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

SELLA ABDELKADER

BOUMERFEG AIMEN

Filière : Hydrocarbures et Chimie
Option : Automatisation des Procédés industriels Commande Automatique

Thème

Etude de SIL appliqué à un Four Industriel & simulation

Devant le jury :

Boumerdiene mohamed said	……	UMBB	Président
Kahoul Fadhila	MC/A	UMBB	Examinateur
Meziane Nacera	MC/B	UMBB	Examinateur
MEGLOULI HOUCINE	MC/A	UMBB	Encadreur

REMERCIMENTS

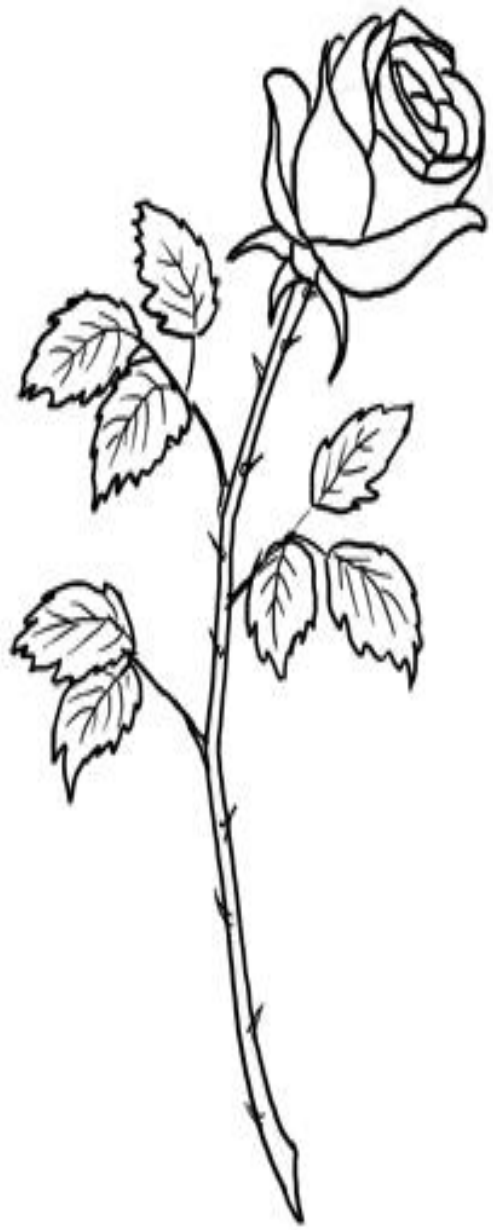
Tout d'abord, Nous remercions le bon dieu de nous avoir donné du courage afin que ce mémoire soit terminé.

Nous tenons à exprimer nos vifs remerciements et nos gratitudes à ***Mr H.MEGLOULIE*** *Docteur à la Faculté des Hydrocarbures et de la Chimie, Université de Boumerdes, qui nous a fait l'honneur d'être rapporteur de ce mémoire. Nous le remercions pour la patience dont il a fait preuve lors de ses relectures mais également pour les différentes discussions fructueuses que nous avons pu tenir ensemble et les lectures attentives lors différentes étapes de la réalisation de ce travail.*

Nous tenons également à remercier ***Mr M.LAKHEMESS*** *Chef service Instrumentation –RA1Z- qui nous a beaucoup aidé durant notre stage pratique.*

Pour tous nos amis sans exception, ils sont nombreux, nous ne pouvons tous les citer mais nous ne les oublions jamais.

Enfin, que toutes les personnes ayant contribué, de près ou de loin, à la réalisation de ce travail, soient chaleureusement remerciées.



Dédicace

A la vie pour ses joies et ses peines

A mes parents, pour leur support et aide

Je dédie ce modeste travail :

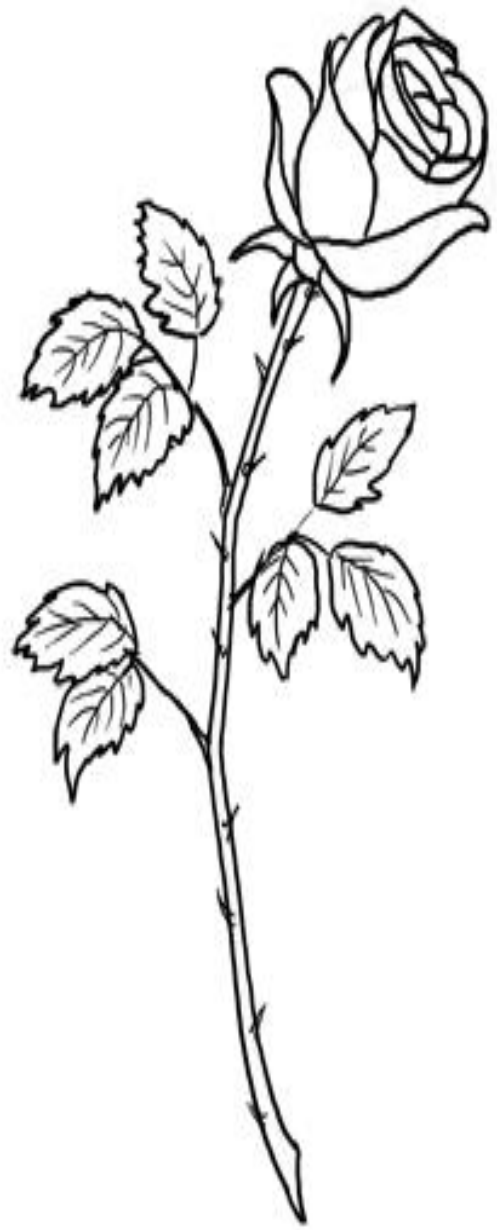
♣ A mon très cher père qui m'a beaucoup encouragé durant toutes mes études

♣ A ma maman, qui m'a donné toujours le courage à terminer mes études

♣ A mon cher frère Abdelalah, à mes chères sœurs

♣ A tous mes amis, avec lesquels j'ai partagé mes meilleurs moments Redha, Houssem Bessam, Hichem, Kacem ,Walid ,Azzedine.

Abdelkader



Dédicace

A la vie pour ses joies et ses peines

A mes parents, pour leur support et aide

Je dédie ce modeste travail :

♣ A mon très cher père qui m'a beaucoup encouragé durant toutes mes études

♣ A ma très chère maman, qui m'a donné toujours le courage à terminer mes études

♣ A mon cher frère HOUSSEM, à ma chère sœur et ses deux petites filles adorable LINA ET SIRINE

♣ A tous mes amis, avec lesquels j'ai partagé mes meilleurs moments Oussama Troy , Oussama arab ,Amir l7ar , Mohamed Haddada , Kamel , abd samad et lechlouch

Aimen

SOMMAIRE

LISTE DES FIGURES

Glossaire

- **1oo2** – (one out of two)
- **ALARP** – As Low As Reasonably Possible : Aussi faible que raisonnablement possible, concept britannique au départ pour définir le niveau d'exigence pour un système de sécurité.
- **CCF** –(common cause failure) systématic failure – défaillances aléatoire .
- **GAME** – Globalement Au Moins Equivalent : Concept utilisé principalement par le Ministère desTransports français (pour les transports aériens et ferroviaires essentiellement) stipulant qu'un nouveau système de transports ne doit pas induire plus de risque que le précédent.
- **HAZOP** – Hazard and Operability Study .
- **HFT**– Hardware Fault Tolerance– Tolérance aux anomalie du matériel .
- **HMI**–Human Machinne Interface – IHM
- **HRA** – Human Reliablility Analysis _ Analyse de la fiabilité humain
- **BPCS** – Basic Process Control System : Système de contrôle commande, habituellement à base de SNCC ou d'API contrôlant un processus industriel
- **EUC** – Equipment Under Control : Installation, machine ou équipement commandé par le BPCS et/ou leSIS
- **E/E/PE** – électrique / électronique / électronique programmable
- **FMEA / AMDE(C**) – Failure Mode and Effects Analysis / Analyse des Modes de Défaillance et de leurs Effets (et de leur Criticité)
- **FPL** – Fixed Programming Language : langage de programmation limité à du paramétrage
- **FSM / SGS** – Functional Safety Management system : Système de Gestion de la Sécurité
- **SRS** – Safety Requirements Specification : Exigences de sécurité ou Spécification Régissant la Sécurité
- **FTR** – False Trip Rate : Taux de déclenchement intempestif
- **FVL** – Full Variability Language : Langage de programmation à pleine variabilité (ADA, C++, Pascal,

Fortran, IL…)

- **LVL** – Limited Variability Language : Langage de programmation à variabilité limitée (dans le cadre de l'IEC 61511, 3 des langages automates de l'IEC 61131-3)
- **Graphes de Markov** – méthode de modélisation des états des systèmes complexes permettant de algébriquement ou matriciellement les paramètres de fiabilité d'un système

- **MOC** – Management Of Change : Gestion des modifications

- **MTBF** – Mean Time Between Failure : Temps moyen entre pannes

- **MTTF** – Mean Time To Failure : Temps moyen avant la première défaillance
- **MTTR** – Mean Time To Repair : Temps moyen de réparation
- **SFF** – Safe Failure Fraction : Taux de pannes sûres (non dangereuses)
- **PFD** – Probability of Failure on Demand : Probabilité de défaillance sur sollicitation
- **PLC** – Programmable Logic Controller : Automate programmable industriel
- **RRF** – Risk Reduction Factor : Facteur de réduction du risque (= 1/PFD)
- **SAS** – Système Automatisé de sécurité

- **SLC** – Safety Life Cycle – Cycle de vie de sécurité
- **SRESW** – Safety Relevant Embedded Software – logiciel embraqué relatif à la sécurité
- **SRASW** – Safety Relevant Application Software – logiciel intégré relatif à la sécurité
- **SIF** – Safety Instrumented Function : Fonction instrumentée de sécurité
- **SIS** – Safety Instrumented System : Système instrumenté de sécurité

- **SIL** – Safety Integrity Level : Niveau d'intégrité de sécurité
- **SRS** – Safety Requirement Specification – Spécification des exigence concernant la sécurité

LISTE DES TABLEAUX

Problématique :

La conduite d'un procédé dans le domaine Pétrole & Gaz implique la connaissance, la surveillance et la maitrise de certains paramètres tels que la pression, la température, le débit, etc… chaque procédé possède ses exigences propres, 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 de système instrumentés de sécurité de ces installations à risque pour le respect des exigences réglementaires.

La situation actuelle de l'instrumentation de la raffinerie d'ARZEW est de technologie très ancienne et la constitution du système de contrôle et de sécurité est aujourd'hui dépassée et ses performances sont peu efficaces. La plus part des instruments ont une précision très faible. L'abandon de fabrication de la pièce de rechange est une préoccupation pour le maintien en service des instruments et des unités de production.

La mise à niveau de l'instrumentation a pour but :

- Améliorer la gestion de la sécurité et du contrôle des unités de la raffinerie
- Améliorer les conditions de d'exploitation des installations
- Maitriser les paramètres de fonctionnement et la qualité des produits
- Avoir un diagnostic sur le fonctionnement des unités, des systèmes et des instruments
- Avoir une traçabilité des faits et des mesures
- Améliorer la gestion de la sécurité et du contrôle des unités stratégique (four)

Ces objectifs seront atteint par :

- Installation de nouveaux PLCs pour la gestion de la sécurité et pour les arrêts d'urgences
- Remplacement des instruments de terrain existant par des instruments intelligents moderne
- Installation de stations de commande des vannes motorisées
- Installation de réseaux de communication

Mais avant de passer à l'étape de réalisation, les équipements de la raffinerie ont fait l'objet d'une étude préalable, visant à déterminer et mettre en œuvre un système instrumenté de sécurité (**SIS**) pour assurer la sécurité fonctionnelle des installations, et réduire les risques à un niveau tolérable. Dans ce modeste travail on procède à l'étude de niveau de SIL d'un équipement stratégique (four) ; qui nous permettra de déterminer et concevoir plus tard le système instrumenté de sécurité adéquat pour cet équipement.

Chapitre 1 :

PRÉSENTATION DE LA RAFFINERIE D'ARZEW (RA1Z)

I.1. Introduction :

Dans ce chapitre, nous allons d'abord présenter le complexe RA1Z

I.2. Historique :

- Signature du contrat avec la société Japonaise **JGC** pour la réalisation de la raffinerie d'Arzew le **30 Juillet 1969**.
- Pose de la première pierre le 19 Juin 1970.
- Démarrage des installations :
  - Utilités Juillet 1972
  - Bitumes Novembre 1972
  - Carburants Décembre 1972
  - Lubrifiants Janvier 1973
- Démarrage de la production des lubrifiants en Janvier 1973.

  Augmentation progressive de la cadence de la production (démarrage de toute la chaîne de fabrication)
- Arrêt en 1974 par manque de vapeur suite à un incident important sur la chaudière à vapeur.
- Nouvelles installations de lubrifiants **:**
- Signature du contrat avec un consortium composé de :
  - **Foster Wheeler.**
  - **Klockner SGP.**
  - **Voest Alpine le 12 Mai 1977.**

pour la réalisation d'un ensemble intégré de production de 120 000 tonnes.

- Ouverture du chantier en Janvier 1979.
- Démarrage des installations en Mars 1984.

I.3. Situation géographique :

La Raffinerie d'ARZEW (NAFTEC RA1Z) occupe une superficie de 150 hectares de la zone industrielle sur le plateau d'EL MAHGOUN à l'Est d'Oran, à environ 5 km de la Mer Méditerranée. La construction de la raffinerie d'Arzew a démarré en 1972, suivie par une extension majeure au début des années '80.

Figure I.1 : Situation graphique de la raffinerie d'Arzew

I.4. Capacité de production :

La capacité de traitement est de **2,5 millions** de tonnes par an pour le pétrole brut Hassi Messaoud arrivant par pipeline, et de **279.000 tonnes** par an pour le brut , réduit

importé (BRI), destine à produire des bitumes.

La raffinerie produit des GPL, des essences (normale et super), du naphta, du kérosène, du gasoil, des fuels, des bitumes (routiers et oxydés) et des lubrifiants (huiles de base, graisses et paraffines). Elle assure l'approvisionnement de la région d'Oran et de son arrière-pays en produits raffinés, les excédents de production sont exportés.

Le site d'implantation du complexe peut être divisé par deux axes Nord/Sud et Est/Ouest. Le Département de production P1 occupe la partie Nord/ Ouest et le Département P2 la partie Sud/Ouest. La zone s'étendant du Nord/Est au Sud/Est est réservée presque exclusivement au stockage des différents produits, aux mélanges et à l'expédition.

- La raffinerie d'Arzew a traité au cours de l'année 2015, **3.5 millions** de tonnes de pétrole brut de Hassi Messaoud et environ **280 000 tonnes** de brut réduit importé. Sa production annuelle en produits finis et semi-finis avoisine les quantités suivantes :

Produit	Quantité (T/an)
Propane	15 000
Butane	70 000
Essence normale	490 000
Essence super	70 000
Naphta	160 000
Gasoil	980 000
Fuel HTS	70 000
Fuel BTS	550 000
Kérosène	120 000
Bitumes routiers	120 000
Bitumes oxydés	20 000
Lubrifiants	160 000
Graisses	70 000
Paraffines	4 000

Tableau I.1 :Production Annuelle de la raffinerie d'Arzew

I.5. Présentation des principales installations de RA1/Z :

Département production P1 :

- **Zone 3 (Utilités P1)**: Les utilités :

Source d'énergie, ses unités approvisionnent la raffinerie en : eau distillé, vapeur, électricité, eau de refroidissement, gaz et air service et instruments.
Elle comprend les unités suivantes :

- **Unité 31 :** production de la Vapeur et de l'Électricité : [31H1(60t/h)-31H2(60t/h)-31H3(120t/h)-31K1:4.5MW (3.5MW exploité)].
- **Unité 32 :** production d'eau distillée.
- **Unité 33** : eau de refroidissement**.**
- **Unité 35 :** réception et distribution de gaz combustible**.**
- **Unité 36 :** air instrument et air service.
- **Unité 67** : installation de lutte contre l'incendie.

- **Zone 4 (Les Carburants) :** elle comprend les unités suivantes :

- **Unité 11** : Distillation atmosphérique :

Cette unité d'une capacité de **2.5 millions** de tonnes est calculée pour produire ce qui suit à partir du brut de Hassi-Messaoud :

- GPL.
- LSRN (naphta léger).
- HSRN (naphta lourd).
- GAS-OIL lourd (HGO), et GAS-OIL léger (LGO).
- kérosène.
- Brut réduit atmosphérique.

Cette unité comprend 02 sections :

- Section de fractionnement principal.
- Section de stabilisation des gaz de tête.

- **Unité 12** : Unité d'Hydrobon-platforming :

Le naphta lourd HSRN provenant de l'unité de distillation atmosphérique contient du souffre, de l'azote, de l'oxygène et d'autre composants constituant un poison pour le catalyseur du platforming. C'est l'unité d'hydrobon qui est destinée à transformer et à éliminer les composants indésirables par hydrogénation.

Le platforming est un procédé catalytique ou on emploi un catalyseur sélectif afin de transformer en présence de l'hydrogène, **l'unifinat** en **produit de base** de meilleure qualité pour la fabrication des essences.

- **Unité 13 :** Récupération-Séparation GPL :

Cette unité a pour but de récupérer le propane et le butane à partir de l'unité de distillation atmosphérique (11) et de l'unité de reforming catalytique (12).

- **Unité 65 :** Torche.

- **Zone 7 (Les Lubrifiants 1) :**

Elle a pour tache de produire les huiles de base à partir du brut réduit atmosphérique (BRA) provenant de l'unité 11 de la zone 4.Elle comprend les unités suivantes :

- **Unité 20 :** stockage d'huile.
- **Unité 21** (distillation sous vide)

Destinée à préparer les distillats qui seront transformés en huile de base, cette unité a pour tache de fractionner le BRA et obtenir:

- Gasoil sous vide (VGO),
- Spindle (SPO),
- Mi-visqueuse (MVO),
- Visqueuse.
- Et le résidu sous vide (RSV) qui est la charge de l'unité22.

- **Unité 22** (désasphaltage au propane)

Le résidu court de l'unité 21 y est traité avec un solvant sélectif, le propane, dans le but d'éliminer l'asphalte.

Le produit obtenu est l'huile désasphaltée (DAO).

- **Unité 23** (extraction au Furfural)

les trois distillats de l'unité 21 et la DAO de l'unité 22 y sont traités afin d'éliminer les aromatiques et par conséquent améliorer l'indice de réfraction , ceci à l'aide d'un solvant , le furfural.

Cette opération donne naissance à 04 raffinats:

- Spindle,
- Mi-visqueuse (SAE10),
- Visqueuse (SAE30),
- Bright stock (BS).

L'extrait débarrassé du furfural est envoyé vers fuel.

- **Unité 24** (déparaffinage /déshuilage au MEK-Toluene)

Le mélange MEK-toluène est utilisé comme solvant sélectif afin d'extraire la paraffine ayant un point d'écoulement élevé des quatre raffinats et obtenir quatre huiles déparaffinées.

- **Unité 25** (hydrofinishing)

Dans le but d'éliminer d'autres composants indésirables que peuvent contenir les quatre huiles (soufre, O2, N2).

- **Zone 10** (Les Bitumes)

Etant donné la faible quantité d'asphalte contenue dans le brut algérien, les bitumes routier et oxydé sont extraits à partir d'un brut importé (BRI). La zone bitume est composée des unités suivantes :

- **Unité 14 (**bitume routier)

Le BRI et l'asphalte récupéré des unités de désasphaltage au propane sont fractionnés pour obtenir différentes coupes de gasoil (LVGO, MVGO, HVGO) et un résidu (sous vide) S/V qui va être traité dans la section de soufflage à l'air pour obtenir du bitume routier.

- **Unité 15** (Bitume oxydé)

Cette unité est destinée à produire du bitume à haut point de ramollissement. Elle traite une charge constituée de bitume direct et HVGO en provenance de l'unité 14, par oxydation poussée avec l'air on obtient du bitume oxydé.

- **Unité 45 :** Chargement bitumes.
- **Unité 49 :** Conditionnement bitumes oxydés.

- **Zone 28 (OFF-SITES) :**

Cette zone a pour mission de stocker les carburants, les additifs, elle fabrique des essences provenant de la zone 4 à partir du platformat, LSRN, HSRN et le butane.

L'expédition des carburants, du butane et du propane se fait par camion, train, canalisations ou par navires de l'ISP.

Elle comprend les unités suivantes :

- **Unité 41 :** installation d'ethylation.
- **Unité 43 :** stockage Fuel-Oil.
- **Unité 44 :** stockage GPL.
- **Unité 47 :** chargement par terre.

- **Unité 48 :** chargement et déchargement par mer.
- **Unité 66 :** traitement et évacuation des rejets.

Expédition et chargement :

L'opération d'expédition et de chargement des carburants finis et semi finis est très importante point de vue économique pour la raffinerie, une partie de la production est destiné au marché local, le reste est destiné à l'exportation tel que naphta, fuel (HTS, BTS) vers (Europe et USA,..) ces opérations sont effectués par quatre voies :

- **Camions citernes :** Chargement au niveau de la rampe (Zone 30), les produits expédiés sont les essences, (super, normal), gasoil et le kérosène, suivant un bon de remplissage.
- **Trains :** L'opération s'effectue dans des wagons citernes (Zone 30).
- **Pipes :** L'acheminement et réalisé par des conduites de tuyauteries de la zone de stockage vers les bacs de petit lac (Naphtal) par l'intermédiaire de deux grandes pompes **47P1** et **47 P2** les produits expédiés sont les essences (normal et super), gasoil et kérosène.
- **Bateau :** L'expédition vers l'étranger par les lignes maritimes au niveau du port d'Arzew. Les produits expédiés sont fuel, et naphta.
- **Zone6 (Mélange et conditionnement des lubrifiants) :**

La zone 6 est composée de trois unités de fabrication de produits finis :

- **Unité 51 :** mélange et conditionnement des huiles**.**
- **Unité 52 :** fabrication et conditionnement des graisses**.**
- **Unité 53/54** : traitement et mélange de la paraffine

Département production P2 :

Suite au besoin croissant en lubrifiants, La deuxième partie de RA1Z: Chaîne d'Huiles Nr2 (département Production P2), fut construite de 1978 à 1980 par un consortium d'entreprises Foster Wheeler- France/ Kloeckner- Allemagne/ Voest Alpine SimmeringGrazPauker- Autriche.

- **Zone 19 (Utilités P2) :** Elle comprend les unités suivantes :

- **Unité 1100 :** production de vapeur (SG1101-SG1102-SG1103).
- **Unité 1200 :** production d'électricité (AT1201 : 8.8MW – (5.6MW exploité)).
- **Unité 1300 :** eau de refroidissement**.**
- **Unité 1400 :** gaz combustible.
- **Unité 1500 :** air service-air instrument.
- **Unité 1600 :** stockage et traitement d'eau.
- **Unité 1700** : torche.
- **Unité 1800** : traitement des effluents

- **Zone 5** : Les huiles de base (HB3, HB4) :

Zone de production des huiles de bases (SPO, SAE30, SAE10, BS).Elle comprend les unités suivantes :

HB3 : composé des unités suivantes:

- **Unité 100 :** distillation sous vide.
- **Unité 150** : huile caloporteur**.**
- **Unité 160 :** traitement des eaux acides.
- **Unité 200 :** desasphaltage au propane.
- **Unité 300 :** extraction au Furfural.

HB4 : comprend les unités suivantes :

- **Unité 400 :** déparaffinage/déshuilage au MEK-Toluene**.**
- **Unité 500 :** hydrofinishing.
- **Unité 600 :** hydrogénation des paraffines.
- **Unité 3000 :** (Mélange, conditionnement et expédition des lubrifiants) :
  - L'unité est destinée à produire des huiles finies à partir des huiles de base fabriquées dans les unités 100 à 500 et des additifs importés.
  - L'unité est dimensionnée pour traiter **120000t/an** d'huile de base.
  - La production d'huile finie, compte tenu d'une quantité moyenne d'additifs de 10%, sera d'environ **132000t/an.**

- **Unité 2800 :** Stockage et expédition des huiles de base**.**
- **Unité 3100 :** Mélange et conditionnement des huiles:

Elle est destinée à fabriquer des huiles finies à partir des huiles debase et des additifs importés. La production se divise en deux grandes catégories :

✓ **Huiles pour moteurs :**

Les huiles pour moteurs représentent environ **81%** du tonnage produit, soit**97000 T/an** d'huile de base à traiter.

- Huiles pour moteur à essence.
- Huiles pour moteurs diesel.
- Huiles pour transmission.

✓ **Huiles industrielles :**

Les huiles industrielles représentent environ **19%** du tonnage produit, soit **23000T/an** d'huile de base à traiter.

- Huiles hydrauliques (TISKA).
- Huiles turbines (TORBA).
- Huiles engrenages (FODDA).
- Huiles compresseur (TORADA).
- Huiles diverses.

- **Unité 3200 :** Préparation et conditionnement des graisses**.**
- **Unité 3300 :** Conditionnement des paraffines.
- **Unité 3400 :** Expédition des produits conditionnés.
- **Unité 3500 :** Expédition des produits en vrac.
- **Unité 3600 :** Réception des additifs et produits chimiques.
- **Unité 3700 :** Installation portuaires: Son rôle consiste :
  - Au déchargement des additifs importés des navires.
  - Au suivis des bacs de stockage (contrôle de température, niveau, pression, etc.)
  - Au transfert des additifs vers RA1Z par camions citerne.
  - Au chargement d'huiles de base dans les navires
- **Unité 3800 :** Pompage eaux brutes.
- **Unité 3900 :** Emballages divisionnaires

(Conditionnement des huiles finies bidon 2 L, 5 L)

- **Zone 16 :**

- Stockage eau brut pour incendie : 1 bac de 30000 T.
- Stockage du naphta : 2 bacs de 30000 T.

- Stockage du naphta : 2 bacs de 10000 T.
  - **Zone 17 :**
- Stockage du kérosène ; 2 bacs de 10000 T, 2 bacs de 20000T.
- Stockage d'essences de 1ere distillation ; 2 bacs.
  - **Zone 18 :** stockage du fuel pour mélange ; 5 bacs de 5000 T
  - **Zone 24** : stockage de gasoils ; 7 bacs.
  - **Zone 25** : stockage de fuel ; 6 bacs.
  - **Zone 26 :** stockage de GPL:
- 1 sphère de propane destinée aux unités lubrifiants et au marché.
- 3 sphères de butanes destinées au mélange de GPL.
- 2 sphères de butanes commerciales.
  - **Zone27 :** récupération des eaux usées ; 2 bassins de séparation et de décantation physique.
  - **Zone 28 :** zone d'expédition des produits finis (ajouts d'additifs, couleurs, odeurs, etc.).
  - **Zone 29 :** stockage du brut réduit importé.
  - **Zone 31 :** contient deux torches (P1)

I.6. *Mission de la Raffinerie d'Arzew* :

Les missions actuelles et futures de la Raffinerie d'Arzew sont au nombre de six:

1. Fournir la totalité du marché Algérien actuel et futur en lubrifiants, paraffines et graisses, dans les limites technologiques des installations.

2. Fournir la région Ouest et Sud Ouest en carburants selon besoins actuels et futurs.

3. Fournir le marché Algérien actuel et futur en bitumes, en coordination avec la Raffinerie de Skikda.

4. Maximiser la valeur des excédents exportables et atteindre les exigences du marché Européen en qualité de produits.

5. Adapter la Raffinerie à l'Essence et au Diesel aux normes et qualités Européennes.

6. Optimiser les consommations en additifs et produits chimiques.

Chapitre 2 :
Définition et concepts de base

II.1. Introduction :

On ne plaisante pas avec la sécurité. Que celle-ci concerne les personnes ou le matériel, elle constitue une notion d'importance croissante, dans tous les secteurs de production industriels. De plus en plus, en effet, « sécurité » rime avec « productivité».

Et comme toujours quand il s'agit de productivité, l'industrie cherche à améliorer, à optimiser ou encore pour ne pas mettre hors service l'ensemble d'une installation lorsqu'il n'est nécessaire d'en isoler qu'une partie. D'autres contraintes, comme la nécessité rencontrée parfois de redémarrer une application sous des conditions initiales précises, ont poussé les ingénieurs à mettre au point des systèmes de sécurité toujours plus intelligents, intégrant des fonctionnalités toujours plus complexes et évoluées.

Mais en dehors des composants indispensables pour permettre aux fonctions de sécurité d'assurer leurs rôles, il reste deux point essentiels qui ont bouleversé ces dix dernière années, ce sont d'une part les bus de sécurité et d'autre part les automates programmables dédiés à la sécurité.

II.2. Les bus de sécurité

Avec l'apparition des bus de terrain, il y a une vingtaine d'années, et le développement des technologies de communication, les milieux industriels ont connu une révolution majeure, tant dans la manière de véhiculer les informations issues des capteurs et actionneurs, que dans la manière de piloter les applications. Les bénéfices ont été largement décrits : réduction des coûts de câblage, d'ingénierie, de maintenance, flexibilité…

Et si pendant longtemps, les bus de communication ne se sont intéressés qu'aux équipements de contrôle-commande, et ont négligé la sécurité, aujourd'hui la donne a changé et les mentalités aussi. il n'y a même pas une dizaine d'années, il n'était pas question de mêler sécurité et bus de terrain sur le même media. Pas assez performants, pas assez ouverts.

Les technologies de la communication de terrain sont désormais éprouvées, et il ne se pose plus de problèmes de sécurité intrinsèques aux supports ou aux protocoles utilisés. Et les premiers bus de terrain permettant de « marier » contrôle-commande et sécurité sont apparus à la fin des années 90.

Il existe aujourd'hui différents types de bus de sécurité, parmi lesquels des solutions dédiées à la sécurité comme le ***Safetybus*** ou des solutions s'intégrant à une offre de bus de terrain existante. C'est le cas de ***Profibus*** avec ***Profisafe,as-interface*** avec ***As-iSafetyatWork*** … sans oublier les plus récents ***comme cc-Link*** . Pratiquement tous les bus ouverts ont, ou auront bientôt, une version sécurité.

II.3. Les automates de sécurité :

Les bus de sécurité viennent le plus souvent se connecter à ce que l'on appelle des APIdS : les automates industriels à la sécurité. C'est au début des années 80 que L'INRS « Institut National de Recherche et de Sécurité » mettait en garde la communauté industrielle a l'égard de l'utilisation d'Automates Programmables Industriels pour la gestion des fonctions de sécurité.
Celle-ci devait être confiée à une logique câble spécifique, permettant la mise en sécurité d'une machine même en cas de défaillance de l'API de commande.

Depuis, un nouveau type d'API a fait son apparition, sous l'appellation APIdS, capable d'assurer la gestion des fonctions de sécurité .En toute rigueur, il est impossible d'assurer intégralement les respects des exigences de sécurité avec des automates programmables industriel standard. Ceux-ci n'ont pas été conçus pour détecter toutes leurs défaillances internes, et ne peuvent pas adopter de position de sécurité le cas échéant. Les automates de sécurité se distinguent des API standard par la mise en œuvre de moyens spécifiques leur permettant de répondre à l'apparition d'une défaillance interne.

Notons qu'il est envisageable qu'un APIdS gère à la fois la commande et la sécurité. Ce type d'architecture peut être rencontré dans le cas de systèmes pour lesquels la commande et les sécurités sont fortement imbriquées, par exemple pour la commande de certaines machines telles que les presses mécanique. Une défaillance de l'APIdS pourrait conduire directement à l'accident, malgré les sécurités initialement prévues. Il faut préciser toutefois qu'un APIdS à justement été construit pour qu'une défaillance matérielle ou logicielle à une commande intempestive soit peu probable. Lorsque la complexité ou le nombre de fonctions de sécurités à traiter est important, il est envisageable de les gérer par un APIdS séparé de la commande fonctionnelle de la machine.

Deux grandes classes d'APIdS cohabitent : les APIdS orientés sécurité des processus, et les APIdS orientés sécurité des machines. Les premiers sont conçus pour assurer la disponibilité d'un processus, c'est-à-dire permettre la poursuite en toute sécurité d'un processus en cours, malgré la défaillance d'une voie de traitement. Ces automates mettent en œuvre des architectures redondantes d'ordre 3 avec « voting », ou des architectures d'ordre 2 avec détection du canal défaillant par le biais d'autotests. Seules ces structures sont capables d'une part de détecter la voie défaillante pour initialiser une procédure d'urgence, et d'autre part de poursuivre le processus en maintenant l'efficacité des sécurités.

Les seconds ont pour mission d'interrompre un mouvement dangereux lorsqu'une voie de traitement est défaillante. Les APIdS orientés sécurité des machine nécessitent des temps de réponse beaucoup plus courts que ceux dédiés à la sécurité des processus .cette différence est fondamentale car elle a une influence évidente, tant sur l'architecture interne des APIdS concernés que sur le contenu des logiciels applicatifs. Ces automates peuvent se contenter d'architectures redondantes d'ordre 2 avec comparateur permettant de vérifier que les deux voies, à partir des mêmes informations d'entrée, donnent les mêmes résultats en sortie. En réalité, les constructeurs d'APIdS dédiés à la machinerie ont

développé pour certains des structures redondantes d'ordre 2 et pour d'autres des structures tri-redondantes.

Il est possible de distinguer trois familles d'applications gérées par des APIdS. La première famille concerne les machines autonomes mettant en œuvre peu d'entrées-sortie, et dont les fonctions logique à réaliser sont assez simples et bien définies (presse, cisailles, presse plieuses……). Dans ce cas, il est possible de figer le logiciel applicatif, de le protéger contre toute modification non contrôlée et ensuite de le dupliquer sur tous les équipements pour lesquels il a été développé.

La deuxième famille rassemble l'ensemble des machines spécialesdéveloppées soit unitairement, soit en série limitées. Contrairement à la première famille, ces applications possèdent des logiciels applicatifs non standards. L'utilisateur ou l'intégrateur développe son propre logiciel applicatif. Ensuite, il doit le verrouiller pour éviter toute modification.

La troisième famille regroupe l'ensemble des applications pour lesquelles le logiciel applicatif gérant les fonctions de sécurité doit être facilement adaptable aux évolutions d'une production automatisée. Ce genre d'exigence est rencontré par exemple dans le bâtiment et les travaux publics. Cette obligation contraint l'intégrateur à fournir un système ouvert ne lui permettant pas de garantir une sécurité pérenne.

II.4. Les architectures redondantes :

Tout système électronique, quel qu'il soit, est caractérisé par une certaine sûreté de fonctionnement et une certaine disponibilité. Ces deux paramètres dépendent notamment de la manière dont sont conçus les systèmes, de la qualité des composants et des techniques de fabrication utilisés. Ils dépendent aussi de la manière dont travaillent les systèmes en interne, notamment des outils d'autodiagnostic et de la fréquence des tests embarqués mis en œuvre.

Bien conçu, fabriqué avec soin, utilisé normalement, un système électronique permet d'obtenir des performances très acceptables pour répondre à la plupart des besoins. Mais il est des applications où cela ne suffit pas. Pour aller plus loin encore, on ajoute des redondances, en multipliant le nombre des processeurs utilisés, et/ou éventuellement des entrées et/ou des sorties.

Il existe plusieurs types de redondances, qui donnent des résultats différents. Dans certaines applications, comme par exemple les serveurs utilisés dans les télécoms, la redondance sera surtout pratiquée pour obtenir une très grande disponibilité du système (quel usager du téléphone ou d'Internet accepte les interruptions de service?).

S'il s'agit de piloter un procédé dangereux, la redondance servira à garantir que le système de sécurité met le processus dans un état sûr quelles que soient les circonstances. Selon le résultat que l'on recherche, les redondances ne se font pas de la même façon. Le choix d'une architecture plutôt qu'une autre dépend en effet du niveau de sécurité que l'on veut atteindre mais aussi du niveau de disponibilité que l'on souhaite.

Avec les redondances relativement simples, on ne peut en général pas obtenir à la fois un niveau élevé de sécurité et une haute disponibilité. C'est l'un ou l'autre. Avec les redondances plus sophistiquées, il est possible d'avoir les deux, mais avec des gradations qui dépendent de l'architecture retenue.

II.4.1.Architecture à une seule unité centrale :

Comme son nom l'indique, il n'y a pas de redondance. Si un défaut dangereux est détecté au niveau de l'unité centrale, un module de diagnostic externe (*watch dog*) permet de déclencher immédiatement un arrêt d'urgence de façon à mettre le processus en sécurité.
Les pannes non dangereuses entraînent également un déclenchement de l'arrêt d'urgence.

II.4.2.Les multiples variantes des architectures dupliquées :

Les systèmes à deux unités centrales existent en de multiples variantes. Les deux unités centrales peuvent avoir des entrées et des sorties communes, ou alors des entrées et des sorties séparées. Ce qui distingue aussices systèmes, c'est la manière dont travaillent les unités centrales (types d'échanges qu'il y a entre elles) et la façon dont sont câblées les sorties qui commandent l'arrêt du processus (en parallèle ou en série).

Prenons par exemple le cas d'une architecture à deux unités centrales, chacune ayant ses propres entrées et ses propres sorties. On a donc deux canaux indépendants. Si les sorties sont câblées en série, il suffit qu'une des deux soit en défaut pour déclencher l'arrêt d'urgence du processus. On se trouve alors dans une configuration 1oo2, si l'on préfère 2-0. Le système est sûr mais il n'est pas tolérant aux pannes (sa disponibilité est peu élevée).Si au contraire les sorties sont câblées en parallèle, il faut que les deux sorties soient simultanément en défaut pour déclencher l'arrêt d'urgence du processus. Ceci réduit le nombre de déclenchements intempestifs. On se trouve alors dans une configuration 2oo2 (ou 2-1-0), qui assure une disponibilité élevée, mais dont la performance de sécurité est très pauvre.

Dans l'optique de fournir une disponibilité et une sécurité importantes, les architecturesdoubles sont maintenant réalisées dans une configuration 1oo2D, où on trouve un double câblage des sorties, à la fois série etparallèle. Cette architecture tolérante aux pannes fonctionne normalement dans unmode 2oo2 (2-1-0), mais revient à un mode 1oo2 (2-0) si une panne se produit et ne peut pas être résolue. De ce fait, sa performancede sécurité dépend évidemmentde l'efficacité des diagnostics internes dusystème, et sa disponibilité opérationnelle de la capacité de ce dernier à résoudre leserreurs et d'isoler le canal en faute, tout en continuant à fonctionner en sécurité sur le canal valide.
Les systèmes 1oo2D ne sont pas tous identiques, et quelques expériences significative sont démontré un manque de disponibilitérésultant de l'exécution des diagnostics decomparaison requis.

II.4.3.les architectures triplées

Tous les systèmes dupliqués un problème en commun : une sévère restriction du temps de fonctionnement en mode canal unique. Quelques fournisseurs tentent de contourner cette restriction en utilisant un modèle mathématique pour prévoir le taux d'exigence du processus, et ainsi allonger le temps de fonctionnement autorisé en canal unique. Cette approche n'est certainement pas recommandée pour la sécurité car les données exploitées dans de tels modèles ne sont qu'approximatives, et les résultats obtenus sont inappropriés pour être utilisés dans des décisions critiques de sécurité.

Les systèmes triplées (**TMR**) sont constitués de trois canaux, avec des sorties câblées à la fois en série et en parallèle. Ils sont très répandus et sont souvent utilisés dans des situations sans réelle justification technique ou économique.

L'architecture **TMR** est à la fois sûre et disponible, elle doit fonctionner en mode 2oo3 (3-2-0) pour des applications de sécurité. Le système **TMR** réalise des diagnostics par vote ou comparaison. De ce fait, il n'est pas autorisé à fonctionner en canal unique, car il manque de diagnostic interne détaillé et ne peut pas être considéré comme sûr. En fait, les limitations de temps sont imposées pour deux canaux en fonctionnement, et des étapes doivent être respectées pour s'assurer que le système s'arrêtera après la perte du second canal La redondance à trois module(**TMR**) est une forme de tolérance au fautes de N-redondance modulaire, où trois système gèrent la sécurité d'un procédé et le résultat est traiter par un système de vote pour produire une seul sortie .

Si n'importe lequel des trois systèmes échoue, les deux autres systèmes peuvent corriger et masquer le défaut. Et si le **voting** échoue alors le système complet échouera. Cependant, en un bon système **TMR**, le **voting** est beaucoup plus fiable que les autres composants **TMR**.

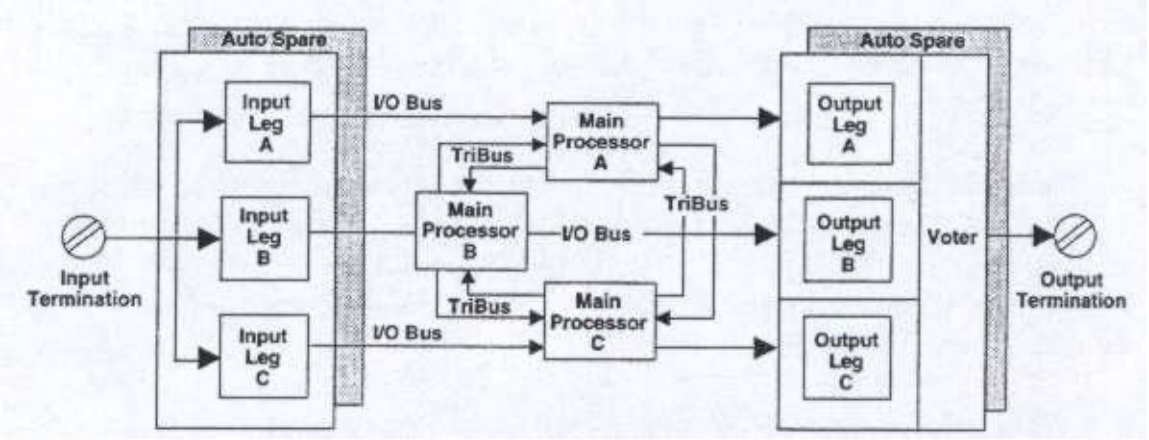


Figure II.1 : L'architecture interne du TMR

Un autre problème affecte l'architecture **TMR** : sa plus grande sensibilité (3 fois supérieure) concernant une erreur de mode commun due d'une part au

troisième niveau de redondance et d'autre part au fait que les canaux multiples partagent un ensemble "hardware" commun, telle une entrée-sortie commune, un module processeur etc. De plus, le coût initial et le coût de fonctionnement (incluant la maintenance) du système sont élevés.

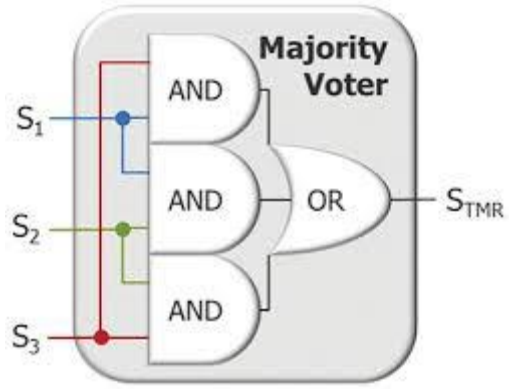


Figure II.2 :Le voting dans un système TMR

II.4.4.les architectures quadruplées :

La nouvelle architecture Quad (**QMR**) est une avancée importante au regard des performances liées à la sécurité. Cette propose quatre processeurs (2 par canal) et remédie aux problèmes associés aux architectures à double processeurs, comme les fautes dangereuses détectées d'un des deux processeurs. Les deux paires des processeurs sont synchronisées et utilisent le même programme. Un comparateur "hardware" et un chien de garde "fail-safe" supervisent le fonctionnement de chaque paire de processeurs pour diagnostiquer et résoudre les anomalies.

De ce fait, cette architecture peut fonctionner en **SIL3** (RC6) aussi bien sur un que deux canaux, pour une période de temps illimitée. Du fait de sa structure double et redondante, l'architecture **Quad** est intrinsèquement plus disponible qu'une architecture triplée. Elle est également meilleure en terme de sécurité. Elle apporte une amélioration d'un facteur trois, tant en disponibilité qu'en sécurité, par rapport à ce qui est normalement fourni par les architectures **TMR**. En outre, elle a une sensibilité significativement moindre aux erreurs de mode commun du fait d'une totale séparation, isolation et fonctionnement des canaux redondants.

Voyons plus précisément le problème de la sécurité. Dans les architectures dupliquées, le point crucial du problème concerne les erreurs dangereuses indétectées d'un les deux processeurs. Un processeur unique ne peut pas s'autocontrôler suffisamment pour être considéré comme complètement sûr, et il existe une possibilité qu'une telle erreur puisse mettre les deux canaux dans un état dangereux, et rendre l'automate incapable de se positionner dans une configuration de sécurité. C'est pourquoi de sévères restrictions de temps de fonctionnement sont imposées au niveau de **SIL3** (RC6) pour les architectures doubles fonctionnant dans des conditions d'erreur.

L'architecture Quad (**QMR**) intègre une paire de doubles processeurs opérant dans un mode de sécurité (2-0) pour chaque canal. Cette configuration augmente de façon significative les diagnostics des processeurs en opération, répond parfaitement aux critères de sécurité concernant les fautes dangereuses indétectées, et par conséquent supprime toutes les restrictions de temps de fonctionnement du système en mode mono canal.

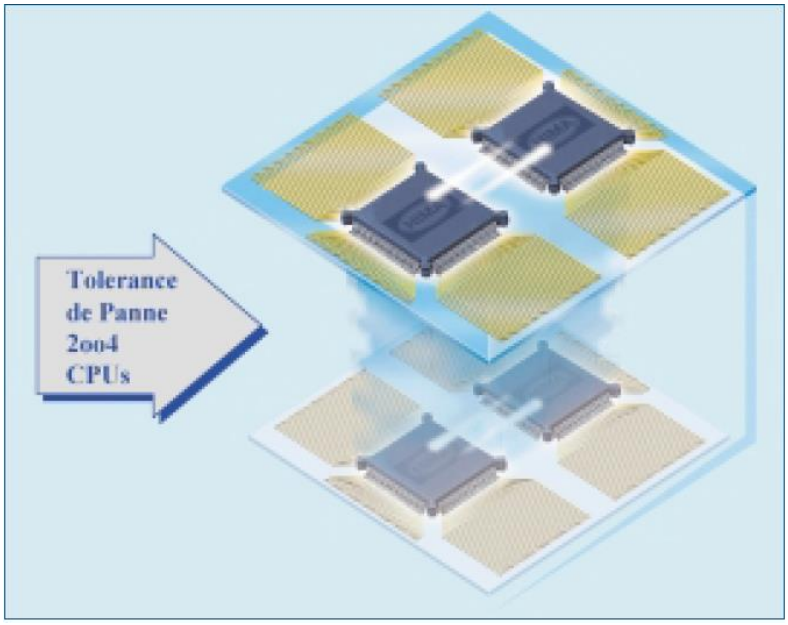


Figure II.3 :L'architecture QMR

Une comparaison des performances de sécurité (**PFD** : probabilité de défaillance sur sollicitation) des différentes architectures de sécurité peut être établie. Si l'on se réfère à l'**ISA TR84.02, Part 2, 1998**, on voit que l'architecture **Quad (2oo4)** est comparable à celle de l'architecture ultra sûre **1oo3**, tandis que l'architecture **TMR 2oo3** est identique à l'architecture **1oo2D**. Cette comparaison conclut à la prédominance de l'architecture **QMR 2oo4** par rapport à l'architecture **TMR 2oo3** ou dupliquée **1oo2D**.

Une autre considération importante dans la performance des systèmes de sécurité est leur capacité de détection de fautes internes de façon rapide et correcte. En effet, les automates de sécurité doivent être capables de répondre dans le temps de sécurité spécifiée (***safety time***).
Le temps de sécurité du processus (**TSP**) d'un processus donné est par essence le temps de tolérance aux pannes, avant d'atteindre une situation dangereuse. Ainsi, si une situation dangereuse existe pour un temps plus long que celui spécifié dans le TSP, le processus entre dans un état dangereux. Compte tenu de ces exigences, l'automate de sécurité doit maintenir un niveau de sécurité par la détection interne de fautes dangereuses et les corriger sans dépasser le **TSP**, ou en conséquence être considéré comme incapable de remplir les conditions de sécurité de ce processus.

Comme exemple typique, on peut citer le Système de Contrôle de Brûleur (**BMS**.) où le TSP d'une seconde est défini par **le TüV (DIN VDE 0116**). Compte tenu que deux cycles d'un automate sont demandés pour détecter et corriger une panne interne, le Temps de Détection et de Correction de la Faute **(TDCF)** de l'automate ne peut pas dépasser *500 ms*. Si l'automate de sécurité ne peut remplir cette condition, il ne peut pas être utilisé pour la sécurité d'application du **BMS.**

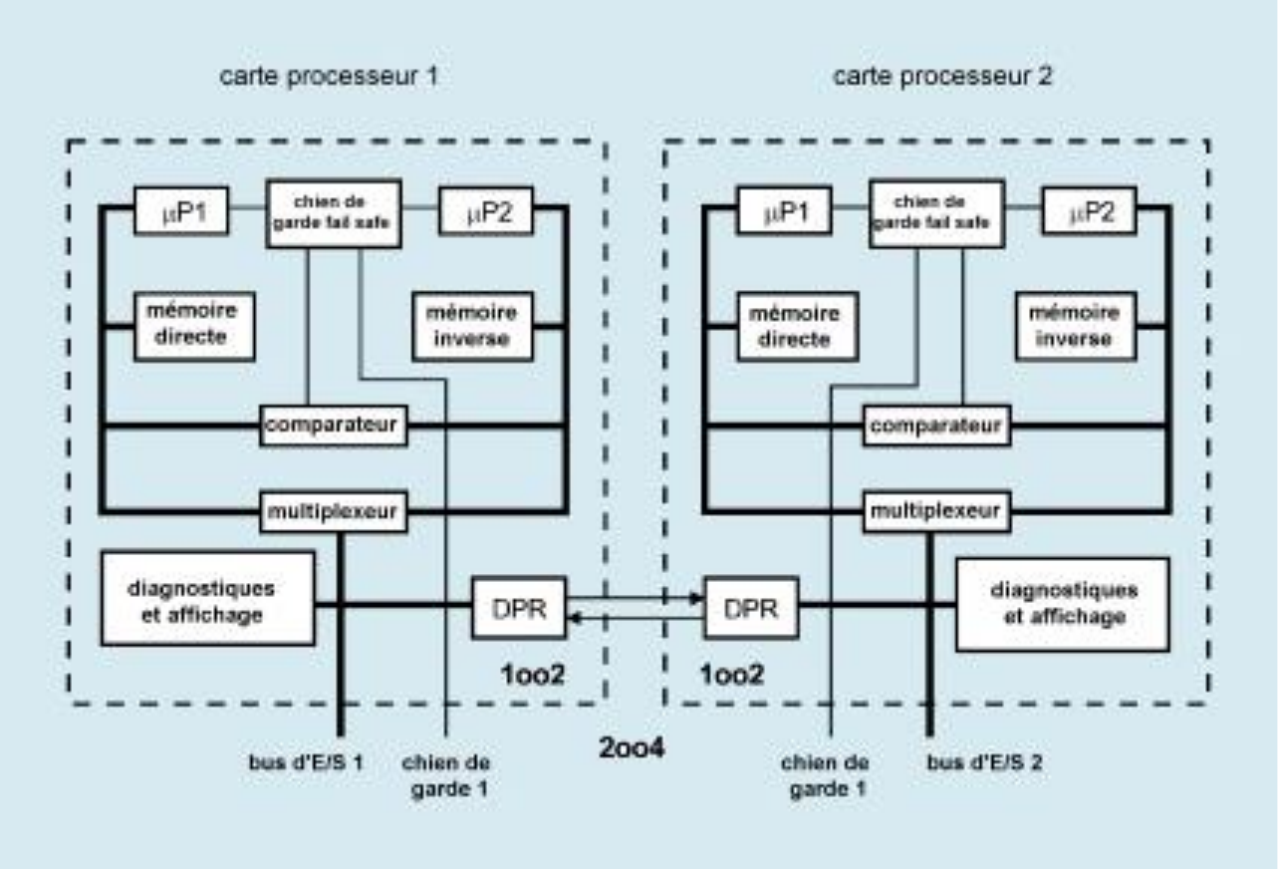


Figure II.4 : L'architecture Quad

II.4.5.Coût de fonctionnement :

Les normes de sécurité existantes et à venir demandent que le **SIS** (Safety Instrumented System/système instrumenté de sécurité) soit installé de façon à atténuer le risque associé au fonctionnement de processus dangereux. Ignorer ces spécifications n'est pas une option à long terme. De même, le coût initial et le coût de fonctionnement du SIS doivent être considérés. Il est reconnu que quelques architectures, du fait de leur complexité inhérente, engendrent des coûts d'achat et de fonctionnement importants. Ceci se vérifie pour des projets de petite taille ou des projets requérant un niveau de sécurité **SIL1** ou **SIL2**. Pour de tels projets, utiliser une architecture triplée (**TMR**) n'a pas de justification économique, compte tenu du coût initial et du coût de fonctionnement.

En outre, si un processus peut être d'un niveau **SIL1** ou **SIL2** au lieu de **SIL3**, des économies significatives peuvent être réalisées dans d'autres domaines (comme

les capteurs), ce qui permettra de ne pas utiliser d'architectures doubles ou triplées comme demandées pour les applications **SIL3**.
L'architecture Quad peut être configurée pour répondre aux exigences de performance des **SIL1, 2** et **3**. Elle peut fonctionner en canal unique ou redondant.

En canal simple, redondant ou triplée un capteur ou un actionneur est demandé pour fonctionner avec chaque boucle de sécurité. Que ce soit dans une configuration simple, sélectivement redondante ou complètement redondante, le niveau de sécurité **SIL3** est atteint.

Si la redondance est ajoutée, la disponibilité augmente considérablement et les performances de sécurité sont maintenues.
Ajouter la redondance ne représente pas un coût très important car les prix du processeur et des modules E/S sont significativement moins élevés que ceux des architectures alternatives. De plus, comme ces modules sont moins complexes, leur **MTBF** est de ce fait plus long et les dépenses de maintenance du système sont substantiellement réduites. Du fait que cette nouvelle architecture est relativement économique, elle apporte un bénéfice additionnel au niveau du contrôleur du processus dont l'automate de sécurité assure la protection.

De nombreuses normes de sécurité ne voient plus d'inconvénient à regrouper le contrôleur du processus et l'automate de sécurité dans un même système.
De même, il n'y a désormais plus de justification économique à vouloir prendre un seul automate de sécurité pour protéger plusieurs contrôleurs de processus. Il en résulte que l'installation du système de sécurité, les tests et la maintenance sont moins complexes et moins sujets à l'erreur humaine.
De plus, pour augmenter la sécurité, l'automate de sécurité dédié à un seul contrôleur de processus est nettement plus facile à maintenir ou à modifier. On élimine aussi toute possibilité d'arrêt d'urgence accidentel des autres unités de processus.

II.4.6.Comparaisondesdifférentesarchitectures redondantes :

a. Systèmes dupliqués

- Diagnostics intrinsèques aux modules.

- Certains automates fonctionnent en disponibilité ou en sécurité : les deux options ne sont pas obligatoirement cumulables.

- Temps de fonctionnement très restreint sur une seule unité centrale : disponibilité inférieure à celle du **TMR**

- Sécurité comparable à celle du **TMR**

- Prix compétitifs.

b. Systèmes triplés (TMR)

- Diagnostics par comparaisons

- Certains automates fonctionnent uniquement en sécurité.

- Temps de fonctionnement restreint sur deux unités centrales

- Pas autorisé à fonctionner en mono canal (1 unité centrale).

- Beaucoup de modes communs

- Niveau de sécurité comparable à celui obtenu avec un système dupliqué

- Prix initial et maintenance élevés : oblige souvent à regrouper plusieurs unités

c. Systèmes quadruplés (QMR) :

- Diagnostics intrinsèques aux modules

- Temps de fonctionnement illimité sur un seul canal : disponibilité supérieure à celle du **TMR**.

- Temps de fonctionnement illimité sur un seul canal en classe 6 (**SIL3**) : sécurité supérieure à celle du **TMR**

- Très peu de modes communs : séparation des canaux

- **MTBF** supérieur à celui du **TMR**

- Coûts d'achat et de maintenance identiquesà celui du dupliqué : convient à des projets de toutes tailles

II.5. L'offre TRICONEX :

Le **TRICON** est un automate programmable industriel, fabriqué et commercialisé par **TRICONEX** avec le plus grand soin, pour constituer, compte tenu des technologies actuelles et des exigences des procédés industriels, un équipement présentant les meilleures caractéristiques de disponibilité, de sécurité et maintenabilité.

Le **TRICON** est un système tolérant aux fautes grâce à son architecture triplée modulaire redondante TMR. IL a été conçu autour d'une architecture totale, depuis les points d'entrées jusqu'aux points de sortes en passant par les processeurs principaux. Chaque module d'entrée/sorties 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 leur données par l'intermédiaire de bus propriétaire à haute vitesse appelé **TRIBUS**. Une fois par période de scrutation, les trois processeurs principaux se synchronisent et communiquent entre eux par le **TRIBUS**.

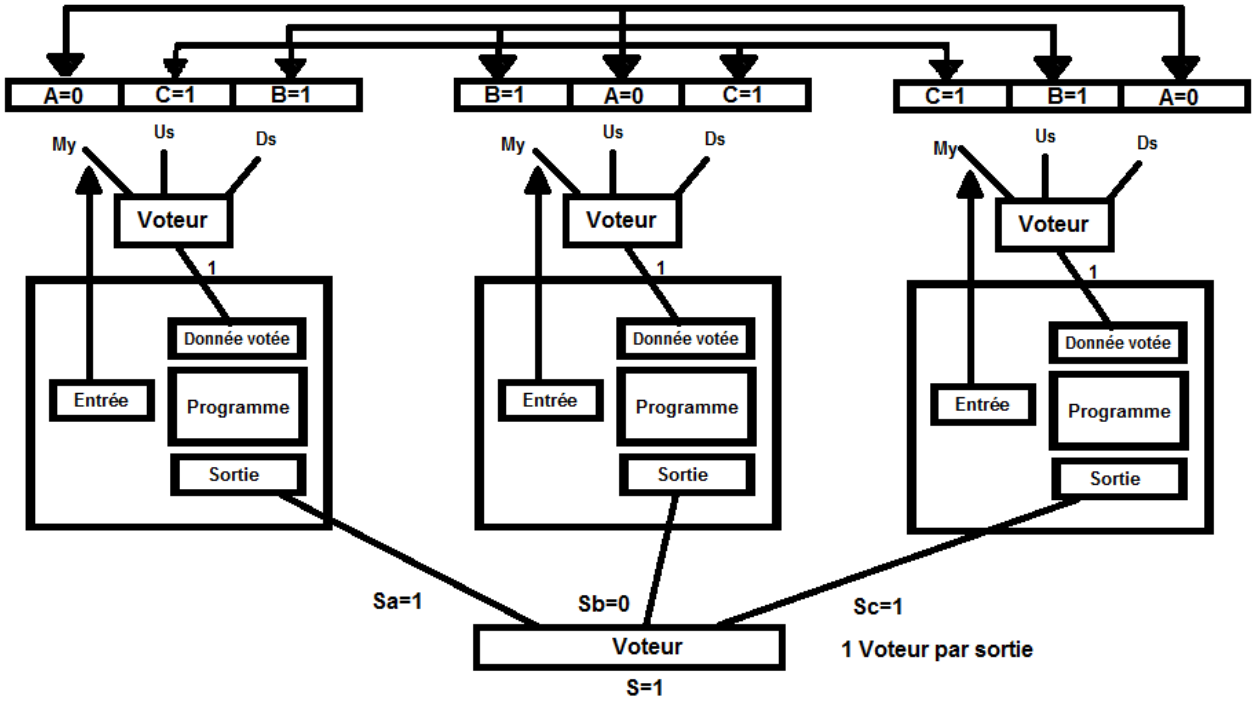


Figure II.5 : LE TRIBUS

Le **TRIBUS** vote les données d'entrées logique, compare les données de sorties et envoie une copie des valeurs d'entrées logiques à chaque processeur principal. 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 TRICON vote également les données de sorties. Cette opération est effectuée au niveau des modules de sorties juste en amont des

bornier de raccordement, ce qui permet de déceler et corriger toute erreur éventuelle entre le vote au niveau du TRIBUS et la sortie.
Pour chaque module d'entrées/sorties, il est possible de loger un module de pièce 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 module de même modèle qui manifeste un défaut n' importe où dans la configuration du système.

Le **TRICON** garantis in contrôle en continu, sans erreur en cas de défaillance des composants, ou de présence de fautes transitoires d'origines internes ou externes. Et la force du **TRICON** réside, justement dans sa tolérance aux pannes qui lui permet de répondre aux exigences d'aujourd'hui des procédés industriels. Cette tolérance aux pannes ne pouvait être réalisée qu'à travers le concept de l'architecture modulaire à redondance triplée(**TMR**).

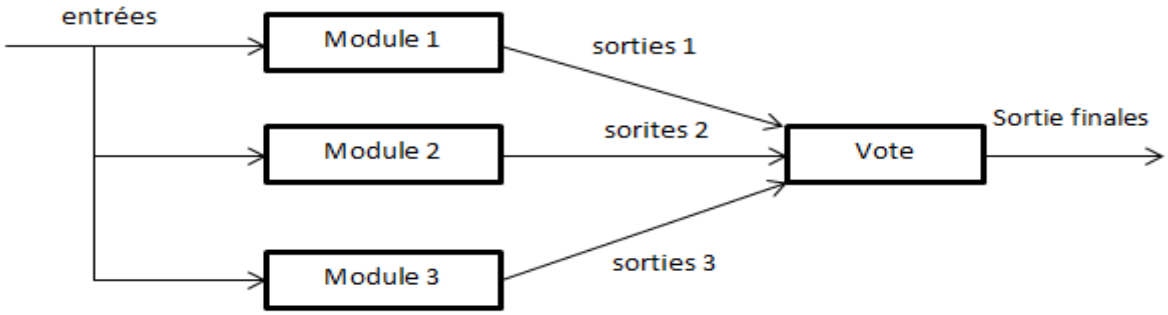


Figure II.6 : L'architecture modulaire à redondance triplée

Le système avec une telle architecture consiste en trois systèmes de contrôle parallèles et distincts intégrés dans un même ensemble matériel. Le vote des données logique de type deux sur trois (**2oo3**) garantit un fonctionnement en continu à haut niveau d'intégrité et sans erreurs. Pour l'utilisateur, le système **TRICON** constitue un seul ensemble matériel, ce qui permet de développer ainsi qu'un seul programme d'application et de le charger dans les trois processeurs en une seule opération. Une fois le programme d'application exécuté, les modules de sortie effectue un vote de type deux sur trois sur les valeurs calculées des sorties transmises par les trois modules processeur, puis envoient le résultat aux borniers de sortie et de là aux organes à commander sur le site.

Le **TRICON** est contrôleur à tolérance d'erreur haut de gamme, basé sur l'architecture redondante **TMR** (Triple Modular Redundant). Premier système triplement redondant, polyvalent et économique de l'industrie, il est le contrôleur de sécurité le plus éprouvé. **TMR** s'appuie sur trois systèmes de contrôle parallèles et isolés, et des fonctionnalités étendues de diagnostic, le tout intégré dans un système unique. Le système garantit une exploitation a haute intégrité, sans erreurs ni interruption, dépourvue de point de dysfonctionnement. Il simplifie le déploiement des applications, car il fonctionne comme un système de contrôle unique, de façon transparente pour l'utilisateur. Les fonctionnalités de diagnostic sont sous-jacentes et transparentes pour le programmeur. Toutes les informations de diagnostic sont stockées dans des variables système, à la disposition de l'utilisateur.

L'utilisation de **TRICON** continue de s'étendre à de nouvelles industries et applications, pour répondre à la demande croissante de sécurité système et/ou de haute disponibilité. Triconex a installé des systèmes de sécurité **TRICON** dans plus de 50 pays, améliorant la sécurité, la fiabilité et la disponibilité d'une large base installée à travers le monde.

II.5.1.Principaux avantages :

- Très haute intégrité en matière de sécurité : le système TRICON est conçu pour être utilisé dans le cadre d'arrêt de sécurité critique nécessitant une intégrité de niveaux 1,2 ou 3, tels que définis dans la norme de sécurité IEC 61508.

- Haute disponibilité : TRICON est compatible avec les systèmes à un, deux ou trois processeurs. Les modules défectueux peuvent être remplacés sans arrêter le système, pour un contrôle ininterrompu.

- Faibles coûts de maintenance : les fonctionnalités de diagnostic intégrées détectent automatiquement les dysfonctionnements des modules, économisant du temps et des ressources.

II.5.2.Principales fonctionnalités :

- Aucun point de panne : la panne d'un seul composant n'affecte pas le bon fonctionnement du système TRICON

- Diagnostic du système TRICON

- Diagnostics étendus : les systèmes TRICON offre un diagnostic complet en ligne, sans matériel ni programmation logicielle supplémentaire.

- Dépannage en ligne : remplacement de modules « à chaud », sans interruption système ou processus, pour une exploitation en continue.

- Programmation aisée : le logiciel de programmation de Triconex, conforme à la norme IEC 61131-3, offre la possibilité de programmer en blocs de fonction, texte structurés ou schémas Ladder, pour une configuration et une émulation de programme rapide.

Figure II.7 : Le TRICON

II.6. Les normes de sécurité :

Les principales normes de référence en matière de sécurité sont l'IEC 61508 (systèmes *de sécurité*) et l'IEC 61511 (systèmes instrumentés de sécurité). La norme **IEC 61508 (IEC, 1998)** est une norme internationale qui porte plus particulièrement sur les systèmes E/E/PE (électriques/électroniques/électroniques programmables) de sécurité. La norme propose une approche opérationnelle pour mettre en place un système de sécurité E/E/PE, en partant de l'étude des exigences de sécurité (avec une définition du périmètre couvert, une analyse et une évaluation du risque) et en prenant en compte toutes les étapes du cycle de vie du système E/E/PE. Un des intérêts de cette norme est d'être générique et donc d'être applicable dans tous les secteurs où la sécurité peut être traitée avec des systèmes E/E/PE : industries manufacturières, industries des processus continus, pharmaceutiques, nucléaires, ferroviaires etc.

La norme **IEC 61511 (IEC 61511,2000)** concerne les **SIS** qui sont basés sur l'utilisation d'une technologie **E/E/PE.** Elle permet de définir des exigences relatives aux spécifications, à la conception, à l'installation, à l'exploitation et à l'entretien d'un **SIS**, de telle manière qu'il puisse être mis en œuvre en toute confiance, et ainsi établir et/ou maintenir les processus dans un état de sécurité convenable. Dans le cas où d'autres technologies sont utilisées pour les unités logiques, il convient aussi d'appliquer les principes fondamentaux de cette norme. Cette norme concerne également les capteurs et les éléments terminaux des **SIS**, quelle que soit la technologie utilisée. Cette norme est spécifique à la production industrielle par processus dans le cadre de **l'IEC 61508**. Nous pouvons ainsi conclure que l'**IEC 61511** est destinée aux intégrateurs et aux utilisateurs, alors que l'**IEC61508** reste une norme générique difficile à mettre en œuvre et dont les fabricants et les fournisseurs de systèmes **E/E/PE** se la sont appropriée.

Ces normes définissent des niveaux **SIL** (*Security Integrity Level*), calculés en fonction de la probabilité moyenne de défaillance sur sollicitation.

Certains fournisseurs n'hésitent pas à revendiquer un niveau de **SIL** pour un équipement. Mais ces informations sont à prendre avec beaucoup de précautions, car en aucun cas le niveau **SIL** ne saurait être une caractéristique d'un équipement. Tout au plus est-il possible d'indiquer une compatibilité avec un niveau de SIL donné. Celui-ci est en effet strictement associé à une fonction de sécurité et à rien d'autre, laquelle est réalisée par la mise en œuvre de plusieurs sous-systèmes : capteurs, traitements, actionneurs.

Par exemple, d'après **l'IEC 61511**, pour atteindre un niveau **SIL3** avec des composants éprouvés, globalement de sécurité positive et dont la configuration est verrouillée, il faut une redondance. Certains fournisseurs n'hésitent donc pas à afficher un niveau Sil4, sans préciser que cela s'entend avec une tolérance à ma panne de deux, ce qui signifie qu'il faudra utiliser trois composantes de redondances pour être compatible avec ce niveau de **SIL**. Dans ce cas le niveau de SIL peut ne pas être atteint, les trois composants identiques introduisant un mode commun de défaillance important.

De la norme à la qualification : la norme **IEC 61511** découle de la norme **IEC 61508** et concerne les systèmes instrumentés de sécurité pour le secteur des industries de transformation. Elle impose des exigences sur la gestion des projets intégrant des fonctions instrumentées de sécurité (SIF) par :

- Des méthodes et techniques de conception et d'évaluation des **SIF** et **SIS**
- L'identification des responsabilités
- Installer un langage commun « Sécurité Fonctionnelle » (concepteur, installateurs, chargée de maintenance, utilisateur, administrateur…

II.6.1. Architecture pour le mode de fonctionnement faible demande (selon l'IEC 61508) :

1) 1oo1

Cette architecture comprend un seul élément, et toute défaillance dangereuse empêche le traitement correct de tout signal d'alarme valide.

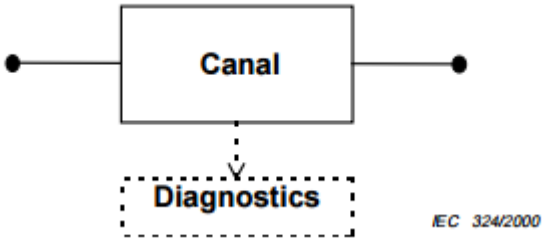


Figure II.8 : Diagramme du bloc physique 1oo1

2) 1oo2 :

Cette architecture comprend deux canaux connectés en parallèle de façon que chacun puisse traiter la fonction de sécurité. Ainsi, il faudrait qu'il y ait une défaillance dangereuse dans les deux canaux pour qu'un signal d'alarme valide ne soit pas traité correctement. On suppose que tout test de diagnostic ne révélerait

que les anomalies découvertes et ne modifierait pas les états de sortie ou la logique majoritaire des sorties.

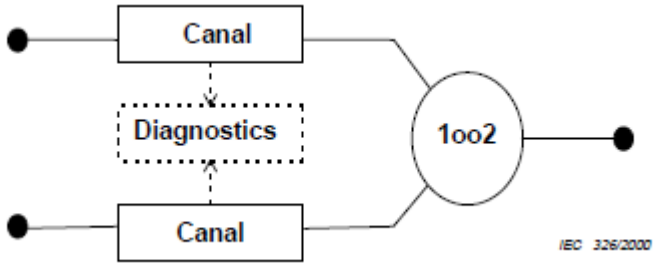


Figure II.9 : Diagramme du bloc physique 1oo2

3) 2oo2 :

Cette architecture comporte deux canaux connectés en parallèle de sorte qu'il est nécessaire que les deux canaux demandent la fonction de sécurité avant que celle-ci ne survienne. On suppose que tout test de diagnostic n'indiquerait que les anomalies découvertes et ne modifierait pas les états de sortie ou la logique majoritaire de sortie.

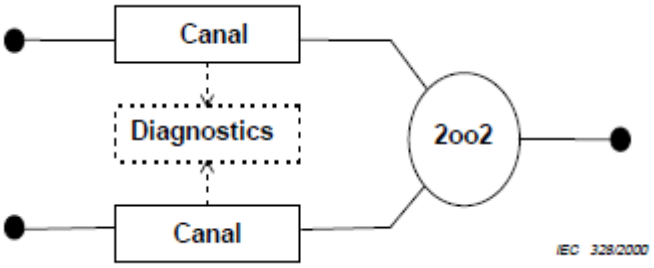


Figure II.10 : diagramme du bloc physique 2oo2

4) 1oo2D :

Cette architecture comprend deux canaux connectés en parallèle. Dans des conditions normales d'utilisation, les deux canaux doivent demander la fonction de sécurité avant que celle-ci ne survienne. De plus, si les tests de diagnostic détectent une anomalie dans l'un des canaux, la logique majoritaire de sortie s'adapte de sorte que l'état de la sortie générale suive alors celui de l'autre canal. Si les tests de diagnostic décèlent des anomalies dans les deux canaux ou une divergence qui ne peut être attribuée à l'un des canaux, la sortie se met alors en sécurité. Pour détecter une divergence entre les canaux, chaque canal peut déterminer l'état de l'autre canal par un moyen indépendant de l'autre canal.

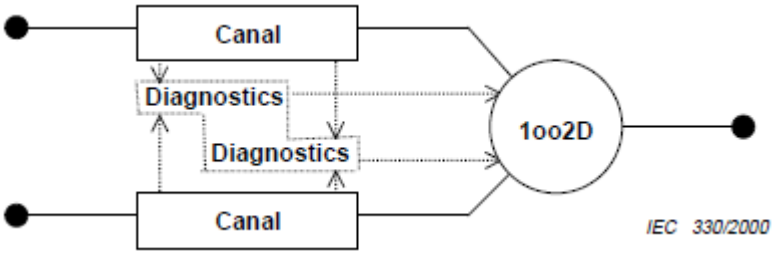


Figure II.11 : diagramme du bloc physique 1oo2D

5) 2oo3 :

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

On suppose que tout test de diagnostic n'indiquerait que les anomalies décelées et ne modifierait ni les états de sortie, ni la logique majoritaire.

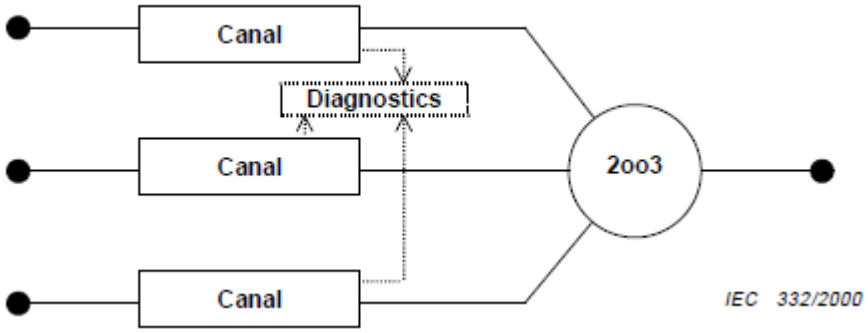


Figure II.12: diagramme du bloc physique 2oo3

II.6.2.Architecture pour le mode de fonctionnement demande élevé ou continue (selon l'IEC 61508) :

Les architecture pour le mode de fonctionnement demande élevé sont identique à celles du mode faible demande, et seule différence réside dans les formules de calcule des **PFD**.

Chapitre3 :

L'ÉTUDE DE SAFETY INTEGRITY LEVEL (SIL)

III.1. Introduction :

Les systèmes Instrumenté de sécurité (**SIS**) sont utilisé pour assurer la sécurité fonctionnelle des installations,i.e :la réduction des risques à un niveau inférieur ou égal au risque tolérable.

Pour concevoir les **SIS**, deux norme de sécurité sont utilisé : **l'ANSI/ISA S84.01-1996** et **l'IEC 61508**. Ces deux normes sont basées sur le principe de l'évaluation de la réduction de la prescription nécessaire pour atteindre un niveau de risque acceptable. Ils établissent les prescriptions relatives à la spécification, la conception, l'installation, l'exploitation et la maintenance du **SIS**, afin d'avoir toute confiance dans sa capacité à amener et/ou à maintenir le procédé dans un état de sécurité.

Les étapes de base requises pour assurer la conformité suivant ces deux normes de sécurité sont :

- ✓ Etablir une cible de sécurité (risque acceptable) du procédé et évaluer le risque existant
- ✓ Identifier les fonctions de sécurité requises et leurs affecter un niveau de protection
- ✓ Déterminer si la fonction instrumentée de sécurité requise
- ✓ Implémenter la fonction instrumentée de sécurité dans un SIS et déterminer le **SIL** du **SIS**
- ✓ Vérifier que le **SIS** permet d'atteindre la cible de sécurité exigée au départ

La norme **IEC 61508** décrit tant la nature de l'évaluation des risques que la réalisation de fonctions de sécurité pour les capteurs, le traitement logique et les actionneurs. Ces mesures comprennent une « suppression des risque » (défauts systématique) et une « maîtrise des risque » (défauts aléatoire).

Ce standard de base, indépendant des applications, décrit les exigences quand aux fonctions de sécurité des composants et systèmes et permet de développer des normes spécifiques branches (par exemple le projet **IEC 61511** « Sécurité fonctionnelle : systèmes de sécurité pour l'industrie des process »).

La norme **IEC 61511** détermine entre autres des critères de sélection pour les composants des fonctions de sécurité, comme par exemple les performances des capteurs et actionneurs.

III.2. Généralités :

III.2.1. Sécurité Fonctionnelle

"Sous-ensemble de la sécurité globale, relatif aux équipements et aux systèmes de contrôle-commande associés, qui dépend du fonctionnement correct de systèmes électriques, électroniques, programmables électroniques (E/E/PE) concernés par la sécurité". Les exemples suivants sont des systèmes E/E/PE concernés par la sécurité :

• un système de déclenchement dans une usine chimique dangereuse,

• un système de signalisation ferroviaire,

• des inter verrouillages de protection et un arrêt d'urgence sur une machine,

• un variateur de vitesse utilisé pour contrôler une vitesse en tant que moyen de protection.

III.2.2. Fonction de sécurité :

La fonction de sécurité doit être implémentée dans un système E/E/PE concerné par la sécurité dont le but est d'atteindre ou de maintenir un état sûr pour les équipements contrôlés, dans le cadre d'un évènement dangereux particulier.

III.2.3. Système concerné par la sécurité :

Système qui implémente les fonctions de sécurité nécessaires pour atteindre ou maintenir un état sûr pour les équipements contrôlés, et qui est destiné à atteindre, seul ou avec d'autres systèmes **E/E/PE** concernés par la sécurité, l'intégrité de sécurité requise par les fonctions de sécurité.

III.2.4. système instrumenté de sécurité *(SIS)*:

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

- **une partie capteur** chargée de mesurer la dérive d'un paramètre (pression, température ...) vers un état dangereux ;
- **une partie système de traitement logique (UTL)** chargée de récolter le signal provenant du capteur, de traiter celui-ci et de commander l'actionneur associé ;
- **une partie actionneur** chargée de mettre le procédé dans sa position de sécurité et de la maintenir.

Figure III.1 : structuregénérald'un système instrumenté de sécurité (SIS)

La probabilité de défaillance sur demande du SIS est déterminée par le calcul et la combinaison des probabilités de défaillance de ses composants. Ces probabilités dépendent des taux de défaillances des composants, des taux de défaillances dangereuses détectées et du facteur qui caractérise les défaillances de cause commune.

III.2.5. Intégrité de sécurité

Probabilité qu'un système concerné par la sécurité exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et dans une période de temps donnée.

III.3. *Niveau d'intégrité de sécurité (SIL)* :

Un **Safety Integrity Level** (**SIL** ou niveau d'intégrité de sécurité) est défini comme un niveau relatif de réduction de risques inhérents à une fonction de sécurité, ou comme spécification d'une cible de réduction de risque. Plus simplement, c'est une mesure de la performance attendue pour une fonction de sécurité (ou **SIF**).

Les exigences pour un niveau donné de SIL ne sont pas toujours cohérentes entre les différentes normes traitant de sécurité. Dans les 'European Functional Safety standards', on trouve la définition de quatre **SIL**, allant de **SIL 1** pour le moins sûr à **SIL 4** pour le plus sûr (grande fiabilité).A chaque **SIL** (valeur discrète de 1 à 4) correspond un niveau de réduction de risque croissant et donc à des exigences croissantes.

Un **SIL** est déterminé à partir d'un certain nombre de facteurs quantifiés dans la gestion du cycle de développement et/ou du cycle de vie… Le concept de SIL s'applique donc au système concerné par la sécurité dans son intégralité et par à un sous-ensemble (i.e. : un capteur).

III.3.1. Les avantages du SIL :

- procédure internationale harmonisée pour l'évaluation de dispositifs de protection
- évaluation de systèmes de conduite de procédé quand aux erreurs systématiques et aux indications statistique relatives aux erreurs aléatoire

- « Life cycle management » définit, c'est-à-dire documentation et gestion de toutes les étapes du cycle de vie se rapportant aux fonctions des équipements
- Evaluation complète de toute l'installation de sécurité
- La sécurité requise peut être obtenue par une instrumentation éprouvée, sans modification exhaustives des techniques de processus.

III.3.2. Relation entre matériel et SIL :

Une confusion courante concerne l'association d'un **SIL** à un matériel. Ce malentendu a été entretenu par de nombreux constructeurs et fournisseurs de matériels qui ont rapidement perçu l'intérêt marketing et économique de labelliser leurs produits en leur associant un « **SIL** ». L'utilisateur a alors logiquement associé le SIL à un élément de la chaine automatisée de sécurité (capteur, transmetteur, automate, vanne, ….etc.) il a donc logiquement abordé la construction du SAS (Système Automatisé de Sécurité) par un simple assemblage de produits au moins labellisés du niveau d'intégrité ciblé.

Mais ; tout comme la conformité d'une machine ne s'obtient pas par assemblage de constituants certifiés **CE**, le SIL d'un **SAS** ne d'obtient pas par assemblage de composants estampillés **SIL**.

Lorsqu'un un matériel est proposé **SIL2**, par exemple, ceci sous-entend qu'il a été validé par le constructeur et/ou labellisé par un organisme tiers. Ce matériel a été jugé capable d'être intégré dans un système instrumenté de sécurité jusqu'à une intégrité de de sécurité de niveau 2 maximum.

Bien que le matériel soit **SIL** capable, une GROSSE marche reste à franchir pour que la fonction de sécurité dans laquelle il sera intégré, soit également **SIL2**. Le **SIL**, c'est avant tout l'intégrité de 'organisation. Le **SIL** est associé à une fonction (**SIF**), il n'est pas associé à un matériel ou à une installation, outre les exigences matérielles, il comprend des exigences humaines et organisationnelles

Le **SIL** correspond à des exigences pour contre les défaillances dangereuses systématique et aléatoires. Les mesures de défense contre les défaillance systématique reposent principalement sur des exigence qualitatives (contrôles, audits, cycle en vie , …..). Les mesures pour contrer les défaillances aléatoires reposent principalement sur exigences quantitative (PFD, **SFF**,….etc.).

Bien que globalement toutes ces normes relatives à la sécurité fonctionnelle utilisent les mêmes paramètres pour évaluer le **SIL** atteint, il existe certaines différences dans les termes et exigences qui reflètent les habitudes et les caractéristiques propres à chaque secteur.

Aussi, en annonçant une valeur **SIL**(n), il convient de préciser à quelle norme il est fait référence.

III.3.3. La relation entre PFD et SIL :

Le tableau suivant donne le SIL du SIS en fonction de la valeur de son PFD (probabilité de défaillance sur sollicitation) et de sa fréquence de sollicitation.

SIL	Faible demande (PFD_{avg})	Demande élevée (Défaillances/heure)
4	$10^{-5}<PFD<10^{-4}$	$10^{-9}<PFD<10^{-8}$
3	$10^{-4}<PFD<10^{-3}$	$10^{-8}<PFD<10^{-7}$
2	$10^{-3}<PFD<10^{-2}$	$10^{-7}<PFD<10^{-6}$
1	$10^{-2}<PFD<10^{-1}$	$10^{-6}<PFD<10^{-5}$

Tableau III.1 : Relation entre PFD et SIL

III.3.4. Détermination du SIL :

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 ;
- **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 le PFD des SIS à partir des probabilités de défaillances de leurs composants. Les méthodes les plus répandues sont :
  - les équations simplifiées,
  - les arbres de défaillances,
  - les approches Markoviennes.

III.4. Matrice de risque :

III.4.1. Définition :

Méthode semi quantitative permettant de déterminer le niveau d'intégrité de sécurité d'un système relatif à la sécurité à partir des facteurs de risque connus.

La procédure est basée sur l'équation suivant : **R = F × C** où

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

F : est la fréquence de l'évènement dangereux en l'absence de systèmes relatifs à la sécurité.

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

Dans notre étude on considère les conséquences sur :

1. Les dommages liés à la santé.
2. Les dommages économiques.
3. Les dommages provenant de dégâts environnementaux.

III.4.2. *Mise en œuvre de la matrice de risque* :

III.4.2.1. *Facteur de réduction* : La fréquence de l'évènement dangereux F est supposée être le résultat de trois facteurs :

1. Taux de demande :

La probabilité que l'évènement dangereux se produit e l'absence de système relatif à la sécurité (mais en présence de dispositif externe de réduction de risque). C'est ce que l'on appelle la probabilité d'occurrence non souhaités.

Pour déterminer le taux de demande il faut définir en première étape les causes de la fonction de sécurité. Dans le tableau suivant les différentes catégories de taux demande sont indiquées.

Catégorie	Taux de demande (intervalle entre les demandes)
D0	Négligeable
D1	< 20 ans
D2	4 à 20ans
D3	6 mois à 4ans
D4	> 6 mois

Tableau III.2: catégorie des taux de sollicitation

2. Exposition et possibilité d'avertit le danger : Les tableaux III.3 et III.4 indiquent les trois catégories pour les deux facteurs :

- Fréquence et durée d'exposition dans une zone dangereuse
- Possibilité d'évité l'événement dangereux

F1	Très rare (<10 homme-minutes/jour)
F2	Occasionnel (<6 homme-heure/jour)
F3	Endroit fréquenté (>6 homme-heur/jour)

Tableau III.3 :Exposition

P1	Dans toute circonstance
P2	Dans quelque circonstance
P3	Peu ou nul

Tableau III.4 : Possibilité d'avertir le Danger

3. La réduction de classification des conséquences : La réduction après l'introduction des deux facteurs F et P est indiquée dans le tableau 5

Possibilité d'avertir le danger	**P3**	**-1**	**0**	**0**
	P2	**-1**	**-1**	**0**
	P1	**-2**	**-1**	**-1**
		F1	**F2**	**F3**
		Exposition		

Tableaux III.5 : Réduction sur la classification des conséquences.

III.4.2.2. *Conséquence sur la santé et la sécurité du personnel* :

L'étude SIL détermine six catégories des Conséquence sur la santé et la sécurité du personnel.

Catégorie	Conséquences
S0	Aucune blessure ou effet sur la santé
S1	Blessure ou effet sur la santé négligeable
S2	Blessure ou effet sur la santé mineur
S3	Blessure ou effet sur la santé grave
S4	Un à trois Fatalité
S5	Fatalités multiples

Tableaux III.6 : Catégories des conséquences sur la santé et la sécurité du personnel

III.4.2.3. *Conséquence économique* :

Les conséquences économiques sont classées en six catégories :

Catégorie	Conséqul2ences
L0	Aucune perte
L1	Perte légère
L2	Perte minime
L3	Perte locale
L4	Perte majeur
L5	Perte étendue

Tableaux III.7 : catégorie des conséquences économiques

III.4.2.4. Conséquence sur l'environnement :

La méthodologie du SIL définit les conséquences sur l'environnement en six, catégories :

Catégories	Conséquence	Description
E0	Sans effet	Aucun impact sur l'environnement, sans incidence financière.
E1	Effet léger	Effet sur l'environnement local à l'intérieur de la limite de la clôture, conséquence financières négligeables
E2	Effet minime	Contamination suffisante pour créer un dégât environnemental, aucun effet permanant sur l'environnement
E3	Effet local	Décharge limitée de toxicité connue, le voisinage est effectué au-delà de la limite de clôture
E4	Effet majeur	Dégât sévère sur environnement, la société devra prendre des mesures supplémentaires pour restaurer l'environnement contaminé et le rendre à son état initial
E5	Effet massif	Dégât constamment sévère sur l'environnement ou nuisance sévère dépassant une large surface, perte commerciale, conséquence financière importante pour préservation de la nature.

Tableaux III.8 : catégorie des conséquences environnementales

III.4.3.La matrice de risque :

La matrice de risque utilisé pour classification du SIL est la suivante :

Catégorie de conséquence			Catégorie du taux de sollicitation				
S	E	L	D0	D1	D2	D3	D4
Santé &sécurité	Environnement	Economique					
S0	E0	L0	-	-	-	-	-
S1	E1	L1	-	-	-	-	1
S2	E2	L2	-	-	-	1	2
S3	E3	L3	-	-	1	2	3
S4	E4	L4	-	1	2	3	4
S5	E5	L5	-	2	3	4	X

Tableau III.9 : La matrice de risque

III.5. Probabilité moyenne de défaillance sur demande :

Pour le mode de fonctionnement faible demande, la probabilité moyenne de défaillance sur demande d'une fonction de sécurité d'un système E/E/PE relatif à la 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. Cela peut être exprimé par la formule suivante :

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$ Ou :

_ **PFD_{SYS}** est la probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système E/E/PE relatif à la sécurité

_ **PFD_S** est la probabilité moyenne de défaillance sur demande du sous-système capteur

_ **PFD_L** est la probabilité moyenne de défaillance sur demande du sous-système logique

_ **PFD_{FE}** est la probabilité moyenne de défaillance sur demande du sous-système élément final

CHAPITRE IV

ETUDE SIL APPLIQUÉE A UN FOUR : 11-F-3 , UNITÉ 11

IV.1. Introduction :

Dans ce chapitre nous allons appliquer la méthode de la matrice de risque pour la détermination du niveau de SIL des fonctions de sécurité attribué au four 11F3 de l'unité 11 (Distillation atmosphérique).

IV.2. Description de l'unité 11 :

Cette unité d'une capacité de 2.5 millions de tonnes est calculée pour produire ce qui suit à partir du brut de Hassi-Messaoud :

Cette unité est subdivisée dans les circuits principaux suivants :

- Circuit préchauffage du naphta.
- Four 11-F-1, 11-F-2, 11-F-3.
- Colonne de distillation 11C-9 .
- Système d'injecteur
- Traitement du Kérosène.
- Module de récupération des gaz torché
- Système de close-drain
- Sour water stripper

IV.3. La matrice Cause / Effet :

Interlock No	Mis en action par	Action (agit) sur
11-I-1551	11-FSLL-129 (bas débit charge four passe 1)	Fermeture : 11-UV-101 Fermeture : 11-UV-102 Ouverture : 11-UV-103 Fermeture : 11-PV-114 Fermeture : 11-UV-114 Fermeture : 11-UV-113 Ouverture : 11-UV-112
11-I-1552	11-FSLL-130 (bas débit charge four passe 2)	Fermeture : 11-UV-101 Fermeture : 11-UV-102 Ouverture : 11-UV-103 Fermeture : 11-PV-114 Fermeture : 11-UV-114 Fermeture : 11-UV-113 Ouverture : 11-UV-112
11-I-1553	11-TSHH-122 (très haute température a la sortie du four)	Fermeture : 11-UV-101 Fermeture : 11-UV-102 Ouverture : 11-UV-103 Fermeture : 11-PV-114 Fermeture : 11-UV-114 Fermeture : 11-UV-113 Ouverture : 11-UV-112
11-I-1554	11-PSLL-116 (Très Basse pression gaz pilote)	Fermeture : 11-UV-101 Fermeture : 11-UV-102 Ouverture : 11-UV-103 Fermeture : 11-PV-114 Fermeture : 11-UV-104 Fermeture : 11-UV-105 Ouverture : 11-UV-106 Fermeture : 11-UV-114 Fermeture : 11-UV-113 Ouverture : 11-UV-112

11-I-1555	11-I-15 (très haut pression au niveau de la colonne)	Fermeture : 11-UV-101 Fermeture : 11-UV-102 Ouverture : 11-UV-103 Fermeture : 11-PV-114 Fermeture : 11-UV-114 Fermeture : 11-UV-113 Ouverture : 11-UV-112
11-I-1556	11-HS-11 (l'arrêt D'urgence)	Fermeture : 11-UV-101 Fermeture : 11-UV-102 Ouverture : 11-UV-103 Fermeture : 11-PV-114 Fermeture : 11-UV-114 Fermeture : 11-UV-113 Ouverture : 11-UV-112
11-I-1557	11-PSLL-115 (très basse pression gaz brûleur)	Fermeture : 11-UV-101 Fermeture : 11-UV-102 Ouverture : 11-UV-103 Fermeture : 11-PV-114
11-I-1558	11-PSHH-115 (Très haute pression gaz brûleur)	Fermeture : 11-UV-101 Fermeture : 11-UV-102 Ouverture : 11-UV-103 Fermeture : 11-PV-114

Tableaux IV.1 : Matrice CAUSE/EFFET

IV.4. *Application de l'étude SIL sur le four 11-F-3 de l'unité 11* :

Dans cette partie de l'étude on procède à la détermination du SIL Traget (cible)

SIL Classification workseet :			
Système	Four 11-F-3	**SIFN° :**	11-I-1551
Définition du SIF :	Très bas débit du NAPHTA dans le premier passe : 1. Fermeture des vannes d'alimentations FG (11-UV-101/102) 2. ouverture de la vanne vers atmosphère (11-UV-103) 3. fermeture de la vanne de gaz bruleur (11-PV-114) 4. fermeture de la vanne d'alimentation FO (11-UV-113/11-UV-114) 5. ouverture de la vanne de circulation (11-UV-112)		
Cause :	Déclenchement des pompes d'alimentation du NAPHTA (11-p-72/11-p-61) ou mal fonctionnement des boucles du contrôle du débit dans les passes du four		
Protection :	(11-FSLL-129) fournit sur la line de décharge de la pompe boosté (cette protection ne peut être appliquée quand le débit est faible dans un seul passe		
Scénario de danger :	Haute température du passe concerné. Cokéfaction peut apparaitre a l'intérieure, et dans le cas externe fusion du tube de passe et causer des dommages interne au four.		
Risque sur la santé et la sécurité du personnel :			
S-valeur :	S0	**S-justification**	Aucune blessure du personnel aux environ n'est prévue
P-valeur :	NA	**P-justification**	
F-valeur :	NA	**F-justification**	
s-Réduction :	NA	**MODS-VALEUR**	S0
D-valeur	D3	**D-justification**	Considérant qu'aucun niveau de protection n'est prévu pour un bas débit dans un seul passe.
SIL Risque	-	(référant à la matrice du risque)	
Risque économique :			
L-VALEUR	L4	**L-Justification**	Dégât important du four ; arrêt du l'unité 11 en aval pour une longe période
D-Eco-valeur :	D3	**D-Eco-justif :**	Considérant qu'aucun niveau de protection n'est prévu pour un bas débit dans un seul passe.
SIL Econ :	3	(référant à la matrice du risque)	
Risque sur l'environnement :			
E-valeur :	E0	**E-justification :**	Pas du risque sur l'environnement
D-env-valeur :	D3	**D-env-justif :**	Considérant qu'aucun niveau de protection n'est prévu pour un bas débit dans un seul passe.
SIL Env :	-	(référant à la matrice du risque)	
Classification SIL :		3	

SIL Classification workseet :

Système	Four 11-F-3	**SIFN° :**	11-I-1552
Définition du SIF :	Très bas débit du NAPHTA dans le Deuxième passe : 1. Fermeture des vannes d'alimentations FG (11-UV-101/102) 2. ouverture de la vanne vers atmosphère (11-UV-103) 3. fermeture de la vanne de gaz bruleur (11-PV-114) 4. fermeture de la vanne d'alimentation FO (11-UV-113/11-UV-114) 5. ouverture de la vanne de circulation (11-UV-112)		
Cause :	Déclenchement des pompes d'alimentation du NAPHTA (11-p-72/11-p-61) ou mal fonctionnement des boucles du contrôle du débit dans les passes du four		
Protection :	(11-FSLL-130) fournit sur la line de décharge de la pompe boosté (cette protection ne peut être appliquée quand le débit est faible dans un seul passe		
Scénario de danger :	Haute température du passe concerné. Cokéfaction peut apparaitre a l'intérieure, et dans le cas externe fusion du tube de passe et causer des dommages interne au four.		

Risque sur la santé et la sécurité du personnel :

S-valeur :	S0	**S-justification**	Aucune blessure du personnel aux environ n'est prévue
P-valeur :	NA	**P-justification**	
F-valeur :	NA	**F-justification**	
s-Réduction :	NA	**MODS-VALEUR**	S0
D-valeur	D3	**D-justification**	Considérant qu'aucun niveau de protection n'est prévu pour un bas débit dans un seul passe.
SIL Risque	-	(référant à la matrice du risque)	

Risque économique :

L-VALEUR	L4	**L-Justification**	Dégât important du four ; arrêt du l'unité 11 en aval pour une longe période
D-Eco-valeur :	D3	**D-Eco-justif :**	Considérant qu'aucun niveau de protection n'est prévu pour un bas débit dans un seul passe.
SIL Econ :	3	(référant à la matrice du risque)	

Risque sur l'environnement :

E-valeur :	E0	**E-justification :**	Pas du risque sur l'environnement
D-env-valeur :	D3	**D-env-justif :**	Considérant qu'aucun niveau de protection n'est prévu pour un bas débit dans un seul passe.
SIL Env :	-	(référant à la matrice du risque)	
Classification SIL :		3	

SIL Classification workseet :

Système	Four 11-F-3	**SIFN° :**	11-I.1553
Définition du SIF :	Très haute température du NAPHTA à la sortie du four : 1. Fermeture des vannes d'alimentations FG (11-UV-101/102) 2. ouverture de la vanne vers atmosphère (11-UV-103) 3. fermeture de la vanne de gaz bruleur (11-PV-114) 4. fermeture de la vanne d'alimentation FO (11-UV-113/11-UV-114) 5. ouverture de la vanne de circulation (11-UV-112)		
Cause :	Une panne de la boucle de régulation PIC-5/TIC-13 provoque une flamme plus importante que la normale ou une défaillance des pompes d'alimentation du NAPHTA (11-p-72/11-p-61) provocant un bas débit ou mal fonctionnement des boucles du contrôle du débit dans les passes du four		
Protection	FALL-2A protège contre un bas débit dans les passes et TAHH contre une haute température dans la chambre de combustion		
Scénario de danger :	Haute température du NAPHTA causant la cokéfaction qui peut apparaitre à l'intérieure des canalisations et dans le cas extrême fusion des tubes des passes et causer des dommages internes au four et aussi des dommages aux équipements en aval		

Risque sur la santé et la sécurité du personnel :

s-valeur :	S0	**S-justification**	Aucune blessure du personnel aux environ n'est prévue
p-valeur :	NA	**P-justification**	
F-valeur :	NA	**F-justification**	
s-Réduction :	NA	**MODS-VALEUR**	S0
D-valeur	D2	**D-justification**	Considérant que des protections sont prévues
SIL Risque	-	(référant à la matrice du risque)	

Risque économique :

L-VALEUR	L4	**L-Justification**	Dégât important du four ; arrêt du l'unité 11 en aval pour une longue période
D-Eco-valeur :	D2	**D-Eco-justif :**	Considérant que des protections sont prévues
SIL Econ :	2	(référant à la matrice du risque)	

Risque sur l'environnement :

E-valeur :	E0	**E-justification :**	Pas du risque sur l'environnement
D-env-valeur :	D2	**D-env-justif :**	Considérant que des protections sont prévues
SIL Env :	-	(référant à la matrice du risque)	

Classification SIL :	2

SIL Classification workseet :

Système	Four 11-F-3	**SIFN° :**	11-I-1554
Définition du SIF :	Très bas pression du gaz pilote : 1. Fermeture des vannes d'alimentations FG (11-UV-101/102) 2. ouverture de la vanne vers atmosphère (11-UV-103) 3. fermeture de la vanne de gaz bruleur (11-PV-114) 4. fermeture de la vanne gaz pilote (11-UV-104) 5. fermeture de la vanne gaz pilote (11-UV-105) 6. ouverture de la vanne vers atmosphère (11-UV-106) 7. fermeture de la vanne d'alimentation FO (11-UV-113/11-UV-114) 8. ouverture de la vanne de circulation (11-UV-112)		
Cause :	Une basse pression d'alimentation en FUEL GAS en amont.		
Protection	Une alarme PAL-37 est prévue sur la ligne du gaz pilote.		
Scénario de danger :	Accumulation de quantités de gaz non brulé à l'intérieur du four et possibilité d'explosion au redémarrage		

Risque sur la santé et la sécurité du personnel :

s-valeur :	S1	**S-justification**	Blessure légère du personnel à proximité de la fenêtre en cas d'explosion.
p-valeur :	P3	**P-justification**	Peu de chance d'échapper pour le personnel considérant la nature instantanée de l'évènement
F-valeur :	F1	**F-justification**	La présence de l'opérateur n'est pas fréquente a la hauteur des fenêtres.
s-Réduction :	-1	**MODS-VALEUR**	S0
D-valeur	D2	**D-justification**	Considérant que des protections sont prévues.
SIL Risque	-	(référant à la matrice du risque)	

Risque économique :

L-VALEUR	L4	**L-Justification**	Dégât important du four ; arrêt du l'unité 11 en aval pour une longue période
D-Eco-valeur :	D2	**D-Eco-justif :**	Considérant que des protections sont prévues
SIL Econ :	2	(référant à la matrice du risque)	

Risque sur l'environnement :

E-valeur :	E0	**E-justification :**	Pas du risque sur l'environnement
D-env-valeur :	D2	**D-env-justif :**	Considérant que des protections sont prévues
SIL Env :	-	(référant à la matrice du risque)	

Classification SIL :	2

SIL Classification workseet :

Système	Four 11-F-3	**SIFN° :**	11-I-1555
Définition du SIF :	Très haute pression au niveau de la colonne 11C-9 : 1. Fermeture des vannes d'alimentations FG (11-UV-101/102) 2. ouverture de la vanne vers atmosphère (11-UV-103) 3. fermeture de la vanne de gaz bruleur (11-PV-114) 4. fermeture de la vanne d'alimentation FO (11-UV-113/11-UV-114) 5. ouverture de la vanne de circulation (11-UV-112)		
Cause :	Une haute pression au niveau de la colonne 11C-9		
Protection	Une alarme PAL-40 est prévue au niveau de la colonne.		
Scénario de danger :	Suppression de la colonne 11C-9, colonne endommagé et l'arrêt de l'unité en aval		

Risque sur la santé et la sécurité du personnel :

s-valeur :	S0	**S-justification**	Aucune blessure ou effet sur la santé
p-valeur :	NA	**P-justification**	
F-valeur :	NA	**F-justification**	
s-Réduction :	NA	**MODS-VALEUR**	S0
D-valeur	D2	**D-justification**	Considérant que des protections sont prévues.
SIL Risque	-	(référant à la matrice du risque)	

Risque économique :

L-VALEUR	L3	**L-Justification**	Dégât important de la colonne ; arrêt du l'unité 11 en aval
D-Eco-valeur :	D2	**D-Eco-justif :**	Considérant que des protections sont prévues
SIL Econ :	1	(référant à la matrice du risque)	

Risque sur l'environnement :

E-valeur :	E0	**E-justification :**	Pas du risque sur l'environnement
D-env-valeur :	D2	**D-env-justif :**	Considérant que des protections sont prévues
SIL Env :	-	(référant à la matrice du risque)	

Classification SIL :	1

SIL Classification workseet :

Système	Four 11-F-3	**SIFN° :**	11-I-1556
Définition du SIF :	L'arrêt d'urgence : 1. Fermeture des vannes d'alimentations FG (11-UV-101/102) 2. ouverture de la vanne vers atmosphère (11-UV-103) 3. fermeture de la vanne de gaz bruleur (11-PV-114) 4. fermeture de la vanne gaz pilote (11-UV-104) 5. fermeture de la vanne gaz pilote (11-UV-105) 6. ouverture de la vanne vers atmosphère (11-UV-106) 7. fermeture de la vanne d'alimentation FO (11-UV-113/11-UV-114) 8. ouverture de la vanne de circulation (11-UV-112)		
Cause :	Présence de situation d'urgence		
Protection	aucun		
Scénario de danger :	Présence de feu, fuite de gaz ou un grave incident		

Risque sur la santé et la sécurité du personnel :

s-valeur :	S3	**S-justification**	Blessure majeure du personnel aux environ est éventuel
p-valeur :	P2	**P-justification**	Echapper à un incident est possible dans certain circonstances
F-valeur :	F2	**F-justification**	L'opérateur peut être présent occasionnellement
s-Réduction :	-1	**MODS-VALEUR**	S2
D-valeur	D3	**D-justification**	Considérant qu'il y a aucune protection
SIL Risque	1	(référant à la matrice du risque)	

Risque économique :

L-VALEUR	L3	**L-Justification**	Dégât important du four ; arrêt du l'unité 11 en aval
D-Eco-valeur :	D3	**D-Eco-justif :**	Considérant qu'il y a aucune protection
SIL Econ :	2	(référant à la matrice du risque)	

Risque sur l'environnement :

E-valeur :	E0	**E-justification :**	Pas du risque sur l'environnement
D-env-valeur :	D3	**D-env-justif :**	Considérant qu'il y a aucune protection
SIL Env :	-	(référant à la matrice du risque)	
Classification SIL :		2	

SIL Classification workseet :

Système	Four 11-F-3	**SIFN° :**	11-I-1557
Définition du SIF :	Très basse pression du Fuel gaz bruleur : 1. Fermeture des vannes d'alimentations FG (11-UV-101/102) 2. ouverture de la vanne vers atmosphère (11-UV-103) 3. fermeture de la vanne du gaz bruleur (11-PV-114)		
Cause :	Une basse pression d'alimentation en Fuel gaz en amont		
Protection	Une alarme PAL-38 est prévue sur la ligne du Fuel gaz bruleur		
Scénario de danger :	Accumulation de quantités de gaz non brulé à l'intérieur du four ou retour de la flamme et possibilité d'explosion.		

Risque sur la santé et la sécurité du personnel :

s-valeur :	S1	**S-justification**	Blessure légère du personnel à proximité de la fenêtre en cas d'explosion
p-valeur :	P3	**P-justification**	Peu de chance d'échapper pour le personnel considérant la nature instantanée de l'évènement
F-valeur :	F1	**F-justification**	La présence de l'opérateur n'est pas fréquente a la hauteur des fenêtre
s-Réduction :	-1	**MODS-VALEUR**	S0
D-valeur	D2	**D-justification**	Considérant que des protections sont prévues
SIL Risque	-	(référant à la matrice du risque)	

Risque économique :

L-VALEUR	L4	**L-Justification**	Dégât important du four ; arrêt du l'unité 11 en aval pour une longue période
D-Eco-valeur :	D2	**D-Eco-justif :**	Considérant que des protections sont prévues
SIL Econ :	2	(référant à la matrice du risque)	

Risque sur l'environnement :

E-valeur :	E0	**E-justification :**	Pas du risque sur l'environnement
D-env-valeur :	D2	**D-env-justif :**	Considérant que des protections sont prévues
SIL Env :	-	(référant à la matrice du risque)	

Classification SIL :	2

SIL Classification workseet :

Système	Four 11-F-3	**SIFN° :**	11-I-1558
Définition du SIF :	Très haute pression de fuel gaz bruleur : 1. Fermeture des vannes d'alimentations FG (11-UV-101/102) 2. ouverture de la vanne vers atmosphère (11-UV-103) 3. fermeture de la vanne du gaz bruleur (11-PV-114)		
Cause :	Une haute pression d'alimentation en Fuel gaz en amont		
Protection	Une alarme PAL-38 est prévue sur la ligne du Fuel gaz bruleur		
Scénario de danger :	Cokéfaction de la charge à l'intérieur des faisceaux radiation et possibilité d'endommagement du bruleur		

Risque sur la santé et la sécurité du personnel :

s-valeur :	S0	**S-justification**	Aucune blessure du personnel aux environ n'est prévue
p-valeur :	NA	**P-justification**	
F-valeur :	NA	**F-justification**	
s-Réduction :	NA	**MODS-VALEUR**	S0
D-valeur	D2	**D-justification**	Considérant que des protections sont prévues
SIL Risque	-	(référant à la matrice du risque)	

Risque économique :

L-VALEUR	L4	**L-Justification**	Dégât important du four ; arrêt du l'unité 11 en aval pour une longue période
D-Eco-valeur :	D2	**D-Eco-justif :**	Considérant que des protections sont prévues
SIL Econ :	2	(référant à la matrice du risque)	

Risque sur l'environnement :

E-valeur :	E0	**E-justification :**	Pas du risque sur l'environnement
D-env-valeur :	D2	**D-env-justif :**	Considérant que des protections sont prévues
SIL Env :	-	(référant à la matrice du risque)	
Classification SIL :		2	

Et en résumé on à :

11-I-1551	SIL
Personnel	-
Economie	3
environnement	-

3

11-I-1552	SIL
Personnel	-
Economie	3
environnement	-

3

11-I-1553	SIL
Personnel	-
Economie	2
environnement	-

2

11-I-1554	SIL
Personnel	-
Economie	2
environnement	-

2

11-I-1555	SIL
Personnel	-
Economie	1
environnement	-

1

11-I-1556	SIL
Personnel	1
Economie	2
environnement	-

2

11-I-1557	SIL
Personnel	-
Economie	2
environnement	-

2

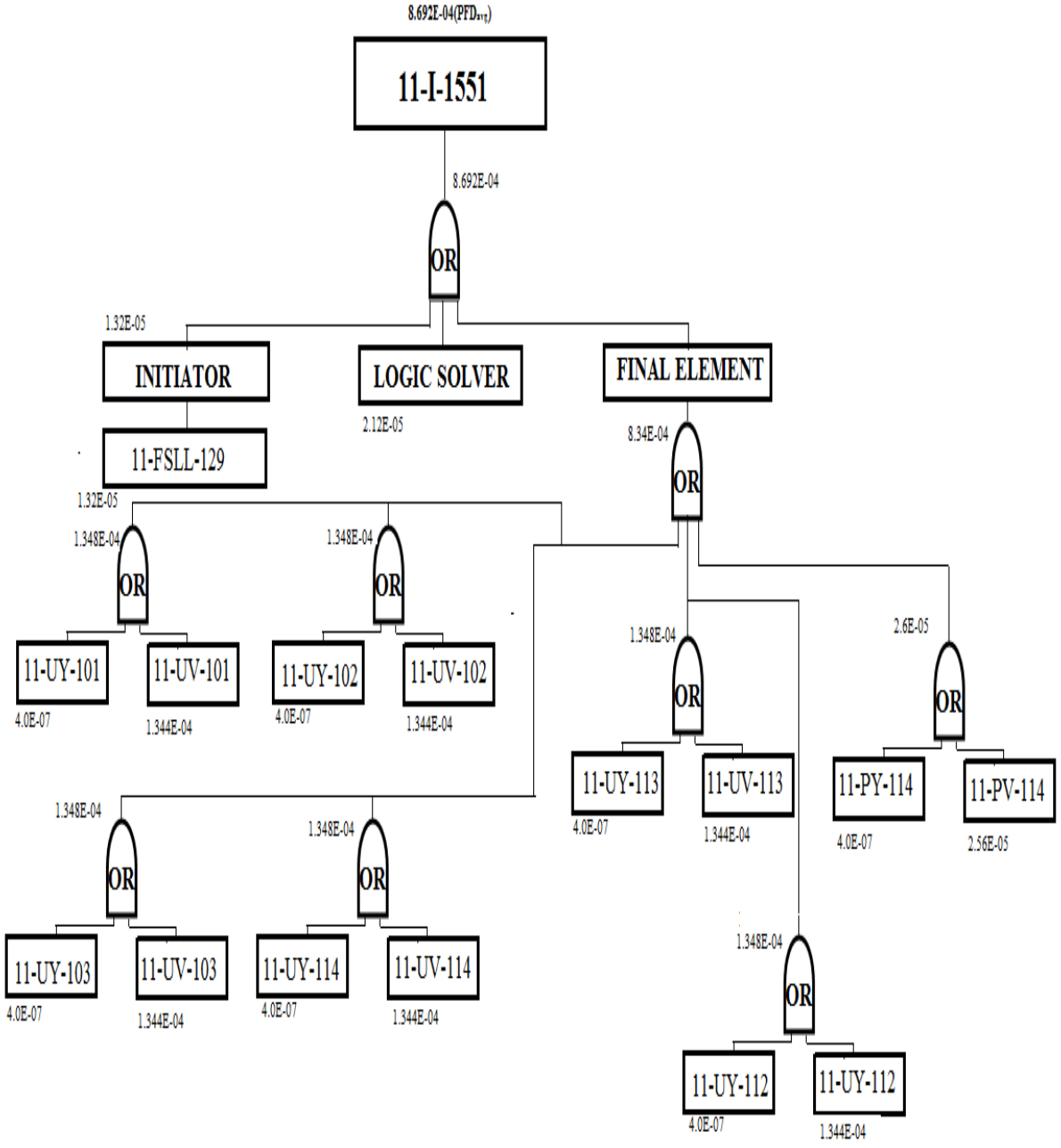
11-I-1558	SIL
Personnel	-
Economie	2
environnement	-

2

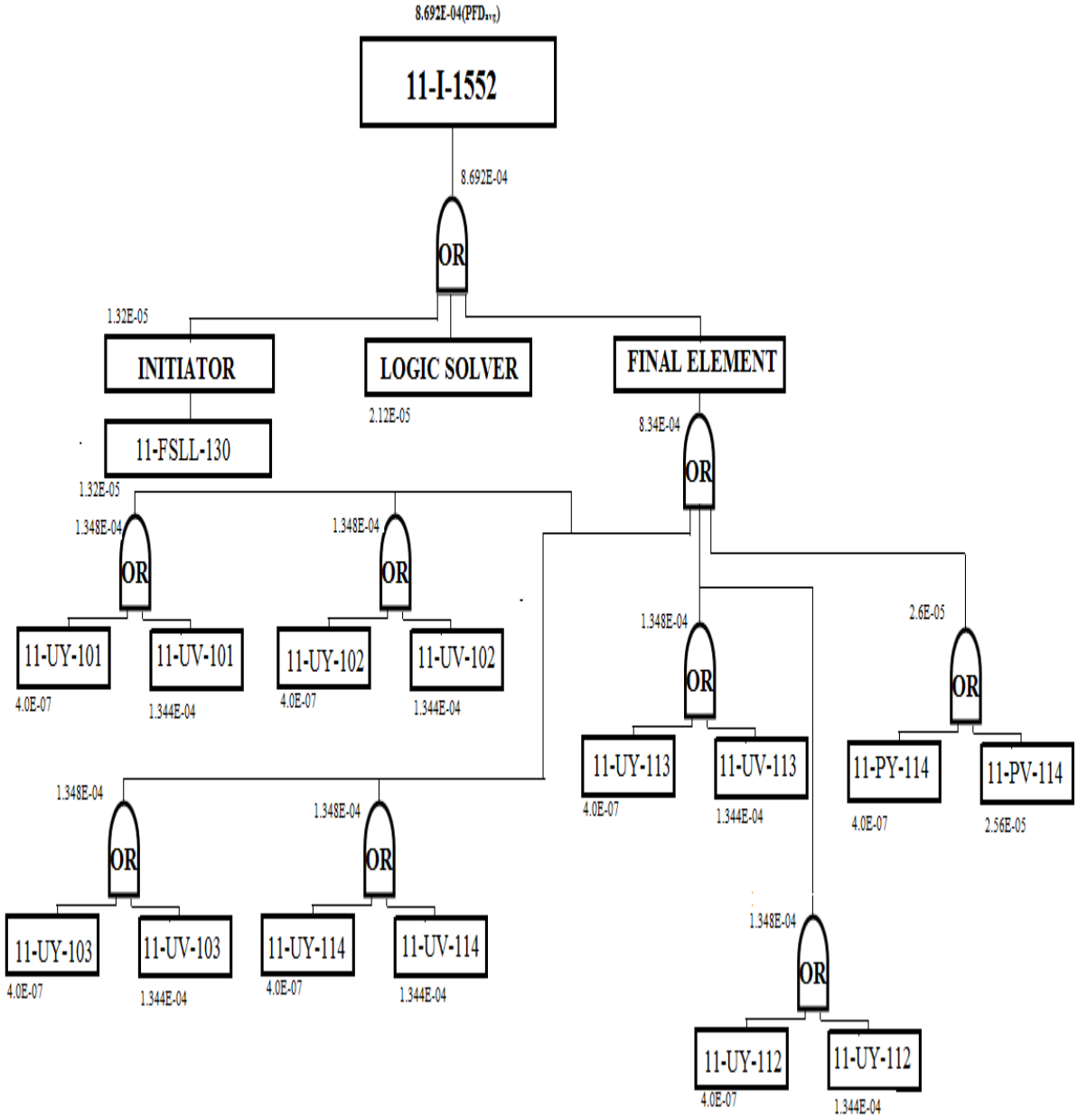
NB : On remarque que le risque dominant est le risque économique.

IV.5. L'arbre CAUSE /EFFET :

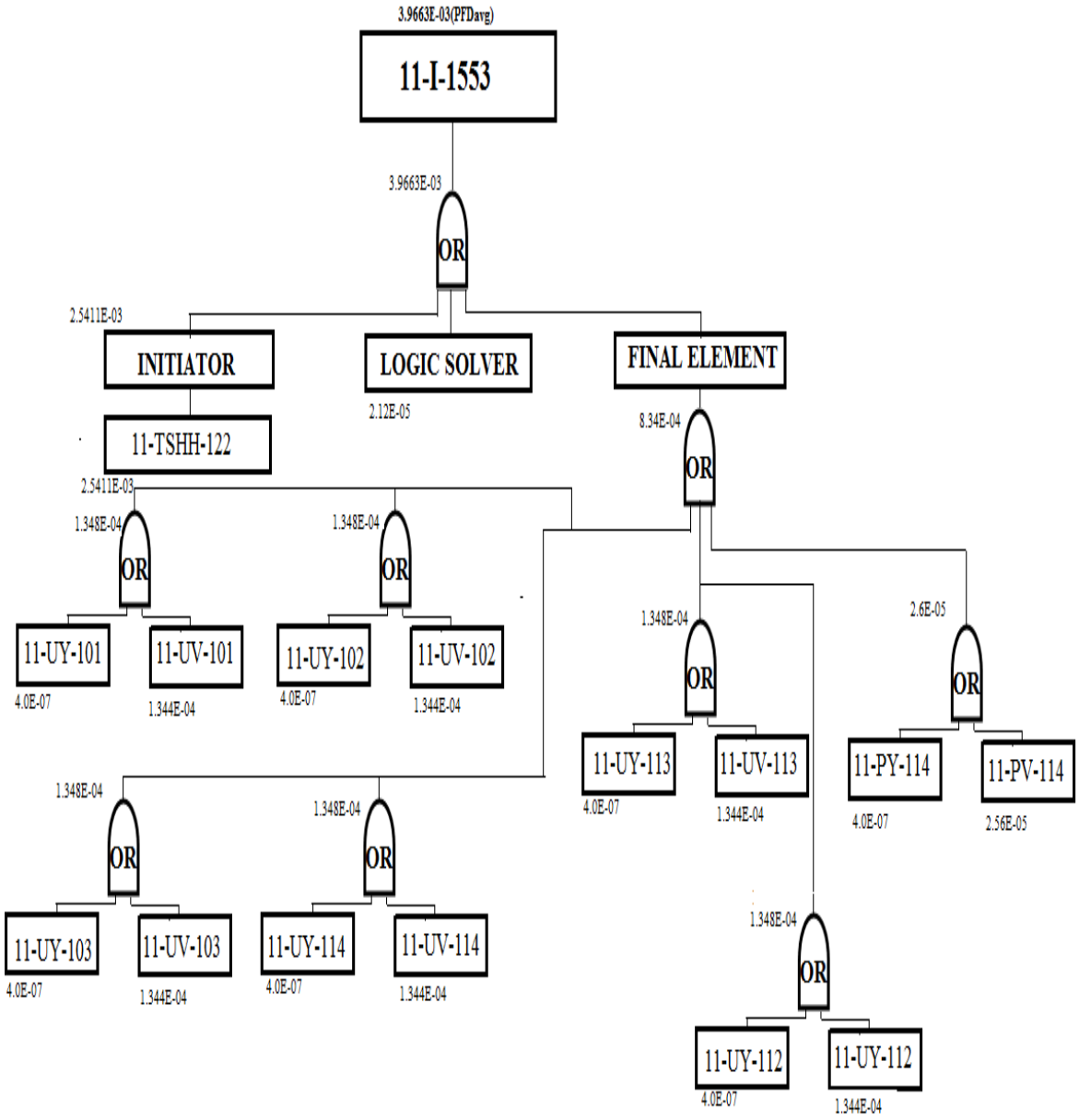
Dans cette partie de l'étude on détermine le SIL calculé :



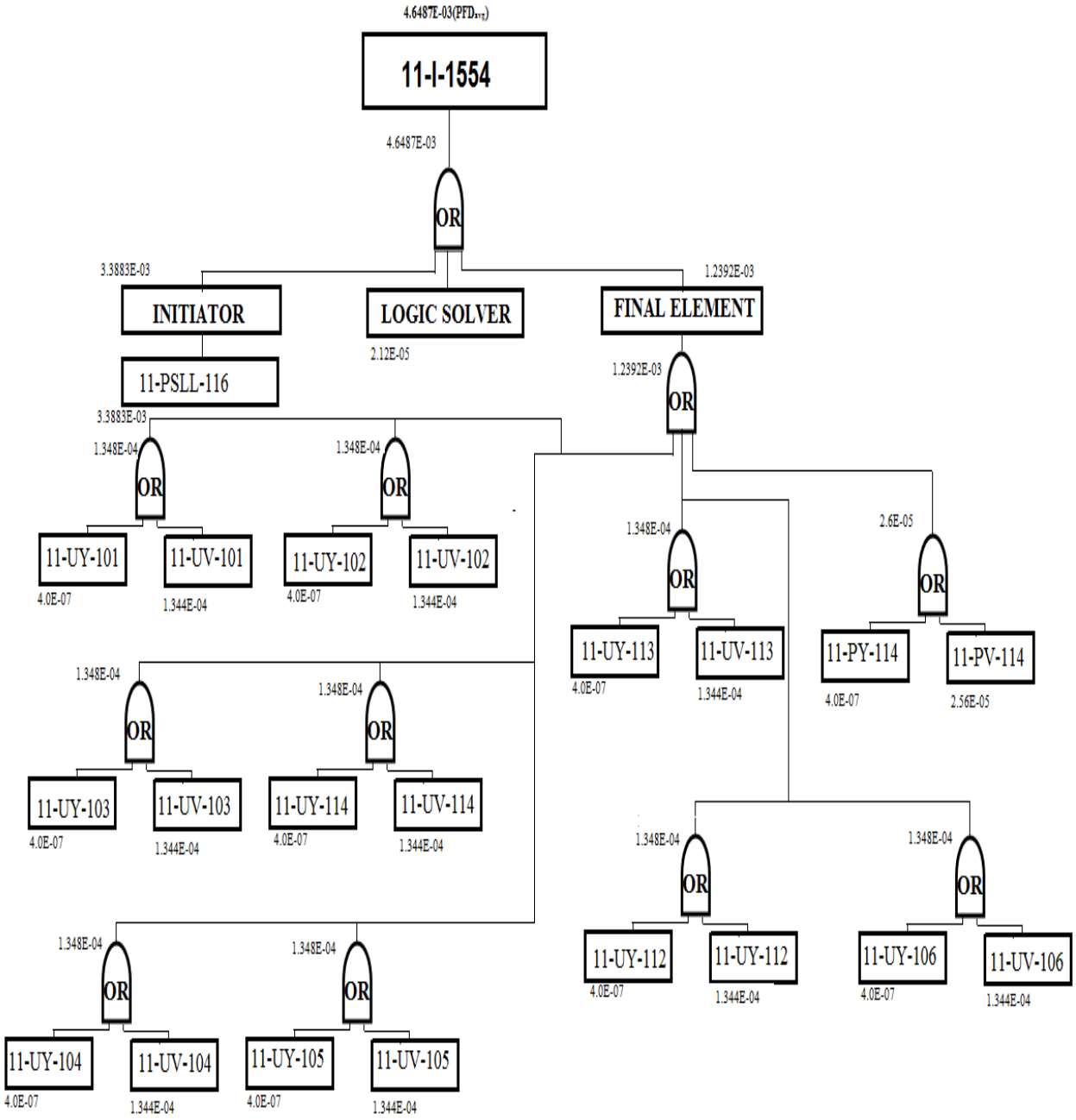
Interlock N°	SIL trajet	SIL
11-I-1551	3	8.692E-04(PFD_{avg})>>>SIL3



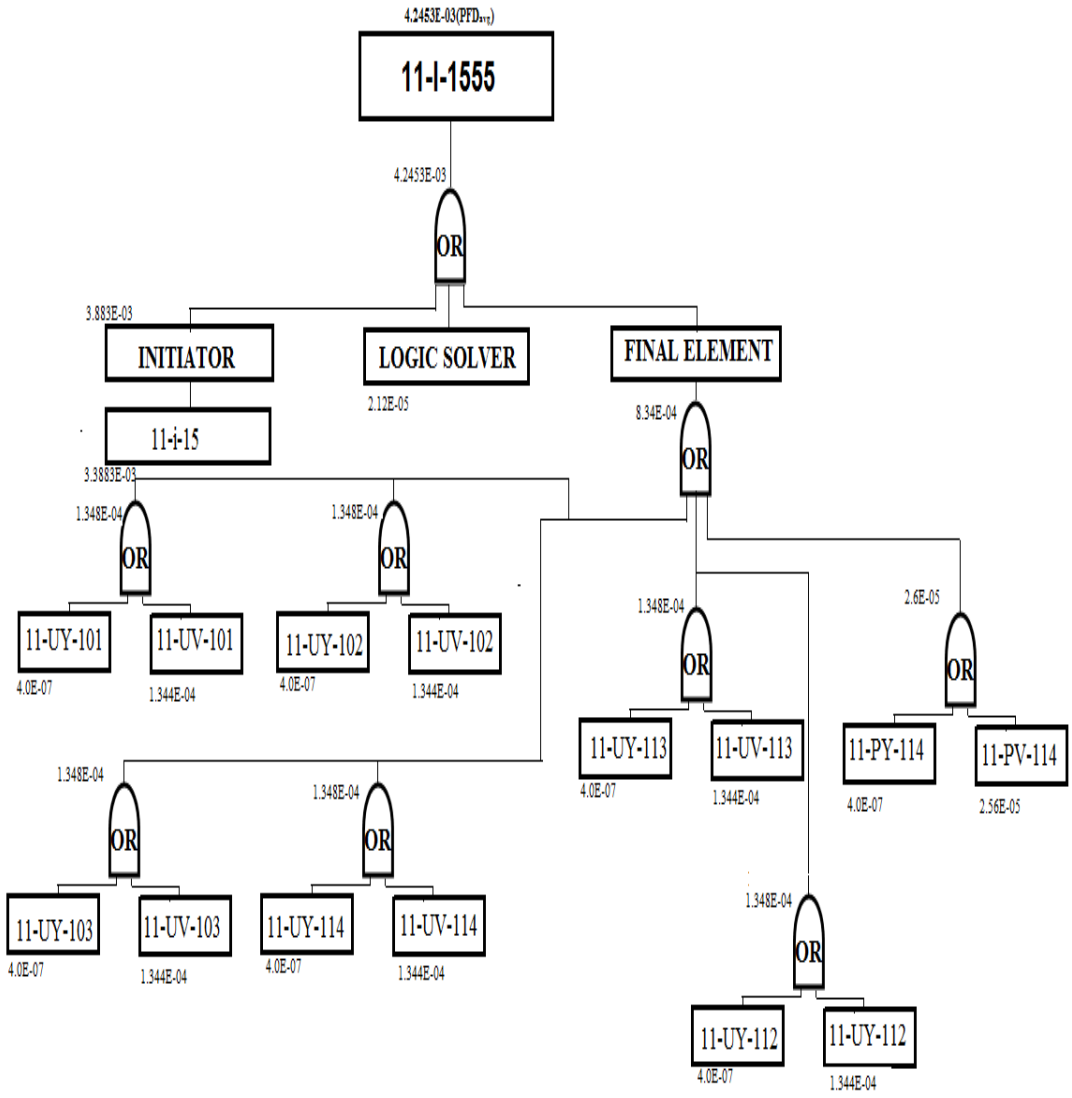
Interlock N°	SIL trajet	SIL
11-I-1552	3	8.692E-04(PFD_{avg})>>>SIL3



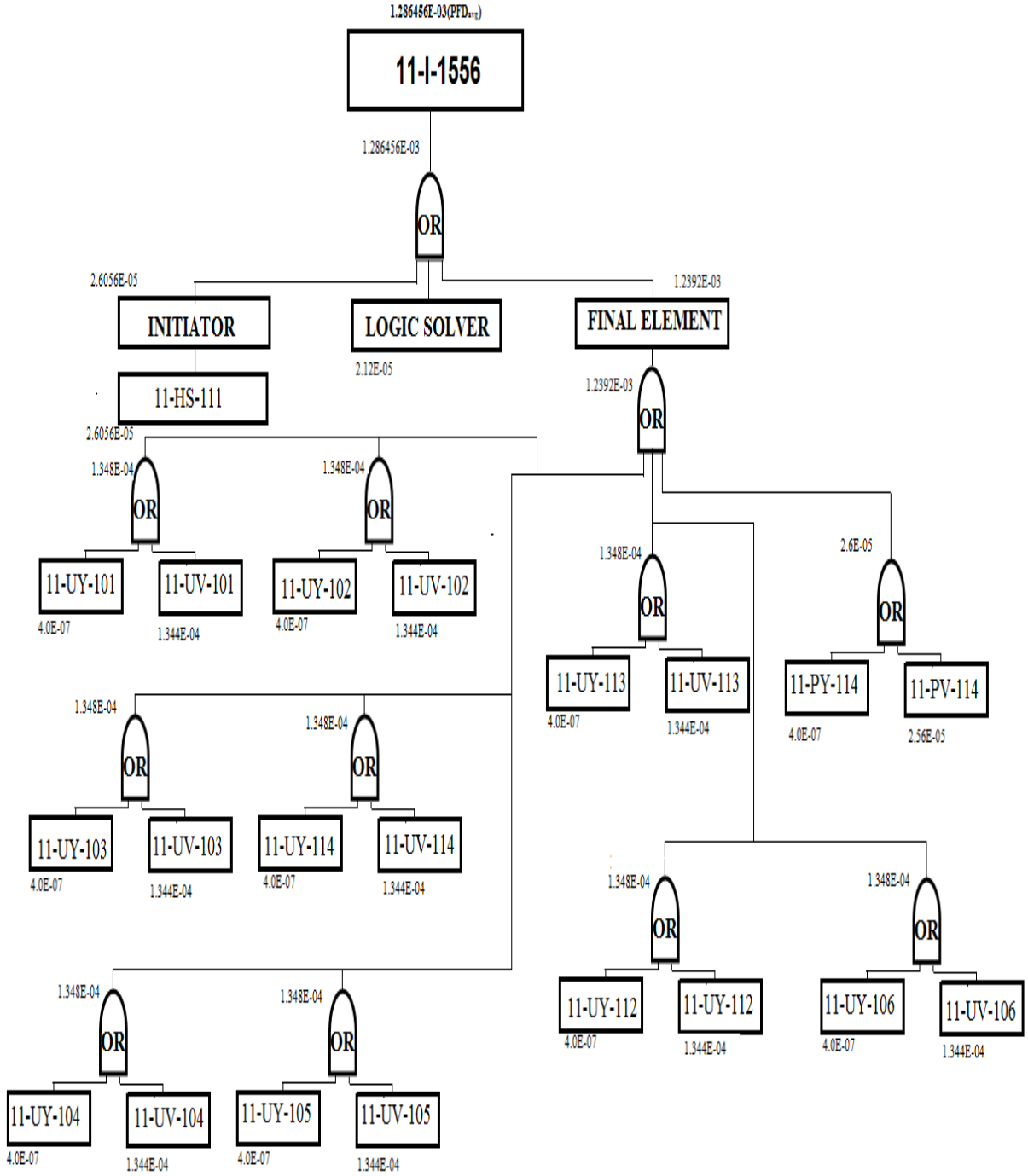
Interlock N°	SIL trajet	SIL
11-I-1553	3	3.9663E-03(PFD_{avg})>>>SIL2



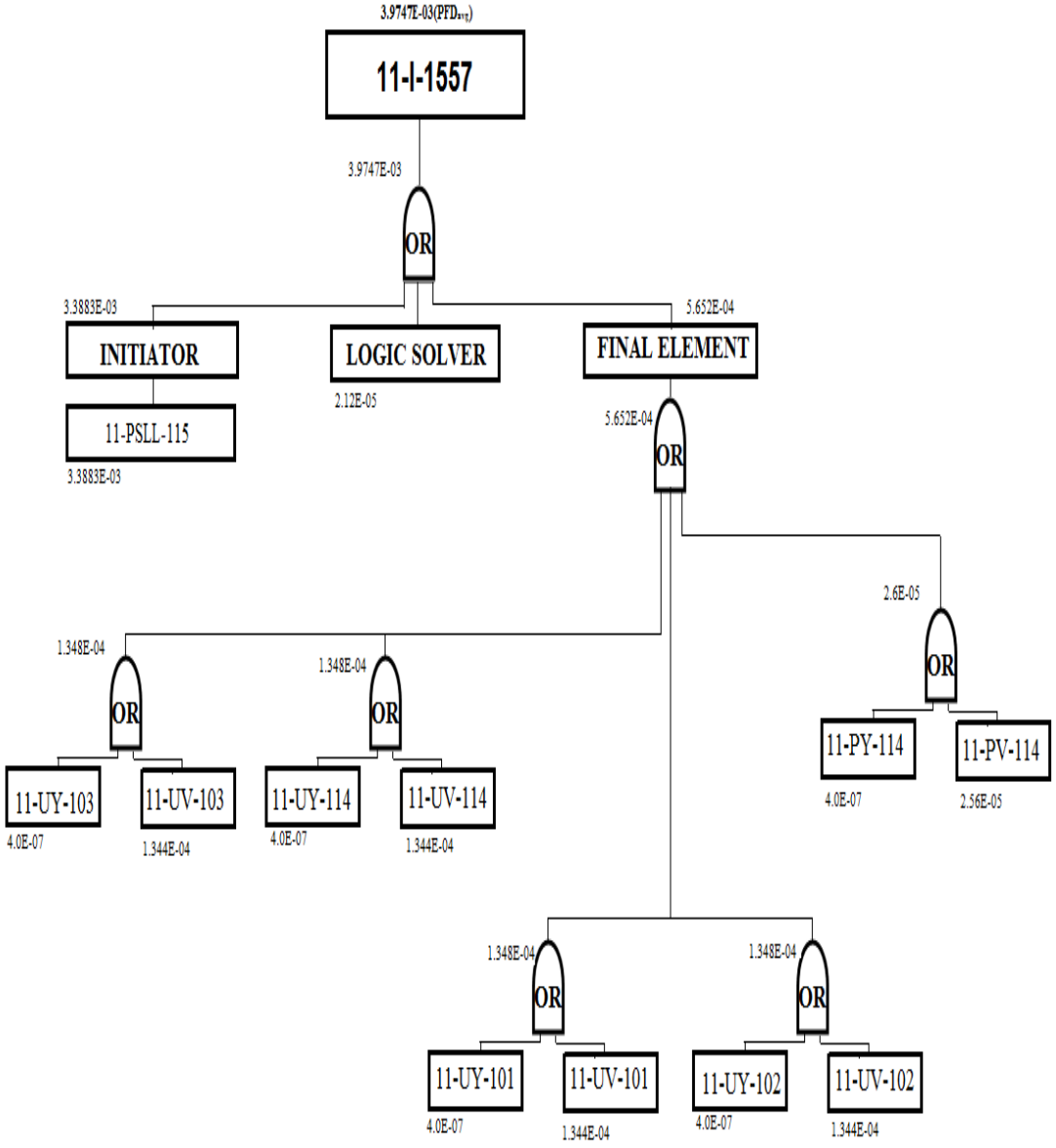
Interlock N°	SIL trajet	SIL
11-I-1554	2	4.6487E-03(PFD_{avg})>>>SIL2



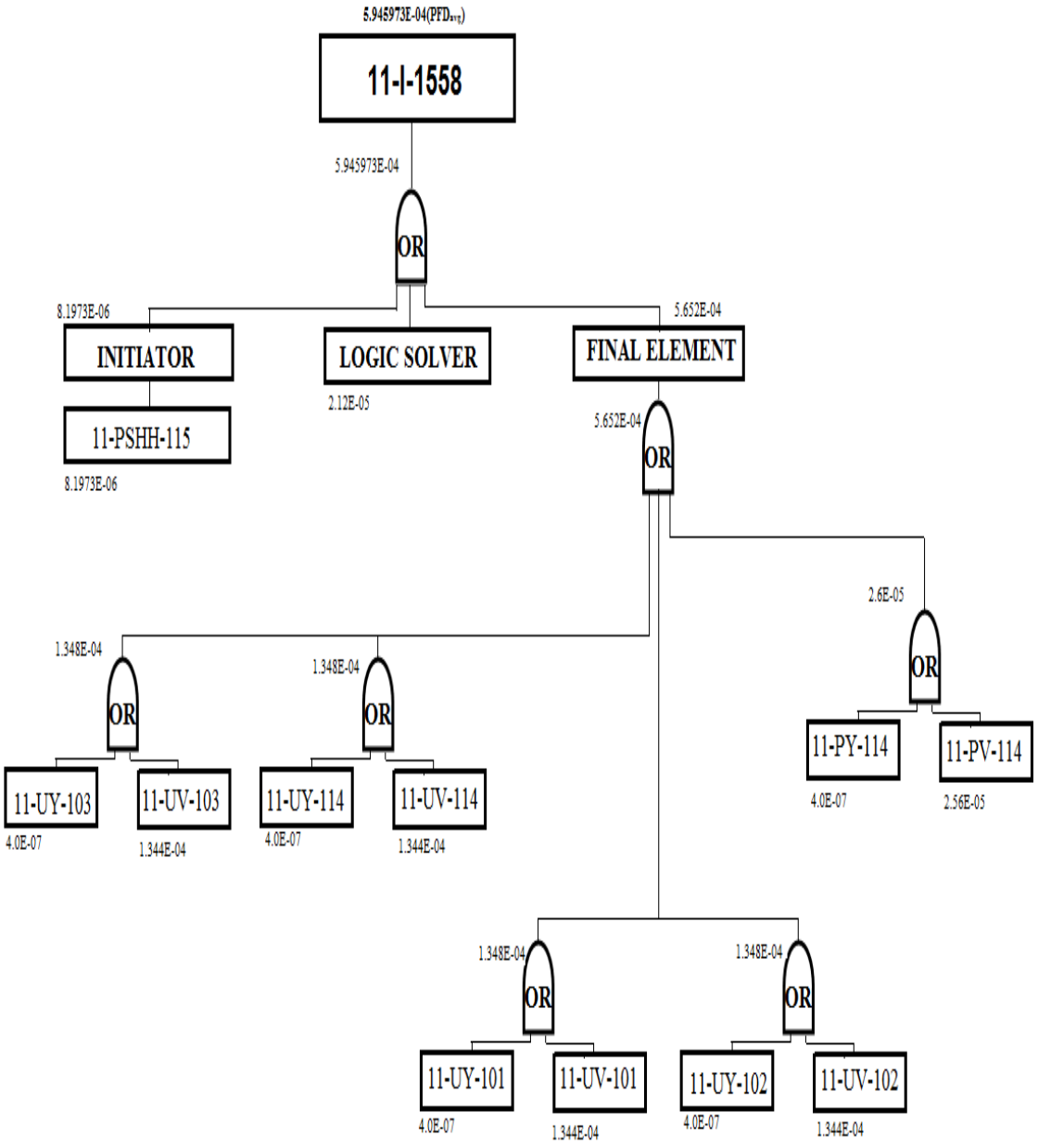
Interlock N°	SIL trajet	SIL
11-I-1555	1	4.2453E-03(PFD_{avg})>>>SIL2



Interlock N°	SIL trajet	SIL
11-I-1556	2	1.286456E-03(PFD_{avg})>>>SIL2



Interlock N°	SIL trajet	SIL
11-I-1557	2	3.9747E-03(PFD_{avg}) >>>SIL3



Interlock N°	SIL trajet	SIL
11-I-1558	2	5.945973E-04(PFD_{avg})>>>SIL2

Chapitre V:

SIMULATION

V.1. Introduction :

Disposer des bonnes informations au bon moment peut aider à réduire les risques, à éviter les temps d'arrêt coûteux, à ce conformé aux réglementations en vigueur, et à réaliser les objectifs de production. Invensys® propose une gamme complète de solutions logicielles de sécurité pour aider à gérer et maintenir les systèmes de sécurité. Cette suite d'applications intelligentes permet de maintenir la sécurité et la rentabilité de production, et de prendre les bonnes décisions au bon moment.

V.2. TriStation 1131 (TS1131) :

Un environnement de développement d'applications et de configuration et conforme à l'IEC61131 pour les contrôleurs à tolérance de panne de Triconex. Le TS1131 prend en charge les blocs de fonction, les schémas LADDER et les langages de programmation structurés et prend en charge les éditeurs de programmation à matrice de cause à effets.

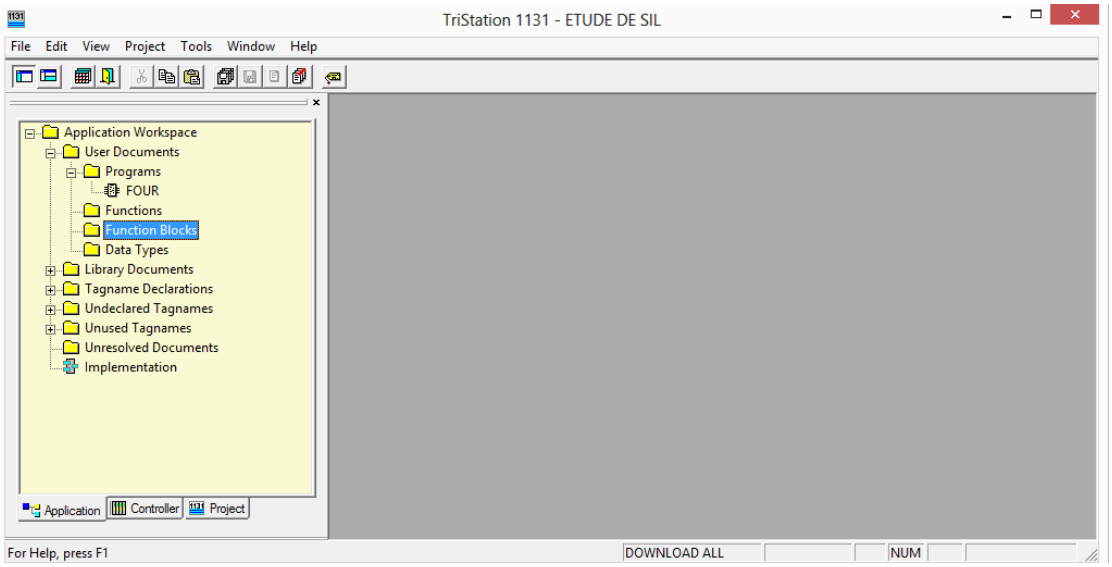


Figure V.1 : interface du programme TriStation

L'application SOE recorder peut collecter des données d'événement de 31 contrôleurs Triconex en réseau simulation, permettant la visibilité de tous les événements critique survenus sur le site.

V.3. TRISIM plus :

TRISIM plus est une « simulation virtuelle » des contrôleurs Triconex Trident et Tricon, avec la fonction de modélisation de base de DYN SIM, TRISIM permet l'accès simulateur à l'émulateur disponible dans le logiciel Tristation 1131.

Tous les produits de la suite DSS (Dynamic Simulation Suite) , y compris TRISIM plus, intègrent l'interface graphique DSS et les fonctionnalité de simulation et de modélisation. L'interface graphique est commune à la construction de modèles et aux instructions. TRISIM plus fournit un sous-ensemble de la librairie de modélisation des

équipements DYNSIM. Et est fourni avec un OTS clé en main d'Invensys, ou pour être exploité par les utilisateurs de Triconex Trident et Tricon pour la vérification du contrôle TMC.

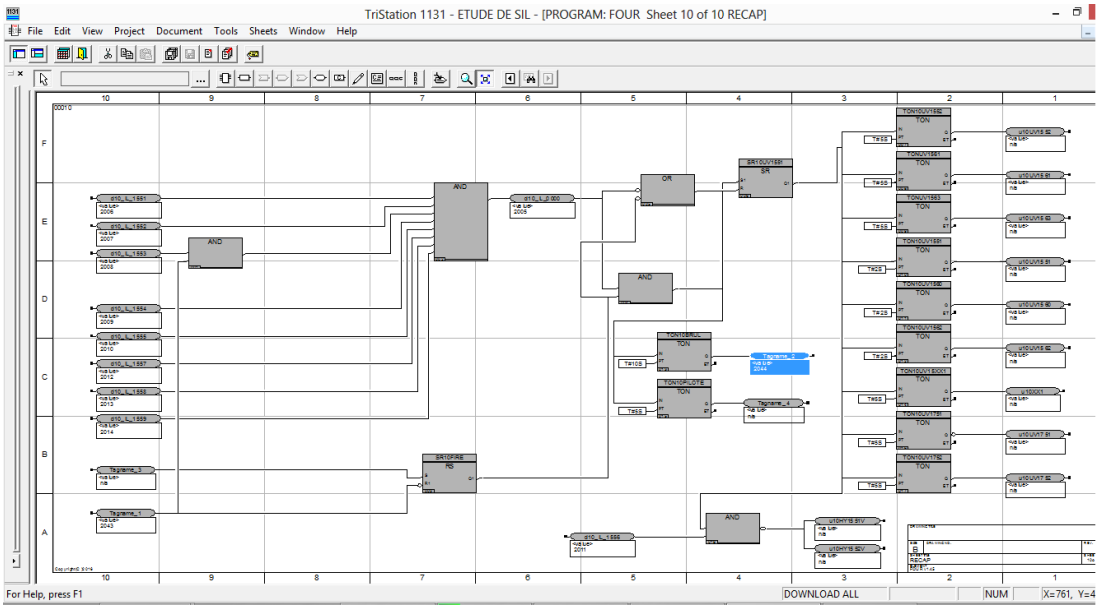


Figure V.2 : Interface du programme de contrôle

a. Principaux avantages :

- Réduit de façon significative les délais de mise en service d'un système de contrôle Triconex,
- Aide les développeurs à concevoir des solutions logicielles de contrôle en temps réel,
- Permet des analyses précises et une maintenance aisée des performances des systèmes Triconex Trident et Tricon,
- Associé à DYNSIM, permet les tests rigoureux des compresseurs et de leur système TMC Triconex Turbomachinery control,
- Permet d'offrir une formation de haut niveau aux opérateurs dans un environnement sécurisé,
- Offre un environnement de mises à niveau idéal pour les techniciens chargé du contrôle engineering.

b. Principales fonctionnalités :

- Fonctionnalité identique aux contrôleurs Tricon et Trident,
- Utilise les outils de configuration standard de Triconex (TriStation 1131 version 4.0 ou ultérieure) ,
- Prend en charge le « tie-back » et la modélisation physique avec la fonctionnalité glisser-déposer,
- Prend en charge tous les algorithmes de block-matching de Trident

V.4. InTouch ® :

InTouch est le logiciel de supervision de référence grâce, notamment, à sa légendaire simplicité d'utilisation, sa fiabilité, son évolutivité, ses performances et des nombreuses fonctionnalités. Avec une approche résolument différente des applications de supervision traditionnelle.

InTouch offre des fonctionnalités graphiques avancées permettant aux développeurs d'être encore plus performant dans le développement et la maintenance des applications. Avec InTouch les opérateurs ont accès à toutes les données de l'atelier ou du bâtiment.

Grace à son aptitude à toujours dépasser des limites, InTouch s'est imposé dans les plus grandes applications. On retrouve les applications InTouch dans tous les environnements industriels et tertiaires.

Figure V.3 : Interface du programme InTouch

Qu'il s'agisse d'application monoposte ou en réseau, InTouch offre une évolutivité et une extension des installations sans remise en cause de l'existant, tout en assurant une

compatibilité ascendante totale des applications, préservant ainsi les investissements réalisés.

InTouch est également supporté en Terminal Server offrant ainsi un accès à la supervision depuis n'importe quel poste bureautique.

Associé à la plateforme Wonderware®, InTouch décupile des capacités en centralisant dans un seul environnement l'exécution de l'application. Dans ce contexte les utilisateurs bénéficient d'une technologie 100% objets offrant des capacités d'évolution encore plus importantes.

a. Principaux avantages :

- Légendaire facilité d'utilisation permettant aux développeurs et aux opérateurs d'être rapidement et facilement productif
- Dispositif inégalé d'intégration et de connectivité à pratiquement tous les systèmes et périphérique
- Représentation graphique stupéfiantes. L'interaction avec votre procès apporte la bonne information aux bonnes personnes au bon moment
- Les migrations de versions se faisant sans interruption, votre investissement en votre application IHM est préservé

b. Principales fonctionnalités :

- Des graphiques de résolution indépendante et des symboles intelligents vont visuellement donner vie à la représentation des installations sur un écran d'ordinateur
- Des scripts sophistiqué vont permettre d'étendre et de personnalisé les applications à des besoins spécifiques
- Compte rendus des alarmes en temps réel et vues historique pour les analyses
- Intégration des contrôles Microsoft ActiveX et .NET
- Bibliothèque extensible contenant de base +500 symboles graphique prêts à l'emploi, ''intelligents'' et personnalisables

V.5. Synoptique :

L'interface Principale de notre simulation est :

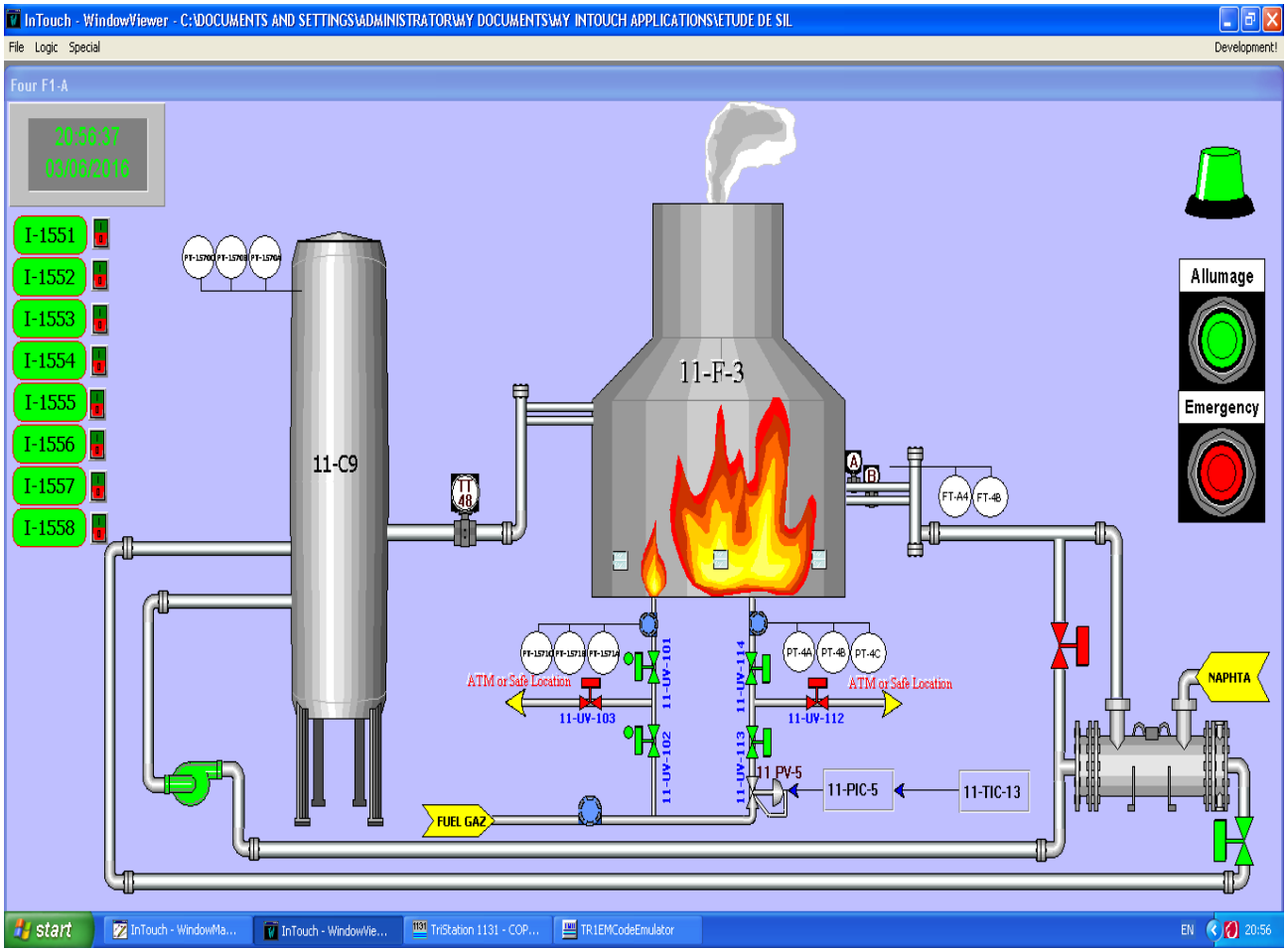


Figure V.4 : Interface Principale de notre simulation

BIBLEOGRAPHIE

- [VIL 98] Villemeur, A Sureté de fonctionnement des systèmes industriels
- [ZAD 65] L. Zadeh, Fuzzy sets, Information and control
- [ZAD 78] L. Zadeh, Fuzzy sets, sets as a basis for a theory of possibility
- [ZHA 03] Zhang, T, Long, W, and Sato, Y, Availability of systems with self-diagnostic components-applying markov model to IEC 61508-6
- Cour de fiabilité (Mr MEGLOULIE)
- Cour de probabilité (Mr boumediane)
- http://www.nrc.gov TriStation 1131 v4.1
- http://www.automation.siemens.com Safety Integrated for Process Automation Techniques de sécurité flexibles et conformes aux normes Brochure · Avril 2008