REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la
Recherche Scientifique

المدرسة الوطنية المتعددة التقنيات
Ecole Nationale Polytechnique

SONELGAZ

École Nationale Polytechnique

Filière QHSE-GRI

Mémoire de projet de fin d'études
pour l'obtention du diplôme d'ingénieur d'état en QHSE-GRI

Proposition d'un système d'arrêt d'urgence au niveau du poste gaz de la centrale électrique TG de TIARET

M^elle^. AMINA DJELDJEL

Sous la direction de M^r^. ABOUBAKR KERTOUS

Présenté et soutenue publiquement le (13/06/2016)

Composition du Jury :

Président	M^me^. SALIHA ZEBOUDJ	Professeur ENP
Rapporteur/ Promoteur	M^r^. ABOUBAKR KERTOUS	Enseignant ENP
Examinateur 1	M^me^. NASSIBA OUSSEDIK	Enseignant ENP
Examinateur 2	M^r^ . FARID LEGUEBEDJ	Enseignant ENP
Examinateur 3	M^r^ . HAKIM ACHOUR	Enseignant ENP

ENP-2016-

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la

Recherche Scientifique

École Nationale Polytechnique

Filière QHSE-GRI

Mémoire de projet de fin d'études

pour l'obtention du diplôme d'ingénieur d'état en QHSE-GRI

Proposition d'un système d'arrêt d'urgence au niveau du poste gaz de la centrale électrique TG de TIARET

M^elle^. AMINA DJELDJEL

Sous la direction de M^r^. ABOUBAKR KERTOUS

Présenté et soutenue publiquement le (13/06/2016)

Composition du Jury :

Président	M^me^. SALIHA ZEBOUDJ	Professeur ENP
Rapporteur/ Promoteur	M^r^. ABOUBAKR KERTOUS	Enseignant ENP
Examinateur 1	M^me^. NASSIBA OUSSEDIK	Enseignant ENP
Examinateur 2	M^r^ . FARID LEGUEBEDJ	Enseignant ENP
Examinateur 3	M^r^ . HAKIM ACHOUR	Enseignant ENP

ENP-2016-

Dédicaces

À mes chers parents,

À mes sœurs : Meriem et Nour el Houda ,

À tous mes proches,

À tous mes amis,

REMERCIEMENTS

Mes remerciements s'adresse tout d'abord à mes encadreurs, Messieurs A.KERTOUS et M.DAHMANI, respectivement Enseignant à l'ENP et Responsable HSE de la centrale électrique de Tiaret, pour leurs suivis, aide et disponibilités tout au long de ce travail.

Je tiens aussi à exprimer toute ma gratitude à Madame S.ZEBOUDJ, Professeur à l'ENP et responsable de la filière QHSE-GRI, pour l'honneur qu'elle me fait en acceptant de présider le jury de soutenance.

Je remercie également les membres du jury, Madame N. OUSSEDIK, Monsieur ACHOUR et Monsieur F. LEGUEBEDJ, Enseignants à l'ENP, pour l'honneur qu'ils me font en acceptant d'examiner mon modeste travail.

Mes remerciements vont également aux employés de la centrale électrique de Tiaret, à leur tête Messieurs: D.MIHOUB et A.GRAICHI, pour leur entière disponibilité, ainsi que leurs conseils tout au long du projet.

J'exprime ma profonde gratitude à mes parents et mes sœurs, pour ces longues années de soutien inconditionnel.

Enfin mes remerciements vont à tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

ملخص

يهدف هذا العمل إلى اقتراح SIS (نظام السلامة) أو بشكل أكثر دقة نظام الاغلاق في حالات الطوارئ في محطة وقود الغاز، محطة توليد الكهرباء في تيارت، ليحل محل النظام الفاشل لصمام الأمن.
لهذا الغرض، تم تقييم المخاطر باستخدام طريقة HAZOP، ثم تم استخدام أسلوب LOPA لحساب *مستوى السلامة الأمنية* المطلوبة لإقتراح النظام .
بعد العثور على مستوى السلامة (3) وعلى أساس المخططات الكهربائية للنظام القديم، قمنا ببرمجة نظام التحكم باستخدام برنامج TIA PORTAL و باختيار جهاز التحكم S7-317F .
في الخطوة النهائية، قمنا بتقييم النظام المقترح لإظهار أدائه، وذلك باستخدام المعادلات التحليلية IEC 61508-6 كما قمنا بحساب *زمن الاستجابة*.

كلمات البحث *: أنظمة السلامة المجهزة، النموذج رقم 61508 اللجنة الكهروتقنية الدولية ، مستوى السلامة الأمنية، زمن الاستجابة، نظام الاغلاق للطوارئ ، LOPA، HAZOP ، AdE ، جهاز التحكم ، التحكم الآلي .*

Abstract

This work aims to provide SIS (Safety Instrumented System) or more accurately an emergency shutdown system at the gas station of gas turbine power plant in TIARET, to replace the failed system of the valve security.
For this purpose, a risk assessment was developed using the HAZOP method, then the LOPA method was used to calculate the required SIL to offer adequate SIS.
After finding a SIL 3 and based on the control circuit diagrams of the old system, we have programmed the control of the valve by using the TIA PORTAL software and choosing the S7-317F as a controller.
In a final step, an evaluation of the proposed system is carried out to show its performance, using the analytical equations of IEC 61508-6 as well as a calculation of the system response time.

- *Key words*

IEC 61508, Safety instrumented system (SIS), safety integrity level (SIL), emergency shutdown system (ESD), HAZOP, LOPA, AdE, automatic control, controller, response time.

Résumé

Ce travail a pour objectif de proposer un SIS (Système Instrumenté de Sécurité) ou plus précisément un système d'arrêt d'urgence au niveau du poste gaz de la centrale électrique turbine à gaz de Tiaret, pour remplacer le système défaillant de la vanne de sécurité.

A cet effet, une étude des risques a été élaborée à l'aide de la méthode HAZOP, puis la méthode LOPA a été utilisée pour le calcul du SIL requis afin de proposer le SIS adéquat.

Après avoir trouvé un SIL de 3 et en se basant sur les schémas électriques de commande de l'ancien système, nous avons programmé la partie commande de la vanne en utilisant le logiciel TIA PORTAL et en choisissant l'automate de sécurité S7-317F.

Dans une dernière étape, une évaluation du système proposé est effectuée pour montrer sa performance, en utilisant les équations analytiques de la norme CEI 61508-6 ainsi qu'un calcul du temps de réponse du système.

- *Mots clés*

Système Instrumenté de Sécurité (SIS), Niveau d'intégrité de sécurité(SIL), CEI 61508, LOPA, HAZOP, Arbre des événements (AdE), système d'arrêt d'urgence (ESD), commande automatique, automate, temps de réponse.

SOMMAIRE

LISTE DES FIGURES

LISTE DES TABLEAUX

ABREVIATIONS ET ACRONYMES

AdD	Arbre des Défaillances.
AdE	Arbre des Evènements.
ALARP	As Low As Raisonably Practicable (aussi faible que raisonnablement possible).
APR	Analyse préliminaire des risques
AMDEC	Analyse des modes de défaillance, de leurs effets et de leur criticité.
CEI / IEC	Commission Electrotechnique Internationale (International Electrotechnical Commission).
DC	Diagnostic Coverage (Couverture du Diagnostic).
DCC	Défaillance de Cause Commune.
KooN	K out of N (K parmi N)
E/E/EP	Electrique / Electronique / Electronique Programmable.
ESD	Emergency Shut Down (système d'arrêt d'urgence).
EUC	Equipment Under Control (équipement sous contrôle).
FSV	Flow Safety Valve
HAZOP	HAZard and Operability study (Analyse de risque et d'exploitation).
INERIS	Institut National de l'Environnement industriel, et des RISques.
INRS	Institut National de la Recherche Scientifique.
IPL	Independent Protection Layer
ISA	Instrumentation, Systems and Automation Society
ISO	International Standardization Organisation for (Organisation Internationale de normalisation).
LOPA	Layer Of Protection Analysis (Analyse des barrières (couches) de protection).
MDT	Mean Down Time (durée moyenne d'indisponibilité après défaillance).
MooN	M out of N (M parmi N).
MTBF	Mean Time Between Failure (durée moyenne entre défaillances consécutives).
MTTF	Mean Time To (first) Failure (durée moyenne de fonctionnement avant la première défaillance).
MTTR	Mean Time To Repair (durée moyenne de réparation).
NF	Norme Française.
OREDA	Off-shore Relaibility Data base.
PAH	Pressure Alarm High (Alarm de Haute Pression).
LAHH	Level Alarm High High
LSHH	Level Switch High High
PAL	Pressure Alarm Low (Alarm de Bas Pression).

PFD Probability of Failure on Demand (probabilité de défaillance à la demande).

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

PFDmoy Probabilité de Défaillance moyenne à la Demande

PFDc Probability of Failure on Demand (probabilité de défaillance à la demande pour le sous-système capteurs).

PFDA Probability of Failure on Demand (probabilité de défaillance à la demande pour le sous-système actionneurs).

PFDU Probability of Failure on Demand (probabilité de défaillance à la demande pour le sous-système unité logique).

PSH Pressure Switch high

PLC Programmable Logic Controller.

PDSL Pressure Differential Switch Load

PDAL Pressure Differential Alarm Load

PSL Pressure Switch low

SIF Safety Instrumented Function

SIL Safety Integrity Level

SIS Safety Instrumented System

PI&D Process and instrumentation Diagram

SRS Systèmes relatifs à la sécurité (safety related systems)

MADS Méthodologie d'analyse des dysfonctionnements des systèmes.

TG Turbine à Gaz.

MOSAR Méthode Organisée systémique d'Analyse des Risques.

GLOSSAIRE

Selon la norme CEI 61508 [IEC61508, 2002] :

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

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

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

Composant : La plus petite partie d'un module, d'un sous-système ou d'un système qu'il est nécessaire et suffisant de considérer pour l'analyse du système. Cette plus petite partie pourra être limitée par les données disponibles donnant les caractéristiques du composant. On sera parfois obligé de rester au niveau module pour l'analyse. La décomposition proposée est donc : Composant / module / sous-système / système.

Architecture : Configuration spécifique des éléments matériels et logiciels dans un système.

Canal : Elément ou groupe d'éléments exécutant une fonction indépendante.

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

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

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

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

Défaillance de cause commune : Défaillance résultant d'un ou plusieurs événements lequel, provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multicanal, conduit à la défaillance du système.

Détecté : Révélé ; Déclaré. Se rapporte au matériel et signifie détecté par les tests de diagnostic, une intervention de l'opérateur (par exemple une inspection physique et des tests manuels), ou lors de l'exploitation normale. Ces adjectifs sont utilisés dans les cas d'anomalie détectée et de défaillance détectée.

Non détecté : Non révélé; Non déclaré. Se rapporte au matériel et signifie non détecté par les tests de diagnostic, une intervention de l'opérateur (par exemple une inspection physique et des tests manuels), ou lors de l'exploitation normale. Ces adjectifs sont utilisés dans les cas d'anomalie non détectée et de défaillance non détectée.

Test de diagnostic : Test en ligne (en fonctionnement) pour détecter des défauts internes au niveau du composant.

Couverture de diagnostic (DC) : Fraction exprimant la décroissance de la probabilité de défaillance dangereuse du matériel résultant du fonctionnement des tests de diagnostic automatique.

Proof test : Test périodique hors ligne réalisé pour détecter des pannes dans un système de telle sorte que le système puisse être réparé afin de revenir dans un état équivalent à son état initiale.

Disponibilité A (t) : Probabilité pour qu'un dispositif soit opérationnel au temps t. Le système peut avoir été réparé dans le passé.

Taux de défaillance λ(t) : C'est la probabilité pour que le système soit défaillant. Cette définition s'applique pour tout type d'éléments (système, sous-système, module, Composant).
Taux de défaillance dangereuse λ_D(t) : C'est la probabilité que le système soit défaillant de telle sorte qu'il soit incapable d'exécuter la fonction de sécurité attendue.

Probabilité de défaillance sur demande PFD (t) (ProbabilityFailure on Demand) : C'est la probabilité sur l'intervalle de temps [0, t] que le système ne puisse pas exécuter la fonction pour laquelle il a été conçu au moment où la demande de cette fonction est faite. C'est un nombre sans dimension.

Probabilité moyenne de défaillance sur demande PFDavg (Average of the probability failure on demand) : C'est la valeur moyenne par rapport à l'intervalle de temps entre proof test (test fonctionnel) de la probabilité de défaillance sur demande. Selon l'existence de proof test ou non, la valeur moyenne se calculera par rapport à l'intervalle de temps Ti entre ces proof tests.
Cette grandeur s'utilise dans le cas des systèmes à faible sollicitation et c'est un nombre sans dimension.

MTTF (Mean Time To Failure): Pour un système que l'on ne répare pas, le MTTF est le temps moyen de fonctionnement avant la première défaillance.

MTBF (Mean Time BetweenFailure) : Le MTBF n'a pas de sens que pour un système réparable. C'est la durée moyenne entre deux défaillances consécutives. Pour un composant simple de taux de défaillance λ qui, après réparation, peut être considéré comme identique à ce qu'il était en début de vie. Dans ce cas-là, d'après le livre de sûreté de fonctionnement de Villemeur [Villemeur, 1998] le **MTBF** est donnée par : $MTBF \approx MTTF = 1/\lambda$

MTTR (Mean Time To Repair): C’est le taux moyen mis pour réparer le système.

MDT (Mean Down Time) : C’est la durée moyenne d’indisponibilité ou de défaillance. Elle correspond à la détection de la panne, la réparation de la panne et la remise en service.

$\mathbf{t_{CE}}$ **:** L’équivalent du temps d'arrêt moyen du canal **(**The channel equivalent mean down time).

$\mathbf{t_{GE}}$ **:** L’équivalent du temps d'arrêt du system **(**The system equivalent down time).

MUT (Mean Up Time) : C’est la durée moyenne de fonctionnement après réparation.

INTRODUCTION GENERALE

1. Problématique

Les installations industrielles peuvent constituer un risque pour les personnes, l'installation et l'environnement. Divers moyens doivent être mis en œuvre pour réduire ces risques. Citons à titre d'exemples, la conception du procédé, le choix des équipements, prévoir des redondances sur les systèmes de contrôle commande du procédé…

Ces moyens ne sont pas toujours suffisants. Pour réduire encore le risque, il faut prévoir des systèmes instrumentés de sécurité (SIS) qui jouent un rôle primordial dans la prévention des accidents pouvant survenir dans les installations industriels. Ils entrent en action lorsque le process se trouve dans des conditions anormales et qu'une situation dangereuse risque de se développer.

Notre travail intitulé : « proposition d'un système d'arrêt d'urgence au niveau du poste gaz de la centrale électrique TG de Tiaret », s'inscrit dans ce contexte.

Nous nous sommes intéressés à la commande automatique de la vanne de sécurité située à l'entrée du poste gaz de la centrale électrique de TIARET, défaillante depuis plusieurs années et qui peut constituer un grand risque pour les personnes et l'installation.

2. Objectif

Pour prévenir les risques au niveau du poste gaz, nous nous fixons comme objectif, la proposition d'un système d'arrêt d'urgence qui remplacera la vanne de sécurité défaillante.

3. Organisation du mémoire

La démarche adoptée est la suivante :

Les notions et les concepts nécessaires ainsi que la démarche de gestion du risque et les méthodes utilisées dans cette dernière sont présentés dans un premier chapitre.

Le chapitre 2 est dédié aux systèmes instrumentés de sécurité (SIS).

Dans le chapitre 3, sont décrits, le logiciel TIA PORTAL, le langage LADDER et les automates.

Le but du chapitre 4 est de définir le champ d'étude, le poste gaz ALSTHOM ainsi que les données nécessaires concernant le système ancien de la vanne.

L'application de la méthode HAZOP pour la détermination des scénarios critiques puis l'utilisation de LOPA pour la détermination du SIL requis seront traités dans le chapitre 5.

Dans le dernier chapitre (6), la programmation de la partie commande du système sous le logiciel Step7, la visualisation et simulation sous le Wincc ainsi que l'évaluation du système proposé sont traitées.

PARTIE BIBLIOGRAPHIQUE

CHAPITRE1

GESTION DES RISQUES

INTRODUCTION

L'objectif de ce chapitre est de donner les concepts et définitions liées à la gestion des risques puis de décrire le processus de gestion des risques et les différentes méthodes utilisées. Seules les méthodes utilisées dans ce mémoire seront présentées.

1. Définitions et concepts

1.1. Notion de danger

Le danger est défini :

- Selon la norme IEC 61508 [IEC61508 ,1998], comme une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes.
- selon le référentiel OHSAS 18001 [OHSAS18001, 1999]: comme une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments.
- Selon Mazouni [Mazouni, 2008], comme une propriété intrinsèque inhérente à un type d'entité ou un type d'évènement qui a la potentialité de provoquer un dommage.

1.2. Notion de risque

Selon VILLEMEUR [Villemeur, 1998], le risque est une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences.

Et selon le référentiel OHSAS 18001 [OHS18001, 1999], le risque est la combinaison de la probabilité et de /des conséquence(s) de la survenue.

D'une manière générale, le risque peut être considéré comme la combinaison de deux facteurs : la fréquence de l'occurrence de l'évènement dangereux et la gravité de conséquences.

$$Risque\ (R) = Probabilité\ (P) \times Gravité\ (G)$$

La figure suivante permet de bien apprécier l'interaction entre les notions de danger et de risque (émergence de la notion de situation dangereuse).

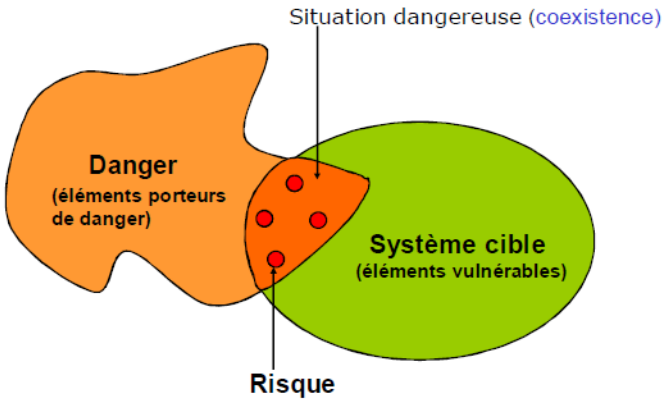


Figure 1. 1: Relation entre les notions de danger et de risque

Le critère de Farmer [Farmer, 1967] permet de définir les notions de risque acceptables et inacceptables (figure 1.2).

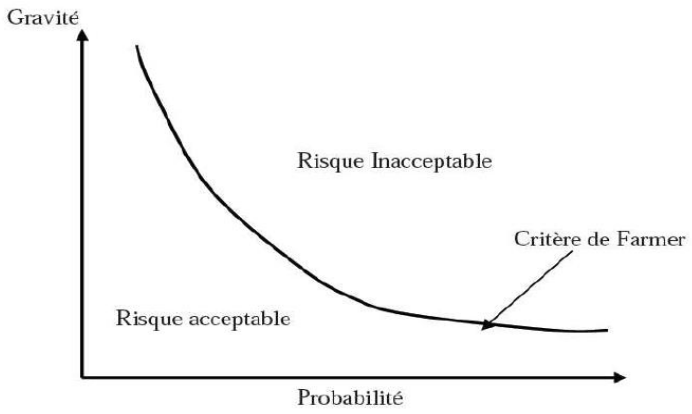


Figure 1. 2: Courbe de Farmer [FARMER, 1967]

1.3. Notion d'ALARP et de risque tolérable

L'objectif primordial en matière de gestion des risques consiste à les réduire à leurs niveaux les plus bas réalisables tout au long de la durée de vie des installations. Les niveaux les plus bas réalisables sont définis par le principe ALARP (As Low as Reasonably Practicable) ou « aussi bas qu'il est raisonnablement possible de faire ») [Jean-Paul Lacoursière, 2012], Le modèle ALARP est illustré sur la Figure 1.3.

Son principe est qu'il existe un niveau de risque qui est intolérable, au-delà duquel tout risque n'est justifiable d'aucune manière et est donc inacceptable. Cela correspond à la zone supérieure du schéma (zone I). En deçà de cette zone se situe la zone ALARP (zone II), pour laquelle tout risque peut être accepté si le bénéfice escompté est suffisant.

La zone inférieure (zone III) est celle du risque résiduel dont le niveau est considéré comme négligeable et, à ce titre, ne nécessite aucune réduction supplémentaire.

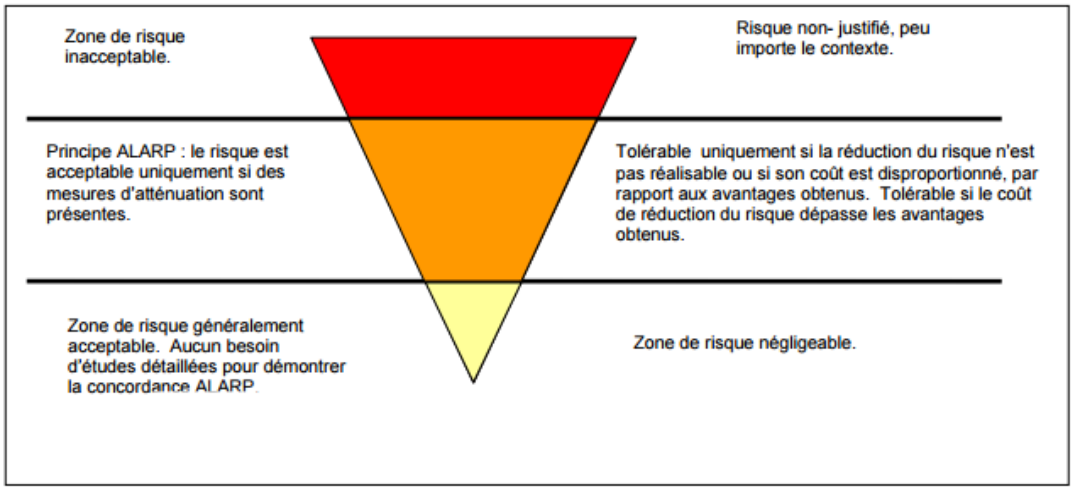


Figure 1. 3: Modèle ALARP

Et donc, le risque n'y est tolérable que :

- si toute réduction supplémentaire du risque est incompatible.
- si la société tire un avantage de l'activité, compte tenu du risque associé.

Pour prendre en compte les concepts ALARP, la mise à niveau d'une conséquence avec une fréquence tolérable peut se faire par l'intermédiaire des classes de risque.

Le tableau 1.1 représente quatre classes de risque pour un certain nombre de conséquences et de fréquences.

Avec :

- **La classe de risque I** : Se situe dans la zone inacceptable ;
- **Les classes de risque II et III** : Sont dans la zone ALARP ; la classe de risque II est juste à l'intérieur de la zone ALARP ;
- **La classe de risque IV** : Se situe dans la zone globalement acceptable.

Tableau 1. 1 : Exemple de classification des accidents en fonction des risques [IEC 61508, 1998]

Fréquence	Conséquence			
	Catastrophique	Critique	Marginale	Négligeable
Fréquent	I	I	I	II
Probable	I	I	II	III
Occasionnel	I	II	III	III
Peu fréquent	II	III	III	IV
Improbable	III	III	IV	IV
Non crédible	IV	IV	IV	IV

1.4. Notion de sécurité

Selon [Desroches et al, 2003], la sécurité concerne la non occurrence d'événements pouvant diminuer ou porter atteinte à l'intégrité du système, pendant toute la durée de l'activité du système, que celle-ci soit réussie, dégradée ou ait échouée.

Et suivant le guide ISO/CEI 73 [ISO, 2002] élaboré par l'ISO (organisation internationale de normalisation) sur la terminologie du management du risque, la sécurité est l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à l'environnement.

La sécurité d'un système peut être définie en termes d'aptitude : « *la sécurité d'un système est son aptitude à fonctionner ou à dysfonctionner sans engendrer d'événement redouté à l'encontre de lui-même et de son environnement, notamment humain* » [Innal, 2008].

1.5. Sécurité fonctionnelle

1. 5. 1. Définition

Selon la norme IEC 61061 [IEC61061, 1998], la sécurité fonctionnelle est le sous-ensemble de la sécurité globale se rapportant à la machine et au système de commande de la machine qui dépend du fonctionnement correct des systèmes électriques de commande relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque.
Selon la norme IEC 61508 [IEC61508, 1998], *la sécurité fonctionnelle est le sous ensemble de la sécurité globale qui dépend du bon fonctionnement d'un système ou d'un équipement en réponse à ses entrées.*

1. 5. 2. Systèmes relatifs aux applications de sécurité

Un système E/E/PE (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité. C'est-à-dire, depuis le capteur, en passant par la logique de contrôle et les systèmes de communication, jusqu'à l'actionneur final, tout en incluant les actions critiques de l'opérateur.

1.6. Notion de fiabilité

La fiabilité est la probabilité qu'un dispositif accomplisse sa fonction voulue lorsque ce dispositif travaille dans les limites prévues et a un instant donné. La fiabilité se note R. C'est une fonction du temps telle que :
R(t) = P (T>t) ; probabilité que le temps T (temps ou la panne intervient) soit supérieur au temps t (temps opérationnel ou temps de fonctionnement), définition de l'ISA [ISA, 1996] ; On peut aussi la définir comme la probabilité que le système ne soit pas défaillant pendant l'intervalle de temps [0, t].

2. Processus de gestion des risques

La gestion des risques peut être définie comme : l'ensemble *des activités coordonnées en vue de réduire le risque à un niveau jugé tolérable ou acceptable*. Cette gestion constitue un processus itératif qui englobe de différentes phases dont l'enchaînement est décrit à la figure 1.4 [INERIS, 2003].

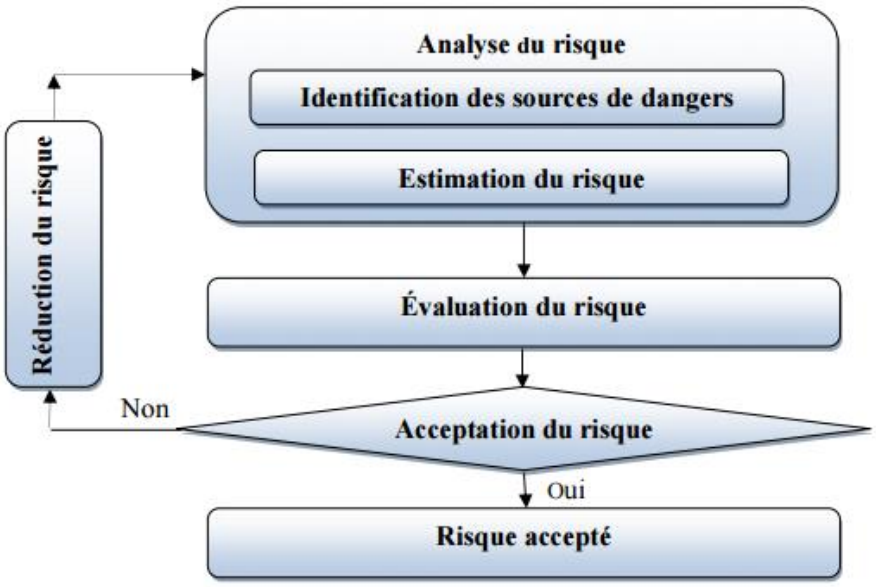


Figure 1. 4: Processus de gestion des risques [ISO, 1999]

Ces différentes phases sont brièvement explicitées comme suit :

2.1. L'Analyse du risque

L'analyse des risques est définie dans le Guide ISO/CEI 51 [ISO, 1999] comme :
« *L'utilisation des informations disponibles pour identifier les phénomènes dangereux et estimer le risque* ».
Cette phase se compose des points suivants :

2. 1. 1. L'identification

L'identification des risques cherche à répondre aux questions suivantes :
Qu'est-ce qui peut se produire ? ; Quand? ; À quel endroit? ; Comment ? ; Pourquoi?
Il s'agit de recueillir l'information qui servira d'abord à identifier tous les risques auxquels la collectivité ou l'organisation est exposée pour ensuite être en mesure de les analyser. Cette collecte de renseignements doit s'effectuer de façon structurée et méthodique puisque les autres étapes du processus seront réalisées sur la base de cette information.

2. 1. 2. L'estimation

vise à estimer le niveau de chacun des risques identifiés. Par un examen approfondi et plus raffiné de l'information recueillie à l'étape de l'identification des risques, la démarche consiste ainsi à établir l'importance respective des divers risques. Pour ce faire, une analyse détaillée des caractéristiques des aléas en cause et de la vulnérabilité des éléments exposés est nécessaire, afin d'en dégager les probabilités d'occurrence et les conséquences potentielles associées.

- Cette estimation peut être réalisée en utilisant différentes méthodes tel que : APR, AMDEC, HAZOP, AdD, sachant que cette phase est réalisée par une équipe multidisciplinaire pour assurer la qualité et l'efficacité de la démarche de gestion des risques .

2.2. Evaluation du risque

Cette phase permet de comparer le risque estimé à celui jugé acceptable ou tolérable, les critères d'acceptabilité du risque doivent résulter d'un consensus entre ces partenaires.

Cette évaluation permet de prendre une décision sur l'acceptabilité ou l'inacceptabilité de chaque risque [ISO,1999] , c'est-à-dire, déterminer s'il convient d'accepter le risque tel qu'il est ou bien de le réduire en rajoutant de nouvelles barrières de sécurité.

2.3. Acceptation du risque

Le niveau de risque quantifié sera positionné dans une matrice d'évaluation et en fonction des critères d'acceptabilité retenus et le risque estimé qu'on juge de l'acceptabilité ou la non acceptabilité du risque [ISO, 1999].Si le risque est jugé acceptable, le processus de gestion de risque est terminé, dans le cas contraire, le processus continue en passant à l'étape de réduction.

2.4. Réduction du risque

Si le risque est jugé inacceptable, une réduction de risque doit être réalisée en mettant en place des mesures préventives pour diminuer la probabilité d'occurrence ainsi que des mesures protectives pour réduire la gravité des conséquences.

La réduction nécessaire du risque est la réduction qui doit être réalisée pour atteindre le risque tolérable dans une situation spécifique (qui peut être définie soit qualitativement ou bien quantitativement) [IEC-61508, 1998].

Les mesures de prévention : sont les mesures préalables mises en place pour empêcher la survenue d'un accident. Par exemple : soupape de sécurité, un disque de rupture ou encore un système automatique d'arrêt d'urgence (*SIS*).

Les mesures de protection : sont mise en place pour limiter les conséquences de la survenue d'un accident en diminuant ainsi sa gravité. Par exemple : une cuvette de rétention assurant le non épandage d'un liquide, un système d'extinction automatique permettant de réduire les effets d'un incendie, les plans de secours et les procédures d'urgence.

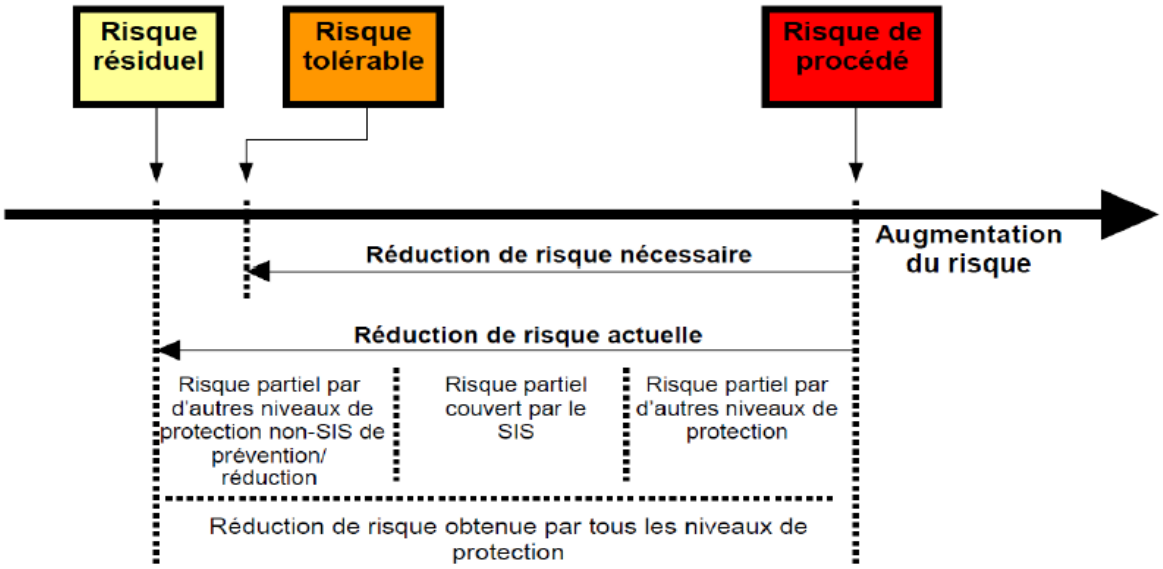


Figure 1. 5: Réduction du risque - Concepts généraux [IEC61511, 2000]

3. Méthodes d'analyse et d'évaluation des risques :

L'INERIS [INERIS DRA 35, 2006] classe les méthodes d'analyse des risques selon deux catégories :

- Méthodes classiques d'analyse des risques ex : APR, HAZOP, AdE, AdD, AMDEC.
- Méthodes intégrées d'analyse des risques ex : LOPA, MOSAR…

Nous intéressons aux méthodes que nous allons utiliser dans ce mémoire.

3.1. HAZOP « Hazard and Operability study »

La méthode HAZOP est dédiée à l'analyse des risques des systèmes thermo-hydrauliques. Considérant les dérives (ou déviations) des principaux paramètres liés à l'exploitation de l'installation. [INERIS DRA 35, 2006], Sa mise en œuvre nécessite la constitution d'un groupe de travail rassemblant autour d'un animateur, garant de la méthode, une équipe pluridisciplinaire ayant une connaissance approfondie de l'installation décrite sur des plans détaillés de circulation des fluides ou schémas PI&D.

Pour chaque partie du système examiné (ligne ou maille), la génération des dérives est effectuée de manière systématique par la conjonction :

- de mot-clé comme par exemple : « pas de », « plus de », « moins de »
- des paramètres associés au système étudié. Des paramètres couramment rencontrés sont la température, la pression, le débit, la concentration mais également le temps ou des opérations à effectuer.

MOT-CLE + PARAMETRE = DERIVE

➢ Le déroulement de la méthode :

- Dans un premier temps, choisir une ligne ou une maille. Elle englobe généralement un équipement et ses connexions, l'ensemble réalisant une fonction dans le procédé identifié au cours de la description fonctionnelle ;
- Choisir un paramètre de fonctionnement ;
- Retenir un mot-clé et étudier la dérive associée ;
- Identifier les causes et les conséquences potentielles de cette dérive ;
- Examiner les moyens visant à détecter cette dérive ainsi que ceux prévu pour en prévenir l'occurrence ou en limiter les effets.
- Proposer des recommandations et améliorations ;
- Retenir un nouveau mot-clé pour le même paramètre et reprendre l'analyse ;
- Lorsque tous les mots-clés ont été considérés, retenir un nouveau paramètre et reprendre l'analyse ;
- Lorsque toutes les phases de fonctionnement ont été envisagées, retenir une nouvelle ligne et reprendre l'analyse.

L'équipe se concentre alors sur les déviations conduisant à des risques potentiels pour la sécurité des personnes, des biens et de l'environnement. Elle examine et définit ensuite les actions recommandées pour éliminer, en priorité, la cause et/ou éliminer ou atténuer les conséquences [Michel ROYER, 2009].

- Paramètres: La méthode HAZOP fait appel à des paramètres spécifiques qui s'expriment par de simples mots (noms ou verbes) caractéristiques de l'intention de la conception (ex. Température, Pression, Débit...etc.) .
- Mots-clés ou mots guides : Parallèlement, la méthode introduit un nombre limité (sept à l'origine) de mots-clés appelés aussi « mots guides » (ex. non ou pas de ; plus de ; moins de ; en plus de ; en partie ; autre que ; inverse).
- Déviations : La combinaison de mots-clés et de paramètres va constituer une dérive, ou déviation, de ce paramètre :

Dans notre étude de cas, cette méthode sera appliquée dans un but d'identification des différents scénarios d'accidents.

Tableau 1. 2 : Exemple d'un tableau pour l'HAZOP

Date : Ligne ou équipement :								
1	2	3	4	5	6	7	8	9
N°	Mot clé	Paramètre	Causes	Conséquences	Détection	Sécurités existantes	Propositions d'amélioration	Observations

3.2. Arbre des évènements (AdE)

C'est une méthode déductive [Villemeur, 1987]. L'arbre d'événement part d'un événement et décrit les différentes conséquences qu'il peut avoir en fonction des conditions dans lesquelles il s'est produit et des événements avec lesquels il se combine.

On construit et on utilise un arbre d'événement dans une démarche d'évaluation a priori. Le point de départ est un incident, une défaillance, une erreur, une agression... dont on veut évaluer les conséquences possibles qui dépendent d'un certain nombre d'autres facteurs. Si on connaît les probabilités associées à ces facteurs on peut calculer en s'appuyant sur l'arbre d'événement la probabilité associée à chacune des conséquences possibles de l'incident initial [Yves Mortureux, 2002].

Son principe est à partir d'un évènement initiateur ou d'une défaillance d'origine, l'analyse par arbre d'évènements permet donc d'estimer la dérive du système en envisageant de manière systématique le fonctionnement ou la défaillance des dispositifs de détection, d'alarme, de prévention, de protection ou d'intervention…[INERIS DRA 35 , 2006].

La démarche à suivre est la suivante :

1- Définir l'événement initiateur à considérer.
2- Identifier et caractérisez les barrières de sécurité mises en place.
3- Construire l'arbre d'événements.
4- Décrire et exploiter les séquences d'événements pour déterminer la nature des événements identifiés en sortie de l'arbre.
5- Quantifier l'arbre d'événements.

L'AdE est le support pour LOPA, pour cela nous ferons appel à cette méthode pour représenter les scénarios d'accidents.

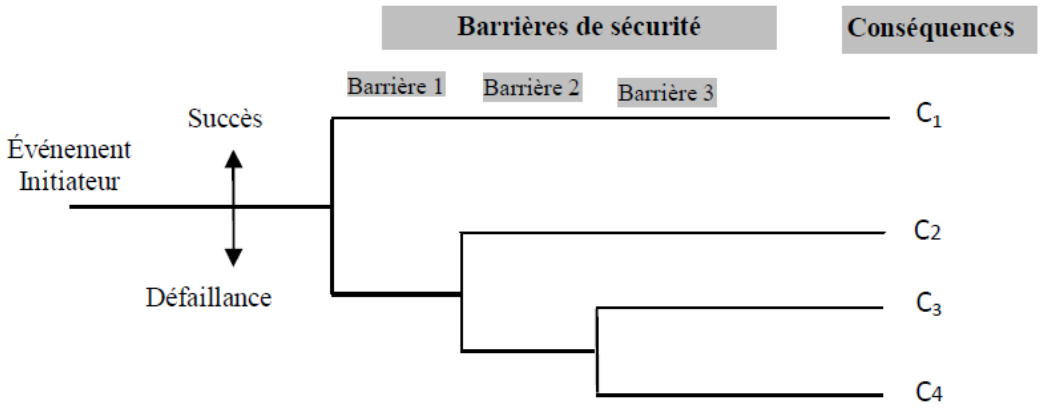


Figure 1. 6 : Schéma d'un AdE avec des barrières de sécurités

CHAPITRE2

SYSTEME INSTRUMENTE DE SECURITE

INTRODUCTION

L'objectif d'un SIS est de réaliser une ou plusieurs *fonctions de sécurité,* c'est-à-dire des fonctions prévues pour assurer ou maintenir un état de sécurité d'équipements commandés (EUC, pour « *Equipment Under Control* ») par rapport à un événement dangereux spécifique (par exemple, fuite, incendie, explosion). Face aux rôles critiques des SIS pour la maîtrise des risques technologiques, en tant que barrières de sécurité, leurs capacités à accomplir leurs fonctions de sécurité doivent être étudiées. Pour cela, des normes internationales dites de « sécurité fonctionnelle » ont été développées, notamment la principale référence qui est la CEI 61508 sur la sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité [IEC61508, 2002], [IEC61508, 2010]. La première édition de cette norme date de la fin des années quatre-vingt-dix et début des années deux mille [IEC61508, 2002], et la seconde édition a été publiée en 2010 [IEC61508, 2010].

Dans ce chapitre, nous présenterons en premier lieu ces normes internationales puis nous parlerons des SIS: leurs fonctions, leurs compositions, les différentes architectures, le SIL et les méthodes pour calculer le SIL requis et enfin les exigences de sécurité liées à la conception des SIS.

1. Cadre normatif

1.1. Norme CEI 61508 :

La CEI 61508 adopte une approche basée sur le risque afin de proposer une méthode générale pour la spécification d'exigences de sécurité, et concerne tout le cycle de vie de sécurité des systèmes et du logiciel. De plus, cette norme à caractère générique sert de base à l'élaboration de normes de produit et d'application sectorielle. Parmi les normes d'application sectorielle, figure notamment la CEI 61511 [IEC61511, 2004] pour les industries des procédés, et dont une équivalente américaine est l'ANSI/ISA S84.00.01-2004 [ISA, 2004]. Des exemples de normes de produit sont la CEI 62061 [IEC62061, 2005] pour les machines, et l'EN 50402 [ECES, EN50402, 2005] pour les systèmes de détection de gaz. La structure générale de la norme CEI 61508, avec les parties correspondantes (parmi les sept qui la composent), est comme suit :

1. définition des exigences globales de sécurité : concept, définition globale du domaine d'application, analyse des dangers et des risques, exigences globales de sécurité (Partie 1, Sections 7.1 à 7.5) ;

2. allocation des exigences de sécurité aux SIS (Partie 1, Section 7.6) ;

3. spécification des exigences de sécurité des SIS, afin d'obtenir la sécurité fonctionnelle requise (Partie 1, Section 7.10) ;

4. phase de réalisation, pour la conception des SIS en conformité avec la spécification des exigences de sécurité, concernant les systèmes (Partie 2) et les logiciels (Partie 3) ;

5. installation et mise en service, validation globale de la sécurité, avec les planifications associées (Partie 1, Sections 7.8, 7.9, 7.13, et 7.14) ;

6. exploitation, maintenance et réparation (avec la planification associée), modification et remise à niveau, mise hors service ou au rebut (Partie 1, Sections 7.7 et 7.15 à 7.17).

D’autres exigences concernent toutes les phases du cycle de vie de sécurité des SIS, au sujet de : la documentation (Partie 1, Section 5) ; la gestion de la sécurité fonctionnelle (Partie 1, Section 6) ; l’évaluation de la sécurité fonctionnelle (Partie 1, Section 8) ; et la vérification (Partie 1, Section 7.18). La Partie 4 donne les définitions et les abréviations utilisées dans la norme. Enfin, les autres parties sont informatives : la Partie 5 et la Partie 6 fournissent respectivement des lignes directrices pour l’application de la Partie 1 et des Parties 2 et 3 ; et la Partie 7 présente des techniques et des mesures.

La figure (figure 2.1) [Smith et Simpson, 2004] montre la norme CEI 61508 générique et ses normes filles par secteur d’activité

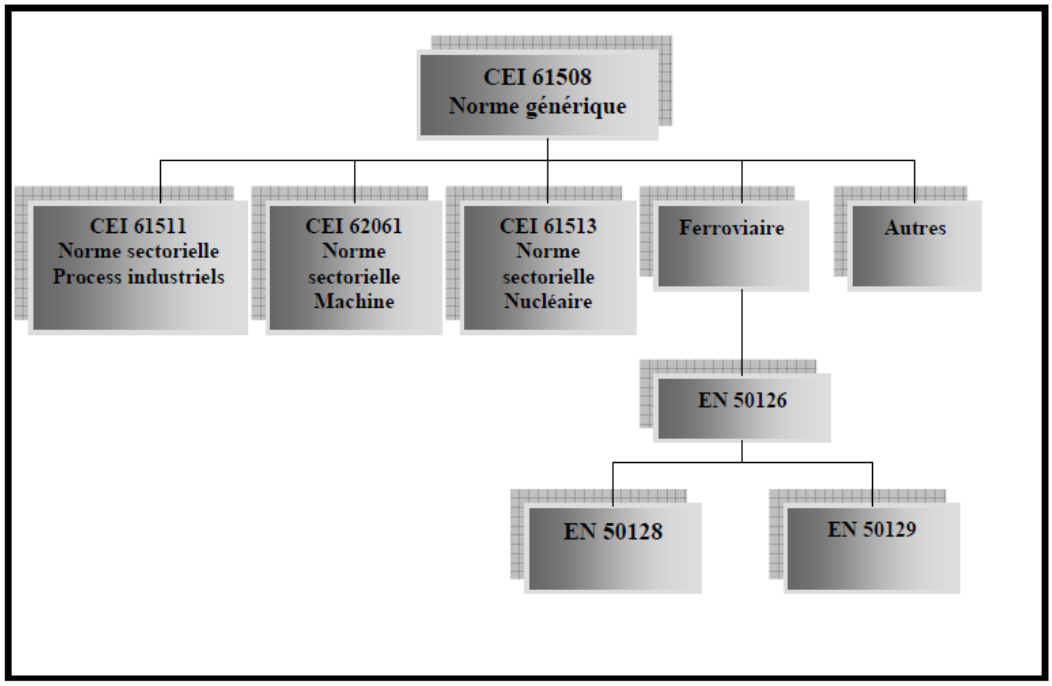


Figure 2. 1: Norme CEI 61508 et normes dérivées [Smith et Simpson, 2004]

1.2 .Norme CEI 61511

L'IEC 61511, s'intéresse à la sécurité fonctionnelle des SIS pour le secteur de l'industrie des procédés continus.

Elle comprend trois parties :

1. Cadre, définitions, exigences pour le système, le matériel et le logiciel,

2. Lignes directrices pour l’application de la CEI 61511-1,

3. Conseils pour la détermination des niveaux exigés d’intégrité de sécurité.

Cette norme permet de définir des exigences relatives aux spécifications, à la conception, à l’installation, à l’exploitation et à l’entretien d’un SIS, afin d’avoir toute confiance dans sa capacité à amener le procédé dans un état de sécurité.

1.3. Norme CEI 62061

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

1.4. Norme ISA-84

La norme ISA-84 était acceptée par l'institut national américain des normes (American National Standards Institute, ANSI) en mars 1997. Elle spécifie les exigences pour la conception, l'installation, l'utilisation et la maintenance des systèmes instrumentés de sécurité [Summers, 2000]. Elle dispose uniquement de trois niveaux d'intégrité de sécurité, SIL1 à SIL3.

2. Système instrumenté de sécurité SIS

2.1. Définition d'un SIS

La norme CEI 61511 [IEC61511, 2003] définit les systèmes instrumentés de sécurité de la façon suivante : système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux).

La norme CEI 61508 [IEC61508, 2002] définit quant à elle les systèmes relatifs aux applications de sécurité par : un système E/E/PE (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.

Un système instrumenté de sécurité est un système visant à mettre le procédé en 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…) [Sellak, 2007].

Les systèmes suivants en sont des exemples :

- Système d'arrêt d'urgence (*ESD : Emergency Shut down Systems*), utilisé, par exemple, dans les industries chimique et pétrochimique.
- Système d'arrêt automatique de train (*ATS : Automatic Train Stop*), utilisé dans le domaine ferroviaire.
- Système de freinage de l'automobile.
- Air-bag.
- Système de détection de surface d'un avion.
- Equipements médicaux critiques de traitement et de surveillance.

2.2. Fonction instrumenté de sécurité SIS

La fonction instrumentée de sécurité est définie comme étant la fonction de sécurité avec niveau d'intégrité de sécurité (SIL) spécifique qui est nécessaire pour maintenir la fonction de sécurité [Fal et Ldurka, 2000].

Une SIF est définie pour obtenir un facteur de réduction du risque mise en œuvre pour un SIS. Lorsque le SIS est considéré comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une fonction de sécurité [Mkhida, 2008], [Charpentier, 2002].

Une fonction instrumentée de sécurité est à réaliser par un système instrumenté de sécurité (ou par une combinaison des composantes de ce système), par un système relatif à la sécurité basé sur une autre technologie ou par un dispositif externe de réduction de risque. [Mkhida, 2008]

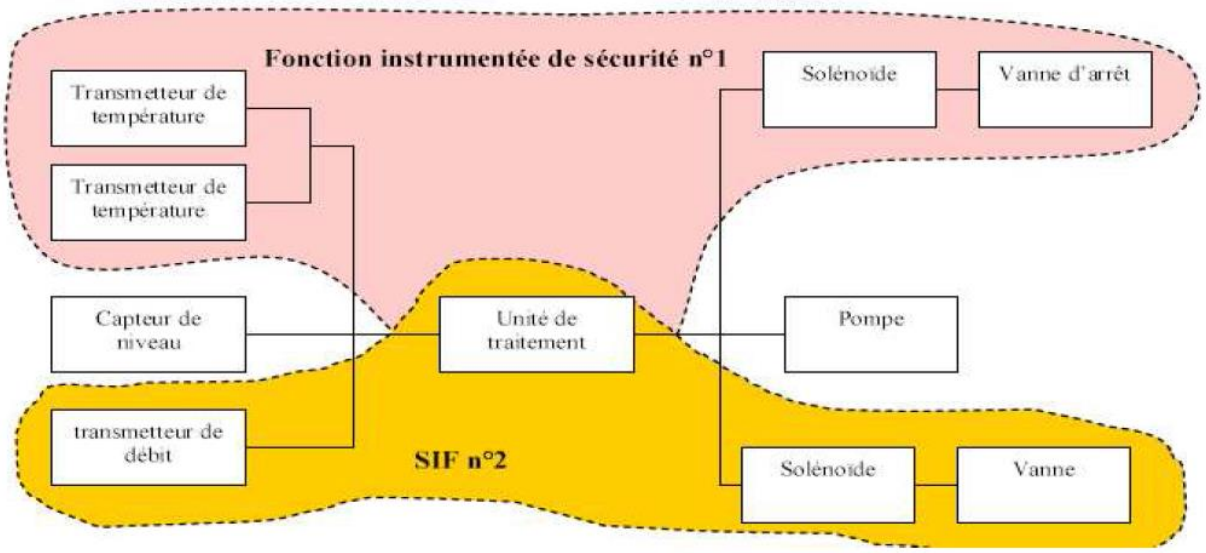


Figure 2. 2: Fonction instrumentée de sécurité [Mkhida, 2008]

2.3. Exigences de sécurité des SIS en accord avec la norme CEI 61508

En tant que notions fondamentales de la CEI 61508 se trouvent les exigences de sécurité des SIS. Celles-ci concernent les *fonctions de sécurité* et les *niveaux d'intégrité de sécurité* associés. La spécification des exigences des fonctions de sécurité des SIS consiste à décrire toutes les fonctions de sécurité qui leurs sont allouées (sur la base de l'analyse des dangers et des risques, et afin d'atteindre l'objectif de risque tolérable), qui sont nécessaires pour obtenir la sécurité fonctionnelle requise. De plus, doivent être spécifiés : le temps de réponse requis pour la réalisation des fonctions de sécurité ; les interfaces entre les SIS et les opérateurs ainsi que les autres systèmes ; les comportements requis des SIS en cas d'anomalies; les modes de fonctionnement de l'EUC; et toutes autres informations pertinentes susceptibles d'influencer la conception des SIS.

Une fonction de sécurité peut alors être sollicitée selon trois modes de fonctionnement [IEC61508, 2010] : *faible sollicitation*, lorsqu'elle n'est réalisée que sur sollicitation (afin de faire passer l'EUC dans un état de sécurité spécifié), et où la fréquence des sollicitations n'est pas supérieure à une par an ;

Sollicitation élevée, lorsqu'elle n'est réalisée que sur sollicitation, et où la fréquence des sollicitations est supérieure à une par an ;

Et *continu*, lorsqu'elle maintient l'EUC dans un état de sécurité en fonctionnement normal (à noter que cette classification diffère de celle de la précédente édition de la norme [IEC61508, 2002]).

La probabilité pour qu'un SIS accomplisse de manière satisfaisante les fonctions de sécurité spécifiées (dans toutes les conditions énoncées et dans une période de temps spécifiée) est l'*intégrité de sécurité* [IEC61508, 2010] (ce qui correspond en fait à la « disponibilité » du SIS. L'intégrité de sécurité comprend : l'intégrité de sécurité du matériel, qui est relative aux *défaillances aléatoires du matériel*, c'est-à-dire survenant de manière aléatoire et résultant d'un ou de plusieurs mécanismes de dégradation potentiels au sein du matériel ; et l'intégrité de sécurité systématique, qui est relative aux *défaillances systématiques*, c'est-à-dire liées de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés [IEC61508, 2010]. Pour chaque fonction de sécurité, une exigence relative à l'intégrité de sécurité cible est allouée (sur la base de l'analyse des dangers et des risques, et afin d'atteindre l'objectif de risque tolérable). Les intégrités de sécurité sont alors classées selon quatre niveaux discrets, nommés *niveaux d'intégrité de sécurité* (SIL, pour « *safety integrity levels*»), dont le niveau 4 possède le plus haut degré d'intégrité, et le niveau 1 le plus bas. Pour cela, un *objectif chiffré de défaillance* est spécifié selon le mode de sollicitation de la fonction de sécurité : *probabilité moyenne d'une défaillance dangereuse lors de l'exécution sur sollicitation de la fonction de sécurité* (*PFDavg*, pour « *average probability of failure on demand*»), définie comme une indisponibilité moyenne , pour un mode de faible sollicitation ; et *fréquence moyenne d'une défaillance dangereuse par heure* (*PFH*, pour « *probability of failure per hour*»), exprimée par heure.

En plus du niveau d'intégrité requis pour chaque fonction de sécurité, avec l'objectif chiffré de défaillance correspondant, et du mode de fonctionnement (faible sollicitation, sollicitation élevée, continu) de chaque fonction de sécurité, la spécification des exigences sur l'intégrité de sécurité des SIS doit comprendre : le cycle de service et la durée de vie requis ; les contraintes sur les essais périodiques ; les valeurs extrêmes des conditions environnementales des SIS ; les limites d'immunité électromagnétique ; et les contraintes relatives aux possibilités de défaillances de causes communes.

2.3. Propriété des SIS

• Les systèmes instrumentés de sécurité nécessitent une source d'énergie extérieure pour remplir leur fonction de sécurité.

• On retrouve tout ou partie de ces différents éléments pour constituer des chaînes de sécurité.

• Plusieurs capteurs ou actionneurs peuvent être reliés à une même unité de traitement.

• Toutes les combinaisons de capteurs, d'unité de traitement et d'actionneurs qui sont exigées pour accomplir des fonctions de sécurité sont considérées comme une partie de systèmes instrumentés de sécurité.

• Les capteurs, l'unité de traitement, les éléments finaux sont des équipements de sécurité et réalisent des sous-fonctions de sécurité. L'ensemble des sous-fonctions réalise la fonction de sécurité.

2.4. Composition d'un SIS

2. 4. 1. Composition minimale d'un SIS

Le SIS est un système permettant de mettre le procédé en état de sécurité stable et de la maintenir lorsque le procédé comporte un risque réel (explosion, incendie)

Les SIS sont constitués de différents éléments unitaires reliés entre eux par des moyens de transmissions. Au minimum, on retrouve en série un capteur, une unité de traitement et un actionneur [Ayault ,2005].

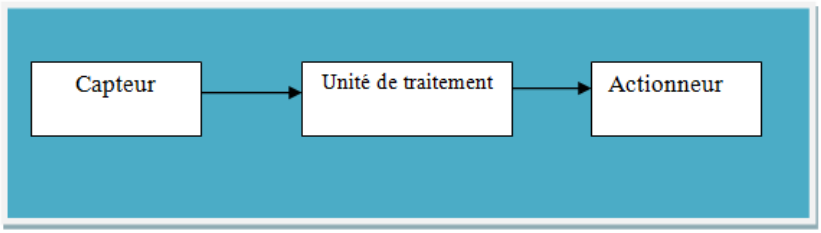


Figure 2. 3 : Schéma d'un SIS simple

A. Capteur

Est un équipement qui délivre, à partir d'une grandeur physique, une autre grandeur, souvent électrique (tension, courant, résistance), fonction de la première et directement utilisable pour la mesure ou la commande [Ayault, 2005].

Cette grandeur physique peut être la température, la pression, le niveau, le débit, la concentration d'un gaz.

B. Unité de traitement

Chargée de récolter le signal provenant du capteur, de traiter celui-ci et de commander l'actionneur associé ;

La fonction "traitement" peut être plus ou moins complexe [Ayault, 2005].

Les unités de traitement peuvent être classées en deux catégories selon leur technologie :

- Les technologies câblées, à base de composants logiques élémentaires (relais), liés entre eux électriquement (ou de manière pneumatique).
- Les technologies programmées, à base de centrales d'acquisition ou d'alarmes, d'automates programmables (API), de systèmes numériques de contrôle commande (SNCC), de calculateurs industriels ou de cartes électroniques à microprocesseurs.

C. Actionneur

Chargé de transformer le signal (électrique ou pneumatique) en phénomène physique qui permet de commander le démarrage d'une pompe, la fermeture ou l'ouverture d'une vanne….

On parle d'actionneur pneumatique, hydraulique ou électrique [Ayault, 2005].

Il agit directement ex : vanne d'arrêt d'urgence ou indirectement ex : vanne solénoïde.

2. 4. 2. Composition d'un SIS en fonction des tâches à accomplir

Le système instrumenté de sécurité a pour but de réaliser plusieurs fonctions. Ces dernières peuvent se décomposer en plusieurs taches (fermeture de plusieurs vannes, arrêt de plusieurs machines,..), c'est pour cela, on trouve au sein d'un SIS le montage en parallèle de plusieurs actionneurs.

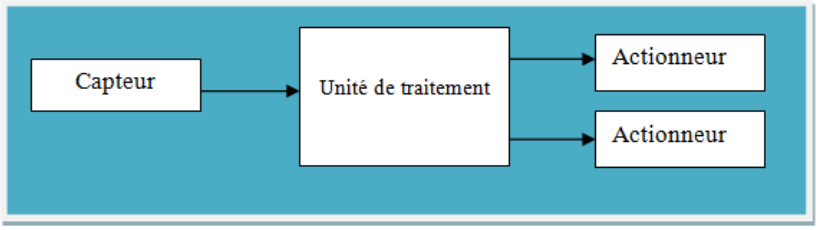


Figure 2. 4: Schéma d'un SIS effectuant plusieurs taches

- On trouve aussi le montage en parallèle de plusieurs capteurs afin de répondre à un besoin de réception d'informations différentes (Pression et température d'un fluide…), l'unité de traitement gère l'information soit par un opérateur logique or par les calculs.

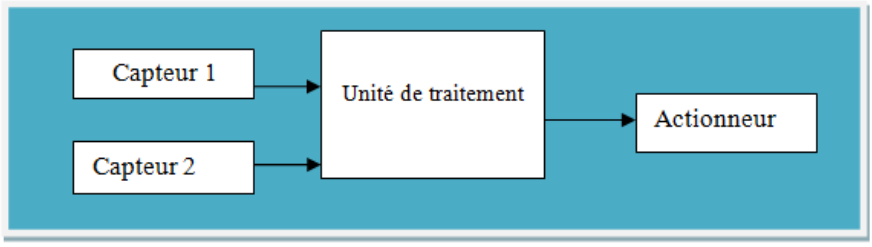


Figure 2. 5: Schéma d'un SIS recevant plusieurs informations

2. 4. 3. Redondance au sein d'un SIS

La redondance au sein d'un SIS consiste à doubler tous les composants d'un SIS (redondance totale) ou une partie de ses composants (redondance partielle).

On distingue plusieurs types de redondance :

La redondance active : qui est une redondance telle que tous les moyens d'accomplir une fonction requise fonctionnent simultanément.

La redondance passive : qui est une redondance telle qu'une partie seulement des moyens d'accomplir une fonction requise est en fonctionnement, le reste n'étant utilisé sur sollicitation qu'en cas de défaillance de la partie en fonctionnement.

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

Les architectures les plus souvent rencontrées relatives à ce dernier type de redondance sont les suivantes [Charpentier, 2002] :

- **Architecture 1*oo*1 :**

Cette architecture de base est composée d'un seul canal et qu'en conséquence toute défaillance dangereuse induit la perte de la fonction de sécurité en cas de demande. De plus, toute défaillance sûre conduit à l'exécution de cette fonction en absence de demande. Cette architecture minimale, qui ne tolère pas de défaillance, ne peut être utilisée dans des applications de sécurité. Le bloc-diagramme physique ainsi que le schéma électrique de principe relatif à cette architecture sont donnés à la figure 2.6 [CEI 61508-6, 2000] [Charpentier, 2002]. Les diagnostics y sont présents pour assurer la détection des défaillances (dangereuses et sûres) en vue de les réparer immédiatement.

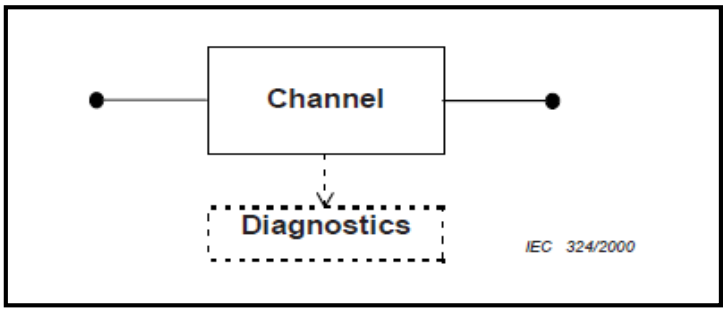


Figure 2. 6: Schéma de principe d'une architecture 1oo1

- **Architecture 1*oo*1D :**

C'est une architecture monocanale dans laquelle les tests de diagnostics sont capables de couper l'énergie de sortie en cas de détection de fautes. Les signaux en provenance du canal de traitement et ceux issus du système de diagnostic sont capables de supprimer l'alimentation de la charge, ce qui conduit à deux possibilités de passer dans un état sûr [Charpentier, 2002].

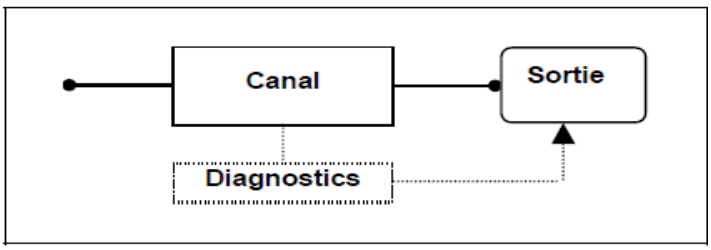


Figure 2. 7: Schéma de principe d'une architecture 1oo1D

La sortie peut être modélisée par deux relais câblés en séries, ouverts au repos.

A la mise sous tension, le canal ainsi que le circuit de diagnostic ferment les contacts des relais correspondants. En passe en état sur (relais ouvert) si la fonction de sécurité est activée ou si les diagnostics ont détecté une défaillance.

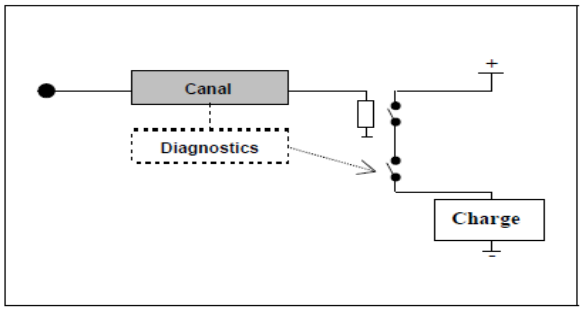


Figure 2. 8: Schéma électrique de principe d'une architecture 1oo1D

- **Architecture 1*oo*2 :**

Cette architecture consiste en deux canaux réalisant chacun la fonction de sécurité .La fonction de sécurité est exécuté dès qu'un canal en fait la demande, ce qui correspond à une fonction OU entre les deux canaux. Il faut donc une défaillance des deux canaux pour conduire à la défaillance de la fonction de sécurité sur demande.

Dans cette configuration, les tests de diagnostic signalent les fautes mais ne changent pas l'état de la sortie. La détection des fautes a pour but de remettre le système à l'état initial suite à réparation [Charpentier, 2002].

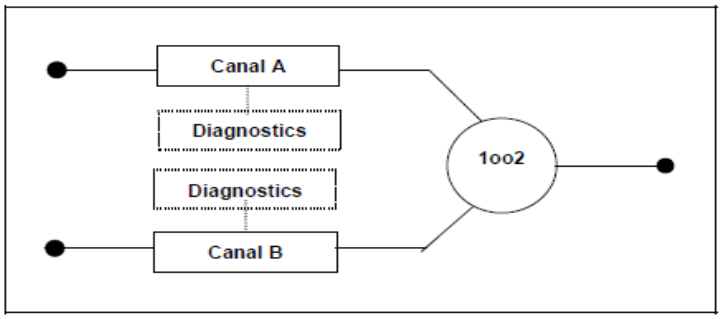


Figure 2. 9: Schéma de principe d'une architecture 1oo2

L'activation de la fonction de sécurité se traduit par l'ouverture des relais de sortie, Si une voie est défaillante avec sa sortie active (relais fermé), l'autre voie peut désactiver la décharge (ouvrir les relais) et assurer la fonction de sécurité.

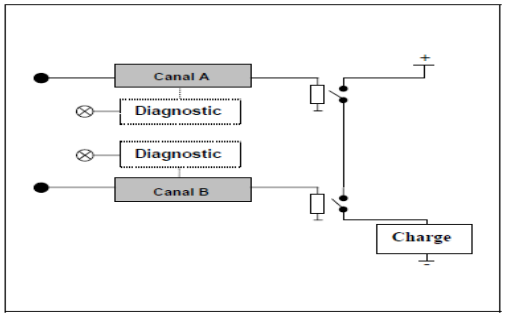


Figure 2. 10: Schéma électrique de principe d'une architecture 1oo2

- **Architecture 2*oo*2 :**

Cette architecture consiste en deux canaux connectés en parallèles, de sorte que les deux canaux doivent demander la fonction de sécurité pour que celle-ci soit activée. L'opération logique correspond à un ET entre les sorties des deux canaux. Le système a un comportement dangereux dès qu'une défaillance survient dans un des deux canaux.

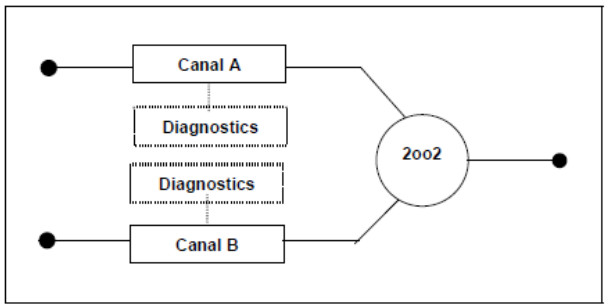


Figure 2. 11 : Schéma de principe d'une architecture 2oo2

La sortie est modélisée par deux relais câblés en parallèle, ouverts au repos. En fonctionnement normal, l'activation de la fonction de sécurité se traduit par l'ouverture des relais correspondant à chaque canal.
Le système a un comportement dangereux dès qu'une défaillance dangereuse survient dans un des deux canaux [Charpentier, 2002].

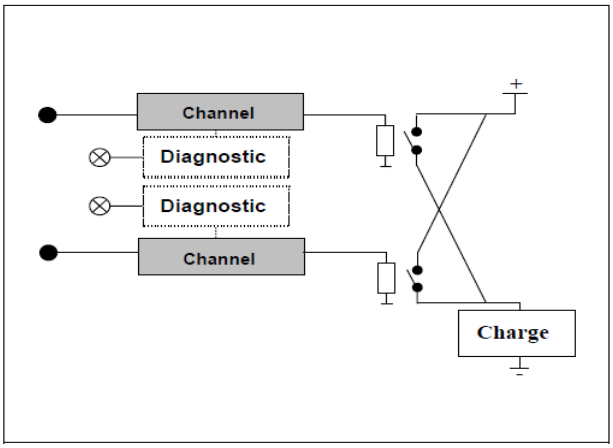


Figure 2. 12 : Schéma électrique de principe d'une architecture 2oo2

- **Architecture 2*oo*3 :**

Cette architecture consiste en trois canaux connectés en parallèles 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 [CEI 61508,1998], voir figure 2.13.

Dans cette configuration, les tests de diagnostic signalent les fautes mais ne changent pas l'état de la sortie.

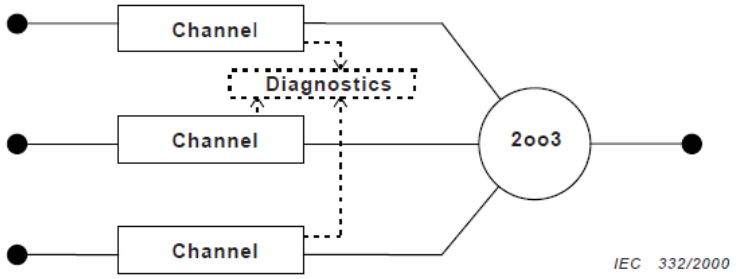


Figure 2. 13 : Schéma de principe d'une architecture 2oo3

- **Architecture 1*oo*3 :**

Cette architecture est composée de trois canaux connectés en parallèles, la fonction de sécurité est exécuté dès qu'un des trois canaux on fait la demande.

Dans cette configuration, les tests de diagnostic signalent les fautes mais ne changent pas l'état de la sortie.

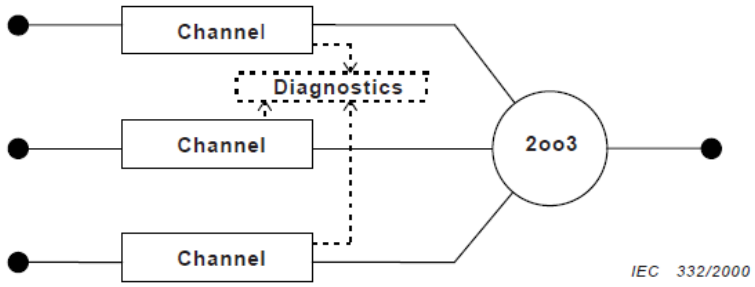


Figure 2. 14 : Schéma de principe d'une architecture 1oo3

2.5. Niveau d'intégrité de sécurité SIL

Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisée par des systèmes E/E/EP relatifs à la sécurité selon la norme IEC 61508 [IEC 61508, 2002] ou des fonctions instrumentés de sécurité selon la norme IEC 61511 [IEC61511, 2003].

La norme IEC 61508 [IEC61508, 2002] fixe le niveau d'intégrité de sécurité (SIL) qui doit être atteint par un SIS qui réalise la Fonction Instrumentée de Sécurité (SIF). Elle donne le SIL en fonction de sa probabilité de défaillance moyenne (PFDavg) sur demande pour les SIS faiblement sollicités. Ou en fonction de probabilité de défaillance par heure (PFH) pour les SIS fortement sollicités ou agissant en mode continu.

Le SIL est défini, selon l'IEC61508 [IEC61508, 2002], en 04 niveaux (plus le SIL est élevé, plus la disponibilité du système de sécurité est élevée).

Le SIL exigé est ensuite vérifier par le calcul de la PFD. La probabilité moyenne de défaillance sur demande d'une fonction de sécurité du système instrumenté de sécurité est déterminée par le calcul et la combinaison de La probabilité moyenne de défaillance sur demande pour tous les sous-systèmes assurant ensemble la fonction de sécurité. Cela peut être exprimé par la formule suivante [IEC 61508, 2002]

$$PFD_{syst} = PFD_C + PFD_U + PFD_A$$

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

PFD_C: Probabilité moyenne de défaillance sur demande du sous-système capteur.

PFD_A : Probabilité moyenne de défaillance sur demande du sous-système unité de traitement.

PFD_A : Probabilité moyenne de défaillance sur demande du sous-système actionneur.

2.6. Méthodes pour déterminer le SIL requis du SIS

Il existe trois méthodes pour la détermination du SIL requis :

2. 6. 1. Graphe de risque

Cette méthode a été introduite par la norme allemande DIN V 19250 [DIN V 19250, 1994], afin de pouvoir exprimer le risque sous forme de classes. La démarche est fondée sur l'équation caractérisant le risque (*R*) sans considérer les moyens instrumentés de sécurité : $R = f .C$, où f et C sont respectivement la fréquence et la conséquence de l'événement dangereux en l'absence de *SIS*.

La fréquence de l'événement dangereux f est généralement composée de trois facteurs :

F : la fréquence et la durée d'exposition aux dangers,

P : la possibilité d'éviter l'événement dangereux,

W : la probabilité de l'occurrence de l'événement dangereux sans moyen de protection (probabilité de l'occurrence non souhaitée).

La combinaison des quatre paramètres précédents (*C, F, P, W*) peut ramener à une configuration comparable à celle présentée à la figure 2.15 [CEI 61508-5, 1998].

Les paramètres (*C, F, P, W*) et leur pondération doivent être précisément définis pour chaque situation dangereuse. Une phase de calibrage ou d'étalonnage du graphe de risque est nécessaire. Elle permet d'adapter les paramètres en prenant en compte les spécificités de l'entreprise, la réglementation et les normes du secteur d'application.

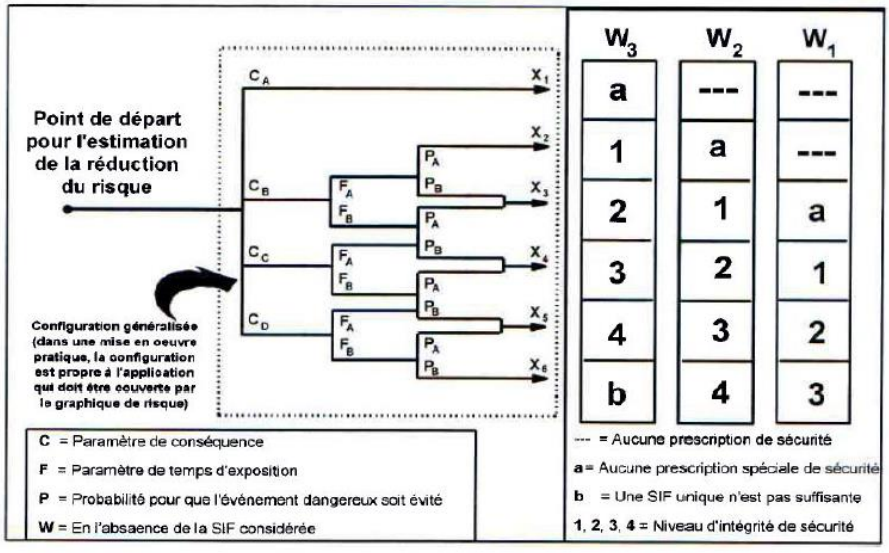


Figure 2. 15 : Schéma général du graphe de risque

Chaque échelon indique le niveau de SIL nécessaire auquel doit satisfaire le système relatif à la sécurité pris en considération.

2. 6. 2. Matrice de risque

Dite aussi matrice de gravité ou matrice des couches de protection, La matrice de risque intègre plusieurs fonctions de sécurité sous réserve de leur indépendance [IEC61508, 1998]. La matrice possède trois dimensions : la gravité, la probabilité d'occurrence de l'accident potentiel et le nombre de dispositifs de sécurité qui sont déjà mis en place pour empêcher le développement du danger en un accident [BEUGIN, 2006]. La structure de la matrice de risque dépend du domaine spécifique d'activité [BEUGIN, 2007].

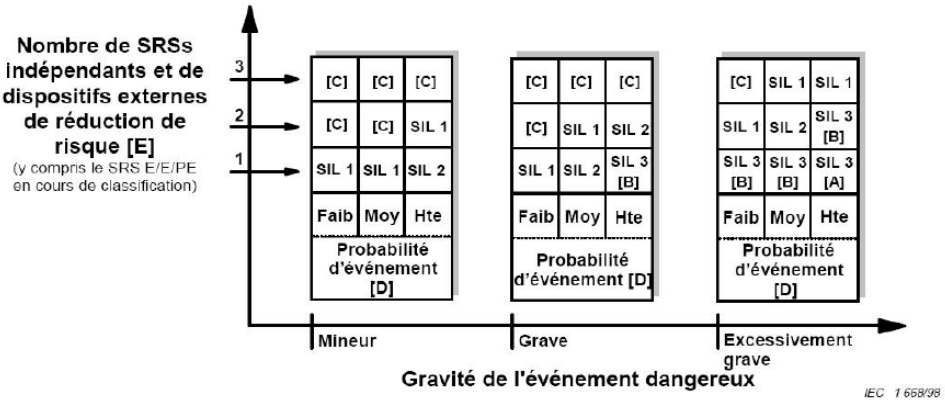


Figure 2. 16 : Exemple de matrice de gravité (principes généraux)

- **[A]** Un *SRS E/E/PE SIL3* n'apporte pas une réduction suffisante de risque à ce niveau de risque. Des mesures supplémentaires de réduction de risque sont nécessaires.
- **[B]** Un SRS *E/E/PE SIL3*, peut ne pas apporter une réduction suffisante de risque à ce niveau de risque. L'analyse des risques et des dangers est requise pour déterminer si des mesures supplémentaires de réduction de risque sont Nécessaires.
- **[C]** Un *SRS E/E/PE* n'est probablement pas nécessaire.
- **[D]** La probabilité d'événement est la probabilité que l'événement dangereux survienne sans système relatif à la sécurité ou sans dispositif externe de réduction de risque.
- **[E]** La probabilité d'événement et le nombre total de couches de protection indépendantes sont définis en relation avec l'application spécifique.

2. 6. 3. LOPA

La méthode la plus utilisée pour l'allocation des niveaux d'intégrité de sécurité est celle fondée sur principe d'analyse par couches de protection (*LOPA*: *Layers Of Protection Analysis*), voir figure 2.17 [CEI 61511, 2003] [CCPS, 2001]. Elle a été développée à la fin des années 1990 par le CCPS (*Centre for Chemical Process Safety*) [CCPS, 2001].

La méthode LOPA est une méthode semi-quantitative plus fréquemment utilisée pour :

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

✓ **Notion de couche de protection indépendante :**

La méthode LOPA introduit la notion de couche de protection indépendante (Independent Protection Layer [IPL]) :

Si pour une barrière, l'un de ces quatre critères ne peut pas être vérifié, le CCPS recommande alors de ne pas la retenir en tant que IPL (figure 2.17).

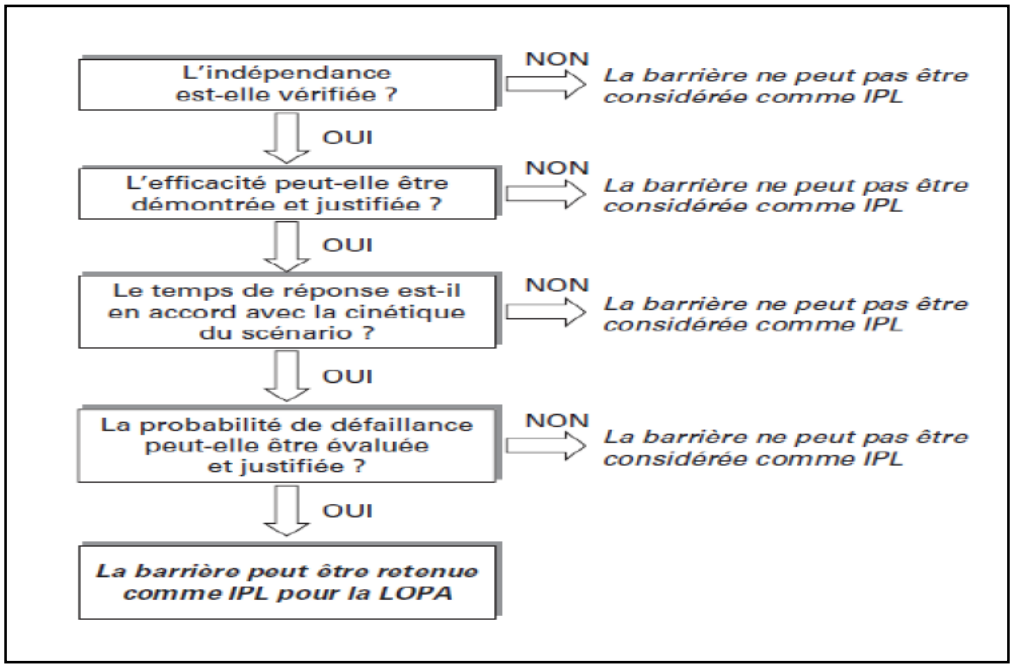


Figure 2. 17 : Processus de sélection d'une barrière en tant que IPL[CCPS, 2001]

✓ **Déroulement de la méthode LOPA :**

La démarche généralement retenus [CCPS, 2001] ; [Chanyang et al ,2008] pour réaliser une analyse par la méthode LOPA est la suivante :

- l'établissement des critères d'acceptabilité et de sélection des scénarios d'accidents à évaluer.
- Développement des scénarios d'accidents.
- Identification des fréquences des évènements initiateurs.
- Identification des couches de protection indépendantes et de leurs probabilités de défaillances à la demande.
- Détermination des fréquences des scénarios d'accidents.
- Evaluation des scénarios d'accidents par rapport aux critères d'acceptabilité du risque.

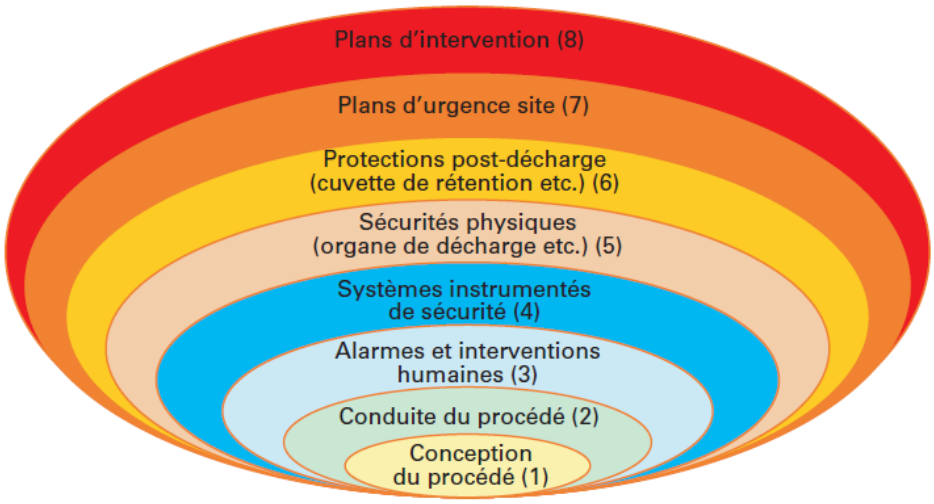


Figure 2. 18 : Différentes couches de protection suivant LOPA [CCPS, 2001]

La fréquence de l'événement redouté (scénario d'accident) s'obtient en multipliant la fréquence de l'événement initiateur et les probabilités moyennes de défaillance à la demande (*PFDmoy*) de chaque *IPL* s'opposant à ce même événement.

$$f^C = f^{IE} \times \prod_i PFD^i_{moy}$$

f^C : Fréquence de réalisation de la conséquence *C*,

f^{IE}: Fréquence de l'événement initiateur,

PFD^i_{moy}: Probabilité moyenne de défaillance sur demande de la barrière *i*. L'équipe *LOPA* doit déterminer cette quantité pour chaque barrière considérée.

La réduction du risque assignée à la fonction de sécurité du *SIS* s'obtient en comparant la fréquence de l'événement redouté à l'objectif de sécurité (fréquence tolérable : *ft*).

$$PFD^{SIS}_{moy} \leq \frac{f_t}{f^{IE} \times \prod_{i \neq SIS} PFD^i_{moy}}$$

2.6. Conception des SIS en accord avec la norme CEI 61508

Avant de débuter la phase de réalisation des SIS, les phases de définition, d'allocation, et de spécification des exigences de sécurité ont été menées. En particulier, les informations suivantes sont disponibles :

- Les fonctions de sécurité allouées aux SIS ;
- Le mode de fonctionnement de chaque fonction de sécurité ;
- Les objectifs chiffrés de défaillance, avec les SIL correspondants.

Tableau 2. 1 : Niveau d'intégrité de sécurité SIL : objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à faible sollicitation (Extrait de la norme CEI 61508 [IEC 61508, 2010]).

Niveau d'intégrité de sécurité (SIL)	Probabilité moyenne d'une défaillance dangereuse lors de l'exécution sur sollicitation de la fonction de sécurité (PFDavg)
SIL 4	$10^{-5} \leq \text{PFD} \leq 10^{-4}$
SIL 3	$10^{-4} \leq \text{PFD} \leq 10^{-3}$
SIL 2	$10^{-3} \leq \text{PFD} \leq 10^{-2}$
SIL 1	$10^{-2} \leq \text{PFD} \leq 10^{-1}$

Tableau 2. 2 : Niveau d'intégrité de sécurité SIL : objectifs chiffrés de défaillance pour une fonction de sécurité en mode de fonctionnement à sollicitation élevé ou continu (Extrait de la norme CEI 61508 [IEC 61508, 2010]).

Niveau d'intégrité de sécurité (SIL)	Fréquence moyenne d'une défaillance dangereuse par heure (PFH)
SIL 4	$10^{-9} \leq \text{PFH} \leq 10^{-8}$
SIL 3	$10^{-8} \leq \text{PFH} \leq 10^{-7}$
SIL 2	$10^{-7} \leq \text{PFH} \leq 10^{-6}$
SIL 1	$10^{-6} \leq \text{PFH} \leq 10^{-5}$

L'objectif de la phase de réalisation est de concevoir des SIS en conformité avec la spécification des exigences de sécurité. La phase de réalisation consiste en la spécification des exigences de conception ; la conception et le développement des SIS ; l'intégration ; les procédures d'installation, de mise en service, d'exploitation, et de maintenance ; et la validation (avec la planification associée).
La conception des SIS est basée sur une décomposition en sous-systèmes qui comprennent un ou plusieurs éléments (capteurs-transmetteurs, unités de traitement, actionneurs) et qui, lorsqu'ils sont réunis, permettent la réalisation de la ou des fonctions de sécurité allouées.

Les *contraintes architecturales* (portant sur l'intégrité de sécurité du matériel), pour chaque élément (ou sous-système) du SIS, sont basées sur les trois critères suivants [IEC 61508,2010] :

▪ La *tolérance aux anomalies du matériel* (*HFT*, pour « *hardware fault tolérance* ») de l'élément, qui est égale à *N* si *N+1* correspond au nombre minimal d'anomalies susceptibles de provoquer la perte de la fonction de sécurité ;

▪ La *proportion de défaillance en sécurité* (*SFF*, pour « *safe failure fraction* ») de l'élément, définie par le rapport des taux de défaillance moyens des défaillances en sécurité et dangereuses détectées (automatiquement par les essais de diagnostic en ligne), et des défaillances en sécurité et dangereuses (la méthode de calcul du *SFF* est présentée dans l'Annexe C de la Partie 2 de la norme) ;

▪ le *type d'élément*, qui est de « type A » si les modes de défaillance de tous ses composants sont bien définis, si son comportement dans des conditions d'anomalies peut être entièrement déterminé, et s'il existe des données de défaillance suffisamment fiables pour justifier des valeurs de taux de défaillance relatifs aux défaillances dangereuses ; et de « type B » si au moins l'une de ces conditions n'est pas vérifiée.

Le SIL maximal admissible pour une fonction de sécurité exécutée par un élément du SIS est alors donné dans les Tableaux 2.3 et 2.4, selon le type de l'élément. Pour un SIS constitué de plusieurs éléments, le SIL maximal admissible pour une fonction de sécurité allouée au SIS résulte alors de combinaisons de SIL, suivant des règles présentées dans la norme (Partie 2, Section 7.4.4.2).

Des travaux sur les contraintes architecturales des SIS, en accord avec la CEI 61508, ont été présentés dans la littérature [M.A Lundteigen, 2009]. En particulier, la pertinence de l'utilisation du *SFF* comme critère de sécurité a souvent été remise en cause [Y.Langeron, 2007] [F.Innal, 2006] [J.P.Signoret, 2007], tout comme les règles tout comme les règles de combinaisons de SIL lorsqu'un SIS est constitué de plusieurs éléments [Y.Langeron, 2008]. Une approche alternative a donc été introduite dans la seconde édition de la norme CEI 61508 [IEC 61508,2010], qui est basée sur le retour d'exploitation et qui n'utilise ni le *SFF*, ni les règles de combinaisons de SIL.

Une *HFT* minimale pour chaque élément (ou sous-système) du SIS exécutant une fonction de sécurité est alors définie, telle que donnée dans le Tableau 2.5.

Tableau 2. 3 : Niveau d'intégrité de sécurité (SIL) maximal admissible pour une fonction de sécurité exécutée par un élément (ou sous-système) de « type A » (extrait de la norme CEI 61508 [IEC61508, 2010]).

SFF	**Tolérance aux anomalies du matériel**		
	0	**1**	**2**
< 60%	SIL1	SIL2	SIL3
60% - < 90%	SIL2	SIL3	SIL4
60% - < 99%	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4

Tableau 2. 4 : Niveau d'intégrité de sécurité (SIL) maximal admissible pour une fonction de sécurité exécutée par un élément (ou sous-système) de « type B » (extrait de la norme CEI 61508 [IEC61508, 2010]).

SFF	**Tolérance aux anomalies du matériel**		
	0	**1**	**2**
< 60%	Not allowed	SIL1	SIL2
60% - < 90%	SIL1	SIL2	SIL3
60% - < 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

Tableau 2. 5 : Tolérance minimale aux anomalies du matériel pour chaque élément (ou sous-système) exécutant une fonction de sécurité d'un SIL spécifié, pour une approche basée sur le retour d'exploitation (d'après la norme CEI 61508 [IEC61508, 2010])

Niveau d'intégrité de sécurité (SIL)	tolérance minimale [a] aux anomalies du matériel (*HFT*)
SIL 4	*HFT = 2*
SIL 3	*HFT = 1*
SIL 2	*HFT = 0* ou *1*[b]
SIL 1	*HFT = 0*

a : Pour des éléments de « type A », il est possible, dans certains cas, d'avoir des *HFT* minimales plus faibles si cela est justifié du point de vue de la sécurité (cf. CEI 61508, Partie 2, Section 7.4.4.3.2).
b : Pour cette ligne, *HFT = 0* pour une fonction de sécurité en mode de fonctionnement à faible sollicitation, et *HFT = 1* pour une fonction de sécurité en mode de fonctionnement à sollicitation élevée ou continu. Les autres lignes sont indépendantes du mode de fonctionnement de la fonction de sécurité.

2.7. Adéquation des *SIS* aux niveaux d'intégrité de sécurité requis (*SIL* réel)

La norme CEI 61508 montre que la satisfaction aux mesures cibles de sécurité (SIL requis) se fait par l'observation simultanée des trois prescriptions suivantes :

- ***Prescriptions qualitatives*** : minimisation de l'occurrence des défaillances systématiques par l'application des différentes prescriptions pendant les différentes phases du cycle de vie de sécurités du *SIS*.
- ***Prescriptions quantitatives (probabilistes)*** : par le calcul de la probabilité moyenne de défaillance (*PFDmoy*), ou par heure (*PFH*), du *SIS* due exclusivement à des défaillances aléatoires du matériel.

Si la mesure cible du risque (en d'autre terme, le *SIL* spécifié lors de l'analyse des risques) n'est pas remplie, la conception du *SIS* sera changée jusque à la satisfaction de la mesure cible.

- ***Contraintes architecturales.*** La détermination du *SIL* de manière probabiliste via le calcul de la valeur moyenne de la *PFD* ou de la *PFH*, n'offrirait pas la garantie d'une précision suffisante, selon la norme CEI 61508. Il conviendrait donc de confirmer ou de corriger la valeur ainsi trouvée pour le *SIL* en appliquant une autre méthode de détermination, de nature différente : la prise en compte des contraintes architecturales.

Dans notre cas, nous allons utiliser les contraintes architecturales pour évaluer le SIS.

- Les différentes formules concernant la *PFDmoy* sont regroupées au tableau 2.6.

Tableau 2. 6 : Formules analytiques relatives aux PFDmoy des architectures KooN selon la CEI 61508-6

Architectures	PFDmoy [IEC 61508-6,2010]
1oo1	$(\lambda DD + \lambda DU).t_{CE}$
1oo2	$2((1-\beta_D)\lambda DD+(1-\beta)\lambda DU)^2 t_{CE}.t_{GE}+\beta_D\lambda DDMTTR+\beta\lambda DU(T1/2+MRT)$
1oo3	$6((1-\beta_D)\lambda DD+(1-\beta)\lambda DU)^3 t_{CE}.t_{GE}t_{G2E}+\beta_D\lambda DDMTTR+\beta\lambda DU(T1/2+MRT)$
2oo2	$2\lambda D.t_{CE}$
2oo3	$6((1-\beta_D)\lambda DD+(1-\beta)\lambda DU)^2 t_{CE}.t_{GE}+\beta_D\lambda DDMTTR+\beta\lambda DU(T1/2+MRT)$

Avec :

$t_{CE}=\frac{\lambda DU}{\lambda D}(T1/2+MRT)+\frac{\lambda DD}{\lambda D}MTTR$

$t_{GE}=\frac{\lambda DU}{\lambda D}(T1/3+MRT)+\frac{\lambda DD}{\lambda D}MTTR$

$t_{G2E}=\frac{\lambda DU}{\lambda D}(T1/4+MRT)+\frac{\lambda DD}{\lambda D}MTTR$

MTTR (Mean Time To Restoration) : temps moyen de restauration d'une défaillance dangereuse détectée.

MRT (Mean Repair Time) : temps moyen de restauration d'une défaillance dangereuse non détectée.

La norme suppose que **MTTR=MRT**

$\beta_{DD}=\beta_D$

$\beta_{DU}=\beta$

La norme ne tient pas compte des défaillances de cause commune pour les architectures série, en l'occurrence la configuration 2oo2.

Avec :

$PFDavg = \frac{1}{Ti}\int_0^{Ti} PFD(t)dt$

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

DC = $\frac{\sum \lambda_{DD}}{\sum \lambda_D}$

$\lambda DD = DC.\lambda D$

$\lambda DU = (1 - DC).\lambda D$

avec :

λDD: taux de défaillance aléatoire dangereuse détecté.

λDU *:* taux de défaillance aléatoire dangereuse non détecté.

$\lambda = \lambda S + \lambda D$

avec :

λS: taux de défaillance aléatoire en sécurité du matériel,

λD: taux de défaillance aléatoire dangereuse du matériel.

$\lambda D = \lambda DD + \lambda DU$

$\lambda S = \lambda SD + \lambda SU$

avec :

$\lambda SD, \lambda SU$ *:* taux de défaillance aléatoire en sécurité du matériel respectivement, détecté (D) et non détecté (U).

$\lambda SD = DCs.\lambda S$.

$\lambda SU = (1 - DCs).\lambda S$

DCs représente la couverture de diagnostic des défaillances aléatoires en sécurité.

$\lambda x = \lambda xind + \lambda xDCC = (1 - \beta_x)\lambda x + \beta_x \lambda x$

β_x est le pourcentage des *DCC (* L'indice « *ind* » signifie défaillances indépendantes dont l'occurrence n'affecte qu'un seul composant de l'architecture *KooN*, tandis que « *x* » est utilisé pour rendre compte de la partition précédente des défaillances (*DU, DD, SU, SD*).

CHAPITRE3

PRESENTATION DU LOGICIEL TIA PORTAL ET DE L'AUTOMATE PROGRAMMABLE

INTRODUCTION

Les API (Automate Programmable Industriel) ont pour fonctions de remplir des taches de commande pour élaborer des actions en suivant une algorithme appropriée à partir d'informations données par des capteurs, cet algorithme est écrit par un logiciel de programmation des API.

Dans ce chapitre, nous présenterons l'automate programmable siemens S7-300F qui a été choisi ainsi que le langage de programmation utilisé.

Dans ce qui va suivre nous allons étudier le logiciel de programmation et de supervision TIA PORTAL.

1. Généralités sur les Automates

L'automate Programmable Industriel, API (en anglais Programmable Logic Controller, PLC) est un type particulier d'ordinateur, robuste et réactif, ayant des entrées et des sorties physiques, utilisé pour automatiser des processus comme la commande des machines sur une ligne de montage dans une usine, ou le pilotage de systèmes de manutention automatique.

Dans ce chapitre, nous présenterons l'historique et l'architecteur de ces outils puissants ainsi les langages de programmation utilisée. Nous nous intéresserons, également à présenter les différentes gammes SIMATIC de Siemens.

1 .1 . Historique

Les automatismes séquentiels ont été réalisés, depuis longtemps, à base de relais électromagnétiques. L'inconvénient est qu'il s'agit d'un système câblée ce qui impose la refonte complète du câblage et ceci pour la moindre modification dans l'ordonnancement des séquences. En 1966, l'apparition des relais statiques a permis de réaliser divers modules supplémentaires tel que le comptage, la temporisation, le pas à pas ... Cependant cette technologie avait le même problème : technologie câblée.

En 1968 et à la demande de l'industrie automobile nord-américaine, sont apparus les premiers dispositifs de commande logique aisément modifiable : les PLC (Programmable Logic Controller) par *Allen Bradley*, *Modicom* [Slim Ben Saoud].

1 .2 . Définition d'un API (Automate Programmable Industrial)

Selon la norme NFC 63-850: L'API est un appareil électronique qui comporte une mémoire programmable, par un utilisateur automaticien, à l'aide d'un langage adapté pour le stockage interne des instructions composant les fonctions d'automatisme. Ainsi, la logique séquentielle et combinatoire, la temporisation, le comptage, le décomptage, la comparaison, le calcul arithmétique, le réglage, l'asservissement et la régulation…servent à commander, mesurer et contrôler au moyen de modules d'entrées et de sorties (logiques, numériques ou analogiques) différentes sortes de machines ou de processus, en environnement industriel.

C’est donc une machine électronique qui se place entre deux grands courants : la logique câblée et le calculateur universel. Elle se distingue par plusieurs caractéristiques et est conçue pour fonctionner dans des ambiances industrielles qui peuvent être sévères [Slim Ben Saoud].

1 .3 . Architecture des automates

Les automates peuvent être de type compact ou modulaire :

- de type compact. On distinguera les modules de programmation (LOGO de Siemens, ZELIO de Schneider, MILLENIUM de Crouzet ...) des micros automates. Cet automate intègre le processeur, l'alimentation, les entrées et les sorties. Selon les modèles et les fabricants, il pourra réaliser certaines fonctions supplémentaires (comptage rapide, E/S analogiques ...) et recevoir des extensions en nombre limité. Ces automates, de fonctionnement simple, sont généralement destinés à la commande de petits automatismes.
- de type modulaire. Le processeur, l'alimentation et les interfaces d'entrées / sorties résident dans des unités séparées (modules) et sont fixées sur un ou plusieurs racks contenant le "fond de panier" (bus et connecteurs). Ces automates sont intégrés dans les automatismes complexes ou puissants, capacité de traitement et flexibilité sont nécessaires dans ce cas.

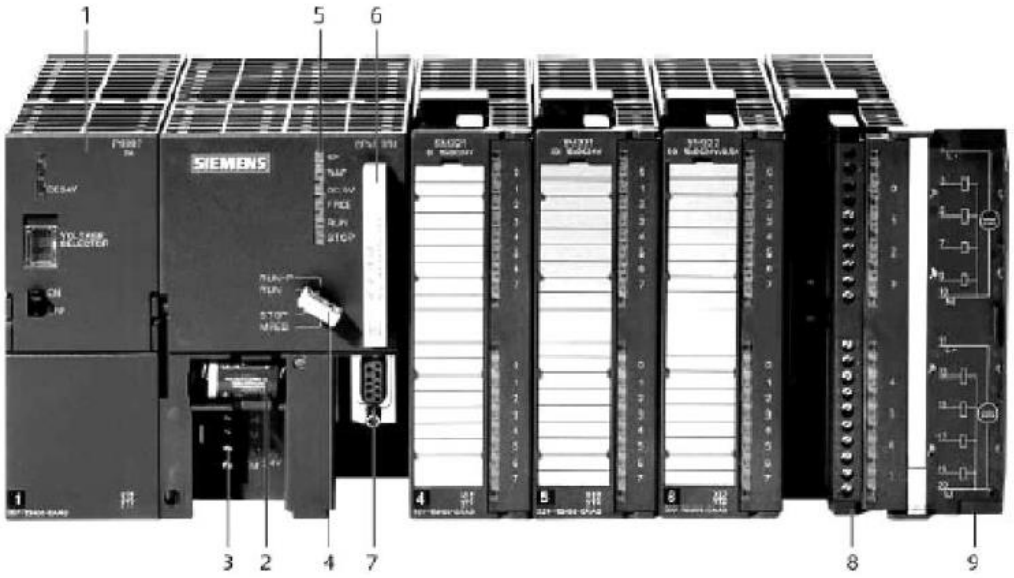


Figure 3. 1 : Automate modulaire (Siemens)

1 Module d'alimentation
2 Pile de sauvegarde
3 Connexion au 24V cc
4 Commutateur de mode (à clé)
5 LED de signalisation d'état et de défauts
6 Carte mémoire
7 Interface multipoint (MPI)
8 Connecteur frontal
9 Volet en face avant

1 .4 . Structure interne

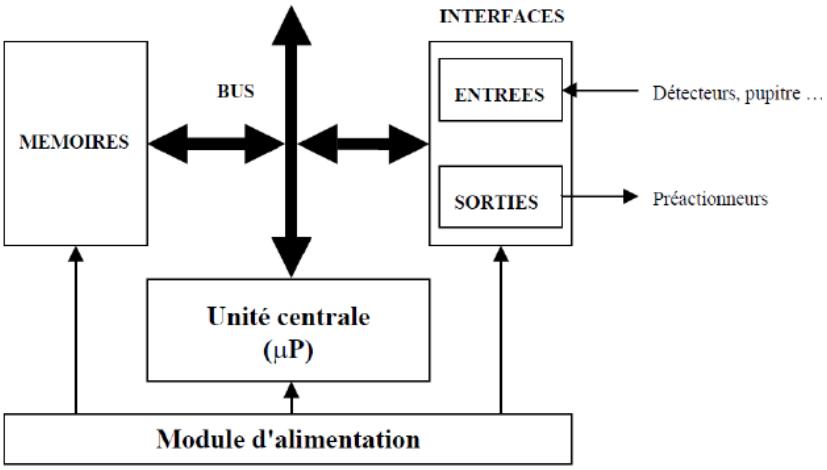


Figure 3. 2 : La structure interne d'un automate

- Le module d'alimentation assure la distribution d'énergie aux différents modules.
- L'unité centrale à base de microprocesseur réalise toutes les fonctions logiques, arithmétiques et de traitement numérique (transfert, comptage, temporisation ...).
- Le bus interne permet la communication de l'ensemble des blocs de l'automate et des éventuelles extensions.
- Les mémoires permettent de stocker le système d'exploitation (ROM ou PROM), le programme (EEPROM) et les données système lors du fonctionnement (RAM). Cette dernière est généralement secourue par pile ou batterie. On peut, en règle générale, augmenter la capacité mémoire par adjonction de barrettes mémoires type PCMCIA.
- Les interfaces d'entrées / sorties :
  - L'interface d'entrée permet de recevoir les informations du processus ou du pupitre.
  - L'interface de sortie permet de commander les divers pré-actionneurs et éléments de signalisation du processus tout en assurant l'isolement électrique.

1 .5 . Langages de programmation

La norme IEC 61131-3 (Commission Électrotechnique Internationale) définit cinq langages qui peuvent être utilisés pour la programmation des automates programmables industriels. Ces langages peuvent être divisés en deux catégories [P.Jargot].

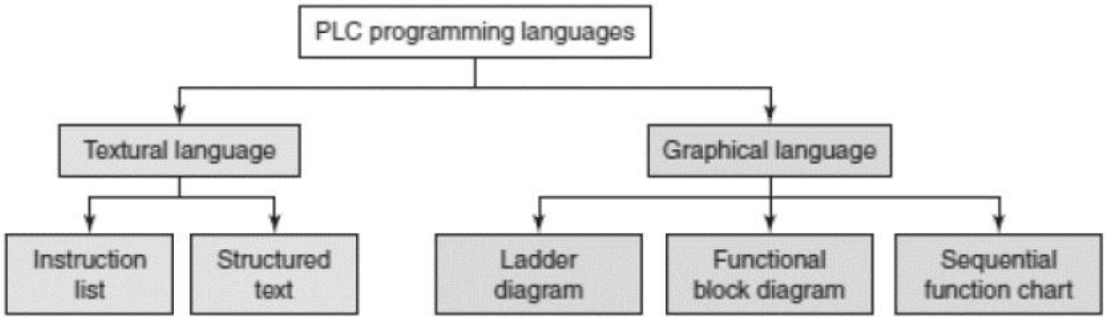


Figure 3. 3 : langages de programmation

- **Langages graphiques**

- SFC « Sequential Funiculite Chart » ou GRAFCET
- LD « LadderDiagram » ou schéma à relais
- FBD « Function Block Diagram » ou schéma par bloc.

- **Langages textuels**

- ST « structured text » ou texte structuré
- IL « Instruction List » ou liste d'instructions

On s'intéresse au langage graphique LD « Ladder Diagram » qui sera utilisé par la suite pour la programmation.

✓ **Langage Ladder LD (Ladder Diagram)**

Le LD est une représentation graphique qui traduit directement des équations booléennes en un circuit électrique et ce en combinant des contacts et des relais à l'aide de connexions horizontales et verticales ; les contacts représentent les entrées (contact normalement ouverts, contacts normalement fermés, …) et les relais représentent les sorties (relais directs, relais inversés,…). Les diagrammes LD sont limités sur la gauche par une barre d'alimentation et par la masse sur la droite.

Par exemple la fonction logique : s = a. (c + $\bar{d}$.b) est réalisée par le diagramme suivant:

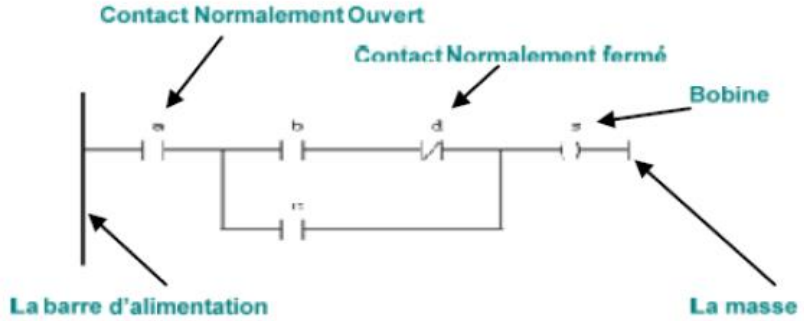


Figure 3. 4 : Exemple d'un programme en Ladder

1 .6 . Présentation du SIMATIC S7 300

Par le biais de la gamme SIMATIC des produits Siemens . L'intégration globale de tout l'environnement d'automatisation est réalisée grâce à :

• Une configuration et une programmation homogène des différentes unités du système.

• Une gestion cohérente des données.

• Une communication globale entre tous les équipements d'automatisme mis en œuvre.

Il existe différentes variantes de la gamme SIMATIC : SIMATICS7, C7, M7.

La gamme SIMATIC S7 comporte 3 familles : S7 200, S7 300 et S7 400.

On s'intéresse à la famille S7 300 :

- S7300 est un mini-automate modulaire pour les applications d'entrée et de milieu de gamme, avec possibilité d'extensions jusqu'à 32 modules, et une mise en réseau par l'interface multipoint (MPI), PROFIBUS et Industriel Ethernet.

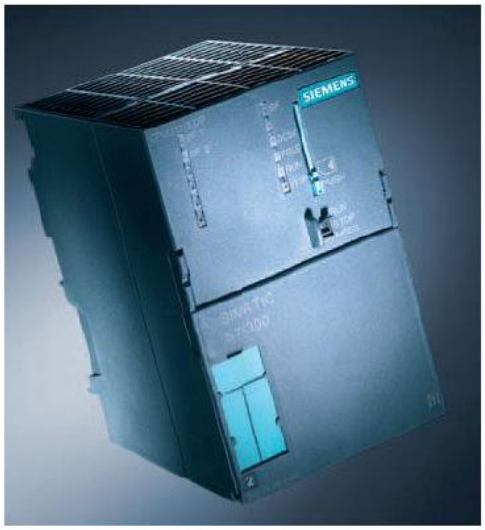


Figure 3. 5 : l'API S7 300

Parmi les automates de la famille S7 300, Nous avons choisi l'API SIMATIC S7-317F-2 PN/DP schématisé ci-dessous, ayant les caractéristiques suivantes :

Figure 3. 6 : CPU 317F-2 PN/DP

• Le CPU de sécurité dotée d'une grande capacité mémoire pour les programmes et de capacités fonctionnelles importantes pour les applications exigeantes, pour la réalisation d'automates de sécurité dans des installations exigeant un haut niveau de sécurité.

• Satisfait aux exigences de sécurité jusqu'à SIL 3 selon CEI 61508 et PL e selon ISO 13849.1

• Les modules de périphérie de sécurité sont raccordables en configuration décentralisée via l'interface PROFINET (PROFI safe) et/ou via l'interface PROFI BUS DP (PROFI safe) intégrée.

• Les modules de périphérie de sécurité de l'ET 200M peuvent également être raccordés en configuration centralisée.

• Possibilité d'utiliser les modules standards en configuration centralisée ou décentralisée pour des applications non sécuritaires.

• Component based Automation (CBA) sur PROFINET.

• Contrôleur PROFINET IO pour l'exploitation de périphéries décentralisées sur PROFINET.

• Interface PROFINET avec commutateur 2 ports.

• Appareil PROFINET intelligent générique (Proxy) sur PROFI BUS DP dans Component based Automation (CBA).

2. Présentation du logiciel TIA Portal

Le portail Totally Integrated Automation (portail TIA) intègre différents produits SIMATIC dans une application logicielle qui permet d'accroître la productivité et l'efficacité. Les produits TIA fonctionnent ensemble dans le portail TIA pour assister toutes les tâches de création de solutions d'automatisation.

Dans une tâche d'automatisation typique :

● Un automate commande le processus à l'aide du programme,

● Un pupitre opérateur permet de conduire et de visualiser le processus [SIEMENS, 2009]

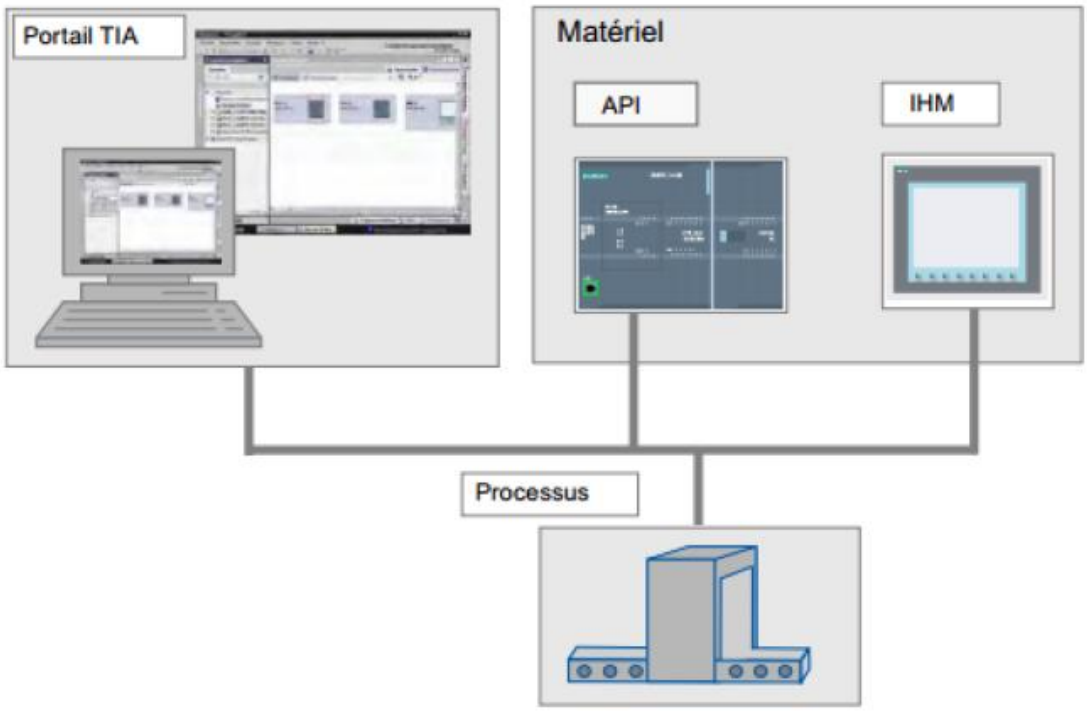


Figure 3. 7: TIA Portal

2.1. Concepts d'ingénierie

Grâce au portail TIA, la commande et la visualisation sont configurées dans un système d'ingénierie homogène. L'ensemble des données est stocké dans un projet. Les composants pour la programmation (STEP 7) et la visualisation (WinCC) ne sont pas des programmes autonomes mais des éditeurs d'un système qui accèdent à une base de données commune. Toutes les données sont enregistrées dans un fichier de projet commun.

Pour toutes les tâches, une interface utilisateur commune permettra d'accéder à tout moment à toutes les fonctions de programmation et de visualisation.

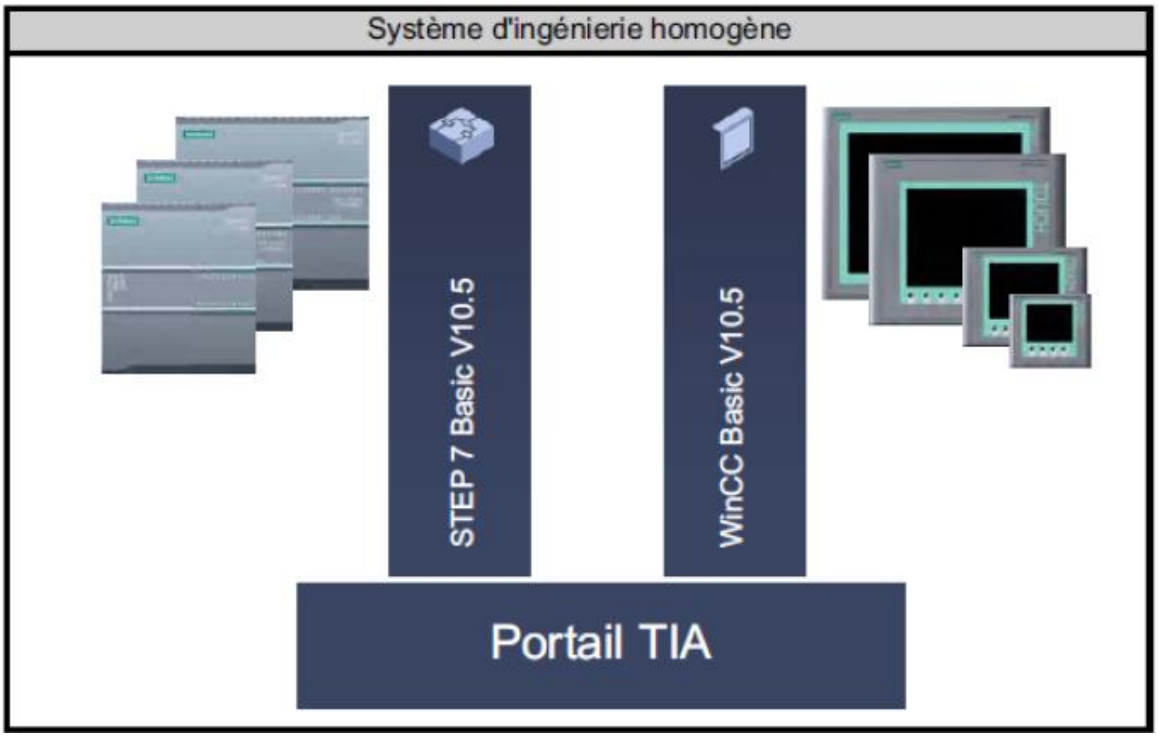


Figure 3. 8: Système d'ingénierie

2 .2 .Gestion des données

- Gestion centralisée des données :

Dans le portail TIA, l'ensemble des données est stocké dans un projet. Les données d'application modifiées, par exemple les variables, sont actualisées automatiquement dans tout le projet, sur plusieurs appareils si nécessaire.

- Adressage symbolique global :

Lorsqu' une variable de process est utilisée dans plusieurs blocs de différents automates et dans des vues IHM (Interface Homme Machine), il est possible de la créer ou la modifier à n'importe quel endroit dans le programme. Le bloc et l'appareil dans lesquels la modification doit se faire sont indifférents. Le portail TIA offre les possibilités suivantes pour la définition de variables API :

● Définition dans la table des variables API

● Définition dans l'éditeur de programmes

● Définition par association avec des entrées et sorties de l'automate

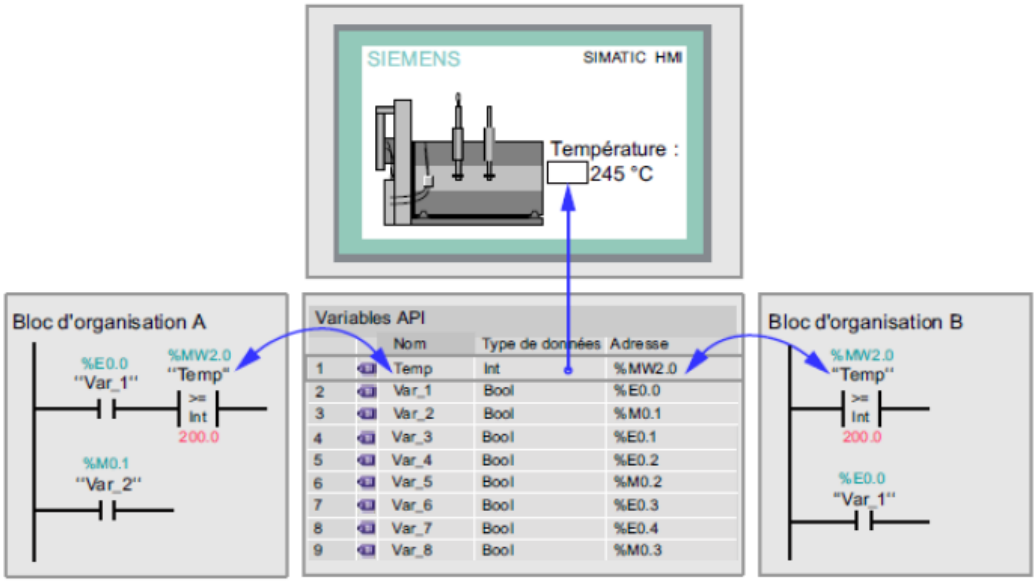


Figure 3. 9: Gestion des données

2.3. Les avantages du Portail TIA

Les avantages du Portail TIA sont les suivants :

- Gestion commune des données
- Manipulation homogène des programmes, données de configuration et données de visualisation
- Edition simple par glisser-déplacé.
- Chargement aisé des données dans les appareils
- Commande homogène
- Configuration et diagnostic graphiques.

2 .4 . Vue du Portail TIA

La vue du portail offre une vue orientée tâche sur les outils. Elle a pour but de faciliter la navigation dans les tâches et données du projet. A cet effet, les fonctions de l'application sont accessibles via des portails distincts, en fonction des principales tâches à réaliser. La figure suivante montre la structure de la vue du portail :

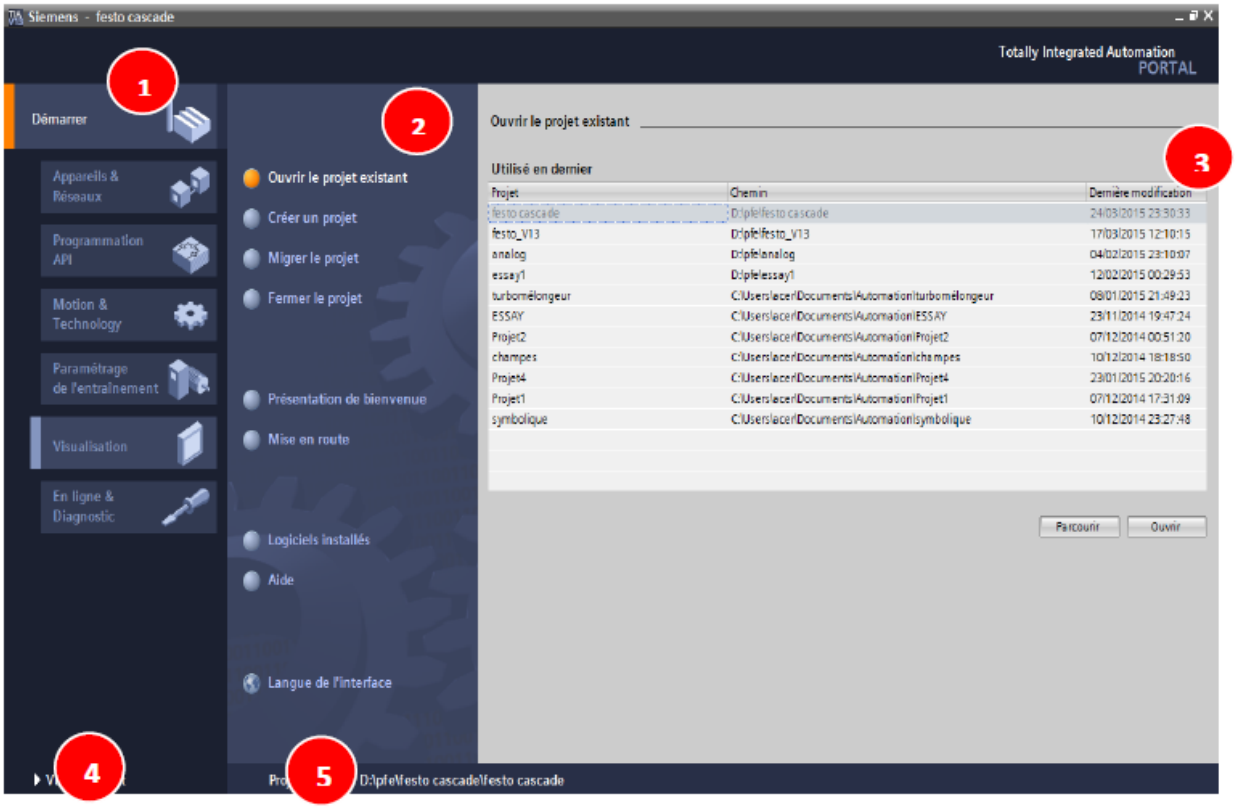


Figure 3. 10: la vue du portail

① Les portails mettent à disposition les fonctions élémentaires requises par chaque type de tâche. Les portails proposés dans la vue du portail dépendent des produits installés.

② En fonction du portail sélectionné, les actions qui peuvent être exécutées dans ce portail sont proposées ici. L'appel d'une aide contextuelle est proposé dans chaque portail.

③ La fenêtre de sélection est disponible dans chaque portail. Son contenu s'adapte à la sélection en cours.

④ Le lien "Vue du projet" permet de basculer dans la vue du projet.

⑤ Affichage du projet actuellement ouvert: Indique quel est le projet actuellement ouvert.

2.5 .Vue du projet

La vue du projet correspond à une vue structurée de l'ensemble de ses composants.

Dans la vue du projet, existent différents éditeurs à l'aide desquels sont créés et édités les composants du projet correspondants.

La figure suivante montre la structure de la vue du projet :

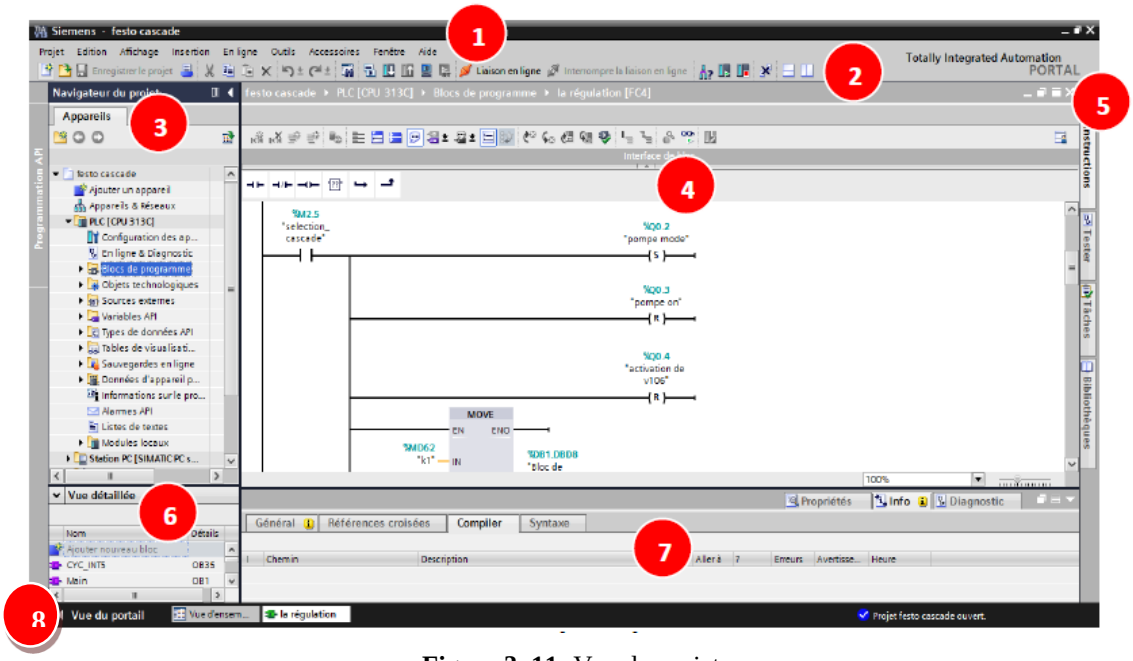


Figure 3. 11: Vue du projet

① La barre des menus contient toutes les commandes nécessaires pour réaliser une tâche.

② La barre d'outils met à notre disposition des boutons qui permettent d'exécuter les commandes les plus fréquemment utilisées. L'accès à ces commandes est ainsi plus rapide que via des menus.

③ Le navigateur du projet permet d'accéder à tous les composants et données du projet. Il est possible par exemple de réaliser les actions suivantes dans le navigateur du projet :

- Ajouter de nouveaux composants
- Editer des composants existants
- Interroger et modifier les propriétés de composants existants

④ La zone de travail affiche les objets qu'il faut ouvrir afin de les éditer.

⑤ Des Task Cards en fonction de l'objet édité ou sélectionné sont disponibles. Ils figurent dans une barre sur le bord droit de l'écran et peuvent être ouverts ou fermés à tout moment.

⑥ La vue détaillée affiche certains contenus d'un objet sélectionné. Il peut s'agir par exemple de listes, de textes ou de variables.

⑦ La fenêtre d'inspection affiche des informations supplémentaires sur un objet sélectionné ou sur des actions exécutées.

⑧ Le lien "Vue du portail" permet de basculer dans la vue du portail.

PARTIE PRATIQUE

CHAPITRE4

PRESENTATION DU CHAMP D'ETUDE

INTRODUCTION

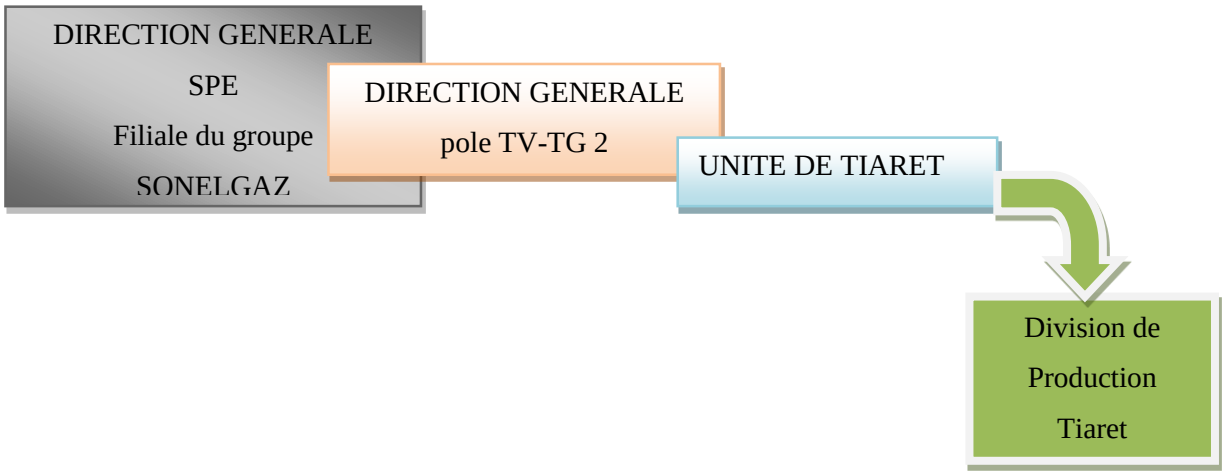
Notre champ d'étude se situe dans le poste gaz ALSTHOM.

Nous commencerons par présenter la centrale électrique TG de TIARET puis nous expliquerons le process de production d'électricité et les différents skid du poste gaz et en derniers lieu, nous nous intéresserons à la vanne de tête FSV 100 (ses caractéristiques ainsi que sa commande pneumatique) qui représente notre problématique.

1. Organisation générale de l'établissement

La Centrale est une Division de Production de l'unité de Tiaret, cette unité est affilé au pôle TG-TV centre (pole de production de SONELGAZ Production Electricité filiale de SONELGAZ).

L'organigramme ci-après donne la position hiérarchique de l'entité.



Le siège de l'unité s'occupe de la gestion administrative et technique de l'unité tandis que la division s'occupe de l'exploitation des groupes et la production de l'énergie électrique.

2. Implantation

La centrale de TIARET est une usine de production d'énergie électrique. Elle est entourée par des terrains agricoles et un terrain vague. Elle est implantée à 3 Km de la protection civile et du groupement de la gendarmerie Nationale et à 07 Km du centre de la ville de TIARET, s'étalant sur un espace de 4 hectares.

Sa capacité de production est de 404 MW divisée en deux groupes de Turboalternateurs FIAT et ALSTHOM utilisant le Gaz Naturel comme combustible.

Le rôle principal de la centrale est de produire de l'énergie électrique à partir de la combustion du gaz naturel. Elle alimente avec d'autres centrales en parallèles, un réseau national interconnecté qui part de l'Est à l'Ouest .L'exploitation de ce réseau est assuré par le dispatching, situé au niveau d'Alger, de la charge avec en moyenne une tension de 220 kV et une fréquence de 59 Hz (puissance de réseau national est 5000 MW)

2 .1 . Centrale FIAT

Elle comporte quatre Groupes de puissance de 26 MW chacun.

Chaque groupe est constitué de :

- 1 turbine à gaz du type TG20B2,
- 1 moteur de lancement,
- 1 coupleur hydraulique,
- 1 vireur,
- 1 pompe axillaire de graissage,
- 1 bac à huile de graissage de 8000 litres
- 1 alternateur,
- 1 excitatrice,
- 1 réducteur de vitesse.

2 .2 . Centrale ALSTHOM

Elle comporte trois Groupes de puissance de100 MW et ont été montés par la compagnie française ALSTHOM.

Chaque groupe est constitué de :

- 1 turbine à gaz du type TG9001E,
- 1 moteur virage,
- 1 pompe axillaire de graissage,
- 1 pompe de secours,
- 1 pompe haute pression,
- 2 pompes de circulation d'eau de refroidissement d'huile,
- 2 pompes de circulation d'eau de refroidissement alternateur,
- 2 ventilateurs,
- 1 dispositif de démarrage (un moteur de lancement, un convertisseur de couple et un réducteur des auxiliaires
- 1 bac à huile de graissage de 12000 litres,
- 1 bâche de reprise de 6000 litres,
- 1 bâche de charge de 6000 litres,
- 1 alternateur,
- 1 excitatrice,
- 1 système d'aspiration,
- d'aéroréfrigérants pour les turbines,
- d'aéroréfrigérants pour les alternateurs,

Le combustible principal des turbines est le gaz naturel. Le combustible de secours est le fuel (avec un point éclair minimum de 55°C).

3. Le gaz naturel

le gaz naturel est un produit inodore, incolore (pour des raisons de sécurité il est odorisé) est environ 1,5 fois plus léger que l'air (densité =0,6).

C'est un gaz extrêmement inflammable.il donne lieu à des mélanges explosifs(en présence d'une source d'allumage) avec l'air, dans des limites d'inflammabilité inférieures et supérieures respectivement de 5,3 à 15% en volume.

Il n'a pas d »effet toxicologique connu. Cependant il présente un danger d'asphyxie à haute concentration (teneur en oxygène insuffisante). De plus une combustion incomplète (défaut d'air) peut produire du monoxyde de carbone et être à l'origine d'un risque d'intoxication par les fumés.

Le gaz naturel étant distribué sous pression, sa détente provoque un refroidissement rapide et des risques de gelures.

Le gaz naturel est acheminé sur site par Gazoduc. Il arrive à une pression de 60 bars ; il est ensuite réduit à 21 bars pour le groupe ALSTHOM et 15 bars pour le groupe FIAT à travers un poste de détente puis il est acheminé vers les turbines.

En considérant la rupture complète ou partielle de la conduite d'alimentation principale de gaz naturel, deux types d'évènements peuvent être supposés :

- L'incendie
- L'explosion

Tableau 4. 1 : Les caractéristiques du gaz naturel (méthane)

PARAMETRE	GAZ NATUREL (METHANE)
Densité gazeuse (condition atm)	0,6
Chaleur de combustion (kJ/g)	50
Limite d'inflammabilité dans l'air (%vol)	5,3-15
Energie minimale d'inflammation (mJ)	0,29
Température d'auto-inflammation (°C)	540
Température de flamme (°C)	1875
Limite de détonabilité (%vol)	6,3-13,5
Taux de combustion dans l'air (condition atm) Vitesse de flamme laminaire (m/s)	40
Energie explosive (Kg TNT/m3)	7,03
Vitesse de flamme dans l'air (m/s)	37
Vitesse de détonation dans l'air (km/s)	1,8

4. Principe de fonctionnement d'une tranche de production

- Le groupe thermique turbine à gaz est constitué par une turbine gaz entraînant un alternateur, pour assurer une production électrique à la fréquence de 50 Hz.
- Le groupe turbine à gaz est constitué par une turbine à gaz à un seul arbre en cycle simple entraînant un alternateur.
- Dans la turbine à gaz. La combustion d'un mélange Air-gaz est utilisée pour produire la puissance sur l'arbre nécessaire à l'entraînement de l'alternateur principal, du compresseur et de certaines auxiliaires.
- La turbine à gaz comporte un dispositif de démarrage à moteur de lancement, des auxiliaires, un compresseur axial, un système de combustion et une turbine à trois étages.
- Au démarrage. Le moteur de lancement transmet son couple à la ligne d'arbre turbine à travers un convertisseur de couple et le réducteur des auxiliaires, qui comme son nom l'indique, entraîne un certain nombre d'auxiliaire comme les pompes par exemple.
- Dès que la ligne d'arbre est mise en mouvement par le moteur de lancement, l'air atmosphérique est aspiré, filtré et dirigé à travers les graines d'admission vers l'entrée du compresseur axial à (17 étages – Alsthom – 18 étages Fiat).
- A la sortie de compresseur, l'air pénètre dans un espace annulaire entourant les 14 chambres (Alsthom), 08 chambres (Fiat) de combustion puis dans l'espace situé entre l'enveloppe des chambres et les tubes de flamme.
- Le combustible est introduit par les injecteurs dans chacune des chambres de combustion où il est mélangé à l'air de combustion provenant du compresseur. La mise à feu est réalisée par deux bougies d'allumage (pour Fiat) pour Alsthom une seule suffit.
- La flamme se propage dans les autres chambres à travers les tubes d'interconnexion qui les relient entre elles au niveau de la zone de combustion.
- Les gaz chauds venant des chambres de combustions traversent les trois étages turbines, chaque étage est constitué par un ensemble d'aubes fixes suivi d'une rangée d'aubes mobiles. Dans chaque rangée d'aubes fixes, l'énergie cinétique du jet de gaz augmente tandis qu'apparaît une diminution de la pression dans la rangée adjacente d'aubes mobiles, une partie de l'énergie cinétique du jet est convertit en travail utile transmis au rotor de la turbine.
- Le travail fourni au rotor de la turbine sert à faire tourner l'alternateur et en partie à l'entraînement du compresseur axial et des auxiliaires de la turbine. Par définition un alternateur est une machine électro-magnétique destinée à fournir un courant alternatif
- Il est composé principalement d'une partie fixe appelée stator et qui est solidaire du massif et d'une partie mobile tournante appelée rotor accouplé à celui de la turbine par des brides.
- Ces deux parties comportent un circuit magnétique et sont séparées par un espace vide permettant la rotation appelée l'entrefer.

- Le rotor support l'enroulement qui crée le champ magnétique (inducteur) et le stator contient l'enroulement où apparaît la puissance électrique (induit).
- Le champ magnétique est créé par la rotation du rotor correspondant à la vitesse nominale de la tribune qui est de 3000 tr / mn.
- A cette vitesse, le champ magnétique qui est la conséquence d'une puissance mécanique est transformé en puissance électrique au niveau des bornes du stator qui est le siège de puissance électrique qui doit être évacuée vers l'extérieur (réseau).

5. Poste gaz ALSTHOM

Le poste gaz assure l'alimentation de la turbine, en gaz de bonne qualité . Il permet de filtrer, déshydrater, réchauffer et détendre le gaz à la pression et à la température de fonctionnement des groupes, c.à.d. de préparer le combustible nécessaire pour le fonctionnement de la turbine.

Le poste gaz ALSTHOM est composé de :

- **Skid séparateur :**

Le séparateur permet de piéger les bouchons d'hydrocarbures susceptibles d'être entraînés par le courant gazeux. Les liquides et les impuretés se déposent au fond de la cuve du séparateur, elles sont évacuées vers une citerne.

Il y a deux vannes d'isolement installées à l'entrée du poste gaz.

- **Vanne de sectionnement :**

C'est une vanne manuelle d'isolement 100V, situé a l'entré de poste gaz.
Elle a pour rôle d'isoler la ligne principale du gaz naturel de manière sur en cas d'arrêt normal ou de longue durée.

- **Vanne de sécurité :**

C'est une vanne de sécurité principale FSV100, à commande pneumatique situé après la vanne 100V.
Elle a pour rôle d'isoler la ligne gaz de manière rapide et sure. En cas d'urgence.
Elle fonctionne selon deux modes : commande automatique ou manuelle

Lorsque le niveau des impuretés « condensas » est très haut, le détecteur de niveau provoque la fermeture de la vanne d'isolement et arrête des groupes.

- **Skid de filtration :**

- Le gaz provenant du skid primaire passe dans le filtre à cartouche qui élimine les impuretés solides et la poussière.

- Les cartouches doivent être remplacées lorsque la pression différentielle aux bords du filtre atteint le seuil d'encrassement.

- Un système de séparation magnétique attire les particules métalliques.

- Un nettoyage périodique permet d'éliminer les dépôts recueillis.

- On le trouve après la séparation primaire, il est composé de deux filtres, le 1er est en service 200FI et le 2ième est un filtre de secours 201FI, ils sont composés d'une partie à cartouche associé à un système de séparation magnétique, leur rôle est d'éliminer toutes particules métalliques ou magnétique, les poussières et les gouttelettes de condensât.

- **Réchauffage de gaz.**

Apres le skid de filtration on a un réchauffeur de gaz qui permet de porter la température du gaz à 40°C Le gaz circule dans des faisceaux de tuyaux échangeur. Deux chaudières assurent le réchauffage en deux modes de fonctionnement.

- **Réchauffage d'attente :**

La chaudière chauffe l'eau à une température de 88°C. Le gaz ne circule pas à l'intérieur de cette chaudière. Quand la température d'eau descend au-dessous de 86°C, un ordre est donné pour l'ouverture de la vanne du brûleur de ¼ de tour Lorsque la température eau monte au-dessus de 88°C la vanne se ferme et les brûleurs s'éteignent. Ainsi cette chaudière gardera en secours une réserve d'eau chaude en cas de problèmes sur l'autre chaudière.

- **Réchauffage en mode TIC300 :**

L'échauffement du gaz est assuré par le régulateur qui contrôle la température sur la sortie chaudière.

La température du gaz est prise sur la tuyauterie sortie chaudière. Le signal température est envoyé vers le régulateur TIC300 qui convertit ce signal en pression pour commander la vanne des brûleurs. Le signal élaboré par le régulateur est proportionnel à l'écart qui existe entre la température prélevée sur la sortie et la consigne préréglée (40°C).

- **Skid de détente**

Situent après les chaudières et à côté de la citerne de méthanol.

On distingue trois rampes de détente en parallèle, chaque ligne est capable d'assurer le débit nécessaire et elle est composée par :

1- Un détendeur avec clapet de sécurité de haute pression.
2- Deux vannes d'isolement, entrée et sortie.
- Une vanne manuelle
- Une vanne pilotée.
3- Soupape de décharge ou de sécurité

Le détendeur a pour rôle de ramener la pression gaz de 60 bars en entrée vers une valeur de fonctionnement de groupe 20 bars.

La vanne de régulation maintient la pression de sortie à la valeur d'exploitation préréglée 20 bars ----- 30°C.

Un dispositif de sortie interrompe le passage du gaz en cas d'anomalies (basse ou haute pression).

- **Skid final**

-Ce skid est placé juste en avant de chaque groupe. Il comporte un filtre a cartouche, une vanne de sectionnement et un séparateur des condensât.

Les condensas sont évacués par une vanne.

La turbine est arrêtée en cas où les condensas atteignent un niveau très haut.

- **Skid - cuve a condensât -**

Il comporte un ballon de stockage des condensas provenant du piège à liquide (séparateur), les différents filtres et les soupapes de sécurité.

- **Comptage :**

Sur la ligne de distribution vers les skid finals, le tronc de comptage est Composé de :

- Dispositif de mesure de débit ;

- Thermomètre de mesure de température ;

- Manomètre de mesure de pression.

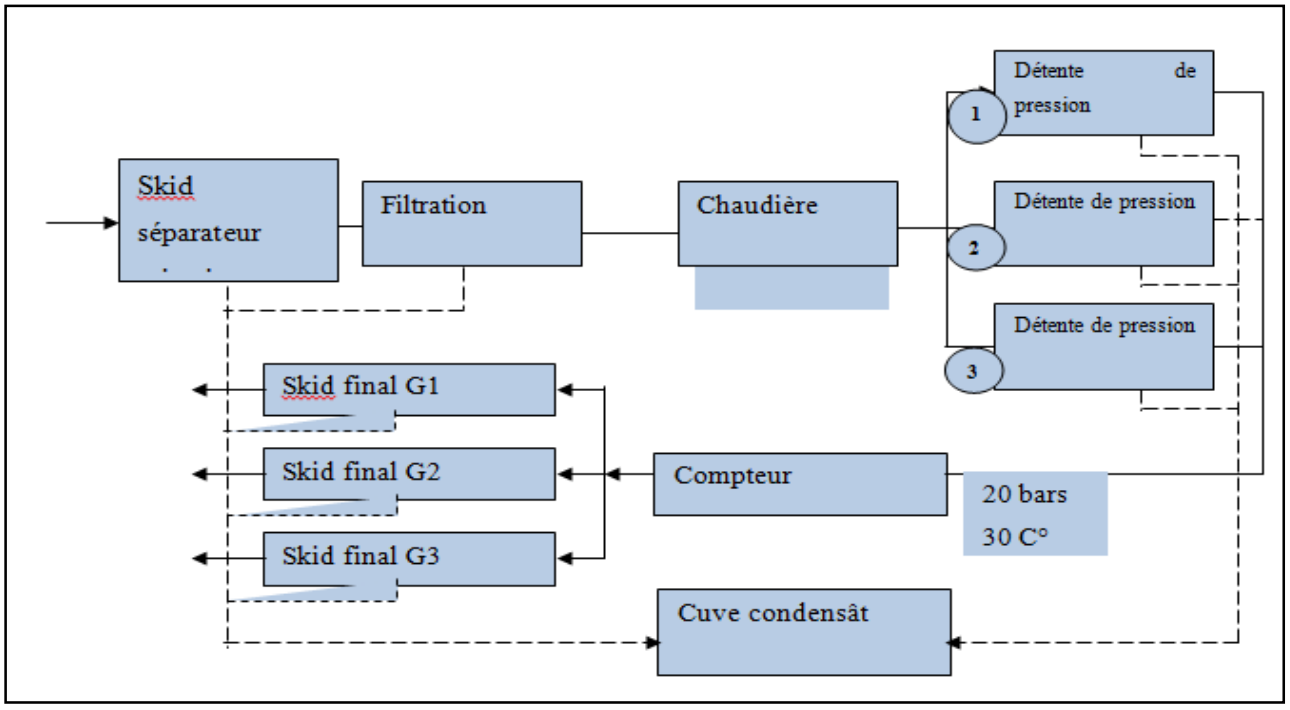


Figure 4. 1 : Schéma bloc simplifié du poste gaz ALSTHOM

6. La vanne de tête FSV 100

La vanne de sectionnement montée sur notre installation est une vanne à bille appelé aussi vanne de tête de sectionnement 10'' a boisseau sphérique équipée d'un système de commande pneumatique à simple effet avec des contacts de fins de course comme la montre la figure suivante :

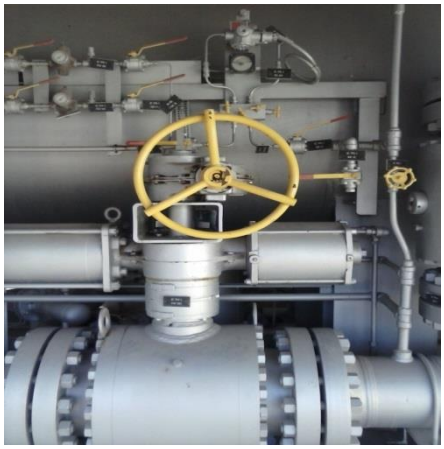


Figure 4. 2 : la vanne de tête FSV 100

6. 1. Les caractéristiques de la vanne

- La vanne possède les caractéristiques présentées dans le tableau suivant :

Tableau 4. 2 : Les caractéristiques de la vanne de sécurité FSV 100

vanne	
Constructeur	MAPEGAZ
Type de vanne	A bille à passage intégral
Opérateur de commande	Servomoteur pneumatique à simple effet avec ressort de rappel
Fluide	Gaz naturel pression max 10 bars
Pression	28 à 70 bars
Temps de manœuvre	Ouverture 5 secondes fermeture= 2 secondes
Commande	Fermeture et ouverture
Commande local	Oui
Commande manuelle de secours	Oui
Commande à distance	Oui
Nombre d'électrovanne de commande	Deux électrovannes de type ADFEEX D II CT6
Commande manuelle des électrovannes	oui
Tension de commande	125 vcc
Pression de commande	7 bars
Commande à distance	Fermeture d'urgence
Commande locale	Fermeture et ouverture (panneau au installé du voisinage du poste gaz
Indicateur de position	Fin de cours : Un à l'ouverture et Un à la fermeture

Les autres caractéristiques sont présentées dans l'annexe C.

6. 2. La commande de la vanne

La vanne FSV 100 comporte deux types de commande :

6. 2. 1. Commande locale

La commande manuelle devra être possible sans apport d'énergie électrique en conséquence la commande manuelle prévu sera par:

- Manipulation par volant manuelle : Fermeture et ouverture à la main par un volant horizontal.
- Commande par vanne : cette commande existe sur le panneau de commande.

- Fermeture manuelle par vanne: Commande locale du distributeur pneumatique avec un verrouillage de sécurité

- Ouverture manuelle par vanne : Commande locale du distributeur pneumatique avec un verrouillage de sécurité.

6. 2. 2. Commande à distance

Elle se fait à partir de l'armoire de commande (salle de contrôle) par émission de tension (125VCC) sur les électrovannes fermeture placées au niveau de l'armoire de commande électropneumatique

- **Commande d'urgence :**

a- Fermeture par manque d'alimentation électrique (tension de commande)
b- Fermeture sur pression différentielle (pressostat différentiel installée)

- Les tableaux suivants présentent les pressostats responsables de la fermeture et l'ouverture de la vanne ainsi que leurs seuils de déclenchement.

Tableau 4. 3 : Les Pressostats responsables de la fermeture et l'ouverture de la vanne FSV 100

Repère	Indication en salle de contrôle	Action	Observation
PSH 100	PAH 100	Ferme la FSV 100	Pressostat donnant l'ordre de fermeture de la vanne de tête par pression haute en amont de celle-ci.
PSL 100	PAL 100	Ferme la FSV 100	Pressostat donnant l'ordre de fermeture de la vanne de tête par pression basse en amont de celle-ci.
LSHH 100	LAHH 100	Ferme la FSV 100	Alarme niveau très très haut séparateur primaire donnant ordre de fermeture de la vanne de tête.
PDSL 100	PDAL 100	Autorisation d'ouverture de la FSV 100	Pressostat différentiel autorisant l'alimentation de l'électrovanne de commande pneumatique de la vanne de tête.

Tableau 4. 4 : Consignes des différents pressostats pour la fermeture de la vanne

Repère	Consigne
PSH 100	77 bars
PSL 100	28 bars
LSHH 100	500 mm
PDSL 100	0,5 bars

CHAPITRE5

DETERMINATION DU SIL REQUIS

INTRODUCTION

Ce chapitre est consacré à la détermination du SIL requis pour la réalisation du SIS adéquat à l'aide de la méthode LOPA. Pour ce faire, la démarche suivante est adoptée:

1- Faire une étude HAZOP afin de choisir les scénarios les plus critiques.
2- Estimer les évènements initiateurs associés aux conséquences graves choisis.
3- Développer ces scénarios à l'aide des arbres d'évènements AdE en spécifiant les barrières de sécurités qui peuvent éliminer ou réduire les conséquences graves.
4- Estimer les valeurs de fréquences des évènements initiateurs ainsi que les valeurs de PFD pour toutes les barrières.
5- Calculer la fréquence de chaque scénario puis déduire le PFD du SIS et donc le SIL requis à l'aide des tables présentées dans la norme CEI 61508.

- **Justification de l'utilisation de la méthode LOPA**

LOPA c'est une méthode précise et rigoureuse, ajoutant que la disponibilité de certains éléments nous a permis d'utiliser cette méthode pour déterminer le SIL requis pour le SIS .
Ces éléments sont les suivants :

- Fréquence tolérable d'accident ***Ft*** : elle doit être spécifiée de façon numérique (dans notre cas Ft du risque explosion est estimé à 1/100000 [UKOOA, 2003]).
- La fréquence de l'événement initiateur : ***FEi***. Elle peut être obtenue en utilisant le retour d'expérience, le jugement d'expert ou encore en utilisant des méthodes de prédiction appropriées (AdD, Chaînes de Markov, etc).
- Les probabilités de défaillances des couches de protection : ***PFD***.

Sachant que l'HAZOP a des informations en commun avec LOPA , En intégrant HAZOP et LOPA , on aura une analyse de haute qualité, ce qui nécessite moins de ressources.

1. Etablissement des critères d'acceptabilité

L'appréciation des risques consiste à juger de leur « acceptabilité ». Pour cela, chaque scénario (ou ensemble de scénarios) est positionné dans une matrice (dite « matrice de risques ») selon sa fréquence et sa gravité.
Par exemple, cette matrice est une transcription de celle présente dans la réglementation française [Bulletin Officiel, 2010], (à noter que cette matrice n'est pas valable pour toutes les applications, par exemple, le régime de la pyrotechnie et le stockage de gaz souterrain répondent à d'autres règles) :

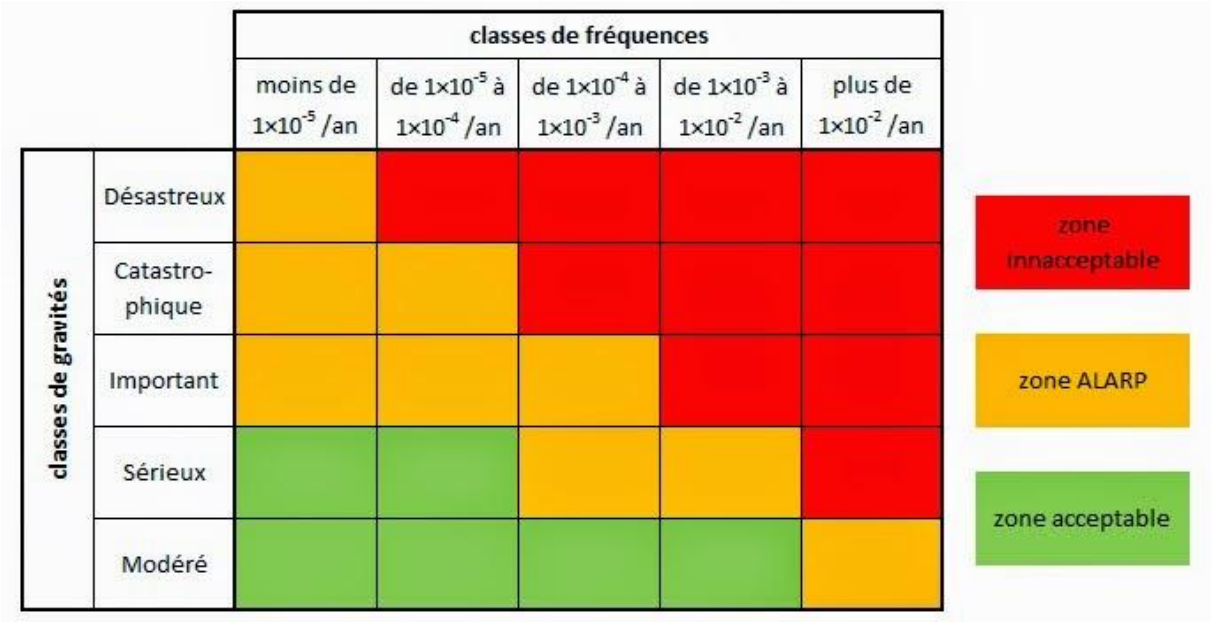


Figure 5. 1 : Matrice des risques [Bulletin Officiel, 2010]

En abscisse figurent des classes de fréquences et en ordonnée des classes de gravités, telles que définies par un arrêté [Journal Officiel, 2005].
Chaque risque (associé à un scénario ou à un ensemble de scénarios) ainsi reporté dans la matrice peut alors se situer dans l'une de ces zones d'acceptabilité :

Zone acceptable : le risque est acceptable en l'état. Il convient alors de s'assurer par un management approprié que le risque soit maintenu dans cette zone tout au long du cycle de vie de l'installation.
Zone ALARP : le risque est accepté sous condition que toutes les mesures de réduction du risque envisageables dont le coût n'est pas disproportionné par rapport aux bénéfices attendus ont été mises en œuvre. Il convient alors de s'assurer par un management approprié que le risque réponde toujours aux conditions ALARP et qu'il n'évolue pas dans la zone inacceptable au cours du cycle de vie de l'installation.
Zone inacceptable : le risque n'est pas acceptable en l'état et il est donc exigé de mettre en place des mesures de réduction du risque afin de faire passer ce dernier dans la zone acceptable ou, a minima, ALARP.

Tableau 5. 1 : Echelle de gravité

Niveau de gravité des conséquences	Zone délimitée par le seuil des effets létaux significatifs	Zone délimitée par le seuil des effets létaux	Zone délimitée par le seuil des effets irréversibles sur la vie humaine
Désastreux	Plus de 10 personnes exposées(1).	Plus de 100 personnes exposées.	Plus de 1000 personnes exposées.
Catastrophique	Moins de 10 personnes exposées.	Entre 10 et 100 personnes.	Entre 100 et 1000 personnes.
Important	Au plus 1 personnes exposée.	Entre 1 et 10 personnes exposées.	Entre 10 et 100 personnes.
Sérieux	Aucune personne exposée	Au plus 1 personne exposée.	Moins de 10 personnes exposées.
Modéré	Pas de zone létalité hors de l'établissement		Présence humaine exposée à des effets irréversibles inférieur à une personne.
(1) personne exposée :en tenant compte le cas échéant des mesures constructives visant à protéger les personnes contre certains effets et la possibilité de mise à l'abri des personnes en cas d'occurrence d'un phénomène dangereux si la cinétique de ce dernier et de la propagation de ses effets le permettent.			

Tableau 5. 2 : Echelle de probabilité

fréquence	Moins de 10^{-5}/ans	De 10^{-5}à 10^{-4}/ans	De 10^{-4}à 10^{-3}/ans	De 10^{-3}à 10^{-2}/ans	Plus de $10^{-2}/ans$
Signification	Evènement possible mais extrêmement peu probable.	Evènement très improbable.	Evènement improbable.	Evènement probable.	Evènement courant.
	N'est pas impossible au vu de la connaissance actuelle, mais non rencontré au niveau mondial sur un très grand nombre d'années.	S'est déjà produit dans ce secteurs d'activités, mais a fait l'objet de mesures correctives réduisant significativement sa probabilité.	Un évènement similaire déjà rencontré dans le secteur d'activité ou dans ce type d'organisation au niveau mondial sans que les éventuelles corrections intervenues depuis apporte une garantie de réduction significative de sa probabilité.	S'est produit et/ou peut se produire pendant la durée de vie de l'installation.	S'est produit sur le site et/ou peut se produire à plusieurs reprises pendant la durée de vie de l'installation , malgré d'éventuelles mesures correctives.

2. Etablissement de l'étude HAZOP au niveau du poste gaz ALSTHOM

Dans le but de sélectionner les scénarios les plus critiques afin de les évaluer à l'aide de la méthode LOPA, nous avons effectué une étude HAZOP en nous basant sur les schémas P&ID présentés en annexe D.

Tableau 5. 3 : Tableau HAZOP, Nœud N° 1« skid séparateur primaire »

Paramètre	Déviation	Causes	conséquences	Mesures existantes	recommandations
pression	Pas de pression	Pas d'alimentation du gaz à l'entré	-Arrêt des groupes -perte économique	Indicateur de pression (60bars) By-pass avec report de position en position o/f en salle de commande -capacité de retenu du liquide	Réserve en combustible secondaire
	Surpression	-Arrivage du gaz naturel à une haute pression.	-Rupture de la ligne principale du gaz -éclatement /explosion	- manomètre -pressostat différentiel -évacuation automatique des condensats -indicateur de niveau et alarme de colmatage -indicateur visuel et alarme de niveau haut des condensats	-Vérification périodique de la tuyauterai, des vannes et des joints --système automatique d'arrêt d'urgence SIS
	basse pression	-les fuites au niveau des joints -corrosion de la tuyauterai	-Rupture de tuyauterai -Incendie -explosion	- manomètre -pressostat différentiel -vanne de tête -détecteur de gaz - réseau anti-incendie -joint isolant pour protection cathodique	-Vérification périodique de la tuyauterai, des vannes et des joints -système automatique d'arrêt d'urgence SIS

Température	Haute température	-climat -augmentation de pression	-augmentation de pression - Bouchage des conduites.	-thermomètres -régulateur TIC 300(contrôle de température) -vanne de tête	
	Faible température	-climat -Sous pression	Sous pression - Givrage des conduites. - Givrage des vannes.	-thermomètres -chaudière - régulateur TIC 300 -citerne de méthanol	augmenter la température d'eau dans la chaudière de plus de 90°c

débit	Pas de débit	-Pas d'alimentation du gaz à l'entré - Fermeture intempestive de la vanne de tête	-arrêt de l'installation	Indicateur de niveau	système d'alimentation secondaire (by-pass).
	Faible débit		-perte de charge	- détecteur de gaz - système d'arrosage.	Vérification périodique de la tuyauterai, des vannes et des joints
	Haut débit	-augmentation des condensats	-Niveau élevé des condensats -explosion	- cuve des condensats -détecteur de niveau sur la cuve	Vérification périodique de la tuyauterai, des vannes et des joints

Les autres Tableaux HAZOP sont présentés dans l'annexe A.

3. Estimation des conséquences selon les critères d'acceptabilités

Les scénarios les plus critiques sont représentés dans le tableau suivant :

Tableau 5. 4 : Estimation des conséquences

Conséquence	Gravité
Surpression qui peut provoquer une explosion	Catastrophique
Une très baisse de pression qui peut provoquer une explosion par retour de flamme	Catastrophique
Une augmentation de niveau des condensats qui peut provoquer une explosion	Catastrophique

Comme les trois scénarios sont les plus critiques qui peuvent engendrer une grande explosion, les conséquences estimées ci-dessus sont jugées de catégories catastrophiques.

4. Sélection des scénarios à évaluer par LOPA

En se référant aux tableaux HAZOP présentés précédemment, les scénarios les plus critiques ont été sélectionnés et présentés dans le tableau suivant :

Tableau 5. 5 : Sélection des scénarios à évaluer

N° de Scénario	Scénario	Conséquences	Evènement initiateur	Fréquence des Ei	Référence
1	La défaillance du régulateur externe peut causer une surpression à l'entré gaz qui peut provoquer une explosion.	Surpression qui peut provoquer une explosion	Défaillance d'un système de régulation de pression	1,0E-01	[ICSI, 2009], [CCPS,2001]
2	Un cisaillement d'une conduite de gaz en aval de la vanne de tête FSV100 provoque une fuite qui provoque une baisse de pression peut aller jusqu'à une explosion.	Une très baisse de pression qui peut provoquer une explosion par retour de flamme	Fuite en aval de la vanne de tête	1,0E-03	[CCPS,2001]
3	La défaillance du régulateur de niveau peut engendrer un niveau très haut des condensats qui peut provoquer une explosion.	Une augmentation de niveau des condensats qui peut provoquer une explosion	Défaillance d'un système de régulation de niveau	1,0E-01	[ICSI, 2009], [CCPS,2001]

5. Fréquences des évènements initiateurs

A partir de L'étude HAZOP réalisée, les évènements initiateurs des conséquences définis ci-dessus sont regroupés dans le tableau suivant :

Tableau 5. 6 : Fréquence des évènements initiateurs

Evènement initiateur	Fréquence des Ei	Référence
Défaillance d'un système de régulation de pression	1,0E-01	[ICSI, 2009],[CCPS,2001]
Fuite en aval de la vanne de tête	1,0E-03	[CCPS,2001]
Défaillance d'un système de régulation de niveau	1,0E-01	[ICSI, 2009], [CCPS,2001]

Remarque : On considère généralement que les défaillances de systèmes de régulation sont provoquées dans 15% des cas par la logique, pour 50% par les actionneurs et pour 35% par les capteurs [ICSI, 2009] .

6. Identification des couches de protection indépendantes

Les IPLs et leurs PFDs sont données dans le tableau suivant :

Tableau 5. 7 : PFD des IPLs

IPL	PFD	Source
Détection gaz	5,0E-02	[ICSI, 2009]
Alarme &opérateur	1,0E-01	[CCPS, 2001], [ICSI, 2009]
Soupape de sécurité	1,0E-02	[CCPS, 2001], [ICSI, 2009]

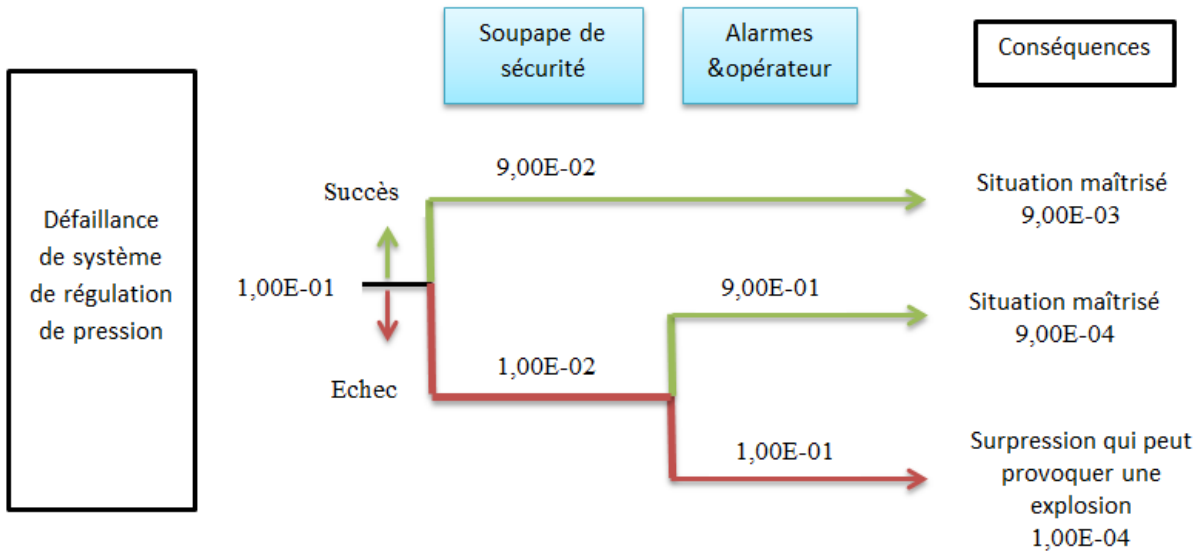
7. Détermination des fréquences de scénarios

Les trois scénarios sélectionnés sont présentés sous forme d'AdE pour faciliter le calcul de la fréquence des scénarios en appliquant l'équation suivante :

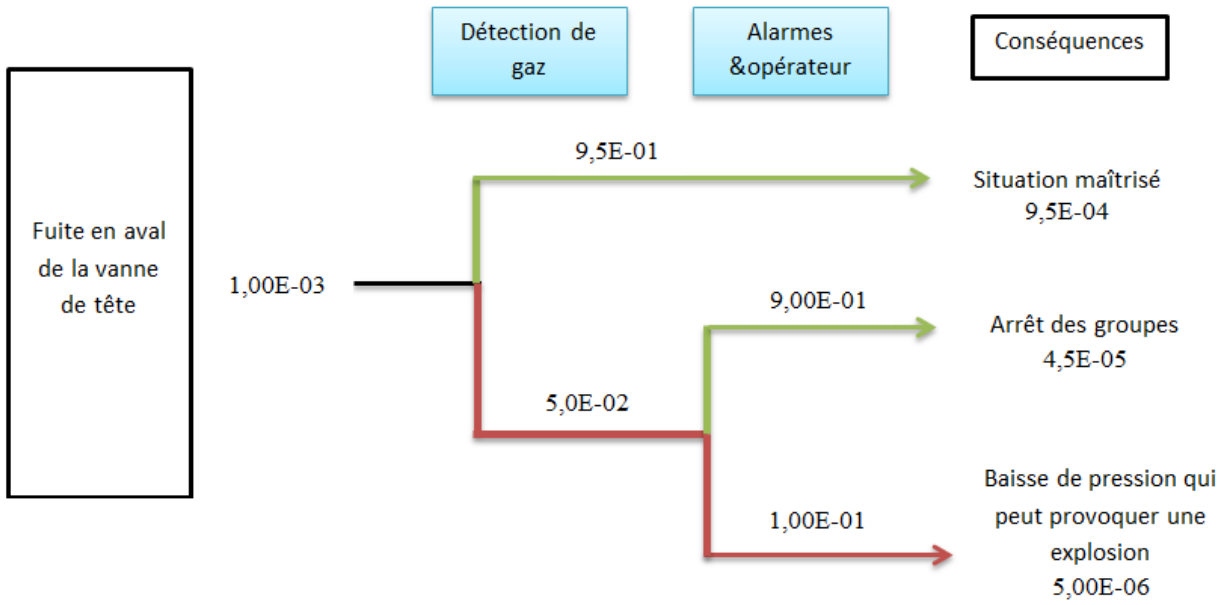
$$f^C = f^{IE} \times \prod_i PFD^i_{moy}$$

Le choix de PFD se réfère au mode de fonctionnement à faible sollicitation.

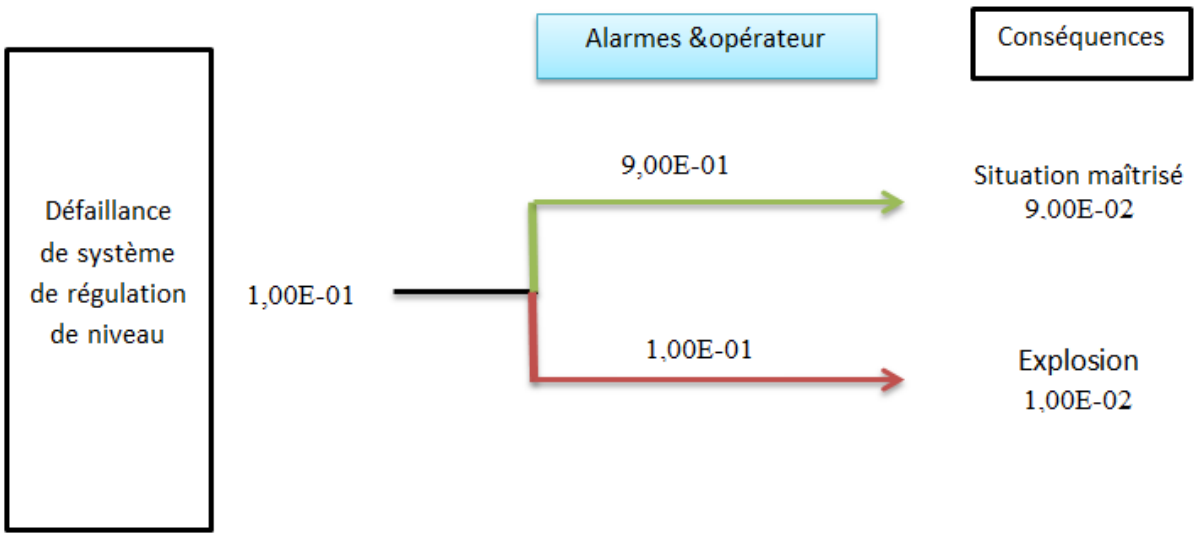
Arbre des évènements pour le scénario N°1 :



Arbre des évènements pour le scénario N°2 :



Arbre des évènements pour le scénario N°3 :



8. Détermination du SIL requis et PFD du SIS

Pour le scénario N°1 :

La défaillance d'un régulateur externe de pression peut engendrer une haute pression en amont de la vanne FSV 100. Une soupape de sécurité installée en dessus du séparateur primaire évacue la surpression. Si la pression atteint 77 bars, le pressostat PSH 100 la détecte et l'alarme PAH se déclenche au niveau de la salle de commande/contrôle pour la fermeture à distance de la vanne de sécurité. Mais comme cette commande est défaillante, un opérateur procédera à la fermeture manuelle de cette vanne.

Les barrières de sécurité qui sont qualifiées IPL sont : alarmes &intervention humaines et soupape de sécurité.

En prenant le cas de l'échec de toutes les barrières en aura comme conséquence une explosion.

Calculant la fréquence de cette conséquence :

$f^{c}= f^{Ei}$* PFD (soupape)* PFD (alarme&opérateur) = 1,00E-04

Pour le scénario N°2 :

Un cisaillement d'une conduite de gaz en aval de la vanne FSV 100 provoque une fuite de gaz qui sera détecté par un détecteur de gaz. La chute de pression qui en résulte peut être mesurée par le pressostat PSL 100 et si la pression descend en dessous du seuil de 28 bars, l'alarme PAL 100 se déclenche au niveau de la salle de contrôle pour commander la fermeture de la vanne de sécurité FSV 100 mais comme celle-ci est défaillante, l'opérateur intervient pour la fermeture manuelle de cette vanne.

Les barrières de sécurité qui sont qualifiées IPL sont : détection de gaz et alarmes et intervention humaines.

En prenant le cas de l'échec de toutes les barrières de sécurité, on aura l'explosion comme conséquence.

Calculant la fréquence de l'explosion de ce scénario :

$f^{c}= F^{Ei}$* PFD (détection gaz)* PFD (alarme &opérateur) = 5,00E-06

- **Pour le scénario N°3 :**

La défaillance d'un régulateur de niveau des condensats peut provoquer une augmentation du niveau des condensats. Cette valeur est mesurée par le pressostat LSHH 100 et si le niveau dépasse le seuil de 500 mm, l'alarme LAHH 100 se déclenche au niveau de la salle de commande pour la fermeture à distance de la vanne de sécurité FSV 100 mais comme cette commande est défaillante, un opérateur procédera à la fermeture manuelle de cette vanne.

Les barrières de sécurité qui sont qualifiées IPL sont : alarmes et intervention humaines.

En prenant le cas de l'échec de toutes les barrières de sécurité, on aura l'explosion comme conséquence.

Calculant la fréquence de l'explosion de ce scénario :

$f^{c}= f^{Ei}$* PFD (alarme &opérateur) = 1,00E-02

- En faisant la somme de toutes les fréquences des conséquences pour les trois scénarios, on obtient : 1,01E-02.

La valeur tolérable de la fréquence pour le risque explosion est définie par : 1,00E-05

- Calculons PFD du SIS :

PFD (SIS) = 1,00E-05 / 1,01E-02

= 9,8E-04

Ce qui implique que : FRR = 1/PFD = 1/ 9,8E-04 = 1,02+03

A partir du tableau 2.1, La valeur de PFD appartient à l'intervalle $10^{-4} \leq$ PFD $\leq 10^{-3}$ d'où le SIL est de 3**.**

CONCLUSION

L’analyse et l’évaluation des risques par la méthode LOPA exige la disponibilité de certaines données et informations sur les différents paramètres d’évaluation des risques telles que, les scénarios d’accidents, les fréquences d’évènements initiateurs ainsi que les probabilités de défaillances des différentes couches de protections existantes. Afin d’aboutir à l’évaluation de ces scénarios, une grille d’évaluation est utilisée pour juger la criticité de ces scénarios.

Cette évaluation montre qu’un SIS doit être implémenté pour augmenter la performance des barrières de sécurité et donc éviter le risque d’explosion.

Le niveau de SIL requis pour le SIS afin d’amener le risque à un niveau jugé acceptable est de 3.

CHAPITRE 6

PROPOSITION DU SYSTEME D'ARRET D'URGENCE

INTRODUCTION

Le système ESD (Emergency Shut-Down system) ou SIS est appelé à répondre à des conditions sur le terrain qui peuvent être dangereuses ou, si aucune action n'a été prise, peut augmenter la situation dangereuse et engendrer des conséquences graves comme l'explosion.
Dans notre cas, la vanne de sécurité FSV 100 qui assure l'arrêt d'urgence en cas d'anomalie est défaillante depuis des années et sa réparation s'est avérée impossible, c'est pour cela que nous allons proposer un système automatique d'arrêt d'urgence à l'aide du logiciel TIA PORTAL, en réalisant le programme par le step7 puis la simulation par le Wincc.

Dans ce qui va suivre, le SIS sera évalué en utilisant les équations analytiques présentées dans la norme CEI 61508-6 version 2010 et en prenant les paramètres de fiabilités des bases de données, pour confirmer que le SIL trouvé correspond au SIL requis que nous avons déjà calculé.

1. Système d'arrêt d'urgence

Le système d'ESD (Emergency Shut Down), connu aussi sous le nom de SIS, consiste à assurer l'arrêt totale des trois groupes de la centrale ALSTHOM en cas de détection d'une anomalie ou d'autres conditions potentiellement dangereuses du procédé, afin de protéger le personnel, les équipements et l'environnement.
Le système d'ESD est un système complètement autonome qui est destiné uniquement à l'arrêt d'urgence.
Le système ESD intervient dans les cas suivants:

- Niveau très très haut des condensats :

Une fois le LSHH 100 arrive au seuil de 500 mm, L'alarme LAHH 100 se déclenche au niveau de la salle de contrôle pour donner l'ordre de fermeture de la vanne FSV 100 pour éviter le risque d'explosion.

- Pression du gaz naturel :

Les seuils bas et haut de pression de gaz sont des facteurs de déclenchement des alarmes PAH et PAL au niveau de la salle de commande pour donner l'ordre de fermeture de la vanne FSV 100.
PSH : 77 bars
PSL : 28 bars

- Différence de pression de gaz naturel:

Pour autoriser l'ouverture de la vanne FSV100, il faut que la différence de pression entre l'amont et l'aval de la vanne atteint la valeur de 0,5 bars, une fois le pressostat différentiel PDSL 100 détecte un $\Delta P = 0,5$ bars, l'alarme PDAL se déclenche au niveau de la salle de commande pour donner l'autorisation de l'alimentation de l'électrovanne pneumatique pour ouvrir la vanne.

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

A- Capteurs

Chaque facteur de déclenchement possède un seul capteur, ce dernier est destiné pour mesurer les paramètres du procédé (pression, niveau des condensats) puis envoyer les signaux vers l'unité de traitement. Ces capteurs sont représentés dans le tableau 4.2 du chapitre 4.

B- Unité de traitement

Nous allons remplacer la commande « logique combinatoire » par un « automate programmable ».

Les API (Automates Programmables Industriels) possèdent des circuits électroniques optimisés pour s'interfacer avec les entrées et les sorties physiques du système, les envois et réceptions de signaux se font très rapidement avec l'environnement. Avec de plus une exécution séquentielle cyclique sans modification de mémoire, ils permettent d'assurer un temps d'exécution minimal, respectant un déterminisme temporel et logique, garantissant un temps réel effectif (le système réagit forcément dans le délai fixé).

Nous allons choisir l'automate SIMATIC S7-317F-2 PN/DP dite CPU de sécurité, qui possède une architecture non redondante et qui peut aller jusqu'à SIL3. (Figure 6.1)

Figure 6.1: CPU S7-317F-2 PN/DP

Cet automate est utilisé dans les installations exigeantes en termes de sécurité. Il assure le pilotage de processus pour lesquels une coupure directe n'entraîne aucun risque pour l'homme ou l'environnement.

• Il satisfait aux exigences de sécurité jusqu'à SIL 3 selon CEI 61508 et PL e selon ISO 13849.1

• Les modules de périphérie de sécurité sont raccordables en configuration décentralisée via l'interface PROFINET (PROFI safe) et/ou via l'interface PROFI BUS DP (PROFI safe) intégrée.

• Les modules de périphérie de sécurité de l'ET 200M sont également raccordables en configuration centralisée.

• Possibilité d'utiliser les modules standards en configuration centralisée ou décentralisée pour des applications non sécuritaires.

Tous les produits SIMATIC ont des fonctions de diagnostic intégrées pour une plus grande disponibilité du système avec lequel un éventuel défaut peut être identifié à l'avance et éliminé.

C- Actionneur ou élément final

L'élément final est composé d'un pré-actionneur qui représente l'électrovanne qui commande l'actionneur, ce dernier est un vérin à simple effet, il ne travaille que dans un sens.

Comme la grande partie des problèmes rencontrés avec les systèmes d'arrêt d'urgence relève aux actionneurs, nous allons proposer la redondance de la vanne , ils seront donc 02 vannes en parallèles (tout ou rien) commandés par le PLC. En cas d'existence de facteur de déclenchement, on observe la fermeture d'une vanne (FSV1) pour couper l'alimentation de gaz, et en cas de défaillance de la FSV1, la FSV2 va la remplacer.

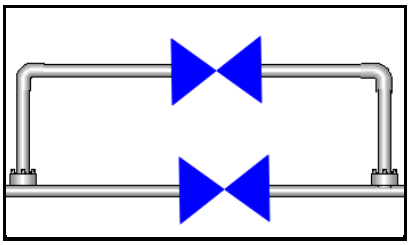


Figure 6. 2 : Architecture 1oo2 des vannes

2. Programmation de la partie commande

Les étapes de travail suivantes sont prévues :

- Création du programme
- Chargement du programme dans l'automate
- Création d'une vue IHM
- Test du programme

2. 1. Création du projet

Les étapes suivantes décrivent comment créer un nouveau projet. Les données et les programmes qui sont générés lors de la création d'une tâche d'automatisation sont stockés de manière ordonnée dans le projet.

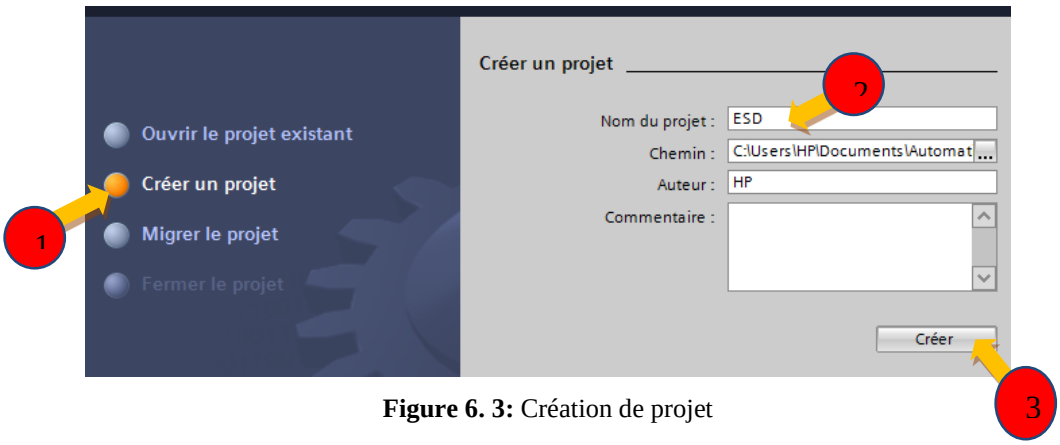


Figure 6. 3: Création de projet

2. 2. Insertion et configuration d'un automate

Les étapes suivantes décrivent comment insérer un automate par le biais de la vue du portail et comment ouvrir sa configuration dans la vue du projet. Le type d'automate que nous avons choisis est SIMATIC S7-300F, CPU S7-317F-2 PN/DP.

Figure 6. 4: Insertion et configuration d'un automate (1)

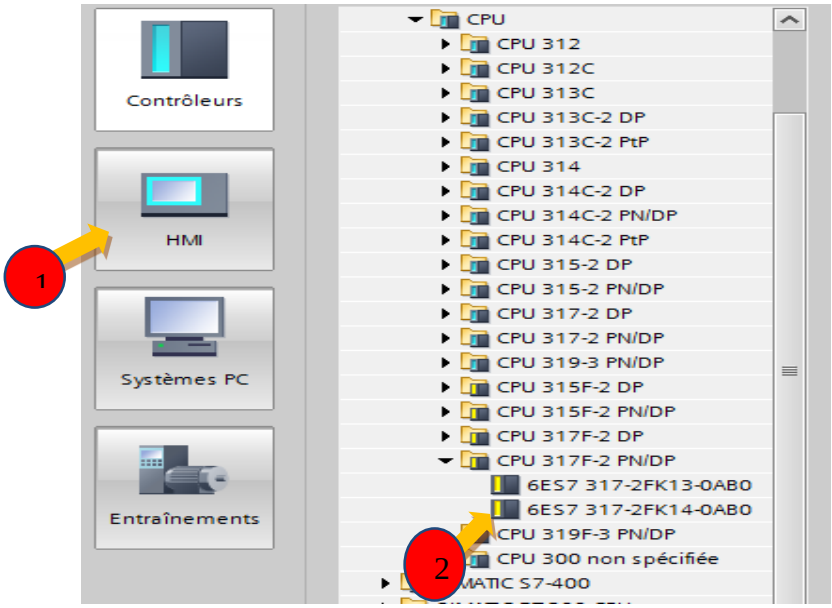


Figure 6. 5: Insertion et configuration d'un automate (2)

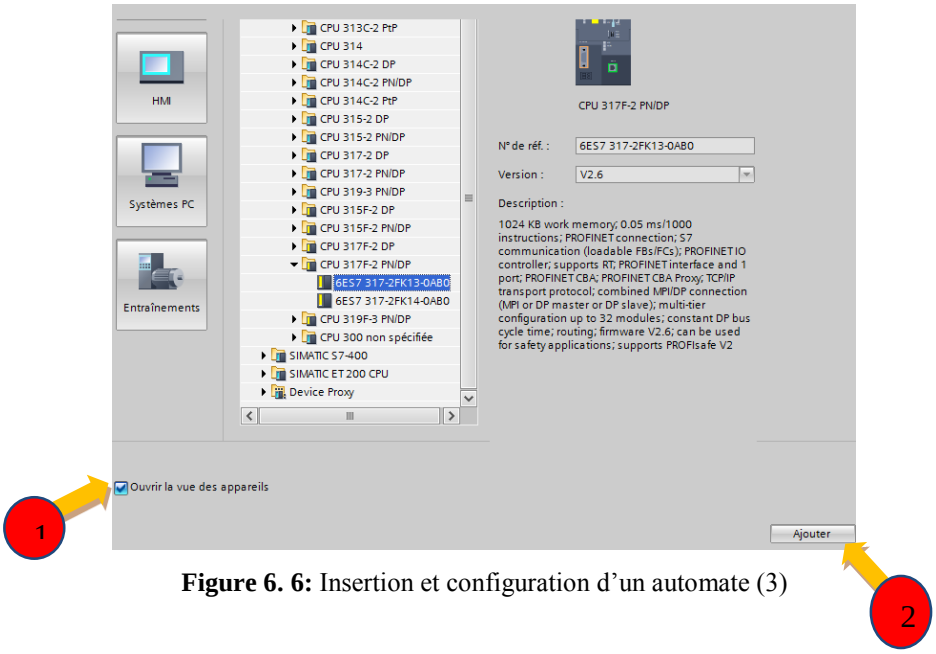


Figure 6. 6: Insertion et configuration d'un automate (3)

Donc, Nous avons créé un nouvel automate dans le projet et nous l'avons ouvert dans la vue des appareils de l'éditeur « Appareils et réseaux ».

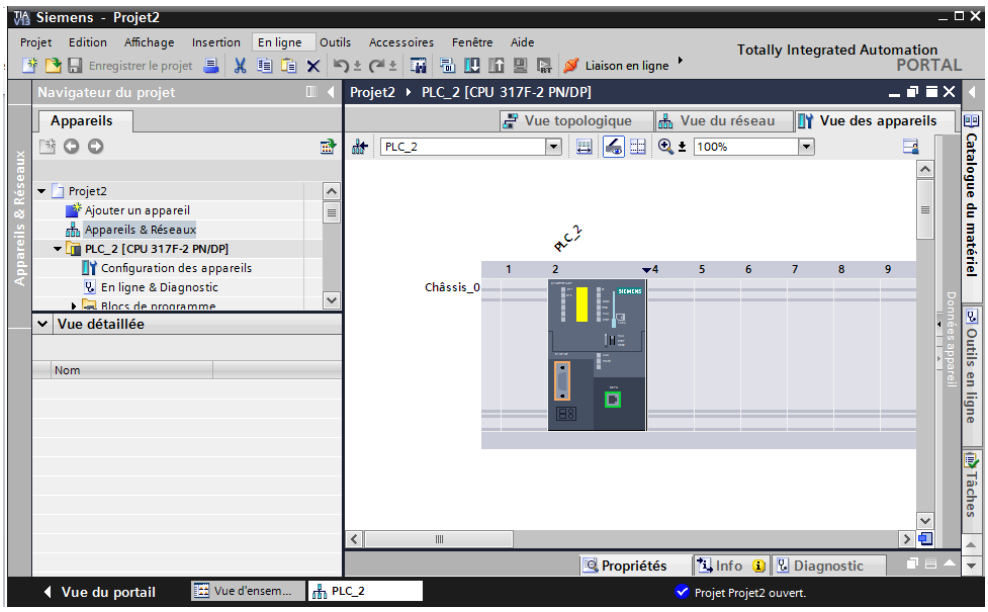


Figure 6. 7 : La vue des appareils de l'éditeur Appareils et réseaux.

2. 3. Présentation de l'éditeur d'appareils et de réseaux

L'éditeur d'appareils et de réseaux est l'environnement de développement intégré pour la configuration, le paramétrage et la mise en réseau des appareils et des modules. Il est composé d'une vue du réseau et d'une vue des appareils. Nous pouvons à tout moment basculer entre ces deux éditeurs.

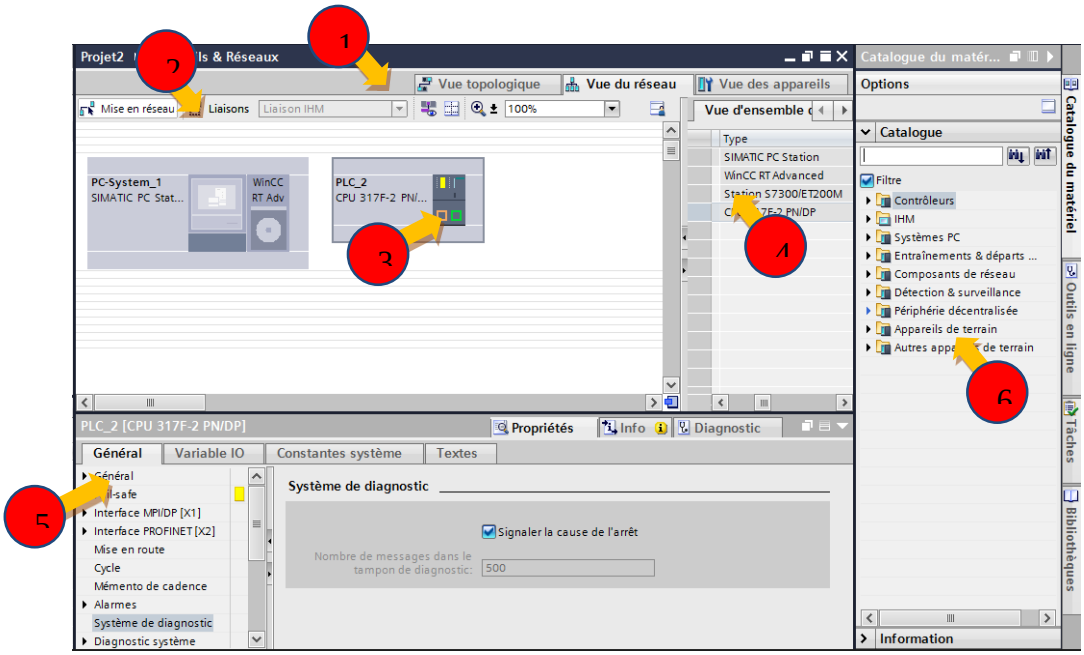


Figure 6. 8: La vue de réseau

① Onglets pour commuter entre la vue des appareils et la vue du réseau

② La barre d'outils contient les outils pour la mise en réseau graphique d'appareils, la configuration de liaisons et l'affichage des informations d'adresse. La fonction zoom permet de modifier la représentation dans la zone graphique.

③ La zone graphique permet d'afficher les appareils mis en réseau, les réseaux, les liaisons et relations. Des appareils du catalogue du matériel (7) peuvent être insérés dans la zone graphique et les interconnecter par le biais de leurs interfaces.

④ La zone tabellaire présente une vue d'ensemble des appareils, connexions et liaisons de communication utilisés.

⑤ La fenêtre d'inspection affiche les informations sur les objets actuellement sélectionnés. Dans l'onglet "Propriétés" de la fenêtre d'inspection.

⑥ Le catalogue du matériel permet d'accéder rapidement aux différents composants matériels. A partir du catalogue du matériel, les appareils et modules requis pour une tâche d'automatisation peuvent être glissés dans la zone graphique de la vue du réseau.

2. 4. Création de la table des variables

Une variable est une grandeur utilisée dans le programme et pouvant prendre différentes valeurs. Les variables sont classées dans les catégories suivantes en fonction de leur domaine de validité :

- Variables locales: Les variables locales sont valables uniquement dans le bloc dans lequel elles ont été définies.
- Variables API: Les variables API sont valables dans tout l'automate.

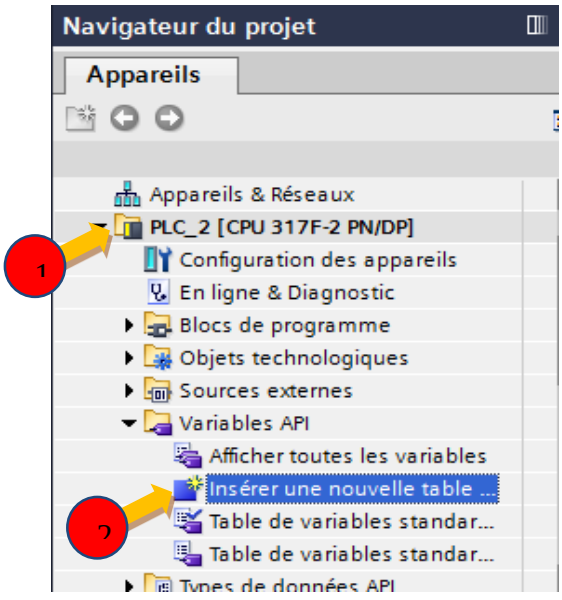
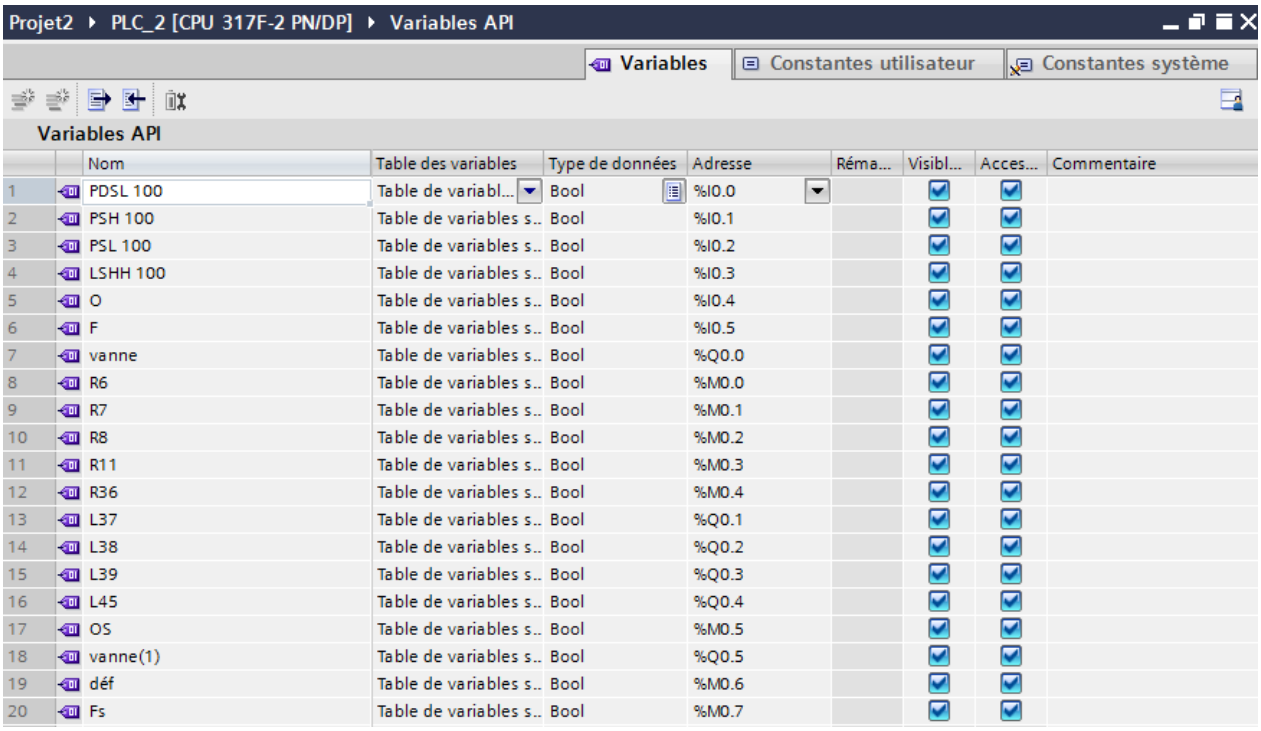


Figure 6. 9: Création de la table des variables

Après l'insertion de la table de variables, on la remplit de la manière suivante :



	Nom	Table des variables	Type de données	Adresse	Réma...	Visibl...	Acces...	Commentaire
1	PDSL 100	Table de variabl...	Bool	%I0.0		☑	☑	
2	PSH 100	Table de variables s..	Bool	%I0.1		☑	☑	
3	PSL 100	Table de variables s..	Bool	%I0.2		☑	☑	
4	LSHH 100	Table de variables s..	Bool	%I0.3		☑	☑	
5	O	Table de variables s..	Bool	%I0.4		☑	☑	
6	F	Table de variables s..	Bool	%I0.5		☑	☑	
7	vanne	Table de variables s..	Bool	%Q0.0		☑	☑	
8	R6	Table de variables s..	Bool	%M0.0		☑	☑	
9	R7	Table de variables s..	Bool	%M0.1		☑	☑	
10	R8	Table de variables s..	Bool	%M0.2		☑	☑	
11	R11	Table de variables s..	Bool	%M0.3		☑	☑	
12	R36	Table de variables s..	Bool	%M0.4		☑	☑	
13	L37	Table de variables s..	Bool	%Q0.1		☑	☑	
14	L38	Table de variables s..	Bool	%Q0.2		☑	☑	
15	L39	Table de variables s..	Bool	%Q0.3		☑	☑	
16	L45	Table de variables s..	Bool	%Q0.4		☑	☑	
17	OS	Table de variables s..	Bool	%M0.5		☑	☑	
18	vanne(1)	Table de variables s..	Bool	%Q0.5		☑	☑	
19	déf	Table de variables s..	Bool	%M0.6		☑	☑	
20	Fs	Table de variables s..	Bool	%M0.7		☑	☑	

Figure 6. 10: table des variables

2. 5. Création d'un bloc d'organisation

Les étapes suivantes décrivent comment ouvrir le bloc d'organisation dans l'éditeur de programme. L'éditeur de programme est l'environnement de développement intégré pour la création du programme.

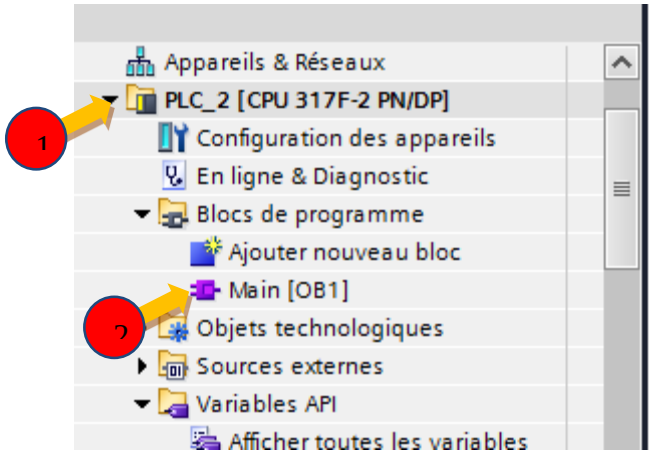


Figure 6. 11 : l'ouverture d'un bloc d'organisation

Nous avons ouvert le bloc d'organisation "Main [OB1]" dans l'éditeur afin de créer notre programme.

➢ Présentation de l'éditeur de programme :

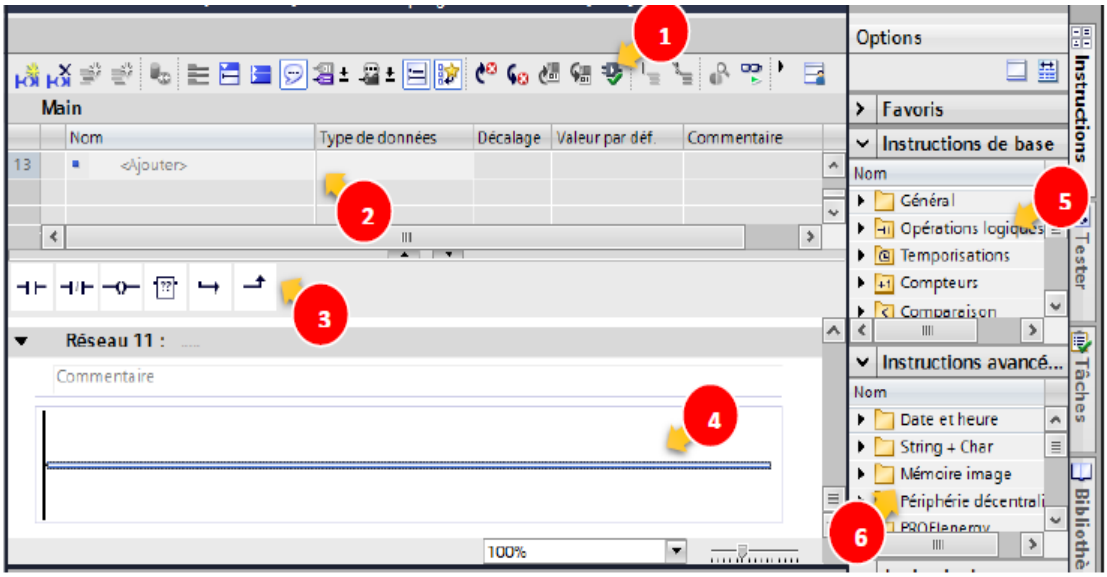


Figure 6. 12: Présentation de l'éditeur de programme

① La barre d'outils permet d'accéder rapidement aux principales fonctions de l'éditeur de programme, par exemple :

- Ajouter, supprimer, agrandir et réduire des réseaux
- Afficher et masquer les opérandes absolus
- Afficher et masquer les commentaires de réseau
- Afficher et masquer les favoris
- Afficher et masquer l'état du programme

② L'interface de bloc sert à créer et à gérer les variables locales.

③ Palette "Favoris" dans la Task Card "Instructions" et Favoris dans l'éditeur de programme.

Les favoris permettent un accès rapide aux instructions souvent utilisées.

④ La fenêtre d'instructions est la zone de travail de l'éditeur de programme. Les tâches suivantes peuvent être exécutées:

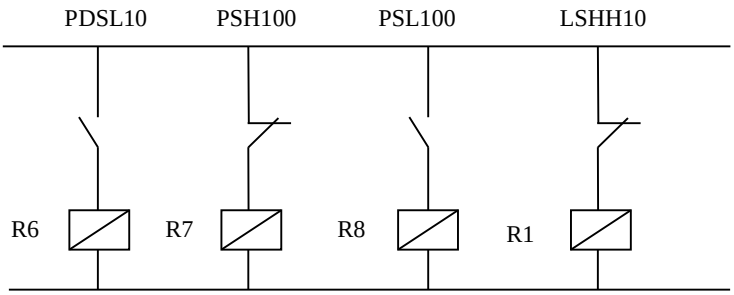
- Créer et gérer des réseaux
- Saisir les titres et commentaires du bloc et des réseaux
- Insérer des instructions et leur affecter des variables

⑤ Palette "Instructions" dans la TaskCard "Instructions"

- A partir des schémas électriques de commande de la vanne FSV 100 présentés dans l'annexe B, nous avons pu faire notre programme en utilisant le langage LADDER.

- D'abord, on représente les schémas nécessaires pour essayer de comprendre la logique de fonctionnement des capteurs :

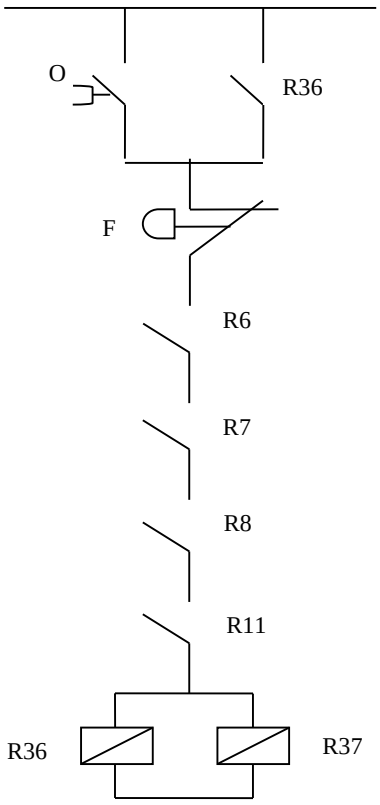
1- Schéma de principe du fonctionnement des capteurs :



Avec :

- R6, R7, R8 et R11 sont des bobines.

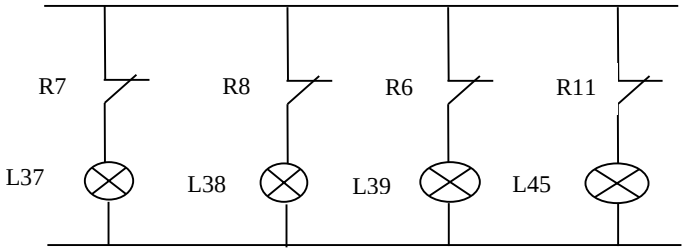
2- Schéma de principe d'ouverture et de fermeture de la vanne :



Avec :

- O : bouton poussoir d'ouverture.
- F : bouton poussoir de fermeture.
- R36 : bobine d'auto alimentation.
- R37 : bobine.
- Fs et Os : des mnémoniques.

3- Schéma de principe des alarmes qui sont représentées par des LEDs :



Avec

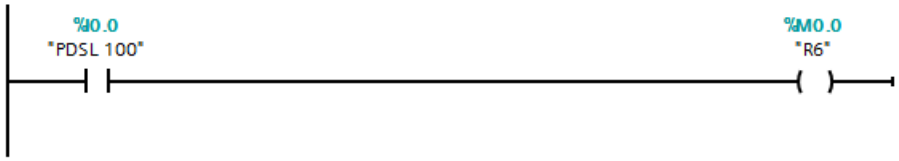
- On déduit les résultats suivants :

Tableau 6. 1 : Principe du système de commande de la vanne

Vanne ouverte : R37 = 1		Vanne fermée : R37 = 0	
LSHH = 0	R11 = 1	LSHH = 1	R11 = 0
PDSL =1	R6 = 1	PDSL =0	R6 = 0
PSH = 0	R7 = 1	PSH = 1	R7 = 0
PSL = 1	R8 = 1	PSL = 0	R8 = 0
O = 1		O = 0	
F = 0		F = 1	
R36 = 1		R36 = 0	

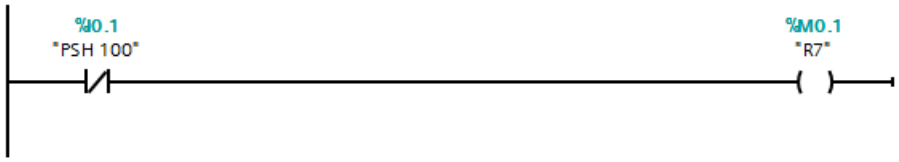
Réseau 1 : .....

Commentaire



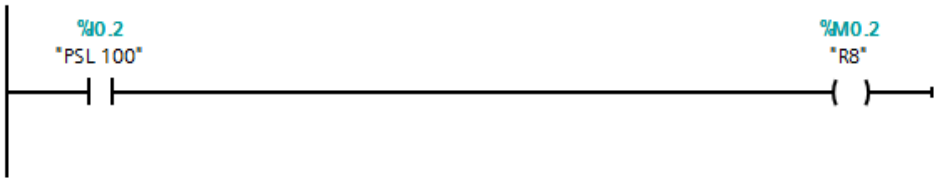
Réseau 2 : .....

Commentaire



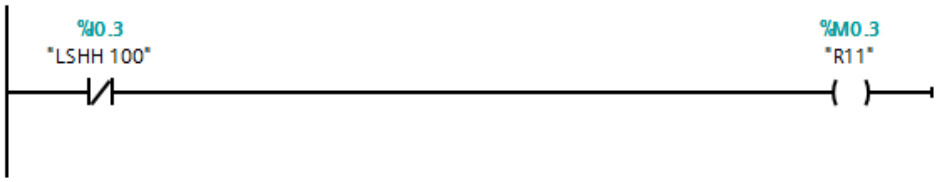
Réseau 3 : .....

Commentaire



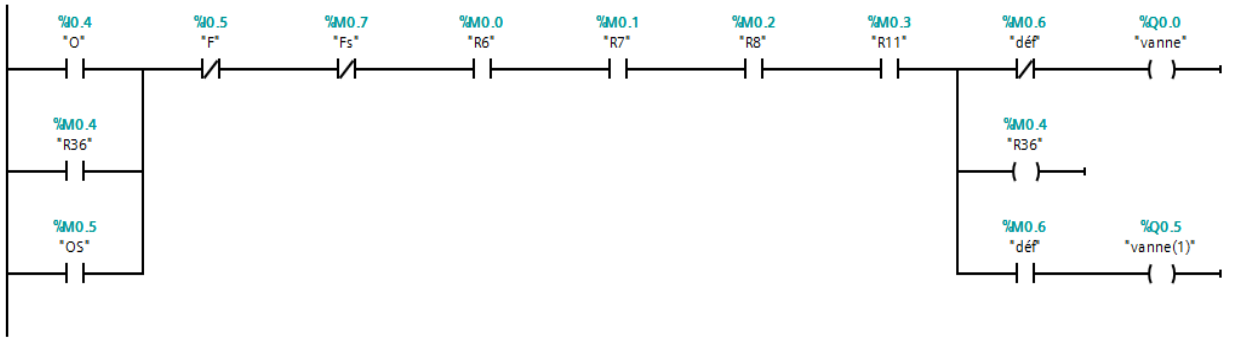
Réseau 4 : .....

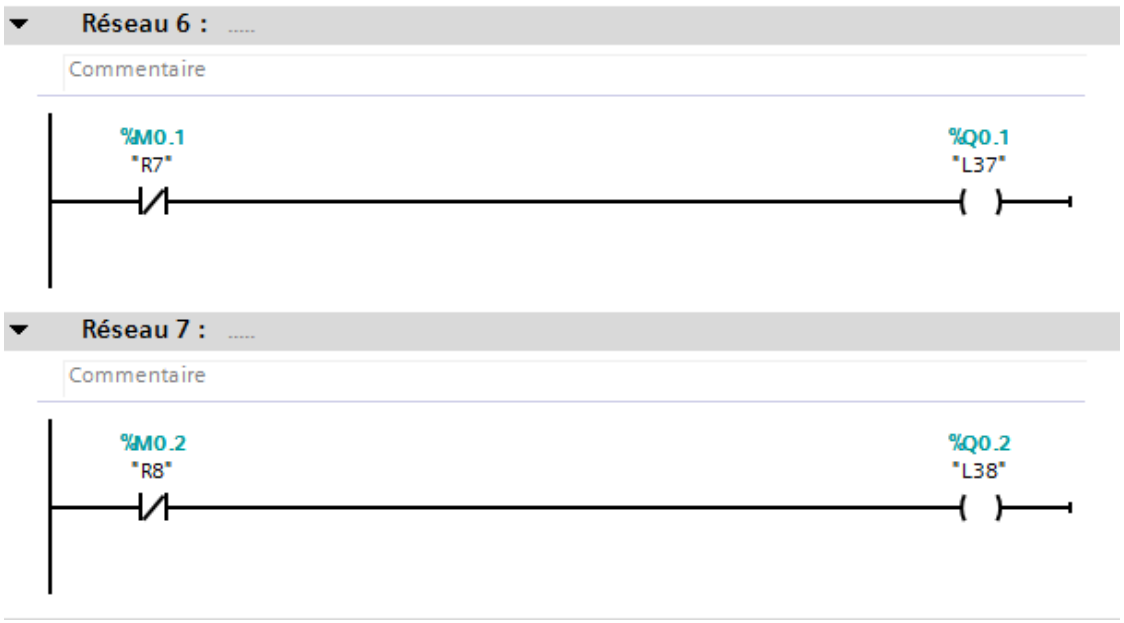
Commentaire

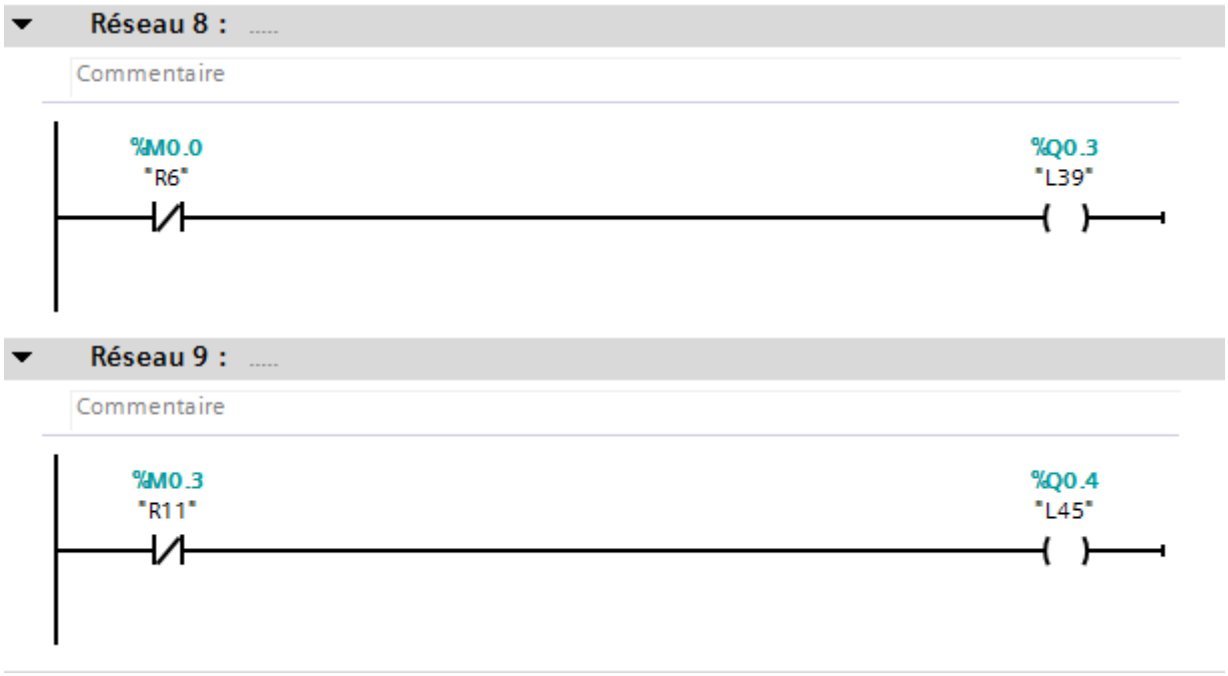


Réseau 5 : .....

Commentaire







2. 6. Création d'une interface IHM

Un système IHM constitue l'interface entre l'utilisateur et le processus. Le processus est piloté par l'automate. L'utilisateur peut visualiser le processus ou intervenir dans le processus en cours par le biais d'un pupitre opérateur.

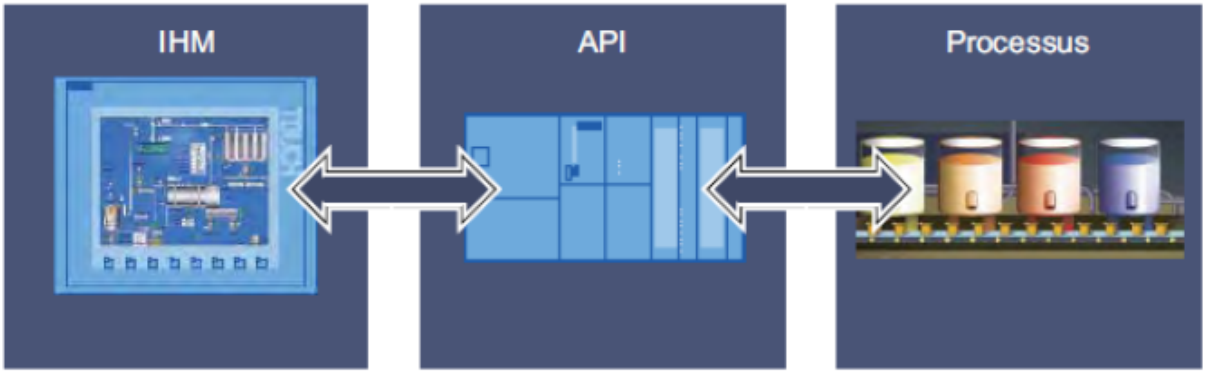


Figure 6. 13: « IHM » l'interface entre l'utilisateur et le processus

2. 6. 1. Création d'un pupitre opérateur avec une vue IHM

Afin d'ajouter un pupitre opérateur, nous avons procédé comme suit:

1. l'insertion d'un nouvel appareil par le biais du navigateur du projet.
2. L'ajout d'une station PC.

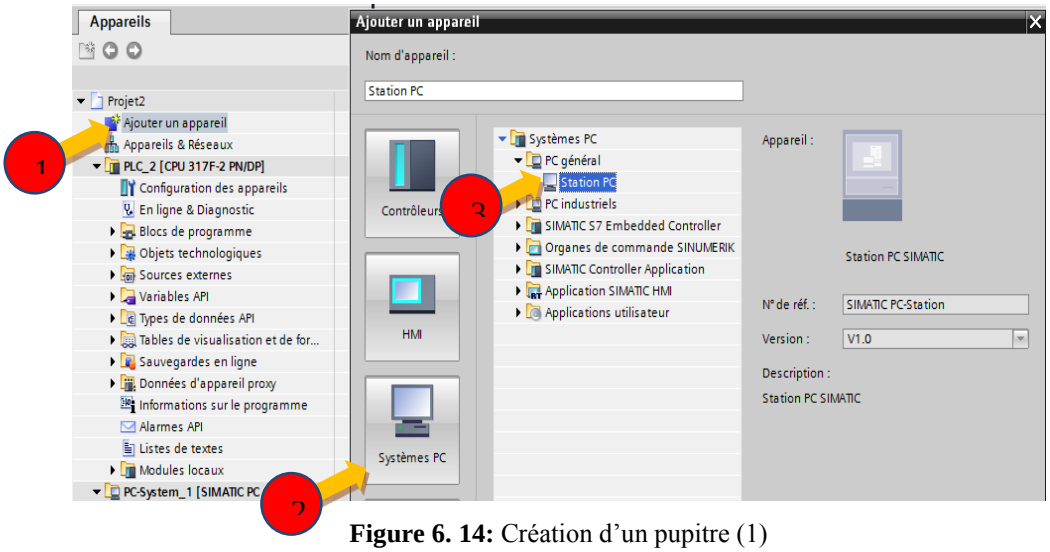


Figure 6. 14: Création d'un pupitre (1)

3. L'ajout du « WinCCRT Advanced » dans la station PC.

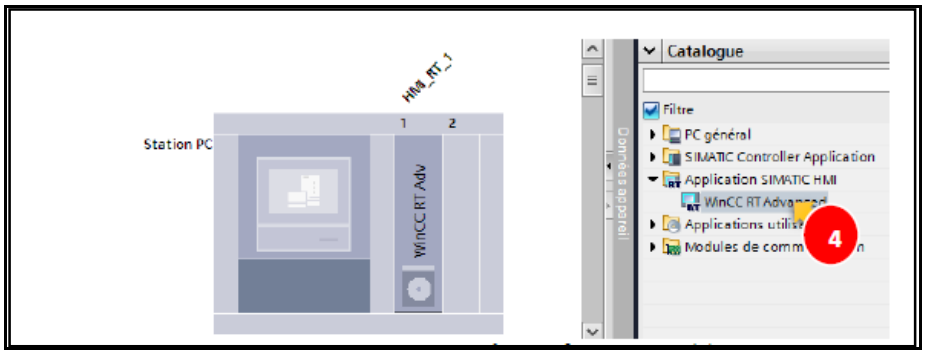


Figure 6. 15: Création d'un pupitre (2)

- Après avoir créé le pupitre, on ajoute maintenant les vues, on clique sur station pc puis HMI_RT puis ajouter une vue.

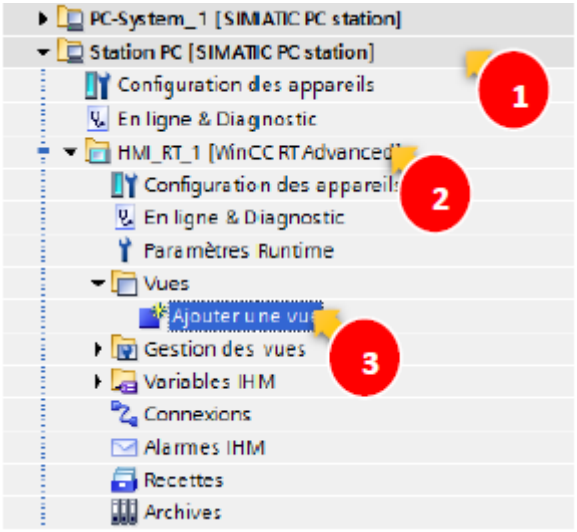


Figure 6. 16: Création d'un pupitre (3)

2. 6. 2. Création d'une connexion entre la station PC et l'automate S7-317F-2

Pour établir une connexion entre la station PC qui inclut le « HMI_RT » et l'automate, on procède comme suite:

1- On ouvre l'éditeur de configuration de connexions en appuyant sur « connexion » :

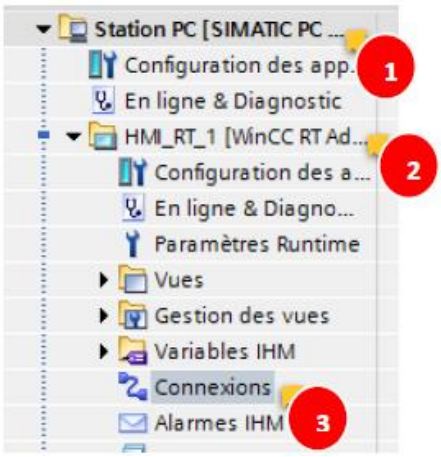


Figure 6. 17 : La connexion entre la station PC et l'automate S7-300F

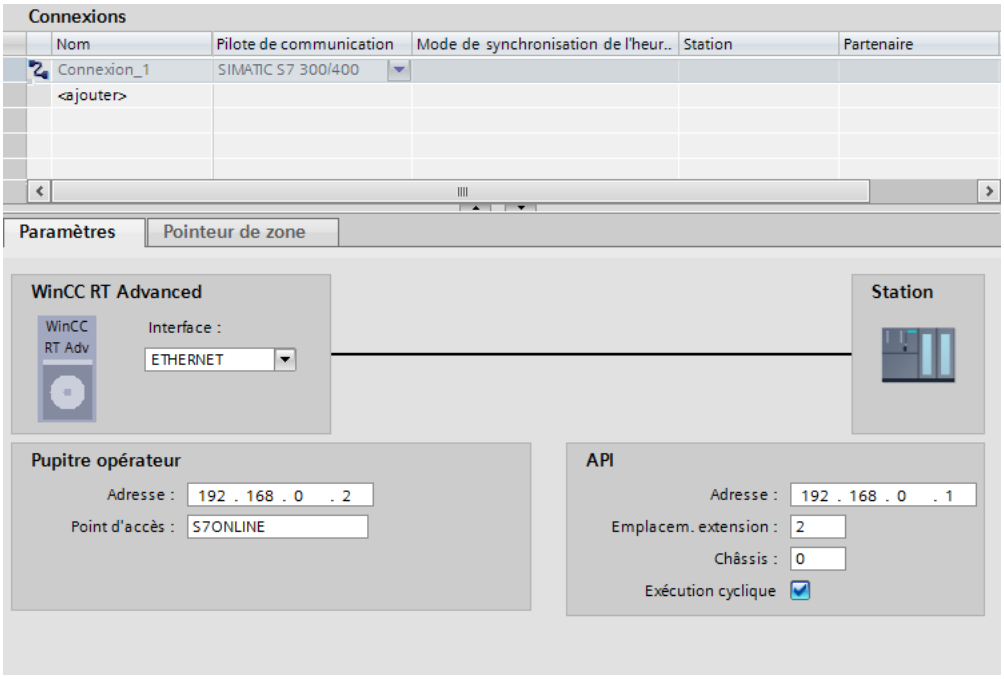


Figure 6. 18: la configuration de la connexion

2- Et maintenant chaque fois qu'une variable API est utilisé dans WinCC, on va lui associe une variable équivalente connecté avec la connexion précédemment configuré.

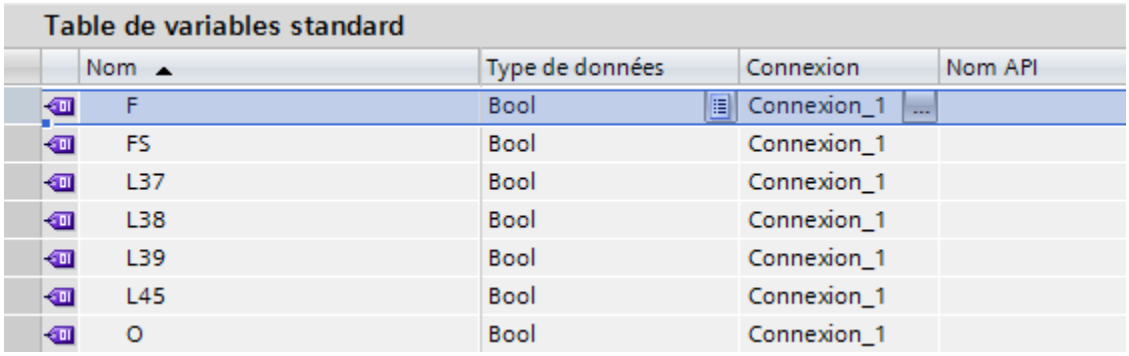


Figure 6. 19: la configuration de la connexion

2. 7. La vue de la supervision

Dans cette partie nous présenterons la vue crée pour la visualisation et la commande du système.

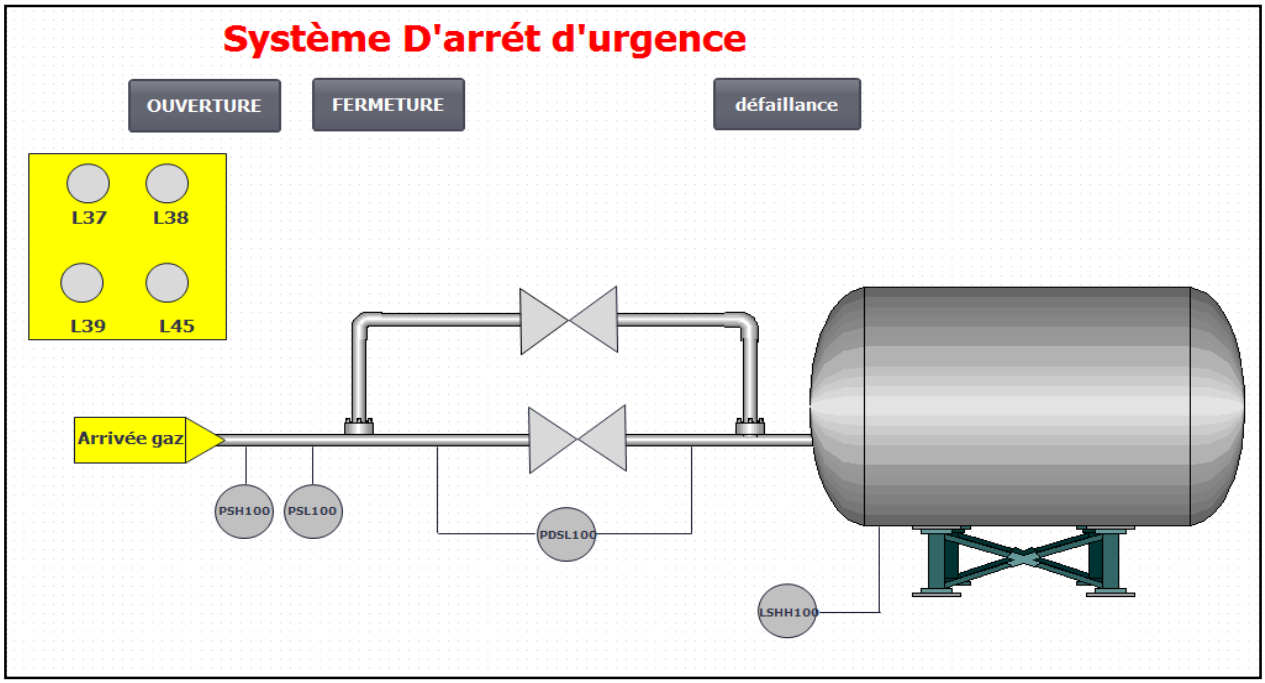


Figure 6. 20: La vue du système ESD

2. 8. La simulation « PLCSIM » et « WINCCRT »

Pour lancer la simulation avec le PLCSIM, on procède comme suite :

1. On compile le matériel et le logiciel.

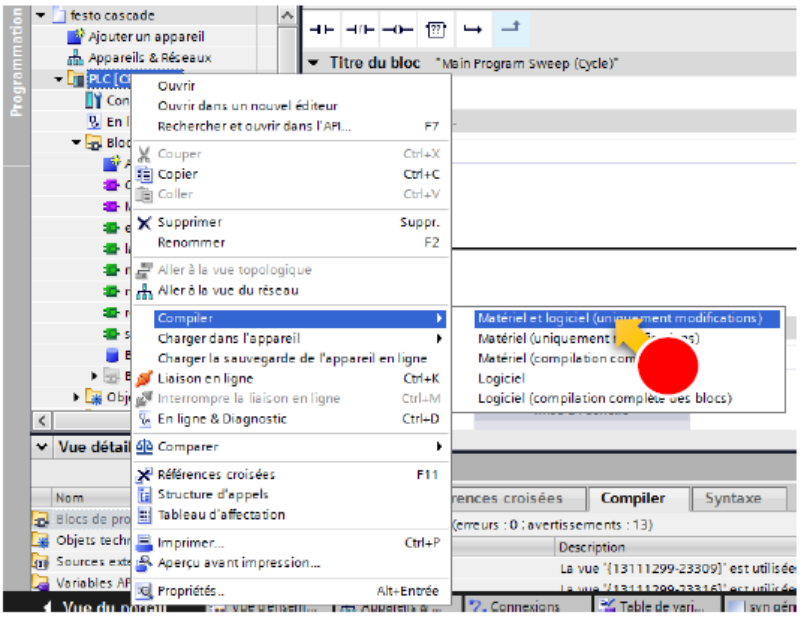


Figure 6. 21 : Compilation du programme

2. Après avoir compilé le programme, on lance la simulation en cliquant sur l'icône «démarrer la simulation» sur la barre d'outils :

Figure 6. 22: La simulation du programme

3. On charge le programme dans l'automate:

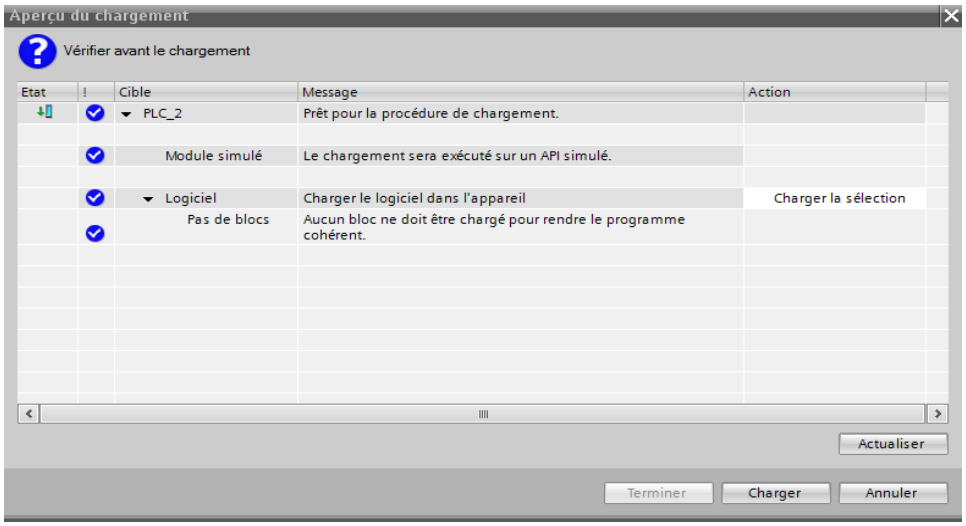


Figure 6. 23: Chargement du programme

4. Et le simulateur « PLCSIM » se lance

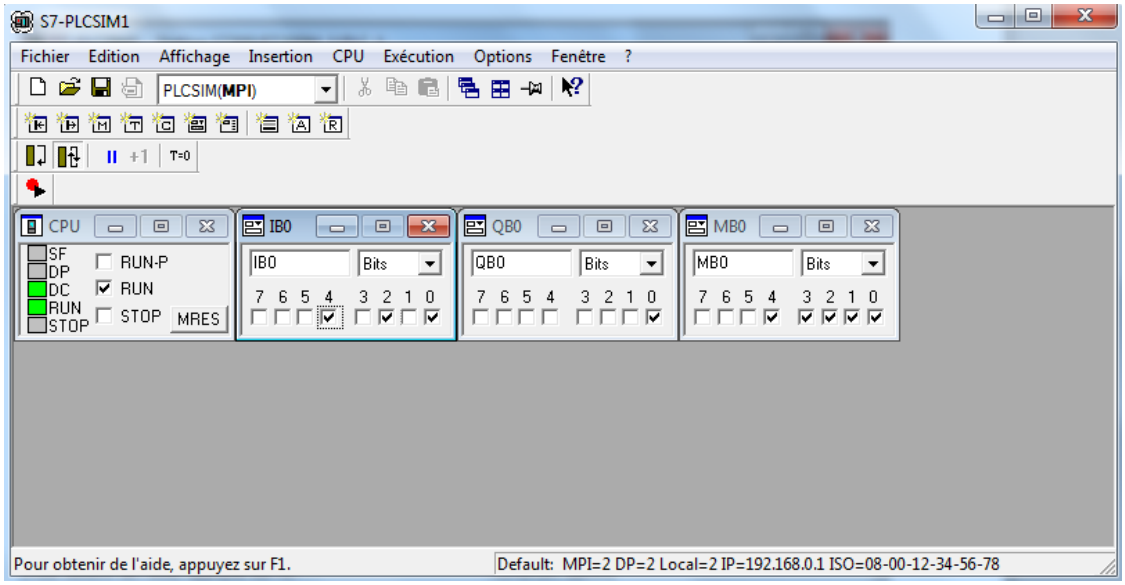


Figure 6. 24 : Lancement de la simulation

- Et pour lancer la simulation de la supervision, on clique sur l'icône de la barre d'outils suivante :

Figure 6. 25 : La simulation WinCCRT

Et le simulateur « WinCC RT » se lance :

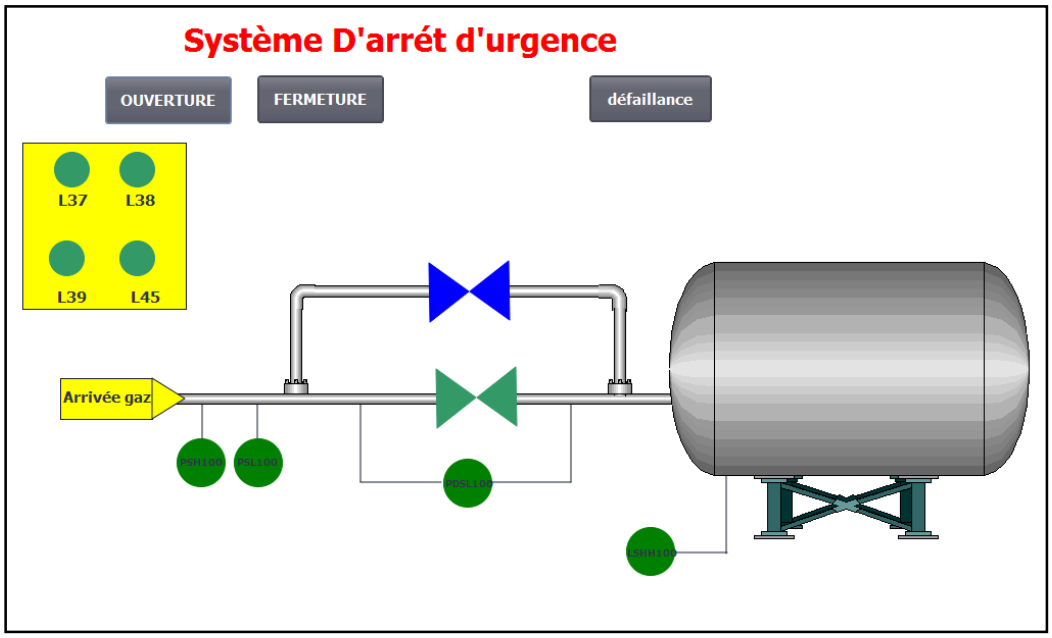


Figure 6. 26 : Vanne FSV 1 ouverte (fonctionnement normale)

- Nous avons choisis la couleur verte de la vanne pour l'ouverture (fonctionnement normale) et la couleur bleu pour la fermeture en cas de d'une anomalie.
- Pour les capteurs (PSH 100 , PSL 100 , PDSL 100, LSHH 100) et les LEDs :

La couleur verte indique que la vanne est ouverte (pas d'anomalie).

La couleur rouge indique que le capteur atteint le seuil (détection d'anomalie) et la LED va se signaler dans la salle de commande (couleur rouge).

❖ Cas d'anomalie N°1 : le PSH 100 atteint le seuil de 77 bars, la vanne FSV 1 se ferme automatiquement (figure 6.27).

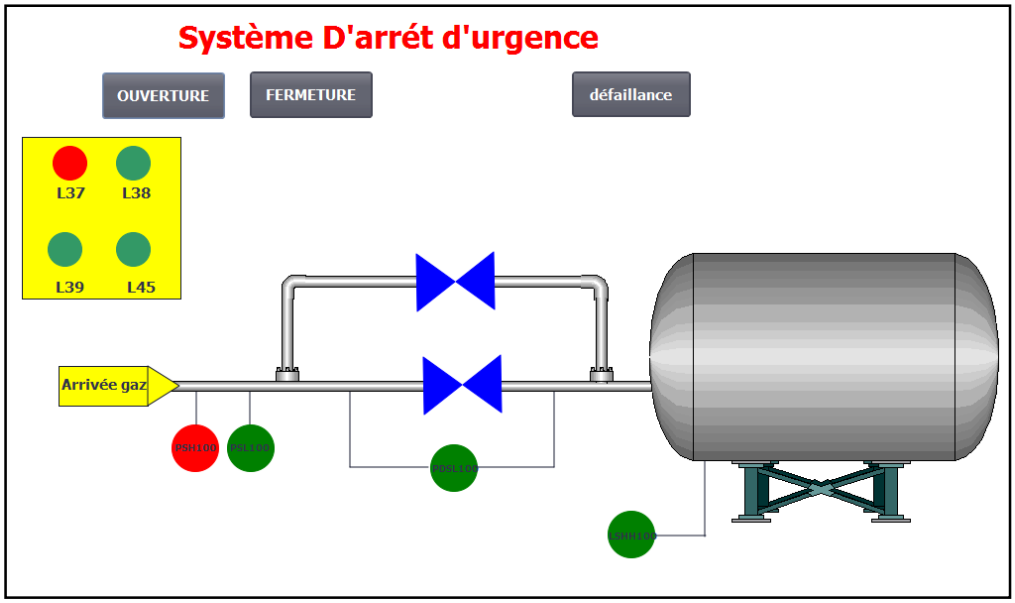


Figure 6. 27 : Fermeture automatique de FSV 1 suite au déclenchement du PAH 100

❖ Cas d'anomalie N°2: le PSL 100 atteint le seuil de 28 bars, la vanne FSV 1 se ferme automatiquement (figure 6.28).

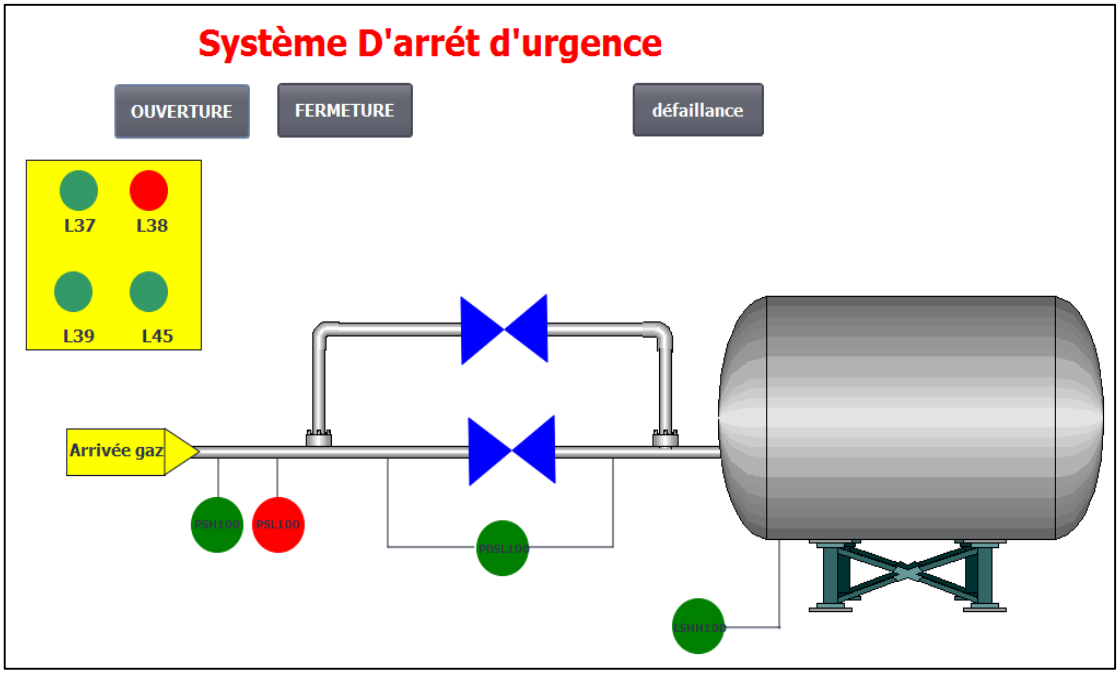


Figure 6. 28 : Fermeture automatique de FSV 1 suite au déclenchement du PAL100

❖ Cas d'anomalie N°3: le LSHH100 atteint le seuil de 500mm, la vanne FSV 1 se ferme automatiquement (figure 6.29).

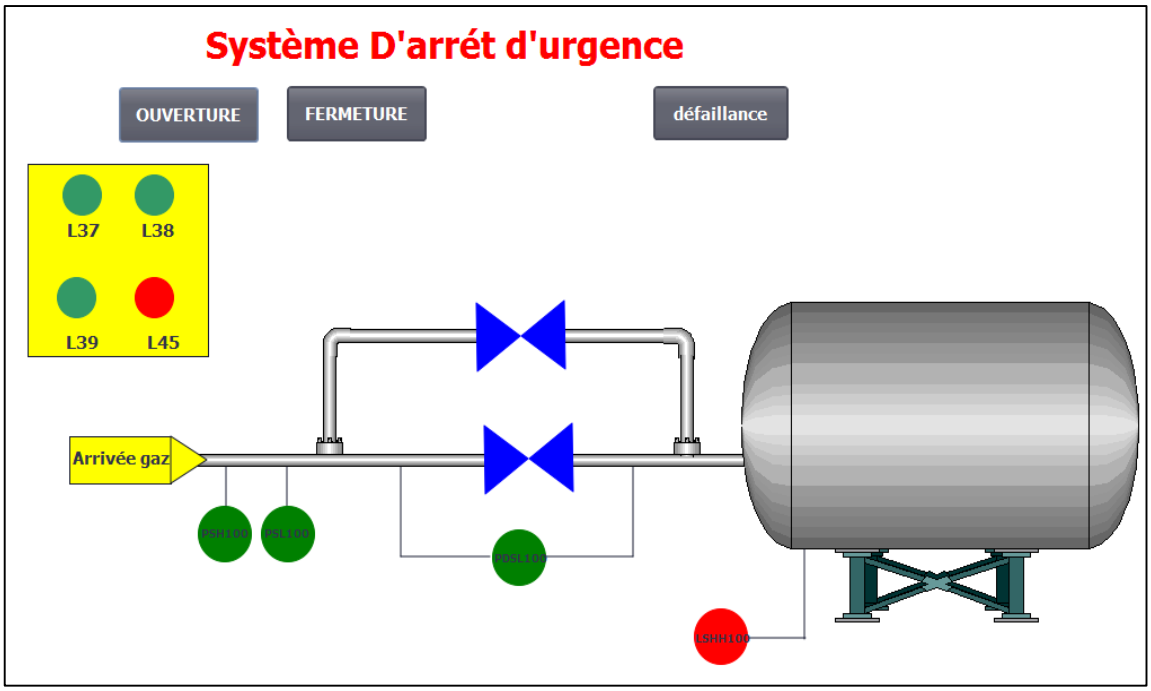


Figure 6. 29: Fermeture automatique de FSV 1 suite au déclenchement du LAHH100

❖ Cas d'anomalie N°4 : le LSHH100 atteint le seuil de 500 mm ainsi que le PSH 100 atteint le seuil de 77 bars au même temps, la vanne FSV 1 se ferme automatiquement (figure 6.30).

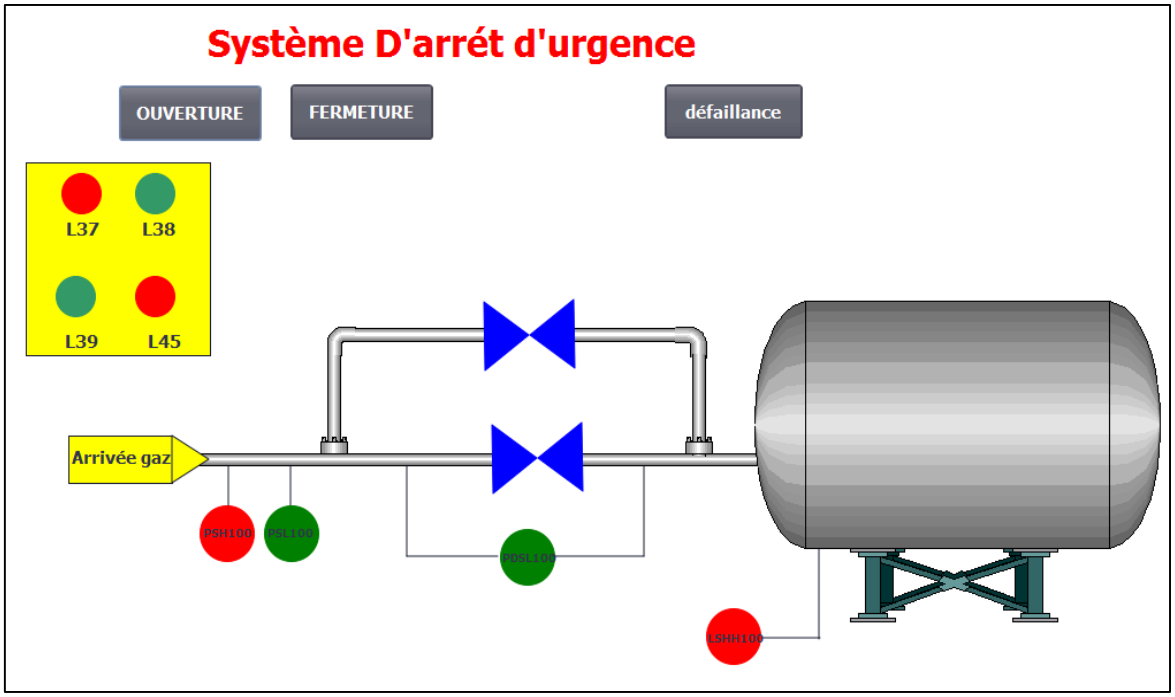


Figure 6. 30 : Fermeture automatique de FSV 1suite au déclenchement du LAHH100 et du PAH100

❖ Cas d'anomalie N°5 : le LSHH100 atteint le seuil de 500 mm ainsi que le PSL 100 atteint le seuil de 28 bars au même temps, la vanne FSV 1 se ferme automatiquement (figure 6.31).

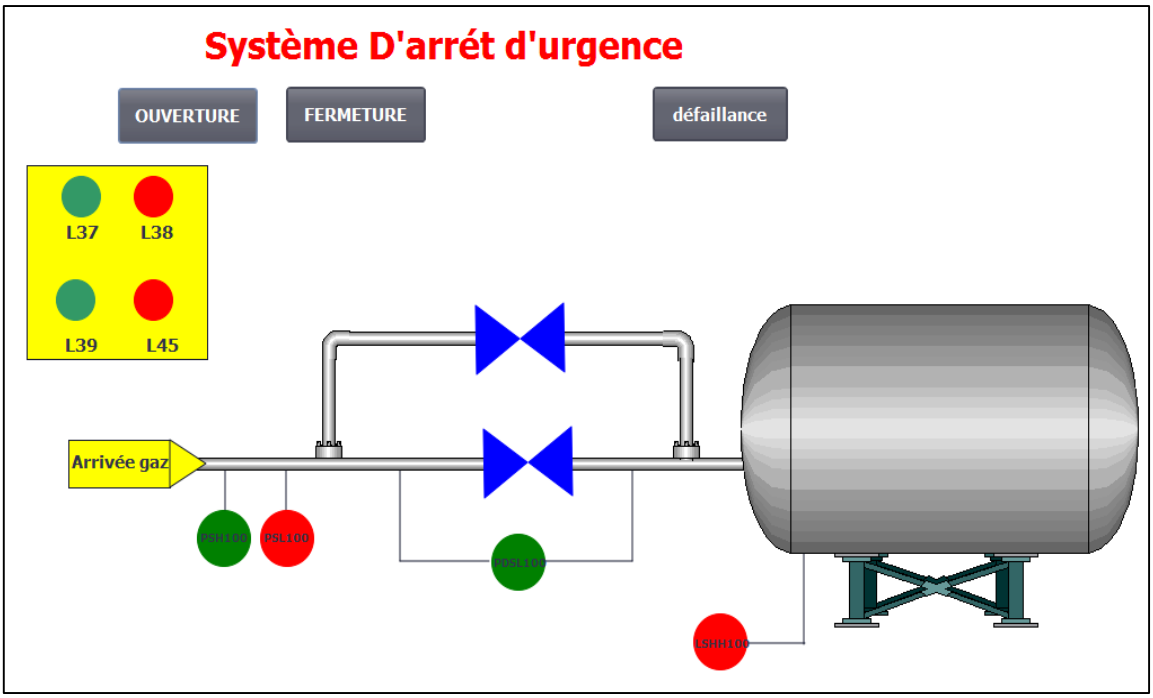


Figure 6. 31: Fermeture automatique de FSV 1 suite au déclenchement du LAHH100 et du PAL100

❖ Si le test de diagnostic détecte une défaillance de la vanne FSV1, la vanne FSV 2 va la remplacer (figure 6.32) et la vanne FSV1 doit être réparé.

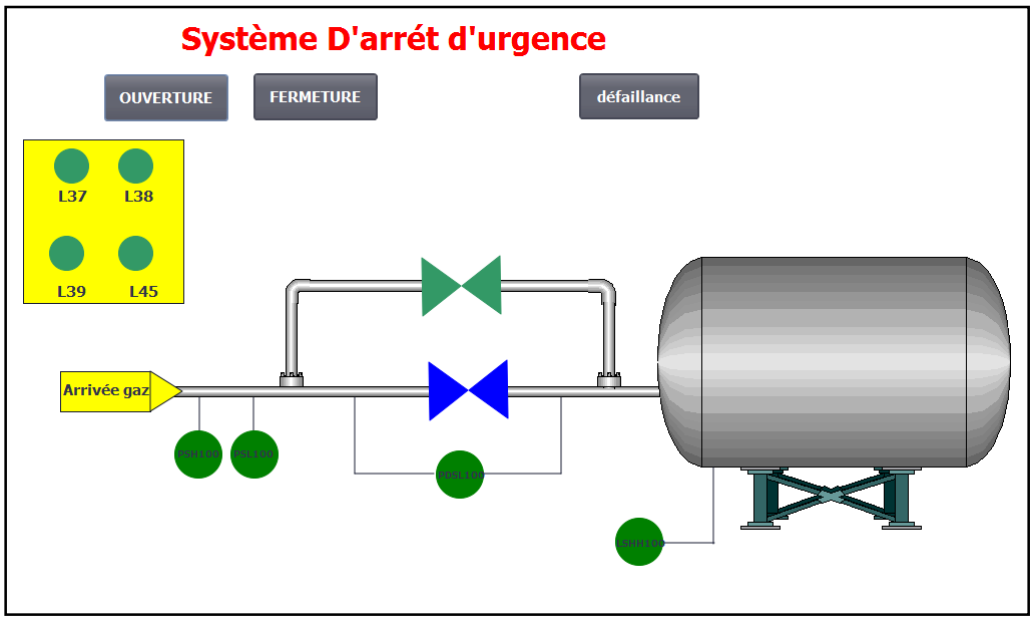


Figure 6. 32 : Vanne FSV 2 ouverte (fonctionnement normale, pas d'anomalie)

3. Evaluation du système (ESD)

A partir de l'analyse de risque faite précédemment, nous avons trouvé que le SIL exigé pour le SIS est de SIL 3.

Le SIL3 exige que la probabilité de défaillance totale à la demande PFD de la fonction de sécurité SIF du SIS doit appartenir à l'intervalle, $10^{-4} \leq \text{PFD} \leq 10^{-3}$

Ainsi : $\text{PFDc} + \text{PFD}_U + \text{PFD}_A \leq 10^{-3}$.

SIL 3 exige :

$\text{PFDc} + \text{PFD}_U + \text{PFD}_A \leq 10^{-3}$

En partant du fait que chaque élément de capteurs du sous-système capteurs peut déclencher le système d'arrêt, cette logique nous permet de représenter les capteurs de ce sous-système en parallèle, autrement dit, ils sont configurés sous l'architecture 1001, le sous-système de PLC que nous avons choisis, il est configuré sous l'architecture 1oo1, alors que pour les éléments du sous-système actionneur on propose de les configurés sous l'architecture 1002.

S1.1	S2.1	S3.1	S4.1
PSH 100	PSL 100	LSHH 100	PDSL 100

A1.1	A2.1
FSV 100	FSV 101

3. 1. Calcul du PFDmoy du SIS par les équations analytiques

Les différentes données nécessaires au calcul ont été tirées des banques de données [OREDA, 2002], [CCPS, 2002], [IEEE, 1984], et [PDS, 2004].

Par manque de données, nous n'avons pas pris en considération dans les différents calculs des probabilités de défaillance de cause commune (ßD=ß=0).

- Sachant que : T1 (intervalle entre tests) = 4380h,

Pour le Capteur de pression (1001) :λD= 5,55.E-6, MTTR= 5,3h

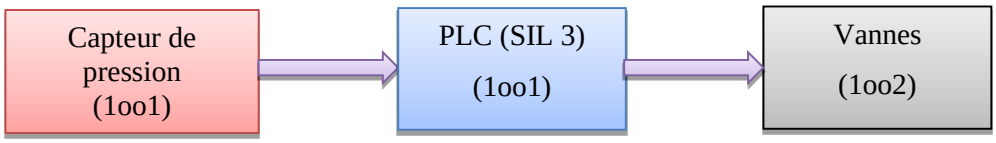
Pour le Capteur de niveau (1001) :λD= 24,7.E-6, MTTR= 11,4h

Et pour le PLC (2003) :λD= 1.E-10, MTTR= 10,2h

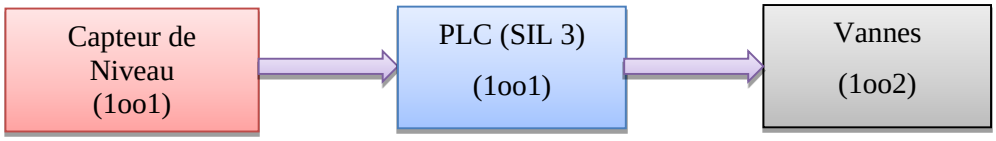
Et pour les vannes (1002) :λD= 90,84.E-6, MTTR= 14,4h

- Comme il y'a 3 capteurs de pressions et 1 capteur de niveau, nous présentons les deux schémas simplifiés du SIS pour les calculs que nous allons effectuer :

➢ Première cas (avec capteur de pression) :



➢ Deuxième cas (avec capteur de niveau) :



Nous utilisons le tableau 2.6 pour le calcul.

Tableau 6. 2 : Calcul du PFDmoy par les équations analytiques (Première cas)

	Capteur de pression (1oo1)	**PLC (1oo1)**	**Actionneur (1oo2)**	**SIS**	
	PFD	**PFD**	**PFD**	**PFD**	**SIL**
DC= 60 %	0,00489	8,86.E-8	8,79.E-3	1,36.E-2	1
DC= 90 %	0,00124	2,29.E-8	6,17.E-4	1,85.E-3	2
DC= 99 %	1,5.E-4	3,21.E-9	1,11.E-4	2,61.E-4	3

Tableau 6. 3 : Calcul du PFDmoy par les équations analytiques (Deuxième cas)

	Capteur de niveau (1001)	PLC (1oo1)	Actionneur(1oo2)	SIS	
	PFD	PFD	PFD	PFD	SIL
DC= 60 %	0,0219	8,86.E-8	8,79.E-3	3,06.E-2	1
DC= 90 %	5,69.E-3	2,29.E-8	6,17.E-4	6,3.E-3	2
DC= 99 %	8,22.E-4	3,21.E-9	1,11.E-4	9,33.E-4	3

- **Interprétation :**

Selon les résultats obtenus, le SIL du SIS est égale à 3 pour un taux de diagnostic DC=99% et pour les deux schémas du SIS, ce qui correspond au SIL requis déjà trouvé, d'où l'importance des tests de diagnostic avec un taux de couverture DC élevé pour la détection des défaillances dangereuses dans les capteurs, l'unité de traitement ou l'actionneur.

3. 2. Calcul du temps de réponse du SIS

Rappelons que le temps de réponse correspond à l'intervalle de temps entre le moment où le système d'arrêt d'urgence automatique, dans un contexte d'utilisation, est sollicité et le moment où la fonction de sécurité assurée par ce système est réalisée dans son intégralité. Ainsi le temps de réponse de ce système est égal au temps de réponse du sous-système de capteurs + le temps de réponse de l'automate + le temps de réponse du sous-système d'actionneurs.

Pour le sous-système de capteurs, on a pris un temps de réponse de 1ms pour chaque capteur et en prenant en compte le cas extrême c.à.d. le déclenchement de deux capteurs au même temps (Tableau 6.4).

Tableau 6. 4 : Temps de réponse des sous-systèmes

	Sous-système de capteurs	Unité de traitement	Sous-système d'actionneurs
Temps de réponse (ms)	2	$2{,}5.10^{-5}$	2.10^{3}

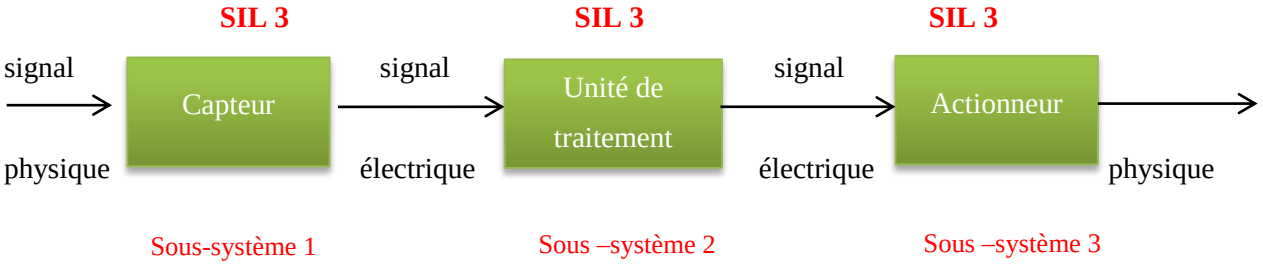
Temps de réponse (SIS) = $2 + 2{,}5.10^{-5} + 2.10^{3}$

Temps de réponse (SIS) = 2s

Le temps de réponse maximal du système est de **2s**.

3. 3. Prescription des contraintes architecturales

D'après la norme CEI 61511, le SIL3 exige que chaque sous – système doit remplir un de SIL 3 selon le schéma suivant :



En déterminant le type de chaque sous- système du SIS :

La norme CEI 61511 distingue deux types de systèmes : les unités logiques de l'Electronique Programmable (PE) et les autres sous-systèmes (par exemple capteurs, éléments terminaux et unités logiques non PE). Les unités logiques de l'Electronique Programmable (PE) sont rattachées aux systèmes de type complexe (type B) et les autres sous-systèmes sont rattachés aux systèmes de type simple (type A).

Tableau 6. 5 : Type des sous-systèmes

Sous système	Type A	Type B
Capteurs	×	
Unité de traitement		×
actionneurs	×	

On obtiendra les résultats suivants :

Tableau 6. 6 : Niveau d'intégrité de sécurité (SIL) maximal admissible pour une fonction de sécurité exécutée par un élément (ou sous-système) de « type A » (extrait de la norme CEI 61508 [IEC61508, 2010]).

SFF	Tolérance aux anomalies du matériel		
	0	**1**	**2**
< 60%	SIL1	SIL2	SIL3
60% - < 90%	SIL2	SIL3	SIL4
60% - < 99%	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4

Tableau 6. 7 : Niveau d'intégrité de sécurité (SIL) maximal admissible pour une fonction de sécurité exécutée par un élément (ou sous-système) de « type B » (extrait de la norme CEI 61508 [IEC61508, 2010]).

SFF	Tolérance aux anomalies du matériel		
	0	**1**	**2**
< 60%	Not allowed	SIL1	SIL2
60% - < 90%	SIL1	SIL2	SIL3
60% - < 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

A partir des tableaux ci-dessus et pour chaque sous-système de SIL 3 (types A et B), à chaque fois que la tolérance aux anomalies augmente, la proportion de défaillance en sécurité (SFF) diminue.

CONCLUSION

Nous avons pu voir à travers ce chapitre, l'application du logiciel TIA PORTAL pour l'élaboration d'une commande d'une vanne de sécurité ainsi que sa supervision par l'interface HMI (Interface Homme Machine)

Les résultats de la PFD calculé, nous amène à repérer le SIL réel du système étudié, en nous basant sur les plages des valeurs de la PFD associé aux SIL, suite à quoi, nous avons déterminé le SIL réel qui est SIL 3 pour un taux de diagnostic (DC) de 99%.

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

Par rapport aux résultats déclinés après l'étude sur le temps de réponse, nous pouvons affirmer que le SIS proposé répond à la fonction de sécurité pour laquelle il est conçu sur un temps de réponse raisonnable.

CONCLUSION GENERALE

Au terme de ce travail, nous nous proposons de résumer l'essentiel des résultats auxquels nous avons abouti et quelques perspectives de recherche.

Etant donné que le poste gaz est un point à haut risque, nous avons proposé une barrière plus performante et plus fiable consistant en un système d'arrêt d'urgence et ceci afin de maitriser le risque d'explosion et de maintenir l'installation en état de sécurité.

Le calcul du niveau d'intégrité de sécurité est nécessaire pour pouvoir proposer par la suite le SIS adéquat. Pour cela :
Dans une première étape, une partie théorique a consisté à rechercher une démarche globale de gestion des risques et les principales méthodes à appliquer suivie de la présentation des systèmes instrumentés de sécurité, des normes CEI 61508 et du niveau d'intégrité de sécurité.

Dans la deuxième partie, nous avons appliqué la méthode HAZOP pour choisir les scénarios les plus critiques et afin d'aboutir à l'évaluation de ces scénarios, une grille d'évaluation est utilisée pour juger la criticité des scénarios.
L'utilisation de la méthode LOPA nous a permis de trouver que le SIL requis est de 3.
Par la suite, nous avons proposé des architectures pour chaque sous-système du SIS et nous avons programmé la partie commande à l'aide du logiciel step7 suivi d'une simulation du système à l'aide du Wincc.

En dernier lieu, nous avons effectué une évaluation du système à l'aide d'équations analytiques de la norme CEI 61508 ce qui nous a permis de confirmer le SIL requis.

Les résultats de cette étude pourrait certainement servir de base à des études plus poussées, il serait important d'utiliser d'autres méthodes de sûreté de fonctionnement pour l'évaluation des performances des SIS, comme les réseaux de Pétri ou les chaines de Markov.
Une autre perspective intéressante est d'introduire le concept d'approche flou pour traiter l'incertitude des données.

BIBLIOGRAPHIE

[Ayault, 2005] N.Ayault. Evaluation des barrières techniques de sécurité. INERIS, février 2005.

[Beugin, 2006] Beugin, J. Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé. PhD thesis, Université de Valenciennes et du Hainaut-Cambrésis, France. (2006).

[Beugin, 2007] Beugin, J., Renaux, D., and Cauffriez, L. A sil quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems. Reliability Engineering and System Safety, 92:16861700. (2007).

[Bulletin Officiel, 2010],Bulletin Officiel, Circulaire du 10/05/10 récapitulant les règles méthodologiques applicables aux études de dangers, à l'appréciation de la démarche de réduction du risque à la source et aux plans de prévention des risques technologiques (PPRT) dans les installations classées en application de la loi du 30 juillet 2003, BO du MEEDDM n° 2010/12 du 10 juillet 2010, Paris.

[CCPS, 2001] Center for Chemical Process Safety, Layers of Protection Analysis: Simplified Process Risk Assessment, New York, 2001.

[CCPS, 2002] Offshore reliability data handbook, 4th Edition, 2002.

[Chanyang et al, 2008] Chunyang Wei,William J.Rogers,S.Sam Mannan,Layer of protection analysis for relative chemical risk assessment »,Journal of Hazardous Materiel,159,2008.

[Charpentier, 2002] Architecture d'automatisme en sécurité des machines, thèse pour l'obtention du grade de DOCTEUR de l'Institut National Polytechnique de Lorraine. Spécialité : Automatique, 10 Juillet 2002.

[Desroches et al, 2003] A. Desroches, A. Leroy, and F. Vallée. La gestion des risques : principes et pratiques. Lavoisier, France, 2003.

[DIN V 19250, 1994] Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, Berlin, Deutsches Institut für Normung.

[ECES, EN50402, 2005] ECES, EN 50402, Electrical apparatus for the detection and measurement of combustible or toxic gases vapours or of oxygen – Requirements on the functional safety of fixed gas detection systems, Geneva: European Committee for Electrotechnical Standardisation, 2005.

[Fal et Ldurka, 2000] E.Fal, J.Ldurka. Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de process industriels. INERIS, 2000

[Farmer, 1967] Farmer., F. R. ,Siting criteria : a new approach. Atom, chapter 128, page 152166, 1967.

[F.Innal, 2006] F. Innal, Y. Dutuit, A. Rauzy, J.P. Signoret, "An attempt to understand better and apply some recommendations of IEC 61508 standard," In: H. Langseth, G. Cojazzi (eds), p. 1-16, Proceedings of the 30th ESReDA seminar, Trondheim, Norway, June 7-8, 2006.

[Goble, 1998] Goble W.M. Control Systems Safety Evaluation & Reliability. 2nd Edition, 515 pages, ISA. Research Triangle Park, North Carolina 27709, USA.

[IEC 61508-5, 1998] Norme CEI 61508-5. Annexe B. Concepts d'ALARP et de risque Tolérable. International Electrotechnical Commission, Genève, Suisse.1998

[IEC61508, 1998] IEC61508, Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems. International Electrotechnical Commission (IEC), 1998.

[IEC61061, 1998] IEC61061. Stratifiés de bois densifiés, non imprégnés, à usages électriques. International Electrotechnical Commission (IEC), 1998.

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

[IEC61508, 2010] Functional safety of electrical / electronic / programmable electronic safety-related systems, 2nd edition, Geneva: International Electrotechnical Commission, 2010.

[IEC61511, 2000] IEC 61511, Functional safety – Safety instrumented systems for the process industry sector, 1st edition, Geneva: International Electrotechnical Commission, 2000.

[IEC 61508, 2002] Functional safety of electrical / electronic / programmable electronic safety-related systems, 1st edition, Geneva: International Electrotechnical Commission, 2002.

[IEC61508, 2009] Norme CEI 61508, nouvelle version. Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité. Parties 1 à 7, 2009. International Electrotechnical Commission, Genève, Suisse, 2009.

[IEC61511, 2004] IEC 61511, Functional safety – Safety instrumented systems for the process industry sector, 1st edition, Geneva: International Electrotechnical Commission, 2004.

[IEC62061, 2005] IEC 62061, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems, 1st edition, Geneva: International Electrotechnical Commission, 2005.

[IEEE, 1984] IEEE guide to the collection and presentation of electrical, electronic, sensing component, and mechanical equipement reliability data for nuclear-power generating station.IEEE-std-500, 1984.

[INERIS DRA 35, 2006] INERIS DRA-73, Méthode d'analyse de risques générés par une installation industrielle oméga-7, 2006.

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

[ISA, 1996] ANSI/ISA-84.01-1996, application of Safety Instrumented Systems for the Process Industries 1996

[ISA, 2004] ANSI/ISA-84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Research Triangle Park: International Society of Automation, 2004.

[ISO, 1999] Aspects liées à la sécurité : principes directeurs pour les inclure dans les normes , organisation internationale de normalisation ,1999

[ISO, 2002] ISO. Management du risque : Vocabulaire, Principes directeurs pour l'utilisation dans les normes. Organisation internationale de normalisation, 2002

[Jean-Paul Lacoursière, 2012] Jean-Paul Lacoursière, ing. Professeur associé Université de Sherbrooke , Pour une meilleure gestion de nos risques industriels!, Novembre 2012.

[J.P.Signoret, 2007] J.P. Signoret, "High Integrity Protection Systems (HIPS) – Making SIL Calculations Effective," Exploration and Production: The Oil and Gas Review, p. 14-17, 2007.

[Journal Officiel, 2005] Journal Officiel, Arrêté du 29/09/05 relatif à l'évaluation et à la prise en compte de la probabilité d'occurrence, de la cinétique, de l'intensité des effets et de la gravité des conséquences des accidents potentiels dans les études de dangers des installations classées soumises à autorisation, JOn°234du7octobre2005, Paris

[M.A Lundteigen, 2009] M.A. Lundteigen, M. Rausand, "Architectural constraints in IEC 61508: Do they have the intended effect?" Reliability Engineering & System Safety, vol. 94(2), p. 520-525, 2009.

[Mazouni, 2008] Mazouni, M.-H, Pour une Meilleure Approche du Management des Risques : De la modélisation Ontologique du Processus Accidentel au Système Interactif d'Aide à la décision. PhD thesis, Nancy Université, Institut Nationale Polytechnique de Lorraine, France, 2008.

[Michel ROYER, 2009] Michel ROYER , HAZOP une méthode d'analyse des risques , Référence SE4030 ,SE 4031, 10 avr. 2009.

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

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

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

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

[P.Jargot] P.JARGOT, « Langages de programmation pour API, Norme IEC 61131-3 », Technique de l'ingénieur, Vol. S 8 030

[Sellak, 2007] M.Sellak. Evaluation de parametres de sureté de fonctionnement en présence d'incertitudes et aide à la conception : application aux systemes instrumentés de sécurité.Ecole doctorale IAEM Lorraine, 19 octobre 2007.

[SIEMENS, 2009] SIEMENS , SIMATIC Portail TIA , Step7 Basic V10.5

[Slim Ben Saoud] Slim BEN SAOUD, LES AUTOMATES PROGRAMMABLES INDUSTRIELS (API) , chapitre 2.

[Smith et Simpson, 2004] D. J. Smith, K. G. L. Simpson. Functional Safety, a Straight forward guide to applying IEC 61508 and Related Standards. Second edition. Elsevier Butterworth Heinemann, 2004.

[Summers, 2000] A. Summers. Simplified methods and fault tree analysis- Viewpoint on ISA TR84.0.02. ISA Trans 2000;

[UKOOA, 2003] UK Offshore Operators Associations (UKOOA), , Fire and Explosion Guidance. Part 1: Avoidance and Mitigation of Explosions, October 2003.

[Villemeur, 1987] Villemeur A., 1987. Evaluation de la fiabilité, disponibilité et maintenabilité des systèmes réparables : La méthode de lEspace des Etats. Number 2. Eyrolles.

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

[Yves Mortureux , 2002] Yves MORTUREUX , Arbres de défaillance, des causes et d'événement - Arbre de défaillance , Référence SE4050 ,10 oct. 2002.

[Y.Langeron, 2007] Y. Langeron, A. Barros, A. Grall, C. Bérenguer, "Safe failure impact on safety instrumented systems," In: T. Aven, J. Vinnem (eds), vol. 1, p. 641-648, London: Taylor & Francis group, 2007, Proceedings of the European Safety and Reliability Conference, Stavenger, Norway, June 25-27, 2007.

[Y.Langeron, 2008] Y. Langeron, A. Barros, A. Grall, C. Bérenguer, "Combination of safety integrity levels (SILs): A study of IEC61508 merging rules," Journal of Loss Prevention in the Process Industries, vol. 21(4), p. 437-449, 2008.

ANNEXE A

ETUDE HAZOP

Skid N°2: Les filtres

Paramètre	Déviation	Causes	conséquences	Mesures existantes	recommandations
Débit	Pas de débit	-bouchage des filtres -rupture de la ligne d'alimentation des filtres	- arrêt de l'installation	- changement périodique des cartouches - filtre de secours -Détecteur de gaz -réseau anti-incendie	
	Faible débit	-Les fuites -défaillance des vannes -colmatage des filtres	-Epandage produit Déclenchement de l'alarme de la turbine	-évacuation automatique des condensats -indicateur de niveau -alarme du pressostat	
	Haut débit	-défaillance des vannes -augmentation de l'alimentation de gaz	Augmentation de pression	-Contrôle de débit (indicateur de niveau) -nettoyage des bougies magnétique	
Pression	Sous pression	-Rupture de la ligne alimentation. -les fuites	-Epandage de gaz inflammable.	- réseau anti-incendie -Contrôle du débit. - Détecteur de Gaz.	
	Surpression	-Augmentation de la T°. -Feu externe -vannes fermés	-Rupture de la ligne d'alimentation. - fuite dans les points fragiles	-soupapes de sécurité -réseau anti-incendie -indicateur de niveau et alarme de colmatage	

Suite

Skid N°2: Les filtres

Paramètre	Déviation	Causes	conséquences	Mesures existantes	recommandations
Température	Faible température	-climat	-baisse de pression	-Réchauffage après filtration -Ballon de méthanol	
	Haute température	climat	-Augmentation de la pression	-Des indicateurs de pression et de température -soupapes de sécurité	

Skid N°3 : Les détendeurs

Paramètre	Déviation	Causes	conséquences	Mesures existantes	recommandations
débit	Pas de débit	-Fermeture de la vanne - Bouchage au niveau des tuyauterai	-pas d'alimentation -arrêt des groupes	2 rampes de secours (1 automatique et 1 manuelle)	
	faible débit	-Les fuites de gaz -étanchéité des vannes	-Epandage de gaz. - baisse de pression	-Détecteur de GAZ. -compteur de gaz	
	Haut débit	-apport de l'alimentation élevé -ouverture intempestive de la vanne	- Augmentation de la pression	-compteur de gaz -clapet de sécurité	
Pression	Pression faible	-Débit très faible. -non étanchéité de la vanne.	-Baisse d'alimentation. -Risque d'arrêt installation		
		Les fuites	Epandage de gaz. Création d'un mélange favorable,	Détecteurs de Gaz, Alarme. Maintenance des vannes pneumatiques.	
	Haute pression	Mauvaise, régulation de la pression		Soupapes de sécurité (3) -clapet de sécurité	

Suite

Skid N°3 : Les détendeurs

Paramètre	Déviation	Causes	conséquences	Mesures existantes	recommandations
Température	-Faible Température.	-climat -chaudière défaillante -régulation fausse	-Givrage des vannes. -Givrage des conduites. -Fuite de gaz. Epandage des gaz	-Contrôle de température - utilisation des autres 2 rampes	
	-Haute Température	-feu extérieur	Augmentation de la pression. Expansion rapide du gaz. Favorise les fuites et épandage de gaz. Risque d'incendie	-régulation de la température. -Contrôle de pression. -Détecteur de gaz -clapet de sécurité	

Skid N°4 : Le séparateur final

Paramètre	Déviation	Causes	conséquences	Mesures existantes	recommandations
Débit	Pas de débit	-Pas d'alimentation, --Fermeture des vannes en amont du séparateur final.	-arrêt des groupes -		
		Bouchage des filtres	Perte de charge	changement périodique, -évacuation automatique des condensats -capacité de retenu du liquide	
	Débit faible	Précipitation des débris qui mènent au bouchage des filtres.	Risque d'arrêt de l'installation	-Commande manuelle des vannes -indicateur visuel et alarme de niveau haut et tres haut des condensats avec report en salle de commande	
		Défaillance de la vanne en amont.		Maintenance des vannes	
	Haut débit	-Alimentation forcée en gaz. -Défaillance des vannes, -ouverture intempestive.	-Augmentation de la charge -niveau des condensats élevé dans le séparateur.	-Régulateur de débit et de pression -indicateur visuel et alarme de niveau haut et très haut des condensats avec report en salle de commande	

		Augmentation de la pression et/ou de la température	Risque de « UVCE ». Incendie en cas de fuite et présence d'une source d'ignition.	La torche pour la décharge. Régulation de la pression et de la température. -indicateur visuel et alarme de niveau haut et très haut des condensats avec report en salle de commande	
Pression	Basse pression	Faible débit d'alimentation	Risque d'arrêt de l'installation.	-Régulation du débit d'alimentation. -Utilisation des autres lignes d'alimentation (rampes).	
		. Fuite au niveau de la vanne, ou dans la conduite	Risque d'incendie ou d'explosion	Contrôle des vannes. Maintenance. Détecteur de gaz. Alarme au niveau de la salle de commande. Utilisation des autres lignes d'alimentation (rampes)	
	Haute pression	Augmentation de la température.	les fuites. Expansion rapide des gaz, risque d'éclatement des vannes et des conduites, Risque d'explosion.	Détecteurs de Gaz. Régulation de la pression. Système d'arrêt et dépressurisation en aval. Système d'arrosage et anti-incendie.	

Paramètre	Déviation	Causes	conséquences	Mesures existantes	recommandations
Température	Haut température	-feu extérieur Climat (été)	-Augmentation de la pression. - les fuites et - épandage de gaz. -Risque d'incendie ou explosion.	-Régulateur de température TIC 300	
	Basse température	Hiver	-Givrage des vannes. - Givrage des conduites	Détecteur de gaz Indicateur de température (salle de commande) -Utilisation des autres rampes	

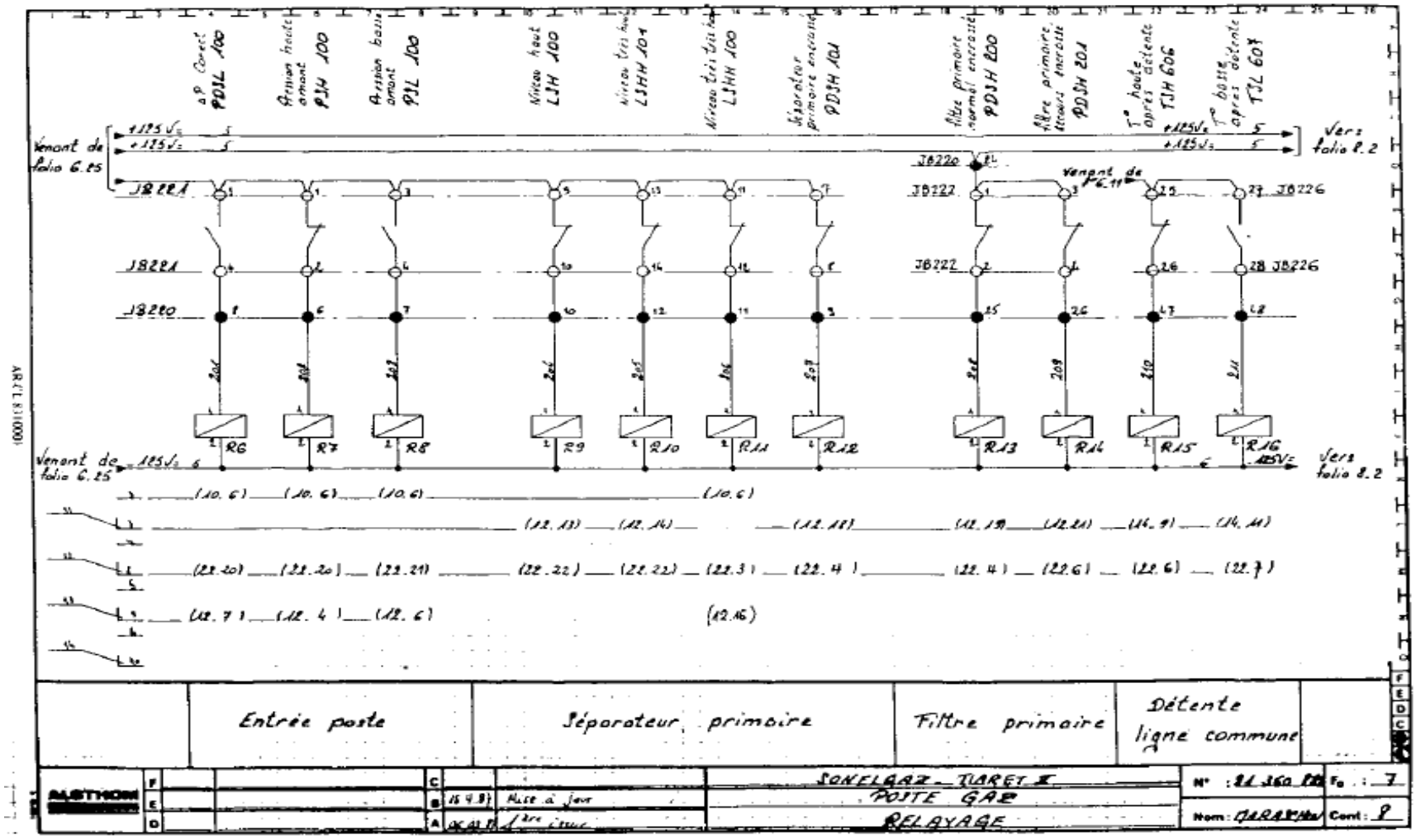
Skid N°5 : la Chaudière

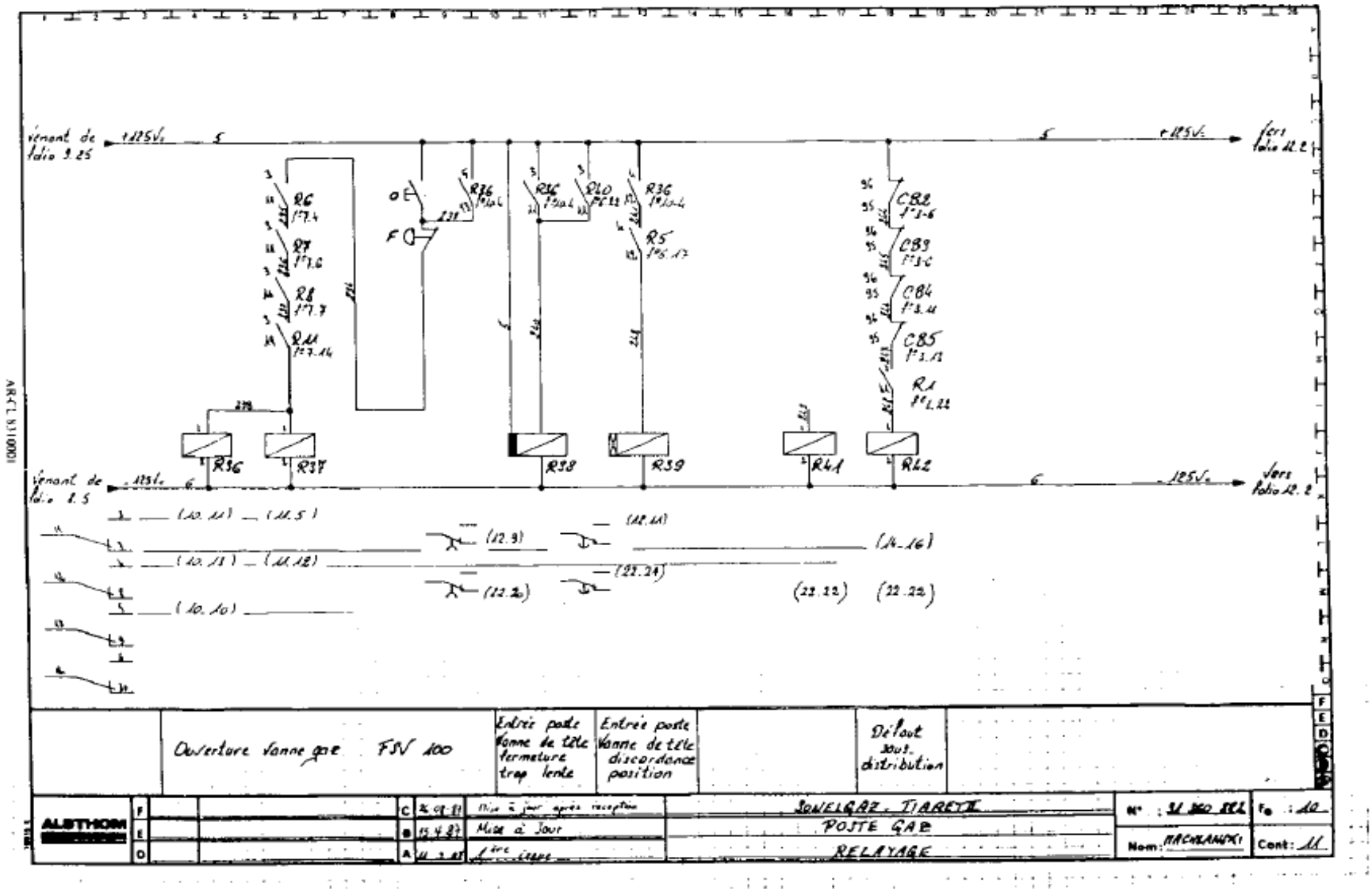
Paramètre	Déviation	Causes	conséquences	Mesures existantes	recommandations
débit	Pas de débit	Pas d'alimentation en gaz Fermeture de vanne en amont	-Non réchauffage du gaz -arrêt des groupes	-2 chaudières -régulateur TIC 300 -niveau visuel et alarme haute et basse -by-pass chaudière	
	Faible débit	Fuites au niveau des conduites	-détérioration de la turbine et des machines /explosion en présence d'une source d'ignition	-Détecteur de gaz	
	Haut débit	-Augmentation de débit d'alimentation suite à une défaillance de la vanne. -Ouverture intempestive	-Explosion -arrêt de l'installation	Contrôle et maintenance des vannes. Comptage	

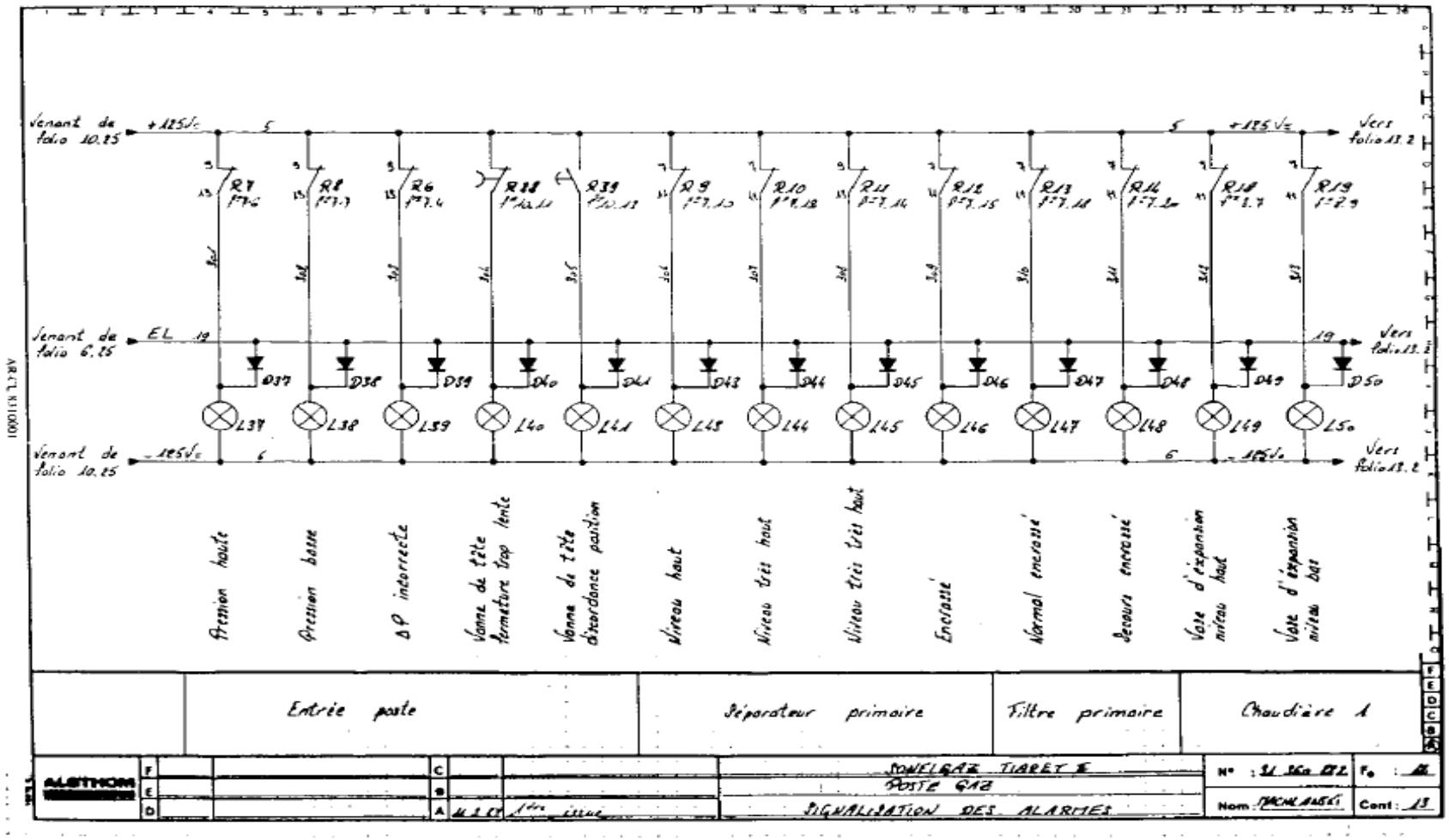
Paramètre	Déviation	Causes	conséquences	Mesures existantes
Pression	basse pression	Détente excessive du gaz dans le détendeur. (P< 20 bars) Ouverture intempestive de la vanne Feu extérieur	-Risque d'arrêt de l'installation (pression de service non atteinte). -Baisse de température risque de givrage des injecteurs,	Régulateur de température TIC 300
	haute pression	Augmentation de la température extérieure ou de la température du gaz	Augmentation de la pression. Favorise les fuites. Surpression dans les conduites	- Détecteur de gaz. Contrôle du débit pour détecter les fuites
Température	Haut température	-feu extérieur Climat (été)	-Augmentation de la pression. - les fuites et - épandage de gaz. -Risque d'incendie ou explosion.	-Régulateur de température TIC 300 -Contrôle de pression. -Détecteur de gaz -système d'arrêt de flamme -thermostat température eau haute - thermostat température eau basse
	Basse température	Hiver -mauvaise régulation de température.	-Givrage des vannes. - Givrage des conduites	Indicateur de température (salle de commande)

ANNEXE B

SCHEMA ELECTRIQUE


Entrée poste
Séparateur primaire
Filtre primaire
Détente ligne commune
SONELGAZ - TIARET
POSTE GAZ
RELAYAGE


Ouverture vanne gaz FSV 100
Entrée poste Vanne de télé fermeture trop lente
Entrée poste Vanne de télé discordance position
Défaut sous distribution
ALSTHOM
SOUELGAZ . TIARET
POSTE GAZ
RELAYAGE
Nom: MACHLAHI


Venant de folio 10.25
+125 V=
Vers folio 13.2
Venant de folio 6.25
EL 19
Vers folio 13.2
Venant de folio 10.25
-125 V=
Vers folio 13.2
Pression haute
Pression basse
ΔP incorrecte
Vanne de tête fermeture trop lente
Vanne de tête discordance position
Niveau haut
Niveau très haut
Niveau très très haut
Encrasse
Niveau encrassé
Détecteur encrassé
Vase d'expansion niveau haut
Vase d'expansion niveau bas
Entrée poste
Séparateur primaire
Filtre primaire
Chaudière 1
SONELGAZ TIARET SE
POSTE GAZ
SIGNALISATION DES ALARMES
1ère issue

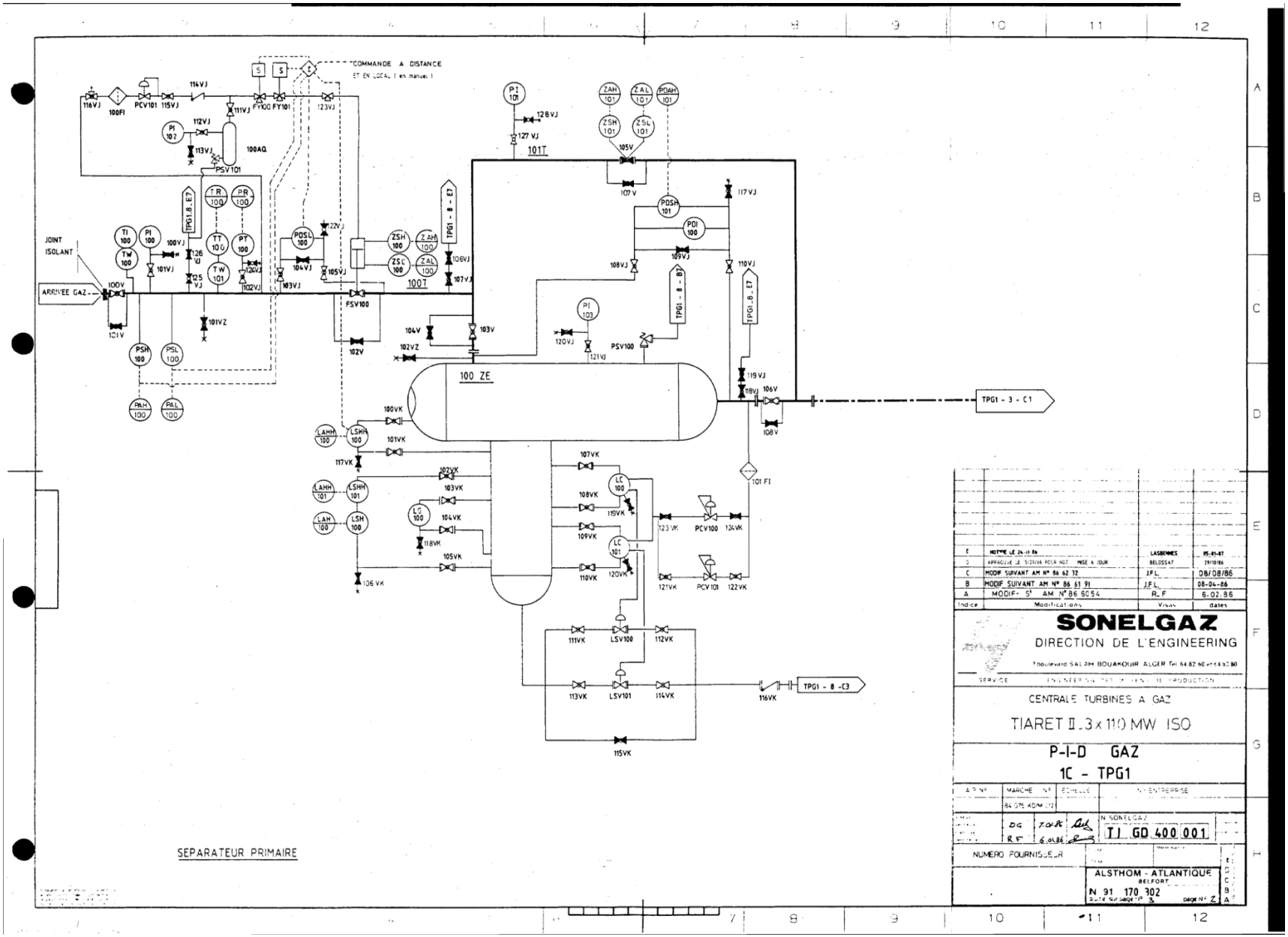
ANNEXE C

CARACTERISTIQUE DE LA VANNE FSV 100

vanne	
Constructeur	MAPEGAZ
Type de vanne	A bille à passage intégral
Matière	Acier
Raccordement	A brides ANSI 600 RF
Numéro de série	157054
Diamètre	10 "
MAX OP	1480 PSI 102 bar
Température	-28 + 50 °c
Débit	100000 Nm3/h
Distance entre bride	787 mm
Nombre de trous	16 Diamètre
Nature du fluide	Gaz naturel (85% de méthane)
Body (Corps)	LF2
Stem (Tige)	17-4PH
ball	17-4PH
Seat (Siége)	316
Closure	LF2
Position de montage	Horizontal
Commande	Manuelle et automatique
Essai hydraulique au corps	150 bars
Essai hydraulique aux sièges	110.3 bars
Norme Pression de teste	API 6 D
Pression de design	102bars
Température de design	-28/50°C
Opérateur	
Opérateur de commande	Servomoteur pneumatique à simple effet avec ressort de rappel
Fluide	Gaz naturel pression max 10 bars
Constructeur de l'opérateur	CAI
type	R203/R250 x2
N° de serie	26351 date mars 1987
Pression	28 à 70 bars
Temps de manœuvre	Ouverture 5 secondes fermeture= 2 secondes
Commande	Fermeture et ouverture
Commande local	Oui
Commande manuelle de secours	Oui
Commande à distance	Oui
Nombre d'électrovanne de commande	Deux électrovannes de type ADF EEX D II CT6
Commande manuelle des électrovannes	oui
Tension de commande	125 vcc
Pression de commande	7 bars
Type de l'opérateur	Passage plein
Indicateur mécanique de position	Oui
Commande et signalisation	
Commande à distance	Fermeture d'urgence
Commande locale	Fermeture et ouverture (panneau au installé du voisinage du poste gaz
Indicateur de position	Fin de cours • Un l'ouverture • Un a la fermeture
Type de boitier	ADF EEX D II CT6

ANNEXE D

SCHEMA P&ID


"COMMANDE A DISTANCE
ET EN LOCAL (en manuel)
100FI
PCV101
FY100
FY101
PSV101
100AQ
101T
100T
100 ZE
JOINT ISOLANT
ARRIVEE GAZ
FSV100
PSV100
TPG1 - 3 - C1
TPG1 - 8 - C3
101 FI
PCV100
PCV101
LSV100
LSV101
SEPARATEUR PRIMAIRE
SONELGAZ
DIRECTION DE L'ENGINEERING
CENTRALE TURBINES A GAZ
TIARET II 3 x 110 MW ISO
P-I-D GAZ
1C - TPG1
TJ GD 400 001
ALSTHOM - ATLANTIQUE
BELFORT
N 91 170 302