N° Ordre……../Faculté/UMBB/2016

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté des Hydrocarbures et de la Chimie

Mémoire de Fin d'Etudes
En vue de l'obtention du diplôme :

MASTER

Présenté par

HADJAZ Fatma

Filière : Automatisation des procédés industriels
Option : Commande automatique

Thème

Systèmes Automatiques de sécurité dans les procédés industriels. Mise en œuvre sur un four industriel par API Triconex.

Devant le jury :

Dr A. CHAIB	FHC	Président
M. Kesseraoui	FHC	Examinateur
A. BENHALLA	FHC	Encadreur

Année Universitaire : 2015/2016

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté des Hydrocarbures et de la Chimie
Département : Automatisation
Filière : Automatisation des procédés industriels
Option : Commande automatique

Mémoire de Fin d'Etudes
En vue de l'obtention du diplôme :

MASTER

Thème

Systèmes Automatiques de sécurité dans les procédés industriels. Mise en œuvre sur un four industriel par API Triconex.

Présenté par :
Etudiante : HADJAZ Fatma

Avis favorable de l'encadreur :
A. BENHALLA

Avis favorable du Président du jury
Nom Prénom **Signature**

Cachet et signature

REMERCIEMENT

Je tiens à remercier Mon enseignant et promoteur Monsieur A. BENHALLA pour m'avoir donné l'opportunité de travailler sur ce sujet, pour ses encouragements, ses précieux conseils et qu'il sache que sa disponibilité, sa serviabilité et sa générosité ont été grandement appréciées.

Je remercie tous les enseignants du département Automatisation, et de l'université de Boumerdès d'une façon plus générale qui ont contribué à ma formation et m'ont fait bénéficier de leur savoir.

Je voudrais également remercier mes camarades du groupe MACA11 avec qui j'ai passé d'agréables années.

Enfin, mes profonds remerciements vont à mes très chers parents pour le soutien et les encouragements qu'ils m'ont prodigués tout au long de mes années d'étude.

A mes très chers parents

A mes trois frères

A mes trois sœurs

A mes neveux

A mes nièces

A tous mes ami(e)s

Je dédie ce modeste travail.

Table des matières

Chapitre II. Système de contrôle et Système de sécurité

Chapitre III. Evaluation des SIL d'un système opérationnel : Four rebouilleur

Liste des figures

Liste des tableaux

Acronymes

BPCS Basic Process Control and safety (Système de commande de processus de base).

CP Processeur de contrôle (Control Processor).

DC Diagnostic coverage (couverture de diagnostic).

DCS Distributed Controller System.

DNBI Dual NodeBus Interface.

E/E/PE Electriques/Electroniques/Electroniques Programmables de sécurité.

EUC Equipement Under Control (Équipement sous-control).

ESD Emergency Shut Down (système d'arrêt d'urgence).

FAL Flow Alarm Low (Alarme de Bas Débit).

FALL Flow Alarm Low Low (Alarme de Très Bas Débit).

FV Flow Valve (Vane de Débit).

FBD Field Bus Module.

FBI Field Bus Interface.

FT Flow Transmitter (Transmetteur de Débit).

HMI Humain-Machine Interface (Interface Humain-Machine).

IEC International Electrotechnical Comission (Commission International d'Electronique).

ISA International Society of Automation (Société Internationale d'Automatisation).

ISO International Organization for Standardization.

MTTR Mean Time To Restoration (Durée Moyenne de Réparation).

PAHH/LL Pressure Alarm High High/Low Low (Alarme de Très Haute /Très Bas Pression).

PAH Pressure Alarm High (Alarme de Haute Pression).

PAL Pressure Alarm Low (Alarme de Bas Pression).

PFD Probability of Failure on Demand (Probabilité de Défaillance à la Demande).

PFH Probability of Failure per Hour (Probabilité de Défaillance par Heure).

PFDavg Average Probability of Failure on Demand (Probabilité de Défaillance moyenne à la Demande).

PLC Programmable Logic Controller (Automate Programmable Industriel).

PSH/L Pressure Switch High/Low (switch de Pression Haute/Bas).

RR Risk Reduction (Réduction de risque).

SIS Safety Instrumented System (Système Instrumenté de Sécurité).

SIF Safety Instrumented Function (Fonction Instrumenté de Sécurité)

.

SIL Safety Integrity Level (Niveau d'Intégrité de Sécurité).

TAH Temperature Alarm High (Alarme de Haute Température).

TAHH Temperature Alarm High High (Alarme de Très Haute Température).

TV Temperature Valve (Vanne de Température).

$\mathbf{T_1}$ Proof-test interval (Interval de Proof Test).

ß Proportion de défaillance de cause commune non détectées.

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.

Glossaire

Sécurité

L’absence de danger ou de risque inacceptable.

Système

Ensemble d’éléments qui interagissent selon un modèle précis, un élément pouvant être un autre système, appelé sous-système, les sous-systèmes pouvant être eux-mêmes soit un système de commande soit un système commandé composé de matériel, de logiciel en interaction avec l’être humain.

Sous-système

Ensemble de modules (automate programmable par exemple). Selon la norme CEI 61508, un élément d'un système peut-être un autre système appelé dans ce cas sous système. Les sous-systèmes peuvent être eux-mêmes soit un système de commande, soit un Système commandé composé de matériel et de logiciel en interaction avec l'être humain.

Norme

Règle élaborée pour satisfaire un besoin commun, basée sur des spécifications techniques mesurables.

Module

Ensemble fonctionnel de composants encapsulés formant un tout (circuit d'entrée ou de sortie, carte électronique).

Composant

La plus petite partie d'un module, d'un sous-système ou d’un système qu'il est nécessaire et suffisant de considérer pour l'analyse du système

Architecture

Configuration spécifique des éléments matériels et logiciels dans un système.

Canal

Elément ou groupe d’éléments exécutant une fonction indépendante.

Redondance

Existence de plus de moyens que strictement nécessaire pour accomplir une fonction requise dans une unité fonctionnelle ou pour représenter des informations par des données.

Disponibilité

La disponibilité est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données.

Défaillance

Cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise.

Défaillance dangereuse

Défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

Système de Contrôle de Procédé de Base (BPCS)

Système qui répond aux signaux d'entrée du procédé, des équipements associés et /ou d'un opérateur et génère des signaux de sortie provoquant le fonctionnement souhaité du procédé et de ses équipements associés.

Système Instrumenté de Sécurité (SIS)

Implémentation d'une ou plusieurs fonctions instrumentées de sécurité. Un SIS est composé de n'importe quelle combinaison de capteurs, solver logiques et élément finaux. Un SIS comporte généralement un certain nombre de fonctions de sécurité ayant différents niveaux d'intégrité de sécurité.

Intégrité de sécurité

Probabilité pour qu'un système relatifs à la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps spécifiée.

Niveau d'Intégrité de Sécurité (SIL)

Niveau discret (parmi 4 possibles) permettant de spécifier les prescriptions concernant l'intégrité des fonctions à allouer aux systèmes E/E/EP relatifs à la sécurité. Le niveau 4 est le plus élevé ; le niveau 1 le plus bas.

Fonction Instrumenté de Sécurité (SIF)

Ensemble d'équipements visant à réduire le risque dû à un danger spécifique (une boucle de sécurité). Elle inclut les éléments qui détectent l'imminence d'un accident, décident d'agir, puis exécutent l'action nécessaire afin d'amener le procédé dans un état de sécurité.

Sécurité Fonctionnelle

Un sous ensemble de la sécurité globale qui dépend du bon fonctionnement d'un système ou d'un équipement en réponse à ses entrées.

Comité Électrotechnique Internationale (IEC)

Organisation mondiale de normalisation composée de l'ensemble de comités nationaux. Elle a pour objet de favoriser la coopération internationale pour toutes nationaux. Elle a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et l'électronique.

Automate Programmable Industriel (PLC)

Dispositif électronique programmable destiné à la commande des procédés industriels à l'aide d'un traitement programmé. Il contient des modules d'entrée /sortie au moyen desquels il est relié aux capteurs et aux actionneurs industriels.

Interface Homme-Machine (HMI)

Interface de commande et de supervision offrant à l'opérateur une représentation visuelle du procédé et des moyens de contrôle, de surveillance et de diagnostic.

Couverture de diagnostic

Fraction exprimant la décroissance de la probabilité de défaillance dangereuse du matériel résultant du fonctionnement des tests de diagnostic automatique.

Taux de défaillance λ(t)

C’est la probabilité pour que le système soit défaillant Cette définition s’applique pour tout type d’éléments (système, sous-système, module, Composant).

Taux de défaillance dangereuse $\lambda_D(t)$

C’est la probabilité que le système soit défaillant de telle sorte qu’il soit incapable d’exécuter la fonction de sécurité attendue.

Probabilité de défaillance sur demande PFD (t) (Probability Failure on Demand)

C'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. C’est un nombre sans dimension.

Probabilité moyenne de défaillance sur demande PFDavg (Average of the probability failure on demand)

C'est la valeur moyenne par rapport à l'intervalle de temps entre proof test (test fonctionnel) de la probabilité de défaillance sur demande. Cette grandeur s'utilise dans le cas des systèmes à faible sollicitation et c’est un nombre sans dimension.

MTTR (Mean Time To Repair)

C’est le taux moyen mis pour réparer le système.

Introduction générale

Les industries se préoccupent non seulement des performances des systèmes en terme de qualité, de productivité et de rentabilité mais aussi en terme de sécurité.

L'installation en sécurité peut comporter plusieurs moyens pour réduire les risques. La conception du procédé, le choix de dispositif et d'équipements de l'installation font partie de ces moyens. L'action sur les systèmes de commande de base de processus (BPCS), qui sont conçus pour surveiller, contrôler et maintenir le process dans un état de fonctionnement normal et sûr, et qui sont employés pour optimiser les conditions de conduite de procédé afin de maximiser la qualité et la production, peut aussi contribuer à réduire les risques. Ces actions restent parfois insuffisantes et il faut réduire encore le risque à un niveau acceptable.

Des systèmes spécifiques appelés systèmes instrumentés de sécurités (SIS) sont introduits pour répondre à ce besoin et intervenir dans le cas où le process se trouve dans des situations dangereuses de fonctionnement tout en garantissant la protection, des personnes, des équipements et de l'environnement.

Les systèmes instrumentés de sécurité sont utilisés pour exécuter des fonctions de sécurité, ils sont aussi appelés boucles de sécurité et ils comprennent tous les matériels, logiciels et équipements nécessaires pour obtenir la fonction de sécurité désirée. Ils ont pour objectif de mettre le procédé en position de repli de sécurité lorsqu'il évolue vers une voie comportant un risque réel (explosion, feu, etc.), c'est-à-dire vers un état stable ne présentant pas de risque pour les personnes, l'environnement ou les biens. Les normes IEC 61508 [IEC61508 98] et IEC 61511 [IEC61511 00] ont établi les prescriptions relatives à la spécification, l'exploitation et la maintenance de ces systèmes.
La norme CEI 61508 est une norme multisectorielle traitant de l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP tandis que la norme CEI 61511 est une déclinaison orientée vers les industries des procédés. Ces deux normes définissent les niveaux d'intégrité de sécurité (SIL, Safety Integrity Levels) et fixent le niveau de réduction du risque que doit atteindre le SIS. Il existe 4 niveaux possibles, notés SIL1 à SIL4. Ces deux normes de sécurité fonctionnelle introduisent une approche probabiliste pour l'évaluation quantitative de la performance du système instrumenté de sécurité. Elles définissent un critère important pour caractériser les SIS : la probabilité moyenne de défaillance sur demande

(PFDavg : Average Probability of Failure on Demand) pour les SIS faiblement sollicités (moins d'une sollicitation par an) et la probabilité de défaillance par heure (PFH : Probability of Failure per Hour) pour les SIS fortement sollicités.

L'évaluation du niveau d'intégrité de sécurité est déterminée par des méthodes qualitatives et quantitatives [SAL 06b], [SAL 08]. Parmi les méthodes quantitatives les plus utilisées pour déterminer le niveau de SIL d'une SIF, la méthode des équations simplifiées est décrite dans la partie 5 de la norme IEC 61508 [IEC 61508 98].

Le premier chapitre est dédié aux systèmes instrumentés de sécurité (SIS). Un tour d'horizon est effectué décrivant les normes de sécurité relatives aux SIS. La norme CEI 61508 est la norme générique et dispose 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 que au développement des méthodes d'évaluation de SIL en s'intéressant particulièrement à la méthode des équations simplifiées.

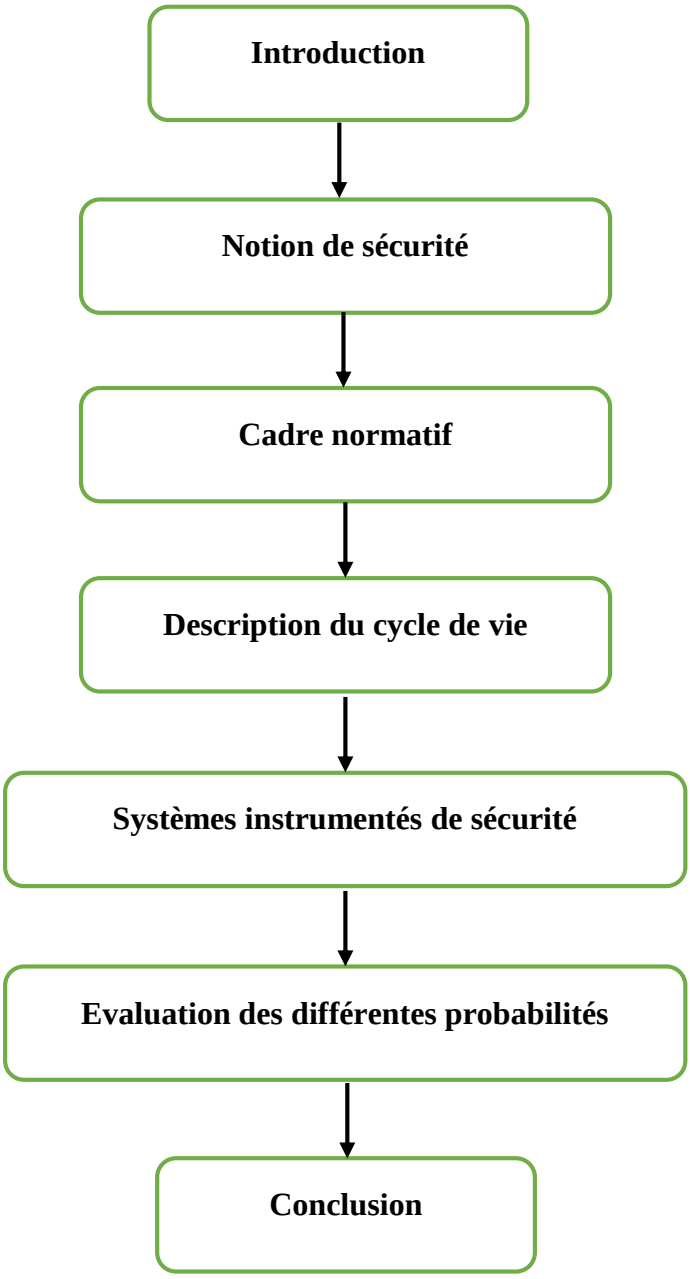
Dans le second chapitre, on présentera les moyens utilisés pour assurer le contrôle-commande (DCS) et la sécurité (APIdS) d'un four industriel dans une installation pétrolière. Le concept d'intégration des systèmes de sécurité (SIS) et de contrôle (BPCS), les différentes architectures existantes et de mettre en relief les différences existantes entre ces systèmes dans la conception et la fonctionnalité.

Enfin, on finira par l'évaluation de la performance des systèmes instrumentés de sécurité d'un four rebouilleur où les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation, etc.) sont des valeurs pouvant être connues et validées par retour d'expérience.

Ce travail de mémoire sera clôturé par une conclusion générale résumant le travail accompli.

CHAPITRE I

SYSTEME INSTRUMENTE DE SECURITE



I.1. Introduction

Généralement les systèmes industriels présentent des risques pour les personnes, équipements et l'environnement, diverses sécurités doivent être mises en œuvre. Ces types de sécurité utilisent des moyens contribuant soit à la prévention soit à la protection pour réduire les risques de dysfonctionnement. Les Systèmes Instrumentés de Sécurité (SIS) sont utilisés comme moyens de sécurité pour réaliser des Fonctions Instrumentées de Sécurité (SIF) afin de mettre le procédé dans un état de repli de sécurité si le processus se trouve dans des conditions dangereuses de fonctionnement. La Commission Internationale d'Electronique (CEI), ou "International Electrotechnical Commission" (IEC), a normalisé les systèmes de sécurité ; Norme IEC 61508 en 1998 [IEC61508 98] et IEC 61511 en 2000 [IEC61511 00]. [MEC 11].
L'objet de ce chapitre est de donner dans un premier temps une définition de certains termes et concepts utilisés dans le cadre de la sécurité fonctionnelle des systèmes de sécurité.
Par la suite, un aperçu sur les principales normes de sécurité utilisées pour concevoir les SIS est donné. La définition des SIS est détaillée. La dernière partie s'intéresse aux différentes méthodes, citées par les normes de sécurité et utilisées pour déterminer les niveaux SIL des SIS.

I.2. Notion de sécurité

Suivant le guide ISO/CEI 73 [ISO 02] élaboré par l'ISO (organisation internationale de normalisation) sur la terminologie du management du risque, la sécurité est l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à l'environnement.[MEC 11]

I.2.1. Principes généraux de protection

Nous pouvons distinguer les mesures de sécurité par leur mode d'action : les sécurités passives et les sécurités actives.

I.2.1.1. Sécurités passives

La sécurité passive désigne tous les éléments mis en jeu afin de réduire les conséquences d'un accident lorsque celui-ci n'a pu être évité. Elle agit par sa seule présence, sans intervention humaine ni besoin en énergie (exemple : bâtiment de confinement, cuvette de rétention, etc.).
L'isolation électrique est une mesure passive et préventive.

I.2.1.2. Sécurités actives

La sécurité active désigne tous les éléments mis en jeu afin d'éviter les accidents. Elle nécessite une action, une énergie et un entretien (exemple : détecteur, vannes, etc.).

La sécurité d'une installation repose sur l'utilisation de ces deux modes d'action. Une préférence est donnée au mode passif quand il est techniquement possible. Des critères de qualité sont exigés pour le mode actif, notamment la tolérance à la première défaillance : doublement de l'organe de sécurité (redondance). La sécurité fonctionnelle reste l'un des moyens les plus importants pour la prise en compte des risques. D'autres moyens de réduction ou d'élimination des risques, tels que la sécurité intégrée dans la conception existent également.

I.2.2. Sécurité fonctionnelle

La norme CEI 61508 dans sa partie 4 définit la sécurité fonctionnelle comme un sous ensemble de la sécurité globale qui se rapporte au système commandé (EUC, Equipement Under Control) et qui dépend du fonctionnement correct du système E/E/EP relatif à :

- la sécurité basée sur une autre technologie.
- La sécurité des dispositifs externes de réduction de risque.

La norme CEI 61511 définit la sécurité fonctionnelle comme un sous-ensemble de la sécurité globale qui se rapporte au processus et au système de commande de processus de base (BPCS, Base Process Control System) et qui dépend du fonctionnement correct du système instrumenté de sécurité et d'autres couches de protection. Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

La sécurité fonctionnelle permet de contrôler les risques inacceptables qui pourraient :

- porter atteinte à l'intégrité des personnes.
- dégrader l'environnement.
- altérer des équipements.

I.3. Cadre normatif

I.3.1. Norme CEI 61508

La CEI 61508 [CEI 00] est une norme multisectorielle qui traite l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP, c'est-à-dire qu'elle concerne à la fois le matériel et les logiciels. Cette norme est orientée « performances » en laissant à l'utilisateur le soin de réaliser son analyse de risque et elle lui propose des moyens pour réduire

ce risque. Le statut de norme de base de la CEI 61508 ne s'applique pas dans le contexte de systèmes E/E/PE concernés par la sécurité de faible complexité, pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Par exemple, un système comportant des fins de course et des relais électromécaniques reliés à un disjoncteur peut être étudié sans avoir recours à la CEI 61508.

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

Cette norme s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs électriques/électroniques/électroniques programmables. Elle comprend 7 parties :

1. Définition des prescriptions générales qui sont applicables à tous types de matériel,
2. Prescriptions spécifiques et supplémentaires pour les systèmes E/E/PE (S. E/E/PE) - aspect matériel,
3. Prescriptions spécifiques et supplémentaires pour les systèmes E/E/PE - aspect logiciel,
4. Définitions et abréviations utilisées,
5. Lignes directrices pour la détermination des niveaux d'intégrité de sécurité - méthode et exemple,
6. Lignes directrices pour la mise en œuvre des prescriptions relatives aux systèmes E/E/PE,
7. Présentation des techniques et des mesures.

La norme CEI 61508 est la base d'autres normes sectorielles (ex : machines, procédés continus, ferroviaire, nucléaire) ou de produits (ex : variateurs de vitesse). Elle influence donc le développement des systèmes E/E/PE et des produits concernés par la sécurité à travers tous les secteurs. Le système CEI 61508 est constitué d'une norme générique et de normes filles par secteur d'activité.

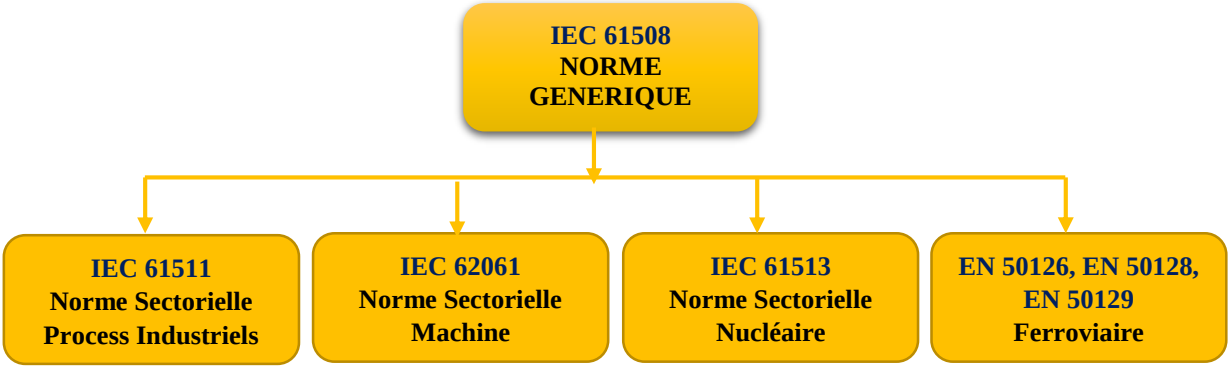


Figure I.1. : Norme CEI 61508 et normes dérivées

La norme IEC 61508 est générique. Les normes sectorielles qui en sont issues sont totalement compatibles, elles ne font que préciser les modalités d'application.

Les caractéristiques de la norme :

- Elle concerne toutes les phases du cycle de vie des matériels et du logiciel (depuis la conceptualisation, en passant par la conception, l'installation, l'exploitation, la maintenance, jusqu'à la mise hors service) ;
- Elle fournit une méthode de développement pour réaliser la sécurité fonctionnelle des systèmes relatifs à la sécurité ;
- Elle définit des niveaux d'intégrité de sécurité (SIL) des systèmes E/E/PE relatifs à la sécurité ;
- Elle décrit une approche basée sur l'analyse de risque pour déterminer les niveaux d'intégrité de sécurité (SIL) à atteindre pour un risque donné ;
- Elle fixe des objectifs quantitatifs de défaillances dangereuses des systèmes de sécurité en fonction des niveaux d'intégrité de sécurité ;
- Elle décrit les principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité, mais n'utilise pas le concept de sécurité intrinsèque, adapté à des systèmes peu complexes dont les modes de défaillances sont connus.

I.3.2. Norme CEI 61511

La norme sectorielle CEI 61511 concerne les systèmes instrumentés de sécurité pour le secteur les processus industriels. Cette norme comprend trois parties :

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

Cette norme établit des prescriptions relatives au cycle de vie en sécurité comprenant la spécification, la conception, l'installation, la maintenance et le démantèlement d'un système instrumenté de sécurité, afin d'avoir toute confiance dans sa capacité à amener le procédé dans un état de sécurité.

La norme CEI 61511 restreint le périmètre aux systèmes pour des applications SIL 1 à 3 (les applications SIL 4 ne pouvant être traitées par un SIS seul). Les applications qui nécessitent l'utilisation d'une fonction instrumentée de sécurité de niveau d'intégrité de sécurité SIL 4 sont rares dans l'industrie de processus. Ces applications doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité [CEI 03].

I.3.3. Norme ISA-84

La norme ISA-84 a été acceptée par l'institut national américain des normes (American National Standards Institute, ANSI) en mars 1997. Elle spécifie les exigences pour la conception, l'installation, l'utilisation et la maintenance des systèmes instrumentés de sécurité La norme ISA-84 dispose uniquement de trois niveaux d'intégrité de sécurité, SIL1 à SIL3. C'est une norme nationale contrairement à la norme CEI 61511 qui est une harmonisation de normes de plusieurs pays. ISA est en cours de développement.

I.4. Description du cycle de vie de sécurité

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 d'un système instrumenté de sécurité vise à s'assurer que toutes les activités nécessaires pour obtenir la sécurité fonctionnelle sont conduites et qu'il peut être démontré pour les autres qu'elles ont été exécutées dans un ordre approprié.

Pour toutes les phases du cycle de vie en sécurité, une planification pour la sécurité doit définir les critères, les techniques, les mesures et les procédures à employer pour :

- Garantir que les objectifs de sécurité fonctionnelle et de niveau d'intégrité de sécurité pour tous les modes pertinents du procédé seront atteints ;
- Assurer une installation et une mise en service correctes du système instrumenté de sécurité ;
- Garantir l'intégrité de sécurité des fonctions instrumentées de sécurité après l'installation du SIS ;
- Maintenir l'intégrité de sécurité durant l'exploitation (essais périodiques, etc.) ;
- Gérer les phénomènes dangereux liés au procédé pendant la phase de maintenance du système instrumenté de sécurité.

La figure I.2 montre un cycle de vie simple similaire à celle montrée dans la norme [Bait 11].

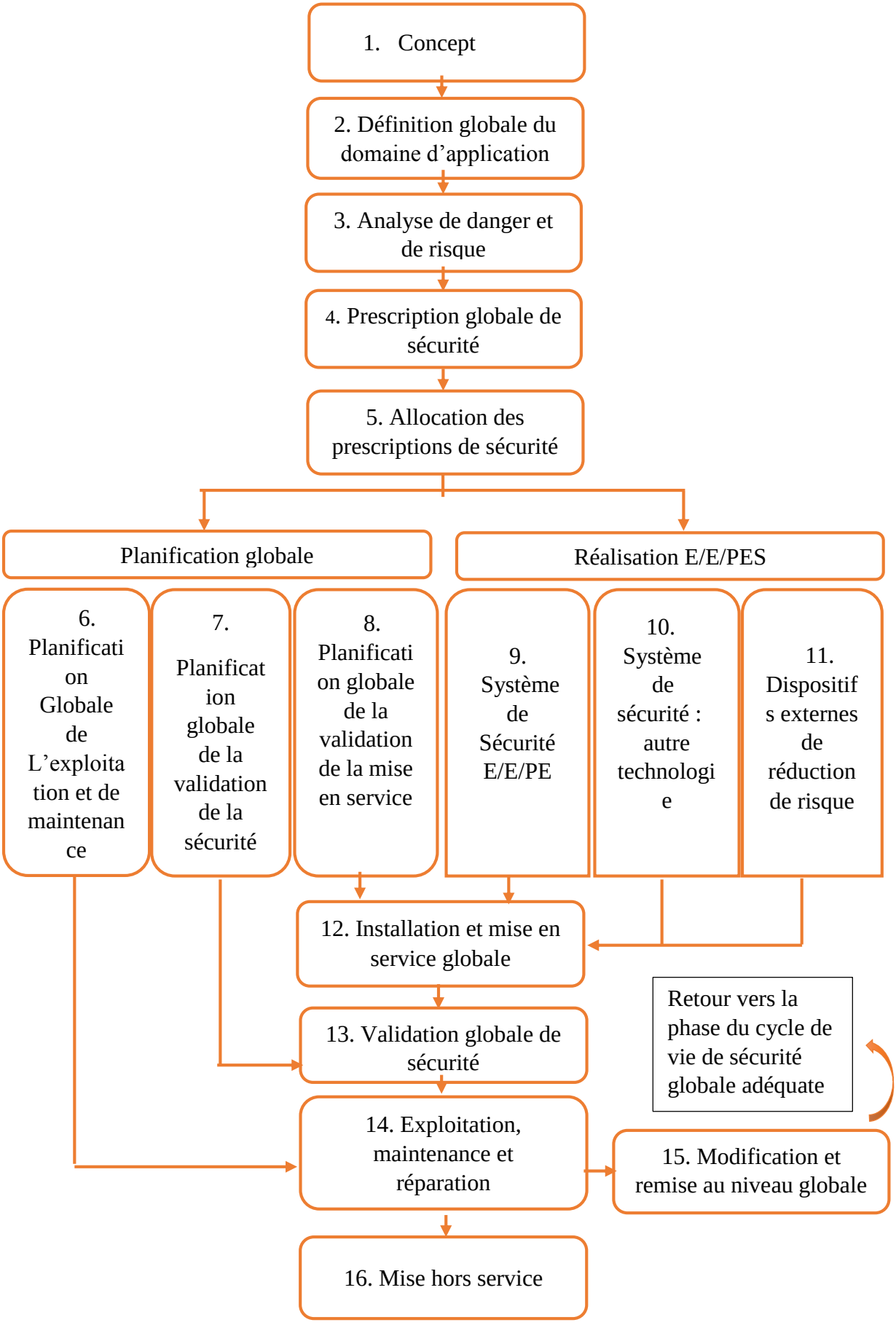


Figure I.2 : Le cycle de vie des SIS selon la norme CEI 61511 [PEI 11]

I.5. Systèmes instrumentés de sécurité

I.5.1. Définition d'un SIS

La norme CEI 61511 [CEI 03] définit les systèmes instrumentés de sécurité de la façon suivante : système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux).

La norme CEI 61508 [CEI 00] définit quant à elle les systèmes relatifs aux applications de sécurité par : un système E/E/PE (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.

Les systèmes instrumentés de sécurité sont donc utilisés comme moyens de prévention et comportent une proportion importante de systèmes électriques, électroniques ou encore électroniques programmables (E/E/EP).

Un système instrumenté de sécurité est un système visant à mettre le procédé en position de repli de sécurité lorsqu'il évolue vers une voie comportant un risque réel (explosion, feu, etc.).

I.5.2. Propriétés d'un SIS

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

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

I.5.3. Constitution d'un SIS

Les SIS sont constitués de différents éléments unitaires reliés entre eux par des moyens de transmissions. Un SIS se compose de trois éléments comme le montre la figure I.3 :

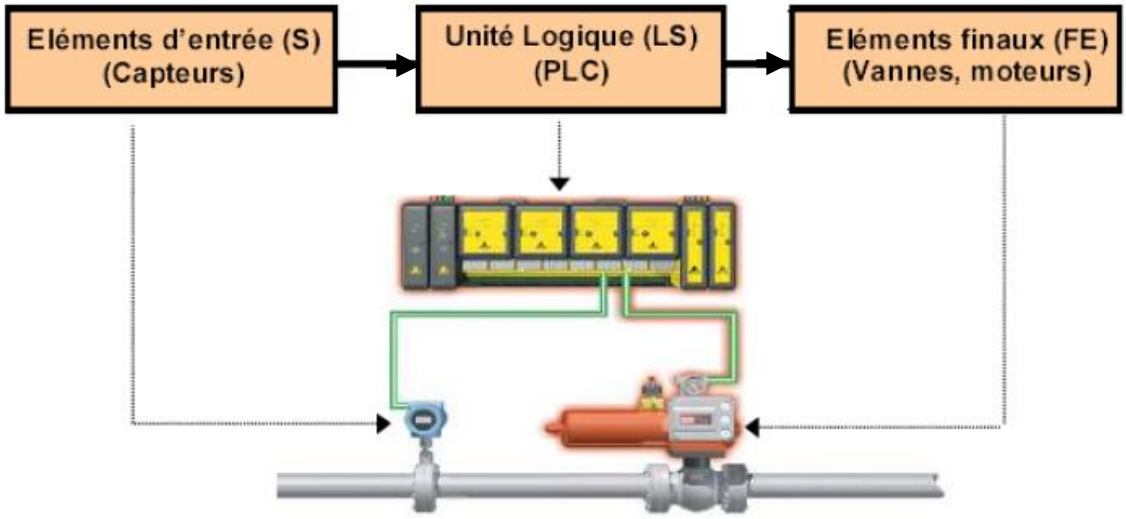


Figure I. 3 : Schéma d'un SIS simple

A. Capteur (Sensor)

Elle est constituée d'un ensemble d'éléments d'entrée (ex : capteurs détecteurs) qui surveillent l'évolution des paramètres physico-chimiques représentatifs du comportement du procédé (température, pression, niveau…).

B. Unité de traitement (Logic Solver)

Ce sous-ensemble d'éléments logiques réalise le processus de prise de décision qui s'achève par l'activation du troisième sous-système FE (Final Element). Le sous-système LS peut être un automate programmable ou un micro-ordinateur doté de logiciels spécifiques.

C. Actionneur (FE)

Il agit directement (ex : vannes d'arrêt d'urgence) ou indirectement (ex : vannes solénoïdes) sur le procédé pour neutraliser sa dérive en mettant, en général, le système à l'arrêt (état sûr) au terme d'un délai qui doit être spécifié pour chaque fonction de sécurité.

Enfin, l'unité de traitement est reliée aux capteurs et aux actionneurs par des moyens de transmission. Il peut s'agir de câbles électriques, de lignes téléphoniques, d'ondes hertziennes

(transmission par talkie-walkie…), ou de tuyauteries (transmission pneumatique ou hydraulique).

Les capteurs, l'automate et les actionneurs sont des équipements de sécurité. Un équipement de sécurité est un élément d'un SIS qui remplit une sous-fonction de sécurité.

Exemples :

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

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

I.5.4. Redondance au sein d'un S.I.S

L'atteinte de certains niveaux de SIL nécessite une tolérance aux anomalies du matériel. Les composants à fiabilité infinie n'existant pas, la bonne pratique est de mettre en place des redondances.

Par exemple, au lieu d'utiliser un capteur de pression, on en utilisera 2 ou 3, avec un système de vote pour déclencher l'action de sécurité. A noter que la redondance peut être réalisée avec du matériel identique ou avec du matériel de technologie différente, ce dernier type de redondance permet de limiter les modes communs de défaillance.

Le choix des architectures aura un impact sur la fiabilité, ainsi que la disponibilité.

La redondance m/n qui est une redondance telle qu'une fonction n'est assurée que si au moins m des n moyens existants sont en état de fonctionner ou en fonctionnement.

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

Avec n=nombre de canaux indépendants, et m=nombre de signaux nécessaires au déclenchement de l'action de sécurité :

1oo1 (m=n=1) : Cette architecture (1 out of 1) comprend un seul élément, et toute défaillance dangereuse de cet élément empêche le traitement correct de tout signal d'alarme valide.

1oo2 (m=1 et n=2) : Cette architecture (1 out of 2) comprend deux éléments connectés en parallèle de façon que chacun puisse traiter la fonction de sécurité. Tant qu'un élément est opérationnel, la sécurité est garantie.

2oo2 (m = n = 2) : Cette architecture (2 out of 2) comprend deux éléments connectés en parallèle de sorte qu'il est nécessaire que les deux éléments ayant une fonction de sécurité avant que celle-ci ne survienne. La défaillance dangereuse d'un seul élément empêche le traitement correct de tout signal d'alarme valide.

2oo3 (m = 2 et n = 3) : Cette architecture (2 out of 3) comprend trois éléments 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 élément donne un résultat différent des deux autres éléments. Tant que deux éléments sont opérationnels, la sécurité est garantie. Il faudrait la défaillance dangereuse des deux éléments pour qu'un signal d'alarme valide ne soit pas traité correctement.

I.5.5. Fonction instrumentée de sécurité (SIF)

La fonction instrumentée de sécurité est définie comme étant la fonction de sécurité avec niveau d'intégrité de sécurité (SIL) spécifique qui est nécessaire pour maintenir la fonction de sécurité. La fonction de sécurité est définie comme la fonction qui doit être réalisée par un SIS. Cette fonction de sécurité a pour but de maintenir un état sécurisé du process. Une fonction instrumentée de sécurité peut être considérée comme une barrière de protection fonctionnelle alors que le système instrumenté de sécurité est considéré comme un système réalisant cette barrière de sécurité.

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

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

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

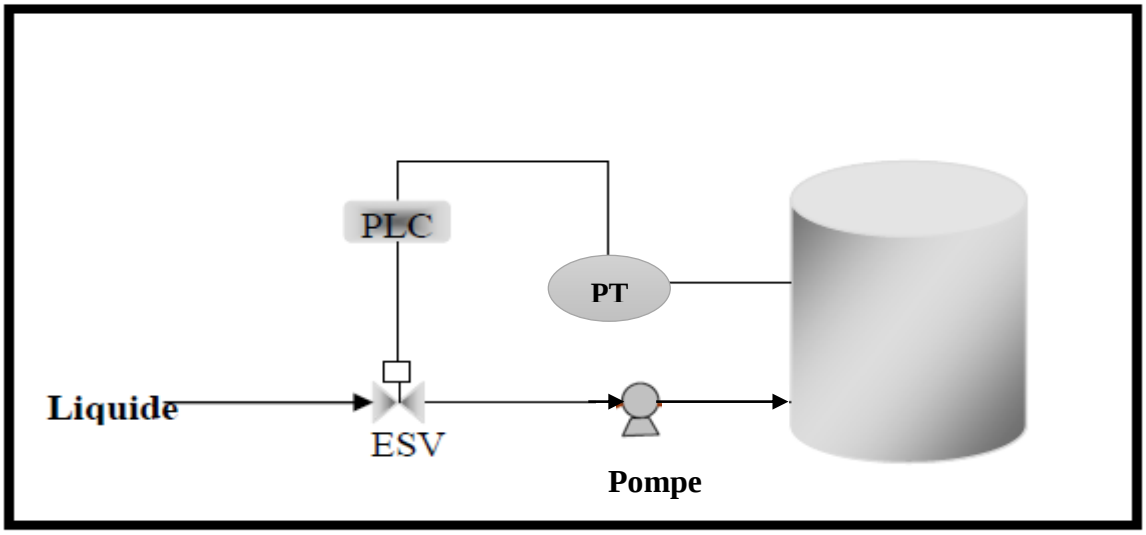


Figure I.4 : Exemple de fonction instrumentée de sécurité

I.5.6. Le système instrumenté de sécurité comme couche de protection

Les différentes couches de protection contribuent de manière indépendante à la réduction du risque grâce à des moyens de contrôle de prévention ou d'intervention.

La figure (I.5) montre le concept des couches de protection et la composition des différents types de systèmes relatifs à la sécurité (SRS) comme définis dans la norme CEI 68511-3. Il est à noter qu'il existe une distinction claire entre les BPCS et les SIS comme composantes des couches de protection. L'objectif primaire d'un BPCS est d'optimiser les conditions de conduite de procédé afin de maximiser la qualité et la production. Les systèmes instrumentés de sécurité s'appliquent pour prévenir des situations dangereuses (prévention) et réduire les conséquences d'événements dangereux (protection). La distinction est motivée par le fait que le BPCS n'est nécessairement pas utilisé pour contribuer à la réduction de risque et parfois il est lui-même source de risques potentiels. [MKH 08]

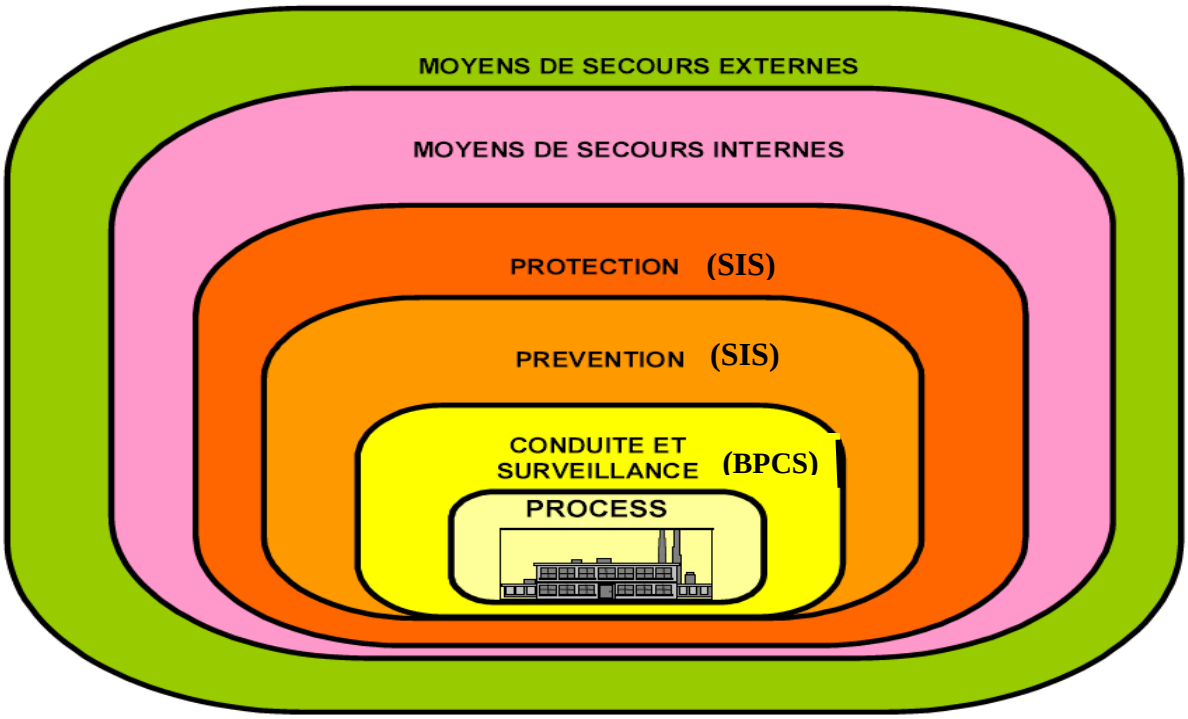


Figure I.5 : Les couches de protection

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

La partie prévention des couches de protection est assurée par les dispositifs de sécurité mécaniques, par les alarmes suivies d'action et par les systèmes instrumentés de sécurité de

prévention. La protection est assurée par des dispositifs de sécurité mécaniques, la supervision par l'opérateur et par les systèmes instrumentés de sécurité d'atténuation [KNE 02]. Les moyens de secours internes et externes concernent respectivement les procédures d'évacuation lors de l'occurrence d'une situation critique.

Il faut aussi différencier le BPCS qui est le système de commande de base du processus et le SIS qui est le système instrumenté de sécurité. En effet, le BPCS est aussi composé de capteurs, de régulateurs et d'éléments finaux. Bien que les architectures apparaissent similaires, les fonctions sont différentes entre le BPCS et le SIS. La fonction primaire d'une boucle de régulation est généralement de maintenir une variable de processus dans des limites prescrites. Le SIS surveille une variable de processus et commande une action lorsque c'est exigé.
Les SIS sont rarement activés et durant les opérations normales du processus, ils demeurent statiques or dormants. La période moyenne entre l'occurrence d'événements dangereux est souvent estimée à plus d'une dizaine d'années. Avec le BPCS, les signaux de commande sont normalement dynamiques. Les modes de défaillances diffèrent aussi entre un BPCS et un SIS.

I.5.7. Niveaux d'intégrité de sécurité

Les normes CEI 61508 et CEI 61511 définissent le niveau d'intégrité de sécurité (Safety Integrity Level : SIL) pour définir le niveau de réduction du risque que doit avoir le système de protection. Plus le SIL à une valeur élevée, plus la réduction du risque est importante. Par exemple un système de SIL 4 apporte une réduction de risque entre 10000 à 100000 alors qu'un système de SIL 1 comporte un facteur de réduction de risque compris entre 10 à 100 seulement. L'utilisation des niveaux SILs permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel menant aux évènements dangereux identifiés pendant l'analyse de risque.
La qualité requise du SIS s'exprime par le SIL et mesure la réduction du risque obtenue par les moyens de prévention fournis par le SIS.
La norme IEC 61508 [IEC61508 02] fixe le niveau d'intégrité de sécurité (SIL) qui doit être atteint par un SIS qui réalise la Fonction Instrumentée de Sécurité (SIF). Elle donne le SIL en fonction de la probabilité de défaillance moyenne (PFDavg) sur demande pour les SIS faiblement sollicités. Ou en fonction de probabilité de défaillance par heure (PFH) pour les SIS fortement sollicités ou agissant en mode continu. Dans ce mémoire, nous nous plaçons dans le contexte des SIS faiblement sollicités (moins d'une sollicitation par an).

Le mode de fonctionnement à faible sollicitation (lorsqu'une défaillance apparaît) est généralement attribué aux systèmes de protection, activités lors de l'occurrence d'un événement indésirable.

Il est important de souligner que le concept de SIL s'applique uniquement à un système instrumenté de sécurité (SIS) dans son intégralité et pas à un composant pris individuellement. A partir de l'architecture du système instrumenté de sécurité réalisant la fonction instrumentée de sécurité faiblement sollicitée, la moyenne de la probabilité de défaillance à la demande PFDavg (Average Probability of Failure on Demand) est évaluée sur un intervalle [0, t] [IEC61508 98].

I.6. Evaluation des différentes probabilités [HAB 03]

Pour l'évaluation du niveau d'intégrité de sécurité (SIL) par référence à la norme CEI61508, il est nécessaire de calculer la probabilité de défaillance à la demande de la fonction de sécurité liée au système instrumenté de sécurité.

Dans la norme CEI61508, les différentes architectures de SIS étudiées sont composées de canaux. Chacun d'eux peut avoir aussi bien des défaillances détectables par test de diagnostic de taux λ_{DD}que des défaillances non détectables de taux λ_{DU}. Ces deux taux sont considérés comme constants.

- Nous nous plaçons dans le cas où le SIS est faiblement sollicité (moins d'une fois / an), d'où le besoin d'évaluer la *PFD.*
- Nous nous intéressons à l'évaluation du *PFDavg* du *SIS*. C'est pourquoi nous utilisons les taux de défaillance $\lambda_D$des composants qui désignent les taux de défaillance dangereuse non détectés λ_{DU} et les taux de défaillance détectés λ_{DD}.

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \quad (1.1)$$

La norme CEI 61508 définit un taux de couverture de diagnostic pour les tests automatiques de diagnostic comme le rapport de taux de défaillances dangereuses détectées (par un test de diagnostic) sur le taux total des défaillances dangereuses (détectées et non détectées).

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \quad (1.2)$$

Ces défaillances dangereuses font passer le système de l'état normal à l'état de défaillance dangereux.

Le taux de défaillance constant $\lambda(t) = \lambda$ est pris comme hypothèse pour la plupart des estimations statistiques, cela s'applique seulement si la durée de vie utile des composants n'est pas dépassée [CEI 00]. Dans notre cas, et comme c'est préconisé par la norme, nous considérons des taux de défaillance des composants constants sur toute la durée de vie du système.

R(t) représente la fiabilité : $R(t) = e^{-\lambda t}$ (1 .4)

La probabilité de défaillance est donnée par : $F(t) = 1 - R(t)$ (1.5)

Si la demande est rare, alors dans ce cas : $e^{-\lambda t} \approx 1 - \lambda t$, l'approximation est arrêtée au premier ordre.

La probabilité de défaillance vaut alors : $PF(t) = \lambda t$, et la probabilité de défaillance moyenne est donnée par : $PF_{avg} = \frac{1}{T}\int_0^T PF\ (t)dt$ (1.6)

La probabilité de défaillance sur demande qui concerne le système entier est donnée par :

$$PFD_{avg} = \frac{1}{Ti}\int_0^{Ti} PFD\ (t)dt \quad (1.7)$$

Dans le cas de l'approximation faite ci-dessus, on aura : $PFD_{avg} = \frac{\lambda Ti}{2}$ (1.8)

I.6.1. Architecture 1oo1

Cette architecture se compose d'un seul canal, il faut une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande [IEC61508].

$$PFD_{avg} = \lambda_{DU} \cdot \frac{T1}{2} \quad (1.9)$$

λ_{DU} : taux de défaillance dangereuse non détectés.

T_i: time interval between manual functional tests of the com-ponent.

I.6.2. Architecture 1oo2

Cette architecture se compose de deux canaux identiques fonctionnant en redondance active, 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 [IEC61508].

$$PFD_{avg} = \frac{1}{3}(\lambda_{DU} \cdot \frac{T1}{2})^2 \quad (1.10)$$

I.6.3. 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 de deux autres canaux [IEC61061 98].

$$\mathrm{PFD}_{\mathrm{avg}} = (\lambda_{\mathrm{DU}} \cdot \frac{\mathrm{T1}}{2})^2 \qquad (1.11)$$

I.6.4. Les probabilités de défaillances

La norme IEC 61508 [54] spécifie deux indicateurs de la sécurité relatifs aux systèmes électroniques programmables dédies aux applications de sécurité. Ces deux paramètres utilisés pour l'évaluation des performances des SIS suivant les deux modes de défaillance cités par les normes de sécurité. Ces modes sont le mode de défaillances dangereuses et le mode de défaillances sûres. Ces indicateurs sont donnés sous forme de probabilités de défaillance dangereuse (PFD) et de défaillance en sécurité (PFH).

- **Probabilité moyenne de défaillance à la demande (PFD)**

La probabilité moyenne de défaillance à la demande, notée PFDavg représente tout simplement l'indisponibilité moyenne d'un système E/E/EP relatif à la sécurité, qui rend ce dernier incapable d'effectuer correctement sa fonction de sécurité, lorsqu'il est faiblement sollicité.
La dénomination PFD utilisée dans la norme est d'autant moins adéquate. Elle désigne la probabilité de défaillance dangereuse à la sollicitation. La PFDavg est la mesure d'une indisponibilité moyenne sur une période spécifiée.

- **Probabilité de défaillance dangereuse par heure (PFH)**

La probabilité d'une défaillance dangereuse par heure PFH (Probability of a dangerous Failure per Hour), est parfois appelée "fréquence des défaillances dangereuses ", ou "taux défaillances dangereuses ", ou nombre de défaillances dangereuses par heure ".

Dans les tableaux (I.1 et I.2), les fonctions instrumentées de sécurité ainsi que les systèmes instrumentés de sécurité sont différenciés selon le mode de fonctionnement par l'utilisation des paramètres PFD et PFH. Chaque SIL est délimité par une borne maximale et une borne minimale [MKH 08].

Fonctionnement à la demande		
Niveau d'intégrité de sécurité SIL	**Probabilité moyenne de défaillance (PFDavg)**	**Réduction du risque RR**
4	$10^{-5} \leq PFD \leq 10^{-4}$	$100\,000 \leq RR < 10\,000$
3	$10^{-4} \leq PFD < 10^{-3}$	$10\,000 \leq RR < 1\,000$
2	$10^{-3} \leq PFD < 10^{-2}$	$1\,000 \leq RR < 100$
1	$10^{-2} \leq PFD < 10^{-1}$	$100 \leq RR < 10$

Tableau I.1- Probabilité de défaillance à la demande

Fonctionnement par heure	
Niveau d'intégrité de sécurité SIL	**Probabilité de défaillance dangereuse par heure PFH**
4	$10^{-9} \leq PFH < 10^{-8}$
3	$10^{-8} \leq PFH < 10^{-7}$
2	$10^{-7} \leq PFH < 10^{-6}$
1	$10^{-6} \leq PFH < 10^{-5}$

Tableau I.2- Probabilité de défaillance dangereuse par heure

La probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système instrumenté de sécurité est déterminée par le calcul et l'addition de la probabilité moyenne de défaillance sur demande pour tous les sous-systèmes assurant ensemble la fonction de sécurité. Cela peut être exprimé par la formule suivante [IEC 61508 02] :

$$\mathbf{PFD_{sys} = PFD_c + PFD_u + PFD_a}$$

$\mathbf{PFD_{sys}}$: est la probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système instrumenté de sécurité.

$\mathbf{PFD_c}$: Probabilité moyenne de défaillance sur demande du sous-système capteur.

$\boldsymbol{PFD_u}$ **:** Probabilité moyenne de défaillance sur demande du sous-système unité traitement.

$\mathbf{PFD_a}$: Probabilité moyenne de défaillance sur demande du sous-système actionneur.

I.6.5. Paramètres Influant sur le calcul de SIL

Après avoir déterminé les exigences du SIS à travers la classe SIL, il faut définir le SIS, et plus précisément les solutions technologiques aptes à satisfaire.

La chaîne de sécurité doit remplir sa mission lors de la sollicitation (aspect sécurité), tout en évitant de provoquer des déclenchements intempestifs (aspect disponibilité).

La qualité de la chaîne de sécurité dépend de plusieurs critères :

- Taux de défaillance (λ). Le taux de défaillance est un terme relatif à la fiabilité des équipements ou composants défini comme l'inverse du MTTF (Mean Time To Failure), le temps moyen jusqu'à la première défaillance. Son symbole est la lettre grecque lambda (λ). Le taux de défaillance s'exprime en FIT (Temps moyen entre pannes). En anglais, le taux de défaillance est nommé Failure rate
- Facteur de mode commun ou facteur ß .Dans le cas de structure redondante (multiple canaux), les modes communs représentent les défaillances qui peuvent apparaitre dans les canaux suite à une même cause.
- Taux de Couverture de diagnostic DC (qualité et étendue des tests automatiques). La norme CEI 61508 définit un taux de couverture de diagnostic pour les tests automatiques de diagnostic comme le rapport de taux de défaillances dangereuses détectées (par un test de diagnostic) sur le taux total des défaillances dangereuses (détectées et non détectées).
- Temps moyen de réparation MTTR (remise en service après défaillance non déclenchant), avec ses corollaires que sont l'organisation de la maintenance et la gestion des pièces de rechange.
- Périodicité des tests manuels (organisation des tests, portée des tests).

I.6.6. Détermination des niveaux de SIL requis

L'évaluation du niveau d'intégrité de sécurité d'un SIS est déterminée par des méthodes qualitatives et quantitatives. Elles permettent ; d'examiner les différents dangers provenant du système opérationnel et de déterminer le SIL de la SIF pour réduire la criticité du danger analysé. L'objectif global de ces méthodes est de décrire une procédure d'identification des SIF, d'établir les niveaux de sécurité correspondant et de les mettre en œuvre dans un SIS afin de ramener le procédé dans l'état de sécurité.

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

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

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

- **Méthodes quantitatives** : Il s'agit des méthodes qui permettent de calculer la 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.

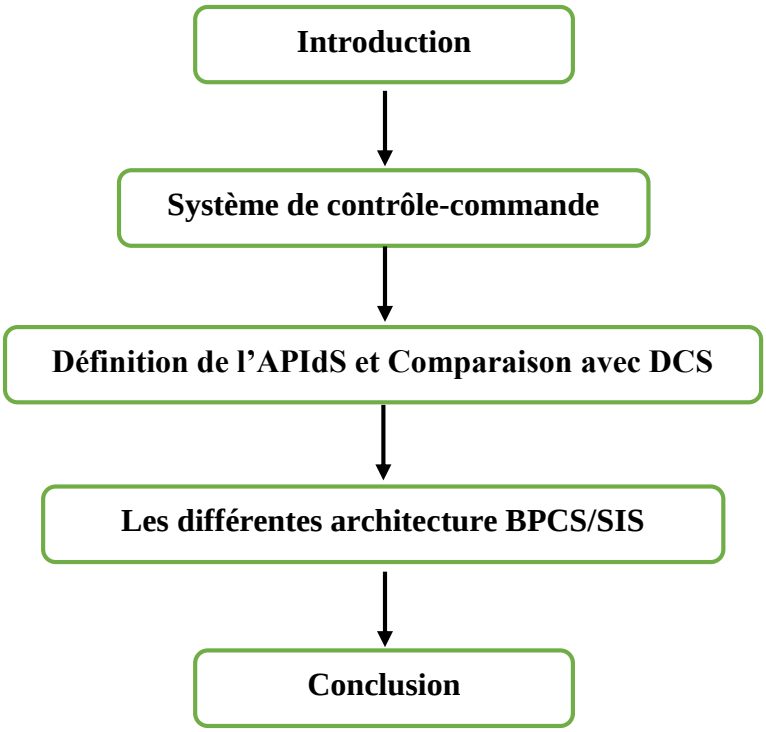
I.7. Conclusion

Dans ce chapitre nous avons précisé l'organisation de la norme CEI 61508 et défini les systèmes instrumentés de sécurité, qui sont utilisés pour détecter des situations dangereuses et diminuer leurs conséquences pour atteindre des niveaux de risques tolérables. Il convient à cet effet de rappeler que la CEI 61508 de même que ses normes filles sont actuellement devenues la référence par excellence pour la mise en œuvre de ce type de systèmes. Une brève description des normes relatives aux systèmes de sécurité est donnée, suivie d'une description des différentes méthodes utilisées pour déterminer le SIL d'un SIS.

Rappelons dans le cadre de ce travail la méthode des équations simplifiées est choisi comme approche d'évaluation du SIL.

CHAPITRE II

SYSTEME DE CONTROLE ET SYSTEME DE SECURITE



II.1. Introduction

La conduite d'un procédé dans le domaine pétrole & gaz implique la connaissance, la surveillance et la maîtrise de certains paramètres tels que la pression, la température, le débit etc. Chaque procédé possède ses propres exigences, et chaque équipement a ses conditions de fonctionnement. Le système de contrôle-commande doit satisfaire ces besoins. Les installations industrielles dans le domaine pétrole & gaz présentent des risques pour les personnes, l'environnement et les équipements, d'où la nécessité de mise en œuvre des systèmes de mise en sécurité de ces installations à risque pour le respect des exigences réglementaires.

Dans ce chapitre on présente, pour le procédé étudié, qui est le four H401, les moyens utilisés pour assurer la commande et la sécurité. Nous présenterons également les différentes architectures d'association de ces deux systèmes et les avantages et les inconvénients pour chaque architecture. Enfin, on conclut par l'architecture utilisée pour le procédé étudié.

II.2. Système de contrôle-commande

Dans l'industrie des procédés, la fonction de contrôle commande est utilisée pour atteindre les objectifs de quantité et de qualité, réduire la main d'œuvre, les erreurs humains, et améliorer la disponibilité des équipements.
Au début, les fonctions de contrôle étaient, principalement pneumatiques et électropneumatiques localisées sur le terrain ou partiellement déportées, en salle technique.
Les premiers systèmes centralisés ont été introduits dans les années 70 et le contrôle a été relocalisé en salle de contrôle avec des tableaux de contrôle à portée des opérateurs.

Le système de contrôle distribué DCS est utilisé dans les procédés industriels pour assurer la conduite, la surveillance et le contrôle des équipements distribués.

II.2.1. DCS (distributed control system) I /A Series

Le système I / A Series (Intellegent / Automation) est un système d'automatisation intelligente de procédé industriel comersialisé par FOXBORO.

C'est un système numérique de contrôle à commande distribuée, utilisé pour le contrôle des procédés industriels tels que pétrole, gaz et nucléaire. Ses éléments constitutifs échangent entre eux les informations via des réseaux de communications.

Il se compose essentiellement de deux parties :
-Partie équipement ou matériels (hardware).
-Partie logiciel (software).

II.2.2. Description du DCS :

Le DCS est constitué de plusieurs sous–systèmes :

- Les dispositions d'entrées/sorties.
- Les contrôleurs individuels (PLC régulateurs).
- Les interfaces opérateurs (écran).
- La station de travail ingénieur.
- Le réseau de communication (bus) pour l'échange des informations.

II.2.3. Fonction de base de DCS

Les fonctions de base à réaliser par un système numérique de contrôle de commande de procèdes industriels sont :

- Echange des signaux industriels avec le procédé.
- Traitement en temps réel des données échangées.
- Traitement en temps différé des données échangées.
- Interface homme-machine interactive pour la surveillance du système et la conduite du procédé.
- Disponibilité d'outils de développement et de mise au point.

II.2.4. Les caractéristiques de DCS

- **La notion distribution :** Les notions de base de conduite du procédé sont distribuées sur plusieurs dispositifs (stations) assurant en cas de défaillance matérielle, la continuité pour la plupart des fonctions.
- **La notion de redondance :** Elle offre une possibilité de redondance pour augmenter la fiabilité du système et diminuer les déclanchements intempestifs.
- **La notion d'ouverture :** Le DCS est un système ouvert qui a l'avantage de communiquer avec d'autre systèmes indépendants tels que : ESD, APIdS(TRICONEX), scada, F&G.
- **La notion de disponibilité des informations :** La disponibilité des informations en temps réel et l'historique des données grâce aux réseaux de communication et la capacité mémoire du DCS.
- **La notion de surveillance continue :** La visualisation de l'évolution des paramètres et la lecture des données qui se fait par une surveillance continue.

II.2.5. Architecture de base de DCS I/A Séries de FOXBORO utilisée dans de le module MPP0

L'architecture du DCS englobe les stations, les imprimantes et les réseaux pour le fonctionnement du système. La notion d'ouverture de cette architecture permet d'ajouter d'autres systèmes pour la sécurité et l'arrêt d'urgence. Le système d'arrêt d'urgence « ESD » est basé sur un automate APIdS(Triconex) qui est indispensable pour la sécurité du procédé. Ce système est indépendant et connecté au DCS via un port de communication (NODEBUS) juste pour la visualisation de certains paramètres ESD sur les stations d'opérateurs.

L'architecture de base du DCS se présente sur les quatre niveaux suivants :

Niveau 1 : Raccordement (Instruments de mesure et de contrôle).

Niveau 2 : Acquisition des signaux (Les modules d'entrée /sortie du procédé).

Niveau 3 : La conduite du procédé par l'intermédiaire des stations opérateur.

Niveau 4 : Interface opérateur (partie de supervision et de gestion du module).

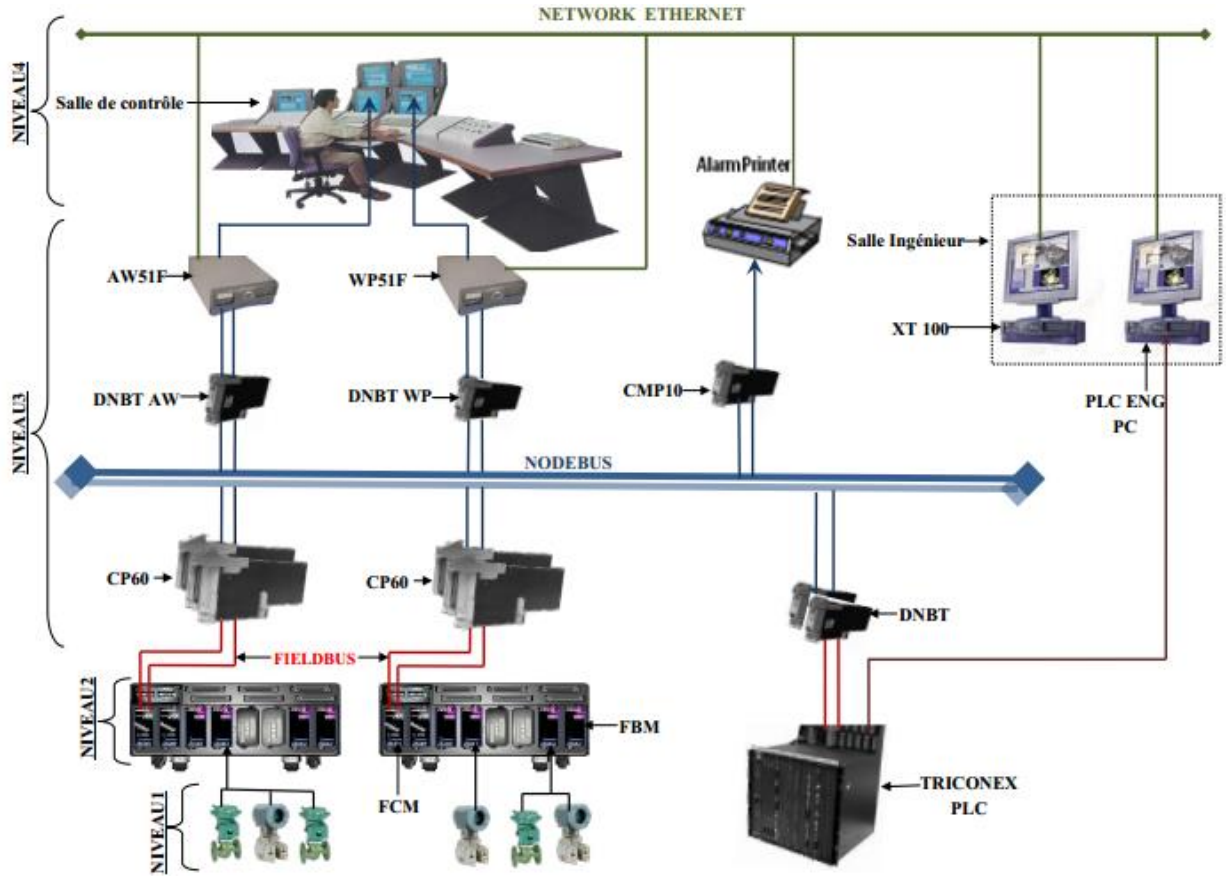


Figure II. 1: Architecture de base du DCS I/A série FOXBORO

II.2.6. Aspect matériel/DCS

A. Les cartes d'entrées/sorties (E/S) ou FBM (Field Bus Module)

Les modules d'E/S FBM réalisent les fonctions générales suivantes :

- Interface entre les signaux industriels du processus automatisé et le processeur de contrôle.
- Conversion des signaux industriels en signaux numériques (acquisition) et inversement (commande).

B. Processeur de contrôle (CP) :

Le traitement en temps réel des données échangées avec le procédé se fait par des processeurs de contrôle redondants.

Le processeur a pour but de satisfaire les fonctions suivantes :

- La communication avec les **FBM** via le **Field bus interface**
- Exécution des fonctions algorithmiques de traitement en continu (les fonctions de régulation PI, PID etc.).
- Production des alarmes : si un paramètre dépasse le seuil opérationnel, le processeur envoie une alarme à la station opérateur.
- Communication avec les autres stations via le réseau **NODEBUS.**

- La redondance des processeurs

Pour des raisons de sécurité l'architecture de DCS a mis en place une redondance entre deux processeurs de contrôle connectés entre eux. Ils acquièrent les mêmes données et ils contiennent le même programme. Mais l'un est en position maitre et l'autre est en position esclave. Si un problème apparaît au niveau du processeur actif, le second va prendre le contrôle (position maitre) et le traitement se fait en permanence.

C. Processeur d'application

Les fonctions d'un processeur d'application sont :

- Surveillance du système.
- Gestion de base de données.
- Exécution de programme applicatif ou utilitaire.

D. Processeur de communication :

Le processeur de communication fournit les fonctions nécessaires aux autres stations du réseau pour communiquer avec des imprimantes.

E. Processeur de visualisation (WP)

Le processeur de visualisation réalise l'interface en temps réel entre l'utilisateur et le système I/A séries. C'est l'interface homme-machine.

F. Processeur double application et visualisation (AW)

Cette station réalise les fonctions d'un processeur d'application et celles d'un processeur de visualisation. Elle peut être connectée à un réseau I/A séries ou utilisée comme station de configuration hors-ligne.

II.2.7. Aspect communication/DCS

A. Réseau de communication (Field Bus)

Il permet au processeur de contrôle de communiquer avec les cartes d'E/S FBM. Ce réseau est un bus qui a comme support physique un câble coaxial ou fibre optique selon la distance entre le processeur de contrôle et les cartes E/S.

B. Réseau système local (RL)

Le réseau local permet d'assurer la communication entre des stations du système I/A.

C. Le réseau de communication NODEBUS

Le réseau de communication Nodebus de contrôle à temps réel, relie le processeur central (CP) aux armoires et unité centrale (UC) qui se trouvent dans la salle de contrôle.

D. Réseau ETHERNET

C'est le réseau LAN interne utilisé pour la connexion des HMI. Il permet

- Le transfert des fichiers de configuration.
- Le transfert de données (exemple : liaison du PC du laboratoire avec la base de données I/A série).
- L'acquisition des données du procédé, les messages et les données historiques.

II.2.8. Aspect logiciel/DCS

- Système d'exploitation du CP40 est VRTX.
- Gestionnaire de visualisation WP : FOX VIEW.
- Gestionnaire d'alarme : AW.
- Construction du synoptique : Fox Drew.
- Langage de commande UNIX.

II.3. Description de l'APIdS et Comparaison avec DCS

Le Triconex est un Automate Programmable Industriel dédié Sécurité (APIdS), cet automate se distingue des API standards par la mise en œuvre de moyens spécifiques qui lui permet de répondre de manière définie à l'apparition d'une défaillance d'un de leur composant.

Ces APIdS possèdent une fiabilité supérieure à la normale :

- ✓ Par la redondance de l'unité centrale (UC) assortie d'un mécanisme comparaison des résultats permettent de déceler la défaillance d'une des UC ;
- ✓ Par la redondance d'autres éléments essentiels tels les modules d'entrées ; les coupleurs avec test par le bloc UC ;
- ✓ Par la mise en œuvre périodique de programme élaborés d'autotest, capables de mettre en évidence des pannes dormantes, c'est-à-dire dont les effets ne sont pas encore apparus.

Le système ESD indépendant est connecté au DCS via un port de communication juste pour la visualisation de certaines variables ESD sur les stations d'opérateurs. La liaison entre TRICONEX et le Nodebus DCS Séries I/A de Foxboro, se réalise par un module de communication avancé ACM (Advanced Communication Module) de Triconex.

II.3.1. Automate Programmable Industriel dédié Sécurité (Triconex)

Les APIdS sont en premier lieu destinés aux procédés des industries chimiques, pétrochimiques, chaudières de centrales thermiques etc. Les objectifs sont à la fois la sécurité (typiquement SIL 3 selon IEC 61508) et une haute disponibilité.

Ces automates sont bien adaptés pour gérer des process et en particulier des systèmes ESD.

Le Triconex est un système de sécurité et de contrôle basé sur une architecture TMR (Triple Module Redondant). Ce système TMR (redondance triple modulaire) est composé de trois systèmes de contrôle parallèles distincts intégrés dans un même ensemble matériel. Le vote des données logiques de types deux sur trois garantit un fonctionnement en continu à haut niveau d'intégrité et sans erreur.

Il existe même des systèmes QMR (quadruple redondance modulaire), ils sont exploités avec 4 canaux redondants, en cas de perte d'un canal le système est dégradé en TMR avec vote 2 sur 3 (dit "2 out of 3", noté 2oo3). Les TMR et QMR sont des systèmes de sécurité avec redondance fonctionnelle. Ils sont conçus de manière à permettre le remplacement de toutes les cartes sans couper l'alimentation.

La redondance modulaire triplée (TMR) est une forme de tolérance de panne, dans laquelle trois systèmes effectuent un processus et ce résultat est traité par un système de vote pour produire une seule sortie. Si l'un des trois systèmes échoue, les deux autres systèmes peuvent corriger et masquer le défaut.

II.3.2. Principaux éléments du TRICON

Figure II.2 : Automate Programmable TRICONEX

- **Les alimentations (Deux alimentations par châssis)**

- Alimentations duales, chacune est capable de supporter la charge du châssis.
- Alarme de température.
- Alarme de pile de sauvegarde.
- 2 régulateurs par chaîne (6 par module).
- Immunité totale au bruit.
- Changement de l'unité en ligne.

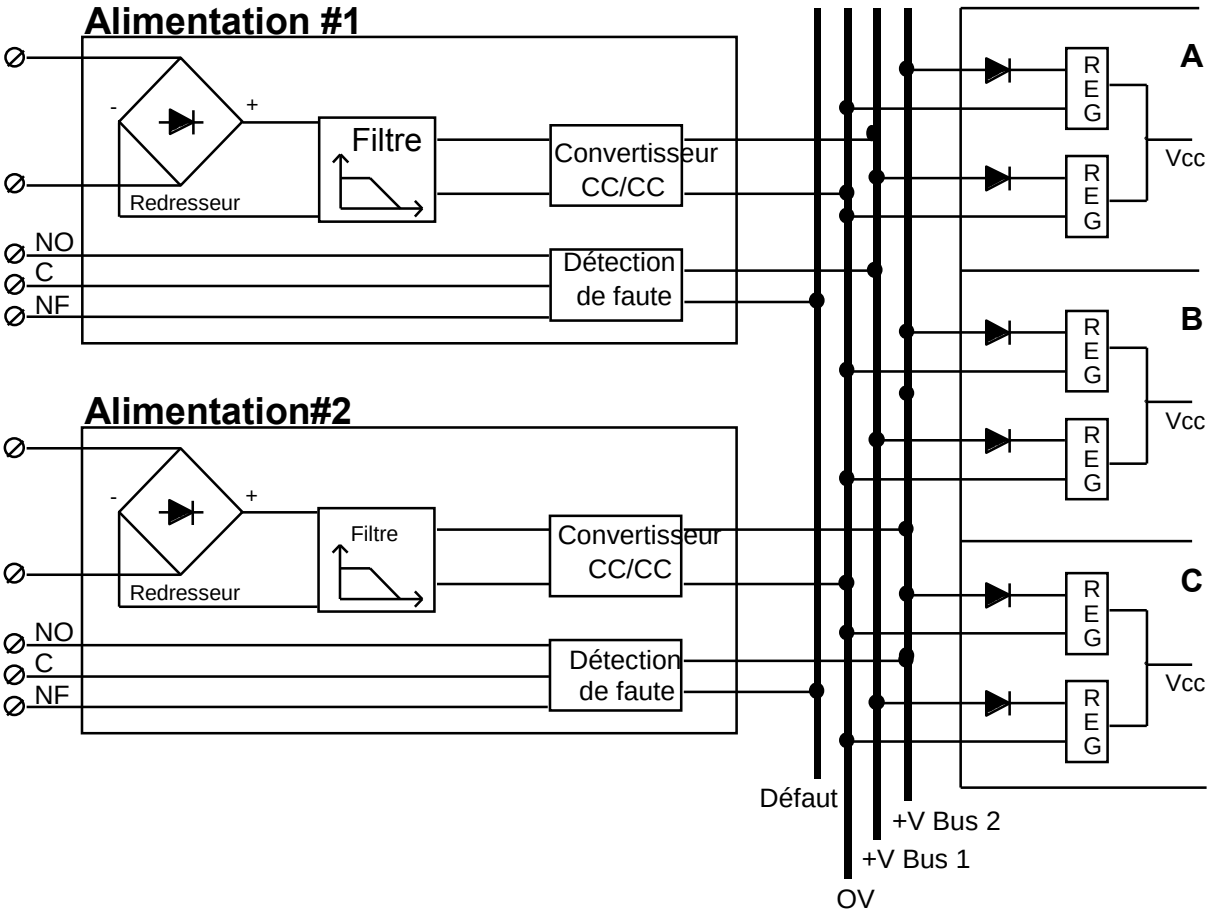


Figure II.3 : Architecture duale de l'alimentation

- **Les unités centrales**

- 3 modules séparés sont configurés en architecture T.M.R (Triple Module Redondance).

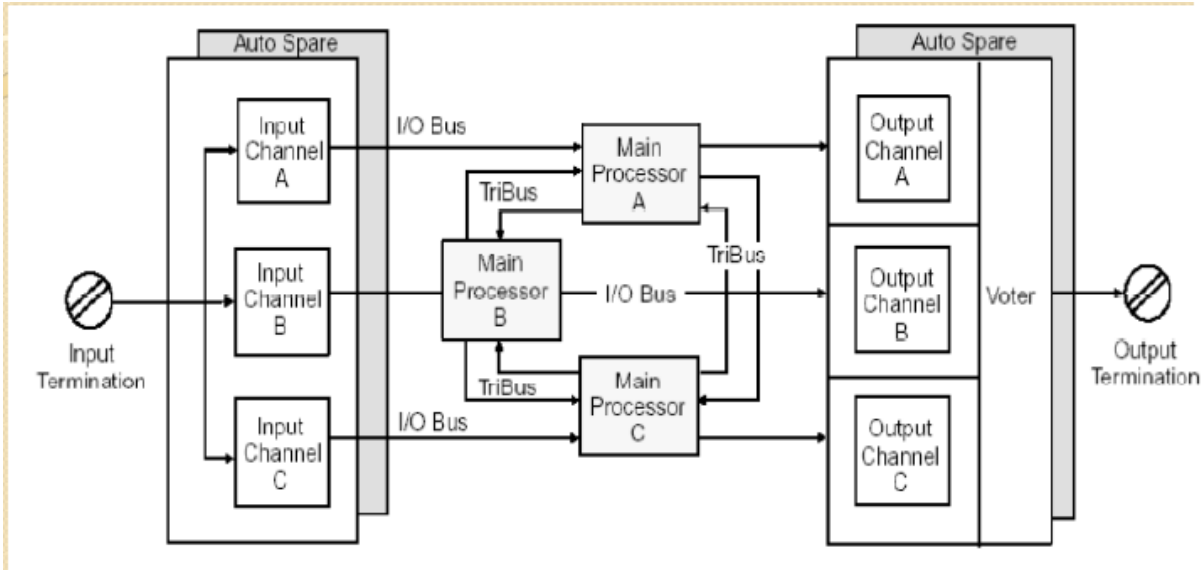


Figure II.4 : Architecture TMR simplifiée

Le triconex a été conçu autour d'une architecture triplée, depuis les points d'entrées jusqu'aux points de sorties en passant par les processeurs principaux.

Chaque module d'entrée/sortie contient trois chaines de traitement redondantes et indépendantes. Chaque chaine de traitement des modules d'entrées lit les données du procédé et transmet cette information au module processeur principal auquel elle est rattachée.

Les trois processeurs principaux échangent leurs données par l'intermédiaire du bus propriétaire à haute vitesse appelé TRIBUS.

Le TRIBUS vote les données d'entrées logiques compare les données de sorties et envoie une copie des valeurs d'entrées logiques à chaque processeur principal (FigureII.4). Les processeurs principaux exécutent le programme d'application et transmettent les valeurs calculées aux modules de sorties. Outre le vote des données d'entrées, le triconex vote également les données de sorties. Cette opération est effectuée au niveau des modules de sorties juste en amont des borniers de raccordement ce qui permet de trouver et corriger une erreur éventuelle entre le vote au niveau du TRIBUS et de la sortie.

- **Les modules d'entrées /sorties**

- Modules triplés dialoguant avec les processeurs en utilisant un bus d'E /S triplé.

- **Les modules de communications**

- Bus de communications triplés assurant la communication entre les processeurs et les modules de communication.

II.3.3. Les caractéristiques de TRICONEX

Les principaux avantages et caractéristiques de l'architecture TMR du système TRICONEX sont les suivants :

- Pas de point unique de défaillance.
- Un très haut niveau de disponibilité.
- Un très haut niveau de sécurité.
- Une maintenance à moindre coût.
- La possibilité d'une maintenance différée.
- La possibilité d'un archivage de données avec SOE « Sequence Of Events ».
- Un isolement total de tous les niveaux.
- Des liaisons de communications redondantes à haute vitesse.

II.3.4. Différences DCS/Triconex

Il existe une distinction claire entre le BPCS et le SIS comme composantes des couches de protection.

Il est important de comprendre les différences fondamentales entre le système de contrôle de procédé de base qui est le (DCS) et le système de contrôle de sécurité qui est le (TRICONEX)

II.3.4.1. DCS (Actif / Dynamique)

Le DCS est actif et dynamique. Par conséquent, la plupart des défaillances de contrôle sont auto-révélées. La défaillance est immédiatement observée par l'operateur qui réagit en conséquence. Généralement on n'a pas besoin de tests et diagnostic avancés pour révéler ce genre de défaillance.

II.3.4.2. Triconex (Passif / Dormant)

Le Triconex est un système de sécurité passif ou dormant. Il opère sur des périodes de temps prolongées. Il surveille de façon continue l'état des composants des boucles quand elles sont pourvues d'une couverture de diagnostic, analyse les mesures reçues du site.

A titre d'exemple, pour une boucle de surveillance de pression haute, le système réagit seulement si la pression atteint une certaine valeur préconfigurée, si la pression n'arrive jamais à cette valeur la fonction de sécurité liée à cette pression ne va jamais réagir. Beaucoup de défaillances de ces systèmes de sécurité ne sont pas auto détectées et révélées.

Les systèmes instrumentés de sécurité sont utilisés pour prévenir des situations dangereuses (prévention) et réduire les conséquences d'événement dangereux (protection).

La distinction est motivée par le fait que le BPCS n'est pas nécessairement utilisé pour contribuer à la réduction de risque, et parfois il est lui-même source de risques potentiels, et cela nécessite une intervention du SIS.

La figure ci-dessous montre la complémentarité d'un SIS mettant le système en sécurité lors d'une défaillance du système de contrôle /commande.

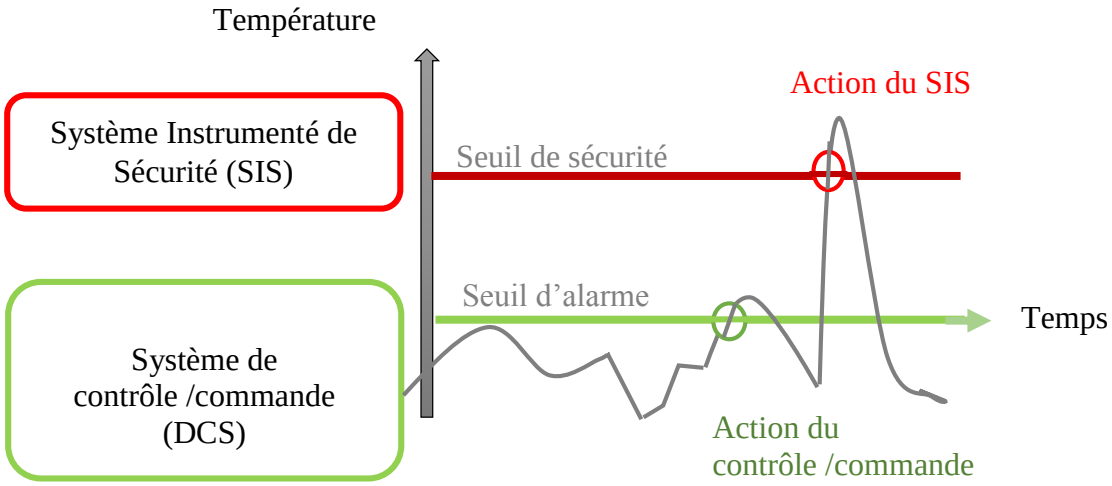


Figure II.5 : Intervention du SIS à la défaillance du système de contrôle/commande

La figure ci-dessus représente une courbe représentative d'un paramètre 'température' en fonction du temps. Intervention d'un SIS dans le cas où la température est très élevée.

Les différences physiques et fondamentales existantes entre un système de contrôle DCS et un système instrumenté de sécurité à base de Triconex sont résumées dans le tableau suivant :

Système DCS	Système Triconex
Degré de flexibilité	
Une grande flexibilité pour développer et maintenir les applications complexes de contrôle. Amélioration ou modification dans la configuration Software et mise en œuvre.	Une fonctionnalité fixe, attentivement minimisée lors de la conception. Une procédure rigide pour la modification de système.
Mode de défaillance	
En cas de défaillance, aucune garantie sur l'état du sortie du système.	Etat prévisible en cas d'échec fonctionnel indiqué dans le système.
Conception de sécurité	
Les stratégies de réparation et de maintenance. Il permet une grande variété de la maintenance et de la modification. Risque accepté pendant la maintenance afin d'éviter l'arrêt de toute l'installation.	Une possibilité limitée pour la maintenance du matériel, pendant le fonctionnement du procédé. Aucune modification pendant le fonctionnement du procédé.
La stratégie du test	
Pas de besoin de tester le système régulièrement, excepté quelques instruments de secours.	Une procédure explicite pour le test automatique des défaillances non détectées des instruments de sécurité.

Tableau II.1- Comparaison BPCS/TRICONEX

II .4. Les différentes architectures BPCS / SIS

Après la publication des normes de sécurité, où les connaissances dans l'analyse des risques et la protection ont été approfondies, les fabricants ont commencé à élaborer un système de sécurité rentable avec une meilleure protection contre les risques résiduels.

Un **SIS** autonome était la méthode de choix traditionnel, ce qui signifie des exigences de conception et d'exploitation différentes entre le système instrumenté de sécurité SIS et le système et le système de contrôle **BPCS.**

En conséquence, ces deux systèmes ont été développés pour la régulation et la sécurité du processus avec des moyens séparés. Ainsi il y'avait des stations opérateurs différentes dans le BPCS et le SIS et il en était de même pour les autres équipements.

Les utilisateurs finaux se sont rendus compte que cette configuration était trop couteuse, car un SIS "n'est pas rentable".

D'autres architectures sont alors été proposées qui intègrent au moins le BPCS et le SIS.

On le présente rapidement dans le point suivant.

II.4.1. Les degrés d'intégration

On distingue principalement quatre degrés d'intégration entre le BPCS et le SIS

- **BPCS et SIS Séparés**

C'est une méthode traditionnelle, elle signifie que les deux systèmes de contrôle et de sécurité sont complétement séparés, ils peuvent être de deux fournisseurs différents et utiliser des outils de gestions distincts.

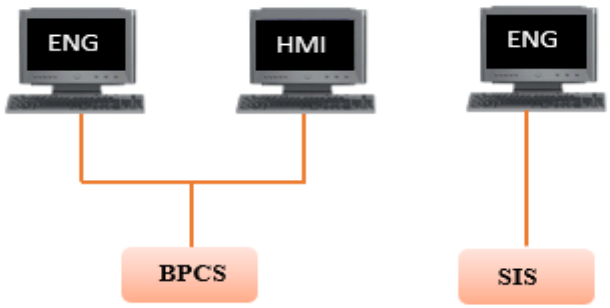


Figure II.6 : BPCS et SIS séparés

- **BPCS et SIS Interfacés**

Le système de contrôle de procédés BPCS et le système de sécurité SIS sont basés sur un matériel différent mais ils sont reliés par une passerelle sécurisée qui assure un échange contrôlé de données d'alarmes et de mesures en quantité et en direction, et par des signaux tout ou rien câblés pour les déclenchements d'urgences.

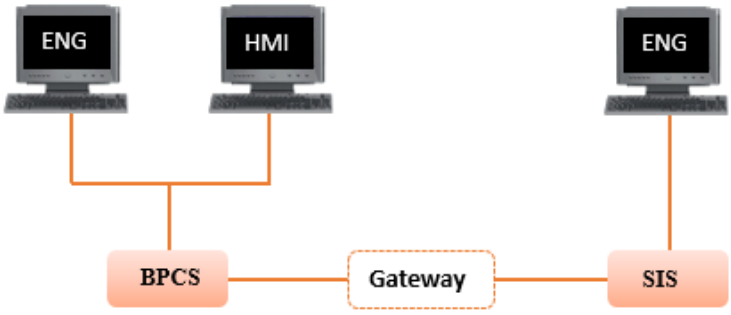


Figure II.7 : BPCS et SIS interfacés

- **BPCS et SIS Intégrés**

Le système de contrôle de procédés et le système de sécurité sont basés sur un matériel différent, mais possèdent un système de communication homogène et peuvent partager des outils de gestions des systèmes.

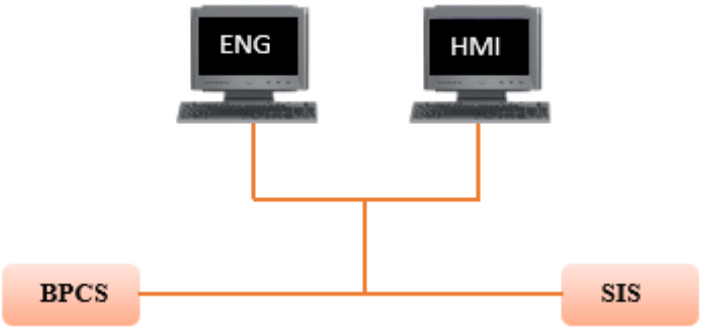


Figure II.8 : BPCS et SIS intégrés

- **BPCS et SIS Communs**

Le BPCS et le système de sécurité sont regroupés dans le système de conduite de procédés. Ils utilisent un matériel commun (contrôleur, bus de terrain, périphérie décentralisé).

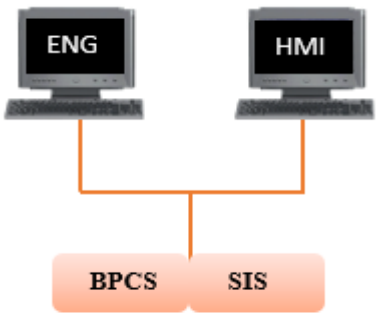


Figure II.7 : BPCS et SIS communs

L'intégration totale des systèmes SIS et BPCS, basée sur l'utilisation d'un matériel commun, reste toujours le choix des fournisseurs qui cherchent une minimisation des coûts et une meilleure rentabilité.

II.4.2. Avantages et Inconvénients

Niveau d'intégration	Outils d'Ingénierie		Systèmes et réseaux	
	Avantages	**Inconvénients**	**Avantages**	**Inconvénients**
Séparé		Coûts d'installation et d'ingénierie élevé. Coût du cycle de vie élevé pour la modification et la maintenance des deux systèmes séparés.	Meilleure protection contre les cyber-attaques. Les défaillances du BPCS n'ont aucun impact sur le SIS. Evite les causes communes des défaillances.	Coût très élevé du cycle de vie pour la modification et la maintenance des deux systèmes différents.
Interfacé		Coût d'installation élevé. Frais supplémentaires pour la formation et la maintenance.	Réduit les causes communes des défaillances.	Modes de défaillance inconnus. Augmentation des risques de cause commune.
Intégré	Diminution des coûts du cycle de vie de la maintenance et de formation.	Besoin d'un personnel qualifié.	Diminution des Frais du hardware, avec l'utilisation commune des matériels.	Causes communes des défaillances des deux systèmes. Impact des défaillances d'un système sur l'autre. Besoin d'une conception stricte pour éviter que les défaillances conduisent à des conditions dangereuses.
Commun	Frais les moins élevés sur le cycle de vie, la maintenance et la formation.			Réduction du nombre de couches de protection. Les défaillances de cause commune peuvent être très dangereuses.

Tableau II.2 - Avantages et inconvénients des intégrations BPCS/SIS

Le système étudié dans notre travail, qui est le four H401, regroupe le système de contrôle-commande (DCS) et système de sécurité (TRICONEX). Ces deux systèmes utilisent un matériel commun (Architecture BPCS/SIS communs) pour assurer à la fois la commande et la sécurité du four H401.

II.5. Conclusion

Dans ce chapitre, nous avons présenté les moyens de contrôle-commande (DCS) et de sécurité (APIdS), utilisés pour le four H401 de module MPP0 de l'installation pétrolière à Hassi R'mel.

Nous avons comparé ces deux types de systèmes afin de relever la spécificité de chacun d'entre eux et de montrer un exemple de réalisation des exigences de commande et de sécurité.

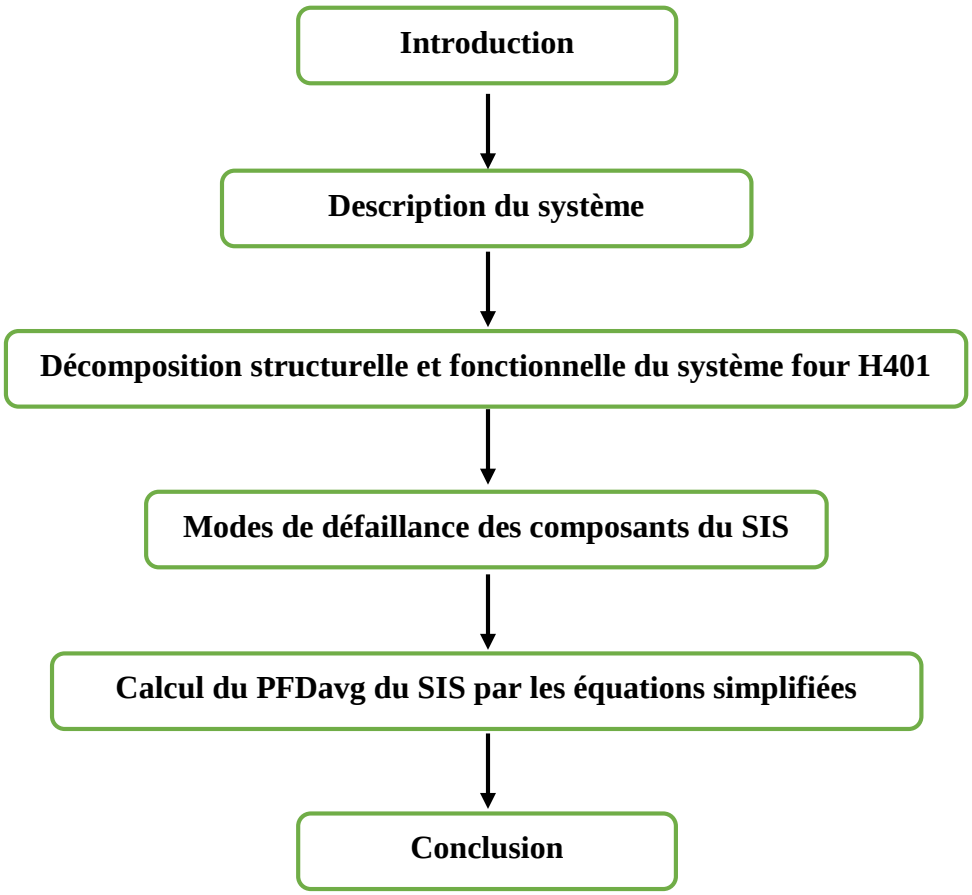
Les architectures d'association de ces deux types de systèmes ont été présentées rapidement et nous avons situé le procédé étudié parmi ces architectures.

Dans le chapitre suivant, nous allons détailler l'étude du four H401 et l'évaluation de la performance (en terme probabiliste) des SIS.

CHAPITRE III

EVALUATION DES SIL D'UN SYSTEME OPERATIONNEL :

FOUR REBOUILLEUR



III.1. Introduction

Le module « MPP0 » est le plus ancien des installations pétrolières à Hassi R'Mel. Son rôle est le traitement du gaz naturel en le séparant pour obtenir le gaz de vente (C_1, C_2), GPL (C_3, C_4) et le condensât (C_5^+).

Le module est constitué de différentes installations (ballons de séparation, colonnes de distillation, échangeurs, fours…).

Le four H401 est considéré comme la partie qui joue un rôle important dans le fonctionnement du module.

Dans ce chapitre notre étude s'intéresse au four que nous décrivons dans la suite.

III.2. Description du système

La figure ci-dessous présente une vue réelle d'un four H401 cylindrique vertical.

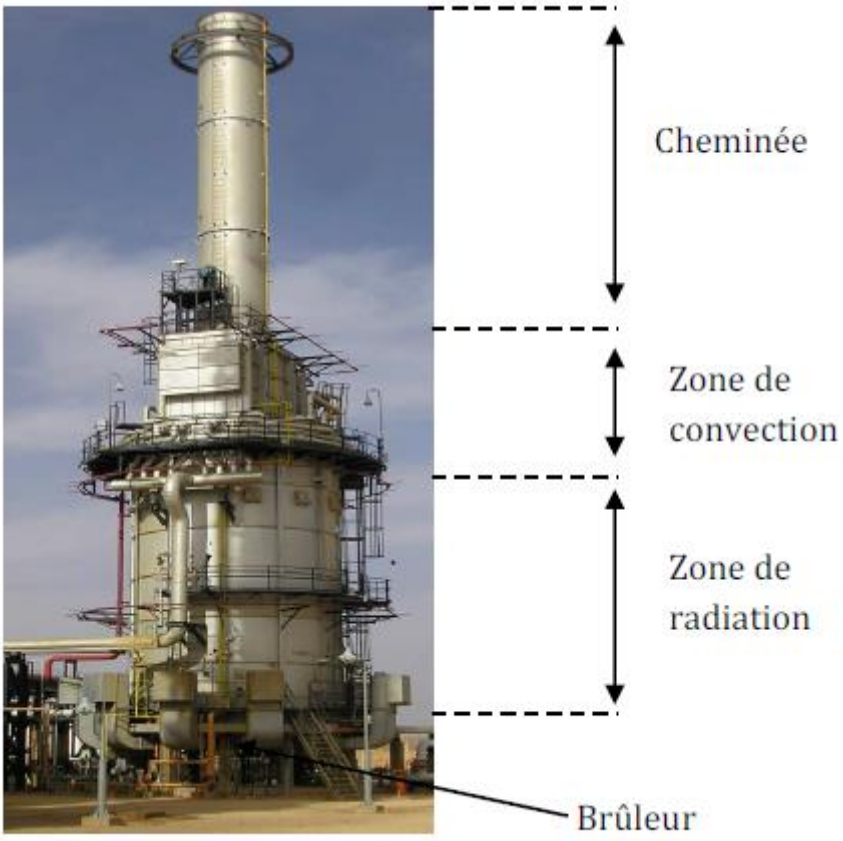


Figure III.1 : Le Four Rebouilleur H401

III.2.1. Rôle du four H401 et zones constitutives

Le rôle du four dans une unité pétrolière est d'apporter la chaleur nécessaire pour réchauffer un fluide en le portant à des niveaux de température élevés.

Dans le MPP0, les hydrocarbures liquides (Liquide qui contient gaz sec (C_1, C_2), GPL (C_3, C_4) et condensât (C_5^+)) du fond de la colonne T401 passe à travers la pompe P401, dans le rebouilleur H401 à 145°C. Le fluide sortant porter à 180° est renvoyé vers la colonne comme reflux chaud pour séparer les gaz légers (C_1, C_2).

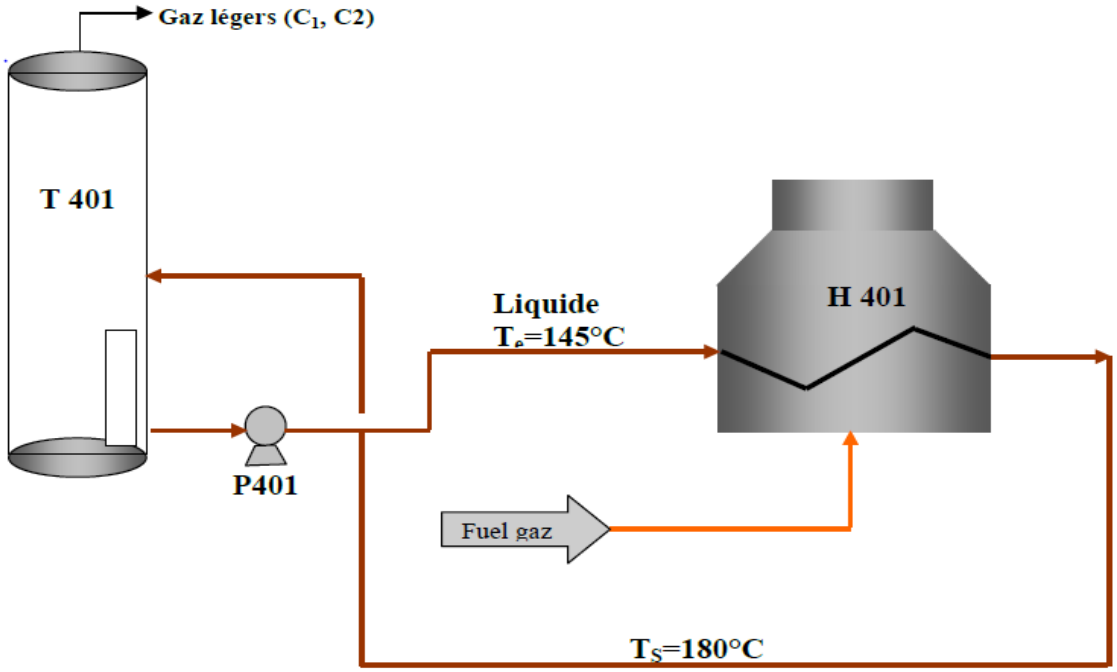


Figure III.2 : Le four H401 pour l'échauffement du liquide

Le four H401 est de type cylindrique vertical composé de deux zones :

- **Zone de radiation (rayonnement)**

  Elle constitue la chambre de combustion ou foyer dans laquelle des tubes sont exposés à la flamme et reçoivent la chaleur principalement par radiation.

  Le produit de combustion est du fuel gaz.

- **Zone de convection**

  Située à la sortie des fumées de la chambre de combustion. Elle est constituée des faisceaux de tubes placés perpendiculairement à la direction des fumées.

  L'échange de chaleur s'effectue principalement par convection.

III.2.2. Constitution du four H401

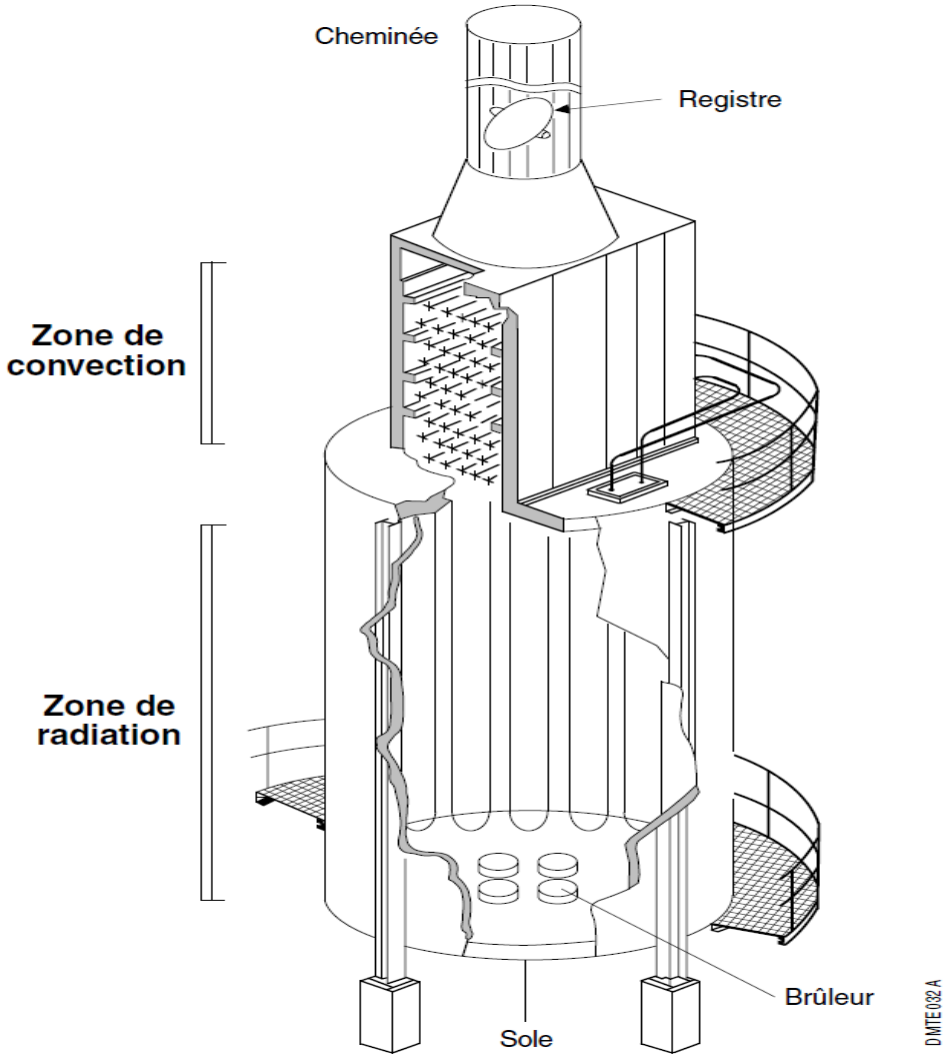


Figure III.3 : Une vue écorchée d'un four cylindrique vertical

Faisceaux tubulaires

Le four H401 possède 08 faisceaux tubulaires, les faisceaux tubulaires sont généralement constitués de tubes droits, reliés entre eux par des coudes à **180 °** soudés sur les tubes. Le choix du matériau pour les faisceaux des tubes repose sur les critères suivants :

- Résistance à la corrosion par le fluide chauffé.
- Résistance à l'oxydation par les fumées chaudes.
- Résistance mécanique en température.

Brûleurs

Les brûleurs ont pour fonction de réaliser la combustion et donc d'assurer :

- Le mélange du combustible et du comburant.
- L'inflammation du mélange.

Les pilotes

Le but des pilotes est de garantir une flamme continue pour l'amorçage de la combustion du gaz venant des brûleurs.

Cheminée

Elle sert à l'évacuation des fumées.

Registre

Le registre introduit sur le circuit des fumées une perte de charge plus ou moins grande selon son ouverture, c'est l'organe de réglage du tirage.

Les soufflantes d'air

Les soufflantes d'air sont utilisées pour purger l'intérieur des fours après chaque arrêt. Cette procédure est très importante pour la sécurité des fours et ses installations.

III.3. Décomposition structurelle et fonctionnelle du système four H401

La figure (III.4) montre un schéma simplifié de la décomposition du système four H401.

La description du système étudié se fait par une décomposition en quatre sous-systèmes (contrôle, alimentation, alarme et arrêt d'urgence), pour identifier les différentes fonctions de chaque partie et l'intervention du système ESD dans le cas de déclenchement du four.

En cas de défaut de température très élevée (TAHH) du liquide à l'intérieur et à la sortie du four, Une visualisation au niveau de DCS par une alarme est effectuée pour alerter l'opérateur pour qu'il intervienne sur la vanne manuelle TV. Le système ESD provoque la coupure d'alimentation du fuel gaz.

En cas de défaut de débit très bas (FALL) du liquide entrant dans le four, le système ESD provoque la coupure d'alimentation du fuel gaz. Une visualisation au niveau de DCS par une alarme est effectuée pour alerter l'opérateur pour qu'il intervienne sur la vanne manuelle FV.

L'augmentation ou la diminution de la pression du fuel gaz (PAL/H) provoque l'intervention du sous-système ESD sur la fermeture des vannes automatiques UZV401A et UZV401B pour couper l'alimentation du gaz combustible (fuel gaz), et sur l'ouverture de la vanne automatique UZV401C pour dégager le gaz combustible restant dans les vannes UZV401A et UZV401B vers l'atmosphère.

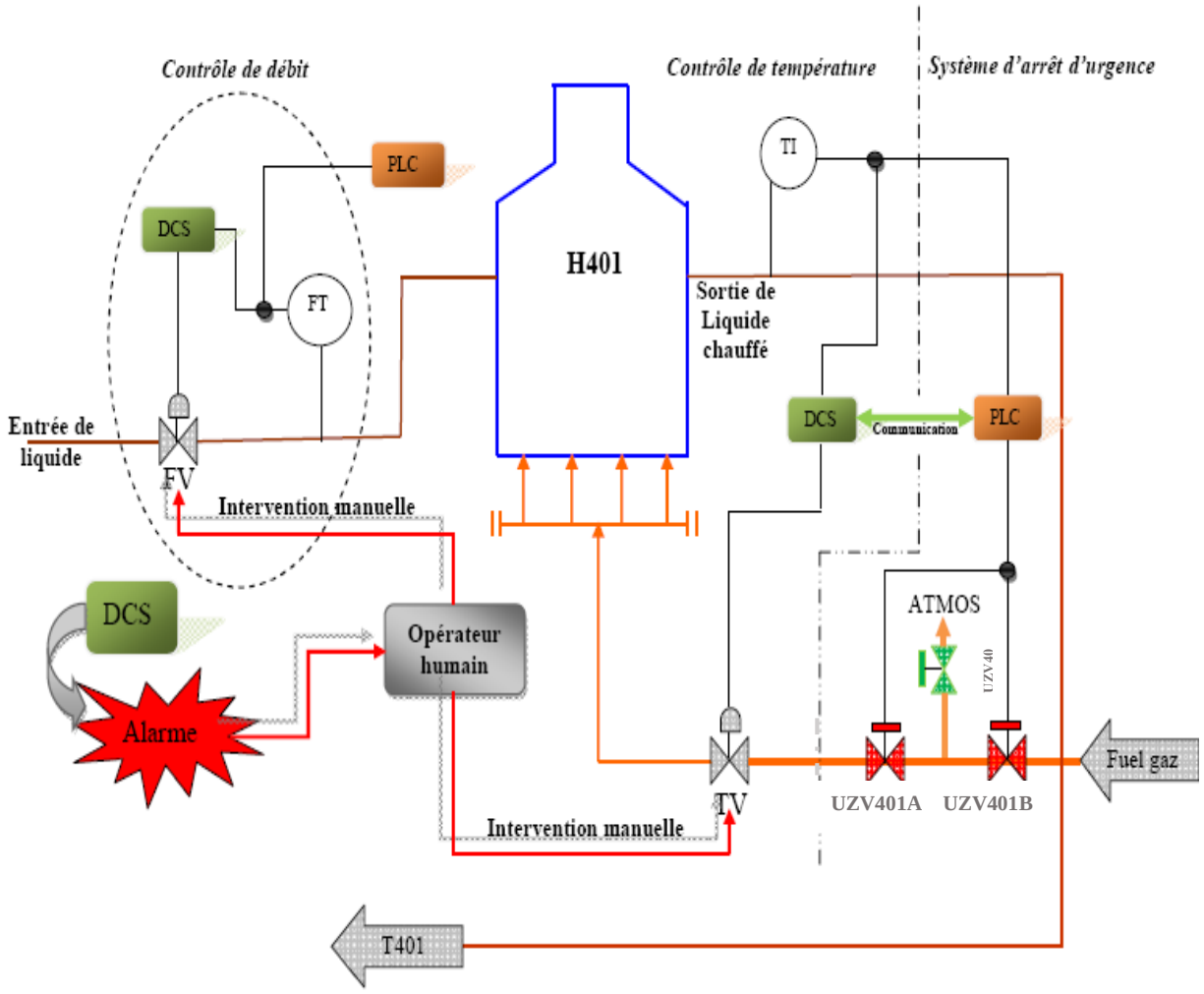


Figure III.4 : Schéma du système four rebouilleur

III.3.1. Sous-système d'alimentation

Sous-systèmes (SS)	Équipements (E)	Composants (C)
SS1 : circuit d'alimentation [Alimentation du four rebouilleur]	**E11 :** circuit comburant (Fuel Gaz) [Assure l'alimentation en combustible]	**C111 :** Vanne TV [régulation de pression de fuel gaz en fonction de la température de liquide]
		C112 : Pilotes [Garantir une flamme continue pour l'amorçage du fuel gaz]
		C113 : Brûleurs [Réaliser la combustion de fuel gaz]
	E12 : circuit Liquide [Assure l'alimentation en liquide du fond de la colonne]	**C121 :** Pompes P401 A/B [pomper le liquide à l'entrée du four]
		C122 : Vanne FV [régulation de débit de liquide]
		C123 : Serpentin [Assure la circulation et l'échauffement du liquide]

Tableau III.1- Sous-système d'alimentation

III.3.2. Sous-système de contrôle

Le contrôle dans le four porte sur les fonctions suivantes : - la température de sortie du fluide de procédé doit être maintenue à **180°C**. - le débit du fluide de procédé dans le four doit être maintenu à **800m^3/h**.

Sous-systèmes (SS)	**Équipements (E)**	**Composants (C)**
SS2 : de contrôle [contrôle des paramètres du procédé]	**E21 :** contrôle de débit [Contrôle le débit du liquide à l'entrée du four]	**C211 :** DCS (SOLVER) [Adaptation du débit de liquide à l'entrée du four par action sur la vanne FV]
		C212 : Débitmètre FT [Mesure le débit du liquide à l'entrée de four]
	E22 : contrôle de température [Contrôle la température du liquide à l'intérieur et à la sortie du four]	**C221 :** DCS (SOLVER) [Adaptation de température de liquide à la sortie de four par action sur la vanne TV]
		C222 : Thermocouple TI [Mesure la température du liquide à la sortie du four]
		C223 : Indicateurs de température TJI [Indique la température]

Tableau III.2- Sous-système de contrôle

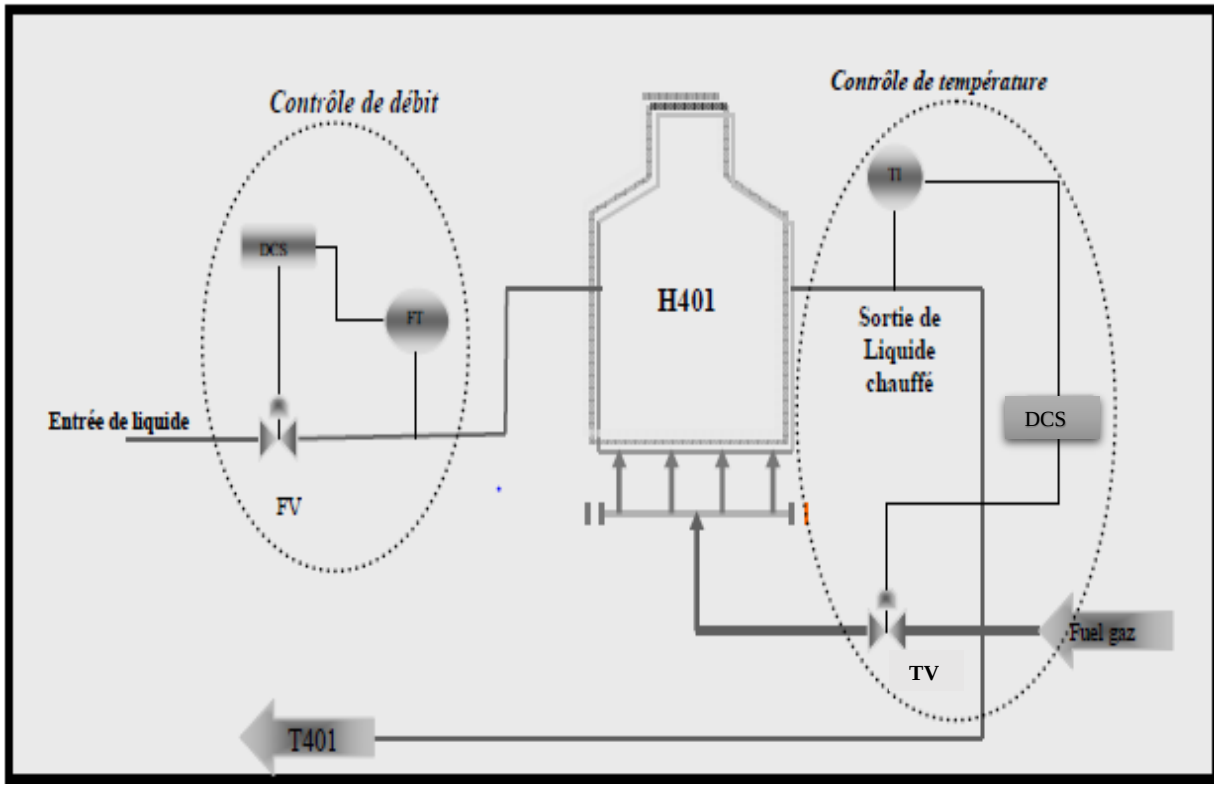


Figure III.5 : Système de contrôle dans le four H401

Ce système de contrôle comprend :

- un capteur de température (TI)
- un capteur de débit (FT)
- vannes de régulation de température et débit (TV, FV)
- automate de régulation

Le contrôle de débit de liquide à l'entrée du four, se fait par un système de contrôle qui comprend un débitmètre (FT) pour mesurer le débit du liquide et qui envoie le signal à salle de contrôle (DCS), pour alerter l'opérateur humain par une alarme (FALL) au cas où le débit de liquide est bas 530m^3 /h et le faire intervenir manuellement sur la vanne (FV).

Le contrôle de température de liquide chauffé à la sortie du four, se fait par un système de contrôle qui comprend, un thermocouple comme indicateur de température (TI) qui va envoyer le signal à la salle de (DCS) et alerter l'opérateur par une alarme (TAHH) à 320°C pour qu'il intervienne sur la vanne (TV).

III.3.3. Sous-système d'alarme

Dans le cas où le système de contrôle tombe en panne, c'est-à-dire n'exécute pas sa fonction, le système d'alarme peut être utilisé pour alerter les opérateurs pour qu'ils interviennent afin de rendre le système à l'état stable.

Sous-système (SS)	**Equipement (E)**	**Composant (C)**
SS3 : d'alarmes [Alerter l'opérateur par un signal audio-visuel]	**E31 :** TAH [alarme de haute température du fluide à chauffer]	**C311 :** Thermocouple TI [Mesure la température du liquide à la sortie du four]
		C312 : DCS [Adaptation de la mesure de haute température à une alarme audio-visuelle]
	E32 : FAL [alarme de bas débit du liquide 530m^3/h]	**C321 :** Débitmètre FT [Mesure le débit du liquide à l'entrée de four]
		C322 : DCS [Adaptation de la mesure de bas débit à une alarme audio-visuelle]
	E33 : PAL/H [alarme de basse et haute pression de fuel gaz (300 g/cm^2) / (1Kg/cm^2)]	**C331 :** Pressostat PSL [mesure la pression de fuel gaz]
		C332 : DCS [Adaptation de la mesure de basse pression à une alarme audio-visuelle]

Tableau III.3- Sous système d'alarme

III.3.4. Sous-système d'arrêt d'urgence (système instrumenté de sécurité)

Le système d'ESD (Emergency Shut Down), consiste à assurer l'arrêt total du four H401 en cas de perturbation de système de contrôle, de détection d'une anomalie ou d'autres conditions potentiellement dangereuses du procédé, afin de protéger le personnel, les équipements et l'environnement.

Le système d'ESD (système d'arrêt d'urgence) se compose de capteurs, d'unité de traitement et d'actionneurs.

Le système d'ESD est un système complètement autonome qui est destiné uniquement à l'arrêt d'urgence. Il intervient dans les cas suivants :

Température

- Très haute température du fluide à chauffer : TAHH : 320 °C.
- Très haute température dans la cheminée : TAHH : 550 °C.

Débit bas du fluide à chauffer

Le seuil bas de débit du liquide est un facteur de déclenchement du four, plus ce débit décroît, plus la température du liquide augmente :

- Alarme de très bas débit : FALL : 380 m^3/h.

Pression du fuel gaz

Les seuils bas et haut de pression de fuel gaz sont des facteurs de déclenchement du four

- Alarme de très basse pression : PALL : 150g/Cm^2.
- Alarme de très haute pression : PAHH : 1.3Kg/Cm^2.

III.3.4.1. Les capteurs

Chaque facteur de déclenchement possède un seul capteur, ce dernier est destiné à mesurer les paramètres du procédé dans le four (température, débit, pression) puis envoyer les signaux vers l'unité de traitement.

- TSHH capteur de très haute température du fluide à chauffer.
- TI capteur de très haute température de la cheminée.
- FSLL capteur de très bas débit du fluide à chauffer.
- PSHH/LL capteur de très basse/très haute pression du fuel gaz.

III.3.4.2. Unité de traitement PLC (TRICONEX)

L'architecture adoptée sera modulaire triplée TMR, avec 03 processeurs séparés à structure de bus triplex. Tous les systèmes sont en parallèles. Chaque processeur exécutera le programme d'application simultanément et indépendamment, en vérifiant les données, en exécutant les instructions logiques et contrôle les signaux.

La technologie TMR (Triple Modular Redundant) de Triconex utilise trois systèmes de contrôle parallèles isolés et plusieurs possibilités de diagnostic intégrées dans un seul système. Le système utilise le principe de 2 sur 3 votes pour assurer une très grande intégrité, une absence d'erreur et un fonctionnement ininterrompu.

Le voteur 2 out of 3 assure un signal à la sortie s'il y a un signal sur deux voies des systèmes qui ne sont pas échoué sur les trois voies. Si l'un des trois systèmes échoue, les deux autres systèmes peuvent corriger et masquer le défaut.
Le système doit procéder automatiquement au contrôle de tous ses composants pour identifier les défaillances. Ces essais de diagnostic seront exécutés au démarrage du système et pendant son exploitation.

Lors de la détection d'une défaillance, une alarme descriptive sera générée pour signalisation visuelle.

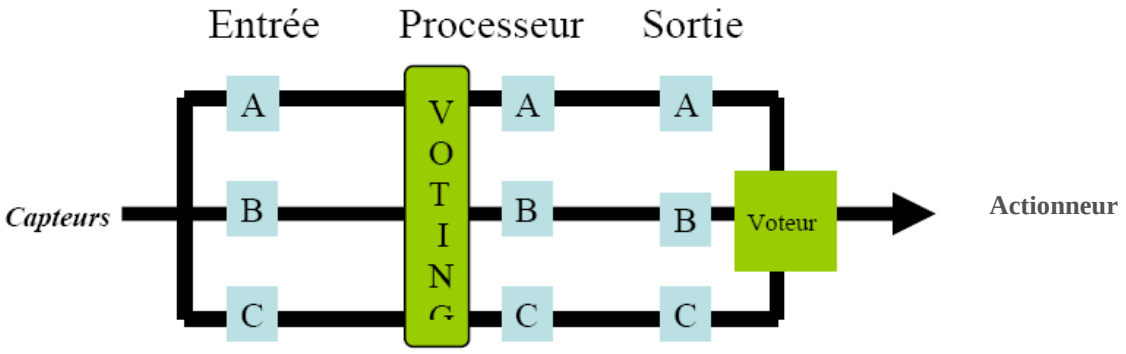


Figure III.6 : Architecture 2oo3 de PLC

III.3.4.3. Les actionneurs

Ce sont des 02 électrovannes (tout ou rien) en parallèle commandées par le PLC.
En cas d'existence de facteur de déclenchement, on observe la fermeture des vannes (FV1, FV2) pour couper l'alimentation de fuel gaz.

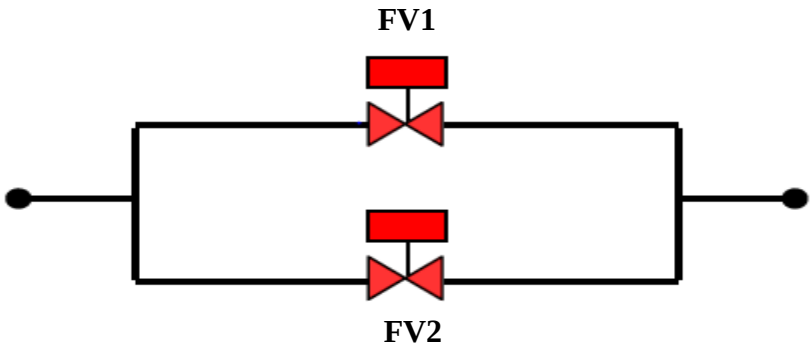


Figure III.7 : Architecture 1oo2 des vannes

III.4. Modes de défaillance des composants du SIS

Le tableau (III.4) montre les principaux modes de défaillances pouvant affecter les composants du SIS.

N°	Composants	Modes de défaillances
1	Capteurs	Indication erronée - Plus que la valeur réelle - Moins que la valeur réelle - Pas d'indication
2	PLC	- Entrées défectueuses - Sorties défectueuses
3	Vannes	- Bloquée ouverte - Fermeture intempestive

Tableau III.4- Principaux modes de défaillance des composants

III.5. Calcul du PFDavg du SIS par les équations simplifiées

Pour calculer les PFD_{avg} de notre SIS, nous avons utilisé les expressions obtenues par les équations simplifiées.

La méthode des équations simplifiées est la méthode qui est utilisée par les industriels.

Tous les calculs effectué concernent le SIS décrit par le schéma suivant :

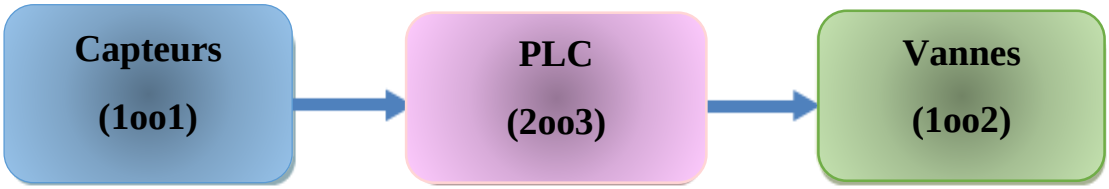


Figure III.8 : Schéma du SIS

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.

Les différentes données nécessaires au calcul ont été tirées des banques de données OREDA 2002 [ORE 02], et PDS Data Handbook 2004[PDS, 2004].

Nous rappelons que :

DC : le taux de couverture de diagnostic $\mathrm{DC} = \frac{\sum \lambda_{DD}}{\sum \lambda_{D}}$;

λ_D : Taux de défaillance $\lambda_D = \lambda_{DU} + \lambda_{DD}$;

λ_{DU} : Taux de défaillance dangereuse non détecté ;

λ_{DD} : Taux de défaillance dangereuse détecté ;

MTTR : Indice de maintenabilité (Mean Time To Repair) $\mathrm{MTTR} = \frac{\text{Temps d'arrêt total}}{\text{Nombre d'arrêts}}$;

DC=60%				
Paramètre / Composant	λ_D **(1/h)**	λ_{DD} **(1/h)**	λ_{DU} **(1/h)**	**MTTR (h)**
Capteur	1.5×10^{-6}	0.9×10^{-6}	0.6×10^{-6}	**9.8**
Vanne	2.7×10^{-6}	1.62×10^{-6}	1.08×10^{-6}	**12**
PLC	10^{-8}	0.6×10^{-8}	0.4×10^{-8}	**10.2**

Tableau III.5- Valeurs des taux de défaillance, et de la MTTR pour DC=60%

DC=90%				
Paramètre / Composant	λ_D **(1/h)**	λ_{DD} **(1/h)**	λ_{DU} **(1/h)**	**MTTR (h)**
Capteur	1.5×10^{-6}	1.35×10^{-6}	0.15×10^{-6}	**9.8**
Vanne	2.7×10^{-6}	2.43×10^{-6}	0.27×10^{-6}	**12**
PLC	10^{-8}	0.9×10^{-8}	0.1×10^{-8}	**10.2**

Tableau III.6- Valeurs des taux de défaillance, et de la MTTR pour DC=90%

DC=99%				
Paramètre / Composant	λ_D **(1/h)**	λ_{DD} **(1/h)**	λ_{DU} **(1/h)**	**MTTR (h)**
Capteur	1.5×10^{-6}	1.49×10^{-6}	0.015×10^{-6}	**9.8**
Vanne	2.7×10^{-6}	2.67×10^{-6}	2.7×10^{-8}	**12**
PLC	10^{-8}	0.99×10^{-8}	9.9×10^{-11}	**10.2**

Tableau III.7- Valeurs des taux de défaillance, et de la MTTR pour DC=99%

Les formules de PFDavg obtenues par la méthode des équations simplifiées [HAB 03]

$$\mathrm{PFD}_{\mathrm{avg}}^{1oo1} = \lambda_{DU}.\frac{T_1}{2}\ ,\ \mathrm{PFD}_{\mathrm{avg}}^{1oo2} = \frac{1}{3}\left(\lambda_{DU}.\frac{T_1}{2}\right)^2,\quad \mathrm{PFD}_{\mathrm{avg}}^{2oo3} = \left(\lambda_{DU}.\frac{T_1}{2}\right)^2$$

	Capteur 1oo1		**PLC 2oo3**		**Actionneur 1oo2**		**Système SIS**	
	PFD	**SIL**	**PFD**	**SIL**	**PFD**	**SIL**	**PFD**	**SIL**
DC=60%	0.001314	**2**	0.76E-10		1.867E-6		0.0013	**2**
DC=90%	3.285E-4	**3**	4.796E-12		1.165E-7		3.285E-4	**3**
DC=99%	3.285E-5	**4**	0.47E-13		1.165E-9		3.28E-5	**4**

Tableau III.8- Calcul du PFDavg par les équations simplifiées

- Sachant que : T1=4380h,

Le tableau III.8 montre la diminution de défaillance dangereuse pour un DC de 60%, 90% et 99% correspondant respectivement à un SIL 2, 3 et 4. Nous constatons que la variation du taux de couverture de diagnostic implique une variation du niveau de SIL du système. Nous avons pu retenir ses résultats :

- L'augmentation du DC fait diminuer la PFD.
- La PFDavg du SIS étudié est influencée par la PFD du capteur car le SIS est composé d'un seul capteur (1oo1).
- L'élément critique dans le SIS est le capteur.

III.6. Conclusion

Dans ce chapitre nous avons utilisé la méthode des équations simplifiées pour montrer comment et sous quelles hypothèses on pouvait utiliser les formules analytiques proposées dans la norme. La méthode des équations simplifiées (normes IEC 61508) a été utilisée pour évaluer la PFDavg du SIS du four rebouilleur. Nous avons pu obtenir les résultats suivants :

- La PFDavg du SIS étudié est influencée par la PFD du capteur car le SIS est composé d'un seul capteur (1oo1)
- Selon le concepteur, le SIS du four rebouilleur est certifié SIL2 ; ce qui correspond, selon les résultats obtenus par la méthode utilisée, à une PFDavg de l'ordre de 10^{-3}pour un DC=60%. Or cet ordre est pratiquement donné par la valeur de la PFDavg du capteur qui constitue à cet égard un élément critique pour le SIS.

Conclusion générale

Dans ce mémoire, nous avons évoqué la problématique de la sécurité dans les procédés industriels. Nous avons étudié les notions clés comme la sécurité et la sécurité fonctionnelle. Ensuite, nous avons présenté les systèmes instrumentés de sécurité.

Les systèmes instrumentés de sécurité sont utilisés pour détecter des situations dangereuses et atténuer leurs conséquences pour atteindre des niveaux de risques tolérables.

Les industries qui mettent en œuvre un SIS, doivent le faire conformément aux règles et recommandations définies par la norme CEI 61511.Nous avons précisé l'organisation de la norme CEI 61508 pour les systèmes de sécurité, ainsi que sa norme fille CEI 61511 pour les systèmes de sécurité dans l'industrie des procédés.

Ces normes de sécurité fonctionnelle introduisent une approche probabiliste pour l'évaluation quantitative de la performance du SIS et la qualification de cette performance par des niveaux de sécurité références.

Nous avons introduit les probabilités dans la mesure de niveaux d'intégrité, cela a entrainé la mise en place de nouveaux concepts tels que les notions de calculs de probabilité moyenne de défaillance à la sollicitation *PFDavg* ou de défaillance par unité de temps. Différentes techniques sont néanmoins préconisées dans les annexes de la norme sans toutefois exclure toute méthode pertinente de calcul probabiliste. Parmi les méthodes citées, on trouve les équations simplifiées. La performance que nous avons calculé permet alors de qualifier le niveau SIL du SIS selon les niveaux définis par la norme qui en sont l'un des points clés. Cette évaluation s'apparente à un calcul d'indisponibilité de la fonction de sécurité.

D'autre part, comme les budgets d'investissement, d'exploitation et de maintenance sont des points sensibles dans l'industrie, on doit réduire les couts de maintenance en intégrant les SIS aux systèmes basiques de contrôle de procédé, avec des outils d'ingénierie communs au BPCS (DCS) et SIS (Triconex).

L’objectif du dernier chapitre était d’évaluer la performance au sens probabiliste des systèmes instrumentés d’un four rebouilleur.

Nous avons utilisé la méthode des équations simplifiées (normes IEC 61508) pour évaluer la PFDavg du SIS du four rebouilleur. Mais au préalable, une revue détaillée des équations simplifiées pour les architectures constituant ce SIS a été réalisée. Nous avons pu obtenir le résultat suivant : Selon le concepteur, le SIS du four rebouilleur est certifié SIL2, ce qui correspond, selon les résultats obtenus par la méthode utilisée à une PFDavg de l’ordre de 10^{-3} pour un DC=60%. Or cet ordre est pratiquement donné par la valeur de la PFDavg du capteur qui constitue à cet égard un élément critique pour le SIS.

Nous avons conclu à la nécessité d’augmenter la disponibilité de cet élément. Pratiquement, une architecture 1oo2 pour le sous-système « capteurs » permet le passage d’un SIL2 vers un SIL3 pour la fonction de sécurité du SIS.

RÉFÉRENCES

[Bait 11] S. Baitiche : « La gestion des niveaux de sécurité intégrée (System Integrated Level) dans un procédé au niveau du GL2Z ». Thèse Magister soutenue à l'école doctorale de la gestion des risques industriels et environnement d'Oran, 2011.

[CHER 10] L. chergui : « Diagnostic des Défaillances et Optimisation des Architectures des Systèmes Instrumentés de Sécurité : Apport de la Logique Floue ». Thèse Magister soutenue à l'institut d'Hygiène et Sécurité de Batna- Spécialité- Gestion Du Risque, 2010.

[CEI 03] CEI 61511, Sécurité fonctionnelle des systèmes instrumentés pour les industries de Process. Commission Electrotechnique Internationale, Genève, Suisse 2003.

[CEI 00] CEI 61508. Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité. Commission Electro technique-International, Genève, Suisse, 2000.

[CEI 61508 98] IEC61508, Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems. International Electrotechnical Commission (IEC), 1998.

[DEI O2] DEI SVALDI, D. et M. KNEPPERT. Gestion des fonctions de sécurité par automate programmable dédié à la sécurité (APIdS), Coll. Notes scientifiques et techniques de l'INRS, 224, Paris, Institut national de recherche et de sécurité (INRS), 2002, 24 p.

[F.BOUS 13] F.Bouslimani : « Systèmes Automatiques de Sécurité Dans L'Industrie Des Procèdes ». MFE soutenu à la Faculté des Hydrocarbures et de la Chimie de Boumerdes – Spécialité Commande des Procédés Industriels, 2013.

[INRS 04] Institut national de recherche et de sécurité (INRS), Paris, 2003, 35 p. en santé et en sécurité du travail (IRSST), 2004, 11 p.

[PIE 11] Pierre David Pierre sureté de fonctionnement : Norme SIL, Copyright, 2011, 29p.

[PAQ 91] PAQUES, Joseph-Jean. Règles sommaires de sécurité pour l'utilisation des automates programmables industriels *(API)*, Rapport B-028, Montréal, Institut de recherche Robert- Sauvé en santé et en sécurité du travail (IRSST), 1991, 19 p.

[HAB 03] Dr.Habil. Josef Börcsök Prof-Ing HIMA Comparison of PFD calculation, 2003.

[HAD 14] F.Hadjaz : Description Général De l'instrumentation et de la Maintenance de MPP0 Rapport de stage de la Licence dans le Module MPPO, Hassi R'mel, juin 2014.

[ISA 96] ISA, Application of Safety Instrumented Systems for the process Industries, ANSI / ISA-S84.01, 1996.

[KNE 02] B.Knegtering,Safety lifecycle management in the process industries:the development of a qualitative safety-related information analysis technique.Phd thesis, Technische Universiteit Eindhoven,2002.

[KED 03] A.Keddici et K.Guehfez : « Etude de la boucle cascade LIC4011/FIC4011 Niveau Fond Du Dé-éthaniseur T401 Train 1 MPP0 Hassi R'mel », MFE soutenu à la Faculté des Hydrocarbures et de la Chimie de Boumerdes – Spécialité Commande des Procédés Industriels, 2003.

[MKH 08] A.Mkhida. « Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence». Thèse de Doctorat soutenue à l'Université de Nancy. Le 14 novembre 2008.

[MEC 11] W.Mechri. Evaluation de la performance des systèmes instrumentés de sécurité à paramètres imprécis. Thèse de Doctorat. Avril 2011.

[OREDA, 2002] Offshore reliability data handbook. OREDA, 2002.

[OHS 99] OHSAS18001, Système de management de la santé et de la sécurité au travail-Spécification - BSI, Afnor, 1999.

[PDS, 2004] Reliability Data for safety instrumented systems.PDS data handbook, September 2004.

[PRO 11] : PROFLUID, le SIL Safety Integrity Level Niveau d'intégrité de sécurité, Guide SIL, 2011.

[RAB 13] B.Rabah : « Etude de l'implémentation des Systèmes Instrumentés de Sécurité par des méthodes semi-quantitatives dans un environnement de connaissances imparfaites ».Thèse Magister soutenue à l'institut d'Hygiène et Sécurité de Batna-Spécialité- Gestion du Risque ,2013.

[SEK 13] S .Sekiou : « Diagnostic des Défaillances des Systèmes Instrumentés de Sécurité : Simulation et Etude Expérimentale ». Thèse Magister soutenue à l'institut d'Hygiène et Sécurité Industrielle de Batna–Spécialité Gestion de Sécurité ,2013.

[SAL 07] M.Sallak : « Évaluation de paramètres de sureté de fonctionnement en présence d'incertitudes et aide à la conception : application aux systèmes instrumentés de sécurité ». Thèse de Doctorat soutenue à l'Ecole doctorale IAEM lorraine, 19 octobre 2007.

[SAL 06b] Sallak, M., Simon, C., and Aubry. J.-F, Evaluating safety integrity level in presence of uncertainty. In KONBIN, the 4th International Conference on Safety and Reliability, Krakow, Poland, 2006.

[VIL 80] A.Villemeur, Sûreté de fonctionnement des systèmes industriels, Eyrolles, 1988.

COURS INVENSYS TRICONEX ADAPTE Document SONATRACH.
COURS SNCC/DCS Document SONATRACH.
WWW. TRICONEX.COM Triconex General Purpose Invensys.