeux Réglementaires

L'historique des catastrophes dans le monde a marqué la mémoire humaine à jamais. L'évolution de la réglementation est étroitement liée aux catastrophes ayant produit de nombreuses victimes. Les enjeux réglementaires ont pour objectif de se maintenir en conformité avec la réglementation en vigueur.

Dans ce contexte, l'Algérie a mis en disposition une stratégie de la prévention des risques industriels majeurs, traduite par la loi **04/20** du 25/12/2004 relative à la prévention des risques majeurs et à la gestion des catastrophes dans le cadre du développement durable.

En France, nous retenons l'arrêté du 4 octobre 2010, relatif à la prévention des risques accidentels au sein des Installations Classées pour la Protection de l'Environnement (ICPE), soumises à autorisation, il définit des dispositions relatives à la prévention des risques liés au vieillissement de certains équipements (réservoirs aériens cylindriques verticaux, capacités, tuyauteries, massifs des réservoirs, cuvettes de rétention, mesures de maîtrise des risques instrumentées)[15].

2.4. Enjeux Economiques

Les accidents industriels sont accompagnés d'une perte partielle ou totale de l'installation, d'un arrêt de la production et de la perte des recettes. Ajoutant ainsi, les coûts de dédommagement des victimes et de la réparation des dommages. De plus, l'image de marque d'une entreprise est généralement affectée après un accident majeur, en particulier, si l'enquête révélait l'absence de dispositifs de maîtrise des risques.

3. Objectifs

Les recherches sur les SIS tiennent une grande partie des travaux réalisés sur la sécurité industrielle. De ce fait, le niveau d'avancement de la technologie d'instrumentation et d'automatisation reflète la performance de ces systèmes, particulièrement, au niveau des installations à haut risque.

Dans cette optique, l'objectif de ce travail est, d'abord, de proposer une démarche complète d'évaluation de la performance des SIS, au regard des objectifs de disponibilité et de sécurité, Ainsi proposer une allure qui parte des scénari critiques aux SIS, et de la configuration des SIS aux indicateurs de performance.

Pour atteindre cet objectif principal, il est favorable de s'appuyer sur les résultats des recherches effectuées par l'INERIS, surtout, en ce qui concerne les indicateurs de performance, à savoir que notre travail est cadré par les deux normes CEI 61508 et CEI 61511.

Il est important de rappeler que nous allons évaluer la performance du système d'arrêt d'urgence automatique du four rebouilleur H201. Ceci assure le rebouillage de la colonne de distillation, d'où l'importance de cet unité dans le bon fonctionnement de l'usine afin d'assurer le traitement typique du gaz brut. En conséquence, les résultats de ce travail vont servir comme références au plan de développement des installations du Groupe SONATRACH.

Conclusion

Ce chapitre a permis de s'introduire dans le sujet, comprendre le pourquoi de cette étude, poser une problématique de la maitrise des barrières techniques de sécurité dans le secteur pétrolier, ses enjeux qui demeurent une préoccupation majeure des industriels, des autorités et de toute la société, puis mettre en lumière la démarche suivie pour le traitement du sujet concernant, « **l'évaluation de la performance des systèmes instrumentés de sécurité –système d'arrêt d'urgence du rebouilleur H201** ».

Chapitre II : De la sécurité fonctionnelle à la maitrise des risques

Introduction

Parallèlement à l'évolution du progrès technique et de l'industrialisation, la prévention des risques industriels s'est considérablement développée tout au long du dernier siècle [16]. Les travaux normatifs appliqués à ce cadre font appel à des domaines scientifiques et techniques multiples ; sciences pour l'ingénieur, sciences humaines et sociales, sciences de la vie. Nous limitons ici notre propos au domaine technique des instruments et des systèmes de sécurité automatisés.

Afin d'éviter des dommages sur les personnes, l'environnement ou les biens qui peuvent être occasionnés, les industriels sont amenés à mettre en place des Barrières Techniques de Sécurité (BTS). Parmi ces barrières, les systèmes instrumentés de sécurité (SIS), sont caractérisés par le fait qu'une défaillance peut avoir des conséquences graves, tant sur la vie des personnes que du point de vue économique et/ou environnemental [17].

Dans ce chapitre, l'intérêt est porté sur les notions générales et les concepts liés à la sécurité fonctionnelle et à la maitrise des risques. Nous nous focalisons sur les principes de la norme CEI 61508, qui est issue d'un large consensus international, pour décliner de nombreux textes qui non seulement ne peuvent être ignorés, mais qui doivent avantageusement guider les développements des concepteurs. Finalement, nous présentons l'approche d'évaluation des BTS proposée par l'INERIS.

1. Notions générales

Afin de maintenir les performances des systèmes de sécurité, il convient à faire des analyses approfondies, à l'image des modélisations du comportement fonctionnel et dysfonctionnel des systèmes, puis les évaluer [18]. La sécurité des processus industriels dépend de l'interaction du contrôle, et de la maîtrise permanente de trois variables essentielles : le produit, le procédé et le facteur humain.

1.1. Notion de système

La notion de système a été utilisée probablement par les militaires (système d'armes) vers 1945. Au début, cette notion a progressé très lentement, puis brutalement ; depuis 1960 environ, elle s'est imposée dans le domaine technique [11].

La notion de système fait l'objet de la définition suivante [10]: « ...ensemble de matériels, de logiciels, d'hommes, organisé pour assurer des fonctions données dans des conditions données... ».

Un système peut être considéré de plusieurs façons :

- depuis son environnement, comme élément spécifique de type « boîte noire » avec des entrées et des sorties qui permettent d'en étudier le fonctionnement ;
- de l'intérieur, par la mise en évidence :
  - de ses caractéristiques physiques (par décomposition organique en sous-systèmes et composants),
  - de ses modes d'organisation (relationnelles, hiérarchiques, ...),
  - de ses propriétés (autonomie, robustesse, vulnérabilité, ...),
  - de son comportement (dynamique d'évolution, productivité, ...).

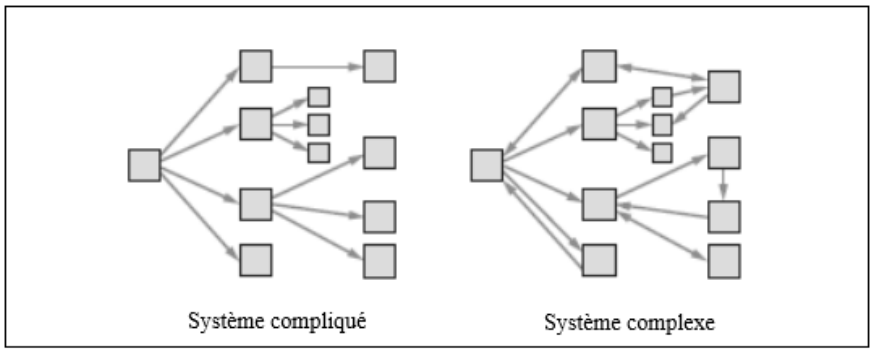


Figure 2.1 - Complexité d'un système [2]

1.2.Intégrité de Sécurité

La sécurité reste un terme très général. Il n'existe pas, actuellement, de consensus pour une normalisation [19]. Parallèlement, il n'existait pas une définition de la sécurité au sens large des normes internationales. Cependant, le guide 51 élaboré par l'organisation internationale de standardisation (ISO) et CEI intitulé « Aspects de la sécurité » définit la sécurité comme étant « l'absence de risque inacceptable » [20].

D'après la norme CEI 61508, l'intégrité de sécurité est la probabilité qu'un système de sécurité Electrique / Electronique / Electronique Programmable (E/E/EP) puisse exécuter de manière satisfaisante les fonctions de sécurité spécifiées dans toutes les conditions énoncées dans une période déterminée [21].

Le haut niveau d'intégrité de sécurité correspond, à la plus faible probabilité qu'un système de sécurité ne parvient pas à remplir ses fonctions de sécurité spécifiées, ou ne parvient pas à adopter un état spécifique requis.

1.2.1. Intégrité des systèmes de sûreté

La sûreté de l'installation exige que les équipements et les systèmes assurant les fonctions fondamentales de sûreté du processus de traitement (contrôle de pression, refroidissement du gaz brut, torché les résidus et confinement) soient disponibles en permanence [22].

Or, un incendie par exemple peut perturber fortement le fonctionnement de ces systèmes que ce soit, directement par la destruction d'une partie du système, ou indirectement en provoquant, par exemple, un dysfonctionnement due à l'augmentation de la température ambiante.

1.2.2. Sécurité des personnes

Cet objectif nécessite la mise en œuvre de dispositions d'évacuation rapide des personnes, quel que soit l'endroit où elles se trouvent, aussi la protection des équipes d'intervention dans le cas où un accident se produit. Toutes les infrastructures de l'installation doivent comporter, en conséquence, un réseau permettant à partir de toute unité de rejoindre l'extérieur.

1.2.3. Sécurité des équipements et maintien de la disponibilité

Plus globalement, les matériels vieillissants sont les plus régulièrement touchés par des défaillances, qui se traduisent immédiatement par une baisse de l'activité. Cela se traduit aussi par des pertes financières liées aux coûts de remise en état, aux pertes de production ou à la baisse de disponibilité [23].

1.3.Notion de réduction des risques

1.3.1. Principe général

La réduction des risques consiste à mettre en œuvre un ensemble de mesures, que ce soit de protection et/ou de prévention, afin de diminuer la valeur de risque quantifiée à un niveau acceptable. La réduction du risque nécessaire peut être obtenue en combinant un ou plusieurs SIS ou d'autres mesures de protection.

Les résultats d'une évaluation des risques nous permettent d'élaborer un document dans lequel il est indiqué la procédure suivie, les dangers identifiés et les mesures de réduction des risques employées pour réduire les risques à un niveau acceptable [20].

La réduction du risque nécessaire est la réduction qui doit être réalisée pour satisfaire le risque tolérable (risque acceptable) associé à une situation spécifique. Le concept de réduction des risques est d'une importance fondamentale dans le développement des exigences de sécurité pour les produits et les systèmes.

La prévention des accidents se rapporte à l'élimination de dangers ou à la diminution de l'occurrence d'événements redoutés, par l'amélioration de la sécurité des dispositifs de contrôle, ou par l'implantation des moyens empêchant l'apparition ou la propagation des dangers.

La protection vient après l'échec des moyens de prévention, et se rapporte à l'atténuation des conséquences d'un accident par des moyens limitant les dommages (systèmes de secours, procédures d'urgence).

La figure 2.2 représente un modèle de risque généralisé pour illustrer des principes généraux. Un modèle de risque associé à application spécifique, devra être élaboré en tenant compte de la manière dont la réduction du risque est réalisée. Autrement dit, il peut être différent de celui de la figure 2.2.

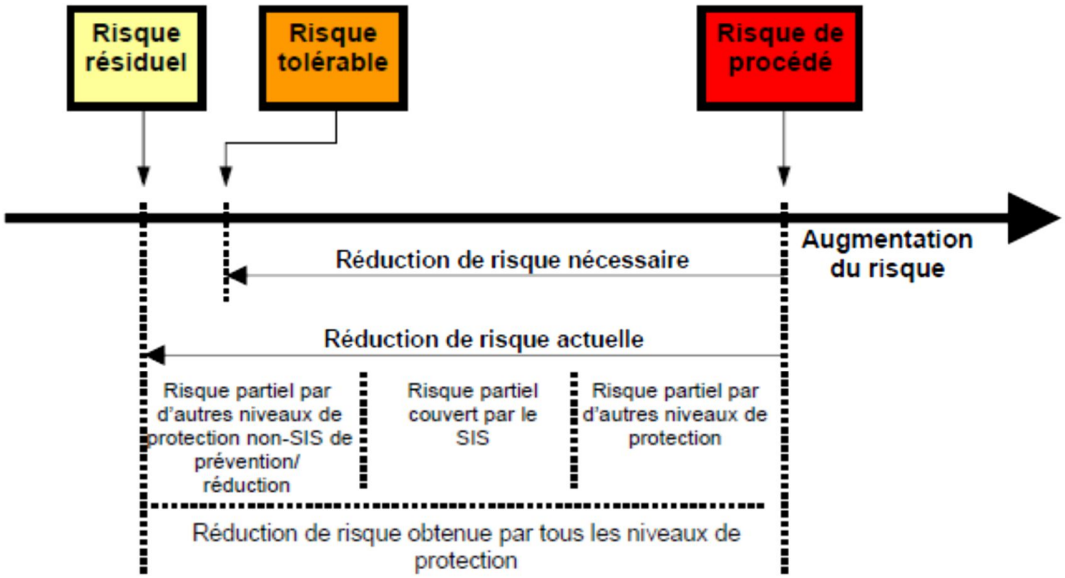


Figure 2.2 - Réduction du risque : Concepts général [5]

Les différents risques indiqués dans la figure ci-dessus sont les suivants :

- **Risque de procédé (risque industriel)** : risque encouru par un équipement sous contrôle (EUC), son système de commande, et les facteurs humains associés pour les événements dangereux spécifiés. Aucun dispositif de protection spécifique n'est pris en compte dans la détermination de ce risque.
- **Risque tolérable** : risque accepté dans un contexte fondé sur les valeurs actuelles de la société.
- **Risque résiduel** : risque encouru par l'EUC, son système de commande et les facteurs humains associés pour les événements dangereux spécifiés, y compris les dispositifs externes de réduction de risque.

1.3.2. Modèle ALARP

Les SIS sont l'un des dispositifs les plus utilisés pour réduire les risques associés aux d'accidents majeurs. Ils peuvent être trouvés sous forme de divers systèmes tels que : système d'arrêt d'urgence, système feu et gaz et système de protection des machines. Un seul SIS fournit normalement une protection contre un seul danger, cela pose un dilemme pour les concepteurs quand ils essaient de répondre aux besoins globaux de réduction de risque aussi bas que raisonnablement possible (ALARP).

1.3.2.1.Concepts

Le principe ALARP impose d'amener les risques au plus bas niveau possible, ou jusqu'à un niveau qui soit aussi faible que possible de manière raisonnable [5]. Si un risque se situe entre les deux extrêmes (c'est-à-dire la zone inacceptable et la zone globalement acceptable) et si le principe ALARP a été appliqué, le risque résultant est le risque tolérable pour l'application concernée. Cette approche des trois zones est illustrée à la figure 2.3.

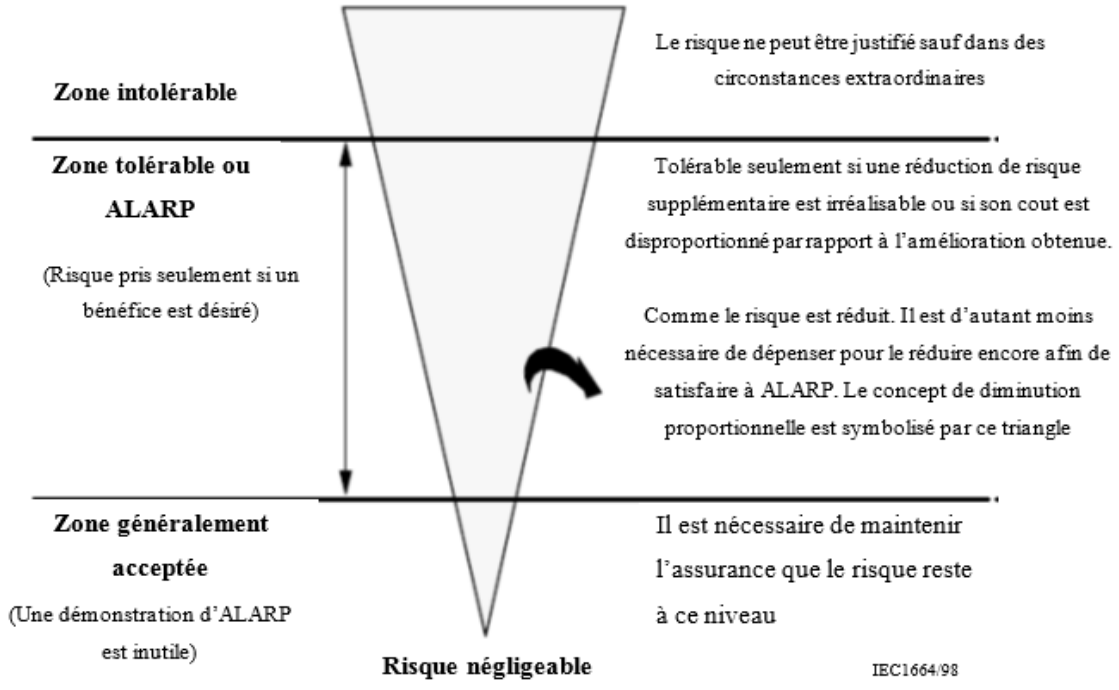


Figure 2.3 - Risque tolérable et ALARP [5]

1.3.2.2.Barrières de réduction des risques

Ce concept de barrières repose sur le principe des moyens mis en œuvre pour réduire les risques. Ces différents moyens sont prévus pour intervenir de manière graduelle dans le temps. En d'autres termes, ces différentes couches vont être «sollicitées » tour à tour avec un objectif de bloquer le déroulement du scénario d'accident ou d'en réduire les effets [24].

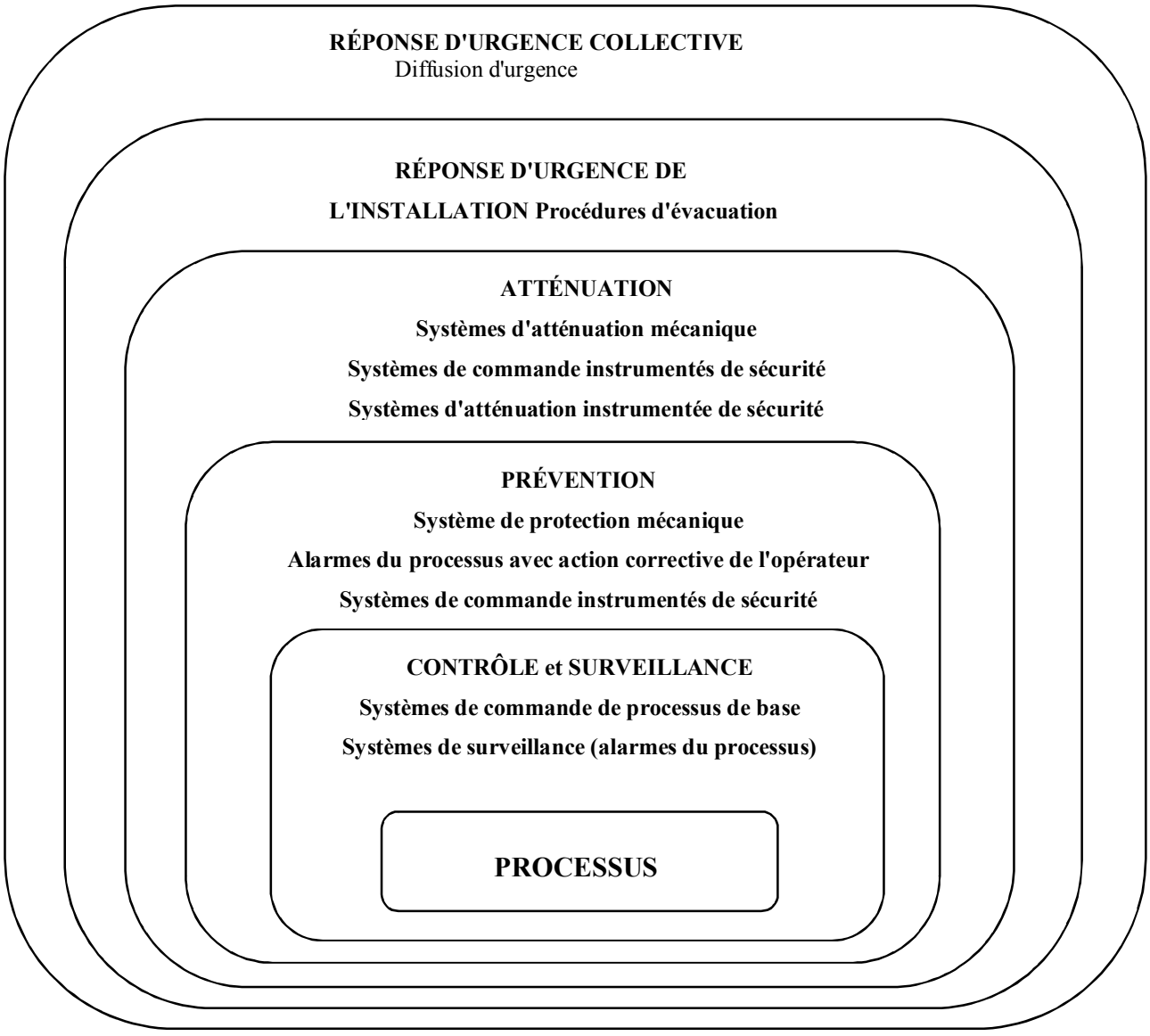


Figure 2.4 - Méthodes habituelles de réduction de risque rencontrées dans les industries de process [6]

1.4.Notion de défaillance

Une défaillance se définit comme étant « l'altération ou la cessation de l'aptitude d'un ensemble à accomplir sa ou ses fonction(s) requise(s) avec les performances définies dans les spécifications techniques » [25].

Un ensemble est défaillant si ses capacités fonctionnelles sont interrompues (panne ou arrêt volontaire par action d'un système interne de protection ou une procédure manuelle équivalente).

1.4.1. Typologie des défaillances techniques

Pour un fiabiliste, la défaillance d'un composant est perçue comme la transition adjugée entre son état « bon » et un état « mauvais » où il n'est plus utilisable [26]. Au niveau du chapitre 4 de la norme CEI 61508, nous trouvons la typologie suivante [21]:

1.4.1.1.Défaillance systématique

Elle est liée d'une manière déterministe à une certaine cause, qui ne peut être éliminée par une modification de la conception ou du processus de fabrication, des procédures opérationnelles, de la documentation ou d'autres facteurs pertinents.

1.4.1.2.Défaillance dangereuse

C'est la défaillance d'un élément et / ou d'un sous-système et / ou d'un système qui joue un rôle dans la mise en œuvre de la fonction de sécurité qui :

a) empêche une fonction d'agir quand c'est nécessaire (mode à la demande) ou bouscule une fonction de sécurité à l'échec (mode continu) de telle sorte que l'EUC est mis dans un état dangereux ou potentiellement dangereux ; ou

b) diminue la probabilité quand la fonction de sécurité fonctionne correctement en cas de besoin.

1.4.1.3.Défaillance non dangereuse

C'est la défaillance d'un élément et / ou le sous-système et / ou d'un système qui joue un rôle dans la mise en œuvre de la fonction de sécurité qui :

a) Résulte dans le fonctionnement intempestif de la fonction de sécurité à mettre l'EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité ; ou

b) Augmente la probabilité de l'opération parasite de la fonction de sécurité de mettre la EUC (ou une partie de celui-ci) dans un état de sécurité ou de maintenir un état de sécurité.

1.4.2. Causes de défaillances

Le tableau 2.1 précise les principales causes de défaillances des structures et les principales mesures préventives ou parades à mettre en œuvre pour réduire le risque.

On remarque qu'il y a deux types de mesures permettant de réduire le risque ou les effets de défaillances :

- des mesures préventives, destinées à diminuer la probabilité de défaillance :
  - prise en compte à la conception,
  - facteurs de sécurité,
  - démarche assurance qualité,
  - inspection en service.
- des mesures de précaution, destinées à diminuer les effets d'une éventuelle défaillance :
  - mesures de protection,
  - tolérance au risque.

Tableau 2.1 – Causes de défaillances et mesure pour réduire le risque.

Conditions de service	**Cause de la défaillance**	**Parades**
Conditions de fonctionnement normal	• Surcharge • Problèmes de matériaux • Vieillissements dus à des mécanismes de dégradation physiques (corrosion, fatigue...)	- Prise en compte à la conception - Facteurs de sécurité - Essais - Inspections en service - Mesures de protection
Conditions accidentelles	• Causes accidentelles - agression par un tiers - incendie - explosion • Événements naturels (séisme, grand froid, tempête...)	- Prise en compte à la conception - Mesures de protection - Surveillance
Erreurs humaines	• Erreur humaine - à la conception - à la fabrication - à l'exploitation • Défaut d'organisation	- Assurance qualité - Audit indépendant - Surveillance - Inspection - Tolérance au risque - Mesures de protection - Formation du personnel

2. Norme CEI 61508

Les systèmes électriques/électroniques sont utilisés depuis des années, pour exécuter des fonctions liées à la sécurité dans la plupart des secteurs industriels. La norme CEI 61508 présente une approche générique de toutes les activités liées au cycle de vie de la sécurité des systèmes E/E/EP, qui sont utilisés pour réaliser des fonctions de sécurité.

La norme CEI 61508 ne couvre pas les aspects de confidentialité et/ou d'intégrité qui sont liés à la mise en place de précautions de sécurité. Ainsi elle ne vise pas à empêcher les personnes non autorisées à endommager ou affecter la sécurité réalisée par les systèmes E/E/PE concernés par la sécurité [17].

2.1.Champ d'application

La norme CEI 61508 s'applique aux systèmes de sécurité E/E/EP destinés à exécuter des fonctions de sécurité. Elle concerne les applications pour lesquelles un défaut des systèmes est susceptible d'avoir un impact considérable sur la sécurité des personnes, de l'environnement et des installations. À ce jour, cette norme constitue l'un des principaux textes de référence pour la spécification, la conception et le fonctionnement opérationnel des SIS. En revanche, l'apparition de cette norme n'est pas récente puisque sa déclinaison en norme française date de 1999 (NF EN 61508) [27].

2.2.Chapitres de la norme

L'IEC 61508 est composée de sept chapitres :

- CEI 61508-1. Exigences générales [1];
- CEI 61508-2. Exigences pour les systèmes électriques/ électroniques/électroniques programmables concernés par la sécurité [28];
- CEI 61508-3. Exigences pour le logiciel [29];
- CEI 61508-4. Définitions et abréviations [21];
- CEI 61508-5. Exemples de méthodes pour la détermination des niveaux d'intégrité de la sécurité [5];
- CEI 61508-6. Directives pour l'application de la CEI 61508-2 et de la CEI 61508-3 [30];
- CEI/IEC 61508-7. Vue d'ensemble de mesures et de techniques [3].

La norme CEI/IEC 61508 propose une approche globalisée de la sécurité, au sens de sécurité innocuité, que l'on pourrait comparer au système ISO 9000 pour la qualité.

Cette norme s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs E/E/EP. Elle comprend 7 parties (figure 2.5), afin de couvrir les multiples aspects des systèmes E/E/PE :

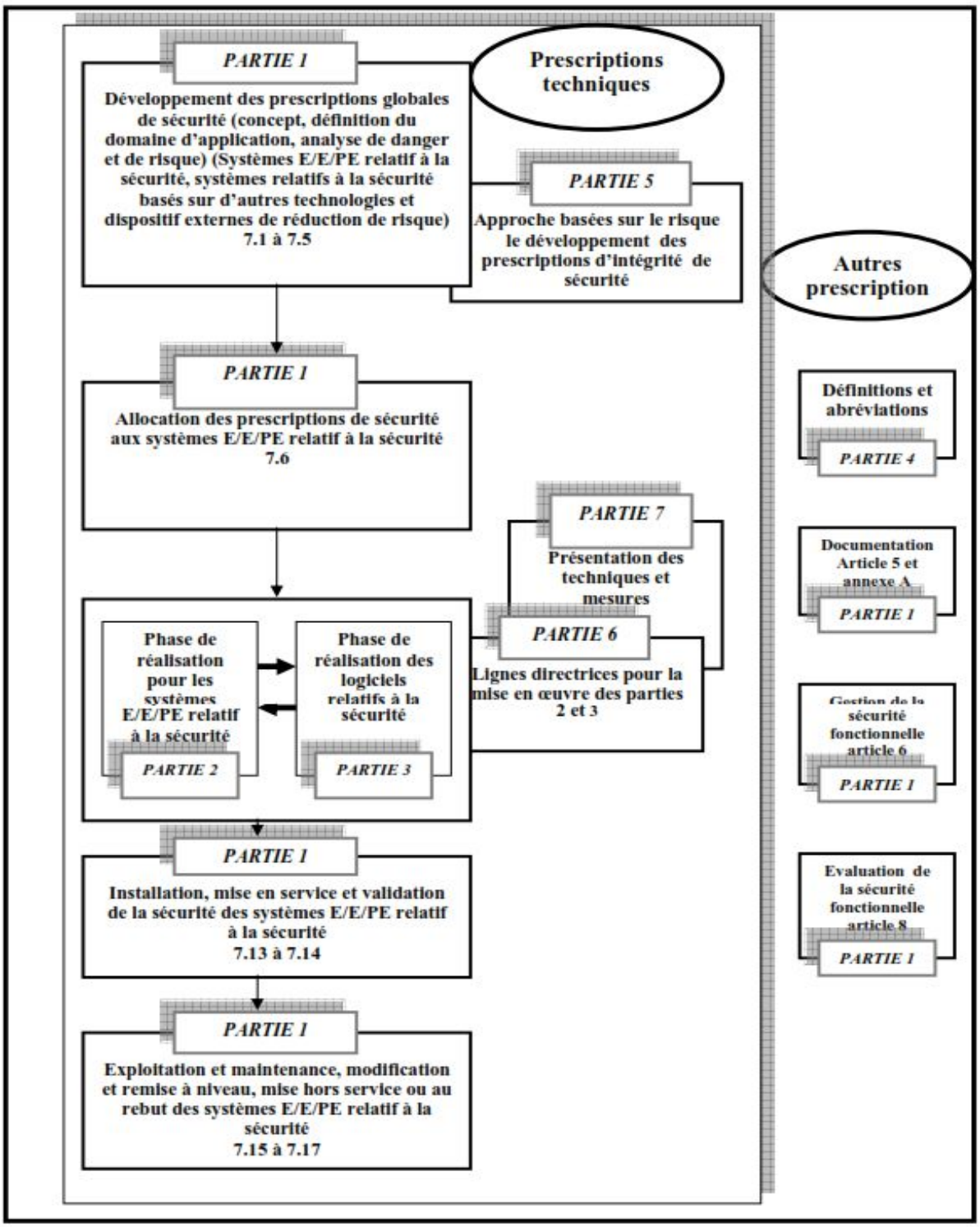


Figure 2.5 - Structure générale de la norme IEC 61508 [3]

2.3.Objectif de la CEI 61508

La norme internationale CEI 61508, Sécurité Fonctionnelle des systèmes E/E/EP concernés par la sécurité, a pour but de :

- Fournir le potentiel de technologie E/E/PE pour améliorer à la fois les performances économiques et la sécurité,
- Permettre des développements technologiques dans un cadre global de sécurité,
- Fournir une approche système, techniquement saine, suffisamment flexible pour le futur,
- Fournir une approche basée sur le risque pour déterminer les performances des systèmes concernés par la sécurité,
- Fournir une norme générique pouvant être utilisée par l'industrie, mais qui peut également servir à développer des normes sectorielles (par exemple : machines, usine chimiques, ferroviaire ou médical) ou des normes produit (par exemple : variateurs de vitesse),
- Assurer les moyens aux utilisateurs et aux autorités de réglementation d'acquérir la confiance dans les technologies basées sur l'informatique.

2.4.Limites de la CEI 61508

Le succès de la CEI 61508 n'est pas quelque chose qu'on aurait pu être facilement prédit, c'est ainsi que Rainer FALLER a commenté dans son article « Expérience tirée des projets sur la norme CEI 61508 et ses conséquences » [31].

La Norme IEC 61508 et ses normes dérivées constituent un document volumineux difficile à lire et à interpréter. L'ambiguïté possible dans l'interprétation encourage beaucoup à utiliser la norme comme une boîte à outils où ils sortent et nécessitent la mise en œuvre ou de ce qu'ils comprennent ou estiment qu'il est intéressant [31].

Les limites de la norme CEI 61508 sont liées à la complexité et à la difficulté de son utilisation. Plusieurs utilisateurs de l'CEI 61508 ont mentionné la nécessite d'être guidés, tant ses notions paraissent complexes, et difficiles à mettre en œuvre. Beaucoup de prescriptions ne sont pas assignées à une certaine gamme de niveaux d'intégrité de sécurité ou à la complexité de la conception. En conséquence, Cela rend la norme difficile à utiliser pour de petits projets et rend la gestion de la sécurité fonctionnelle trop chère pour des petites et moyennes entreprises.

2.5.Sécurité fonctionnelle

La sécurité fonctionnelle se définit comme étant « un sous-ensemble de la sécurité globale, relatif aux équipements et aux systèmes de contrôle-commande associés, qui dépend du fonctionnement correct de systèmes (E/E/PE) concernés par la sécurité » [21].

Les exemples suivants sont des systèmes E/E/EP concernés par la sécurité :

- Un système de déclenchement dans une usine chimique dangereuse,
- Un système de signalisation ferroviaire,
- Des inter-verrouillages de protection et un arrêt d'urgence sur une machine,
- Un variateur de vitesse utilisé pour contrôler une vitesse en tant que moyen de protection,
- Autres systèmes concernés par la sécurité non dédiés à la sécurité.
- L'analyse des risques détermine si la sécurité fonctionnelle est nécessaire pour assurer une protection adéquate contre chaque risque significatif. Si c'est le cas, alors cela doit être pris en compte de manière appropriée lors de la conception [32].

2.6.Cycle de vie de sécurité

La notion de cycle de vie de sécurité global proposée par la norme CEI 61508 est à rapprocher des principes édictés par la norme EN ISO 12100 [16]. Elle correspond à une démarche générale de conception destinée à systématiser toutes les activités nécessaires, afin d'assurer le niveau d'intégrité de sécurité (SIL) prescrit pour une application et les systèmes E/E/PE relatifs à la sécurité qu'elle nécessite.

Partant du principe qu'il est nécessaire de construire la sécurité à chaque étape de la vie d'un système, la norme structure les prescriptions pour couvrir l'ensemble des activités qui correspondent au cycle de la vie d'un SIS.

En conséquence, la norme CEI 61508 est fondée 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, la figure 2.6. Le cycle de vie fournit un guide complet pour l'établissement des caractéristiques et spécifications relatives aux fonctions de sécurité allouées aux SIS.

Dans toute fonction de processus, la sécurité fonctionnelle obtenue dépend d'un certain nombre d'activités exécutées de manière satisfaisante, l'adoption d'une approche systématique du cycle de vie de sécurité vis-à-vis les systèmes E/E/EP, vise à s'assurer que toutes les activités nécessaires pour obtenir la sécurité fonctionnelle, sont conduites et exécutées dans un ordre approprié. La CEI 61508-2 présente un cycle de vie typique (annexe 3).

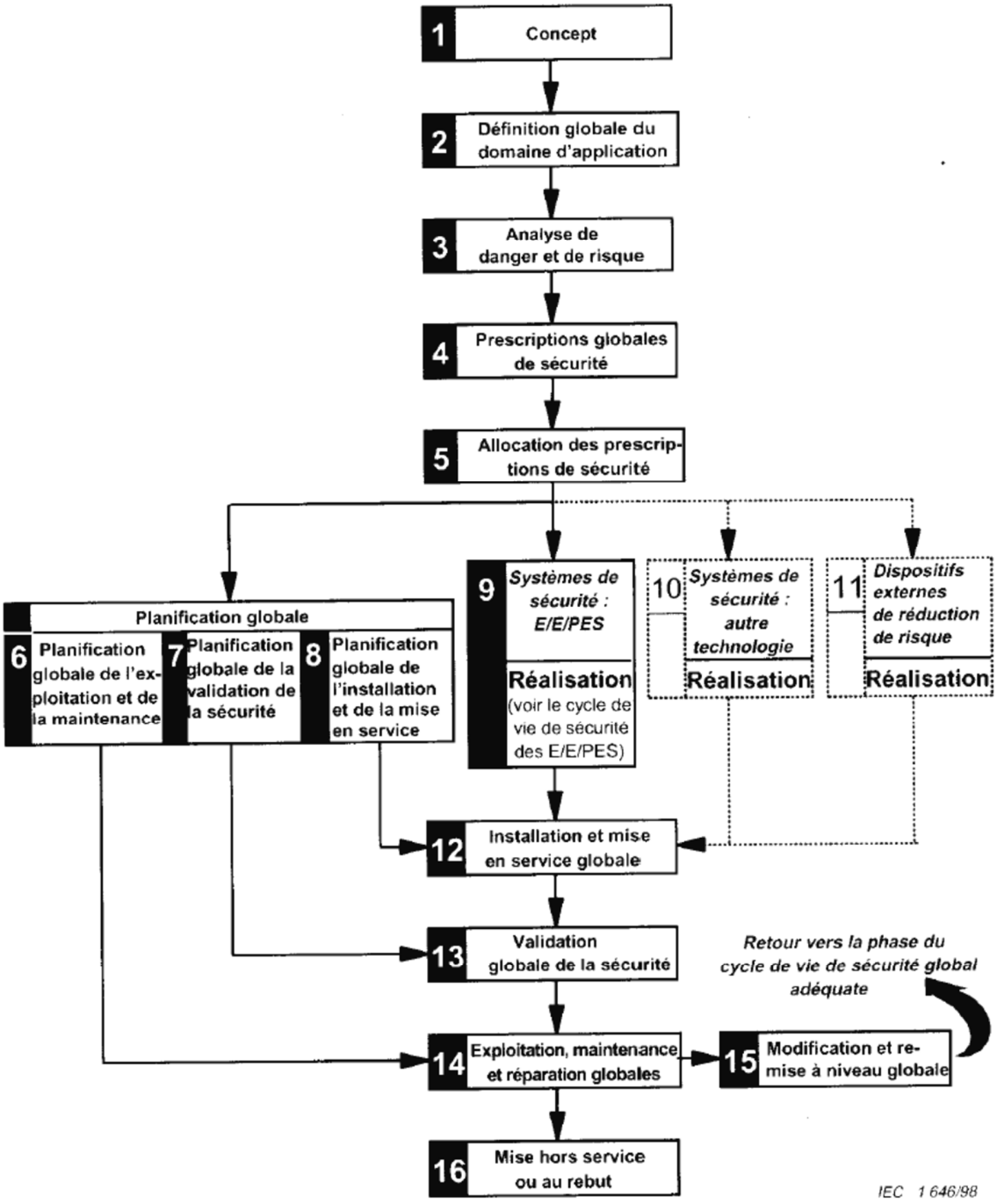


Figure 2.6 - Cycle de vie de sécurité globale [1]

3. Evaluation de la performance des barrières technique de sécurité (BTS)

Dans la réglementation française, les exploitants industriels doivent justifier les choix de conception des équipements de sécurité mis en place sur leurs installations, afin d'atteindre un niveau de risque aussi bas que possible, compte-tenu de l'état des connaissances et des pratiques et de la vulnérabilité de l'environnement de l'installation. Dans ce contexte, l'Institut National de l'Environnement Industriel et des Risques (INERIS) a proposé une réflexion pour éclaircir et faciliter la manipulation des outils d'évaluation des Barrières Techniques de Sécurité (BTS). Dans ce qui suit, une présentation de cette méthodologie [7].

3.1.Présentation générale

L'INERIS de par son expérience avec les risques industriels, par le biais des plusieurs recherches effectuées et les différentes articles publiés sous le logo OMEGA, une méthodologie a fait l'objet d'une proposition pour évaluer la performance des BTS, cette dernière permet :

- à l'exploitant de disposer d'une méthodologie pour évaluer la performance des BTS appelées aussi mesures de maîtrise des risques (MMR),
- à l'inspection des installations classées et à des organismes tiers-experts de disposer indirectement d'outils permettant d'apprécier l'évaluation des performances des barrières techniques de sécurité faite par l'exploitant des installations et présentée dans les études des dangers.

3.2.Types de BTS

Les barrières de sécurité (ou mesures de maîtrise des risques) sont de trois types :

- Les barrières techniques,
- Les barrières humaines,
- Les barrières qui font intervenir les barrières techniques et humaines. Ces barrières sont appelées systèmes à action manuelle de sécurité. Dans la catégorie des barrières techniques de sécurité, il peut s'agir de dispositifs de sécurité ou de systèmes instrumentés de sécurité

3.2.1. Dispositifs de sécurité

Un dispositif de sécurité est en général un élément unitaire, autonome, ayant pour objectif de remplir une fonction de sécurité, dans sa globalité.

Un dispositif peut être classé en 2 catégories :

- Les dispositifs passifs qui ne mettent en jeu aucun système mécanique pour remplir leur fonction et qui ne nécessitent ni action humaine (hors intervention de type maintenance), ni action d'une mesure technique, ni source d'énergie externe pour remplir leur fonction. On retrouve notamment dans cette

catégorie les cuvettes de rétention, les disques de rupture, les arrête-flammes ainsi que les murs coupe-feu.

- Les dispositifs actifs qui mettent en jeu des dispositifs mécaniques (ressort, levier…) pour remplir leur fonction. On retrouve notamment dans cette catégorie les soupapes de décharge et les clapets limiteurs de débit. Ils peuvent nécessiter une source d'énergie externe pour fonctionner.

3.2.2. Systèmes Instrumentés de sécurité (SIS)

Les systèmes instrumentés de sécurité (SIS) sont des combinaisons de capteurs, d'unité de traitement et d'actionneurs (équipements de sécurité) ayant pour objectif de remplir une fonction ou sous-fonction de sécurité. Un SIS nécessite une énergie extérieure pour initier ses composants et mener à bien sa fonction de sécurité. Un SIS est composé de trois sous-fonctions : il s'agit des sous-fonctions « détection », « traitement de l'information» et « action ».

3.2.3. Systèmes à action manuelle

Les systèmes à action manuelle de sécurité sont des barrières mixtes à composantes techniques et humaines : l'opérateur est en interaction avec les éléments techniques du système de sécurité qu'il surveille ou sur lesquels il agit.

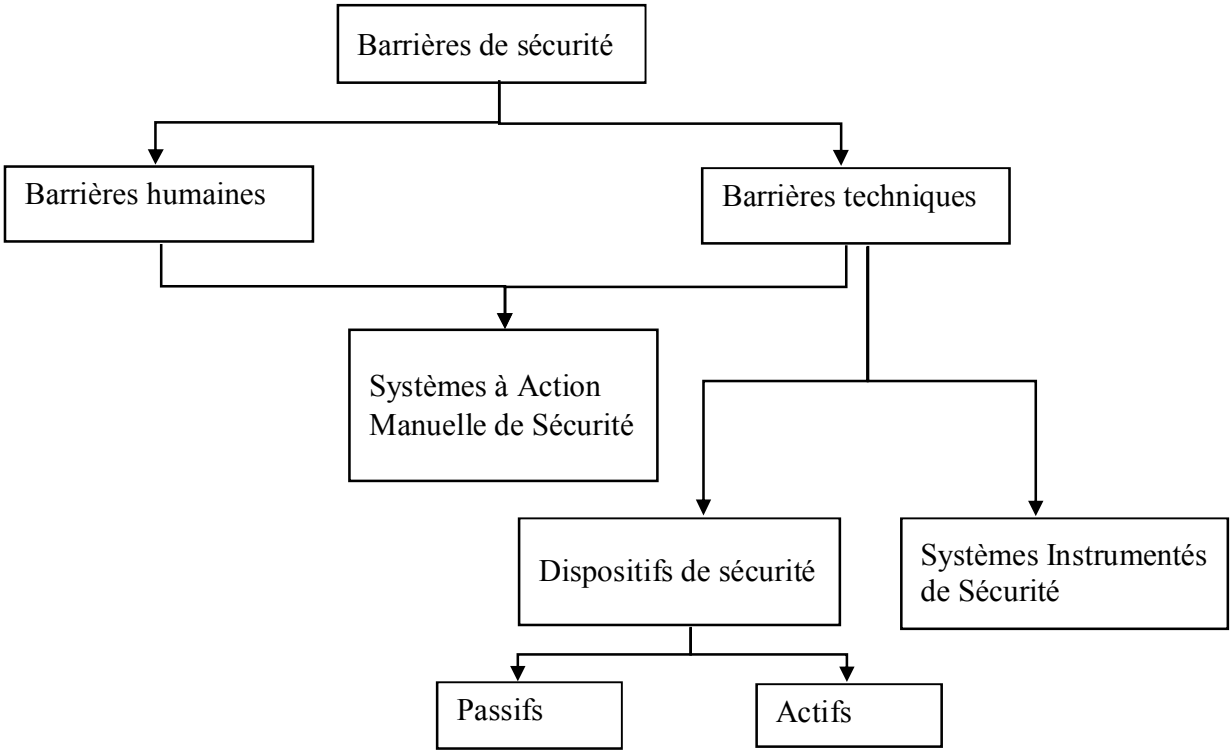


Figure 2.7 - Typologie des Barrières Techniques de Sécurité [7]

3.3.Critères de performance des BTS

3.3.1. Niveau de confiance (NC)

L'évaluation des probabilités d'occurrence des phénomènes dangereux fait intervenir les facteurs de réduction de risques induits par les barrières de sécurité. L'INERIS a retenu pour qualifier le facteur de réduction de risques le niveau de confiance (NC) de la barrière.

Dans les normes CEI 61508 et CEI 61511, l'évaluation des facteurs de réduction de risque repose sur deux aspects :

- L'aspect qualitatif : l'architecture définit des SIL maximums ;
- L'aspect quantitatif : les calculs de fiabilité permettent de déterminer les paramètres liés à la fiabilité (Probabilité moyenne de défaillance PFD_{avg} et taux de défaillance instantané PFH) qui conditionnent également le niveau de SIL. C'est le SIL minimum issu des deux approches qui doit ensuite être retenu pour le SIL du système.

L'INERIS retient, dans sa démarche explicitée dans cette partie, les aspects qualitatifs. Il est ainsi supposé que les caractéristiques des systèmes (données relatives à la fiabilité) permettent d'assurer la contrainte quantitative. Le SIL d'un dispositif peut conduire à déterminer un NC, sous réserve de la mise en œuvre adéquate du système sur site et que les conditions de la certification du dispositif soient les mêmes que celles d'utilisation du dispositif sur site.

3.3.2. Efficacité

L'efficacité est l'aptitude de la barrière de sécurité à remplir la fonction de sécurité pour laquelle elle a été choisie, dans son contexte d'utilisation et pendant une durée donnée de fonctionnement. L'efficacité est évaluée notamment pour un scénario d'accident précis [7].

La mesure d'efficacité s'exprime en pourcentage d'accomplissement de la fonction de sécurité définie, en considérant un fonctionnement normal de la barrière (non dégradé). Le pourcentage d'efficacité peut varier pendant la période de sollicitation de la BTS.

Dans beaucoup de situations, l'efficacité est de 100%. Ainsi, une soupape de sécurité correctement dimensionnée permettra de prévenir l'éclatement du réservoir qu'elle protège. De même, une vanne parfaitement étanche permettra d'isoler une fuite de substance en cas de perte de confinement sur une canalisation.

Mais une barrière de sécurité peut ne pas être efficace à 100% ; elle sera alors retenue comme barrière de sécurité mais l'intensité du phénomène dangereux associé au fonctionnement de la barrière est alors évaluée en tenant compte de l'efficacité réelle de la barrière.

3.3.3. Temps de réponse

Le temps de réponse correspond à l'intervalle de temps entre le moment où une barrière de sécurité, dans un contexte d'utilisation, est sollicitée et le moment où la fonction de sécurité assurée par cette barrière de sécurité est réalisée dans son intégralité [7].

Selon cette définition, le temps de réponse intègre :

- Le temps nécessaire au fonctionnement d'une détection de l'incident suite à sa sollicitation,
- Le temps nécessaire à la transmission de l'information à la ou les barrières de sécurité devant remplir la fonction de sécurité,
- Le temps nécessaire à la réalisation de l'action de sécurité.

Le temps de réponse de la barrière technique de sécurité peut a priori être obtenu de deux façons:

- soit en réalisant des mesures de temps de réponse, sur site, des barrières de sécurité (dispositifs de sécurité, équipements de sécurité et chaîne complète de sécurité),
- soit en additionnant les temps de réponse des dispositifs constituant la barrière de sécurité. Ces temps de réponse peuvent être fournis par les constructeurs.

Il est à noter que, comme le montrent les résultats statistiques d'une étude, il faut être prudent avec les performances annoncées des dispositifs de sécurité par les fabricants.

Cette étude comporte des essais menés sur 107 matériels en 5 ans, seulement un sur deux répondait globalement à l'ensemble des spécifications annoncées [7].

Conclusion

Dans ce chapitre, nous avons d'abord rappelé la définition de certains concepts utilisés dans le cadre de la sécurité fonctionnelle des systèmes de sécurité. A ce titre, la démarche générale de la gestion des risques a également été présentée et brièvement expliquée. Puis nous avons précisé l'organisation de la norme CEI 61508 relatives aux systèmes de sécurité, qui sont utilisés pour détecter des situations dangereuses et diminuer leurs conséquences pour atteindre des niveaux de risques tolérables.

Nous avons précisé que la démarche générale de la CEI 61508 s'appuie sur le principe du cycle de vie de sécurité, dont l'analyse des risques en constitue le pilier capital. Cette étape permet de définir la réduction nécessaire du risque que le SIS doit assurer, en matière de niveaux d'intégrité de sécurité (SIL). En fin, le prochain chapitre est consacré à la présentation des SIS d'une manière détaillée, accompagnée des formules numériques dédiées à la détermination des SIL à travers les méthodes quantitatives.

Chapitre III : Systèmes Instrumentés de Sécurité

-

Introduction

Diverses types de sécurité sont mise en œuvre lorsque les systèmes automatisés présentent des risques qui menace l'homme, l'environnement ou les biens. Ces systèmes utilisent des moyens contribuant soit à la prévention ou à la protection, afin de limiter les conséquences d'un évènement non-souhaitable ou un état de dysfonctionnement.

L'existence de plusieurs niveaux de risques dans les différentes installations de process, fait qu'il y a divers façons pour la conception des Systèmes Instrumentés de Sécurité (SIS). Ils sont utilisés pour exécuter des fonctions de sécurité dans les industries présentant des phénomènes dangereux. Ce sont des moyens chargés de la surveillance du procédé suivant certaines limites associées aux paramètres contrôlés (au-delà desquelles, il pourrait devenir dangereux) et du déclenchement d'organes de sécurité lorsqu'un danger se présente.

La caractérisation de ces systèmes dépend de la périodicité des tests de vérification (mensuelle, trimestrielle, annuelle ou une fois par arrêt), du niveau de redondances appropriées (simple, double ou bien triple) et de leurs compositions internes (analogiques, l'analyse intelligente, quantitative ...).

La 1ère partie de ce chapitre porte sur les systèmes instrumentés de sécurité, leurs constitutions (élémentaires ou complexes), modes de fonctionnement et tests relatifs à ces derniers.

La 2ème partie va être consacrée pour la norme fille sectorielle spécifique à l'industrie du process la norme générique CEI 61508.

Le 3ème partie de ce chapitre porte sur les critères essentiels pour d'évaluation de la performance des SIS, ces définitions et comment les obtenus pour chaque type de SIS ou type de contrôle.

La dernière partie de ce chapitre est basé sur les différentes configurations architecturelles des Systèmes Instrumentés de Sécurité.

1. Concept de Systèmes Instrumentés de Sécurité

1.1. Définition d'un SIS

D'après la norme CEI 61508 [21], un SIS fait l'objet de la définition suivante: « c'est un système E/E/PE relatif aux applications de sécurité, il comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité».

La norme CEI 61511 [33] quant à elle, elle définit les SIS comme étant «un 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 logique (s) et d'élément(s) terminal (aux) ».

Les SIS visent à mettre le procédé en état stable qui ne présente pas de risque pour l'environnement et les personnes lorsque le procédé s'engage dans une voie comportant un risque réel (explosion, feu…) [8].

1.2.Constitution élémentaire d'un SIS

Les SIS sont constitués de différents éléments unitaires reliés entre eux par des moyens de transmissions. Au minimum, on retrouve en série un capteur, une unité de traitement et un actionneur [34] (figure 3.1).

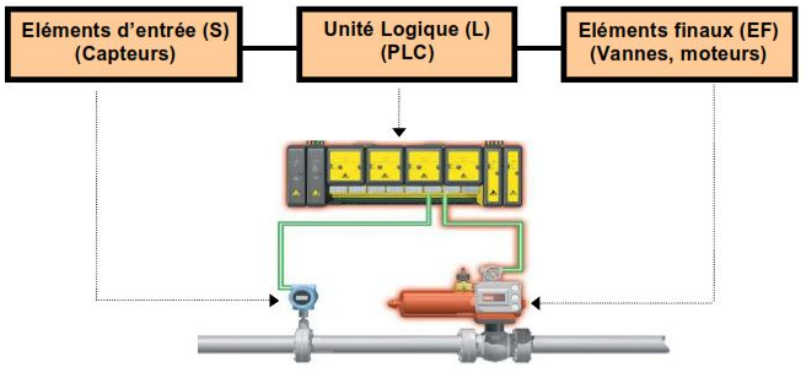


Figure 3.1 – Système Instrumenté de Sécurité

1.3.Fonction Instrumentée de Sécurité

La fonction instrumentée de sécurité est définie comme étant la fonction de sécurité avec un SIL spécifique qui est nécessaire pour maintenir la fonction de sécurité [35].

C'est une fonction réalisée par un système E/E/PE relatif à la sécurité, basé sur une autre technologie, ou par un dispositif externe de réduction de risque, prévue pour assurer ou maintenir un état de sécurité de l'élément commandé par rapport à un événement dangereux spécifique [36].

1.4.Mode de fonctionnement

1.4.1. Faible sollicitation

La fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et la fréquence des sollicitations n'est pas supérieure à une par an [37].

Une barrière de sécurité est en mode de sollicitation à faible demande lorsque la fréquence des demandes d'opération n'est pas plus grande qu'une par an et pas plus grande que le double de la période des tests de révision CEI61508-4, Sections 3.5.12 et 13 [21].

1.4.2. Forte sollicitation

La fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et la fréquence des sollicitations est supérieure à une par an [37]. Dans la plupart des cas, le mode de sollicitation est de forte demande.

1.4.3. Mode continu

La fonction de sécurité maintient l'EUC dans un état de sécurité en fonctionnement normal en permanant [37].

1.5.Test relatif aux SIS

1.5.1. Définition

les SIS sont des barrières de sécurité, afin de veiller au maintien de leurs performances dans le temps, il faut les tester, c'est-à-dire, il faut simuler la situation de danger et vérifier si la fonction de sécurité pour laquelle elle a été mise en place est bien réalisée [10].

1.5.2. Rôle des tests

Ces tests permettent :

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

Ils peuvent être considérés comme complets ou partiels (i.e. détection d'une partie uniquement des défaillances) [38].

1.5.3. Intervalle du test

L'intervalle est la période de l'heure à laquelle le test a eu lieu. La fréquence de contrôle varie pour chaque SIS et dépend du niveau de la technologie, l'architecture du système cible et son SIL. Par conséquent, l'intervalle de test est une composante importante pour le calcul de la probabilité de défaillance à la demande (PFD)[38].

1.5.4. Type de test

Il existe plusieurs type de test pour la surveillance des SIS, notamment citant :

1.5.4.1.Test diagnostic

Les tests de diagnostic agissent au niveau composant/interne, non pas au niveau de la fonction de sécurité qui permettent de détecter les erreurs aléatoires dues au matériel, car ils sont des tests en ligne (en fonctionnement).

Ainsi, les tests de diagnostic sont effectués périodiquement et automatiquement pour détecter les défauts latents cachés qui empêchent le SIS de répondre à une demande [9].

1.5.4.2.Proof test

Proof test est une exigence des systèmes instrumentés de sécurité, qui ayant pour but l'assurance du bon fonctionnement des systèmes. Le test doit inclure la vérification du système : l'unité logique, les détecteurs avec les éléments finals.

Selon les normes CEI61508-4 [21] et CEI62061 [39], le Proof test un test périodique hors ligne réalisé pour détecter des pannes dans un système de telle sorte que le système puisse être réparé afin de revenir dans un état équivalent à son état initial.

L'INSA/ISA S84.01 [40], déclare que, lorsqu'on augmente la fréquence du proof test, on vérifiera plus souvent que la fonction de sécurité est bien disponible (dans le cas où le DC serait minimum ou insuffisant, si on ne peut pas ou ne sait pas réaliser un test de diagnostic satisfaisant).

Pascal Lamy [9] (chercheur de l'Institut National De Recherche Scientifique – INRS) définis le proof test comme un test fonctionnel de la fonction de sécurité hors fonctionnement automatique sans perturbation de process, d'autre terme, c'est une activité périodique devant être conduite selon une procédure afin de détecter les défauts latents qui empêchent le système de sécurité de remplir sa fonction de sécurité.

1.5.5. Comparaison entre tests

Les critères de comparaison entre les tests (proof test et test de diagnostic) sont : **l'intervalle entre test** ou **la périodicité**, **la détection des pannes**…

Le proof test est un test hors fonctionnement (arrêt total de l'installation) par contre le test diagnostic ce fait lors en mode de fonctionnement normal de l'installation.

Mais, en règle générale, un proof test à une périodicité beaucoup plus importante qu'un test de diagnostic ceci est dû à la langueur de l'intervalle entre test (plus grand pour le proof test).

Alors que le test de diagnostic est plutôt une détection interne en fonctionnement, pour le proof test, la détection des pannes ce fait pour tout le système.

Le proof test permet de détecter les pannes latentes qui n'ont pas été vues par les tests de diagnostic.

2. Approche normative (CEI 61511)

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

Elle comprend trois parties :

- CEI 61511-1 : relative aux cadre, définitions, exigences pour le système, le matériel et le logiciel [33],
- CEI 61511-2 : présente les lignes directrices pour l'application de la CEI 61511-1 [41],
- CEI 61511-3 : Conseils pour la détermination des niveaux exigés d'intégrité de sécurité [42].

La norme CEI 61511 limite le périmètre aux systèmes pour des applications de niveau d'intégrité de sécurité (SIL) 1 à 3.

Les applications de SIL 4 ne pouvant être traitées par un SIS seul, ce qui nécessitent l'utilisation d'une fonction instrumentée de sécurité (SIF) de niveau d'intégrité de sécurité SIL 4, ces dernières sont rares dans l'industrie de process. Elles doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de la sécurité [4, 6, 43].

3. Critères de performance des SIS

3.1. Taux de défaillance

Notons que le $\lambda(t)$ est associé à un fonctionnement continu du système. Il représente la probabilité qu'un système soit défaillant. Cette définition s'applique pour tout type d'élément (système, sous-système, module, composant ou canal) [9].

Remarque : Dans la plupart des cas, le constructeur ne fournit qu'un taux de défaillance globale (du système ou du sous-système), en effet, d'après Lamy Pascal (INRS), il ne sera pas nécessaire de descendre au niveau « composant » [9].

De nombreux critères qualitatifs, notamment sur l'architecture fonctionnelle de la barrière, sont alors requis pour un SIL donné [8] [9]. La partie quantitative se fait quant à elle par l'un des deux indicateurs suivants CEI61508-1 [1]:

- Probabilité de défaillance à la demande (**PFD**) pour une barrière à faible demande de sollicitation.
- Probabilité de défaillance par heure (**PFH**) pour une barrière à forte demande de sollicitation.

3.1.1. Probabilité moyenne de défaillance à la demande

La PFD, est la probabilité sur l'intervalle de temps [0,t] que le système ne puisse pas exécuter la fonction pour laquelle il a été conçu au moment où la demande de cette fonction est faite, notée PFD[1] (ou *Probability of Failure on Demand* en anglais) [9]. C'est un nombre sans dimension.

Dans le cas d'un système mono canal :

$$\mathbf{PFD(t) = 1 - Fiabilité = 1 - R(t)} \text{ ;}$$

Avec : la **Fiabilité** [38] (ou Reliability en anglais) : est la probabilité qu'un dispositif accomplisse sa fonction voulu lorsque ce dispositif travaille dans des conditions de temps et de limites prévues .

Notons que R(t), représente une fonction du temps telle que : $R(t) = P(T>t)$; c'est-à-dire : probabilité que le temps T (temps où la panne intervient) soit supérieur au temps t (temps opérationnel ou temps de fonctionnement [40]; on peut aussi la définir comme la probabilité que le système ne soit pas défaillant pendant l'intervalle de temps [0,t].

La norme CEI 61508 [30] propose dans la partie 6, une technique possible de calcul des probabilités de défaillance du matériel pour les systèmes E/E/EP relatifs à la sécurité installés conformément à la CEI 61508 [1], la CEI 61508 [28] et la CEI 61508 [29].

Un système est alors défini par l'ensemble *(M, N, λ) (annexe 4 : pour la définition des variables)*, et une politique de tests peut être défini de façon équivalente par l'ensemble *(E, t_1, t_2, …, t_n)* ou l'ensemble *(E,* T_1,T_2,…..T_n*)*.

On distingue plusieurs types de PFD, mais avant de développer chacun de ces derniers, nous allons d'abord passer par plusieurs notions comme de la disponibilité élément nécessaires à leur calcul.

[1] Cette notion est en fait à la base des probabilités ou la somme de la probabilité d'un événement et de son complément doit être égale à 1.

3.1.1.1.Calcul de la disponibilité

Pour chaque élément du système, une partie avec un taux de défaillance égal à $\boldsymbol{E \cdot \lambda}$ est révisable par n'importe quel test de révision, qu'il soit partiel ou complet, et l'autre partie avec un taux de défaillance égal à $\boldsymbol{(1 - E) \cdot \lambda}$ n'est révisable que par des tests complets.

Le diagramme de fiabilité correspondant est décrit sur la figure 3.2 :

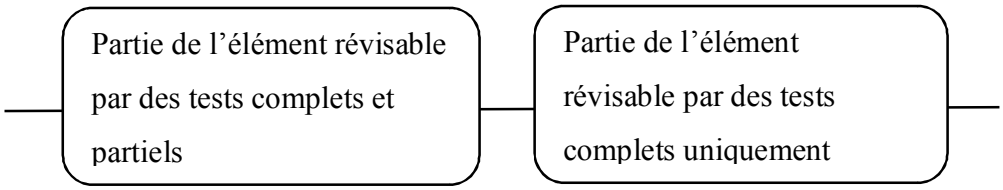


Figure 3.2 - Diagramme de fiabilité d'un élément soumis à des tests de révision complets et partiels

La disponibilité du composant au temps *t* est alors :

$$\boldsymbol{A_e(t) = e^{E.\lambda.\, t_{i-1}}.\, e^{-\lambda.t}} \qquad \text{Pour : } \mathbf{t_{i-1} \leq t < t_i}$$

La disponibilité du système au temps *t* est alors :

$$\boldsymbol{A(t) = \sum_{x=M}^{N}[S(M,N,x).\, e^{x.E.\lambda.\, t_{i-1}}.\, e^{-x.\lambda.t}]} \qquad \text{Pour : } \mathbf{t_{i-1} \leq t < t_i}$$

Avec, S (M, N, x) est la somme, définit par :

$$\boldsymbol{S(M,N,x) = \sum_{k=M}^{x}[\binom{N}{x}.\binom{x}{k}.(-1)^{x-k}]} \qquad \text{Pour : } x = M, \ldots, N$$

Par conséquent, l'indisponibilité U(t) est alors :

$$\mathbf{U(t) = 1 - A(t)}$$

Cas particulier : Lorsque le produit $\lambda \cdot \tau$ est relativement faible ($\lambda \cdot \tau < 10^{-2}$), les approximations suivantes peuvent être faites, en utilisant des développements de Taylor :

$$\boldsymbol{A_e(t) \approx 1 + E.\lambda.\, t_{i-1} - \lambda.t} \qquad \text{Pour : } t_{i-1} \leq t < t_i$$

Et : $$\boldsymbol{A(t) \approx 1 - \binom{N}{M-1}.\lambda^{N-M+1}.(t - E.t_{i-1})^{N-M+1}} \qquad \text{Pour : } t_{i-1} \leq t < t_i$$

Le système est défini comme mentionnée sur la figure ci-dessous (voir annexe 4) :

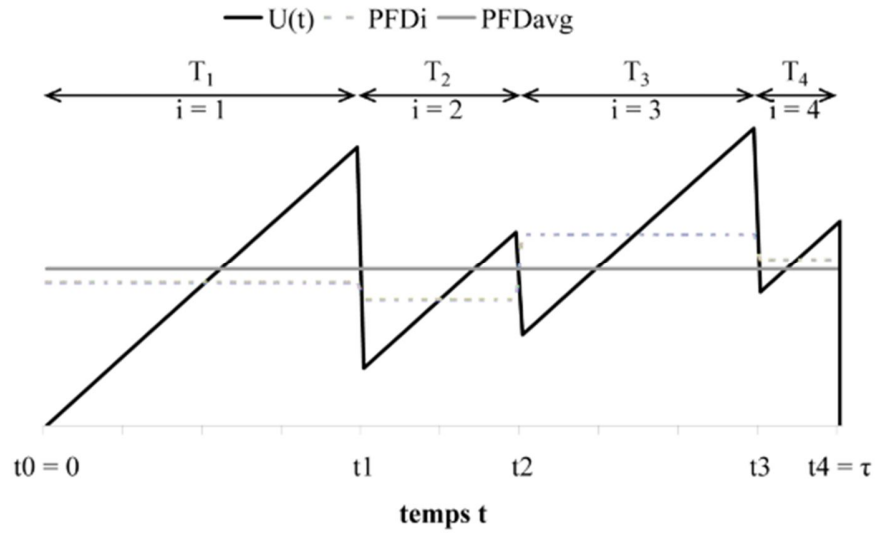


Figure 3.3 -Notations pour les probabilités de défaillance à la sollicitation (PFD) exemple n = 4 [10]

3.1.1.2.Calcul de la PFD$_i$

PFD$_i$ (Probability of Failure on Demand), c'est la probabilité moyenne que le système ne soit pas capable d'accomplir la fonction de sécurité (indisponibilité moyenne) dans l'intervalle de temps entre le *(i – 1)* et l'$i^{ème}$ test de révision ($[t_{i-1}, t_i]$), on l'obtient par les relations suivantes :

On a:

$$\boldsymbol{PFD_i = \frac{1}{T_i} . \int_{t_{i-1}}^{t_i} U(t).dt}$$

3.1.1.3.Calcul de la PFD$_{avg}$

PFD$_{avg}$: c'est la probabilité moyenne que le système ne soit pas capable d'accomplir la fonction de sécurité (indisponibilité moyenne) dans l'intervalle de temps entre deux tests complets ([0 ; t_n]).

À la suite de chaque test complet, le système est restauré dans des conditions « comme neuves », de telle sorte que *PFD$_{avg}$* peut être évaluée sur l'intervalle de temps entre deux tests complets.

Les probabilités moyennes que le système ne soit pas capable d'accomplir la fonction de sécurité, dans l'intervalle de temps entre le $(i-1)^{ème}$ et le $i^{ème}$ test de révision, et dans l'intervalle de temps entre deux tests complets, sont donc :

$$\boldsymbol{PFD_{avg} = \frac{1}{\tau} . \sum_{i=1}^{n} T_i . PFD_i}$$

3.1.1.4.Calcul de la PFD_{max}

PFD_{max} : c'est la probabilité maximale que le système ne soit pas capable d'accomplir la fonction de sécurité (indisponibilité maximale) dans l'intervalle de temps entre deux tests complets (*[0 ; t_n]*), i.e. *max (U(t))* avec la condition $t_0 \leq t \leq t_n$.

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

D'après Pascal Lamy (membre de l'INRS) [9], elle est notée **PFH** (ou *Probability of a dangerous Failure per Hour*), cette notion prend en compte les intervalles entre tests. S'il n'y a aucun moyens de réparation, elle est défini par :

$$\mathbf{PFH} = \frac{\mathbf{PFD}}{\boldsymbol{T_i}}$$

Dans le cas des systèmes à forte sollicitation, on utilise cette grandeur.

3.2.Différents temps relatifs aux SIS

On distingue de multiples temps relatifs aux systèmes dans toutes les phases du cycle de vie de sécurité des équipements E/E/EP, dans cette section nous allons définir ces derniers accompagnés par leurs formules mathématiques (figure 3.4).

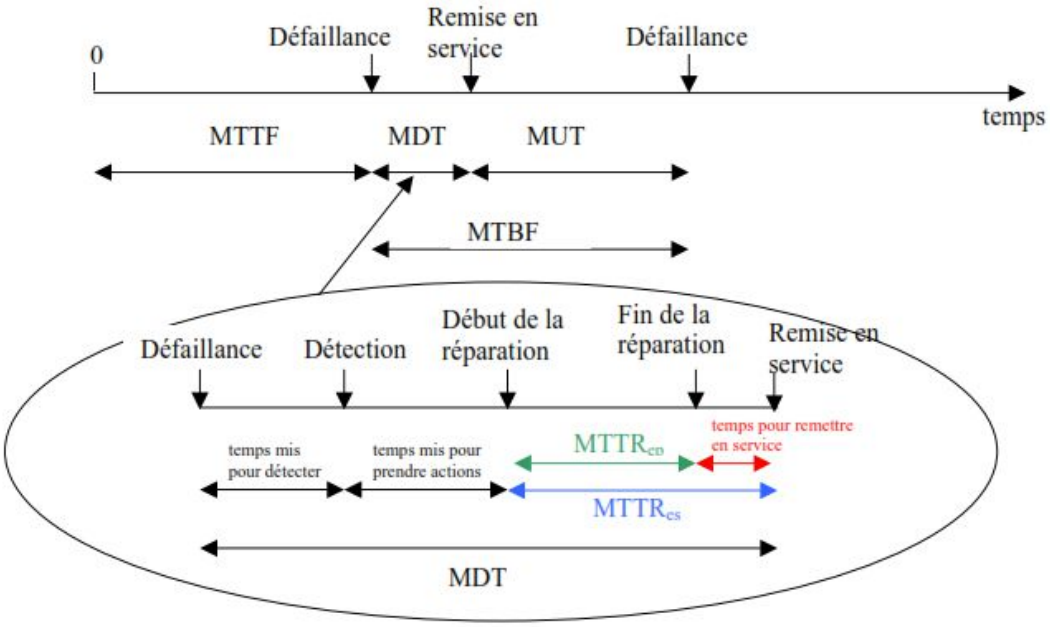


Figure 3.4 – Différents temps relatif aux SIS[9]

3.2.1. MTTF

En Anglais ce terme signifier « Mean Time To Failure » ; pour un système que l'on ne répare pas, le MTTF est le temps moyen de fonctionnement **avant la première** défaillance [39].

La définition de MTTF [44] est :

$$\boldsymbol{MTTF = \int_0^x R(t)dt}$$

3.2.2. MTBF

Le **MTBF** veut dire en anglais « Mean Time Between Failure », il n'a de sens que pour un système réparable. Il représente la durée entre deux (2) défaillances consécutives [39].

Pour un composant simple de taux de défaillance **λ** qui, après réparation, peut être considéré comme identique à ce qu'il était en début de vie, dans ce cas-là, d'après le livre de sûreté de fonctionnement de Villemeur [44] le **MTBF** est donnée par l'équation suivante:

$$\boldsymbol{MTBF \approx MTTF = \frac{1}{\lambda}}$$

3.2.3. MTTR

Ce terme représente le temps moyen mis pour réparer le système, on le trouve en anglais « **M**ean **T**ime **T**o **R**epair » [44] [39], cette définition crée une grande confusion avec celle de la norme générique CEI 61508, qui le définit comme étant le « Mean Time To Restoration » [45]; donc, il faudra alors préciser les termes :

- **$MTTR_{ep}$**: pour **M**ean **T**ime **T**o **R**epair,
- **$MTTR_{es}$**: pour **M**ean **T**ime **T**o **R**estoration.

La déférence entre les deux temps (**$MTTR_{ep}$** et **$MTTR_{es}$**) est liée au fait que l'on considère ou non le temps mis pour remettre en service l'équipement, pour le **$MTTR_{es}$**, il l'inclut.

Remarque : Pour notre cas, nous avons considéré que la durée entre la fin de la phase de réparation et la remise en service est nulle, donc :

$$\mathbf{MTTR_{ep} = MTTR_{es}}$$

3.2.4. MDT

C'est la durée moyenne d'indisponibilité ou de défaillance [39]. Elle correspond à la détection de la panne, la réparation de la panne et la remise en service [44].

Le MDT se décompose en multiple temps, comme mentionné dans la formule ci-dessous :

$$\boldsymbol{MDT = \begin{matrix}\textbf{temps mis pour}\\ \textbf{détecter la défaillance}\end{matrix} + \begin{matrix}\textbf{temps de réaction avant la mise en place}\\ \textbf{des actions pour réparer}\end{matrix} + MTTR_{es}}$$

Pour les systèmes où la réparation s'effectue hors-service, c'est le cas où, nous pouvons enlever l'élément défaillant sans perturber le fonctionnement du système ; le $MTTR_{es}$ ne comprend plus le $MTTR_{ep}$ ce qui permet de diminuer le temps d'indisponibilité du système [44].

3.2.5. MUT

Mean **U**p **T**ime ; c'est la durée moyenne de fonctionnement après réparation. Sans approximation, le **MUT** est la somme suivante :

$$\boldsymbol{MTBF = MUT + MDT}$$

3.3.Taux de Couverture - Diagnostic Coverage (DC)

3.3.1. Définition

Selon Lamy Pascal (INRS), le taux de couverture a été ainsi défini comme étant la probabilité ($P \in [0\,,1]$) qu'une panne soit détectée [9].

La norme CEI61508 [5] quant à elle, elle définit ce taux pour les tests automatiques de diagnostic comme étant le rapport du taux de défaillance des pannes dangereuses détectées (par un test de diagnostic) sur le taux de défaillance total des pannes dangereuses (détectées et non détectées).Il correspond à la couverture du diagnostic en ligne.

Il est compris entre 0 et 100%. Un taux de 0% signifie qu'aucune panne révélée ne pourra être détectée [36].

3.3.2. Formule de calcul

a. La définition la plus générale selon Lamy Pascal (INRS) [9], pour calculer le taux de couverture est donnée par la formule suivante :

$$\boldsymbol{Taux\ de\ Couverture = \frac{Somme\ des\ taux\ de\ défaillance\ des\ composants\ détectés\ en\ panne}{Somme\ des\ taux\ de\ défaillance\ de\ tous\ les\ composants}}$$

b. Selon la norme générique CEI61508 [5] [9], le taux de couverture est donné par la formule suivante :

$$\boldsymbol{DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Total\ Dangereuse}}}$$

Tel que : **DC** : est le taux de couverture (ou Diagnostic Coverage, en Anglais).

$\boldsymbol{\lambda_{DD}}$: est le taux de défaillance des pannes dangereuses détectées (par un test de diagnostic).

$\boldsymbol{\lambda_{total\ dangereuse}}$: est le taux de défaillance total des pannes dangereuses, c'est-à-dire : la somme des taux de défaillances dangereuses détectées et non détectées.

3.3.3. Evaluation du Diagnostic Coverage

Selon l'ISA [40] [9] (Instrumentation, Systems and Automation Society), l'évaluation du DC se fait à travers les étapes suivantes :

1ère Etape : Faire une analyse des modes de défaillances et des diagnostics.

2ème Etape : Déterminer les défaillances possibles.

3ème Etape : Distinguer les défaillances si elles peuvent être détectées.

4ème Etape : Calculer le DC selon le rapport (voir 3.2.2.b) à l'aide des taux de défaillances et non pas uniquement à l'aide du nombre des défaillances.

3.4.Caractère déterminé du composant avec leur SIL équivalent

La PFD du système ne permet pas à lui seul d'évaluer un SIL. Des contraintes sur l'architecture viennent limiter le SIL maximum.

Un composant (un capteur, un actionneur ou un système de traitement non électronique et non programmable) est spécifié par un des trois types des caractères disponibles :

3.4.1. Type A

Ce type indique que le composant est à sécurité positive (à manque) et éprouvé par l'usage (ou certifié) et avec autodiagnostic (ou avec mise en œuvre de plusieurs tests) et protégé en accès aux réglages internes [36].

3.4.2. Type B

Ce type indique que le composant est à sécurité positive (à manque) ou avec autodiagnostic. Correspond au type S (Composant standard) [36].

3.4.3. Non type A/B

Ce type indique que le composant est à sécurité négative (à émission) et sans autodiagnostic. Il correspond au type NS (Composant non sécurisé).

4. Configuration architecturelle d'un SIS

La norme internationale CEI 61508 dans sa 7ème partie [3] vise à fournir un moyen d'assurer que la sécurité est effectivement atteinte sur la base de la fonctionnalité des systèmes liés à la sécurité.

4.1.Architecture MooN

Généralement, pour une architecture MooN, le premier chiffre désigne le nombre d'éléments que l'on doit avoir en état de marche pour que le système assure la fonction de sécurité et le second chiffre indique le niveau de redondance [3].

Le système est divisé en N éléments, et qu'il est capable d'accomplir de manière satisfaisante la fonction de sécurité spécifiée si et seulement si M de ces éléments (n'importe lesquels) sont opérants (système « M-sur-N », et en anglais, « M-out-of-N ») [10].

4.2.Architecture 1ooN

Toutes les architectures de type 1ooN ont le même principe de fonctionnement. Pour celles-ci nous allons prendre comme exemple l'architecture lorsque N= 1 et N=2.

On peut facilement en déduire que le nombre de défaillances dangereuses provoquant l'inhibition de la fonction de sécurité est égale à N.

Cependant, le nombre de défaillances sûres conduisant au déclenchement intempestif du SIS est égal à 1.

4.2.1. Architecture 1*oo*1

Les figures ci-dessous montrent que cette architecture de base comprend un seul canal et donc un seul chemin matériel que peut parcourir un signal dans la chaîne de traitement d'une demande [3].

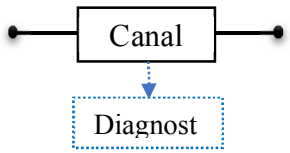


Figure 3.5 - Blocs-diagramme physique 1oo1 [8]

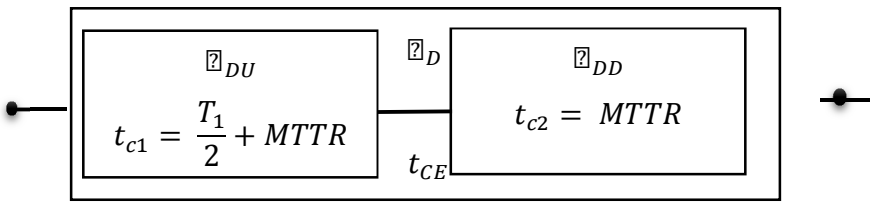


Figure 3.6 - Diagramme de fiabilité 1oo1 [8]

Dans le cas de l'architecture 1oo1, toute défaillance dangereuse entraîne la défaillance du système.

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 3.5 [42] [38]. Les diagnostics y sont présents pour assurer la détection des défaillances (dangereuses et sûres) en vue de les réparer immédiatement.

4.2.2. 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).

4.3.Architecture 2oo3

Cette architecture comprend trois canaux connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie, de telle sorte que l'état de sortie n'est pas modifié lorsqu'un seul canal donne un résultat différent des deux autres canaux [46], figure 3.7.

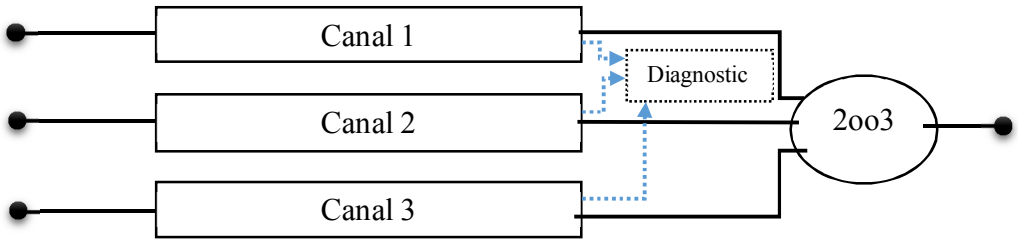


Figure 3.7 - bloc-diagramme physique pour 2oo3

Ceci dit, le nombre de défaillances nécessaires aussi bien à l'empêchement de l'exécution de la fonction de sécurité qu'au déclenchement intempestif du *SIS* s'élève à deux.

4.4.Lien entre les architectures et le PFD du système

Le tableau 3.1 et la figure 3.8, expliquent le lien entre la PFD et les architectures :

Tableau 3.1 – Lien entre PFD et MOON

Voting	PFD_{avg}
1oo1	$\lambda_{DU} * (\frac{T}{2})$
1oo2	$\frac{\lambda_{DU}{}^2 * T^2}{3}$
2oo2	$\lambda_{DU} * T$
2oo3	$(\lambda_{DU})^2 * T^2$

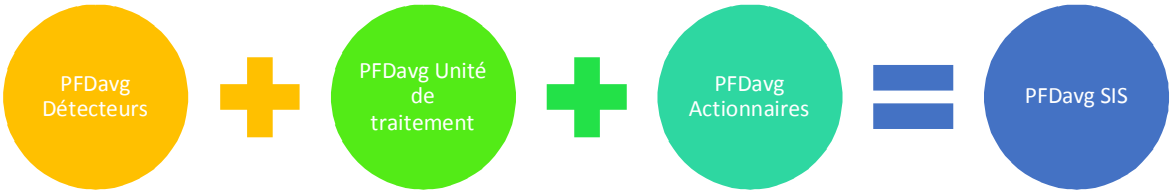


Figure 3.8 – Relation entre les éléments du SIS

5. Détermination du niveau d'intégrité de sécurité (SIL)

Le SIL (Safety Integrity Level) ou niveau d'intégrité de sécurité, permet de spécifier les prescriptions concernant l'intégrité de chaque fonction de sécurité exécutée par les systèmes E/E/EP. Quatre niveaux de SIL allant de 1 à 4 permettent de caractériser ces systèmes :

- **SIL 4** : renvoyant au niveau de sécurité le plus « **élevé** ».
- **SIL 1** : renvoyant au niveau de sécurité le plus « **faible** ».

5.1. Description générale sur le SIL

La notion de SIL s'applique au système de sécurité dans sa globalité, et non pas à un élément ou sous-ensemble de celui-ci. Néanmoins, certains fournisseurs de matériel en font aujourd'hui un argument commercial.

Pour un mode de fonctionnement à faible sollicitation (ou à la demande), la correspondance entre le niveau de SIL et la PFD est présentée dans le Tableau 3.2. Ce mode de fonctionnement est typique des systèmes de sécurité qui sont « activés » uniquement sur dépassement de valeurs seuils (dérive du mode de fonctionnement normal d'une installation).

Pour un mode de fonctionnement à forte sollicitation, la correspondance entre le niveau de SIL et la fréquence de défaillances dangereuses visée par heure est présentée dans le tableau 3.3. Ce mode de fonctionnement est typique des systèmes qui agissent en permanence pour réduire un risque. Lorsque la fréquence des demandes de fonctionnement sur un système relatif à la sécurité est plus grande qu'une par an, ou supérieure à la fréquence des tests périodiques, ce système est considéré répondre au critère de forte sollicitation (demande élevée ou mode continu).

Il existe principalement deux types de méthodes qui permettent de déterminer le niveau de SIL requis d'un SIS :

- **les méthodes qualitatives** : le niveau de SIL est évalué à partir de la connaissance des risques associés au procédé ;
- **les méthodes semi-quantitatives** : le niveau de SIL est évalué en fonction de la gravité de risque et de sa fréquence d'occurrence.

L'atteinte du niveau de SIL requis est ensuite vérifiée à l'aide de méthodes quantitatives qui permettent de calculer la PFD d'un SIS à partir des probabilités de défaillance des éléments qui le compose. Pour se faire, diverses techniques d'analyse peuvent être utilisées :

- des équations simplifiées ;
- des arbres de défaillances ;
- des approches markoviennes.

Tableau 3.2 - Définition des niveaux SIL pour un mode de fonctionnement à faible sollicitation

Niveau d'intégrité de sécurité	**Probabilité de défaillance dangereuse par ans**	**Facteur de réduction du risque**
SIL 1	10^{-1} à 10^{-2}	10 à 100
SIL 2	10^{-2} à 10^{-3}	100 à 1000
SIL 3	10^{-3} à 10^{-4}	1000 à 10000
SIL 4	10^{-4} à 10^{-5}	10000 à 100000

Tableau 3.3 - Définition des niveaux SIL pour un mode de fonctionnement à forte sollicitation

Niveau d'intégrité de sécurité	**Probabilité de défaillance dangereuse par ans**	**Facteur de réduction du risque**
SIL 1	10^{-5} à 10^{-6}	10 à 100
SIL 2	10^{-6} à 10^{-7}	100 à 1000
SIL 3	10^{-7} à 10^{-8}	1000 à 10000
SIL 4	10^{-8} à 10^{-9}	10000 à 100000

5.2.Détermination du SIL requis

Afin de bien respecter les prescriptions relatives à la sécurité fonctionnelle exigées par les normes CEI 61508 et CEI 61511, il faut d'abord défini la notion du niveau d'intégrité de sécurité (SIL) relatifs aux fonctions instrumentées de sécurité (SIF), Dont le but de fixer le niveau de réduction du risque, c'est - à - dire le SIL que doit avoir le SIS. Plus le SIL à une valeur élevé, plus la réduction du risque est importante.

Il existe plusieurs méthodes de détermination du SIL, telles que présentées dans les normes CEI 61508 et CEI 61511, à savoir que le SIL correspond 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).

5.2.1. Méthodes qualitatives

Il s'agit de méthodes qui permettent de déterminer le niveau de SIL à partir de la connaissance des risques associés au procédé. L'utilisation d'une méthode qualitative reconnait un certain nombre de simplification de paramètres doivent être introduits. Ils permettent de qualifier le phénomène dangereux (accident) en fonction des connaissances disponibles.

5.2.1.1.Graphe de risque

La démarche de cette méthode est basée sur l'équation caractérisant le risque (R) sans considérer les moyens instrumentés de sécurité [5]:

$$\mathbf{R = f*C}$$

Où :

R : est le risque en l'absence de systèmes relatifs à la sécurité.

f : est la fréquence de l'événement dangereux en l'absence de systèmes relatifs à la sécurité.

C : est la conséquence de l'événement dangereux (les conséquences pourraient être liées aux dommages associés à la santé et à la sécurité ou aux dommages provenant de dégâts environnementaux).

Dans le cas présent, la fréquence de l'événement dangereux **f** est supposée être le résultat de trois facteurs exerçant une influence :

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

- La probabilité que l'événement dangereux se produise en l'absence de systèmes relatifs à la sécurité (mais en présence de dispositifs externes de réduction de risque). C'est ce que l'on appelle la probabilité d'occurrence non souhaitée.

On obtient les quatre paramètres de risque suivants :

- conséquence de l'événement dangereux (C),
- fréquence et durée d'exposition au danger (F),
- possibilité d'éviter l'événement dangereux (P),
- probabilité de l'occurrence non souhaitée (W).

Le tableau 3.4 définit les paramètres du graphe de risque :

Tableau 3.4 - Description des paramètres du graphe de risque [4]

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

La combinaison des quatre paramètres précédents (*C, F, P, W*) peut ramener à une configuration comparable à celle présentée à la figure 3.9 [5]

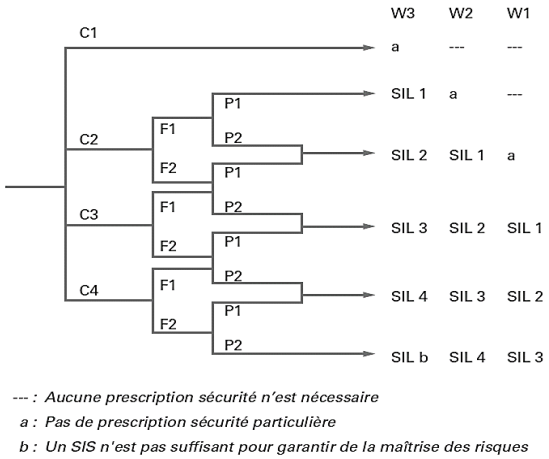


Figure 3.9 - Graphe de risque : Schéma général [4]

Tableau 3.5 : Définition des paramètres du graphe de risque [47]

Paramètre		**Hiérarchisation**	**Critère d'évaluation**
C	Conséquence de l'événement dangereux.	C1	Incident mineur.
		C2	Blessures graves sur plusieurs personnes avec décès possible de l'une d'entre elles.
		C3	Mort de deux personnes.
		C4	Nombre de morts supérieur à deux.
F	Fréquence et durée d'exposition au danger.	F1	Faible fréquence d'exposition (exposition rare à fréquente dans une zone dangereuse).
		F2	Forte fréquence d'exposition (exposition fréquente à permanente dans une zone dangereuse).
P	Possibilité d'éviter l'événement dangereux.	P1	Possible dans certaines conditions.
		P2	Impossible.
W	Probabilité d'occurrence de l'événement.	W1	Faible probabilité.
		W2	Probabilité moyenne.
		W3	Forte probabilité.

5.2.1.2.Matrice de gravité

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) (voir Annexe 1 pour un exemple simplifier d'une matrice de gravité).

5.2.2. Méthodes quantitatives

Une méthode quantitative qu'est utilisée pour la détermination des niveaux d'intégrité de sécurité, c'est l'analyse par couches de protection (LOPA).

Précisément, Cette méthode est une méthode semi-quantitative et trouve plusieurs applications notamment :

- Compléter l'analyse menée dans l'HAZOP si le groupe de travail considère le scénario trop complexe ou que les conséquences sont trop importantes.
- Déterminer les niveaux de SIL requis pour les fonctions instrumentées de sécurité (SIF).
- Evaluer l'impact de la modification du procédé ou des barrières de sécurité ;
- Analyser de manière plus détaillée certains scénari d'accidents.

Les couches utilisées par la méthode LOPA 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). Le tableau de l'annexe 2, illustre un exemple de format de la feuille de calcul que l'on peut utiliser lors d'une étude LOPA.

5.3.Allocation du SIL (réel)

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

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

- Les équations simplifiées,
- Les arbres de défaillances,
- Les chaînes de Markov.

Conclusion

Dans ce chapitre nous avons abordé les systèmes instrumentés de sécurité, en premier lieu tous les concepts utilisés dans les SIS, leurs constitution et leur mode de fonctionnement avec les différents type des tests relatifs à leur révisons.

En deuxième lieu, nous avons détaillé tous les critères de performance des SIS, notamment les probabilités de défaillance, tel que : PFD_{avg}, PFD_{max},…avec le taux de défaillance, diagnostic coverage - DC, tous ces derniers sont associés avec leurs formules mathématiques extraite de la norme fille CEI61511 (relative à l'industrie du process ou de transformation) de la norme générique des SIS, CEI 61508. Puis nous avons montrés sur les différentes architectures des SIS, les méthodes de détermination du niveau SIL réel ou SIL requis à travers les méthodes de calcul : quantitative et qualitative.

Dans le prochain chapitre, nous allons appliquer les concepts et les formules prédéfinis dans ce chapitre, relatifs à notre démarche choisie pour l'évaluation du système d'arrêt d'urgence automatique du rebouilleur H201.

Chapitre IV : Evaluation de la performance de système d'arrêt d'urgence automatique, du rebouilleur H201

Introduction

La démarche d'évaluation de la performance des systèmes instrumentés de sécurité est appliqué au four H201, ce dernier est associé à un procédé de traitement du gaz naturel (Annexe 5) qui traite le gaz brut pour obtenir le gaz de vente (C1, C2), GPL (C3, C4) et le condensât. Le procédé se situe dans le module « MPP1 », au niveau d'une installation gazière à Hassi R'Mel.

Dans ce module, le four H201 est la partie la plus sensible, parce qu'il joue un rôle important dans le fonctionnement du module. Il est composé des éléments suivants : chambre de combustion, brûleurs, circuit d'alimentation gaz et liquide et du système de contrôle.

La complexité des architectures du SIS et la difficulté 'de l'évaluation de certains critères de performance impose l'utilisation d'un logiciel. Notre travail englobera une combinaison de deux approches, l'une pour de la conception des systèmes et l'autre pour l'évaluation des BTS. Nous allons évaluer le SIL, l'efficacité et le temps de réponse du système d'arrêt d'urgence automatique.

Nous déterminerons ensuite la conformité du système envers chaque critère de performance afin d'apprécier la performance globale du système étudié.

1. Présentation de l'entreprise

L'Algérie dispose d'un riche potentiel en **gaz naturel** et le gisement le plus important se trouve à Hassi R'mel (HRM) dans la wilaya de Laghouat à environ 600 km de la capitale. L'exploitation du gisement de HRM a été commencée dans les années 60.

1.1. Situation géographique

Le tableau suivant résume la situation géographique de la région de HRM :

Tableau 4.1 – Situation géographique

Hassi R'Mel	Situation	525 Km au sud d'Alger entre Laghouat et Ghardaïa		
	Altitude	760m		
	Paysage	Vaste plateau rocailleux		
	Climat		**Eté**	**Hiver**
		Humidité moyenne	19%	34%
		Amplitude varient	45°C	-5°C

1.2. Organisation du champ gazier

L'homogénéité du réservoir et la nature de l'effluent sont les raisons pour lesquelles le choix d'un modèle de développement est basé sur un schéma d'exploitation alterné, comportant trois zones d'exploitation (Tableau 4.2) avec 2 zones de réinjection réparties entre ces derniers (figure 4.1).

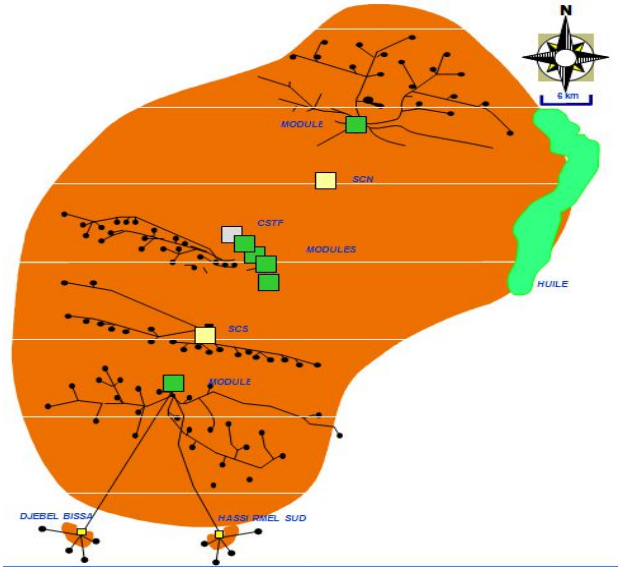


Figure 4.1 – les zones d'exploitation à HRM

Le tableau 4.2 contient les zones d'exploitation avec leur constitution internes :

Tableau 4.2 – Les zones d'exploitation HRM

Zone	Description
Nord	constituée du module 3 (MPP 03) et de la station de compression dit Nord ;
Centre	composée des 3 modules de traitements (MPP 0 ,1 et 4), des communs (Phase B), le CSTF, la station SRGA et le CNDG ;
Sud	constituée du module 2 (MPP 02), de la station de compression Sud, CTG DJB et du CTG –HR SUD.

Les puits en exploitation sont répartis comme suit :

- 162 puits producteurs de gaz ;
- 55 puits injecteurs de gaz ;
- 28 puits producteurs d'huile.

Les unités de Hassi R'mel sont composées de :

- 05 Modules (MPP 0,1,2,3 et 4) de traitement de gaz, production de gaz sec (ou gaz de vente), condensât, GPL;
- 02 Centres de traitement de gaz : CTG Djebel Bissa et HR/SUD ;
- 01 Centre de stockage et de transfert ;
- 02 Stations de réinjection de gaz : SCN et SCS ;
- 05 Centres de traitement d'huiles CTH1/2/3/4 et CTH SUD ;
- 01 Station de récupération des gaz associés (SRGA).

2. Description du four

Les rebouilleurs sont des équipements incontournables dans les unités de traitement du gaz brut, ils permettent de réchauffer le fond des colonnes (dééthaniseur et débutaniseur).

Notre présente étude portera sur le four H201 du train 1, module 1, qui permet de réchauffer le fond de la colonne T201 dé-éthaniseur pour une meilleur séparation de condensat.

Les séquences de fonctionnement et de sécurité sont assurées par un système à relais.

Les facteurs de déclenchement sont intégrés à différent niveaux pour une protection maximal de ces équipements.

2.1.Présentation générale

La figure 4.2 est un schéma représentatif du Four H201 du train 1, Module 1.

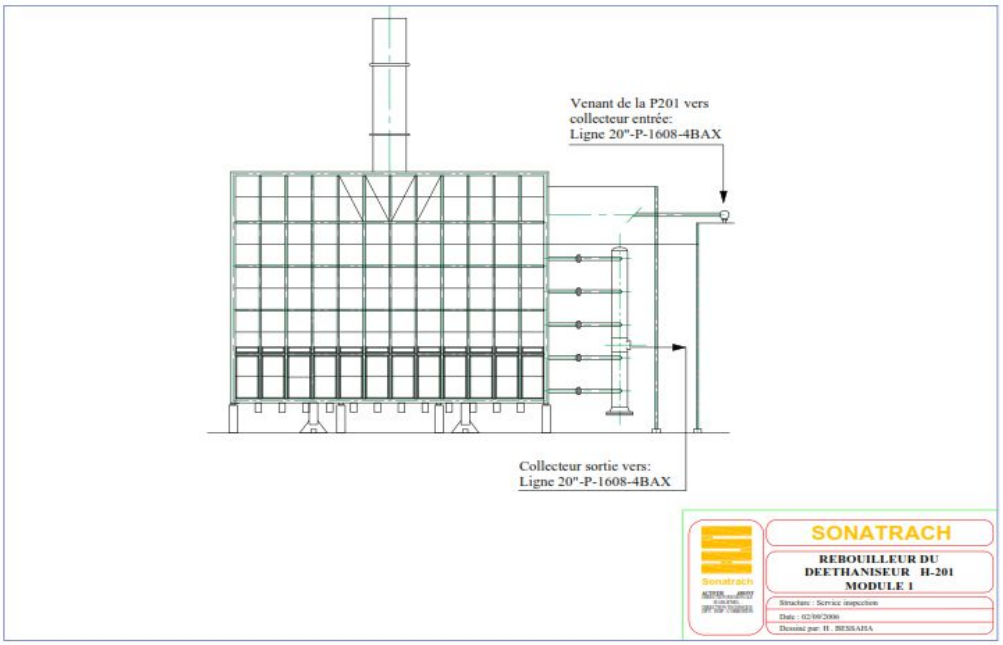


Figure 4.2 – Représentation schématique du four H201 du train 1, Module 1

Le tableau 4.3 illustre les informations collecter sur le four H201 qui représente notre cas d'étude :

Tableau 4.3 – Fiche technique du four H201

<table>
<tr><td>Unité</td><td colspan="3">Train 2 Module 1</td><td colspan="5"></td></tr>
<tr><td>Nom</td><td colspan="3">Rebouilleur du dééthaniseur</td><td>Repère</td><td colspan="2"></td><td colspan="2">12-H201</td></tr>
<tr><td>Code</td><td colspan="3">API RP 530</td><td>Date démarrage</td><td>1994</td><td>Dernier inspection</td><td colspan="2">Juin 2014</td></tr>
<tr><td>Diamètre (tube)</td><td colspan="3">168,3 mm</td><td>Constructeur</td><td colspan="4">SEC INDUSTRIES Bld d'anneaux Chateauroux France</td></tr>
<tr><td>Longueur(tube)</td><td colspan="3">12192 mm</td><td></td><td>2231</td><td>Date de Fabrication</td><td colspan="2">1993</td></tr>
<tr><td>Fluide</td><td colspan="3">Hydrocarbure</td><td>Parts</td><td>Epaisseur (mm)</td><td>Matériau</td><td>Nombre Tube</td><td>Diamètre Tube</td></tr>
<tr><td rowspan="5">Paramètres Opératoires</td><td></td><td>Pression (kg/cm2)</td><td></td><td>Paroi</td><td>/</td><td>/</td><td rowspan="2">10 passes</td><td rowspan="2">168,3</td></tr>
<tr><td></td><td></td><td></td><td>Tube</td><td>7,11</td><td>A 106 Gr B</td></tr>
<tr><td></td><td></td><td></td><td>Calandre</td><td>/</td><td>PWHT</td><td colspan="2">Oui</td></tr>
<tr><td>Sce</td><td>26</td><td>180</td><td>Radiographie</td><td>API 661</td><td>Volume</td><td colspan="2">17400 litres</td></tr>
<tr><td>Cal</td><td>27,5</td><td>370</td><td>Poids à Vide</td><td>/</td><td colspan="3"></td></tr>
<tr><td>Epr</td><td>55</td><td>Ambiante</td><td colspan="5">/</td></tr>
</table>

2.1.1. Partie rebouilleur

Cette partie contient les éléments nécessaires à l'allumage du four.

- 12 brûleurs pilotes.
- 12 brûleurs principaux.

2.1.1.1.Description du circuit fuel gaz

L'entrée principale de fuel gaz est équipée d'un filtre et d'une vanne d'autorégulatrice de pression PCV201, le circuit principal se partage ensuite en deux circuits différents :

a. Circuit pilote

Le passage de fuel gaz dans ce circuit est contrôlé par les vannes suivantes :

- Les vannes tout ou rien de sécurité : SDV 241, SDV 251, SDV 231
- Les électrovannes individuelles de chaque pilote : SDV 271-1 à SDV 271-12.
- Vanne de contrôle de pression du gaz PCV 211.

b. Circuit bruleur principal

Le passage du fuel gaz dans ce circuit est contrôlé par les vannes suivantes :

- Les vannes tout ou rien de sécurité : SDV 211, SDV 221, SDV 231
- Vanne de contrôle de débit : FCV 271, ce dernier sert à réguler la température de sortie du circuit condensat.
- Vanne de contrôle de pression du gaz PCV 221.

Le principe de démarrage et de conduite de chaque four est la suivante :

- Mise en condition de démarrage et allumage des pilotes et bruleurs en local par actions manuelles sur les organes locaux, ou sur la face avant du tableau de commande local.
- Conduite du four depuis la salle de contrôle par surveillance des diverses indications de températures, pressions, débit, ainsi que des différentes alarmes présentes au niveau du tableau de contrôle.

La seule action possible depuis la salle de contrôle concerne la sécurité est l'arrêt du four par action sur bouton poussoir de Mise Hors Service, cette dernière a pour conséquence la fermeture des vannes automatiques d'alimentation en gaz des circuits pilotes et des bruleurs.

Figure 4.3 - tableau local du four H201

2.1.2. Parties commande et signalisation

Cette partie contient les éléments nécessaires à l'automatisation du démarrage et de la surveillance du four H201.

2.1.2.1.Signalisations et alarmes

a. Signalisations

Un certain nombre de signalisations sont reportées sur le tableau local 4.4 afin de faciliter le démarrage et la surveillance du four depuis les unités :

Tableau 4.4 - Principe de signalisation des composantes

Circuit	Composant	Nombre de composant	Position
Pilote	Electrovanne	12	Fermée
			Ouverte
	Electrovanne d'alimentation	3	Ouverte
			Fermée
Bruleur	Vanne manuelle	12	Ouverte
			Fermée
	Electrovanne d'alimentation	3	Ouverte
			Fermée
/	Registre de la cheminée	1	Ouverte
			Fermée
Air	Vantelles d'arrivée	1	Ouverte
Pilote	Détecteur de flamme	12	Présence individuelle de flamme
Air	Ventilation	1	Arrêt
		1	En cours
		1	Autorisation
Pilote	Allumage pilotes	1	Autorisation
Bruleurs	Allumage bruleurs	1	Autorisation

b. Alarme

Le tableau suivant représente toutes les alarmes ayant des actions de sécurité signalées au niveau du tableau local, et de la signalisation sur le tableau de la salle de contrôle :

Tableau 4.5 – Alarmes et descriptions

Alarme	Code	Description
PAHH	201	Pression très haute gaz combustible.
PALL	201	Pression très basse combustible.
PAHH	231	Pression très haute sortie condensat.
TAHH	231	Température très haute sortie condensat.
FSLL	201	Débit très bas condensat.
TAHH	281	Température très haute entre convection / radiation.
TAHH	271	Température très haute fumées.
HRS	/	Arrêt d'urgence, hors service SDC (Salle De Contrôle).

BAL	201	Arrêt manque de flammes.
BAL	211	Ouverture brûleur non autorisé.
BAL	221	Alarme défaut de flammes.

Ces alarmes sont regroupées sur un ensemble de verrines, sur la partie supérieure du tableau local, au-dessus des différents boutons poussoirs, commutateurs, voyants, utilisés pour les séquences d'automatisme.

c. Commande

Cette partie comporte un certain nombre d'équipements électriques de commande :

- Commutateur de deux positions pour mise le circuit commande sous tension (1).
- Commutateur de deux positions pour By-pass/ pression de Gaz (1).
- Commutateur de deux positions pour By-pass /débit très bas de condensat (1)
- Commutateur de deux positions pou By-pass/klaxon (1).
- Commutateurs de deux position pour By-pass /Détecteur de flammes pour chaque pilote (12).
- Bouton poussoir d'arrêt d'urgence (2).
- Boutons poussoir marche / moteurs pour chaque ventilateur K201 et K202 (2).
- Boutons poussoir arrêt/ moteurs pour chaque ventilateur K201 et K202 (2).
- Bouton poussoir arrêt /pilotes par fermeture électrovannes circuit GAZ pilotes (1).
- Boutons poussoir ouvertures/ électrovannes individuelles pour chaque pilote (12).
- Boutons poussoir fermetures/ électrovannes individuelles pour chaque pilote (12).
- Boutons poussoir allumage individuel de chaque pilote (12).

2.1.3. L'appareillage électrique

Dans le tableau local on trouve un automate à logique câblée.

L'appareillage électrique est le moyen intermédiaire entre la source d'alimentation et le récepteur de chaque installation, son rôle est d'assurer trois fonctions : protection électrique, sectionnement et commande.

2.1.3.1. Alimentation

Il y a deux alimentations différentes (voir figure 4.4) :

a. Un transformateur (380/110 VAC) qui alimente :

- Les 12 transformateurs d'allumage des pilotes.
- Les 12 amplificateurs détecteurs de flammes.

b. Un transformateur (380/24 VCC) qui alimente tous les relais de commandes, les temporisateurs, la bobine contacteur principale, les voyants de signalisation et les alarmes.

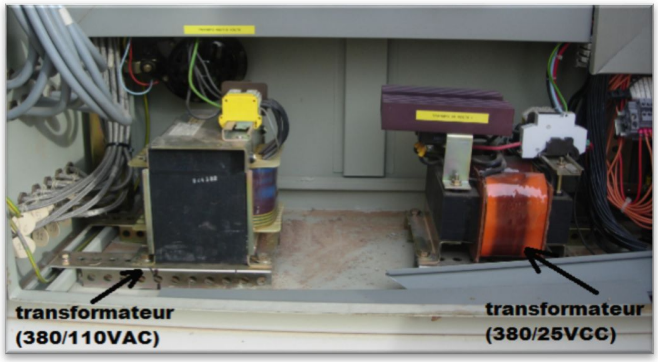


Figure 4.4 – Les transformateurs d'alimentation

2.1.3.2.Relais de commande

C'est un appareil dans lequel un phénomène électrique (courant ou tension), contrôle la commutation ON/OF d'un élément mécanique. Il est doté d'un bobinage comme organe de commande. La tension appliquée à ce bobinage va créer un champ magnétique capable de faire déplacer les trois contacts mobiles.

Dans le tableau local il y a 84 Relais, chaque relais contient une bobine alimentée par une tension continue 24VCC et trois contacts NO / NF (Normalement Ouvert / Fermé).

2.1.4. Liste des alarmes

- FAL 201 Débit bas condensat.
- FALL 201 Débit très bas condensat.
- PAL 201 Pression basse combustible.
- PALL 201 Pression très basse combustible.
- PAH 201 Pression haute combustible.
- PAHH 201 Pression très haute combustible.
- TAH 211 Température haute convection/radiation.
- TAHH 271 Température très haute convection/radiation.
- PAL 211 Pression basse gaz pilote.
- TAH 221-1 à 10 Température de peau de tube radiation.
- TAH 231 Température haute sortie condensat.
- TAHH 231 Température très haute sortie condensat.

- TAH 241 Température haute cheminée.
- TAHH 281 Température très haute cheminée.
- Arrêt d'urgence Mise hors service.
- PAH 231 Pression haute condensat.
- PAHH 231 Pression très haute sortie condensat.
- FAL 271 Débit bas combustible.
- FAH 271 Débit haut combustible.
- XA 201 Défaut électrique.
- BAL 201 Arrêt manque de flammes.
- BAL 211 Alarme défaut de flammes.
- BAL 221 Ouverture brûleur non autorisé.

2.2.Analyse structurelle et fonctionnelle

Pour une meilleure compréhension du système faisant l'objet de notre étude, nous avons opté pour la description du système. Cette dernière se fait à travers une analyse structurelle et fonctionnelle qui semble indispensable. Le but de cette analyse est de décomposer le système en identifiant les différentes fonctions qui composent chaque partie du système étudié.

Le tableau 4.6 résume tous les résultats obtenus par cette analyse :

Tableau 4.6 – Analyse fonctionnelle et structurelle

Système	**Sous-système**		**Equipement**		**Composant**	
	Code	**Description**	**Code**	**Description**	**Code**	**Description**
Four rebouilleur H201	**SS_1**	Sous-système de circuit d'alimentation du rebouilleur.	**E_{11}**	Circuit comburant (Fuel Gaz) assure l'alimentation en combustible.	**C_{111}**	**FCV271** : contrôle la température de sortie du circuit condensat.
					C_{112}	**PCV 211** : vanne de contrôle de pression du gaz.
					C_{113}	**12 pilotes** : garantissent une flamme continue pour l'amorçage du fuel gaz SDV241/251.
					C_{114}	**FV281-1 à 12** : 12 brûleurs (réalise la combustion de fuel gaz)..
			E_{12}	Circuit liquide (Condensat) : assure l'alimentation en huile des échangeurs.	**C_{121}**	**Pompes P201 A/B/C** pour pomper le condensat à l'entrée du four.
					C_{122}	**Vanne FV33** : régule le débit de condensat.
					C_{123}	Serpentin : assure la circulation et l'échauffement du condensat.
			E_{13}	Circuit d'air : assure une meilleure combustion.	**C_{131}**	**K201** : Soufflantes d'air
	SS_2	Sous-système de contrôle des	**E_{21}**	Contrôle de débit	**C_{211}**	**DCS** (SOLVER) : Adaptation du débit de

		paramètres du procédé.		(Contrôle le débit du liquide à l'entrée du four).		condensat à l'entrée de four par action sur la vanne FV 33.
					C_{212}	**FT 33** : Débitmètre, mesure le débit du liquide à l'entrée du four.
			E_{22}	Contrôle de la température du liquide à l'intérieur et à la sortie du four.	C_{221}	**DCS** (Solveur) : adaptation de la température du liquide à la sortie du four par action sur la vanne TV201.
					C_{222}	**TI** (Thermocouple) : mesure la température du liquide à la sortie du four.
					C_{223}	**TI** : Indicateurs de température locale.
	SS_3	Sous-système d'alarmes : conçu pour alerter l'opérateur par un signal audio-visuel.	E_{31}	**FAL 201** : alarme de bas débit du condensat à l'entrée du four. **PAL/ PAH 231** : alarme de basse/ haute pression de fuel gaz.	C_{311}	**FT** 201 (Débitmètre) : mesure le débit du liquide à l'entrée de four. **PT** 231 (Transmetteur de pression) : mesure de la pression de fuel gaz.
					C_{312}	**DCS** : Adaptation de la mesure de température, débit et pression à une alarme audio-visuelle dans la salle de contrôle.
	SS_4	Sous-système d'arrêt d'urgence qui met le four à l'état d'arrêt avec la coupure de l'alimentation en fuel gaz.	E_{41}	**FALL 201**: alarme de très bas débit du condensat. à l'entrée du four. **PALL/PAHH 201**: alarme de très basse ou très haute pression de fuel gaz.	C_{411}	**FT** 201 : Débitmètre. **PT** 201 : Transmetteur de pression. **BAL** : 12 Détecteurs de flamme (Ultraviolet).
					C_{412}	**SDV211/ SDV221** : Isolement de la ligne de gaz combustible.

				TAHH 231: alarme de très haute température du condensat. **BAL** 201/211/221: détecteurs de flamme.	C_{413}	**Solveur** (Relais de sécurité) : assure les missions de mise en sécurité du four par action sur les vannes SDV211/221.

3. Détermination des scénari critiques

Dans cette étape, nous allons déterminer les scénari critiques qui peuvent se produire au sein du four, et cela, en se basant sur une étude HAZOP élaborée par le bureau d'étude DET NORSKE VERITAS (DNV). Une Partie de cette étude est présenté dans l'annexe 6, l'utilisation de la méthode HAZOP permet d'identifier les causes, les conséquences et les barrières de sécurité mises en œuvre dans le système pour faire face au développement de ces scénari.

L'étude HAZOP en question présente un ensemble de scénari dangereux, toutefois nous avons choisi les plus critiques, plus particulièrement, ceux pour lesquels le four se déclenche. Les scénari sont présentés dans le tableau 4.7.

Nous remarquons que la déviation « Pas/ pas assez de débit » est omni présente dans les évènements les plus dangereux. Ainsi nous retenons que cette déviation correspond aux scénari les plus critiques, retenons aussi que, d'après l'annexe 6, la conséquence provoquant un incendie ou une explosion est la plus catastrophique. Ainsi nous centrerons notre étude sur les ces deux éléments.

Tableau 4.7 - Scénari critiques ressortis de l'étude HAZOP

Déviation	Causes	Conséquences	Préventions	Protection
Pas/ pas assez de débit	Vanne FV33 sortie fond de colonne vers T202 bloquée fermée (défaillance de la boucle de régulation).	Réduction du débit d'arrivée de condensat à partir du four H201 avec montée en T° du pot sortie des tubes condensat du four.	FICAL201 alarme bas débit refoulement des pompes P201A/B/C.	TAHH271 alarme haute T° cheminée qui arrête le four.
Pas/ pas assez de débit	Vanne FV33 sortie fond de colonne vers T202 bloquée fermée (défaillance de la boucle de régulation).	Rupture des tubes du four H201 avec risque d'explosion / d'incendie du four.	FALL201 alarme bas débit refoulement des pompes. P201A/B/C qui arrête le four (fermeture des vannes brûleurs d'alimentation en fuel gaz).	Clapet anti-retour ligne d'alimentation en condensat depuis le four H201.
Pas/ pas assez de débit	Vanne LV13 sortie ballon eau glycol V207D fermée par défaillance de la boucle de régulation de niveau (cas représentatif des ballons glycol)	Entraînement de glycol dans les tubes du four H201 avec formation de dépôts.	Inspection périodique des tubes du four.	TAHH281 alarme haute T° zone de radiation qui arrête le four.

4. Evaluation des critères de performance

4.1.Niveau d'Intégrité de sécurité (SIL)

Pour arriver à une évaluation du SIL, nous allons déterminer le SIL requis ensuite nous calculerons le SIL réel, à la suite de quoi, nous comparerons les deux pour vérifier la conformité du système envers les dispositions des normes CEI 61508 et CEI 61511. A noter que, La notion de SIL est largement développée dans ces normes.

4.1.1. Détermination du SIL requis

Dans cette partie nous avons comme tache la détermination du SIL requis, pour ce faire, nous utiliserons une méthode qualitative qui est très utilisée lors de la conception des systèmes de sécurité, de par sa facilité d'application et sa rapidité de résolution, c'est la méthode du graphe de risque.

Le graphe de risque est une méthode dédiée aux SIS, qui permet de définir le niveau de SIL requis en fonction de paramètre prédéfinis.

4.1.1.1.Application du graphe de risque

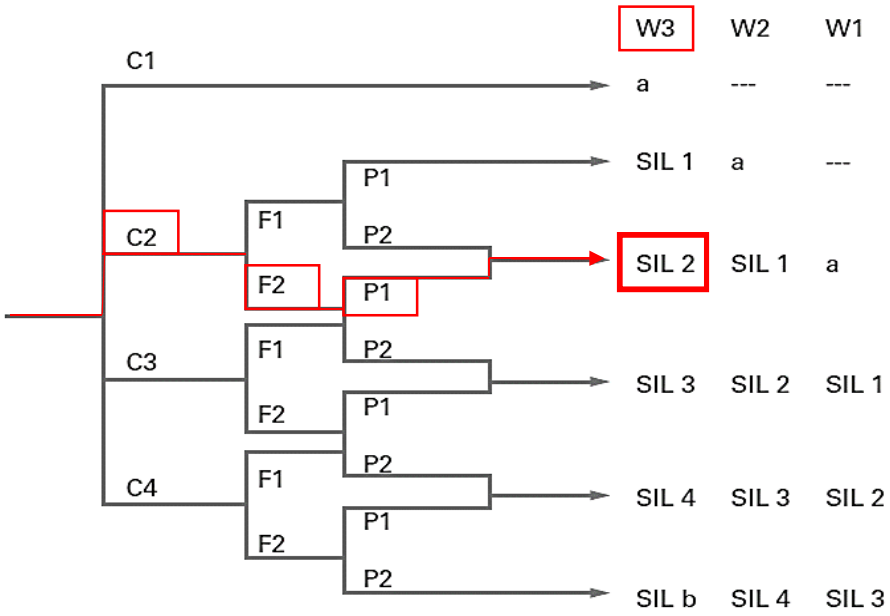
Le choix des conséquences à étudier est fonction de la méthodologie d'évaluation des risques adoptée par l'entreprise et des ressources qu'elle doit mettre en place pour affiner l'analyse.

Tableau 4.8 - Caractérisation des paramètres C, P, F et W

Scénario	Pas/ pas assez de débit			
Evènement dangereux	un incendie ou une explosion	Conséquence de l'événement dangereux (C),	Blessures graves sur plusieurs personnes avec décès possible de l'une d'entre elles.	C2
		Fréquence et durée d'exposition au danger (F),	Fréquence d'exposition importante (exposition fréquente à permanente dans une zone dangereuse).	F2
		Possibilité d'éviter l'événement dangereux (P),	Possible dans certaines conditions.	P1
		Probabilité de l'occurrence non souhaitée (W).	Forte probabilité (en 30 ans, 3 incendies, seulement chez SONATRACH).	W3

4.1.1.2.Présentation des résultats

En appliquant les résultats du tableau 4.8 sur la figure 3.8 (chapitre 3), nous trouverons la figure 4.5 :



--- : Aucune prescription sécurité n'est nécessaire

a : Pas de prescription sécurité particulière

b : Un SIS n'est pas suffisant pour garantir de la maîtrise des risques

Figure 4.5 – modèle du graphe de risque

Cela, nous ramène à déduire le SIL requis du système d'arrêt d'urgence automatique du four, qui correspond à un SIL 2.

4.1.2. Calcul de SIL réel

Le calcul du SIL réel du système d'arrêt d'urgence automatique correspondant au four H201 comporte deux étapes :

- La modélisation du système pour faciliter l'étude et permettre son insertion sur l'interface du logiciel.
- Le calcul de la probabilité de défaillance à la demande (PFD) en se basant sur l'architecture du système modélisé.

Nous effectuerons, à la fin des calculs, une discussion accompagnée d'une interprétation sur les résultats trouvés.

4.1.2.1.Présentation de l'outil de simulation (Module SIL)

Le Module SIL fait partie d'une série de modules qui compose le logiciel **GRIF** développé par TOTAL. Cet outil est conçu pour évaluer la PFD d'un système instrumenté de sécurité (SIS). Plus exactement, il quantifie l'indisponibilité d'un système modélisé à l'aide d'un arbre de défaillances. L'événement redouté est considéré comme étant la non-détection d'une panne dangereuse. Les arbres de défaillances utilisés pour faire les calculs sont composés de trois parties : capteurs, solveur, actionneurs. La fonction instrumentée de sécurité (SIF) traitée est une fonction d'arrêt dans une unité à process continu et dont le fonctionnement est en mode "sollicitation rare".

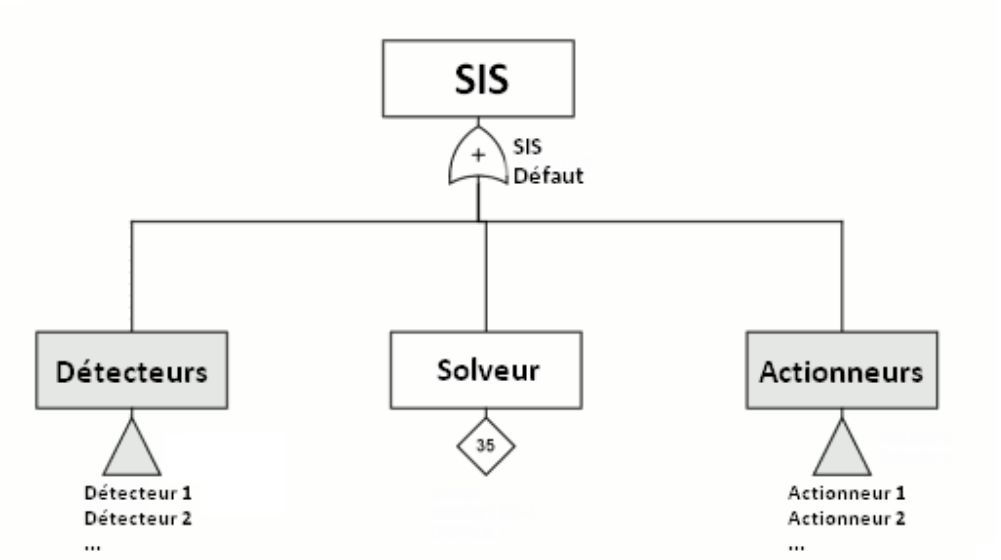


Figure 4.6 - Arbre de défaillance d'un SIS

Le modèle d'arbre de défaillance utilisé par le module SIL pour modéliser les SIS est représenté dans la figure 4.6. Nous relevons que l'élément unité de traitement (Solveur) est considéré comme étant un nœud de défaillance secondaire (induite par une défaillance externe au composant), alors que le détecteur et l'actionneur sont représentés par des nœuds de transfert ce qui indique qu'un sous arbre défini ailleurs peut être greffé en dessous de l'un d'eux ou tous les deux.

4.1.2.2.Hypothèses

- Le système d'arrêt des brûleurs est un système faiblement sollicité (moins d'une fois / an), d'où le besoin d'évaluer la PFD et non pas la PFH (probabilité de défaillance par heure). Dans ce cas, la PFD instantanée est assimilée à une indisponibilité instantanée.

- Nous utilisons les taux de défaillances λ_D des composants qui désignent les taux de défaillances dangereuses non détectées λ_{DU} et les taux de défaillances détectées λ_{DD}. Ces défaillances dangereuses font passer le système de l'état normal à l'état de défaillance dangereuse.
- Les composants sont réparables. Ainsi nous estimons que chaque composant possède un réparateur et la durée d'une réparation est fortement négligeable devant le temps entre deux pannes.
- Chaque "événement" est indépendant, ce qui signifie que les défaillances des composants doivent être indépendantes, mais aussi que la réparation d'un composant ne dépend pas de celle d'un autre (il y a autant de réparateurs que de composants).
- Le système est considéré statique du point de vue de son architecture. C'est à dire qu'il n'est pas possible de prendre en compte des reconfigurations.

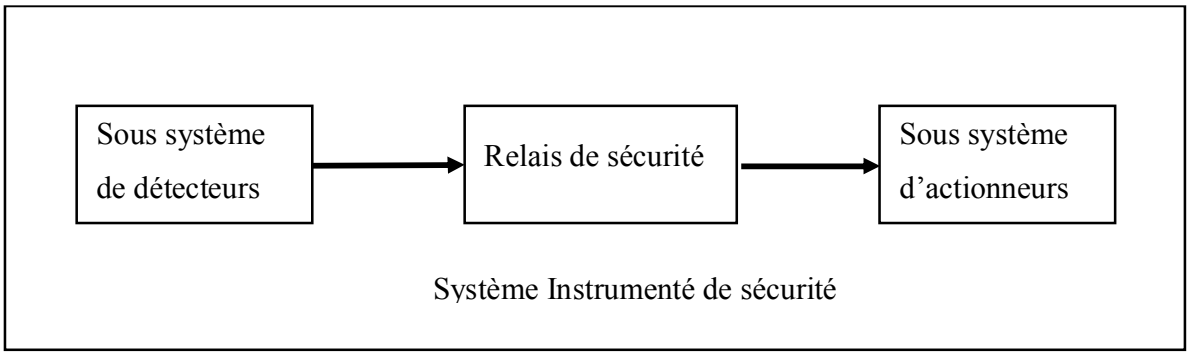


Figure 4.7 - Schématisation d'un SIS

- L'ensemble des paramètres utilisés (Lambda (λ), MTTR, ...) sont constants. La probabilité moyenne de défaillance sur demande du système instrumenté de sécurité est déterminée par le calcul et la combinaison de La probabilité moyenne de défaillance sur demande pour tous les sous-systèmes assurant ensemble la fonction de sécurité (sous système de détecteurs, relais de sécurité et sous système d'actionneurs).

4.1.2.3. Eléments d'entrée

Les éléments d'entrée représentent les données du système étudié, majoritairement, ce sont des données techniques, au regard du taux de défaillance, temps de réparation... etc. Ces éléments nous permettent de faire dérouler le module de calcul. Ils sont partagés en catégories, les éléments d'entrée caractérisant le sous-système de détecteurs, les relais de sécurité et enfin ceux du sous-système d'actionneurs.

Nous rappelons que les données présentées ci-dessous ont été extraites de base de données OREDA [48] et de la base documentaire du logiciel GRIF.

a. Sous-système de détecteurs

Comme l'indique son nom, le système de détecteurs est composé d'un ensemble de détecteurs, tel que chacun d'entre eux accomplit une fonction bien déterminée.

Tableau 4.9 - Données relatives aux éléments du sous-système des détecteurs

	Intervalle entre les tests (ans)	Lambda (λ_i) 10^{-6} h^{-1}	DC (%)	MTTR (heures)	Temps d'échange (heures)	Défaillance due aux tests (probabilité)
PAHH 201	3	5,75	90	48	8	0
PALL 201	3	5,75	90	48	8	0
PAHH 231	3	5,75	90	48	8	0
TAHH 231	3	5,70	90	48	8	0
FSLL 201	3	3,59	90	48	8	0
TAHH 281	3	5,70	90	48	8	0
TAHH 271	3	5,70	90	48	8	0
BAL 201	3	1.05	80	72	8	0
BAL 211	3	1.05	80	72	8	0
BAL 221	3	0.84	80	72	8	0

Tous les détecteurs représentés dans le tableau 4.9 sont des éléments simples sauf pour BAL 201, BAL 211 et BAL 221, qui sont des éléments complexes parce qu'ils sont l'issue d'une combinaison de détecteurs de flamme. Il existe 12 détecteurs de flamme (UV) (F) liés à 12 relais de sécurité. Le calcul des taux de défaillance de ces trois unités est fait en se basant sur la figure 4.8 et la logique dévoilée par les relais de sécurité correspondants, comme illustré dans la figure du schéma électrique du sous-système II des relais de sécurité relatif aux détecteurs de flamme (BAL).

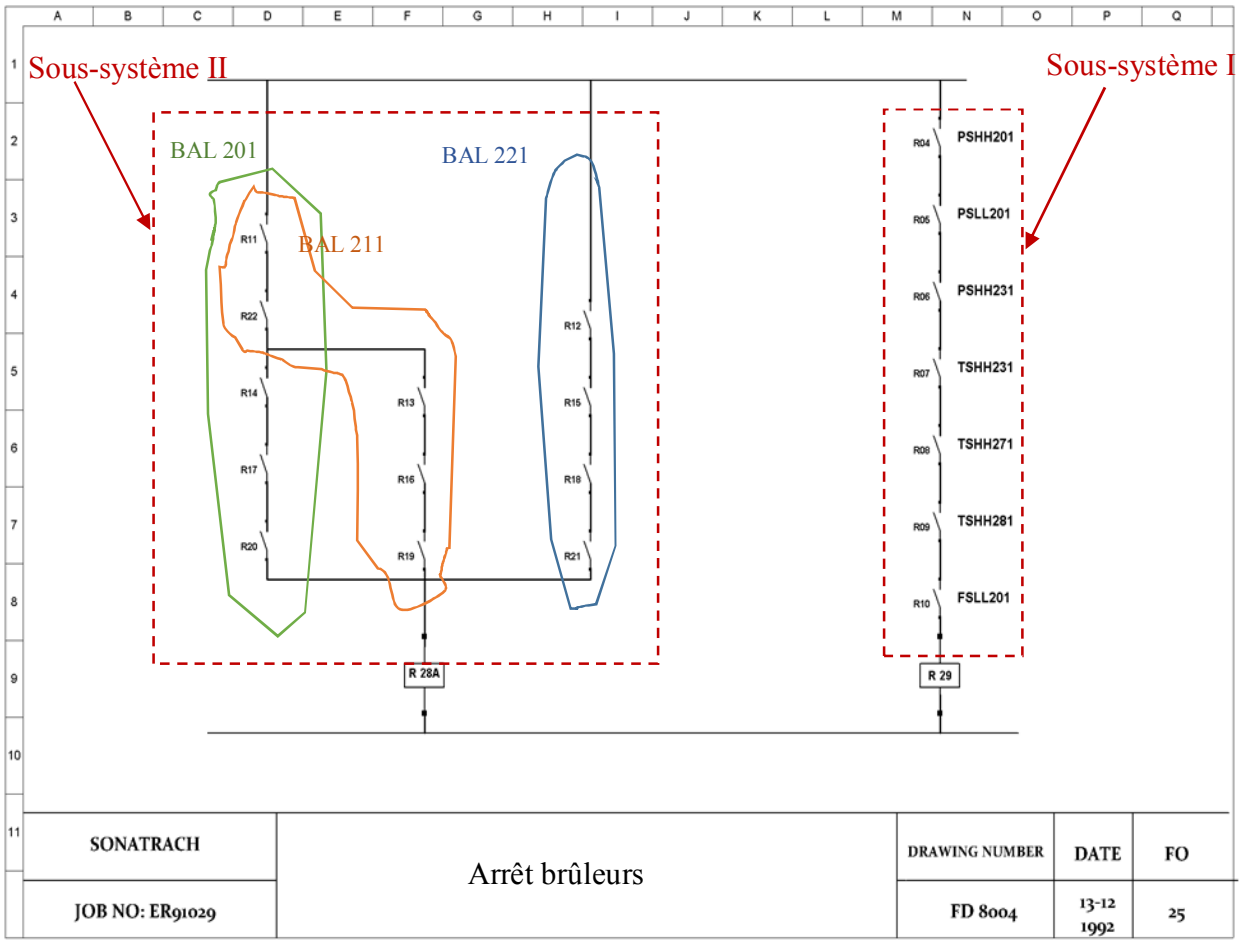


Figure 4.8 - Relais de sécurité relatifs au système d'arrêt des bruleurs

Formule générale pour le calcul du taux de défaillances associé

Pour calculer le taux de défaillances équivalent, nous allons appliquer des formules de la sureté de fonctionnement :

- **Configuration en série** : le taux équivalent est la somme de tous les taux qui sont en série, comme suit :

$$\lambda_{éq} = \sum_{i=1}^{n} \lambda_i \quad ; \text{tel que i = 1…n (n : est le nombre des composants)}$$

- **Configuration parallèle**, le taux équivalent est donnée par la formule suivante, pour : λ_1 et λ_2 en parallèles, leur $\lambda_{éq}$ est calculer comme suit :

$$\frac{1}{\lambda_{éq}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} \quad => \quad \lambda_{éq} = \frac{\lambda_1 + \lambda_2}{\lambda_1 + \lambda_2}$$

Le tableau 4.10 résume les formules de calcul des taux de défaillance spécifique pour chaque association des composants de nos sous-systèmes :

Tableau 4.10 : Calcul de $\boldsymbol{\lambda_{éq}}$

Type de configuration	Taux de défaillance équivalent ($\lambda_{éq}$)
Configuration en série	$\boldsymbol{\lambda_{éq} = \sum_{i=1}^{n} \lambda_i}$ **; avec : i = 1…n**
Configuration en parallèle	$\boldsymbol{\lambda_{éq} = \frac{\lambda_1 * \lambda_2}{\lambda_1 + \lambda_2}}$ **; avec : i = 1…n**

Détermination des taux de défaillance (λ) associés aux détecteurs de flamme (F)

Pour calculer le taux de défaillances équivalent aux détecteurs de flamme, il faut d'abord avoir la valeur du taux de défaillances relatif à un seul détecteur de flamme (nous n'avons besoin que d'un seul taux de défaillance correspond à un détecteur de flamme, tous les détecteurs de flamme étant identiques).

La base de données OREDA, nous donne :

$$\boldsymbol{\lambda_{i\ (détecteur\ de\ flamme)} = 0.21 * 10^{-6} h^{-1}}$$

Pour **BAL 201** :

$\lambda_{BAL\ 201} = (\lambda_{F11} + \lambda_{F22} + \lambda_{F14} + \lambda_{F17} + \lambda_{F20})$

$= (0{,}21.10^{-6} + 0{,}21.10^{-6} + 0{,}21.10^{-6} + 0{,}21.10^{-6} + 0{,}21.10^{-6})$

$$\boldsymbol{\lambda_{BAL\ 201} = 1{,}05.\ 10^{-6}\ h^{-1}}$$

Pour **BAL 211** :

$\lambda_{BAL\ 211} = (\lambda_{F11} + \lambda_{F22} + \lambda_{F13} + \lambda_{F16} + \lambda_{F19})$

$= (0{,}21.10^{-6} + 0{,}21.10^{-6} + 0{,}21.10^{-6} + 0{,}21.10^{-6} + 0{,}21.10^{-6})$

$$\boldsymbol{\lambda_{BAL\ 211} = 1{,}05.\ 10^{-6}\ h^{-1}}$$

Pour **BAL 221** :

$\lambda_{BAL\ 221} = (\lambda_{F12} + \lambda_{F15} + \lambda_{F18} + \lambda_{F21})$

$= (0{,}21.10^{-6} + 0{,}21.10^{-6} + 0{,}21.10^{-6} + 0{,}21.10^{-6})$

$$\boldsymbol{\lambda_{BAL\ 221} = 0.84.\ 10^{-6}\ h^{-1}}$$

Le tableau 4.11 résume toutes les données relatives aux taux de défaillance équivalent aux BAL qui sont composés les détecteurs de flammes du four :

Tableau 4.11 – Données sur les taux de défaillance équivalent aux BAL

BAL	201	211	221
$\lambda_{éq}$ **(h^{-1})**	$1{,}05.10^{-6}$	$1{,}05.10^{-6}$	$0{,}84.10^{-6}$

b. Relais de sécurité

Les relais de sécurité sont des appareils qui réalisent des fonctions de sécurité. Une fonction de sécurité vise à atténuer, en cas de danger, les risques existants. Ces blocs logiques de sécurité surveillent ainsi une fonction spécifique. Grâce à la mise en série avec d'autres relais, ils assurent l'ensemble de la surveillance d'une unité ou de l'installation.

Détermination du taux de défaillances (λ_{RS}) associé à l'ensemble des relais de sécurité :

Nous avons 19 relais de sécurité repartis sur 3 branches parallèles comme suit :

- **Branche 1** : contient 4 relais en série relatif au sous-branche BAL 221 du sous-système détecteur de flamme.
- **Branche 2** : contient 2 relais en série avec 2 sous-branches en parallèle identique, chacune contient 3 relais en série relatifs aux sous-branches BAL 201 et BAL 211 du sous-système de détecteur de flamme.
- **Branche 3** : contient 7 relais en série relatif au sous-système de détecteurs (sensors).

Le tableau 4.12, représente les taux de défaillance associés à chaque branche :

Tableau 4.12 – Composition des branches du sous-système relais de sécurité

Branches		**Composition des relais**
$\mathbf{B_{R1}}$		$\lambda_{R12} + \lambda_{R15} + \lambda_{R18} + \lambda_{R21}$
$\mathbf{B_{R2}} = B_{R21} + B_{R22}$	B_{R21}	$\lambda_{R11} + \lambda_{R22}$
	B_{R22}	$(\lambda_{R13} + \lambda_{R16} + \lambda_{R19})// (\lambda_{R14} + \lambda_{R17} + \lambda_{R20})$
$\mathbf{B_{R3}}$		$\lambda_{R11} + \lambda_{R22} + \lambda_{R14} + \lambda_{R17} + \lambda_{R20} + \lambda_{R17} + \lambda_{R20}$

La formule suivante explique la combinaison entre toutes les branches :

$$\boldsymbol{\lambda_{RS} = \lambda\,(B_{R1})\ //\ \lambda\,(B_{R2})\ //\ \lambda\,(B_{R3})}$$

De plus :

$$\boldsymbol{\lambda_{RS} = \lambda\,(B_{R1})\ //\ ((\lambda\,(B_{R21}) + \lambda\,(B_{R22}))\ //\ \lambda\,(B_{R3})}$$

Sachant que tous les relais de sécurité sont identiques, la valeur trouvée du taux de défaillance est :

$$\boldsymbol{\lambda_{Ri} = 5.10^{-8}\ h^{-1}}$$

Le tableau 4.13 est relatif aux résultats trouvé pour le calcul des taux de défaillance associé à chaque branche :

Tableau 4.13 – Calcul des $\lambda(B_{Ri})$ équivalant

		$\lambda(B_{Ri})$ équivalant en (h^{-1})	
Branche		Calcul	Résultat
$\mathbf{B_{R1}}$		$4 * 5 * 10^{-8}$	$\lambda(B_{R1}) = 20.10^{-8}$
$\mathbf{B_{R2}} = B_{R21} + B_{R22}$	B_{R21}	$2 * 5 * 10^{-8}$	$\lambda(B_{R21}) = 10.10^{-8}$
	B_{R22}	$\frac{1}{\lambda(B_{R22})} = \frac{1}{(3 * 5 * 10^{-8})} + \frac{1}{(3 * 5 * 10^{-8})}$	$\lambda(B_{R22}) = 7{,}5.10^{-8}$
$\mathbf{B_{R3}}$		$7 * 5 * 10^{-8}$	$\lambda(B_{R3}) = 35.10^{-8}$

Nous rappelons que le taux de défaillance total de sous-système relais de sécurité est donné par la formule suivante qui explique la combinaison entre toutes les branches :

$$\boldsymbol{\lambda_{RS} = \lambda\,(B_{R1})\ //\ \lambda\,(B_{R2})\ //\ \lambda\,(B_{R3})}$$

De plus :

$$\boldsymbol{\lambda_{RS} = \lambda\,(B_{R1})\ //\ ((\lambda\,(B_{R21}) + \lambda\,(B_{R22}))\ //\ \lambda\,(B_{R3})}$$

Le tableau 4.14, explique les calculs faits pour l'obtention du taux de défaillance équivalent pour le système de relais de sécurité :

Tableau 4.14 – Calcul de $\boldsymbol{\lambda_{éq}}$ au sous-système de relais de sécurité

Sous-branche	B_{R1}	$B_{R2} = B_{R21} + B_{R22}$	B_{R3}
$\boldsymbol{\lambda_i}$	20 .E-8 h^{-1}	17,5. 10^{-8} h^{-1}	35.10^{-8} h^{-1}
Formule de λ_{RS}	**$\lambda(B_{R1})$ // $\lambda(B_{R2})$ // $\lambda(B_{R3})$**		
	$\boldsymbol{\frac{1}{\lambda_{RS}} = \frac{1}{20.10^{-8}} + \frac{1}{17,5.10^{-8}} + \frac{1}{35.10^{-8}}}$**		
$\lambda_{éq}$ (RS)	**7,36. 10^{-8} h^{-1}**		

Le tableau 4.15, résume toutes les données relatives aux relais de sécurité :

Tableau 4.15 - Donnée relatives aux relais de sécurité

	Intervalle entre les tests (ans)	Lambda (λ) 10^{-8} h^{-1}	MTTR (heures)	Défaillance due aux tests (probabilité)
Relais de sécurité	**10**	**7,36.**	**36**	**0**

C. Sous-système d'actionneurs

Le sous-système d'actionneurs est composé de deux électrovannes configurées en parallèle, l'objectif assigné à ce sous-système est de fermer la conduite d'alimentation en cas de déclenchement du four H201, c'est-à-dire isolé le four H201 du reste du train.

Le tableau 4.16 illustre toutes les informations collectées soit au niveau de l'entreprise ou dans des bases de données relatives à l'industrie du process (ou de transformation), relatives aux éléments finaux (les actionneurs) de notre système instrumenté de sécurité .Ces éléments sont SDV shutdown valves ou vannes d'arrêt (tout ou rien).

Tableau 4.16 - Données relatives aux éléments du sous-système des actionneurs

	Intervalle entre les tests (ans)	Lambda (λ) 10^{-6} h^{-1}	DC (%)	MTTR (heures)	Défaillance due aux tests (probabilité)
SDV 211	3	16,14	0	N/A	0
SDV 221	3	16,14	0	N/A	0

Notons que le caractère déterminé des détecteurs est de type A, parce que, ce sous-système est lié au Système Distribué de Contrôle (DCS – Distributed Control System), c'est-à-dire, s'il y aura une défaillance dans un détecteur, la salle de contrôle sera informée. Alors que le sous-système d'actionneur ne l'est pas, le caractère déterminé des électrovannes (SDV) est donc de type B.

Le tableau suivant résume comme mentionnée dans le tableau 4.17 :

Tableau 4.17 – Caractère déterminé des éléments du notre système

Caractère du composant / Sous-système	Type A	Type B	Non type A/B
Détecteurs (Sensors)	X		
Actionneurs (Actuators)		X	

4.1.2.4.Modélisation et calculs

a. Modélisation

Pour tout système qui répond à la définition d'un SIS, le Module SIL(GRIF) nous permet de configurer son architecture sous une forme explicite. La configuration de notre système est présentée dans la figure 4.9

En partant du fait que chaque élément de détection du sous-système I (Figure 4.8) peut déclencher le système d'arrêt, cette logique nous permet de représenter les détecteurs de ce sous-système en parallèle, autrement dit, ils sont configurés sous l'architecture 1007, alors que pour les éléments du sous-système II (Figure 4.8), il faut au minimum le déclenchement d'un détecteur de chacune des séries BAL 201, BAL 211 et BAL 211 au même moment, pour déclencher l'arrêt du système, autrement dit ils sont configurés sous l'architecture 3003.

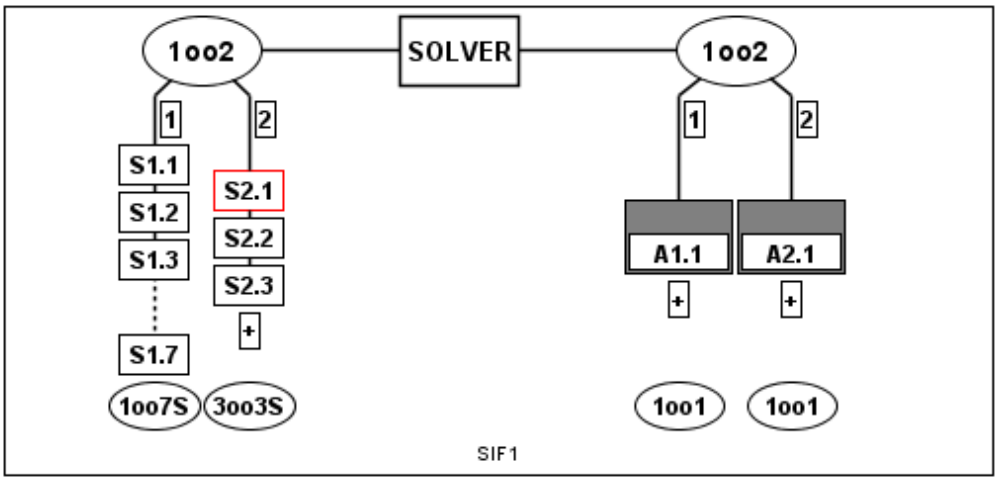


Figure 4.9 - Configuration du système d'arrêt des brûleurs

Tableau 4.18 - Analogie entre les éléments du système d'arrêt des brûleurs et les éléments présentés dans la modélisation du système.

S 1.1	**S 1.2**	**S 1.3**	**S 1.4**	**S 1.5**	**S 1.6**	**S 1.7**
FSLL 201	PAHH 201	TAHH 231	PALL 201	PAHH 231	TAHH 281	TAHH 271

S 2.1	**S 2.2**	**S 2.3**
BAL 201	**BAL 211**	**BAL 221**

A 1.1	**A 2.1**
SDV 211	**SDV 221**

B. Calcul

Le lancement du calcul avec le Module SIL du système modélisé en insérant les éléments d'entrées décrits précédemment, nous dévoile une courbe qui représente l'évolution de la probabilité de défaillance à la sollicitation moyenne (PFD_{avg}) en fonction de du temps (Figure 4.10). L'intérêt de cette courbe se résume dans le fait qu'elle nous permet de déterminer le SIL réel du système. Les Valeurs de la PFD_{avg} et du temps ressorti du calcul sont représentés dans le tableau

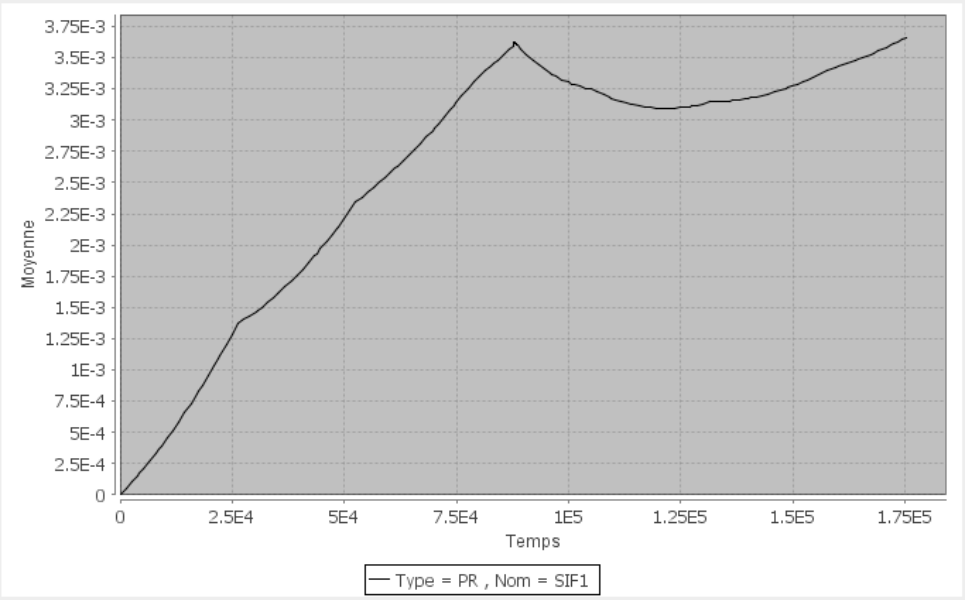


Figure 4.10 - Evolution de la PFD_{avg} en fonction de du temps (heures)

L'avantage de ce module est la détermination de la contribution de chaque sous-système, voire de chaque composant du SIS dans le SIL calculé. La figure 4.11, caractérise chaque composante avec une **PFD_{avg}**, un facteur de réduction de risque (**RRF**) et un SIL calculé.

	PFD Avg	RRF	SIL Calculé	Contribution (%)
Partie Capteur(s)	0	3.13E20	4	0%
Partie Solveur	3.27E-3	306.07	2	89.18%
Partie Actionneur(s)	3.96E-4	2523.04	3	10.82%
SIF	3.66E-3	273.05	2	100%

Figure 4.11 - Contribution de chaque composante du SIS au SIL calculé

Tableau 4.19 : Valeurs de la PFDavg en fonction du temps d'exploitation (heures)

Temps	PFD_{avg}
0	0,00000
1314	0,00005
2628	0,00010
3942	0,00015
4380	0,00017
5256	0,00021
6570	0,00027
7884	0,00033
8760	0,00037
9198	0,00039
10512	0,00045
11826	0,00052
13140	0,00059
14454	0,00066
15768	0,00073
17082	0,00080
17520	0,00083
18396	0,00088
19710	0,00096
21024	0,00104
21900	0,00109
22338	0,00112
23652	0,00120
24966	0,00129
26279	0,00137
26280	0,00137
26280	0,00137
27594	0,00140
28908	0,00143
30222	0,00147
30660	0,00148
31536	0,00150
32850	0,00154
34164	0,00158
35040	0,00161
35478	0,00162
36792	0,00166
38106	0,00171
39420	0,00176
40734	0,00181
42048	0,00186
43362	0,00191
43800	0,00193
44676	0,00197
45990	0,00203
47304	0,00209
48180	0,00213
48618	0,00215
49932	0,00221
51246	0,00228
52559	0,00235
52560	0,00235
52560	0,00235
53874	0,00238
55188	0,00242
56502	0,00246
56940	0,00248
57816	0,00250
59130	0,00254
60444	0,00259
61320	0,00262
61758	0,00263
63072	0,00267
64386	0,00272
65700	0,00277
67014	0,00282
68328	0,00286
69642	0,00292
70080	0,00293
70956	0,00297
72270	0,00302
73584	0,00308
74460	0,00311
74898	0,00313
76212	0,00319
77526	0,00325
78839	0,00331
78840	0,00331
78840	0,00331
80154	0,00335
81468	0,00339
82782	0,00344
83220	0,00345
84096	0,00348
85410	0,00352
86724	0,00357
87599	0,00360
87600	0,00360
87600	0,00360
87602	0,00363
87603	0,00363
87603	0,00363
87653	0,00363
87703	0,00363
87753	0,00363
87803	0,00363
87853	0,00362
87903	0,00362
87953	0,00362
88003	0,00362
88038	0,00362
88053	0,00362
88103	0,00361
88153	0,00361

88203	0,00361
88253	0,00361
88303	0,00361
88353	0,00360
88403	0,00360
88453	0,00360
88503	0,00360
88553	0,00360
89352	0,00357
90666	0,00352
91980	0,00348
91982	0,00348
93294	0,00344
94608	0,00341
95922	0,00338
96362	0,00337
97236	0,00335
98550	0,00333
99864	0,00330
100742	0,00329
101178	0,00328
102492	0,00327
103806	0,00326
105119	0,00325
105120	0,00325
105120	0,00325
105122	0,00325
106434	0,00322
107748	0,00320
109062	0,00318
109502	0,00318
110376	0,00317
111690	0,00315
113004	0,00314
113882	0,00313
114318	0,00313
115632	0,00312
116946	0,00311
118260	0,00310
118261	0,00310
119574	0,00310
120888	0,00310
122202	0,00310
122641	0,00310
123516	0,00310
124830	0,00310
126144	0,00311
127021	0,00311
127458	0,00311
128772	0,00312
130086	0,00313
131399	0,00314
131400	0,00314
131400	0,00314
131401	0,00314
132714	0,00315
134028	0,00315
135342	0,00315
135781	0,00315
136656	0,00316
137970	0,00316
139284	0,00317
140161	0,00318
140598	0,00318
141912	0,00319
143226	0,00320
144540	0,00321
144541	0,00321
145854	0,00322
147168	0,00324
148482	0,00325
148920	0,00326
149796	0,00327
151110	0,00329
152424	0,00331
153300	0,00332
153738	0,00333
155052	0,00335
156366	0,00337
157679	0,00340
157680	0,00340
157680	0,00340
157680	0,00340
158556	0,00341
159432	0,00342
160308	0,00343
161184	0,00344
162060	0,00345
162060	0,00345
162936	0,00346
163812	0,00348
164688	0,00349
165564	0,00350
166440	0,00351
166440	0,00351
167316	0,00353
168192	0,00354
169068	0,00355
169944	0,00357
170820	0,00358
170820	0,00358
171696	0,00360
172572	0,00361
173448	0,00363
174324	0,00365
175199	0,00366
175200	0,00366
175200	0,00366

Approximation polynomiale de la PFD_{avg} :

L'approximation consiste à soustraire une formule en fonction de la variable PFD_{avg} en se basant sur le tableau 4.19 accordé par le module SIL. En conséquence nous allons utiliser le logiciel Matlab, le fichier (.m file) du programme d'approximation est présenté dans l'annexe 7.

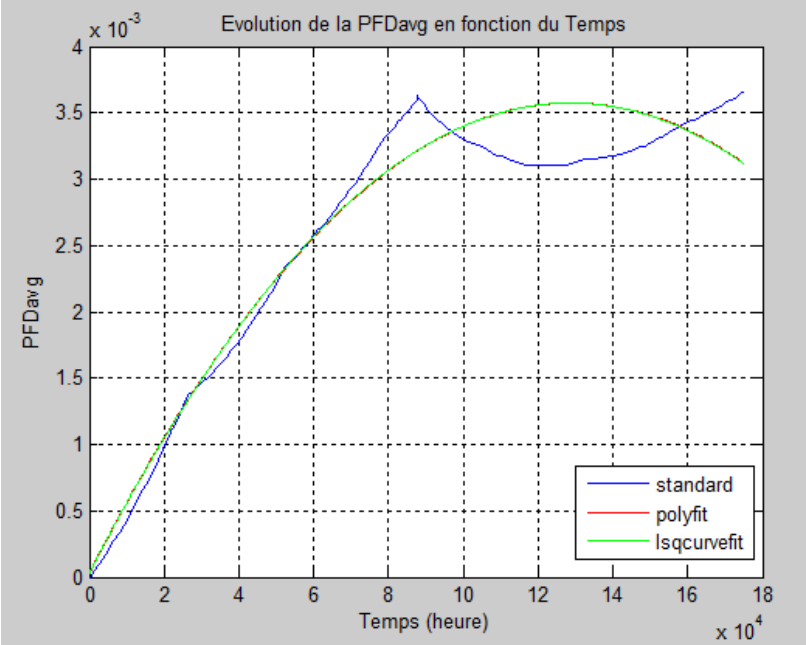


Figure 4.12 - Approximation en utilisant la fonction « Polyfit » et la fonction « lsqcurvefit »

Notons que la courbe en bleu « standard » représente les valeurs calculées par le module SIL, la courbe en vert est l'approximation en utilisant la fonction « Polyfit » alors que la courbe en rouge représente l' approximation avec la fonction « Lsqcurvefit » , les trois courbe sont tracées dans la figure 4.12. Nous remarquons que les deux fonctions « Polyfit « et « Lsqcurvefit » délivrent la même allure, la fonction de celles-ci est calculé par Matlab sous la forme d'un polynôme de deuxième degré :

$$\mathbf{F(x) = -2.132926e\text{-}13 * x^2 + 5.497704e\text{-}08 * x + 3.193612e\text{-}05}$$

Tel que :

- **F(x)** : représente la PFD_{avg}.
- **x** : représente le Temps (heures).

Nous pouvons déterminer le SIL à travers le calcul du maximum de la PFDavg sur la période d'exploitation de l'unité en question. Ainsi nous allons calculer le maximum de la fonction F(x).

Pour cela nous procéderons au calcul de **f(x)** qui est la dérivé de **F(x)** ensuite nous chercherons la solution de l'équation **f(x) = 0**, et en fin nous remplacerons la valeur trouvé dans la fonction F(x).

L'ensemble de ces étapes a été effectué en utilisant Matlab, le fichier (.m file) qui contient la séquence du programme est représenté dans l'annexe 8.

Les résultats trouvés après le déroulement du programme sont :

- Pour le temps : **x = 128880 heures**.
- Pour la PFD_{avg} : **F(x) = 0,0036**.

Donc, nous notons que : **Max (PFD_{avg}) = 3,6. 10^{-3}**

D'après le tableau 3.3 concernant la définition des niveaux SIL pour un mode de fonctionnement à faible sollicitation, le SIL correspondant à une PFDavg de 3,6. 10^{-3} est le SIL 2, parce que :

$$10^{-3} < 3,6.\ 10^{-3} < 10^{-2}$$

4.1.3. Présentation des résultats

La compilation avec le module SIL fait découler l'évolution de la PFD en fonction du temps, à noter aussi les effets des tests périodiques sur l'évolution de la PFD représenté dans la figure 4.13 et enfin la contribution de la valeur de la PFD en chaque niveau SIL.

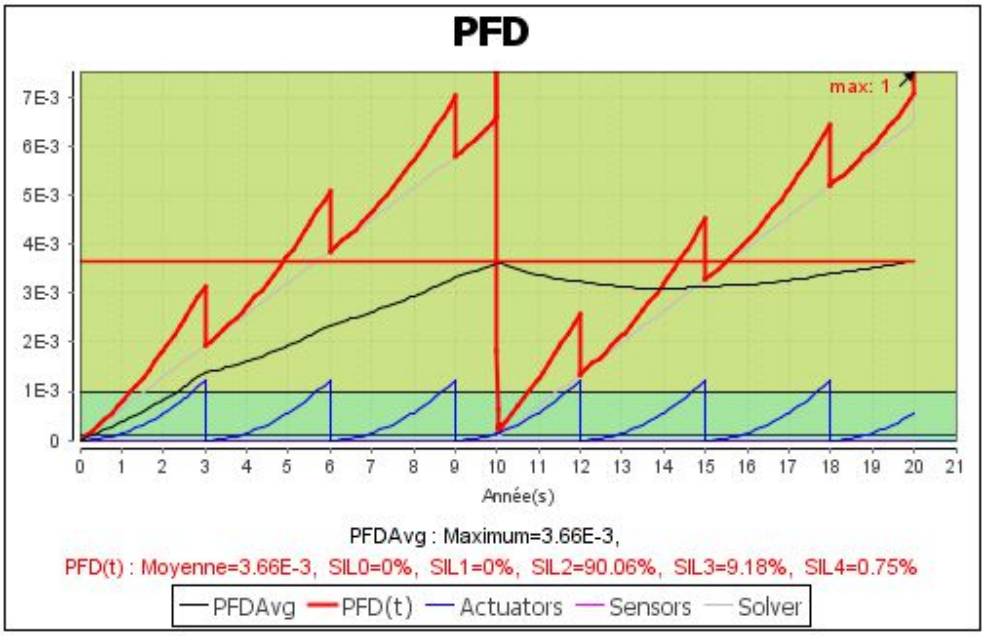


Figure 4.13 - Effet des tests périodiques sur l'évolution de la PFD

Nous retenons de la figure 4.13 les pourcentages suivants **SIL 2 = 90,06 %, SIL 3 = 9,18 %** et **SIL 4 = 0,75 %** qui représentent la contribution de la valeur de la PFDavg pour chaque niveau SIL.

Les tests de révision des systèmes d'exploitation et de sécurité, à l'image des SIS, génèrent une diminution de la PFD à chaque test périodique, cela est confirmé par la figure 4.13. Rappelons que l'objectif de ces tests est de veiller à l'atténuation de toute défaillance et la confirmation du bon état de l'unité en question, c'est ce qui justifier la diminution de la PFD parce que, principalement, il n'y pas de défaillance.

Le maximum de la $\mathbf{PFD_{avg}}$ correspond à la valeur moyenne déduite de la courbe en noire (figure 4.13), est égale à $\mathbf{3{,}66.\ 10^{-3}}$, ce qui répond à un **SIL 2** pour le système. On constate que cette valeur est égale la valeur de la PFDavg calculée dans la partie calcul (partie précédente).

En fin, Le module SIL résume les données de sortie après le traitement dans une fiche technique associée au système étudié, en précisant les valeurs des facteurs spécifiques qui caractérisent le système, nous citons le facteur de réduction du risque (RRF), une estimation du SIL requis, une proposition pour une configuration du système en terme du nombre de capteurs et de détecteurs et finalement le plus important un commentaire sur la conformité du système par rapport aux disposition des normes CEI 61508 et CEI 61511.

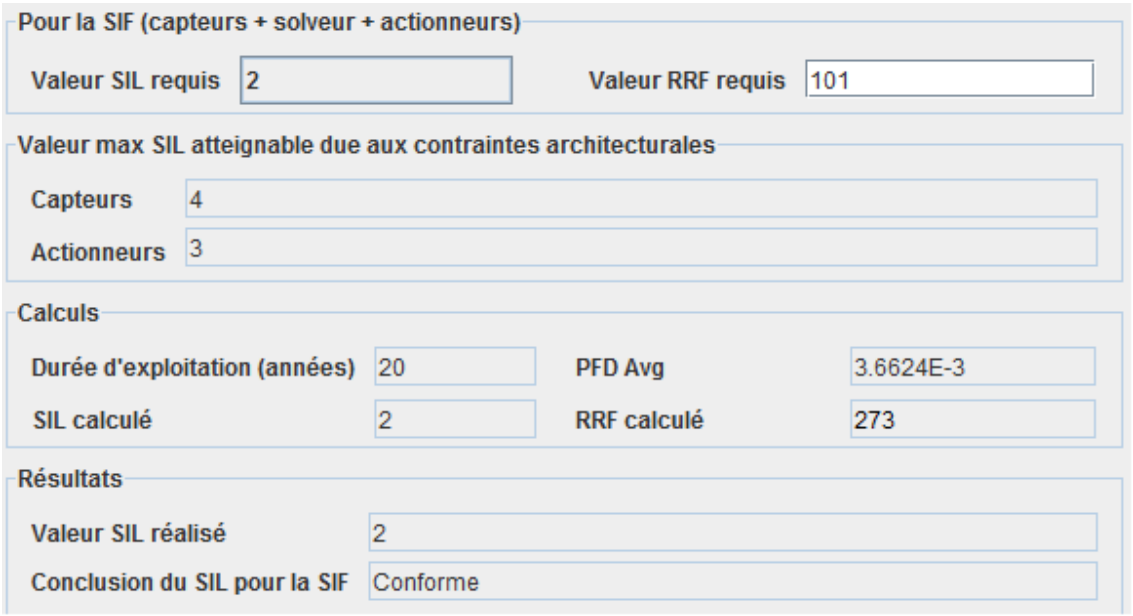


Figure 4.14 - Fiche technique des résultats trouvés par GRIF

4.2.Efficacité

Afin d'évaluer l'efficacité du système de mise en sécurité des fours rebouilleurs MPP1 (système d'arrêt d'urgence automatique), nous avons procédé à l'analyse du retour d'expérience des résultats des tests et d'entretiens des composants du SIS (détecteurs, automate programmable et actionneurs), sur une période d'observation estimée représentative, afin d'évaluer l'efficacité du SIS, traduite par le pourcentage (%) d'accomplissement de la fonction de sécurité pour laquelle il est conçu.

En effet, les tests du SIS sont réalisés par la Direction maintenance (vérification de la séquence soft et hard) pendant les différents arrêts programmés (triennaux). Cependant Nous avons choisi d'étudier la réponse du système d'arrêt d'urgence automatique des fours rebouilleurs des trois trains de l'unité MPP1.

Par conséquent, notre approche consiste à une évaluation de l'efficacité, en élargissant notre champs d'étude (avoir un échantillon représentatif) couvrant les trois fours rebouilleurs-MPP1, sur une période d'observation donnée (du 1996 au 2014) avec une fréquence triennale de test permettant de vérifier la disponibilité du SIS, et ce, pour voir plus de crédibilité et présomption.

A préciser que les SIS en questions sont identiques et se sont soumis aux mêmes conditions d'exploitation et de maintenance.

Ainsi nous présentons les résultats extraits de l'historique de SONTRACH : (Quand le système est fonctionné parfaitement on attribue la valeur 100 %, quand il y a une défaillance (soft/hard) empêchant le système de remplir totalement sa fonction de sécurité on attribue la valeur 0 %).

4.2.1. Arrêt Train

L'Arrêt de chaque train du module (MPP1) se fait périodiquement, chaque 3ans, le tableau joint récapitule les résultats des tests du système d'arrêt d'urgence automatique du four (SIS) (FV201, SDV211/221, SDV271SDV231/SDV261).

4.2.1.1.Rebouilleur H201 du Train 1, MPP1

Tableau 4.20 - Réponse du SIS par rapport à chaque arrêt triennal, Train 1

	1996	2000	2003	2006	2009	2012	2015
Réponse du système (%)	100	100	100	100	100	100	/

4.2.1.2.Rebouilleur H201 du Train 2, MPP1

Tableau 4.21 - Réponse du SIS par rapport à chaque arrêt triennal, Train 2

	1996	2000	2003	2006	2009	2012	2015
Réponse du système (%)	100	100	100	100	100	100	/

4.2.1.3.Rebouilleur H201 du Train 3, MPP1

Tableau 4.22 - Réponse du SIS par rapport à chaque arrêt triennal, Train 3

	1998	2001	2004	2007	2010	2013	2016
Réponse du système (%)	100	100	100	100	100	100	/

4.2.2. Arrêt Module

L'Arrêt du module (MPP1) se fait périodiquement chaque 10 ans, donc par rapport à l'arrêt qui a était effectué en 2006 nous avons trouvé les résultats du tableau 4.23 :

Tableau 4.23 : Réponse du SIS par rapport arrêt décennale, MPP1

	H201 (train1)	H201 (train2)	H201 (train3)
Réponse du système (%)	100	100	100

4.2.3. Calcul de la moyenne

Le tableau 4.24 représente les résultats des moyennes des réponses en % des 3 trains du module 1 obtenu après la collecte des données de l'historique des arrêts programmés.

Tableau 4.24 - Moyenne des réponses du SIS

	H201 (train1)	H201 (train2)	H201 (train3)	Moyenne générale
Moyenne des réponses en %	100	100	100	100

En effet, les résultats de cette évaluation montrent, explicitement, que l'efficacité du système est de 100%, autrement dit, durant toute la période d'exploitation de ce four, le système d'arrêt d'urgence automatique répond à la sollicitation sans aucune défaillance, y compris toutes les composantes du système. Cependant on tient à préciser que cela ne veut pas dire que tout le système d'arrêt d'urgence du train fonctionne à 100%, parce que les résultats des tests relatifs aux composantes des systèmes de sécurité montrent qu'il y a eu des défaillances, notamment des blocages de vannes, lors des tests, mais cela reste en dehors du four étudié.

Finalement, par rapport aux résultats déclinés, nous énonçons que le SIS du four est efficace. Ainsi il répond efficacement à la fonction de sécurité pour laquelle il est conçu.

4.3.Temps de réponse

Rappelons que le temps de réponse correspond à l'intervalle de temps entre le moment où le système d'arrêt d'urgence automatique, dans un contexte d'utilisation, est sollicité et le moment où la fonction de sécurité assurée par ce système est réalisée dans son intégralité. Ainsi le temps de réponse (TR) de ce SIS est égale au TR du sous-système d'actionneur + le TR des relais de sécurité + le TR du sous-système de détecteurs.

Pour déterminer le TR des sous-systèmes nous avons retenu le TR associé à la composante qui à la valeur la plus grande de TR, pour pouvoir étudier le cas le plus critique. Ceci va être appliqué aux détecteurs parce qu'ils sont différents. Cependant, pour les relais de sécurité et les vannes nous allons choisir la valeur commune de TR car ils sont identiques.

Tableau 4.25 - Liste des Valeurs du TR des détecteurs

	Détecteur de pression	Détecteur de température	Détecteur de débit	Détecteur de flamme
Temps de réponse (ms)	10	10	10	15

Tableau 4.26 - Liste des Valeurs du TR d'une série donnant l'action du système

	Composante de détection	Composante de traitement	Composante d'action
Temps de réponse (ms)	15	20	20-40

TR(SIS)max = TR (Détecteur) + TR (Analyseur) + TR (Actionneur)

= 15 + 20 + 40

$$\mathbf{TR(SIS)_{max} = 75\ ms}$$

Le temps de réponse maximal du système est de **75 ms**. Cependant, il n'existe pas de référence pour vérifier la conformité du temps de réponse. Cela relève des cahiers de charges de l'entreprise et des offres de leurs fournisseurs

Conclusion

L'utilisation du graphe de risques nous a permis de déterminer le SIL requis du système d'arrêt d'urgence automatique du four, et cela, en passant par la caractérisation des paramètres C, F, P et W. En conséquence, nous avons trouvé le SIL requis égale à SIL 2.

Les résultats de la PFD calculé par le module SIL, nous ramène à repérer le SIL réel du système étudié, en se basant sur les plages des valeurs de la PFD associé aux SIL. Suite à quoi, nous avons déterminé le SIL réel qui est SIL 2.

La comparaison entre les valeurs du SIL requis et le SIL réel, nous affirme l'égalité entre les deux, de ce fait, nous pouvons conclure que le système étudié est conforme au regard de ce critère de performance, qui est le SIL.

Par rapport aux résultats déclinés de l'étude sur l'efficacité et le temps de réponse, nous énonçons que le SIS du four est efficace. Ainsi il répond à la fonction de sécurité pour laquelle il est conçu sur un temps de réponse raisonnable.

Dans ce chapitre, nous avons montré l'intérêt de l'approche utilisée, au travers une méthodologie qualitative (le graphe de risque pour le calcul du SIL requis) dans un premier temps et quantitative (Arbre de défaillance du GRIF, l'efficacité, le temps de réponse) dans l'évaluation des critères de performance.

Conclusion Générale

La norme CEI 61508 est un référentiel pour la spécification et la conception des SIS. Sa déclinaison sectorielle dans le domaine du process industriel, CEI 61511, est destinée aux concepteurs et utilisateurs de ce domaine. Cette norme de sécurité fonctionnelle introduit une approche probabiliste pour l'évaluation quantitative de la performance des SIS, et la qualification de cette performance par des niveaux d'intégrité de sécurité.

L'évaluation de la performance des SIS prend une part de plus en plus importante dans les analyses de risques, du fait des enjeux humains, environnementaux et économiques liés à l'aptitude des SIS à éviter l'occurrence des scénari dangereux. En effet, les critères de SIL, d'efficacité et de temps de réponse permettent de juger la performance et de conclure sur l'adéquation d'un SIS vis-à-vis d'un phénomène dangereux. Dès lors, il apparaît nécessaire de disposer de méthodes ayant une traçabilité dans le temps, afin d'évaluer avec transparence les critères de performance qui permettent de garantir la bonne maîtrise des risques.

Nous avons montré l'intérêt de la démarche adoptée, à évaluer la performance du système d'arrêt d'urgence automatique du four rebouilleur H201, bien que le système en question soit complexe de part la redondance et le nombre de ses composantes, et aussi, la non disponibilité de tous les données relatives à ces composantes. Nous affirmons que les résultats de l'étude approuvent la performance du système et sa conformité par rapport aux dispositions des normes.

Enfin, notre contribution va servir certainement de base à des études plus poussées, il serait important d'étendre les calculs à d'autres critères de performance, tels que la maintenabilité et la testabilité, et de discuter leurs intégration surtout dans une approche floue. Une autre perspective intéressante, il s'agit d'utiliser d'autres méthodes de sûreté de fonctionnement pour l'évaluation des performances des SIS, comme les réseaux de Pétri ou les chaines de Markov.

Bibliographie

1. Comission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems*, in *Part 1: General requirements*. 2010. p. 1-66.
2. PERES, D.N.e.F., *Analyse des systèmes - Sureté de focntionnement.* technique de l'ingénieur, 2007. **1**(0): p. 1-17.
3. Comission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems* in *Partie 7: Présentation de techniques et mesures*. 2000. p. 1-238.
4. Comission, I.E., *Functional safety – Safety instrumented systems for the process industry sector* in *Part 3: Guidance for the determination of the required safety integrity levels*. 2003. p. 1-10.
5. Comission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems* in *Part 5: Examples of methods for the determination of safety integrity levels*. 2010. p. 1-50.
6. Comission, I.E., *Functional safety – Safety instrumented systems for the process industry sector* in *Part 1: Framework, definitions, system, hardware and software requirements*. 2003. p. 1-15.
7. Nguyen Thuy LE, A.A., Sylvain CHAUMETTE, Sébastien BOUCHET, Valérie DE DIANOUS., *Evaluation des Barrières Techniques de Sécurité - Ω 10.* INERIS, 2008. **1**(0): p. 1-87.
8. 61508-7, I., *Functional safety of electrical/electronic/programmable electronic safety-related systems –*, in *Part 7:Overview of techniques and measures*. 2000, IEC Geneva, Switzerland. p. 238.
9. Lamy, P., *Probabilité de défaillance dangereuse d'un système explications et exemple de calcul.* INRS, 2002: p. 50.
10. Brissaud, F., *CONTRIBUTIONS À LA MODÉLISATION ET À L'ÉVALUATION DE LA SÛRETÉ DE FONCTIONNEMENT DE SYSTÈMES DE SÉCURITÉ À FONCTIONNALITÉS NUMÉRIQUES*, in *Optimisation et Sûreté des Systèmes*. 2011, UNIVERSITÉ DE TECHNOLOGIE DE TROYES avec L'INERIS p. 229.
11. Frédérique BICKING, C.S., Mohamed SALLAK, Jean-François AUBRY, *Aide à la conception de Systèmes Instrumentés de Sécurité par les réseaux de fiabilité de Kaufmann.* **1**(0): p. 1-6.
12. IDDIR, O., *Prinicipes d'évaluation de la probabilité de défaillance des mesures de Maitrise des Risques (MMR).* Management de la sécurité, 2009. **1**(0): p. 1-22.
13. DNV, *Etude de Dangers Module 1*. SONATRACH Activité Amont Division Production, 2010. **1**(0): p. 1-215.
14. M. Arditi, B.d.B., S. Demonet, C. Schaible, M. Sénant, *La maîtrise des risques industriels en France.* France Nature Environnement, 2014. **1**(0): p. 1-128.
15. IDDIR, O., *Mesures de mairtises des risques instrumentées (MMRI) - Etats zero et fiche de vie.* Méthode d'analyse des risques, 2014. **1**(0): p. 1-30.
16. CICCOTELLI, P.C.e.J., *Equipements de travail : sécurité des systèmes programmés.* Sécurité par secteur d'activité et par technologie, 2006. **1**(0): p. 1-23.
17. BOULANGER, J.-L., *Maitrise du SIL et gestion des certificats - Domaine ferroviaire.* Transport ferroviaire, 2011. **1**(0): p. 1-29.
18. ROYER, M., *HAZOP : une méthode d'analyse des risques - Principe.* TECHNIQUES DE L'INGÉNIEUR, 2009. **1**(0): p. 1-23.
19. ZWINGELSTEIN, G., *Sureté de fonctionnement des systèmes complexes - Prinicipaux concepts.* technique de l'ingénieur, 2009. **1**(0): p. 1-34.

20. ISO/IEC, *ISO/IEC PDGUIDE 51.2: Safety aspects — Guidelines for their inclusion in standards*. International Standardisation Organisation (ISO) et International Electrotechnical Commission (IEC), 2012. **2**(0): p. 1-23.
21. Comission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems* in *Part 4: Definitions and abbreviations*. 2010. p. 1-50.
22. KAERCHER, M., *Protection incendie des centrales nucléaires REP.* technique de l'ingénieur, 2004. **1**(0): p. 1-17.
23. ZWINGELSTEIN, G., *Evaluation de la criticité des équipements - Métriques et indicateurs de performance.* technique de l'ingénieur, 2014. **1**(0): p. 1-30.
24. IDDIR, O., *Méthode LOPA : principe et exemple d'application*. technique de l'ingénieur, 2012. **1**(0): p. 1-34.
25. ZWINGELSTEIN, G., *Sureté de fonctionnement des systèmes industriels complexes*
Analyse prévisionnelle et bases de données de fiabilite. Systèmes d'information et de communication, 2009. **1**(0): p. 1-30.
26. GIROUD, M., *Sureté de fonctionnement des systèmes - Principes et définitions.* technique de l'ingénieur, 2005. **1**(0): p. 1-22.
27. IDDIR, O., *Évaluation de la probabilité de défaillance d'un Système Instrumenté de sécurité (SIS).* Management de la sécurité, 2009. **1**(0): p. 1-16.
28. Comission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems* in *Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems*. 2010. p. 1-94.
29. Comission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems* in *Part 3: Software requirement*. 2010. p. 1-38.
30. Comission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems* in *Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*. 2010. p. 1-116.
31. Faller, R., *Project experience with IEC 61508 and its consequences.* Safety Science, 2004. **42**(5): p. 405-422.
32. Automatic, C., *Guide d'interprétation et d'application de la norme iec 61508 et des normes dérivées iec 61511 (isa s84.01) et iec 62061.* ISA - The instrumentation, Systems and Automation Society, 2005. **1**(0): p. 1-46.
33. 61511-1, I., *Functional safety – Safety instrumented systems for the process industry sector*, in *Part 1: Framework, definitions, system, hardware and software requirements* 2003, IEC Geneva, Switzerland. p. 186.
34. N.Ayault *Evaluation des barrières techniques de sécurité*. 2005.
35. E.Fal, J.L., *Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de process industriels.* INERIS 2000.
36. TOTAL, *Module SIL-GRIF*, in *GRaphique Interactifs pour la Fiablilité* 2013, Documentation technique p. 21.
37. DRANGUET, J.-M., *Evolution des normes CEI 61588 et CEI 61511-Révision des normes de la sécurité fonctionnelle IEC 61508-61511.* INERIS, 2009. **3eme rencontres en sécurité fonctionnelle** (Les évolutions Fondamentales): p. 21.
38. Charpentier, P., *Artchitecture d'automatisme en sécurité des machines : Etude des conditions de conception liées aux défaillances de mode commun*. 2002, Nancy Université, : Institut Nationnal Polytechnique de Lorraine, France

39. 62061, I., *Safety of machinery, Functional safety of electrical control systems, electronic and programmable electronic safety-related.* 2005, IEC International Electrotechnical Commission: Geneva, Switzerland. p. 69.
40. ANSI/ISA, *Application of Safety Instrumented Systems for the Process Industries*. 1996, The Instrumentation, Systems, and Automation Society: North Carolina, USA. p. 110.
41. 61511-2, I., *Functional safety – Safety instrumented systems for the process industry sector*, in *Part 2:Guidelines for the application of IEC 61511-1* 2003, IEC publisher Geneva, Switzerland. p. 168.
42. 61511-3, B.I., *Functional safety — Safety instrumented, systems for the process industry sector* in *Part 3: Guidance for the determination of the required safety integrity levels*. 2003, BSI-IEC publisher p. 56.
43. Comission, I.E., *Functional safety – Safety instrumented systems for the process industry sector* in *Part 2: Guidelines for the application of IEC 61511-1*. 2003. p. 1-8.
44. Villemeur, *Sûreté de fonctionnement des systèmes industriels - Fiabilité - Facteurs humains - Informatisation A*. 1988.
45. Chevance, R.J., *Systèmes à haute disponibilité - Concepts* 1999: Technique de l'ingénieur
46. A.C. Torres-Echeverrı, S.M., H.A. Thompson *Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing*. Reliability Engineering and System Safety 2011. **96 (2011)** 545–563.
47. IDDIR, O., *Prinicipes d'évaluation de la probabilité de défaillance des Mesures de Maitrise des Risques (MMR)*. technique de l'ingénieur, 2009. **1**(0): p. 1-22.
48. Management, S.I., *Offshore Reliability - Data Handbook*. OREDA, 2002. **1**(0): p. 1-835.

Annexes

Annexe 1 : Exemple de matrice de gravité

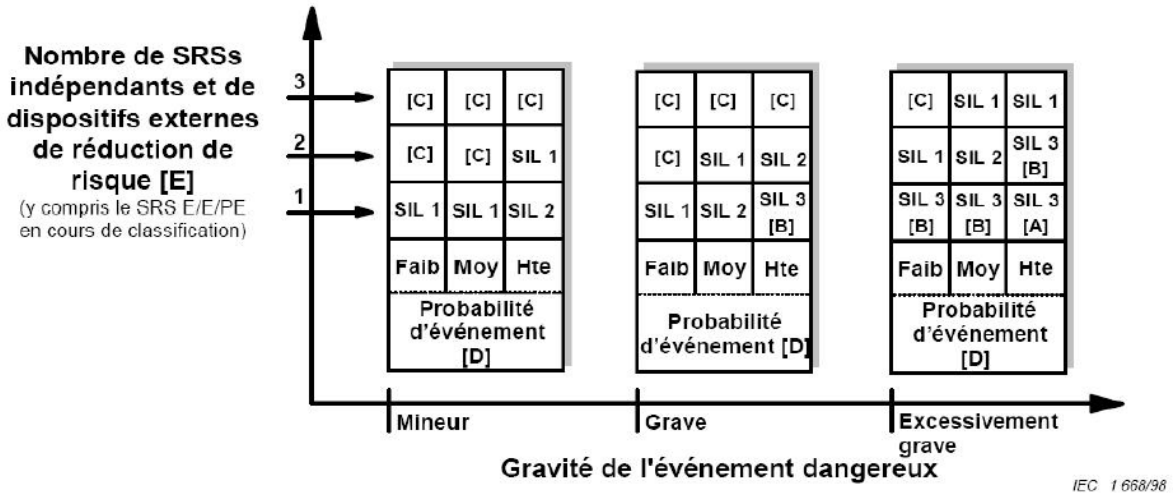


Figure - Exemple de matrice de gravité [5]

Avec :

[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.

Annexe 2 : Exemple d'un tableau de la méthode LOPA

Tableau. - Exemple de tableau LOPA [4]

#	1	2	3	4		5		6	7	8	9	10	11
					PROTECTION LAYERS								
	Impact event description F.3 F.14.1	Severity level F.4 F.14.1	Initiating cause F.5 F.14.2	Initiation likelihood F.6 F.14.3	General process design F.14.4	BPCS F.14.5	Alarms, etc. F.14.6	Additional mitigation, restricted access,F.8 F.14.7	IPL additional mitigation dikes, pressure relief F.9 F.14.8	Inter-mediate event likelihood F.10 F.14.9	SIF integrity level F.11 F.14.10	Mitigated event likelihood F.12 F.14.10	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0,1	0,1	0,1	0,1	0,1	PRV 01	10^{-7}	10^{-2}	10^{-9}	High pressure causes column rupture
2	Fire from distillation column rupture	S	Steam control loop failure	0,1	0,1		0,1	01	PRV 01	10^{-6}	10^{-2}	10^{-8}	Same as above
N													

IEC 3025/02

NOTE Severity Level E = Extensive; S = Serious; M = Minor.

Likelihood values are events per year, other numerical values are probabilities of failure on demand average.

Annexe 3 : Cycle de vie de la sécurité : Systèmes E/E/EP

Tableau - Cycle de vie de la sécurité : Systèmes E/E/EP [28]

Phase ou activité du cycle de vie en sécurité	**Objectifs**	**Données**	**Résultats**
Analyse des risques et conception des couches de protection.	Identification des dangers et des événements dangereux liés au procédé et aux équipements associés, de la séquence d'événements conduisant à un événement dangereux, des risques du procédé associés à l'événement dangereux, des exigences de réduction des risques et des fonctions instrumentées de sécurité requises pour assurer la réduction des risques nécessaire.	Conception du procédé, architecture et organisation humaine.	Description des fonctions instrumentées de sécurité requises et des exigences d'intégrité de sécurité associées.
Affectation des fonctions de sécurité aux couches de protection.	Allocation des fonctions de sécurité aux Couches de protection et pour chaque fonction instrumentée de sécurité, spécification du niveau d'intégrité de sécurité associé.	Description des fonctions instrumentées de sécurité et des exigences d'intégrité de sécurité associées.	Description de l'affectation des exigences de sécurité.
Spécification des exigences de sécurité du SIS.	Spécification des exigences pour chaque SIS, en termes de fonctions instrumentées de sécurité requises et de leur intégrité de sécurité associée, en vue d'assurer une sécurité fonctionnelle appropriée.	Description de l'affectation des exigences de sécurité.	Exigences de sécurité du SIS. Exigences de sécurité du logiciel.
Conception et réalisation du SIS.	Conception du SIS de façon à satisfaire aux exigences concernant les fonctions instrumentées de sécurité et l'intégrité de sécurité.	Exigences de sécurité du SIS. Exigences de Sécurité du logiciel.	Conception du SIS en conformité avec ses exigences de sécurité. Planification des essais d'intégration du SIS.

Installation, mise en service et validation du SIS	Intégration et test du SIS. Validation du fait que le SIS satisfait en tous points les exigences de sécurité en termes de fonctions instrumentées de sécurité et d'intégrité de sécurité.	Conception du SIS. Plan des tests d'intégration du SIS. Exigences de sécurité du SIS. Plan de validation de sécurité du SIS.	SIS en complet état de marche en conformité avec les modifications de conception résultant des tests d'intégration. Validation de la sécurité du SIS. Plan de validation du SIS.
Exploitation et maintenance du SIS.	Vérification du fait que la sécurité Fonctionnelle du SIS est maintenue pendant l'exploitation et la maintenance.	Exigences concernant le SIS. Conception du SIS. Exploitation et maintenance du SIS.	Exploitation et maintenance du SIS.
Modification du SIS.	Réalisation des corrections, améliorations ou adaptations du SIS qui assurent l'obtention et le maintien du niveau d'intégrité de sécurité requis.	Exigences de sécurité du SIS révisées.	Résultats de la modification du SIS.
Retrait de service.	Mise en place d'une procédure de revue, d'une organisation adéquate, et garantie que les SIF restent adéquates.	Exigences de Sécurité du système « à la construction » et documentation du procédé.	SIF démantelé.
Vérification du SIS	Test et évaluation des résultats d'une phase pour s'assurer de leur exactitude et de leur cohérence par rapport aux produits et normes fournis comme données pour cette phase.	Plan de vérification du SIS pour chaque phase.	Résultats de la Vérification du SIS pour chaque phase.
Evaluation de la sécurité fonctionnelle du SIS.	Analyse et appréciation de la sécurité fonctionnelle réalisée par le SIS.	Plan d'évaluation de la sécurité Fonctionnelle du SIS. Exigences de Sécurité du SIS	Résultats de l'évaluation de la sécurité fonctionnelle du SIS.

Annexe 4 : Notation générale relative au calcul des probabilités

La liste [10] suivante représente les natations utilisées dans la prochaine partie relative aux formules de calcul des PFD, plusieurs de ces notations sont représentés sur la figure 3.3 :

Moon Architecture du système, avec $M \leq N$

$\boldsymbol{\lambda}$ Taux de défaillance de chacun des éléments du système.

$\boldsymbol{A_e(t)}$ Disponibilité de chacun des éléments du système au temps t, c'est-à-dire la probabilité que l'élément soit capable d'accomplir la fonction de sécurité au temps t.

$\boldsymbol{A(t)}$ Disponibilité du système au temps t, c'est-à-dire la probabilité que le système soit capable d'accomplir la fonction de sécurité au temps t

$\boldsymbol{U(t)}$ Indisponibilité du système au temps t, i.e. $U(t) = 1 - A(t)$

$\boldsymbol{t_i}$ Instant d'exécution du $i^{ème}$ test de révision (qui peut être partiel ou complet), avec la condition initiale $t_0 = 0$ qui est assimilée à l'exécution du dernier test complet

$\boldsymbol{T_i}$ Intervalle de temps entre le $(i-1)^{ème}$ et le $i^{ème}$ test de révision, i.e. $Ti = ti - ti\text{-}1$

$\boldsymbol{E}$ Efficacité des tests partiels, c'est-à-dire qu'une proportion égale à E du taux de défaillance de chacun des éléments du système correspond à des défaillances qui sont détectées lors de n'importe quel test partiel.

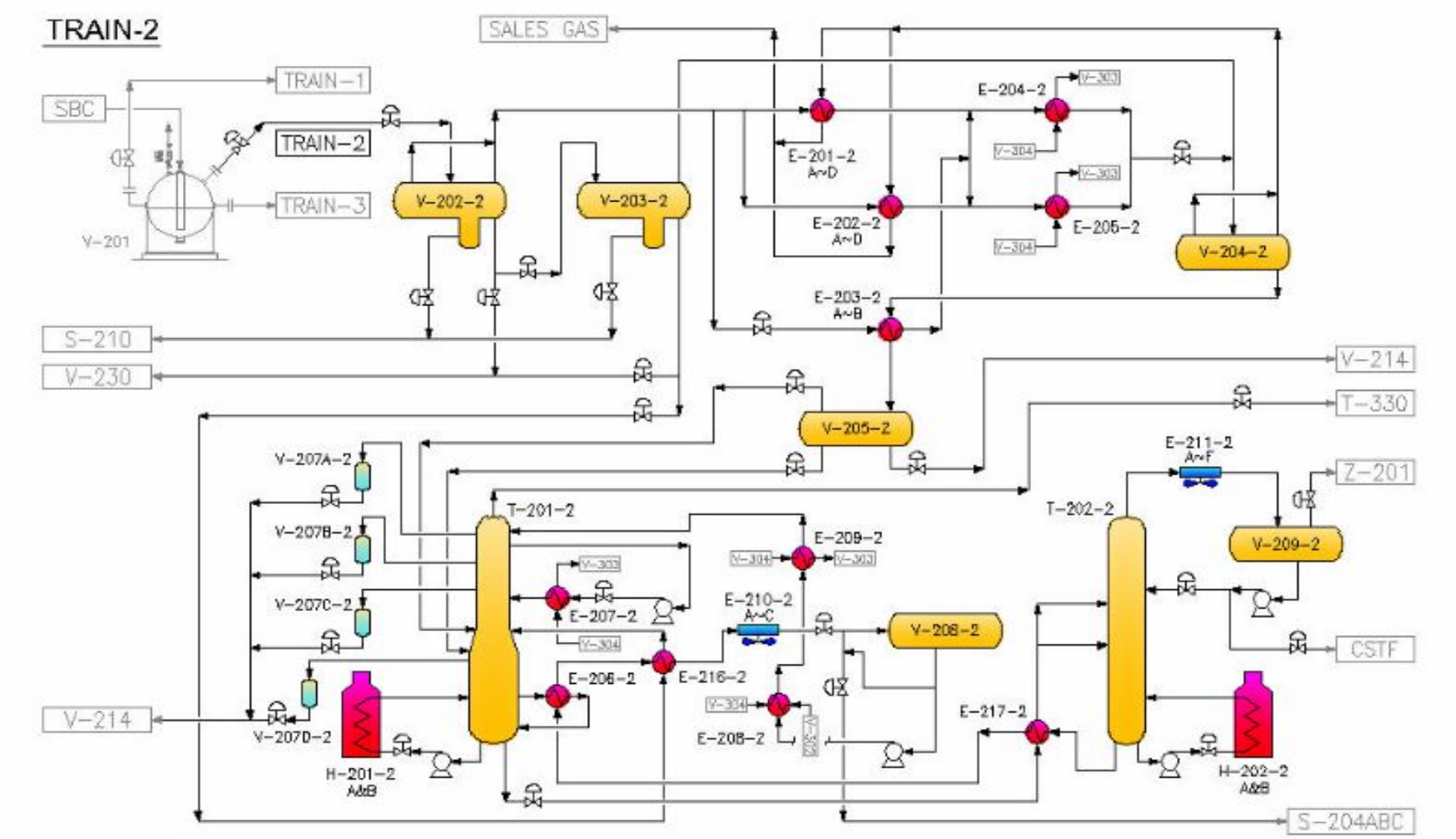
$\boldsymbol{N}$ Nombre total de tests dans un intervalle de temps entre deux tests complets, c'est à dire qu'il y a $(n-1)$ tests partiels, plus le $n^{ème}$ test qui est complet.

$\boldsymbol{T}$ Intervalle de temps entre deux tests complets, i.e. $\tau = t_n$

$\boldsymbol{Obs_i}$ Probabilité de détecter une défaillance lors du $i^{ème}$ test de révision de chaque élément du système.

$\boldsymbol{K}$ Nombre total (équivalent) d'éléments du système qui ont été révisés (avec ou sans détection de défaillance, et suivi ou non d'actions de maintenance) lors du i test de révision.

Annexe 5 : Processus de traitement de gaz Train 1, Module 1 (MPP1), DP, HRM, SH



Annexe 6 : Etude HAZOP

Causes	Acc	Conséquences	G	P	CR	CAT	Préventions	G	P	CR	Cat.	Protection	G	P	CR	Cat.	Recommandations	G	P	CR	CAT
8. Vanne FV33 sortie fond de colonne vers T202 bloquée fermée (défaillance de la boucle de régulation)		1. Montée en niveau du fond de la colonne T201 jusqu'à l'arrivée de condensat à partir du four H201					1. Maintenance des équipements/instruments	G4	P3			1. TAH211 alarme haute T°zone de radiation					53. Etudier la possibilité d'installer un système de vidange automatique du four H201 (système vide-vite)				
		2. Surremplissage de la colonne avec					2. FICAL201 agit sur la FV201					2. TAHH281 alarme haute T°zone de									
		détérioration des plateaux de la T201					(ouverture)					radiation qui arrête le four									
		3. Réduction du débit d'arrivée de condensat à partir du four H201 avec montée en T° du pot sortie des tubes condensat du four.					3. FICAL201 alarme bas débit refoulement des pompes P201A/B/C					3. TAHH271 alarme haute T° cheminée qui arrête									
		4. Rupture des tubes du four H201 avec risque d'explosion/d'incendie du four					4. FALL201 alarme bas débit refoulement des pompes P201A/B/C qui arrête le four (fermeture des vannes brûleurs d'alimentation en fuel gaz)	G4	P2			4. Clapet anti-retour ligne d'alimentation en condensat depuis le four H201									
		5. Fatalités	G4	P4			5. PAH231 alarme haute pression sortie four H201					5. Arrêt d'urgence de l'unité avec décompression et vidange	G3	P1							
		6. Pollution environnementale	G3	P4			6. PAHH231 alarme très haute pression sortie condensat four qui arrête le four	G4	P1			6. Rideau d'eau activé par l'opérateur à partir de la salle de contrôle									
							7. TICAH231 qui agit sur la FCV271 vanne d'alimentation fuel gaz du four H201	G4	P1			7. Vidange rapide du four activée localement par l'opérateur	G2	P1							

Causes	Acc	Conséquences	G	P	CR	CAT	Préventions	G	P	CR	Cat.	Protection	G	P	CR	Cat.	Recommandations	G	P	CR	CAT
							via la FICAH271														
							8. TICAH231 alarme haute T° sortie condensat four					8. Système d'inertage à l'azote									
							9. TAH211 alarme haute T°zone de radiation du four H201					9. Four équipé par des trappes de surpression en cas d'explosion interne									
							10. TAHH231 alarme très haute T°sortie condensat four qui arrête le four					10. Moyens d'extinction mobiles et fixes									
							11. TAHH221:1-10 alarme haute T° pots des tubes	G4	P1			11. POI									
							12. PSV201 sortie four H201 vers colonne T201														
9. Vanne FV201 fermée refoulement pompe P201A/B/C (défaillance de la boucle de régulation)		1. Montée en niveau du fond de la colonne T201 jusqu'à l'arrivée de condensat à partir du four H201					1. Maintenance des équipements/instruments	G4	P3			1. TAH211 alarme haute T°zone de radiation					54. Etudier (ou vérifier) la possibilité d'équiper la vanne FV201 d'un indicateur de position limite switch ouverture/fermeture avec report en salle de contrôle avec coupure de la pompe P201A/B/C				
		2. Surchauffe de la pompe P201A/B/C avec défaillance et fuite vers					2. FALL201 alarme bas débit refoulement des	G4	P2			2. TAHH281 alarme haute T°zone de radiation qui arrête					59. Fiabiliser le système d'inertage à l'azote du four H201 (azote provenant des				

Causes	Acc	Conséquences	G	P	CR	CAT	Préventions	G	P	CR	Cat.	Protection	G	P	CR	Cat.	Recommandations	G	P	CR	CAT
		l'extérieur					pompes P201A/B/C qui arrête le four (fermeture des vannes brûleurs d'alimentation en fuel gaz)					le four					communs)				
		3. risque d'incendie et d'explosion					3. TICAH231 qui agit sur la FCV271 vanne d'alimentation fuel gaz du four H201 via la FICAH271	G 4	P 1			3. TAHH271 alarme haute T°cheminée qui arrête									
		4. Fatalités	G 4	P 4			4. TICAH231 alarme haute T° sortie condensat four					4. Clapet anti-retour ligne d'alimentation en condensat depuis le four H201									
		5. Surremplissage de la colonne avec détérioration des plateaux de la T201					5. TAH211 alarme haute T°zone de radiation du four H201					5. Arrêt d'urgence de l'unité avec décompression et vidange									
		6. Réduction du débit d'arrivée de condensat à partir du four H201 avec montée en T° du pot sortie des tubes condensat du four.					6. TAHH231 alarme très haute T°sortie condensat four qui arrête le four					6. Rideau d'eau activé par l'opérateur à partir de la salle de contrôle									
		7. Rupture des tubes du four H201 avec risque d'explosion/d'incendie du four					7. TAHH221:1-10 alarme haute T° pots des tubes					7. Vidange rapide du four activée localement par l'opérateur									

Causes	Acc	Conséquences	G	P	CR	CAT	Préventions	G	P	CR	Cat.	Protection	G	P	CR	Cat.	Recommandations	G	P	CR	CAT
14. Vanne SOV241/251 bloquée fermée ligne alimentation gaz pilote four H201 (perte d'utilité)		1. Extinction de la flamme pilote					1. Maintenance préventive des équipements/Instruments	G4	P2			1. Tournées des opérateurs									
		2. Envoi de gaz côté brûleurs à travers les vannes manuelles dans l'enceinte du four en cas de soufflage de la flamme brûleurs					2. Détecteur de flamme BAL201 au niveau de chaque pilote qui arrête l'alimentation en fuel gaz côté brûleurs avec alarme en salle de contrôle	G4	P1			2. Ouverture des trappes de surpression du four H201	G3	P1							
		3. Risque d'explosion interne du four H201 en cas d'ignition					3. Procédure de redémarrage du four H201 qui exige la purge du four					3. Moyens d'extinction mobiles et fixes									
		4. Projection de missiles										4. Arrêt d'urgence du train avec isolement, décompression et vidange	G2	P1							

Causes	Acc	Conséquences	G	P	CR	CAT	Préventions	G	P	CR	Cat.	Protection	G	P	CR	Cat.	Recommandations	G	P	CR	CAT
		5. Fatalités	G4	P3								5. POI									
		6. Pollution environnementale	G3	P3																	
15. Vanne SOV211 bloquée fermée ligne alimentation fuel gaz brûleur four H201 (perte d'utilité)		1. Extinction de la flamme brûleur					1. Maintenance préventive des équipements/Instruments	G4	P2			1. Tournées des opérateurs					58. Etudier la possibilité de ramener la position des vannes SOV211, 221, 231 en ouverture/fermeture en salle de contrôle				
		2. Dérive du process par chute de T°dans le four					2. PALL201 qui ferme la vanne SOV221 et envoi décomprime le tronçon SOV211-221 vers torche					2. Ouverture des trappes de surpression du four H201	G3	P1							
		3. Pas de conséquences HSE										3. Moyens d'extinction mobiles et fixes									
												4. Arrêt d'urgence du train avec isolement, décompression et vidange	G2	P1							
												5. POI									
16. Vanne LV13 sortie ballon eau glycol V207D fermée par défaillance de la boucle de régulation de niveau (cas représentatif des ballons glycol)		1. Montée de niveau dans le ballon V207D avec passage d'eau glycolée vers le fond de la colonne.					1. Maintenance préventive des équipements/Instruments	G4	P2			1. TAH211 alarme haute T°zone de radiation									
		2. Entraînement de glycol dans les tubes du four H201 avec formation de dépôts					2. Inspection périodique des tubes du four					2. TAHH281 alarme haute T°zone de radiation qui arrête									

Annexe 7 : Fichier (m. file) approximation polynomiale

```
%Insertion des données
xdata=[0 1314 2628 3942 4380 5256 6570 7884 8760 9198 10512 11826 13140
14454 15768 17082 17520 18396 19710 21024 21900 22338 23652 24966 26279
26280 26280 27594 28908 30222 30660 31536 32850 34164 35040 35478 36792
38106 39420 40734 42048 43362 43800 44676 45990 47304 48180 48618 49932
51246 52559 52560 52560 53874 55188 56502 56940 57816 59130 60444 61320
61758 63072 64386 65700 67014 68328 69642 70080 70956 72270 73584 74460
74898 76212 77526 78839 78840 78840 80154 81468 82782 83220 84096 85410
86724 87599 87600 87600 87602 87603 87603 87653 87703 87753 87803 87853
87903 87953 88003 88038 88053 88103 88153 88203 88253 88303 88353 88403
88453 88503 88553 89352 90666 91980 91982 93294 94608 95922 96362 97236
98550 99864 100742 101178 102492 103806 105119 105120 105120 105122 106434
107748 109062 109502 110376 111690 113004 113882 114318 115632 116946
118260 118261 119574 120888 122202 122641 123516 124830 126144 127021
127458 128772 130086 131399 131400 131400 131401 132714 134028 135342
135781 136656 137970 139284 140161 140598 141912 143226 144540 144541
145854 147168 148482 148920 149796 151110 152424 153300 153738 155052
156366 157679 157680 157680 157680 158556 159432 160308 161184 162060
162060 162936 163812 164688 165564 166440 166440 167316 168192 169068
169944 170820 170820 171696 172572 173448 174324 175199 175200 175200];
ydata=[0.00000 0.00005 0.00010 0.00015 0.00017 0.00021 0.00027 0.00033
0.00037 0.00039 0.00045 0.00052 0.00059 0.00066 0.00073 0.00080 0.00083
0.00088 0.00096 0.00104 0.00109 0.00112 0.00120 0.00129 0.00137 0.00137
0.00137 0.00140 0.00143 0.00147 0.00148 0.00150 0.00154 0.00158 0.00161
0.00162 0.00166 0.00171 0.00176 0.00181 0.00186 0.00191 0.00193 0.00197
0.00203 0.00209 0.00213 0.00215 0.00221 0.00228 0.00235 0.00235 0.00235
0.00238 0.00242 0.00246 0.00248 0.00250 0.00254 0.00259 0.00262 0.00263
0.00267 0.00272 0.00277 0.00282 0.00286 0.00292 0.00293 0.00297 0.00302
0.00308 0.00311 0.00313 0.00319 0.00325 0.00331 0.00331 0.00331 0.00335
0.00339 0.00344 0.00345 0.00348 0.00352 0.00357 0.00360 0.00360 0.00360
0.00363 0.00363 0.00363 0.00363 0.00363 0.00363 0.00363 0.00362 0.00362
0.00362 0.00362 0.00362 0.00362 0.00361 0.00361 0.00361 0.00361 0.00361
0.00360 0.00360 0.00360 0.00360 0.00360 0.00357 0.00352 0.00348 0.00348
0.00344 0.00341 0.00338 0.00337 0.00335 0.00333 0.00330 0.00329 0.00328
0.00327 0.00326 0.00325 0.00325 0.00325 0.00325 0.00322 0.00320 0.00318
0.00318 0.00317 0.00315 0.00314 0.00313 0.00313 0.00312 0.00311 0.00310
0.00310 0.00310 0.00310 0.00310 0.00310 0.00310 0.00310 0.00311 0.00311
0.00311 0.00312 0.00313 0.00314 0.00314 0.00314 0.00314 0.00315 0.00315
0.00315 0.00315 0.00316 0.00316 0.00317 0.00318 0.00318 0.00319 0.00320
0.00321 0.00321 0.00322 0.00324 0.00325 0.00326 0.00327 0.00329 0.00331
0.00332 0.00333 0.00335 0.00337 0.00340 0.00340 0.00340 0.00340 0.00341
0.00342 0.00343 0.00344 0.00345 0.00345 0.00346 0.00348 0.00349 0.00350
0.00351 0.00351 0.00353 0.00354 0.00355 0.00357 0.00358 0.00358 0.00360
0.00361 0.00363 0.00365 0.00366 0.00366 0.00366];
%Utilisation de la fonction Polyfit
fprintf('Methode polyfit')
P=polyfit(xdata,ydata,2)
%Définition de la fonction d' approximation avec Polyfit
H=@(x)+P(1)*x.^2 + P(2)*x + P(3);
fprintf('*** fonction d''approximation avec Polyfit ***')
fprintf('\n')
fprintf('H(x) = %d * x.^2 + %d * x + %d ',P(1),P(2),P(3))
fprintf('\n')
%Utilisation de la fonction lsqcurvefit
fprintf('\n')
fprintf('Methode lsqcurvefit')
x0=[2000;100;10];
[O,resnorm]=lsqcurvefit(@PFDEquationfunc,x0,xdata,ydata)
%Définition de la fonction d'approximation avec lsqcuvefit
```

```
G=@(x)O(1)*x.^2 + O(2)*x + O(3);
fprintf('*** fonction d''approximation avec lsqcuvefit ***')
fprintf('\n')
fprintf('G(x) = %d * x.^2 + %d * x + %d ',O(1),O(2),O(3))
fprintf('\n')
%Insertion des courbes
I=min(xdata):1000:max(xdata);
M=min(xdata):1:max(xdata);
plot(xdata,ydata,'b',I,G(I),'r',M,H(M),'g')
grid
xlabel('Temps (heure)')
ylabel('PFDavg')
title('Evolution de la PFDavg en fonction du Temps')
legend('standard','polyfit','lsqcurvefit')
```

Annexe 8 : Fichier (.m file) Calcul du maximum de la fonction F(x)

```
      clc
%Definition des variables
syms x
%Definition de la fonction F
F = @(x) -2.132926e-13 * x^2 + 5.497704e-08 * x + 3.193612e-05
%Determination du max de la fonction
H=solve(diff(F(x)))
%calcul de la PFD
PFD=F(H)
```