République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Ecole Nationale Polytechnique

Mémoire De Master en Sécurité industrielle
Spécialité : QHSE-GRI

Intitulé

Influence des automates programmables (solveur) sur un des critères de la performance des Systèmes Instrumentés de Sécurité

Système d'Arrêt d'Urgence Automatique du four rebouilleur H201
Train 1, Module1, Division Production,
Sonatrach, Hassi R'mel

Etudié par : **M^elle ASSADI Meriem**
Proposé par : **M^r M CHATTI**
Encadré par : **Mme K DJOUADI**
M^r M CHATI

Promotion Octobre 2015

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

Remerciements

Nous tenons à remercier l'équipe de SONATRACH à HASSI R'MAL pour nous avoir accueilli au sein de son établissement.

Egalement, nous remercions Mme DJOUADI et Mr CHATI pour la confiance qu'ils nous ont accordée en encadrant notre Master. Les conseils avisés nous ont guidés tout au long de ce travail.

Nous exprimons notre gratitude à l'égard de Mme HARIK Enseignante à l'Ecole Nationale Polytechnique d'Alger d'avoir accepté la présidence de notre jury, Et de monsieur BOUSBAI Mohamed, de nous avoir fait l'honneur de faire partie de notre jury de master.

Nous souhaitons remercier l'ensemble de nos professeurs de l'Ecole Nationale Polytechnique d'Alger pour la formation qu'ils nous ont assuré.

Nous remercions enfin tous nos proches pour leur soutien constant et pour l'atmosphère chaleureuse et rassurante qu'ils ont su créer autour de nous, pendant notre stage.

Dédicace

Je dédie ce travail

A mes parents, mon frère et mes sœurs.

A ceux qui m'aiment.

A ceux que j'aime

Meriem…

ملخص

في مجال سلامة الاجهزة والانظمة، ظهرت معايير جديدة على النظام الكهربائي والإلكتروني والبرمجي الالكتروني، مثل المعيار العام للجنة الكهرو تقنية الدولية رقم 61508 والمعايير الاخرى الخاصة بها كالمعيار الخاص بمجال الصناعة رقم61511 والاخر رقم 62061، والتي تهدف إلى قياس احتمال الفشل الخطير عند الطلب، وقياس فشل الأجهزة في النظام. هذا التقييم الكمي هو واحد من الطرق التي يصنف بها مستوى السلامة الامنية للأنظمة، ويعتبر هذا الأخير أحد أهم المعايير المكرسة لتقييم أداء أنظمة السلامة المجهزة.

ويهدف هذا العمل إلى مقارنة تقييم أداء اثنين من اليات الإيقاف في حالات الطوارئ للفرن ه 201، القطار 1، الوحدة 1، قسم الانتاج الخاص بسوناطراك حاسي الرمل. النظامين متطابقين(في النظام الفرعي للكشف والنظام الفرعي للتنفيذ) لكن يختلفان في وحدة المعالجة منطقية.

سوف نقوم بتقييم أداء اثنين من أنظمة السلامة المجهزة وذلك من خلال مستوى سلامة الامنية، النظامين يختلفان في نوع وحدة المعالجة منطقية للبيانات المستعملة. النوع المستعمل في النظام الاول فيستند على المنطق السلكي، و النوع المستعمل في النظام الثاني فيسمى بالتريكونكس.

الكلمات البحث أنظمة السلامة المجهزة، وحدة المعالجة منطقية للبيانات، اللجنة الكهرو تقنية الدولية رقم 61508 رقم61511 ورقم62061، معيار، مستوى سلامة الامنية، تقييم، اليات الإيقاف في حالات الطوارئ...

Résumé

Dans le domaine de la sécurité des machines, de nouvelles normes sont apparues relatives au système Electrique, Electronique et Electronique Programmable E\E\EP. Nous citons, la norme générique CEI 61508 et les normes sectorielles : CEI 61511 et CEI 62061, qui visent à quantifier la probabilité de défaillance dangereuse (PFD), des pannes matérielles d'un système. Cette quantification est un des moyens qui permet de classer les systèmes par niveau de sécurité (SIL), ce dernier est considéré comme un des critères les plus importants pour l'évaluation de la performance des Systèmes Instrumentés de Sécurité.

Ce travail vise à comparer l'évaluation de la performance de deux systèmes d'arrêt d'urgence automatique (ESD) du four rebouilleur H201, Train 1, Module 1, de la Division de Production (DP) à SonatracH Hassi R'mel. Les deux systèmes sont identiques (au niveau du sous-système de détection et du sous-système d'exécution) mais ils diffèrent au niveau de l'unité de traitement logique (PLC).

Nous allons évaluer la performance du SIS des deux systèmes par le niveau de sécurité (SIL), en utilisant deux unités différentes de traitement des données logiques, le premier type est basée sur la logique câblée (système de sécurité à relais) et le 2eme type d'unité est appelé système Triconnex.

Mot clé : SIS, CEI 61508, CEI62061, norme, SIL, unité de traitement logique, arrêt d'urgence.
Mot clé : SIS, CEI 61508, CEI62061, norme, SIL, unité de traitement logique, arrêt d'urgence.

Abstract

In the field of machine safety, new standards have emerged on the Electrical System, Electronics and Electronic Programmable E \ E \ EP, as the generic standard IEC 61508 and its industry standards: IEC 61511 and IEC 62061, that aim to quantify the Probability of dangerous Failure on Demand, called PFD, hardware failures in a system. This quantification is one of the ways that classifies systems security level: Safety Integrity Level (SIL), the latter is considered as one of the most important criteria devoted to assessing the performance of Safety Instrumented Systems.

This work aims to compare the performance evaluation of two automatic emergency shutdown systems (ESD) of the oven reboiler H201, Train 1, Unit 1, Production Division (PD) Hassi R'Mel to Sonatrach. The two systems are identical (at the detection subsystem and execution subsystem) but they differ in the Processing Logic Unit (PLC).

We will evaluate the performance of the SIS of the two systems by the Security Level (SIL), using two different units of processing binary data, the first type is based on wired logic (safety relay system) and second Type unit is called Triconnex system.

Key words: SIS, IEC 61508, IEC62061, Standard, Safety Integrity Level, PLC, ESD, Influence.

Liste des figures

Liste des tableaux

Abréviations et Acronymes

API	Automate Programmable Industriel.
BTS	Barrières Techniques de Sécurité.
CA	Courant alternatif.
CC	Courant continu.
CCPS	Center for Chemical Process Safety (Centre de la sécurité de procédés chimiques).
CEI / IEC	Commission Electrotechnique Internationale (International Electrotechnical Commission).
CPU	Control Processing Unit (Unité Centrale de Traitement).
DC	Diagnostic Coverage (Couverture du Diagnostic).
DCS	Distributed Control System (Système de contrôle distribué).
DNV	Det Norske Veritas.
E/E/EP	Systèmes Electrique, Electronique et Electronique Programmable.
ESD	Emergency Shut Down (système d'arrêt d'urgence).
FALL	Flow Alarm Low Low (Alarm de Trés Bas Debit).
FT	Flow Transmettre (Transmetteur de Débit).
FV	Flow Valve (Vanne de Débit).
GPL	Gaz de Pétrole Liquéfié.
GRIF	Graphiques Interactifs pour la Fiabilité.
HRM	Hassi R'Mel.
HSE	Health Safety & Environment (Sécurité Santé & Environnement).
INERIS	Institut National de l'Environnement Industrielles et des RISques.
MPP	Module Processing Plant (Module de traitement et de production).
MPP1	Module Processing Plant one (Module de traitement et de production N :01) .
MTTR	Mean Time To Repair (durée moyenne de réparation).
NF	Norme Française.
OREDA	Off-shore Relaibility Data base (Base de données de la fiabilité extracôtiers).
P&ID	Piping and Instrumentation Diagram (Schéma de la tuyauterie et de l'instrumentation).
PAH	Pressure Alarm High (Alarm de Haute Pression).
PAHH/LL	Pressure Alarm High High/Low Low (Alarm de Trés Haute /Trés Bas Pression).
PAL	Pressure Alarm Low (Alarm de Bas Pression).
PFD	Probability of Failure on Demand (probabilité de défaillance à la demande).
PFD_{avg}	Average Probability of Failure on Demand (Probabilité de Défaillance moyenne à la Demande).

PFD_{max}	Probability of Failure on Demand-Max(Probabilité de défaillance sur la demande maximale).
PI	Pressure Indicator (Indicateur de pression).
PLC	Programmable Logic Controller (Contrôleur Logique programmable).
PSH/L	Pressure Switch High/Low (switch de Haute/Bas Pression).
PT	Pressure Transmitter (Transmetteur de pression).
RRF	Risk Reduction Factor (facteur de réduction du risque).
SDV	Shutdown Valve (Vanne d'arrêt).
SH	SonatracH.
SIF	Safety Instrumented Function (fonction instrumentée de sécurité).
SIL	Safety Integrity Level (niveau d'intégrité de sécurité).
SIS	Safety Instrumented System (Système Instrumenté de Sécurité).
SOE	Sequence Of Event (données séquence d'événement).
TAH	Temperature Alarm High (Alarm de Haute Temperature).
TAHH	Temperature Alarm High High (Alarm de Trés Haute Temperature).
TI	Temperature Indicator (Indicateur de Pression).
TMR	Triplée Modulaire Redondantes.
TV	Temperature Valve (Vanne de Température).
λ	Taux de défaillance d'un canal.
λ_D	Taux de défaillance dangereuse du canal.
λ_{DD}	Taux de défaillance dangereuse détectée du canal.
λ_{DU}	Taux de défaillance dangereuse non détectée du canal.

Table des matières

Introduction

La démarche de maîtrise des risques vise la réduction des risques existants à travers l'interposition des Barrières de Sécurité. Etant une Barrière Technique de Sécurité (BTS), les Systèmes Instrumentés de Sécurité (SIS) ont pour objectif la détection des déviations pouvant mener à un accident, la mise en œuvre des mesures nécessaires pour conduire à la mise en sécurité des équipements critiques.

Plusieurs documents normatifs ont été élaborés pour guider les constructeurs des SIS dans leur démarche de validation. Parmi ces normes, la norme générique de la Commission Européenne Internationale - CEI 61508 [1], qui est un référentiel, relatif à la sécurité fonctionnelle des systèmes Electrique, Electronique et Electronique Programmable E/E/EP, et la norme sectorielle CEI 61511 (norme fille de la CEI 61508), qui représente un document normatif pour la conception et l'exploitation des SIS.

Pour évaluer la performance des Systèmes instrumentés de sécurité-SIS, dans ce travail, nous allons évaluer l'influence de l'un des composants du système d'arrêt d'urgence automatique du four reboullieur H201 (Train 1 – Module 1 – Division Production, SonatracH Hassi R'mel) sur un des critères de l'évaluation des SIS, représenté par le niveau d'intégrité de sécurité – SIL [2].

C'est dans ce contexte que s'inscrit notre travail, dont l'intitulé est « **Influence des automates programmables (solveur) sur un des critères de la performance des Systèmes Instrumentés de Sécurité –** cas du système d'arrêt d'urgence automatique des brûleurs du rebouilleur H201, train 1, module1 SONATRACH, Hassi R'mel ».

La démarche adoptée pour le traitement de ce projet est repartie en deux parties :

Chapitre 1 : Dans cette partie nous allons définir toutes les notions relatives aux SIS (leurs définitions, mode de fonctionnement, constitution,…) et aux automates programmables (type, mode de fonctionnement, avantages et inconvénients,...),

Chapitre 2 : Le 2ème chapitre a pour objectif l'évaluation du SIL du même système d'arrêt d'urgence en utilisant deux types d'unité de traitement : les relais de sécurité et le Tricon. Une comparaison des résultats obtenus sera ensuite réalisée.

Chapitre I : Etude sur les automates programmables

1. Système Instrumenté de Sécurité

1.1. Définition

D'après la norme CEI 61508 [1], un SIS fait l'objet de la définition suivante : « c'est un système E/E/PE relatif aux applications de sécurité, il comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité».

1.2. Approche normative

Les normes relatives au sujet traité qui vise les machines, les SIS et les API, sont des normes sectorielles (filles) de la norme générique référentiel CEI 61508 dédiée aux systèmes E\E\EP. Dans les parties suivantes nous avons définies brièvement chacune de ces normes.

1.2.1. CEI 61511

La norme sectorielle CEI 61511 [3] est l'une des normes filles de la norme générique CEI 61508, elle est relative à l'industrie du process. Cette norme présente une approche relative aux activités liées au cycle de vie de sécurité, pour satisfaire à ces normes minimales. Cette approche a été adoptée afin de développer une politique technique rationnelle et cohérente. Dans la plupart des cas, la meilleure sécurité est obtenue par une conception de process de sécurité intrinsèque, chaque fois que cela est possible, combinée, au besoin, avec d'autres systèmes de protection, fondés sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable) et qui couvrent tous les risques résiduels identifiés.

Elle comprend trois parties :

- **CEI 61511-1** : relative au cadre, définitions, exigences pour le système, le matériel et le logiciel [3],
- **CEI 61511-2** : présente les lignes directrices pour l'application de la CEI 61511-1 [4],
- **CEI 61511-3** : conseils pour la détermination des niveaux exigés d'intégrité de sécurité [5].

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

Les applications de SIL 4 ne pouvent être traitées par un SIS seul, ce qui nécessite l'utilisation d'une fonction instrumentée de sécurité (SIF) de niveau d'intégrité de sécurité SIL 4, ces dernières sont rares dans l'industrie de process. Elles doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de la sécurité [5].

1.2.2. CEI 62061

La norme CEI 62061 [6] est spécifique au secteur des machines de traitement logique (numérique) dans le cadre de la CEI 61508. Elle est destinée à faciliter la spécification du fonctionnement des systèmes de commandes électriques relatifs à la sécurité par rapport aux dangers significatifs des machines.

Cette norme internationale est destinée à être utilisée par les concepteurs de machines, les fabricants et les intégrateurs des systèmes de commande, et autres, impliqués dans la spécification, la conception et la validation des systèmes de commande électriques relatifs à la sécurité. Elle donne les exigences nécessaires à la réalisation du fonctionnement requis. La CEI 62061 s'est limitée à l'utilisation des trois premiers niveaux d'intégrité de sécurité (SIL).

La norme CEI 62061 a été rédigée dans l'objectif de devenir une norme internationale harmonisée pour la directive Machine. Ceci a été rendu possible en réduisant le périmètre de la CEI 61508 pour n'inclure que des exigences concernant des produits. La commission européenne reconnaît implicitement que l'EN 954-1 [7] est notoirement insuffisante dès que les chaînes de sécurité des machines contiennent des automatismes programmés. Elle recommande (sans encore l'imposer) d'appliquer la CEI 62061 [8].

2. Automates Programmables

2.1.Définition

Une définition d'un API est donnée par la norme française NFC 63-850 : « Appareil électronique qui comporte une mémoire programmable par un utilisateur automaticien à l'aide d'un langage adapté, pour le stockage interne des instructions composant les fonctions d'automatisme comme par exemple :

- Logique combinatoire et séquentielle
- Temporisation, comptage, décomptage, comparaison
- Calcul arithmétique

Réglage, asservissement, régulation, etc. Pour commander, mesurer et contrôler au moyen d'entrées et de sorties (logiques, numériques ou analogiques) différentes sortes de machines ou de processus, en environnement industriel. »

D’une manière générale, un automate programmable industriel se définit comme étant une machine électronique, programmable par un personnel non informaticien et destiné à piloter, en ambiance industrielle et en temps réel, des procédés logiques séquentiels.

2.2.Historique

Les API sont apparus aux USA vers 1969 où ils répondaient aux désirs des industries de l’automobile de développer des chaînes de fabrication automatisées qui pourraient suivre l’évolution des techniques et des modèles fabriqués. L’API s’est ainsi substitué aux armoires à relais en raison de sa souplesse (mise en œuvre, évolution), mais aussi parce que dans les automatismes de commande complexe, les coûts de câblage et de mise au point devenaient trop élevés.

Ces marchés ont donné naissance aux produits de deux des plus grandes entreprises : MODICON et ALLEN BRADLEY.

Le cahier des charges de ces nouvelles machines comprenait aussi des spécifications sur les conditions d’utilisation en milieu industriel perturbé, sur la variété et le nombre des entrées/sorties industrielles, sur la simplicité de mise en œuvre par le personnel en place et naturellement sur les coûts de développement des automatismes. On écartait ainsi les autres solutions programmées traditionnelles : mini-ordinateur, etc.

2.3. Automatismes

L'automatisation d'un procédé (une machine, un ensemble de machines, ou plus généralement un équipement industriel) consiste à assurer la conduite par un dispositif technologique. Le système ainsi conçu doit prendre en compte les situations pour lesquelles sa commande a été réalisée.

L'intervention d'un opérateur est souvent nécessaire pour assurer un pilotage global du procédé (spécification de consigne, de fonctionnement), pour surveiller les installations et reprendre en commande manuelle tout ou une partie du système en cas de nécessité.

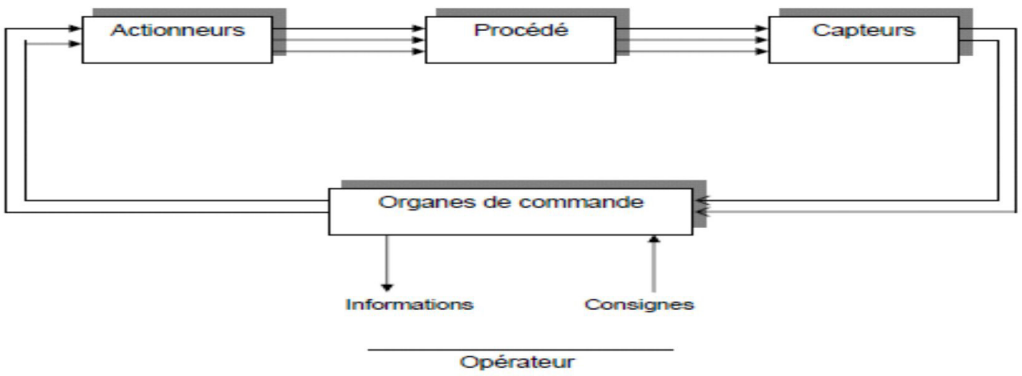

Figure 1.1 - Schéma fonctionnel d'une installation automatisée

2.3.1. Objectif de l'automatisation

La compétition économique impose à l'industrie de produire en qualité et en quantité pour répondre à la demande dans un environnement très concurrentiel, ces objectifs sont :

- Produire à qualité constante ;
- Fournir les quantités nécessaires ;
- Augmenter la productivité.

D'une manière générale, il est important de chercher la diminution des coûts de fabrication. Au quel il convient d'ajouter l'amélioration des conditions de travail.

2.3.2. Fonctions de l'automatisme

Le degré d'automatisation d'un système est extrêmement variable suivant la nature du procédé, sa complexité, la connaissance qu'on en a et les objectifs assignés au projet. On peut distinguer trois fonctions de l'automatisme :

a. Surveillance

La surveillance de grandeurs répond à un objectif de connaissance technique et économique du procédé. Cette fonction est passive au moins dans les très courts termes. L'organe de contrôle reçoit des informations, les analyses et produits des journaux de bord et des bilans.

b. Mode guide opérateur

Cette fonction complète la précédente par des traitements plus élaborés et propose aux responsables du site des actions pour conduire le procédé suivant un critère donné.

c. Commande

Cette fonction a une structure en boucle fermée. Elle correspond à l'automatisation complète de certaines fonctions, depuis l'acquisition des informations, en passant par leur traitement, pour aboutir à une action sur le procédé.

L'homme est seulement chargé des fonctions de surveillance et intervient en cas d'incident pour reprendre le pilotage manuel du procédé, éventuellement aidé par un mode "guide opérateur" correspondant à un fonctionnement dégradé du système.

Pour compléter, il faut introduire la notion de niveau d'automatisation. En effet, les fonctions précédentes sont simples ou complexes selon le procédé ou la partie du procédé auquel elles sont assignées.

Actuellement, de plus en plus, on se dirige vers des unités complètement automatisées. Eviter des systèmes lourds à mettre en œuvre et à exploiter impose une organisation hiérarchisée, répartie

et décentralisée qui permet d'utiliser des unités de traitement plus simples et plus spécialisées (DCS - Distributed Control System).

2.3.3. Technologie des automatismes

L'automaticien dispose de nombreux outils technologiques pour réaliser la commande de son système que l'on regroupe en deux catégories fondamentales :

- Les solutions câblées ;
- Les solutions programmées.

2.3.3.1. Solutions câblées

Les outils câblés sont caractérisés par une mise en œuvre nécessitant l'élaboration de liaisons matérielles (câblage) selon un schéma fourni par la théorie ou par l'expérience.

Chaque opérateur d'équations de commande booléennes est représenté physiquement par un circuit.

Les outils câblés souffrent d'un certain nombre de limitations parmi lesquelles on cite :

- Leur encombrement (poids et volume).
- Leur manque de souplesse vis à vis de la mise en point des commandes et de l'évolution de celles-ci (amélioration, nouvelles fonctions …).
- Le coût de réutilisation des composants.
- La complexité de recherche des pannes et donc de dépannage.
- Une rentabilité financière limitée aux fonctions simples.

2.3.3.2. Solutions programmées

Les outils programmés sont des outils informatiques, c'est à dire des machines destinées à traiter de l'information. Les applications techniques relèvent de l'informatique industrielle.

L'informatique industrielle est une discipline conjuguant les théories de l'automatique et les moyens de l'informatique dans le but de résoudre des problèmes de nature industrielle.

L'informatique offre une alternative technologique à l'automaticien et lui ouvre des possibilités nouvelles liées à la puissance de traitement et aux facilités de mémorisation de l'information. Pendant un certain nombre d'année cependant, l'automaticien dût se transformer en informaticien pour accéder à cette technologie. Depuis 1969 environ, il dispose enfin d'un outil spécialisé : l'automate programmable industriel (API).

2.4.Principe de fonctionnement d'un API

L'automate programmable fonctionne par déroulement cyclique du programme.

Le cycle comporte trois opérations successives qui se répètent normalement comme suit (figure 1.2) :

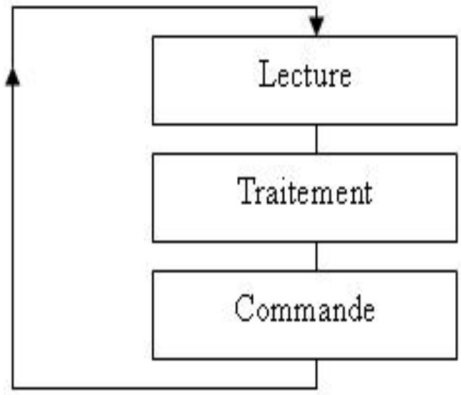

Figure 1.2 – Cycle opératoire d'un API

2.4.1. Lecture

La scrutation des entrées binaires pour transférer leurs états dans la zone image des entrées.

2.4.2. Traitement

Le processeur exécute les instructions de la mémoire programme en fonction des informations de la mémoire des données. Cette exécution se traduit par la modification de certaines variables et leur mise à jour dans la zone correspondante.

2.4.3. Commande

Les images des sorties dans la mémoire des données sont transférées dans le module de sortie pour être convertie en signaux électriques pour la commande des pré-actionneurs et des dispositifs de visualisation. Ces valeurs sont verrouillées jusqu'au cycle prochain.

Ce cycle se répète infiniment tant qu'il n'y a pas d'interruption interne ou externe qui engendre l'arrêt temporaire ou permanent de l'automate. A chaque cycle seul, l'automate fait une mise à jour de ses données en entrée, garde cet état des entrées et passe à la phase de traitement. Cette dernière nécessite un temps prédéfini pour qu'elle soit terminée. Cela dépend de la fréquence du processeur et de la technologie interne et de la nature du traitement aussi.

Une fois terminée, on est dans la troisième et finale phase de sortie, où l'automate met à jour ses signaux de sortie qui dépendent des résultats obtenus lors du traitement des entrées. Ces sorties restent figées jusqu'au prochain cycle.

Chaque fois que l'on minimise le temps d'un cycle, on améliore l'efficacité de notre automate. Malheureusement, le constructeur joue le rôle principal dans ce cas puisqu'il fixe la fréquence

interne en se référant au processeur qu'il a utilisé. Mais l'utilisateur peut minimiser ce temps écoulé en améliorant le coût de son algorithme.

2.5.Architecture matérielle

D'une manière générale, un API est constitué essentiellement de 5 modules (figure 1.3):

- L'unité centrale.
- Le module d'entrées.
- Le module de sorties.
- Le module d'alimentation.
- Le module de communication.

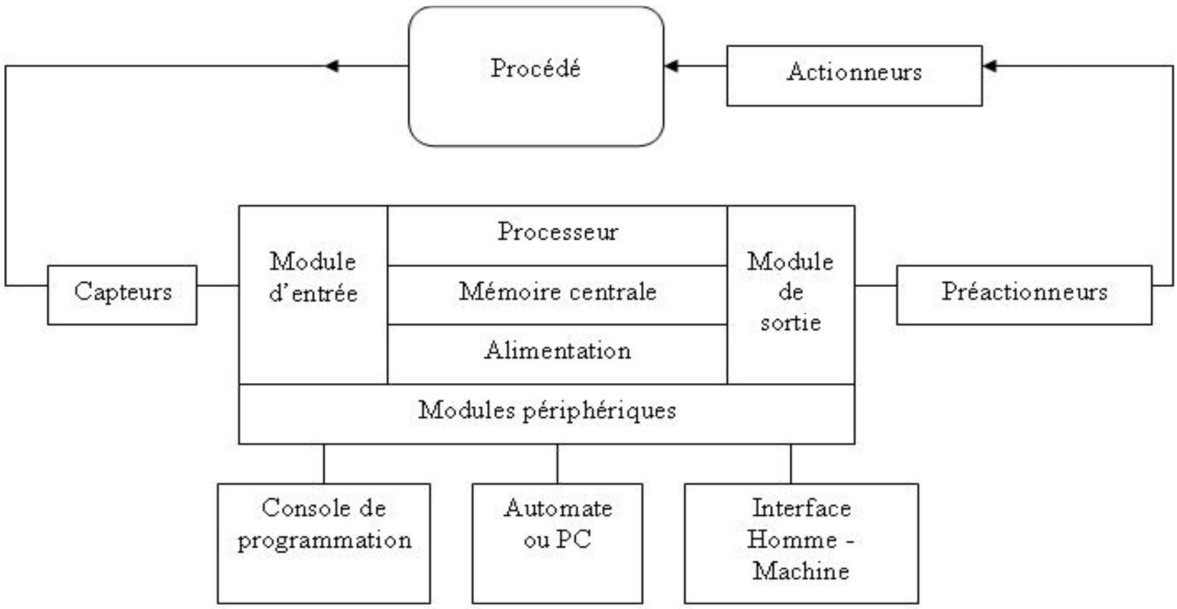

Figure 1.3 – Composition d'un API

Par la suite, nous allons détailler la composition interne d'un API (figure 1.3):

a. **Unité centrale** : constituée du processeur (cœur de l'automate) et de la mémoire centrale.
b. **Mémoire centrale** : elle contient le programme moniteur, le programme utilisateur et les données.
c. **Programme moniteur** : est un logiciel de base qui gère le fonctionnement de la machine et fourni par le constructeur.

d. **Programme utilisateur** contient les instructions du programme à exécuter. Les données sont réparties sur trois catégories :
   - Variables images des entrées.
   - Variables images des sorties.
   - Variables internes : compteurs, temporisateurs, bits internes, etc.

e. **Module d'entrée** : il transforme les signaux provenant des capteurs et des ordres de l'opérateur en signaux compréhensibles par l'automate. Le processeur stocke ensuite ces informations dans la mémoire de données image des entrées afin de les mémoriser.

f. **Module de sortie** : il transmet aux pré-actionneurs et aux dispositifs de dialogue les ordres de commande et de signalisation résultants de l'exécution du programme.

Le processeur vient chercher ses ordres dans la mémoire de données image des sorties, et les transférées en module de sortie qui seront transformés en signaux électriques par la suite.

g. **Module de communication** : sert pour le dialogue entre l'automate et un autre équipement (automate, PC,....).

3. Description du TRICONEX

3.1. Principaux éléments du TRICONEX

Chaque châssis TRICON héberge les éléments suivants :

3.1.1. Modules du système

Une caractéristique importante de l'API est sa modularité. Ainsi la CPU, les modules d'entrées et ceux de sortie sont montés dans les boitiers individuels.

La modularité confère à l'API un avantage sur les systèmes de commande à relais. Un autre avantage de modularité de l'API, est sa capacité de s'adapter aux besoins de l'utilisateur. Ainsi il est possible d'ajouter des modules d'entrées/sorties au fur et à mesure que les besoins le justifient. Seule la capacité de l'API limite le nombre maximum de modules d'entrées/sorties utilisables.

Le TRICON est un automate modulaire, il dispose d'une vaste gamme de modules qui peuvent être combinés à volonté pour constituer un automate particulier adapté à une application donnée. Nous allons présenter ces principaux éléments.

a. Module d'alimentation

Chaque châssis TRICON héberge deux modules d'alimentation disposés selon une configuration redondante.

Le module d'alimentation est disponible en trois versions différentes en fonction de la puissance requise en entrées 230 Volts en CA, 120 Volts en CA et 24 Volts en CC. Les modules d'alimentation (8310 avec 24VCC) conviennent à l'alimentation des circuits internes de l'automate de même qu'à l'alimentation des circuits des capteurs et actionneurs.

b. Module processeur principal (CPU)

Un système TRICON comporte trois modules processeurs principaux, chacun contrôle l'une des trois chaines distinctes du système.

Chaque processeur principal fonctionne en parallèle avec les deux autres comme membre d'une triade. Un microprocesseur de communication d'entrées/sorties traite les données échangées entre les modules processeurs principaux et ceux de communication à travers le bus de communication.

La capacité mémoire est de 2M octets pour chaque module processeur principal modèle 3006 et de 1M octets seulement pour chaque module processeur principal modèle 3007 des systèmes TRICON mono châssis.

Ces piles garantissent l'intégrité du programme et la conservation pour une durée d'au moins six mois en cas d'absence d'alimentation de TRICON.

Les modules processeurs principaux sont alimentés par les modules d'alimentation duale via les relais d'alimentation du châssis principal.

c. Module d'entrées/sorties logique

Les modules d'entrées /sorties logique constituent les interfaces d'entrée et de sortie des signaux logiques de l'automate. Ces modules permettent de raccorder au TRICON avec les capteurs et les actionneurs.

d. Modules de communication

La communication entre systèmes sur un site industriel est essentielle c'est pourquoi, les systèmes TRICON sont conçus pour pouvoir s'adapter avec d'autres systèmes variés y compris avec d'autres systèmes TRICON, le poste TRISTATION 1131, le système numérique de contrôle centralisé SNCC (DCS) et MODBUS.

3.1.2. Châssis

Les châssis constituent des éléments mécaniques, ils remplissent les fonctions suivantes :

- Assemblage mécanique des modules.
- Distribution de la tension d'alimentation.
- Acheminement du bus du fond de panier aux différents modules.

Le TRICON peut supporter un châssis d'extension haute densité qui héberge des modules d'entrées/sorties supplémentaires.

3.1.3. Bornier

Un bornier de raccordement est un élément sur lequel s'effectue facilement le câblage des capteurs et des organes de commande.

Le bornier et son câblage transmettent les signaux d'entrées à un module d'entrée ou bien encore transmettent les signaux en provenance d'un module de sortie directement à l'organe à piloter.

Cette organisation permet de remplacer des modules d'entrées/sorties sans modifier le câblage. Les griffes du support en plastique du bornier viennent s'enticher dans les rails de montage.

3.2.Domaine d'application

L'architecture triplée modulaire, la simplicité d'emplois, la sécurité et la disponibilité font du TRICON la solution économique et conviviale pour les tâches plus diverses dans différentes applications :

- Raffinerie et production gazière.
- Chimie.
- Energie.
- Nucléaire.

Chapitre II : Unités de traitements du système d'arrêt d'urgence et leurs influences sur le SIL réel

1. Process de traitement de gaz du module 1

1.1.Présentation du module 1

Le module 1 (Figure 2.1) a été conçu, réalisé puis mis en service en 1978. Sa tâche principale est le traitement du gaz brut et la récupération du maximum de condensât associé, il est divisé en trois trains identiques. Nous allons nous intéresser uniquement au train 1 ou se trouve le four rebouilleur H201.

Figure 2.1 – MPP1 (Module 1) SH-DP-HR

1.2.Constitution du MPP1

Le module est doté d'un bloc (juste quelques mètres près des trains de traitement) oû se trouve la salle de contrôle qui assure le contrôle des trois trains à travers le système de contrôle distribué - DCS - et le département exploitation avec le bureau de l'HSE et une salle pour les réunions journalieres et le laboratoire (pour l'analyse des échantillons – ou produits).

En plus des trois trains, il y a : une unité de glycol (préparation et régénération), une unité des utilités (air instrument et service, eau ant-incendie, eau de refroidissement) et une unité de stockage (Figure 2.2).

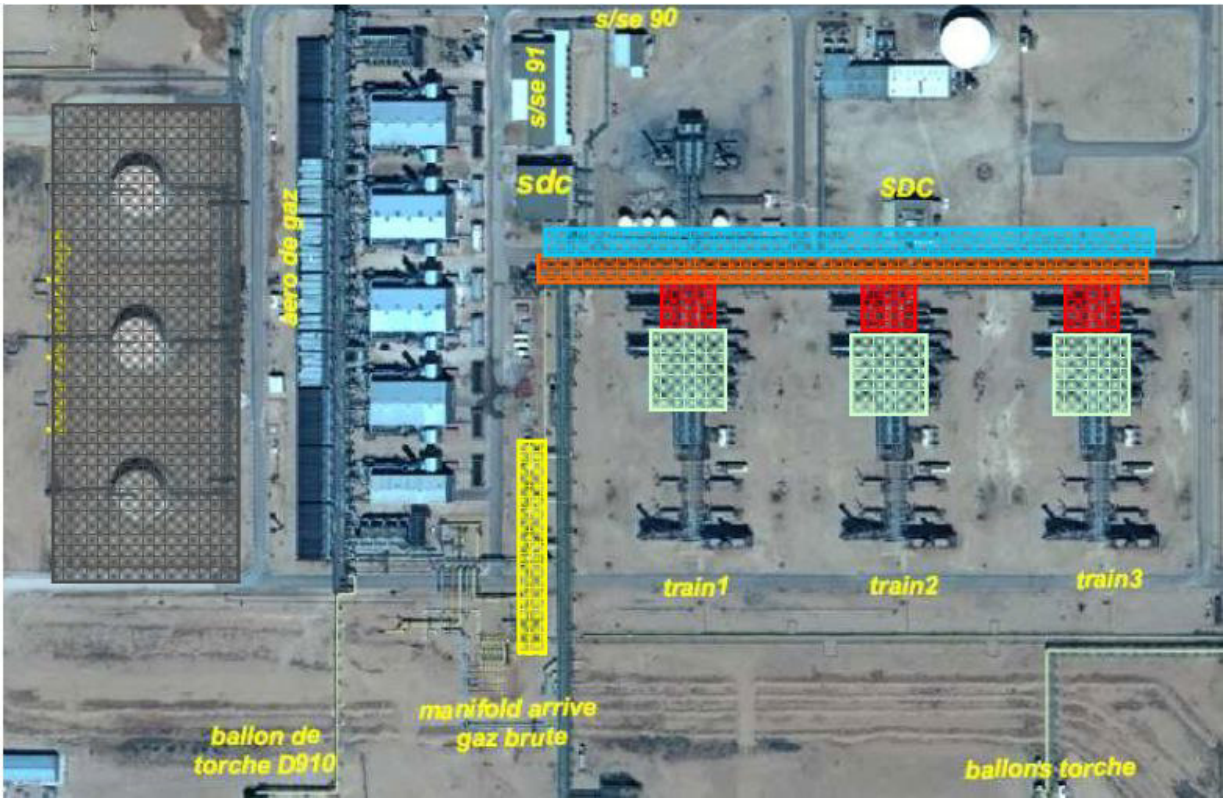

Figure 2.2 – Constitution du MPP1-SH-DP-HR (Google Earth)

1.3. Présentation du four rebouilleur H201

Le module est constitué de différentes installations (ballons de séparation, colonnes de distillation, échangeurs, fours…Figure 2.2). Ces dernières sont destinées à assurer le bon fonctionnement du traitement de gaz.

Dans ce module, le four H201 est considéré comme étant la partie la plus sensible qui joue un rôle important dans le fonctionnement du module. Cette partie de notre étude s'intéresse au système four H201 qui est composé des éléments suivantes : **four H201** (contient les éléments nécessaires à l'allumage du four : 12 pilotes et 12 brûleurs), **circuit d'alimentation fuel gaz**, **circuit condensat** et le **système de contrôle** (le tableau local – figure 2.4 et le DCS de la salle de contrôle – figure 2.3).

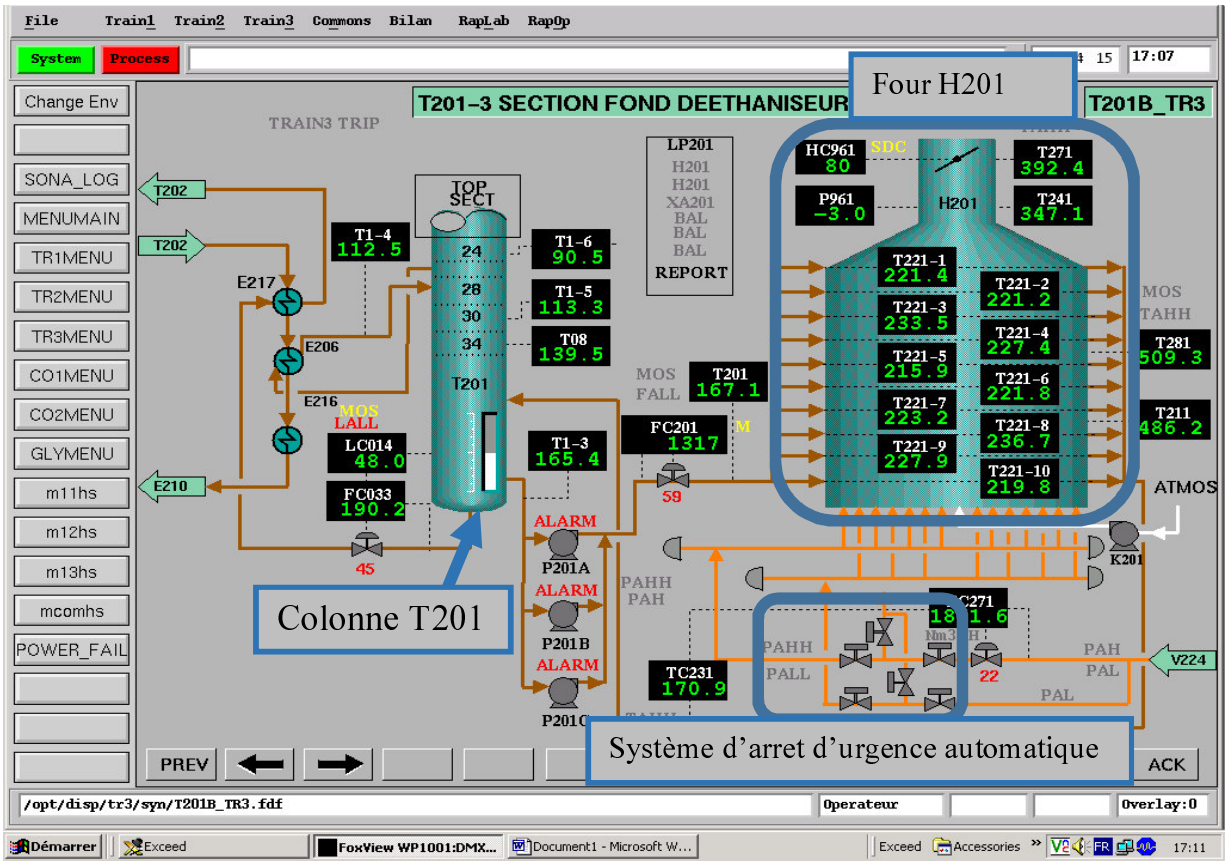

Figure 2.3 – Schéma synoptique du four H201 par le DCS de la salle de contrôle, MPP1-SH-DP-HR

Le rôle du four dans l'unité pétrolière MPP1 est d'apporter la chaleur nécessaire pour réchauffer un fluide en le portant à des niveaux de températures élevées, dans le MPP1 les hydrocarbures liquides (Condensat) du fond de la colonne T201 passent dans le rebouilleur H201 pour être chauffées de 145°C jusqu'à 180°C avant de retourner vers la colonne comme reflux chaud pour séparer les gaz légers (C_1, C_2)

Les séquences de fonctionnement et de sécurité sont assurées par un système à relais (logique câblé), et les facteurs de déclenchement sont intégrés à différents niveaux pour une protection maximale de ces équipements (tableau 2.1).

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

Tableau 2.1 – Alarmes et descriptions

Alarme	Code	Description
PAHH	201	Pression très haute gaz combustible.
PALL	201	Pression très basse combustible.
PAHH	231	Pression très haute sortie condensat.
TAHH	231	Température très haute sortie condensat.
FSLL	201	Débit très bas condensat.
TAHH	281	Température très haute entre convection / radiation.
TAHH	271	Température très haute fumées.
BAL	201	Arrêt manque de flammes.
BAL	211	Ouverture brûleur non autorisé.
BAL	221	Alarme défaut de flammes.

Ces alarmes sont regroupées sur un ensemble de verrines, au niveau de la partie supérieure du tableau local (figure 2.4), au-dessus des différents boutons poussoirs, commutateurs, voyants, utilisés pour les séquences d'automatisme.

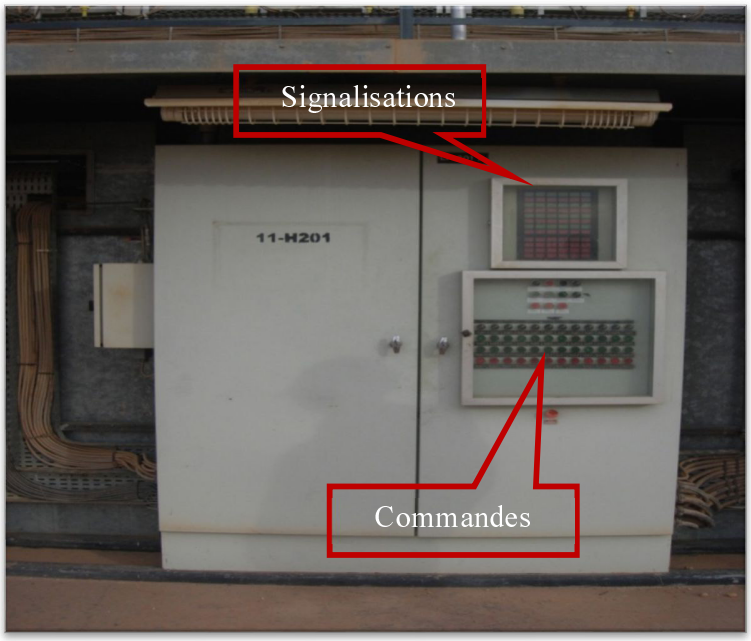

Figure 2.4 - tableau local du four H201

Les produits du fond de la T201 débarrassés du C1 et C2 sont aspirés et refoulés par la pompe (P20 4a/b) à une température de 170°C vers le four H202 ayant la même conception que le H201.

Le liquide suit le même chemin décrit pour le H201, passant par la zone de convection (370°C), zone de radiation (620°C) enfin il retourne à la colonne à une température de 185°C.

2. Description du système d'arrêt d'urgence automatique

2.1.Composition du système

La composition structurelle du système d'arrêt d'urgence automatique du four H201 est illustrée dans le tableau ci-dessous qui représente l'analyse fonctionnelle et structurelle réalisée lors de notre démarche du Projet de fin d'études_PFE [9] sur le four rebouilleur H201, cependant, nous allons juste mentionner la partie qui nous s'intéresse.

Tableau 2.2- Décomposition du sous-système d'arrêt d'urgence automatique du four H201 [9]

Système	Sous-Système(s)		Equipement(s)		Composant(s)	
	Code	**Description**	**Code**	**Description**	**Code**	**Description**
Four rebouilleur H201	**SS_1**	Sous-système d'arrêt d'urgence automatique, qui met le four à l'état d'arrêt avec la coupure de l'alimentation en fuel gaz.	**E_{11}**	**FALL 201** : alarme de très bas débit du condensat à l'entrée du four. **PALL/PAHH 201**: alarme de très basse ou très haute pression de fuel gaz. **PAHH 231 :** alarme de très haute température du condensat. **TAHH 231** : alarme de très haute température du condensat. **TAHH 281** : Température très haute entre convection / radiation. **TAHH 271** : Température très haute fumées. **BAL** 201/211/221: détecteurs de flamme.	**C_{111}**	**FT** 201 : Débitmètre. **PT** 201 : Transmetteur de pression. **BAL** : 12 Détecteurs de flamme (Ultraviolet).
					C_{112}	**SDV211/ SDV221** : Isolement de la ligne de gaz combustible.
					C_{113}	**Solveur** (Relais de sécurité) : assure les missions de mise en sécurité du four par action sur les vannes SDV211/221.

- **Hypothèses :**

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

• Nous utilisons les taux de défaillances λ_D des composants qui désignent les taux de défaillances dangereuses non détectées λ_{DU} et les taux de défaillances détectées λ_{DD}. Ces défaillances dangereuses font passer le système de l'état normal à l'état de défaillance dangereuse.

• Les composants sont réparables. Ainsi nous estimons que chaque composant possède un réparateur et la durée d'une réparation est fortement négligeable devant le temps entre deux pannes.

• Chaque "événement" est indépendant, ce qui signifie que les défaillances des composants doivent être indépendantes, mais aussi que la réparation d'un composant ne dépend pas de celle d'un autre (il y a autant de réparateurs que de composants).

• Le système est considéré statique du point de vue de son architecture. C'est à dire qu'il n'est pas possible de prendre en compte des reconfigurations.

Le SIS du système d'arrêt d'urgence automatique du four H201 est composé de 3 parties (figure 2.5) :

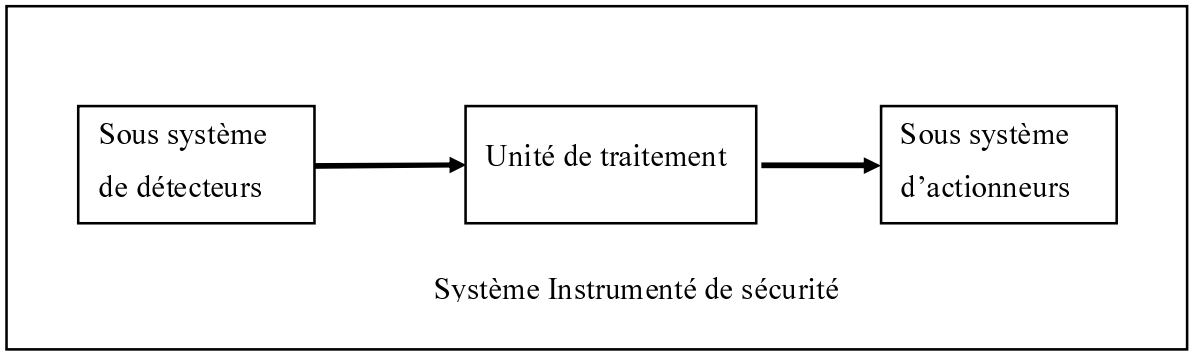

Figure 2.5 - Schématisation d'un SIS

- **Les détecteurs** : ce sont les éléments d'entrée de notre système, responsable de la détection des alarmes ou des anomalies représentées par de multiples facteurs de déclenchement du four.
- **L'unité de traitement** : c'est la partie où le signal est traité, représentée par un système de multiples relais de sécurité.
- **Les actionneurs** : ce sont les exécuteurs de la commande de l'unité de traitement, représentés par des vannes d'arrêt d'urgence (SDV-Shut Down Valve), afin d'isoler le four à travers la fermeture de l'alimentation en fuel gaz du circuit brûleurs.

Définition de la fonctionnement à faible sollicitation : La fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et la fréquence des sollicitations n'est pas supérieure à une par an [15].

Une barrière de sécurité est en mode de sollicitation à faible demande lorsque la fréquence des demandes d'opération n'est pas plus grande qu'une par an et pas plus grande que le double de la période des tests de révision CEI61508-4, Sections 3.5.12 et 13 [16].

Le tableau ci-dessous représente les niveaux d'intégrité de sécurité SIL pour le mode de notre cas d'étude relatif au finctionnement à faible sollicitation :

Tableau 2.3 - Définition des niveaux SIL pour un mode de fonctionnement à faible sollicitation [16]

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

2.2.Description du système à relais

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

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

2.3.Description du système Tricon

Le Tricon est un système tolérant aux fautes grâce à son architecture TMR, il garantit un contrôle en continu, sans erreur en cas de défaillance des composants, ou de présence de fautes transitoires d'origines internes ou externes. Il a été conçu autour d'une architecture triplée totale, depuis les points d'entrées jusqu'aux points de sorties en passant par les processeurs principaux.

3. Configuration architecturelle du système

3.1. Architecture du système avec solveur de type relais de sécurité

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

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

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

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

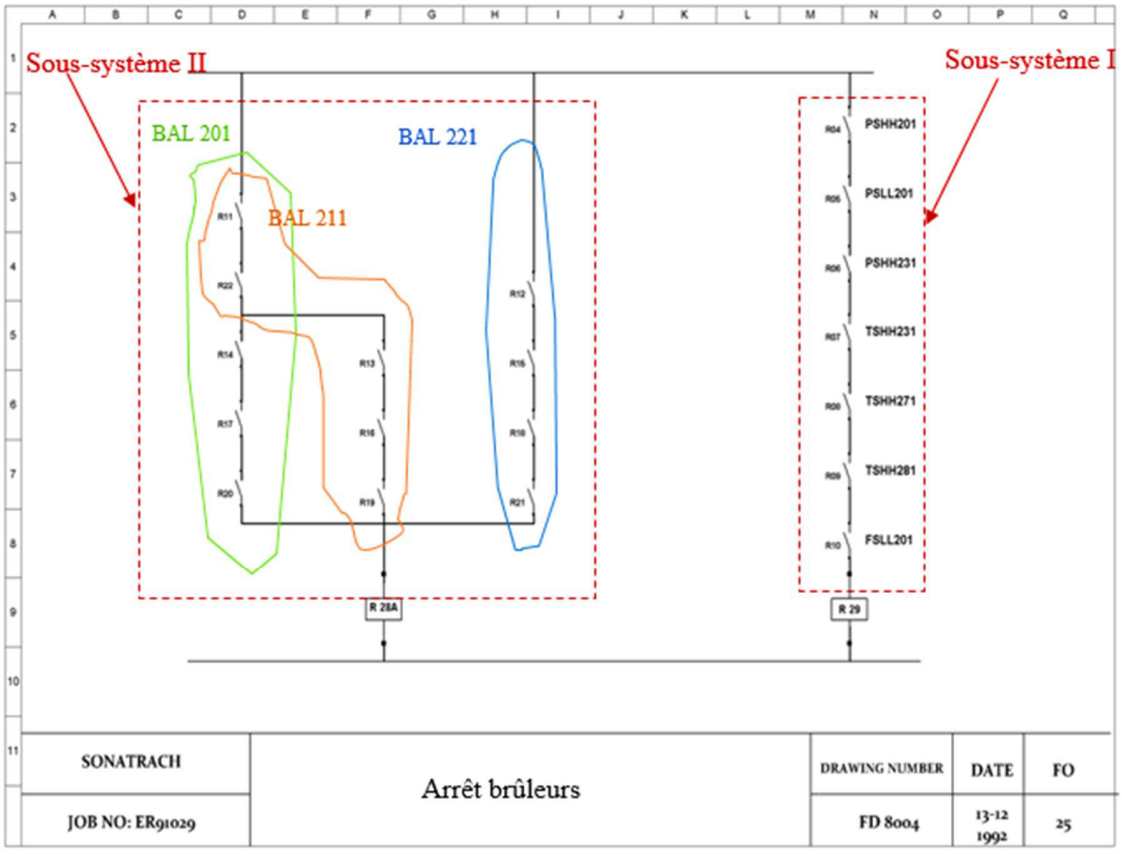

Figure 2.6 - Relais de sécurité relatifs au système d'arrêt des bruleurs [9]

3.2. Architecture du système avec solveur de type Tricon

Dans chaque chaine, le traitement est redondant et indépendant. Chacune de ces chaines 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.

Une fois par vérification ou test triennal ou décennal, les trois processeurs principaux se synchronisent et communiquent entre eux par le TRIBUS. Le TRIBUS vote les données d'entrées logiques, compare les données de sorties et envoie une copie des valeurs d'entrées logique à chaque processeur principal. Les processeurs principaux exécutent le programme d'application et transmettent les valeurs calculées aux modules de sorties juste en amont des borniers de raccordement ce qui permet de décoller et corriger toute erreur éventuelle entre le vote au niveau du TRIBUS et de la sortie.

Pour chaque module d'entrée /sortie, il est possible de loger un module de pièces de rechange à chaud, qui prend la main si une faute est détectée au niveau du premier module en activité. La pièce de rechange à chaud peut aussi être utilisée pour la maintenance de tout modèle qui manifeste un défaut n' importe où dans la configuration du système (Figure 2.7).

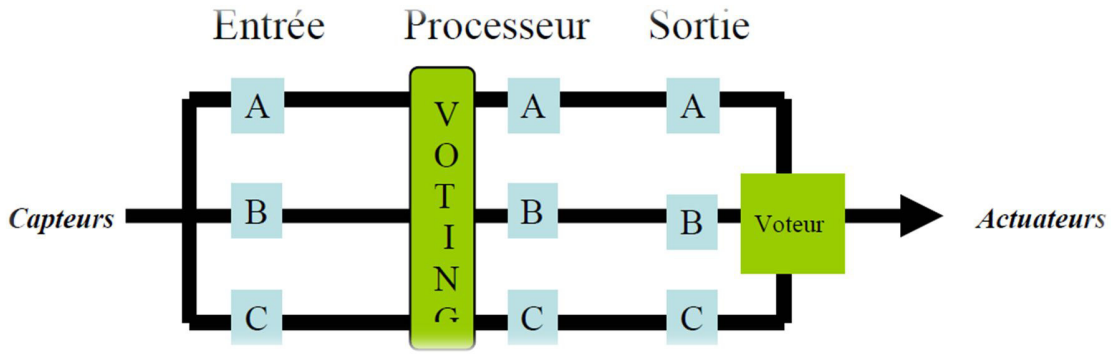

Figure 2.7 - Architecture 2oo3 de PLC

L'architecture adoptée sera modulaire triplex, avec 03 processeurs séparés à structure de bus triplex, tous les systèmes en parallèles. Chaque processeur exécutera ses programmes d'application individuelle simultanément et indépendamment, en vérifiant les données, en exécutent les instructions logiques et contrôle les signaux.

La technologie TMR (Triple Modular Redundant, figure 2.7) 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 voting est de : 2 out of 3 (2 parmi 3) (figure 2.7) c'est-à-dire que lorsque : deux voies sur les trois voies sont positive (ils détectent un signal) nous avons un signal à la sortie du l'API.

Le système (figure 2.8 – figure 2.7) doit procéder automatiquement au contrôle de tous ses composants pour identifier les défaillances. Ces essais de diagnostics seront exécutés au démarrage du système et pendant son exploitation, lors de la détection d'une défaillance, une alarme descriptive sera générée pour une signalisation visuelle.

Figure 2.8 – Triconex

4. Eléments d'entrée pour les deux unités de traitement

Les éléments d'entrée représentent les données du système étudié, ce sont des données techniques, extraites de base de données OREDA [10], PDS [11], IEEE [12], CCPS [13] et de la base documentaire du logiciel GRIF [14], au regard du taux de défaillance, temps de réparation... etc. Ces éléments nous permettent de faire dérouler le module de calcul. Ils sont répartis en 3 catégories, qui sont les composantes essentielles du SIS de notre étude, ce sont caractérisés par le sous-système de détecteurs, les relais de sécurité et le sous-système d'actionneurs.

4.1.Sous-système des détecteurs

Les données d'entrée relatives au composant du SIS (extraites des bases de données OREDA, PDS...) comme : le taux de défaillance, le temps d'échange, MTTR…sont mentionnées dans le tableau ci-dessous (Tableau 2.4) :

Tableau 2.4 - Données relatives aux éléments du sous-système des détecteurs

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

4.2. Système d'unité de traitement

Nous allons utiliser deux types d'unités de traitement différents avec des données techniques différentes, extraites des bases de données différentes relatives à chaque type de PLC.

4.2.1. Système de relais de sécurité

Formule générale pour le calcul du taux de défaillance associé [9]

Pour calculer le taux de défaillance équivalent, nous allons appliquer des formules de la sureté de fonctionnement.

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

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

- Configuration parallèle, le taux équivalent est donnée par la formule suivante, pour :

  $\boldsymbol{\lambda_1}$ et $\boldsymbol{\lambda_2}$ en parallèles, leur $\boldsymbol{\lambda_{éq}}$ est calculer comme suit :

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

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

Tableau 2.5 : Calcul de $\boldsymbol{\lambda_{éq}}$[9]

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

<u>Détermination des taux de défaillance (λ) associés aux détecteurs de flamme (F)</u> [9]

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

La base de données OREDA, nous donne :

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

Pour **BAL 201** :

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

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

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

Pour **BAL 211** :

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

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

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

Pour **BAL 221** :

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

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

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

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

Tableau 2.6 – Données sur les taux de défaillance équivalent aux BAL [9]

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

Détermination du taux de défaillances (λ_{RS}) associé à l'ensemble des relais de sécurité [9]

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

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

Le tableau ci-dessous, les taux de défaillance associés à chaque branche :

Tableau 2.7 – Composition des branches du sous-système relais de sécurité [9]

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

La formule suivante explique la combinaison entre toutes les branches :

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

De plus :

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

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

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

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

Tableau 2.8 – Calcul des $\lambda(B_{Ri})$ équivalent [9]

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

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

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

De plus :

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

Le tableau suivant explique les résultats obtenu par les formules précédantes :

Tableau 2.9 – Calcul de $\boldsymbol{\lambda_{éq}}$ au sous-système de relais de sécurité [9]

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

Les données techniques relatives au système de relais de sécurité pour le système d'arrêt d'urgence du four, sont illustrées dans le tableau ci-dessous (Tableau 2.10) :

Tableau 2.10 – Données relatives au système de relais de sécurité

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

4.2.2. Système Tricon

Les données techniques relatives au Tricon du système d'arrêt d'urgence, sont illustrées dans le tableau ci-dessous (Tableau 2.11) :

Tableau 2.11 – Données relatives au Tricon

Système	Taux de défaillance	DC	MTTR
PLC	**1E-10 h^{-1}**	**90%**	**10.2h**

4.3.Sous-système des actionneurs

Les données techniques relatives aux actionneurs du système d'arrêt d'urgence sont illustrées dans le tableau ci-dessous (Tableau 2.12) :

Tableau 2.12- Données relatives aux éléments du sous-système des actionneurs

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

5. Calcul du SIL

5.1.Présentation de l'outil de modélisation (Module « SIL »)

Le Module SIL fait partie d'une série de modules qui compose le logiciel **GRIF** développé par TOTAL. Cet outil est conçu pour évaluer la PFD d'un système instrumenté de sécurité (SIS).

Plus exactement, il quantifie l'indisponibilité d'un système modélisé à l'aide d'un arbre de défaillances.

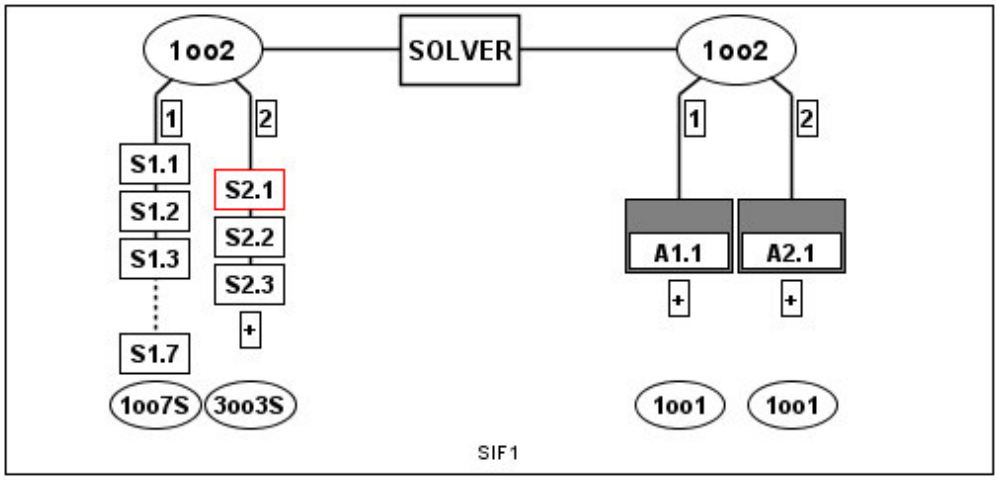

Figure 2.9 – Interface du GRIF, Module SIL

5.2.Calcul du SIL pour l'unité de traitement

5.2.1. Type : logique câblé (Relais de sécurité)

La compilation avec le module SIL fait découler l'évolution de la PFD en fonction du temps, à noter aussi les effets des tests périodiques sur l'évolution de la PFD représenté dans la figure 2.9 et enfin la contribution de la valeur de la PFD en chaque niveau SIL.

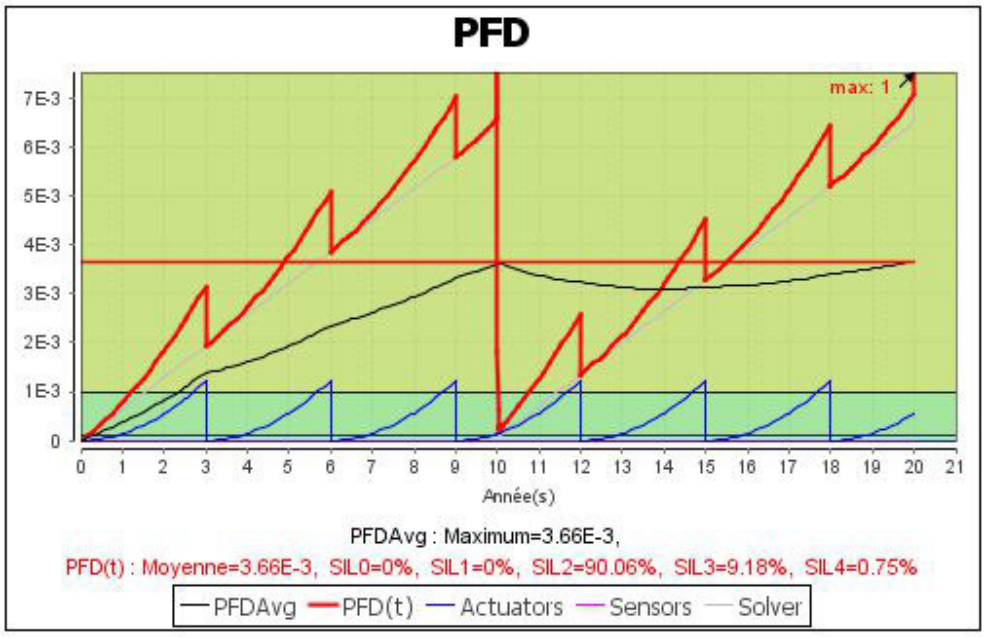

Figure 2.10 - Effet des tests périodiques sur l'évolution de la PFD

Nous retenons de la figure 2.10 les pourcentages suivants **SIL 2 = 90,06 %**, **SIL 3 = 9,18 %** et **SIL 4 = 0,75 %** qui représentent la contribution de la valeur de la PFDavg pour chaque niveau SIL.

Les tests de révision des systèmes d'exploitation et de sécurité, à l'image des SIS, génèrent une diminution de la PFD à chaque test périodique, cela est confirmé par la figure 2.10. Rappelons que l'objectif de ces tests est de veiller à l'atténuation de toute défaillance et la confirmation du bon état de l'unité en question, c'est ce qui justifie la diminution de la PFD parce que, principalement, il n'y a pas de défaillance.

Le maximum de la PFDavg correspond à la valeur moyenne déduite de la courbe en noire (figure 2.10), elle est égale à **3,66. 10^{-3}**, ce qui répond à un **SIL 2** pour le système.

Enfin, le module SIL résume les données de sortie après le traitement dans une fiche technique associée au système étudié, en précisant les valeurs des facteurs spécifiques qui caractérisent le système, nous citons le facteur de réduction du risque (RRF), une estimation du SIL requis, une proposition pour une configuration du système en terme du nombre de capteurs et de détecteurs et finalement le plus important un commentaire sur la conformité du système par rapport aux disposition des normes CEI 61508 ; CEI 61511 et CEI6261.

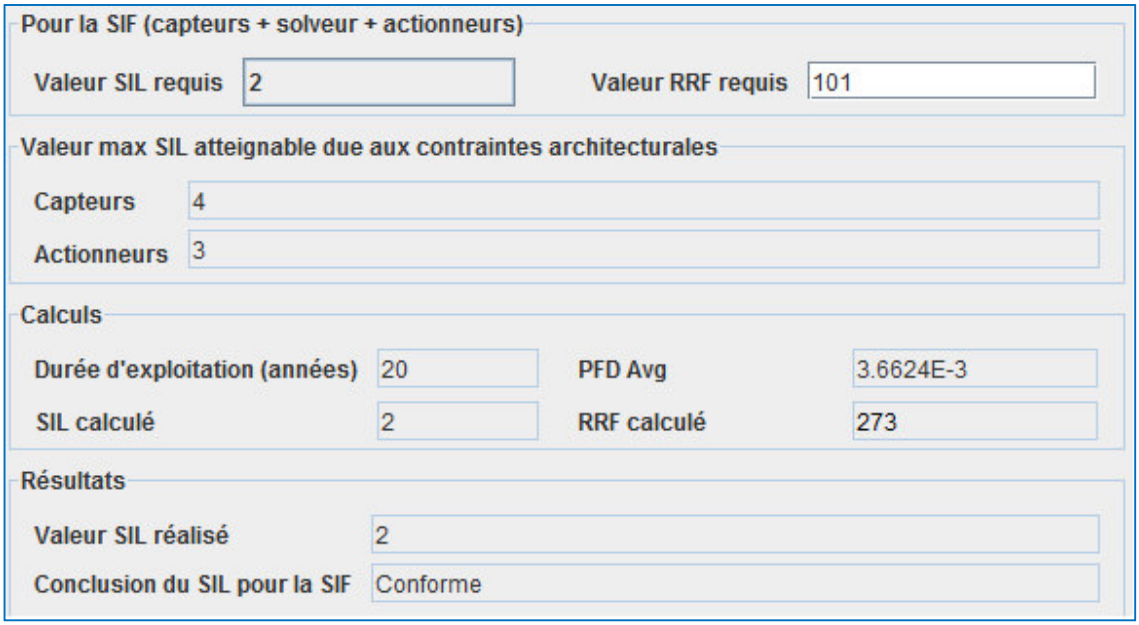

Figure 2.11 - Fiche technique des résultats trouvés par GRIF

D'après le tableau 2.13 la grande contribution au SIL est de la part de l'unité de traitement basé sur les relais de sécurité et le SIF de 100% qui donne un SIL 2.

Tableau 2.13 – Contribution de chaque composant donnée par le GRIF

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

5.2.2. Type : Tricon

Nous allons refaire toutes les étapes précédentes par le GRIF pour calculer le SIL total dans le cas du système Tricon (Solveur).Tous les calculs que nous avons effectués concernés le SIS décrite par le schéma suivant :

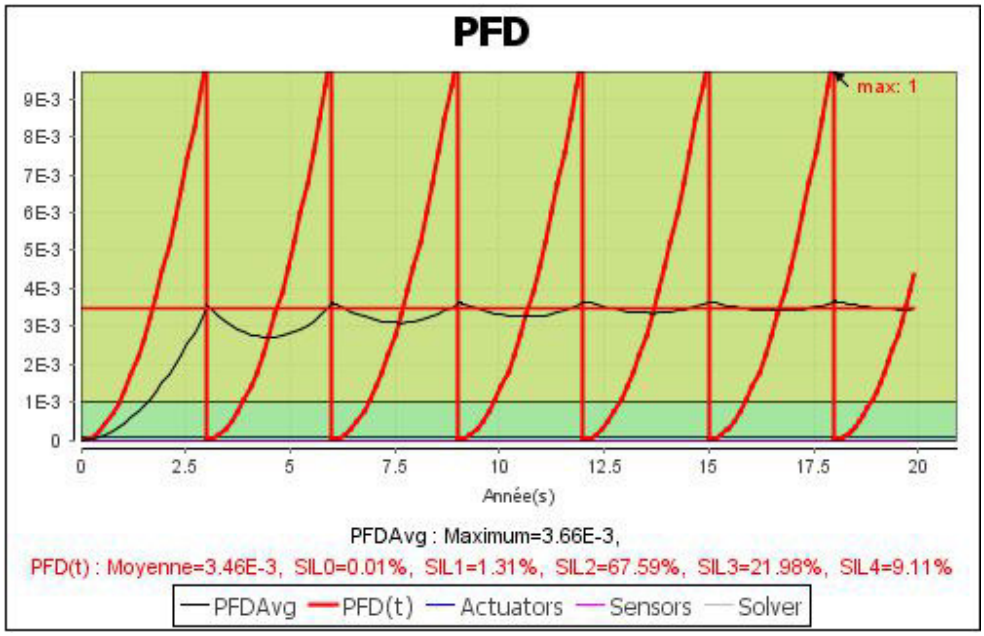

Figure 2.12- Effet des tests périodiques sur l'évolution de la PFD

Nous retenons de la figure 2.12, les pourcentages suivants : **SIL 2 = 67,59 %**, **SIL 3 =21.98%** et **SIL 4 = 9.11 %** qui représentent la contribution de la valeur de la $\mathbf{PFD_{avg}}$ pour chaque niveau SIL.

Les tests de révision des systèmes d'exploitation et de sécurité, à l'image des SIS, génèrent une diminution de la PFD à chaque test périodique, cela est confirmé par la figure 2.12. Rappelons

que l'objectif de ces tests est de veiller à l'atténuation de toute défaillance et la confirmation du bon état de l'unité en question, c'est ce qui justifie la diminution de la PFD parce que, principalement, il n'y pas de défaillance.

Le maximum de la PFD_{avg} correspond à la valeur moyenne déduite de la courbe en noire (figure 2.12), est égale à **3,57. 10^{-3}**, ce qui répond à un **SIL 2** pour le système.

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

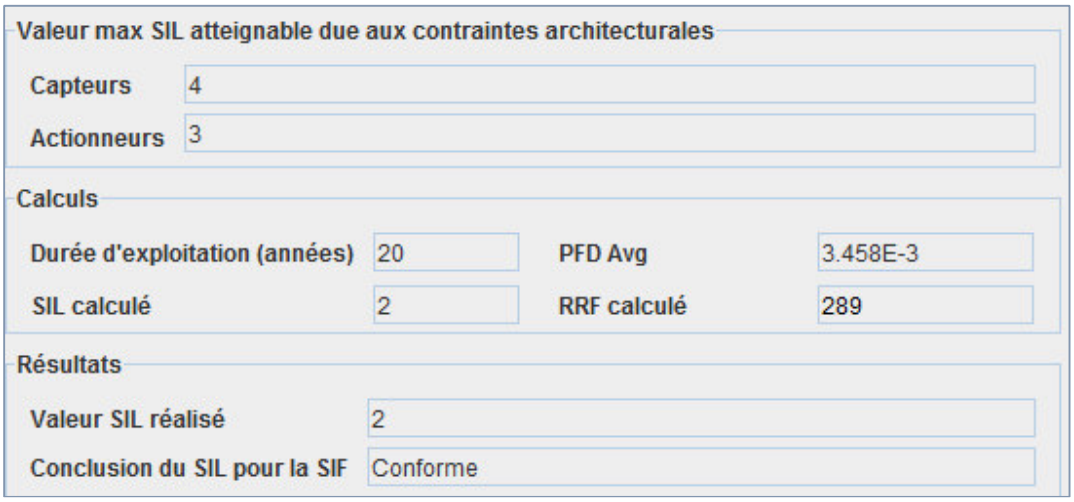

Figure 2.13 – Fiche technique du SIS (solveur-type : Tricon) donné par le GRIF

Tableau 2.14 – Contribution de chaque composant du SIS au SIL

	PFD Avg	RRF	SIL Calculé	Contribution (%)
Partie Capteur(s)	0	3.56E20	4	0%
Partie Solveur	1.05E-4	9564.39	3	3.02%
Partie Actionneur...	3.35E-3	298.25	2	96.98%
SIF	3.46E-3	289.19	2	100%

Nous constatons d'après le tableau 2.14 que dans le cas du solveur « Tricon », la grande contribution au SIL est de la part du sous-système des actionnaires, non pas l'unité de traitement, le SIF de 100% SIL 2. Par contre pour l'unité de traitement le SIL est 3 avec une très faible contribution au SIL du système d'arrêt d'urgence.

Nous allons faire une comparaison entre les résultats obtenus par les systèmes (tableau 2.15) :

Tableau 2.15 – Comparaison entre les deux PLC

Type de PLC	Relais de sécurité	Triconnex
SIL calculé	**2**	**2**
% de SIF en SIL 2	**100**	**100**
Conclusion du SIL pour la SIF	**Conforme**	**Conforme**
PFDavg	**3.66E-3**	**3.458E-3**
RRF	**273**	**289**

Les principaux avantages et caractéristiques de l'architecture TMR du système TRICON sont les suivants (tableau 2.16) :

Tableau 2.16 – Avantages du système Tricon

Avantages du Triconnex	**Pas de point unique de défaillance :**	La défaillance de n'importe quel composant de l'architecture n'a aucune incidence sur le bon fonctionnement de l'ensemble du système TRICON.
	Un très haut niveau de sécurité :	Grâce à son architecture TMR et à sa puissance de diagnostic, le système TRICON atteint le niveau d'intégrité de sécurité 3 .
	Un très haut niveau de disponibilité :	Le système d'architecture TMR fonctionne avec trois modules processeurs. Les modules en défaut peuvent être remplacés sans interruption du fonctionnement du système et ainsi permettre d'assurer un contrôle continu.
	Une maintenance à moindre coût :	Grâce aux systèmes de diagnostic intégrés qui détectent automatiquement les modules en défaut qui doivent être remplacés, il n'est plus nécessaire de recourir à des techniciens hautement qualifiés.
	Une capacité mémoire étendue :	Avec une capacité mémoire jusqu'à 2 M octets, les processeurs principaux fournissent l'espace suffisant pour le programme d'application et la consignation d'états volumineux.
	L'archivage des données séquence d'événement (SOE) :	Le consignateur d'état (SOE) utile à la fois pour maintenance du système et à l'analyse des causes de l'arrêt du procédé.
	Des liaisons de communications redondantes à haute vitesse :	Liaisons vers d'autres systèmes Triconex, les systèmes numériques de contrôle centralisé ou SNCC (Distribued Control System, DCS) et autres équipement.
	La possibilité de déporter les châssis :	Jusqu'à 30 m du châssis principal, par liaisons en cuivre et 12km en fibres optiques.

Conclusion Générale

Les résultats de la PFD calculés par le module SIL pour les deux systèmes d'arrêt d'urgence automatique du four H201, soit avec l'unité de traitement à base des relais de sécurité (le premier système) ou avec le triconnex comme unité de traitement logique (le deuxieme système), en se basant sur les plages des valeurs de la PFD associé aux SIL des deux systèmes, nous avons trouvé un niveau de sécurité 2 (SIL2) pour les deux systèmes. Ce la, affirme l'égalité entre les deux systèmes qui donne un niveau de sécurité 2, mais avec des pourcentages de contibution des autres SIL au SIL réel, qui sont totalement differents.

La comparaison entre les valeurs du SIL réel calculées par le modulo SIL des deux systèmes identiques dans les éléments d'entrées et les éléments de sorties (sous-système de détection et d'exécution) ; cependant, ce different au niveau de la PLC ; les résultats obtenus nous donner un SIL 2 mais on note que la contribution du SIL 3 au SIL 2 a augmenté dans le cas du système triconnex par rapport au système des relais de sécurité, grâce à son architecture de triple modulo redondant et à sa puissance de diagnostic des pannes, avec les multiples inconvénients du système cablé (leurs encombrements « poids et volume » et manque souplesse vis-à-vis de la mise en point de commandes..).

De ce fait, nous pouvons conclure que la performance du SIS par rapport au niveau d'intégrité de sécurité ne change pas si on change l'unité de traitement ; Cependant grâce aux avantages du triconnex et les inconvénients des relais de sécurité, le SIS avec triconnex comme unité de traitement est le plus conforme au regard des résultats obtenus.

Bibliographies

1. Commission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems*, in *Part 1: General requirements*. 2010. p. 1-66.
2. Nguyen Thuy LE, A.A., Sylvain CHAUMETTE, Sébastien BOUCHET, Valérie DE DIANOUS., *Evaluation des performances des Barrières Techniques de Sécurité (DCE DRA-73) Evaluation des Barrières Techniques de Sécurité - Ω 10*. 2008, INERIS France p. 59.
3. Commission, I.E., *Functional safety – Safety instrumented systems for the process industry sector* in *Part 1: Framework, definitions, system, hardware and software requirements*. 2003. p. 1-15.
4. Commission, I.E., *Functional safety – Safety instrumented systems for the process industry sector* in *Part 2: Guidelines for the application of IEC 61511-1*. 2003. p. 1-8.
5. Commission, I.E., *Functional safety – Safety instrumented systems for the process industry sector* in *Part 3: Guidance for the determination of the required safety integrity levels*. 2003. p. 1-10.
6. 62061, I., *Safety of machinery, Functional safety of electrical control systems, electronic and programmable electronic safety-related.* 2005, IEC International Electrotechnical Commission: Geneva, Switzerland. p. 69.
7. 954-1, E., *Sécurité des machines. Partie des systèmes de commandes relatives à la sécurité. Partie 1 : Principes généraux,.* 1996.
8. Rique, B., *Guide d'interprétation et d'application de la norme CEI 61508 et de ses normes dérivées IEC 61511 (ISA-84.01) et IEC 62061*. 2005, ISA - The instrumentation, Systems, and Automation Society: France
9. ASSADI , F., *EVALUATION DE LA PERFORMANCE DES SYSTEMES INSTRUMENTES DE SECURITE - Système d'Arrêt d'Urgence Automatique du Four Rebouilleur H201 - Train 1 - Module 1 - DP SonatracH, Hassi R'mel, Laghouat, ALgerie.*, in *Quality Health Safety Environment -Industrial Risks Management* 2015, Polytechnique National School-Algiers , Algeria Algiers, Algeria p. 117.
10. Management, S.I., *OREDA-Offshore RElaibility Data Handbook* 2002, OREDA Participants Trondheim NORWAY. p. 835.
11. Stein Hauge, P.H., *Reliability Data for Safety Instrumented Systems PDS Data Handbook*, in *PDS Data*. 2004 Edition SINTEF Trondheim, NORWAY. p. 22.
12. IEEE, *Guide to the collection and presentation of electrical, electronic, sensing component, and mechanical equipement reliability data for nuclear-power generating station*. 1984. p. 500.
13. (CCPS), C.f.C.P.S., *Offshore reliability data handbook.* 2002. **4th Edition**.
14. TOTAL, *Module SIL-GRIF*, in *GRaphique Interactifs pour la Fiablilité* 2013, Documentation technique p. 21.
15. DRANGUET, J.-M., *Evolution des normes CEI 61588 et CEI 61511-Révision des normes de la sécurité fonctionnelle IEC 61508-61511.* INERIS, 2009. **3eme rencontres en sécurité fonctionnelle** (Les évolutions Fondamentales): p. 21.
16. Comission, I.E., *Functional safety of electrical/electronic/programmable electronic safety-related systems* in *Part 4: Definitions and abbreviations*. 2010. p. 1-50.