REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Ecole Nationale Polytechnique

Mémoire de projet de fin d'études
pour l'obtention du diplôme d'ingénieur d'état en
Qualité Hygiène Sécurité Environnement
et Gestion des risques Industriels

Fiabilisation de Systèmes Critiques en vue de la Maitrise de Risques Majeurs -Cas Centrale Électrique Hamma II-

MOULOUDI Lamia

TAMSSAOUET Ferhat

Sous la direction de : M. A. KERTOUS Maitre-assistant

M. M. OUADJAOUT Maitre-assistant

Présenté et soutenu publiquement le 22/06/2016

Composition du Jury :

Président :	Mme. S. ZEBOUDJ	Professeur	ENP
Rapporteurs :	M. A. KERTOUS	Maitre-assistant	ENP
	M. M. OUADJAOUT	Maitre-assistant	ENP
Examinateurs :	M. M. BOUSBAI	Maitre-assistant	ENP
	Mme. N. OUSSEDIK	Maitre-assistant	ENP

ENP-2016-

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Ecole Nationale Polytechnique

Mémoire de projet de fin d'études
pour l'obtention du diplôme d'ingénieur d'état en
Qualité Hygiène Sécurité Environnement
et Gestion des risques Industriels

Fiabilisation de Systèmes Critiques en vue de la Maitrise de Risques Majeurs -Cas Centrale Électrique Hamma II-

MOULOUDI Lamia

TAMSSAOUET Ferhat

Sous la direction de : M. A. KERTOUS Maitre-assistant

M. M. OUADJAOUT Maitre-assistant

Présenté et soutenu publiquement le 22/06/2016

Composition du Jury :

Président :	Mme. S. ZEBOUDJ	Professeur	ENP
Rapporteurs :	M. A. KERTOUS	Maitre-assistant	ENP
	M. M. OUADJAOUT	Maitre-assistant	ENP
Examinateurs :	M. M. BOUSBAI	Maitre-assistant	ENP
	Mme. N. OUSSEDIK	Maitre-assistant	ENP

ENP-2016-

ملخص : الهدف من هدا العمل هو التمكين من موثوقية الانظمة الحساسة لمحطة توليد الطاقة الكهربائية الحامة 2 عن طريق تبني طرق امن التشغيل. يرتكز اختيار نسب طرق على المحيط المرتب الذي تتطور فيه هذه الانظمة. هذا و قد قمنا بتحليل المخاطر و حواجز السلامة من اجل تحديد معايير السلامة الغير كافية لتخفيض خطر الحوادث. قمنا بتحسين هذه المعايير من اجل تحقيق السلامة بالاعتماد عل شبكة الموثوقية و تكرار المعدات التقنية في معاير السلامة.

الكلمات الدالة التحليل الوضيفي, المنطق الضبابي HazOp-RPN الضبابية, الرسم البياني الضبابي للخطر, BORA,SIS, SIL,تحليل شجرة الاخطاء الضبابية, شبكة الموثوقية, التفعيل, تكرار المعداة التقنية

ABSTRACT: The aim of this work is to improve the reliability of critical systems of power plant Hamma II by using a dependability approach. The choice of methods was done in light of uncertain environment in which they evolve. We conducted a risk analysis and safety barriers analysis to determine the inadequate safety barriers to mitigate the risk of major accidents. These barriers have been optimized to achieve the safety objectives based on concepts of reliability networks and redundancy.

Key Words : Functional analysis, fuzzy logic, fuzzy HazOp-RPN, fuzzy risk graph, SIS, SIL, BORA, fuzzy fault tree analysis, reliability network, optimization, redundancy

Résumé : Le but de ce travail est de fiabiliser des systèmes critiques de la centrale électrique Hamma II par l'utilisation d'une démarche de sûreté de fonctionnement. Le choix des méthodes s'est fait en tenant compte de l'environnement incertain dans lesquels ils évoluent. Nous avons effectué une analyse de risques et une analyse des barrières de sécurité afin de déterminer les barrières de sécurité insuffisantes pour diminuer le risque d'accidents majeurs. Ces barrières ont été optimisées afin d'atteindre les objectifs de sécurité, en se basant sur les concepts de réseaux de fiabilité et de redondance.

Mots clés : Analyse fonctionnelle, logique floue, HazOp-RPN flou, graphe de risque flou, SIS, SIL, BORA, Arbre de défaillance flou, réseaux de fiabilité, optimisation, redondance

Dédicaces

Je dédie ce travail :

A ma mère et mon père

A Noureddine et toute ma famille

A Adnan et tous mes amis

Ferhat

Je dédie ce travail :

A mon frère Nacim

A Ma mère et Mon père

A Ayoub et tous mes amis

A Ma tante Malika et ses filles et toute la famille

Lamia

Remerciements

Le présent travail a été effectué au sein de la Centrale Electrique Hamma II sous la responsabilité de M. Samir KACI, responsable HSE. Nous tenons à lui adresser nos sincères remerciements ainsi qu'à l'ensemble du personnel des deux départements HSE et exploitation pour leurs disponibilité et leurs efforts qui nous ont permis de réaliser ce travail.

Nous exprimons toute notre gratitude à nos deux encadreurs académiques, Monsieur. Aboubakr KERTOUS, Enseignant à l'ENP, et Monsieur Mohamed OUADJAOUT, Enseignant Chercheur à l'ENP et Directeur du Cycle Préparatoire –ENP, pour le privilège qu'ils nous ont fait en dirigeant notre PFE et pour le suivi continu pour l'aboutissement de ce projet. Leur intérêt, leur soutien et leurs compétences ont été un atout indispensable pour l'accomplissement de notre travail.

Nous aimerions aussi remercier les membres du jury, en premier, Madame Zeboudj, Professeur à l'ENP et Responsable de la Filière QHSE-GRI, qui nous fait l'honneur de présider ce Jury, Madame Oussedik et Monsieur Bousbai, enseignants à l'ENP, qui ont bien voulu accepter d'examiner et de juger ce travail.

Nous adressons nos remerciements au corps professoral de la Filière QHSE-GRI qui nous ont guidés durant ces 3 dernières années, pour leur dévouement à accomplir leur devoir.

Enfin, un grand merci à tous nos amis pour leurs sincères encouragements et nos familles pour leur soutien.
.

Tables des matières

Liste des tableaux

Liste des figures

Liste des abréviations

AdD	Arbre de Défaillance
AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
ATEX	ATmosphere EXplosive
BDD	Bloc Diagramme Barrière
BORA	Barrier and Operational Risk Analysis
CEI	International Electrotechnical Commission
EOP	Estimated Occurrence Probability
FAST	Function Analysis System Technique
FBS	Function Breakdown Structure
FIS	Fuzzy Inference System
HazOp	Hazard and Operability
HazOp-RPN	Hazard Operability-Ranking Priority Number
HSE	Hygiène, Sécurité et Environnement
ISO	International Organization for Standardization
LOPA	Layer Of Protection Analysis
MISO	Multiple Inputs and Single Output
NF	Norme Française
NTNU	Université Norvégienne de Sciences et Technologies
OFAF	Oil Forced- Air Forced
PFD_{avg}	Average Probability of Failure on Demand
PFH	Probability of a dangerous Failure per Hour
P&ID	Piping and Instrumentation Diagram
RIFs	Risk Influencing Factors
RRF	Risk Reduction Factor
SADT	Structured Analysis and Design Technique
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Système Instrumenté de Sécurité
SONELGAZ	Société Nationale de l'Electricité et du Gaz
UKOOA	United Kingdom Offshore Operators Association
UV	Ultraviolet

Introduction générale

Le développement des industries, la complexité croissante de ses procédés ainsi que la prise de conscience grandissante de la société aux notions de sécurité et de développement durable, obligent les entreprises à démontrer leur maîtrise des risques. En effet, avec l'augmentation de la consommation en énergie et en biens, les entreprises ont recours à des procédés critiques utilisant des matières dangereuses et fonctionnant avec des paramètres nominaux portés à l'extrême afin de satisfaire la demande et d'augmenter leur rentabilité. Or, de tels systèmes impliquent des dangers pouvant induire incendies, explosions et autres risques majeurs, sources de dommages pour les personnes, l'environnement ou les biens.

Pour des installations de grande importance (centrale électrique, réseau de communication, réseau d'eau potable, etc.), la maîtrise des systèmes critiques est une obligation de par leur rôle stratégique. L'augmentation de la fiabilité des systèmes critiques revient, donc, à atteindre un double objectif qui est d'assurer la sécurité et la disponibilité des procédés les abritant. Ainsi, les entreprises font l'inventaire des risques que ces systèmes impliquent, de leur nature, des mécanismes qui peuvent conduire au déclenchement d'accidents majeurs. Ils procèdent aussi à l'estimation des conséquences et la fréquence à laquelle ils sont susceptibles de survenir. Une fois le niveau de risque évalué, les entreprises chercheront à le ramener sous un seuil acceptable.

Les moyens à mettre en œuvre pour réduire les risques sont nombreux et variés. En premier lieu, la conception du procédé et le choix des équipements participent à la réduction du risque. On peut agir aussi sur les systèmes de contrôle commande du procédé, en prévoyant par exemple des redondances et des systèmes de repli, en cas de dysfonctionnement. Ces approches ne sont pas toujours suffisantes. Pour réduire encore le risque, il faut prévoir des systèmes de sécurité. Ceux-ci entrent en action lorsque le procédé se trouve dans des conditions anormales de fonctionnement et qu'une situation dangereuse risque de se développer. Il existe différents types de barrières de sécurité. L'une d'elle est la sécurité active instrumentée, dont les systèmes instrumentés de sécurité (SIS, *Safety Instrumented System*) sont les plus répandus et utilisés.

Un système instrumenté de sécurité est un ensemble de composants agencés d'une façon spécifique afin de remplir une fonction de sécurité. Pouvant être lui-même sujet à défaillance ou source de danger, son fonctionnement doit être analysé, et son niveau de fiabilité et d'intégrité démontré afin, de déterminer s'il va remplir sa fonction de sécurité lorsqu'il est sollicité.

Les analyses de risques et des barrières de sécurité sont souvent critiquées pour le caractère subjectif de leur conduite et l'imprécision de leurs résultats. Or, l'incertitude est inhérente à la notion de risque, et ce dernier n'est perçu et appréhendé que par rapport à des facteurs subjectifs. Puisque l'élimination de cette incertitude est impossible, l'on a proposé de la modéliser et de la prendre en compte dans les études qui traitent du risque. Pour ce faire, nous avons eu recours à la logique floue.

En effet, le développement de la théorie de la logique floue a offert les outils nécessaires permettant d'améliorer la qualité des résultats des analyses faites sur le risque. En particulier, l'application se fait pour des environnements incertains où le retour d'expérience et les données permettant de le caractériser sont insuffisants.

Afin d'atteindre l'objectif de cette étude, nous avons suivi une démarche impliquant l'utilisation de plusieurs outils et méthodes à même de donner plus de confiance aux résultats obtenus.

Nous avons, d'abord, étudié le fonctionnement des systèmes critiques de la centrale électrique Hamma II afin d'identifier les modes de défaillance conduisant à la survenance d'accidents majeurs. En introduisant les notions de variables floues, de variables linguistiques et des systèmes d'inférence, nous avons pu caractériser chaque scénario d'accident afin de déterminer ceux dont le niveau de risque est inacceptable.

Ensuite, nous avons étudié les barrières de sécurité mises en place par l'entreprise pour diminuer le risque d'accidents majeurs du point de vue du niveau de la sécurité qu'elles doivent offrir et celle qu'ils peuvent assurer de par leur fiabilité et intégrité.

La fin de ce travail a consisté à améliorer la sécurité offerte par les barrières de sécurité existantes et de concevoir de nouvelles barrières. Les solutions proposées tiennent compte et du coût que doit supporter l'entreprise pour démontrer sa maîtrise de risque, et des exigences de sécurité auxquelles doivent satisfaire les barrières. Cela a été réalisé en optimisant le coût de la modification des barrières par l'ajout d'un minimum de composants permettant d'atteindre les objectifs de sécurité assignés. Une deuxième optimisation s'est faite par rapport à l'architecture de ces barrières, c'est-à-dire l'agencement des différents équipements les composant. Pour ce faire, nous avons essayé de chercher de nouvelles structures impliquant moins de connexions entre les équipements afin de réduire le coût de la barrière. Des éléments de la théorie des graphes ont été utilisés afin de vérifier que l'objectif de réduction de risque est toujours satisfait.

Le présent travail est organisé en quatre chapitres :

1. Le premier chapitre, comportent une brève présentation du groupe SONELGAZ, de la centrale Hamma II et du process de production d'électricité. Ce chapitre comporte aussi une introduction à l'analyse fonctionnelle et à la méthode SADT qui nous a permis de décomposer et de comprendre les systèmes critiques de la centrale.
2. Le deuxième chapitre est organisé en deux parties. Dans la première partie, des notions sur la logique floue sont présentées, ainsi que le système d'inférence de Mamdani. Cette approche est utilisée pour caractériser le comportement des systèmes réels qui ont comme entrées des variables linguistiques et des règles floues.

   Dans la deuxième partie, la méthode HazOp-RPN utilisant l'inférence floue est développée. Elle sera appliquée aux processus critiques de la centrale électrique HAMMA II afin d'identifier, d'estimer et d'évaluer les différents scénarios.
3. Le troisième chapitre s'intéresse à l'analyse des barrières de sécurité. Il est divisé en trois parties. Dans la première partie, des généralités sur les systèmes instrumentés de sécurité ont été présentées. La deuxième partie est consacrée à la détermination du SIL requis des SIS par la méthode de graphe de risque étalonné et flou pour les scénarios d'accidents majeurs sélectionnés dans le chapitre précédent. Dans la troisième partie, nous analyserons les SIS pour leur allouer un SIL, par la méthode BORA qui permet de prendre en compte les conditions d'exploitation dont lesquelles évoluent les systèmes critiques, et par la méthode AdD conventionnelle et AdD flou. Une discussion des résultats termine ce chapitre.
4. Le quatrième chapitre est organisé en trois parties. Dans la première partie, nous citerons les différentes structures de systèmes ainsi que les formules permettant d'obtenir leur fiabilité. Dans la seconde, des notions de base sur la théorie des graphes et les réseaux de fiabilité sont présentées. Dans la dernière partie, nous appliquerons ces concepts afin d'optimiser et de concevoir la structure des SIS.

Une conclusion générale présentant les résultats obtenus termine notre travail, incluant aussi les perspectives de recherche.

Chapitre 1 : Périmètre de l'étude

Introduction

Ce premier chapitre est organisé en trois parties, nous présenterons sommairement le groupe SONELGAZ dans le monde, avant de nous focaliser sur notre cas d'étude : la centrale électrique Hamma II, où nous allons passer en revue son organisation, ses processus et les unités qui la constituent.

Dans la deuxième partie nous présenterons la manière dont nous avons fixé notre périmètre d'étude et les raisons de nos choix des systèmes critiques. Dans la dernière partie, nous définirons l'analyse fonctionnelle et son opportunité pour l'évaluation des risques qui sera conduite plus loin, ainsi qu'une présentation de la méthode SADT, utilisée pour effectuer la décomposition fonctionnelle. Nous allons, par la suite, présenter en détail les systèmes critiques sélectionnés pour cette étude et qui induisent des risques majeurs ainsi que leurs décompositions fonctionnelles par la méthode SADT.

1.1. Présentation de l'organisme d'accueil

Dans cette partie nous allons présenter l'organisme d'accueil SONELAZ ainsi que ses activités

1.1.1. Présentation du groupe SONELGAZ

SONELGAZ est une entreprise algérienne appartenant au secteur économique spécialisée dans la production, le transport et la distribution de l'électricité et du gaz.

Créée en Algérie, l'entreprise s'est progressivement développée pour devenir aujourd'hui un groupe industriel international, composé de 29 filiales et employant plus de 47000 travailleurs.

1.1.2. Activités du groupe SONELGAZ

SONELGAZ est composée de trois branches d'activités : la production, le transport, la distribution et la commercialisation de l'électricité et du gaz, tant en Algérie qu'à l'étranger.

- Activité production : c'est l'activité consistant à transformer l'énergie calorifique ou hydraulique en énergie mécanique puis électrique.
- Activité transport : cette activité englobe le transport de l'électricité et le transport du gaz.
- Activité distribution électricité et gaz : consiste à alimenter l'ensemble des clients industriels et les abonnés domestiques.

Ajoutant aussi que SONELGAZ a toujours joué un rôle prépondérant dans le développement économique et social du pays. Sa contribution dans la concrétisation de la politique énergétique nationale sont à la mesure des programmes de réalisation importants en matière d'électrification

rurale et de distribution publique du gaz, qui ont permis de hisser le taux de couverture en électricité à plus de 99% et le taux de pénétration du gaz à plus de 52 %.[1]

1.1.3. La centrale électrique Hamma II

Conçue et réalisée dans le but de sécuriser la ville d'Alger en matière d'alimentation en énergie électrique et d'assurer un appoint au réseau général interconnecté. La centrale électrique HAMMA II a été mise en service en 2002.

Cette centrale affiche en matière de disponibilité de production, un taux élevé allant jusqu'à 99% supérieur à la moyenne internationale qui est de 95%.

1.1.3.1. Description générale

La centrale est équipée de deux groupes turbines à gaz montés par le constructeur italien ANSALDO sous licence SIEMENS. La puissance totale nominale de base aux bornes usine est égale à 418 MW (209 MW chacune). L'énergie est évacuée à travers un poste de transformation de 220 KV.

La centrale peut fonctionner avec deux combustibles

- Gaz naturel (combustible principal) ;
- Fuel (combustible de secours)

Chaque groupe thermique est alimenté par un système de réseau gaz composé de quatre lignes ou rampes de détente et de pompage du combustible. Le gaz naturel est délivré à la centrale HAMMA II à travers un gazoduc provenant de la ville de Hassi R'Mel.

Les groupes sont installés dans des enceintes appelées « package » et placé dans une salle de machines commune avec possibilités d'exploitation à partir d'une salle de commande.

1.1.3.2. Organisation

L'établissement est placé sous la responsabilité d'un Directeur unique. Il est représenté par un comité de Direction comprenant :

- Le responsable de division Technique ;
- Le responsable de la subdivision Production ;
- Le responsable de la subdivision finance /comptabilité ;
- Le responsable des Ressources Humaines.

Le service Hygiène, Sécurité et Environnement (HSE) est rattaché directement au Directeur de l'établissement. Ce service anime et coordonne la sécurité de l'ensemble de l'établissement ainsi que la formation du personnel.

[1] www.sonelgaz.com

1.1.3.3. Description de l'installation

L'installation est composée d'équipements et d'infrastructures décrits ci-dessous.

1.1.3.3.1. Salle des machines

Dans cette salle, on trouve les différents composants des deux tranches de production tels que : les deux turbines, l'alternateur, le transformateur, et les différents systèmes auxiliaires (système pneumatique, etc.).

1.1.3.3.2. Compresseur

Le compresseur de la turbine est un compresseur axial à 17 étages, muni d'un étage à orientation variable qui permettra de réguler le débit d'air admis au compresseur, ainsi il permet de réguler la température des gaz d'échappement afin d'éviter la baisse du rendement.

1.1.3.3.3. Turbine

La turbine est à quatre étages comportant un châssis horizontalement dédoublé donnant l'accès aux pièces internes ainsi que des aubes de turbine en alliage, démontables individuellement et d'un dispositif d'échappement axial à basse perte idéal pour des applications de récupération de chaleur.

Elle est dotée d'une technologie de refroidissement avancée où l'air de décharge du compresseur est utilisé pour refroidir les composants internes.

1.1.3.3.4. Chambre de combustion

La chambre de combustion de la turbine, est une chambre annulaire munie de 24 brûleurs hybrides, fonctionnant à combustible gazeux et liquide. Elle est conçue de sorte à limiter les émissions des oxydes d'azote (NOx).

1.1.3.3.5. Echappement de la turbine

Le système d'échappement est conçu en vue de mener les gaz chauds (517°) ou en excès à la cheminé d'évacuation.

1.1.3.3.6. Alternateur

C'est l'élément responsable de la transformation de l'énergie mécanique produite par la turbine en énergie électrique sous forme de courant alternatif, devant être débité au réseau interconnecté.

C'est une machine synchrone d'une puissance apparente de 270 MVA et d'un facteur de puissance (cos ϕ= 0.8), sa tension nominale est de 15,75 kV, une fréquence de 50 Hz, et est refroidi à l'hydrogène sous pression.

L'excitation de l'alternateur s'effectue par une excitatrice statique. L'alternateur comporte essentiellement deux enroulements : le rotor et le stator

Le rotor excité par un courant continu, produit un champ tournant au cours de sa rotation. Ce champ engendre des forces électromotrices dans chacune des phases de l'enroulement du stator. Ces forces sont engendrées par le champ rotorique tournant ; elles sont donc en fonction du courant d'excitation et de la vitesse.

1.1.3.3.7. Transformateur

Le transformateur principal de la centrale est un transformateur élévateur de tension, avec un rapport de transformation de (15-75 KV/225 KV) en tension, et de (667,2 A / 9530,9 A) en intensité, sa puissance nominale est de 260 MVA, le refroidissement quant à lui est assuré par un système OFAF (Oil Forced- Air Forced).

1.1.3.3.8. Groupe Diesel de secours

Le groupe Diesel est un moteur thermique destiné à produire l'énergie électrique indispensable au lancement des groupes de la centrale et à l'alimentation des auxiliaires, en cas de rupture de tous les systèmes de transformations.

Ce moteur se caractérise par une puissance active de 4114 KW et d'une puissance apparente nominale de 6050 KVA. Sa vitesse de rotation nominale est de 1000 tr /min à 50 Hz, comptant une tension de 6KV et un courant de 582,2 A.

1.1.3.4. Production d'électricité

Le process de production d'électricité est composé de plusieurs étapes, décrites ci-dessous :

- L'air comprimé en provenance du compresseur pénètre dans l'espace annulaire constituant la chambre de combustion, au même moment où les injecteurs introduisent le combustible qui se mélange à l'air. L'allumage s'effectue grâce à deux bougies rétractables.
- Les gaz chauds issus de la combustion traversent ensuite les quatre étages de la turbine où ils se détendent. Chaque étage se compose d'un ensemble d'aubes fixes suivies d'une rangée d'aubes mobiles. Dans chaque rangée d'aubes fixes, l'énergie cinétique du jet de gaz augmente, en même temps que la pression chute. Une partie de l'énergie cinétique du jet est convertie en travail utile transmis au rotor de la turbine sous la forme d'un couple mécanique.
- Après leur passage dans les aubes du quatrième étage, les gaz brûlés sont évacués vers la cheminée.
- La rotation résultante de l'arbre entraîne le rotor de l'alternateur, l'axe du compresseur ainsi que d'autres auxiliaires.

1.2. Cadre d'étude

Le process de production d'électricité est un process complexe comportant des paramètres de fonctionnements critiques tels que les grandes pressions et les hautes températures et utilisant des matières dangereuses hautement inflammables et explosibles telles que l'hydrogène et le gaz naturel. Les risques induits par ces caractéristiques doivent être évalués et maîtrisés.

L'analyse préliminaire des risques effectués par Mr H. Daoud (Daoud, 2015) a fait ressortir les différents risques présents au niveau de la centrale électrique Hamma II. Cette étude nous a permis de déterminer les systèmes critiques qui induisent les risques majeurs, et qui sont : le système de refroidissement à hydrogène de l'alternateur et le poste gaz qui peuvent être la cause d'explosions et le système fuel d'incendie.

Afin de réaliser la première étape de notre démarche qui est la détermination des scénarios critiques par rapport à chaque système, nous avons eu recours à l'analyse fonctionnelle. Cette dernière nous a permis de mieux les comprendre et de pouvoir déterminer les défaillances qui pourront conduire à la survenance d'accidents majeurs.

1.3. Analyse fonctionnelle

La croissance de la complexité des systèmes impliquerait souvent de considérer le système dans une vue d'ensemble (Noyes, 2007). En effet afin d'évaluer les performances et la conduite des systèmes industriels, c.-à-d. mener une étude de sûreté de fonctionnement, il est recommandé de décrire les différents flux, physiques et informationnels, qui régissent son fonctionnement, la manière dont ils interagissent ainsi que les structures qui les supportent.

1.3.1. Présentation de l'analyse fonctionnelle

L'analyse fonctionnelle est une démarche qui consiste à rechercher, ordonner, caractériser, hiérarchiser et/ou valoriser les fonctions (NF 50-150, 1990). Elle est utilisée dans toutes les phases du développement d'un produit ou d'un processus et est adaptée à tous types de projets pour atteindre des objectifs différents : conception, maintenance, analyse de risques, optimisation, etc. Dans notre cas d'étude nous avons effectué une analyse fonctionnelle pour les systèmes critiques d'un procédé industriel en vue d'une analyse de risques.

Pour rendre compte de la complexité des systèmes, l'analyse fonctionnelle allie analyse structurelle et analyse dynamique (Noyes, 2007). L'analyse structurelle d'un système consiste en une décomposition analytique de ses fonctions opérationnelles en une hiérarchie de sous fonctions. L'analyse dynamique tente de caractériser son fonctionnement (ex : transformations des entrées en sorties) et son évolution (adaptation du système à la mission assurée ou à l'environnement).

Plusieurs méthodes ont été développées afin de faciliter l'analyse. Elles sont basées sur une approche structurée de manière hiérarchique, descendante et modulaire. A partir de raffinements successifs, ces méthodes s'appuient souvent sur un formalisme graphique.
Parmi les méthodes d'analyse figurant dans cette catégorie, on peut citer les méthodes :

- FAST (Function Analysis System Technique);
- FBS (Function Breakdown Structure) ;
- SADT (Structured Analysis and Design Technique).

Cette dernière est la méthode choisie pour l'analyse fonctionnelle des trois systèmes étudiés.

1.3.2. Méthode SADT

SADT (en anglais Structured Analysis and Design Technique) est une méthode d'origine américaine, développée par Softech en 1977 puis introduite en Europe à partir de 1982 par Michel Galiner. Elle se répandit vers la fin des années 1980 comme l'un des standards de description graphique d'un système complexe par analyse fonctionnelle descendante (Thierry, 2008). C'est une méthode d'analyse par niveaux successifs d'approche descriptive.

1.3.2.1. Objectif de la méthode

SADT permet d'organiser les flux de données pour donner une vision globale du système puis par une analyse des niveaux successifs, permet de préciser de plus en plus finement le rôle de chacun des éléments du système. La finesse de cette description dépendra directement des besoins des utilisateurs (Michel, 1990).

1.3.2.2. Modèle SADT

Un modèle SADT représente une image d'un système qu'on veut appréhender. Il est composé de (Boutelis, 2015) :

- Diagrammes d'activités ou actigrammes qui représente l'ensemble des activités du système.
- Diagrammes de données ou datagrammes qui montrent l'ensemble des données du système.

Dans les actigrammes, les actions sont reliées entre elles par des flux de données alors que dans les datagrammes, c'est les données qui sont reliées entre-elles par des flux d'activité (Sindjui, 2014).
Le schéma de base d'un actigramme est présenté dans la figure 1 et il est composé de :

- **La boîte** : représentant une action, une activité.

- **Les entrées** qui sont transformées en sorties par l'action ou servent à alimenter l'action. Elles ne sont donc pas forcément modifiées mais sont nécessaires au fonctionnement de l'action. Elles sont interprétées comme étant des données.
- **Le mécanisme** : effectue la transformation (nous pouvons interpréter ainsi : « le mécanisme est le processeur », l'action étant « le processus »).
- **Le contrôle** : n'est pas transformé par l'action mais permet la transformation. Il peut être vu comme des paramètres ou un déclencheur

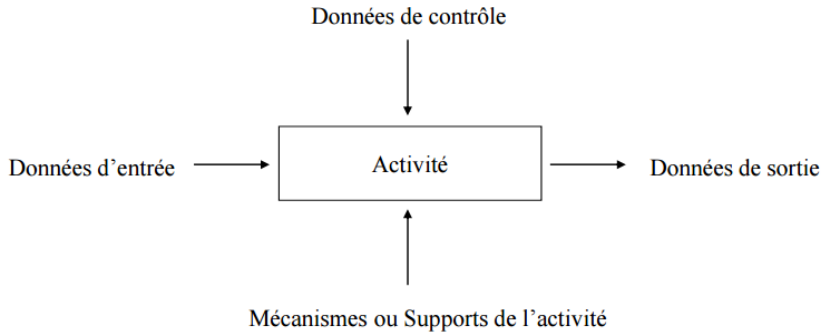


Figure 1 Schéma de base d'un Actigramme

Le schéma de base d'un datagramme est représenté dans la figure 2 et il est composé de :

- **La boîte** qui représente les données.
- **Les entrées** représentant les actions qui produisent les données de la boîte.
- **Les sorties** qui représentent les actions qui utilisent les données de la boîte.
- **Le mécanisme** qui est le support des données.

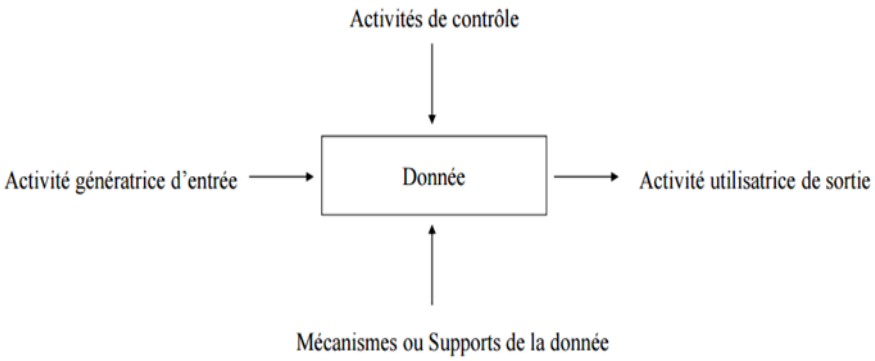


Figure 2 Schéma de base d'un Datagramme

1.3.2.3. Description de la méthode

Au départ, le système est représenté par un module ou boite initiale (A-0) qui est éclatée en plusieurs boîtes représentant le diagramme (A0). Chaque boite du niveau précédent est décomposée en plusieurs autres diagrammes (A1, A2,...). Cette décomposition s'arrête quand le niveau de description souhaité est atteint. Dans le modèle SADT, le nombre de boîtes pour chaque niveau est compris entre 3 et 6.

La démarche d'analyse est donc (Sindjui, 2014):

- descendante car le système est décomposé à partir de sa globalité ;
- modulaire car chaque fonctionnalité est rattachée à un module ;
- Hiérarchique car chaque fonction est ordonnée par rapport aux autres ;

La figure 3 montre un modèle SADT.

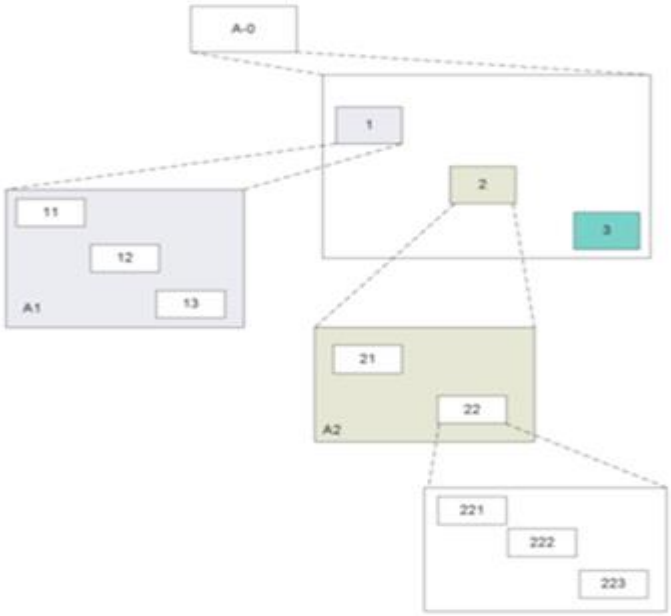


Figure 3 Modèle SADT (Sindjui, 2014)

1.3.3. Application de la méthode SADT aux systèmes étudiés

Dans cette partie nous allons appliquer la méthode SADT décrite sur les trois systèmes critiques identifiés lors de l'analyse des risques préliminaires effectués au sein de l'entreprise (Daoud, 2015).

1.3.3.1. Système de refroidissement de l'alternateur

Lors du fonctionnement de l'alternateur (générateur), celui-ci chauffe selon la puissance fournie au réseau. Il existe plusieurs causes de l'échauffement : les pertes par frottements dans le palier

et entre les balais et les bagues, résistance à la rotation du rotor dans le fluide de refroidissement, la chaleur de la turbine transmise par conduction le long de l'arbre, etc.

Pour ne pas atteindre des températures qui peuvent endommager le bobinage, on utilise un circuit appelé « circuit de refroidissement » entraînant un fluide. Les constructeurs ont opté dans la centrale de Hamma II pour un refroidissement avec de l'hydrogène.

Tous les composants de l'unité sont montés sur un traîneau (SKID) et relié par une tuyauterie à la fourniture du gaz et au générateur.

Le stockage de l'hydrogène a pour but de maintenir automatiquement la pression requise de l'hydrogène ainsi que sa pureté pendant le fonctionnement.

On refroidit l'hydrogène par l'eau déminéralisée dans des aèro-réfrigérants. Quand l'eau traverse les quatre échangeurs, elle absorbe la chaleur de l'hydrogène qui reçoit la fraîcheur et la transmet au générateur.

Au moment où le générateur doit être vidangé de l'hydrogène pour des opérations de maintenance, ce dernier est tout d'abord chassé par CO_2 et ensuite le CO_2 est chassé par l'air. L'emploi du CO_2 vise à éviter, à tout moment, la formation d'un mélange explosif hydrogène-air pendant le remplissage ou lors de la vidange.

Le schéma P&ID du système de refroidissement est présenté dans le l'annexe 1.

Les actigrammes et le datagramme concernant le système de refroidissement à hydrogène sont présentés en annexe 2.

1.3.3.2. Système fuel

Le système fuel est un système de secours. Il fournit l'huile combustible aux brûleurs et contrôle le volume de combustible injecté dans la chambre de combustion. Au cours de l'arrêt, il arrête de manière stable et fiable le débit de l'huile combustible. Le fuel alimente les centrales (les deux groupes) selon deux modes :

- Mode diffusion : Ce mode est activé lorsque la température mesurée à l'échappement est inférieure à 480°C.
- Mode pré-mixte : Quand la température d'échappement mesurée par les thermocouples est supérieure à 480°C, la soupape de la ligne pré-mixte s'ouvre (la soupape de la ligne de diffusion reste ouverte).

Quant à la ligne de retour, elle permet le retour de l'huile combustible non-brulée.

La centrale électrique Hamma II comporte deux cuves de stockage du fuel d'une capacité de 100 m^3 chacune et disposant d'une rétention étanche commune (fosse en béton) d'un volume d'environ 300 m^3.

L'actigramme et le datagramme concernant le système fuel sont présentés en annexe 2.

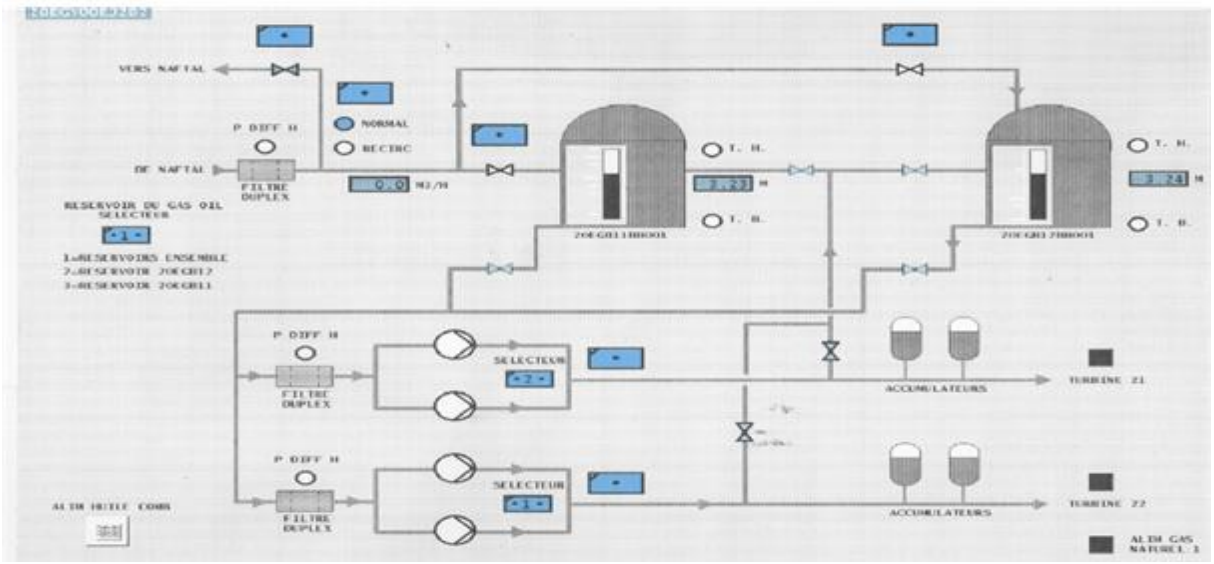


Figure 4 Plan parcellaire du système fuel

1.3.3.3. Poste gaz

C'est le système principal utilisé dans la centrale. L'ensemble du poste gaz de détente, les réchauffeurs, les séparateurs, les filtres et le compteur sont montés sur une plate-forme en béton.

Tableau 1 Caractérisation du poste gaz

Débit poste de détente	120000 m^3h^{-1}
Pression amont détente	35-70 Bar
Pression aval détente	30-32 Bar
Nombre de ligne total	4
Nombre de ligne détente par turbine	1
Débit maximal par ligne	1
Nombre de réchauffeur du gaz par turbine	2(1 en service, 1 en stand-by)

Les éléments principaux constituant le poste gaz (Figure 5) sont :

- Réservoir condensât.
- Séparateur primaire : sa fonction est de débarrasser le gaz d'alimentation des impuretés liquides et solides.

- Filtre à gaz : ils ont pour fonction de séparer le gaz d'alimentation des impuretés solides plus fines en arrivée.
- Réchauffeur.
- Quatre lignes de détente (Rampes) : Le détendeur a pour but de décomprimer le gaz en haute pression à une valeur plus basse et de la maintenir constante aux différentes conditions de débit. - Système de comptage du gaz.
- Le séparateur final : constitue la dernière opération de traitement du gaz en séparant les dernières impuretés liquides et solides apparues après la détente et baisse de température.

L'actigramme et le datagramme concernant le système gaz sont représentés en annexe 2.

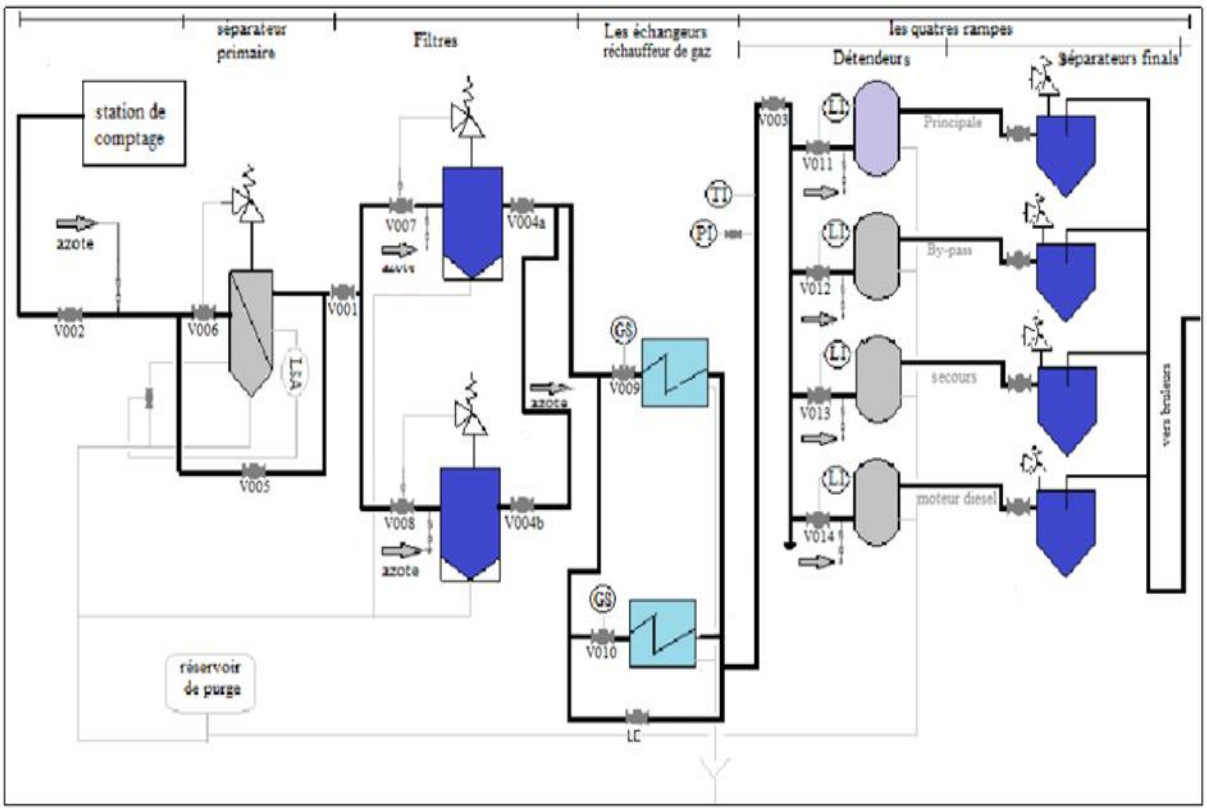


Figure 5 Plan parcellaire du circuit gaz

Conclusion

Nous avons pu à travers ce chapitre situer le champ de notre étude et déterminer les systèmes critiques (système fuel, poste gaz et circuit de refroidissement à hydrogène) induisant les risques majeurs. Par ailleurs, l'analyse fonctionnelle effectuée par la méthode SADT nous a permis de décomposer les systèmes et de définir les différents flux de données et de matières propre à chaque système et qui représentent des informations indispensables pour l'accomplissement des prochaines étapes de notre étude.

Chapitre 2 : Evaluation des risques

Introduction

L'évaluation des risques est la phase finale d'un processus de prise de connaissance sur les risques (ISO 12100, 2010). Elle permet de se positionner et de porter un jugement sur la sécurité d'un équipement, d'une installation ou de tout autre aménagement sur les lieux du travail.

La difficulté reste l'évolution des causes, de plus en plus nombreuses, sournoises et difficiles à pondérer du fait de la complexité des situations. Cette difficulté a été surmontée, par la mise en place de méthodes systématiques permettant de tenir compte de l'ensemble des paramètres régissant un processus et des facteurs pouvant influer son fonctionnement. Ce qui permet d'identifier de la manière la plus exhaustive possible les dangers qui menacent le système.

La deuxième difficulté qui surgit concerne l'étape de l'estimation des risques. Les connaissances utilisées pour la quantification des risques sont généralement issues du retour d'expérience qui s'avère souvent insuffisant pour des installations complexes mettant en jeu plusieurs processus où les accidents et les défaillances sont rares. Dans ce cas, les méthodes usuelles utilisées dans les études de sûreté de fonctionnement ne sont plus adaptées. (Wang, West, & Mannan, 2004) La validité des résultats des études dépend donc de la prise en compte totale ou partielle de l'imperfection des connaissances utilisées. Cela exige des méthodes qui permettent la modélisation et la manipulation de ces imperfections. A cet égard, plusieurs théories de représentation des connaissances imparfaites ont été développées : la théorie des probabilités, la théorie des ensembles flous, la théorie des possibilités et la théorie de l'évidence. (Sellak, 2007)

Nous avons choisi d'utiliser dans notre étude, le système de logique floue avec fuzzification et défuzzification, utilisé dans la plupart des études (Guimaraes & Lapa, 2006).
Ce chapitre est organisé en deux parties. Dans la première partie, des notions sur la logique floue sont présentées, ainsi que le système d'inférence de Mamdani.
Cette approche est utilisée pour caractériser le comportement des systèmes réels qui ont comme entrées des variables linguistiques et des règles floues.
Dans la deuxième partie, la méthode HazOp Hybride utilisant l'inférence floue est développée. Elle sera appliquée aux processus critiques de la centrale électrique HAMMA II afin d'identifier, d'estimer et d'évaluer les différents scénarios.

2.1. Représentation des connaissances imparfaites

Dans cette partie nous allons décrire les formes d'imperfection de connaissances ainsi que le concept de la logique flou.

2.1.1. Formes d'imperfection de connaissances

Les connaissances dont nous disposons sur un système quelconque, pris au sens d'un ensemble d'éléments en relation les uns avec le autres et interférant avec leur environnement, sont en général imparfaites (Meunier, 1995).

L'imperfection dans les connaissances peut être divisée en trois formes principales (Meunier, 1995) :

- Les incertitudes qui représentent un doute sur la validité d'une connaissance ;
- Les imprécisions qui correspondent à une difficulté dans l'énoncé ou dans l'obtention de la connaissance. Ces imprécisions sont aussi appelées « incertitudes du type épistémique » ;
- Les incomplétudes sont des absences totales ou partielles de connaissances sur certaines caractéristiques du système.

2.1.2. Esquisse des théories de représentation des connaissances imparfaites

En ce qui concerne l'incertain, il a d'abord été abordé par la notion de probabilité dès le XVIIme siècle par Pascal et Fermat. La théorie des probabilités fournit une structure mathématique pour l'étude des phénomènes qui présentent des incertitudes aléatoires. Le problème de l'imprécision a été traité par le calcul d'erreurs, restreint aux imprécisions de caractère numérique. (Sellak, 2007) En 1965, Lotfi Zadeh (Zadeh, 1965), Professeur à l'université de Berkley en Californie, a introduit la notion de sous ensemble flou dans une généralisation de la théorie classique des ensembles. Il a ensuite introduit, à partir de 1978 (Zadeh, 1978) la théorie des possibilités qui a été développée par Dubois et Prade (Dubois & Prade, 1988); elle permet de traiter les incertitudes sur les connaissances. L'association de la théorie des possibilités à la théorie des ensembles flous permet le traitement des connaissances à la fois imprécises et incertaines. La théorie des fonctions de croyances permet aussi de traiter ces deux types d'imperfections (Dubois & Prade, 1988), elle est basée sur la modélisation et la quantification de la crédibilité attribuée à des faits. Elle définit le degré avec lequel un événement est crédible ou plausible.

La théorie des probabilités constitue le plus ancien formalisme permettant de traiter les incertitudes dans les connaissances imparfaites. C'est un outil efficace pour le traitement des incertitudes aléatoires et les cas où nous disposons d'une bonne connaissance des événements

et de leurs événements contraires. Elle ne peut cependant pas traiter les imprécisions qui sont une autre forme d'imperfection des connaissances (Dubois & Prade, 1988).

Dans ce qui suit, on introduit la notion des ensembles flous qui permet de traiter, de façon souple, l'aspect imprécis et vague des connaissances imparfaites.

2.1.3. Théorie des ensembles flous

Dans cette section, nous présentons succinctement les concepts fondamentaux de la logique floue qui sont en relation avec les travaux du présent mémoire.

2.1.3.1. Notion d'ensemble flou

Le concept d'ensemble flou (Zadeh, 1965) a été introduit pour éviter les passages brusques d'une classe à une autre et permettre l'appartenance partielle à chacune d'elles.

La définition de l'ensemble flou répond au besoin de représenter des connaissances imprécises telles que celles exprimées en langage naturel. Le caractère graduel des ensembles flous est basé sur l'idée que, plus on se rapproche de la caractérisation typique d'une classe, plus l'appartenance à cette classe est forte (ex., 20 ans caractérise bien la jeunesse, 60 ans ne caractérise plus cette classe d'âge).

Le concept d'ensemble flou permet de traiter

- des classes aux limites mal définies (catégories d'appréciation perçue par un observateur) ;
- des classes intermédiaires entre le "tout" et le "rien" (ex., "presque certain") ;
- le passage progressif d'une classe à une autre (ex., du "petit" au "grand", du "faible" au "fort") ;
- des valeurs approximatives (ex., "autour de 13 de moyenne", "environ 5m de distance"). (Sellak, 2007)

Définition :

Soit $\tilde{U}$ un ensemble référentiel et soit x un élément de $\tilde{U}$. Un sous-ensemble $\tilde{A}$ de $\tilde{U}$ est défini par une fonction d'appartenance $\mu_{\tilde{A}}(x)$ qui prend ses valeurs dans l'intervalle [0, 1]. Cette fonction donne le degré d'appartenance de x dans $\tilde{A}$. Un ensemble ordinaire est un cas particulier de l'ensemble flou ($\mu_A(x)$ ne prend que 0 et 1). Formellement, l'ensemble flou $\tilde{A}$ peut s'écrire comme :

$$\tilde{A} = \{(x, \mu_{\tilde{A}}(x)),\ x \in \tilde{U}\} \qquad (2.1)$$

2.1.3.2. Propriété d'un ensemble flou

Les caractéristiques de l'ensemble flou de $\tilde{U}$ *(figure 6)* les plus utiles pour le décrire sont celles qui montrent à quel point il diffère d'un ensemble classique de *U*. Citons les caractéristiques suivantes :

- *Support d'un ensemble flou* : le support d'un ensemble flou, noté *supp*($\tilde{A}$) est l'ensemble des éléments de $\tilde{U}$ qui appartiennent, au moins un peu, à $\tilde{A}$. C'est la partie de $\tilde{A}$ sur laquelle la fonction d'appartenance de $\tilde{A}$ n'est pas nulle :

$$supp(\tilde{A}) = \{x \in \tilde{U} \,/\, \mu_{\tilde{A}}(x) \neq 0\} \qquad (2.2)$$

- *Hauteur d'un ensemble flou :* la hauteur, notée *h($\tilde{A}$)*, d'un ensemble flou est le plus fort degré avec lequel un élément de $\tilde{A}$ appartient à $\tilde{A}$, c'est-à-dire la plus grande valeur prise par sa fonction d'appartenance.

$$h(\tilde{A}) = supp_{x \in \tilde{A}}\, \mu_{\tilde{A}}(x) \qquad (2.3)$$

- *Ensemble flou normalisé :* l'ensemble flou $\tilde{A}$ de $\tilde{U}$ est dit normalisé si sa hauteur *h($\tilde{A}$)* est égale à 1, c'est à dire contenant des éléments qui n'appartiennent qu'à lui-même.

- *Noyau d'un ensemble flou :* le noyau de l'ensemble flou normalisé $\tilde{A}$, noté *noy*($\tilde{A}$), est l'ensemble des éléments de $\tilde{U}$ pour lesquels la fonction d'appartenance de $\tilde{A}$ vaut 1.

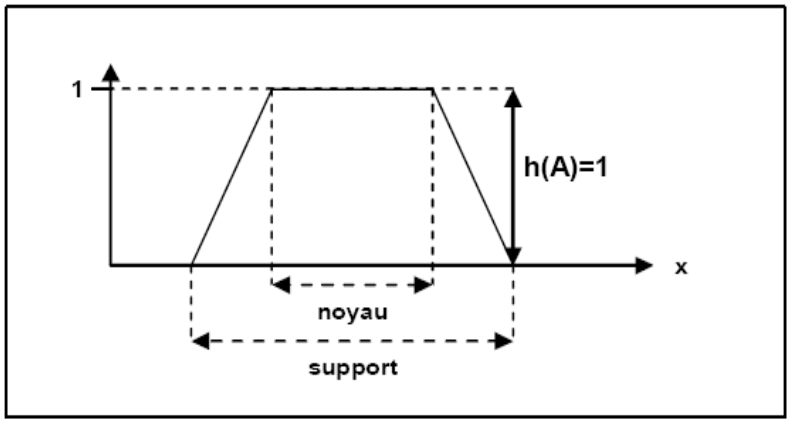


Figure 6 Support, hauteur et noyau d'un ensemble flou

2.1.3.3. Fonction d'appartenance

Les ensembles flous peuvent être définis en leur affectant une fonction continue pour décrire analytiquement ou graphiquement l'appartenance. De ce fait, la représentation des ensembles flous dépend du type de la fonction d'appartenance retenu. Pr. Lotfi Zadeh (Zadeh, 1965) a

proposé une série de fonctions d'appartenance scindée en deux groupes : les fonctions d'appartenance «linéaires» et les fonctions d'appartenance « courbées » ou de forme « gaussienne ».

- La fonction d'appartenance Triangulaire ;
- La fonction d'appartenance Singleton ;
- La fonction d'appartenance Gamma ;
- La fonction d'appartenance Trapézoïdale ;
- La fonction d'appartenance Gaussienne.

Les fonctions d'appartenance les plus répandues sont illustrées par la (figure 7)

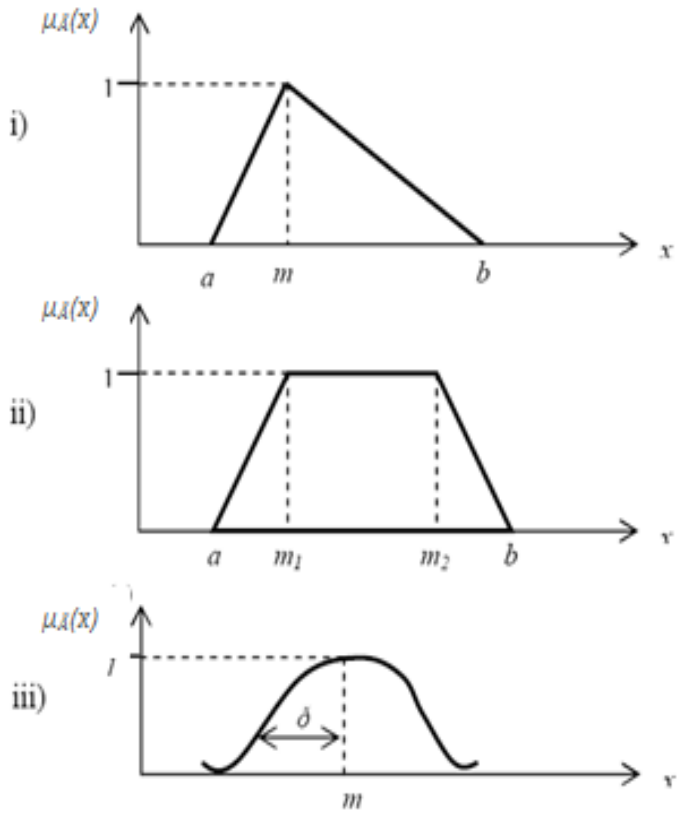


Figure 7 Fonctions d'appartenance : i) Triangulaire ii) Trapézoïdale iii) Gaussienne

- La fonction d'appartenance Triangulaire de la figure ci-dessus est exprimée comme suit :

$$\mu_{\tilde{A}}(x) = \frac{(x-a)}{(m-a)} \qquad a \leq x < m$$

$$= \quad 1 \qquad\qquad x = m \qquad\qquad (2.4)$$

$$= \frac{b-x)}{(b-m)} \qquad m < x \leq b$$

- La fonction d'appartenance Trapézoïdale de la figure ci-dessus est exprimée comme suit :

$$\mu_{\tilde{A}}(x)) = \frac{(x-a)}{(m_1-a)} \qquad a \leq x \leq m_1$$

$$= 1 \qquad m_1 \leq x \leq m_2 \qquad (2.5)$$

$$= \frac{(b-x)}{(b-m_2)} \qquad m_2 \leq x \leq b$$

- La fonction d'appartenance Gaussienne de la figure ci-dessus est exprimée comme suit :

$$\mu_{\tilde{A}}(x) = exp\left(\frac{(-x-m)^2}{2\sigma^2}\right) \qquad (2.6)$$

2.1.3.4. Opération sur les ensembles flous

La théorie des ensembles flous propose plusieurs opérateurs ensemblistes. Les principaux opérateurs et relations flous sont présentés ci-dessous. (Zadeh, 1965)

i. **Inclusion** : On dit que $\tilde{A}$ est inclus dans $\tilde{B}$, et on note $\tilde{A} \subseteq B$, si et seulement si

$$\forall x \in \tilde{U} \qquad \mu_{\tilde{A}}(x) \leq \mu_{\tilde{B}}(x) \qquad (2.7)$$

ii. **Egalité** : On dit que $\tilde{A}$ et $\tilde{B}$ sont égaux, et on note $\tilde{A} = \tilde{B}$, si et seulement si :

$$\forall x \in \tilde{U} \qquad \mu_{\tilde{A}}(x) = \mu_{\tilde{B}}(x) \qquad (2.8)$$

iii. **Complémentation** : On dit que $\tilde{A}$ et $\tilde{B}$ sont complémentaires, et on note $\tilde{A} = \overline{\tilde{B}}$ ou $\overline{\tilde{A}} = \tilde{B}$, si et seulement si :

$$\forall x \in \tilde{U} \qquad \mu_{\tilde{B}}(x) = 1 - \mu_{\tilde{A}}(x) \qquad (2.9)$$

iv. **Intersection** : On définit l'intersection de $\tilde{A}$ et $\tilde{B}$, et on note $\tilde{A} \cap \tilde{B}$ par le plus grand ensemble flou de contenu à la fois dans $\tilde{A}$ et $\tilde{B}$, c'est-à-dire :

$$\forall x \in \tilde{U} \qquad \mu_{\tilde{A}\cap\tilde{B}}(x) = \min\left(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)\right) \qquad (2.10)$$

v. **Réunion** : On définit l'union ou la réunion de $\tilde{A}$ et $\tilde{B}$, et on note $\tilde{A}$ U $\tilde{B}$, par le plus petit ensemble flou de *U* qui contient à la fois $\tilde{A}$ et $\tilde{B}$, c'est-à-dire

$$\forall x \in \tilde{U} \qquad \mu_{\tilde{A}\cap\tilde{B}}(x) = \max\left(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)\right) \qquad (2.11)$$

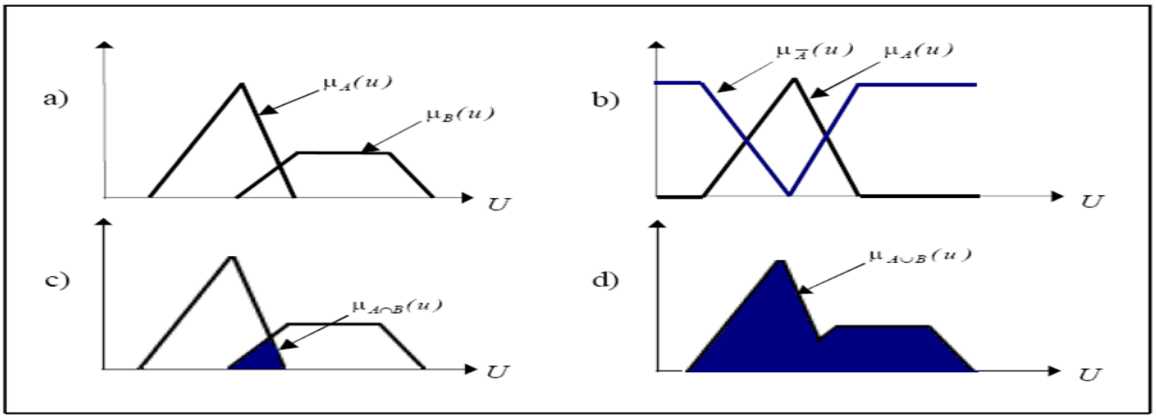


Figure 8 Illustration de quelques opérations sur les ensembles flous : a) Ensembles flous A et B b) $\widetilde{\overline{A}}$ c) Intersection d) Réunion

L'algèbre des ensembles flous est la même que celle des ensembles ordinaires, sauf que le tiers- exclu n'est plus vérifié. En effet, on y retrouve les opérations suivantes :

a) Commutativité :

$$\tilde{A} \cap \tilde{B} = \tilde{B} \cap \tilde{A} \qquad (2.12)$$

$$\tilde{A} \cup \tilde{B} = \tilde{B} \cup \tilde{A} \qquad (2.13)$$

b) Associativité :

$$\tilde{A} \cap (\tilde{B} \cap \tilde{C}) = (\tilde{A} \cap \tilde{B}) \cap \tilde{C} \qquad (2.14)$$

$$\tilde{A} \cup (\tilde{B} \cup \tilde{C}) = (\tilde{A} \cup \tilde{B}) \cup \tilde{C} \qquad (2.15)$$

c) Distributivité :

$$\tilde{A} \cap (\tilde{B} \cup \tilde{C}) = (\tilde{A} \cap \tilde{B}) \cup (\tilde{A} \cap \tilde{C}) \qquad (2.16)$$

$$\tilde{A} \cup (\tilde{B} \cap \tilde{C}) = (\tilde{A} \cup \tilde{B}) \cap (\tilde{A} \cup \tilde{C}) \qquad (2.17)$$

d) Involution :

$$\tilde{\bar{\bar{A}}} = \tilde{A} \qquad (2.18)$$

e) Lois de Morgan :

$$\overline{\tilde{A} \cap \tilde{B}} = \tilde{\bar{A}} \cup \tilde{\bar{B}} \qquad (2.19)$$

$$\overline{\tilde{A} \cup \tilde{B}} = \bar{\tilde{A}} \cap \bar{\tilde{B}} \qquad (2.20)$$

Le tiers-exclu n'étant pas vérifié par les ensembles flous (illustré dans la figuré 9).

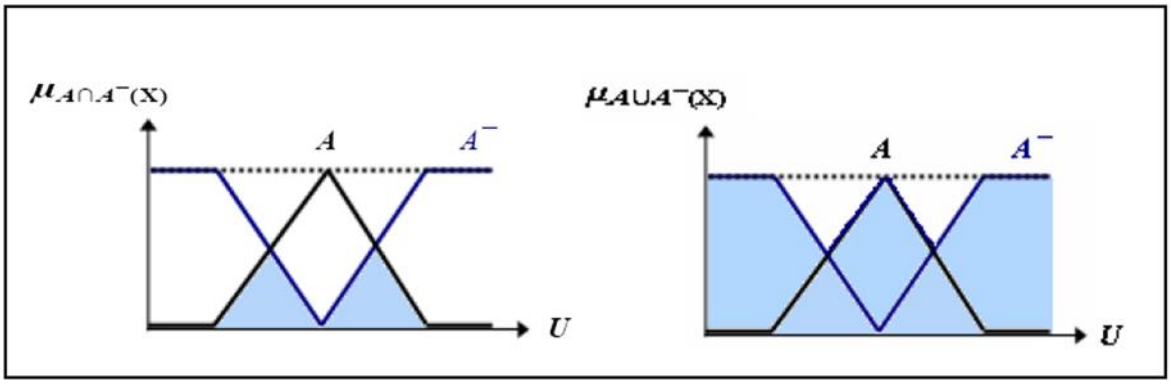


Figure 9 Illustration de la propriété du tiers-exclu

2.1.3.5. Notion de variable linguistique

Le concept de variable linguistique (Zadeh, 1975) est utilisé dans la caractérisation des phénomènes qui sont si complexes ou si mal définis qu'ils ne peuvent être décrits par des termes quantitatifs conventionnels. Ainsi, les valeurs de la variable linguistique sont des termes linguistiques du langage naturel, lesquelles sont modélisés par des ensembles flous. Plus spécifiquement, ces derniers représentent des restrictions sur les valeurs de la variable linguistique et peuvent être vus comme résumant les différentes catégories d'éléments d'un univers de discours (i.e., l'ensemble référentiel).

2.1.3.6. Relation floue

Les relations binaires floues, représentent l'un des concepts les plus importants du point de vue application. Elles généralisent la notion de relation classiquement définie sur les ensembles. Elles mettent en évidence des liaisons imprécises ou graduelles entre les éléments d'un même ensemble. (Zadeh, 1975)

Définition

Soit *U* x *V* le produit cartésien de deux référentiels *U* et *V*. On appelle relation binaire floue entre *U* et *V*, un ensemble flou *R* de *U* x *V*, de fonction d'appartenance μ_R (*x*,*y*) prenant ces valeurs dans l'intervalle [0,1].

Si *U* et *V* sont finis, μ_R (*x*, *y*) peut être représentée par une matrice floue ou par son graphe associé. Si *U* = *V*, *R* est une relation floue définie entre les éléments d'un même référentiel.

Exemple

Soit V =*U* = {1, 2, 3} un ensemble. La fonction d'appartenance μ_R de la relation R :

"approximativement égal", est définie par :

$$\mu_R(x, y) = 1 \quad \text{si } x=y$$

$$\mu_R(x, y) = 0.8 \quad \text{si } |x-y| = 1 \qquad (2.21)$$

$$\mu_R(x, y) = 0.3 \quad \text{si } |x-y| = 2$$

Cette relation peut être représentée aussi sous forme matricielle (tableau 2) :

Tableau 2 Présentation matricielle de la relation R

U / U | $\mu_{R(x,y)}$	1	2	3
1	1	0.8	0.3
2	0.8	1	0.8
3	0.3	0.8	1

2.1.3.7. Implication floue

Une expression conditionnelle du type « Si *X* est *A* Alors *Y* est *B* », où *A et B* sont des ensembles flous sur l'univers *U,* respectivement *V,* est une relation floue *R* sur le produit cartésien *U* x *V qui* est appelée « Règle floue ». *X* et *Y* étant les variables linguistiques décrites respectivement par *A* et *B,* et *R* est caractérisée par une fonction d'appartenance $\mu_R(x, y)$.
Une règle floue est basée sur la notion d'implication floue. Ainsi, la règle « Si *X* est *A* alors *Y* est *B* » peut s'écrire comme « (x, y) est $A \rightarrow B$ », où $A \rightarrow B$ est une implication floue se caractérisant par la valeur de vérité $\mu_{A\rightarrow B}(x, y)$, qui n'est que $\mu_R(x, y)$, soit :

$$\mu_R(x, y) = \mu_{A\rightarrow B}(x, y) = \Phi(\mu_A(x), \mu_B(y)) \qquad (2.22)$$

Où Φ est un opérateur d'implication floue spécifique. Il existe de nombreux opérateurs en logique floue. L'opérateur de Mamdani (Mamdani & Assilian, 1975) est le plus utilisé dans les applications pratiques et est exprimé par une conjonction qu'est le minimum, soit :

$$\Phi(\mu_A(x), \mu_B(y)) = \min(\mu_A(x), \mu_B(y)) \qquad (2.23)$$

2.1.3.8. Système d'inférence de Mamdani

A l'opposé des méthodes quantitatives qui requièrent des équations pour modéliser les comportements des systèmes réels, la logique floue, elle, peut caractériser ces comportements par des variables linguistiques et des règles floues appartenant respectivement aux concepts

des ensembles flous et des systèmes d'inférence floue.

Les systèmes d'inférence floue ont fait leur preuve dans de nombreuses applications et dans plusieurs domaines tels que le contrôle automatique, le traitement de données, l'analyse de décision, les systèmes experts, et les études de sécurité (Sellak, 2007).

Parmi ces systèmes d'inférence, celui proposé par Mamdani et Assilian (Mamdani & Assilian, 1975) est le plus rencontré dans la résolution des problèmes à base de règles floues.

La méthodologie générale des Systèmes d'Inférence Floue (SIF ou FIS en anglais) est donnée dans la figure 10

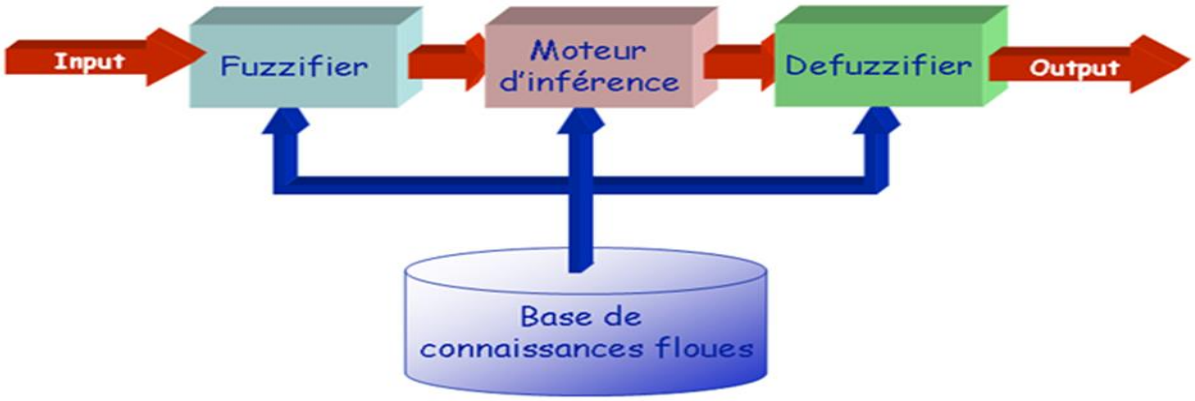


Figure 10 Présentation générale d'un système d'inférence flou (SIF ou FIS)

2.1.3.9. Méthodologie du système d'inférence de Mamdani

Le système d'inférence de Mamdani peut être décrit comme suit (Mamdani & Assilian, 1975) : supposons une base de règles constituée de *n* Si/Alors règles floues avec des entrées multiples constituant les prémisses (antécédents) et une sortie unique constituant la conclusion (Multiple Inputs and Single Output : MISO). Chaque règle *Ri* (*i* =1, …, *n*) est donc de la forme :

$$R_i : \text{si } X_1 \text{ est } A_{i1} \text{ et } \ldots \text{ et } X_m \text{ est } A_{im} \text{ alors } Y \text{ est } B_i$$

Où les X_j (j=1, …, m) et Y sont des variables linguistiques définies respectivement sur les univers $U = U_{1x} \ldots U_{mx}$ et V. Les ensembles flous A_{ij} sont des éléments de la partition linguistique T_j de U_j (univers de la variable X_j).

Pour un vecteur ordinaire d'entrée $u^0 = (u_1^0, \ldots, u_m^0)$, la valeur de la sortie est déterminée suivant les trois étapes suivantes :

- **Fuzzification**

La fuzzification est l'opération qui consiste à convertir une valeur d'entrée ordinaire u_j^0 en sa représentation symbolique, c'est à dire, déterminer les ensembles floues A_{ij} auxquels elle appartient et le degré d'appartenance $\mu_{Aij}(u_j)$ de u_j pour chaque entrée A_{ij}

- **Inférence floue**

Le moteur d'inférence transforme les ensembles flous d'entrée (issus de l'opération de fuzzification) en des ensembles flous de sortie en utilisant la base de règles linguistiques et les opérations d'implication floue.

La sortie floue est obtenue par la méthode d'inférence max-min selon les sous-étapes suivantes :

i) *Repérage du niveau d'activation de chaque règle :* La valeur de vérité attribuée à l'antécédent" (prémisse) de chaque règle *Ri* est calculée puis appliquée à la partie "conclusion" de cette règle. Le calcul se fait comme suit :

$$\alpha_{ij} = \min_j(\mu_{Aij}(\mu_j^0)) \tag{2.24}$$

i) *Inférencement* : Dans l'étape d'inférence, la sortie *Bi* de chaque règle *Ri* est calculée à l'aide de l'opérateur de conjonction (min), d'où $B_I = \alpha_i \wedge B_i$ est donné par :

$$\mu_{\acute{B}i}(v) = \min(\alpha_i, u_{Bi}(v)) \tag{2.25}$$

ii) *L'agrégation* : Pour obtenir la sortie globale du système, les sorties propres à chaque règle sont combinées à l'aide de l'opérateur union. Ainsi $B' = \cup_i B_i = \cup (\alpha_i \wedge B_i)$, avec la fonction d'appartenance :

$$\mu_{\acute{B}}(v) = \max_{i=1,\ldots,n} \mu_{\acute{B}_I}(v) \tag{2.26}$$

- **Défuzzification**

L'étape de défuzzification permet de transformer la sortie floue en une valeur numérique v^0 représentative de *Y* dans *B*. Différents algorithmes de défuzzification ont été développés et il n'y a pas un algorithme meilleur pour toutes les applications. Cependant, la

méthode de « la moyenne des maximums » et la méthode du « centre de gravité » sont le plus fréquemment utilisées. Selon cette dernière, la valeur représentative est donnée par :

$$v^0 = \frac{\int_{v \in V} \mu_{\acute{B}}(v).v.dv}{\int_{v \in V} \mu_{\acute{B}}(v).dv} \qquad (2.27)$$

2.2. Application de la logique floue dans l'évaluation des risques

Du fait du caractère stochastique et incertain du risque, les concepts de la logique floue ont été utilisés juste après leur développement pour le cerner et l'étudier. En effet, quelques années après la publication du premier article sur la logique floue (Zadeh, 1965) Lotfi Zadeh introduisait le concept de la variable linguistique (Zadeh, 1978), et cite l'analyse du risque comme l'un des domaines où il peut être appliqué.

Après cela, d'innombrables travaux ont été publiés, et les concepts de la logique floue ont été utilisés dans toutes les étapes d'analyse du risque (Sellak, 2007).

Dans ce qui suit, nous présenteront la méthode HazOp-RPN utilisant l'inférence floue pour le calcul du RPN.

2.2.1. Méthode HazOp-RPN floue

La méthode HazOp-RPN (*Hazard Operability-Ranking Priority Number*) utilisant l'inférence floue a été proposée pour la première fois par Antonio Guimaraes et Celso Lapa en 2005 (Guimaraes & Lapa, 2006). Ses auteurs la définissent comme une méthode d'évaluation des risques technologiques induits par des déviations dans des paramètres nominaux physiques d'un processus critique évoluant dans un environnement incertain. Cette méthode a été conçue pour être appliquée sur des systèmes passifs, c'est-à-dire ne contenant pas de barrières de protection active, ce qui correspond, en ce point, aux processus sujets de notre étude, où les barrières sont prises en compte dans le prochain chapitre.

2.2.1.1. HazOp conventionnelle

Hazard and Operability Studies (HazOp) est l'une des méthodes d'analyse de risques les plus pratiquées au monde. C'est une méthode inductive adaptée aux systèmes complexes de type thermo-hydrauliques.

2.2.1.1.1. Les étapes de la méthode

La méthode HazOp est constituée des étapes suivantes :

Etape N° 1 : Analyse du système

Cette analyse s'est effectué dans le chapitre précédent avec la méthode SADT afin de déterminer les nœuds représentant chacun une ou plusieurs fonctions suivant les intentions du concepteur et de l'exploitant.

Etape N° 2 : Détermination des déviations

Une déviation est un écart par rapport aux intentions du design et de la conduite des opérations. Elle est obtenue par la combinaison de mots clés et de paramètres donc :

Déviation = Mot-clé + Paramètre

Tel qu'un paramètre est utilisé afin de caractériser l'intention de la conception**.** Le tableau 3 regroupe les paramètres les plus employés dans les études HazOp.

Tableau 3 Exemples de paramètres de la méthode HazOp

Grandeurs physiques mesurables		**Opérations à réaliser**		**Action à réaliser**	**Fontions-situation**
Température	pH	Chargement	Contrôle	Démarrer	Protection
Pression	Volume	Dilution	Séparation	Arrêt	Gel
Niveau	Vitesse	Chauffage	Refroidissement	Echantillonner	Séisme
Débit	Fréquence	Agitation	Transfert	Isoler	Malveillance
Concentration	Quantité	Mélange	Maintenance	Purger	Fuite
Contamination	Temps	Réaction	Corrosion	Fermer	

Les Mots-clés ou mots guide sont joints aux paramètres pour générer les dérives à considérer. Le tableau 4 regroupe la plupart des mots-clés utilisés.

Tableau 4 Les type de dérivation et de mots-clés (CEI 61882, 2001)

Type de dérivation	**Mot-guide/mots clés**	**Exemples d'interprétation**
Négative	Ne pas faire	Aucune partie de l'intention n'est remplie
Modification quantitative	Plus	Augmentation quantitative
	Moins	Diminution quantitative
Modification qualitative	En plus de	Présence d'impuretés – Exécution simultanée d'une autre opération
	Partie de	Une partie seulement de l'intention est réalisée
Substitution	Inverse	S'applique à l'inversion de l'écoulement dans les canalisations ou à l'inversion des réactions chimiques
	Autre que	Un résultat différent de l'intention originale est obtenu
Temps	Plus tôt	Un événement se produit avant l'heure prévue
	Plus tard	Un événement se produit après l'heure prévue
Ordre séquence	Avant	Un événement se produit trop tôt dans une séquence
	Après	Un événement se produit trop tard une séquence

Etape N° 3 : Étude des déviations

Pour chaque nœud, on associe de façon systématique les paramètres aux mots clés pour couvrir de façon exhaustive toutes les dérives potentielles dans l'installation étudiée, qui seront analysées afin de déterminer leurs causes et leurs conséquences.

Etape N° 4 : Détermination des barrières de sécurité

Pour chaque dérive, on examine les moyens visant à détecter cette dernière ainsi que ceux prévus pour en prévenir l'occurrence ou en limiter les effets. Ensuite on propose des recommandations et améliorations.

La méthode HazOp est la seule méthode qui traite de la fiabilité centrée sur les grandeurs physiques naturels (débit, température…) (Guimaraes & Lapa, 2006), c'est pour cette raison qu'elle est la mieux adaptée pour les systèmes thermo-fluides. Mais l'une des insuffisances dont elle souffre, est qu'elle est juste une méthode d'identification et ne constitue pas une aide à la décision. Pour parer à cette insuffisance, le concept du RPN de l'AMDEC est adapté et appliqué pour l'étude HazOp.

2.2.1.2. Ranking Priority Number (RPN)

Les études AMDEC génèrent un index appelé Risk Priority Number (le nombre de priorisation de risque), aussi trouvé dans la littérature sous la dénomination de Risk Priority Ranking (classification de la priorité des risques). Il est calculé pour identifier les principaux modes de défaillance, et servira à l'établissement d'un plan de réduction des risques.

Selon plusieurs auteurs, le RPN conventionnel est composé de :

- La probabilité de l'occurrence de la défaillance (P)
- La gravité de la défaillance sur le système (G)
- Non-Détection (D)

Chaque paramètre constitue une échelle et leur agrégation, donne le nombre de priorisation du risque selon la formule :

$$RPN = P*G*D \tag{2.28}$$

Nous pouvons cependant nous interroger sur certains aspects de cette méthode. Trois principaux problèmes sont à soulever :

- Le premier concerne le processus de cotation des échelles de probabilité, gravité et non détection. Il est constaté que les catégories de ces échelles sont définies de manière franche en leur associant un classement numérique ordinale, ce qui ne s'accorde pas avec la nature incertaine et imprécise de l'information sur les paramètres des situations réelles,

particulièrement en présence d'événements rares ou de systèmes nouveaux en phase de conception. De plus, cette cotation, néglige les effets de confusion entre catégories (i.e., chevauchement des intervalles) qui reflète le raisonnement humain ;

- Le second est dû à la discontinuité des échelles utilisées qui se traduit par des difficultés d'interprétation des résultats de l'évaluation ;
- Le dernier problème concerne la règle de croisement de l'information sur les paramètres P, G et D pour agréger un nombre RPN. Leur produit est couramment utilisé, mains sa signification est fortement contestée pour des échelles ordinales.

C'est à cela que vient répondre les concepts de la logique floue

2.2.1.3. La méthodologie de la HazOp-RPN floue

Les étapes traditionnelles d'une analyse HazOp restent inchangées. Cependant, en intégrant le concept de RPN propre à l'AMDEC, le Hadopi-RPN est défini par :

$$HazOp\_RPN = EOP^* G^*D \qquad (2.29)$$

Les termes de la formule précédente ont une interprétation reliée avec le RPN de l'AMDEC mis à part le paramètre EOP (Estimated Occurrence Probability) qui a été créé pour représenter l'estimation de la probabilité d'occurrence.

L'autre changement qui a été introduit concerne la classification des facteurs de la mesure du risque. Puisque les défaillances dans les procédés industriels passifs sont très rares (Guimaraes & Lapa, 2006), il n'y a pas de bases de données pour qu'un expert puisse construire une table de classification des différents facteurs. La solution à cette question est l'utilisation du système d'inférence floue de Mamdani.

Les différents termes linguistiques reliés à chaque facteur de risque, ainsi que leurs fonctions d'appartenance ont été proposés par Antonio Guimaraes et Celso Lapa (Guimaraes & Lapa, 2006).

L'interprétation des termes linguistiques est présentée dans les tableaux 5 et 6.

Tableau 5 Interprétation des termes linguistique des paramètres gravité et non-détection

Paramètres / **Termes linguistiques**	**Gravité**	**Non-détection**
Mineure	La déviation du paramètre ou la défaillance n'a pas d'effet sur la performance du système.	La déviation reste indétectable jusqu'à la dégradation des performances du système
Faible	La déviation du paramètre ou la défaillance peut causer des petites perturbations mais aucune détérioration n'est observée	La déviation reste indétectable jusqu'à la réduction sévère des performances du système
Modérée	La déviation du paramètre ou la défaillance peut affecter la performance du système	La déviation reste indétectable jusqu'à ce que le système ne puisse pas remplir sa fonction
Elevée	La déviation du paramètre ou la défaillance peut causer des détériorations mineures sur le système et/ou des blessures minimes	La déviation reste indétectable sans avoir fait des inspections et des tests
Très Elevée	La déviation du paramètre peut causer des dommages graves sur le système et/ou peut conduire à des blessures graves et des décès	La déviation reste indétectable même après des inspections et des tests

Tableau 6 Interprétation des termes linguistique du paramètre EOP

Paramètre / **Termes linguistiques**	**EOP**
Impossible	Occurrence impossible pour la défaillance
Très Lointain	Défaillance possible, mais non encore observée
Lointain	Occurrence de la défaillance improbable, même une fois
Probable	Défaillance pouvant survenir une fois
Fréquent	Défaillance pouvant survenir plus d'une fois

Les fonctions d'appartenance triangulaires (a, b, c), les plus communément utilisées, ont été adoptées. Dans différents articles, cette fonction a donnée des résultats satisfaisants dans ce genre de problèmes.

a. Construction des fonctions d'appartenance

Pour construire les différentes fonctions d'appartenance, une question doit être posée : quels éléments x (a, b, c) ont les degrés d'appartenance $\mu(a) = 0$, $\mu(b) = 1$ et $\mu(c) = 0$. Les espaces entre ces trois valeurs sont en relation à l'incertitude par rapport à chaque facteur (EOP, D, G) (Klir & Yuan, 1995)

Les fonctions d'appartenance de la gravité (tableau 7) et de la non-détection (tableau 8) sont très similaires. Par contre, l'incertitude du niveau de EOP (tableau 9) est très grande. La fonction d'appartenance du EOP doit refléter nécessairement cela. Dans ce cas, pour la présenter, nous avons mis de larges intervalles entre les points de la base des fonctions.

Avec la toolbox Fuzzy Logic Designer de matlab[2], nous avons construit graphiquement les fonctions d'appartenance de chaque facteur de risque (figure 11, figure 12 et figure 13).

Tableau 7 Fonctions d'appartenance de la variable Gravité

Termes linguistiques	Niveau	Fonction d'appartenance
Mineure	1	[0 ; 1.515 ; 3.03]
Faible	2	[2.02 ; 3.535 ; 5.05]
Modérée	3	[4 ; 6 ; 8]
Elevée	4	[6.931 ; 8.5 ; 9.902]
Très Elevée	5	[9.09 ; 9.99 ; 10.1]

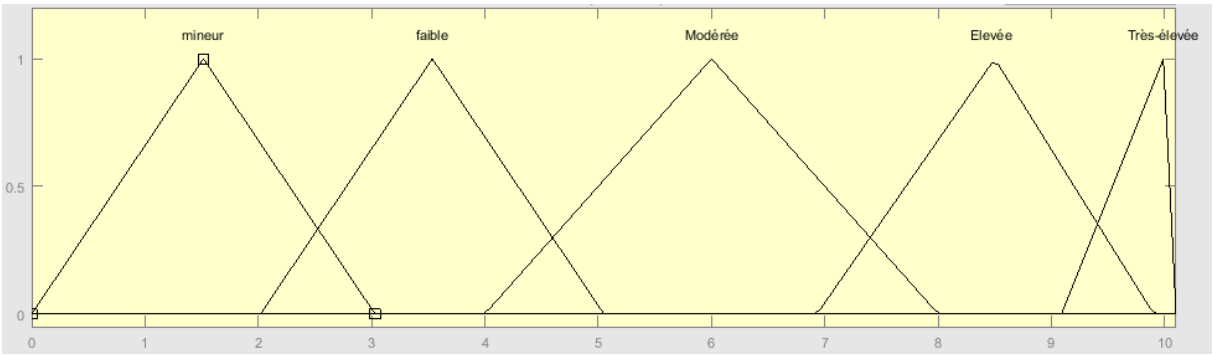


Figure 11 Fonctions d'appartenance de la variable Gravité

Tableau 8 Fonctions d'appartenance de la variable Non-détection

Termes linguistiques	Niveau	Fonction d'appartenance
Mineure	1	[0 ; 1.515 ; 3.03]
Faible	2	[2.051 ; 3.566 ; 5.081]
Modérée	3	[4 ; 6 ; 8]
Elevée	4	[6.931 ; 8.615 ; 9.902]
Très Elevée	5	[9.059 ; 10.1 ; 10.1]

[2] Matlab R2015a

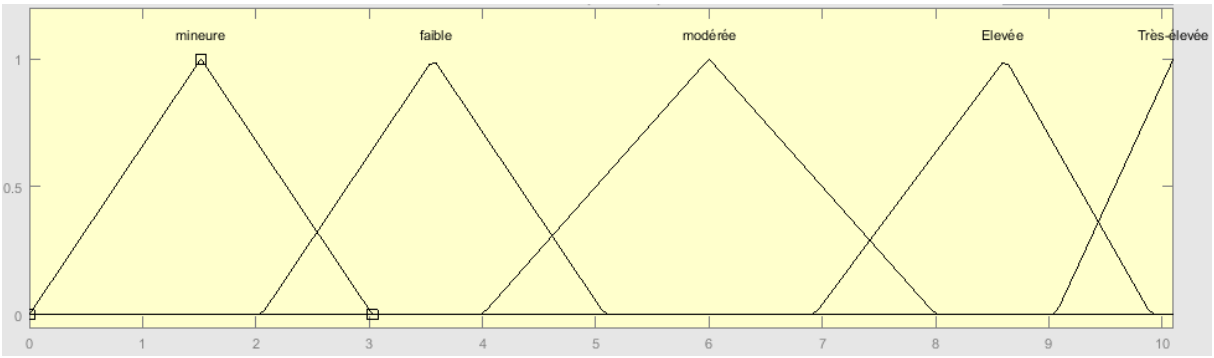


Figure 12 Fonction d'appartenance de la variable Non-Détection

Tableau 9 Fonctions d'appartenance de la variable EOP

Termes linguistiques	Niveau	Fonction d'appartenance
Impossible	1	[0 ; 0 ; 0.1]
Très lointain	2	[0 ; 1 ; 2]
Lointain	3	[1 ; 2 ; 3]
Probable	4	[2 ; 3 ; 4]
Fréquent	5	[3.81 ; 3.96 ; 4.2]

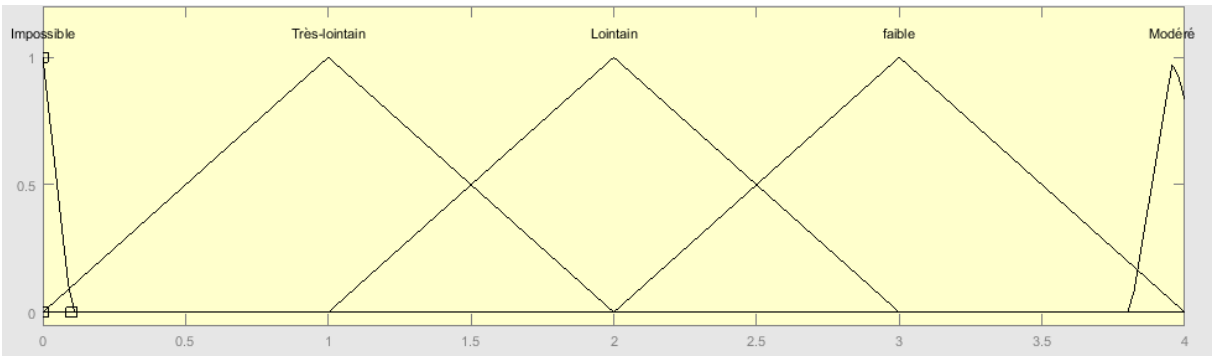


Figure 13 Fonctions d'appartenance de la variable EOP

Le risque (HazOp_RPN) comme sortie de l'AMDEC, peut être linguistiquement exprimé par 9 termes. Les rangs linguistiques ainsi que leurs fonctions d'appartenance sont présentés ci-dessous.

Tableau 10 Fonctions d'appartenance de la sortie HazOp-RPN

Termes linguistiques	Niveau	Rang
Non-existant	1	[0 ; 0 ; 0.1]
Négligeable	2	[0 ; 0.15 ; 0.25]
Très faible	3	[0.15 ; 0.25 ; 0.5]
Faible	4	[0.25 ; 0.5 ; 0.75]
Modéré	5	[0.5 ; 0.75 ; 0.9]
Moins fort	6	[0.75 ; 0.9 ; 1]
Fort	7	[0.75 ; 1 ; 1.5]
Très fort	8	[1 ; 1.5 ; 2]
Majeur	9	[1.5 ; 5 ; 10]

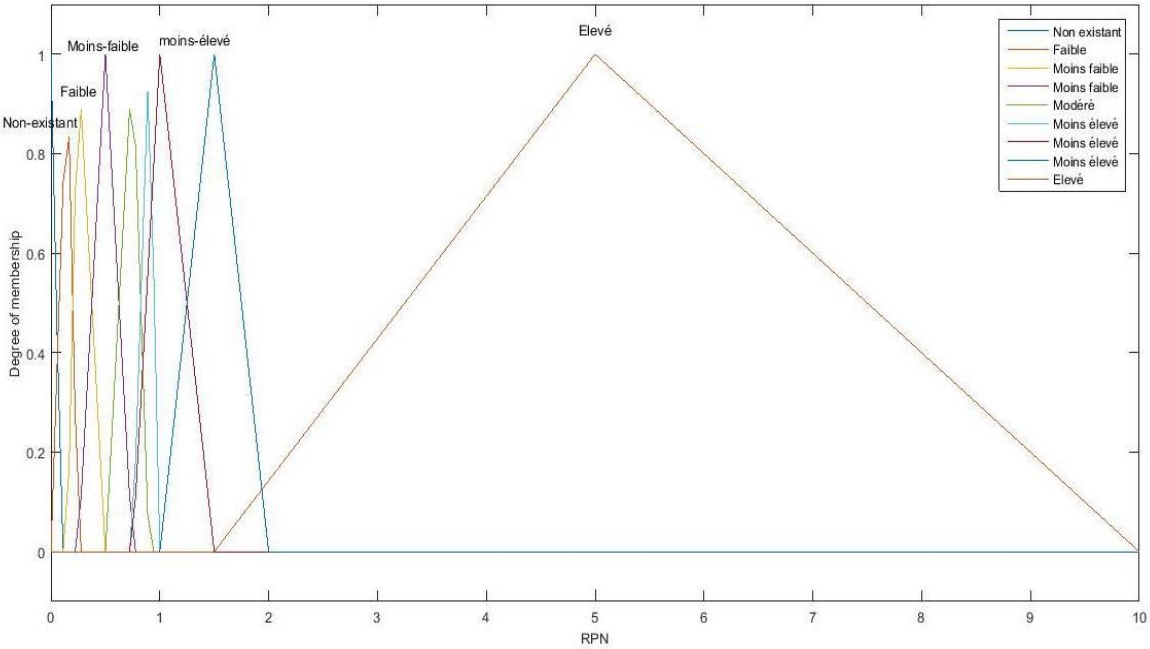


Figure 14 Fonction d'appartenance de la sortie HazOp-RPN

b. L'application de la base des règles floues

Considérons les facteurs : EOP, G et D ainsi que les termes les décrivant (5 termes pour chaque facteur), le système de règle de base floue comportera 125 règles.

Le nombre de règles va être réduit, si le système a été analysé d'une façon simple. Par exemple, considérons ces trois règles :

1. Si EOP est faible et la gravité est modéré et la non-détection est mineure alors le risque est fort.
2. Si EOP est lointain la gravité est modérée et la détection faible, alors le risque est fort.
3. Si EOP est très lointain, la gravité est très élevée et la non-détection est faible alors le risque est fort.

Ces trois règles peuvent être combinées pour lire : Si EOP est faible, la gravité est modérée et la non-détection est mineure ou l'une des combinaisons de ces termes linguistiques alors le risque est fort. En utilisant cette méthode de réduction de règles on atteint un nombre de 16 règles (tableau 11) et les facteurs de risques auront la même importance et les règles le même poids.

Tableau 11 Base de règles floues

EOP	Gravité	Non-détection	RPN
1	0	0	1
3	3	2	6
2	5	1	4
4	3	1	8
3	3	2	8
2	5	1	2
3	3	3	8
3	5	1	7
2	1	3	3
2	5	2	5
4	3	3	9
5	3	3	9
5	4	3	9
5	5	3	9
5	5	4	9
5	5	5	9

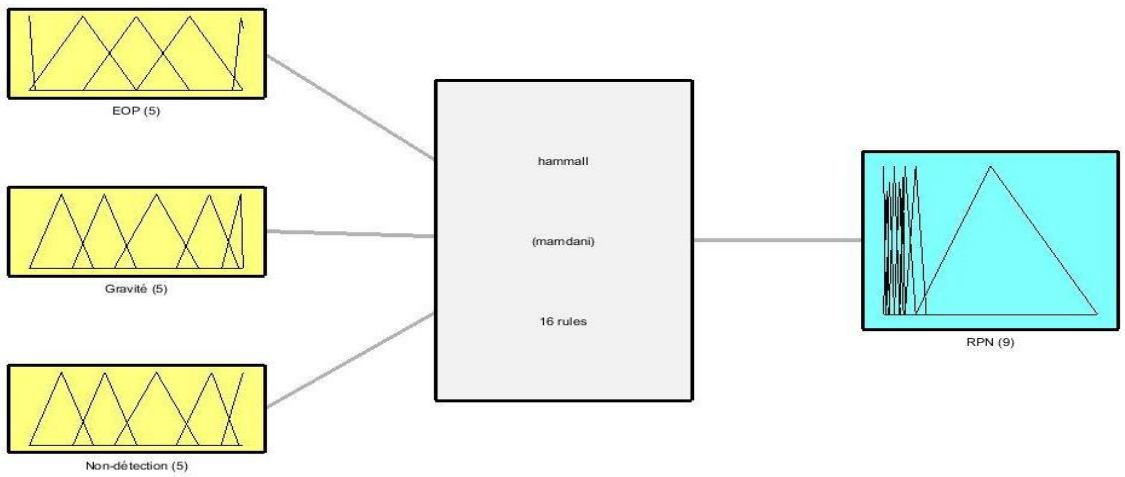


Figure 15 Présentation du système d'inférence de Mamdani sous Matlab

Les calculs de la mémoire du système d'inférence floue FIS générés avec matlab est présentés présenté en annexe 3.

2.2.2.Application de la HazOp-RPN aux cas d'étude

L'application de la méthode HazOp-RPN a été faite pour déterminer les scénarios d'accidents dans les systèmes critiques suivants : système fuel, système de refroidissement à hydrogène de l'alternateur et le poste gaz et l'ensemble des scénarios d'accidents obtenus sont présentés dans les tableaux de l'annexe 4.

La détermination des nœuds et des paramètres de chaque système s'est basée sur la décomposition fonctionnelle effectuée par la méthode SADT.

Le système fuel a été décomposé en 3 nœuds. Les paramètres étudiés pour chaque nœud sont :

- Réservoirs du fuel avec le paramètre : niveau ;
- Pompes avec le paramètre : débit du fuel ;
- Circuit fuel (système fuel) avec le paramètre : débit.

Le système de refroidissement à hydrogène de l'alternateur est constitué de trois nœuds qui sont :

- Circuit de refroidissement avec les paramètres : pression et température ;
- Stockage d'hydrogène avec le paramètre : pression ;
- Générateur H_2/CO_2 avec le paramètre : composition des gaz dans l'alternateur.

Le système poste gaz est décomposé en nœuds

- Circuit gaz avec les paramètres : température pression et débit du gaz ;
- Filtres avec le paramètre : débit du gaz ;
- Echangeur de chaleur avec les paramètres : débit et température de l'eau ;
- Le détendeur avec le paramètre : débit du gaz.

En concertation avec les exploitants de la centrale électrique, nous avons construit les scénarios d'accidents qui peuvent survenir.

Nous avons combiné les paramètres avec les mots-clés pour recenser les déviations pouvant mener à un accident. Ensuite, nous avons identifié les causes et les conséquences de chaque déviation et ainsi construit les scénarios d'accidents.

L'intégration des paramètres, gravité, EOP et non détection a contribué à rendre la méthode HazOp conventionnelle plus quantitative.

Nous avons caractérisé les facteurs de risques de chaque scénario en leur affectant un terme linguistique. Ce dernier est introduit dans système d'inférence de Mamdani par la valeur centrale de sa fonction d'appartenance. Le scénario N°2.4 (baisse de la pression de l'huile d'isolation tel que :

- La cause de cette déviation est la défaillance de la boucle de régulation de l'huile d'étanchéité.

- La conséquence de cette déviation est la création d'une zone ATEX suite à l'épandage du gaz d'hydrogène.
- Pour la détection il existe des capteurs d'hydrogène.

L'estimation de chaque paramètre s'est fait en concertation avec les exploitants de la centrale.

Le tableau 12 synthétise la méthodologie d'affectation des paramètres des scénarios dans le système d'inférence.

Tableau 12 Synthèse de la méthodologie d'affectation des paramètres des scénarios

Scénario N°2.4	EOP	Gravité	Non-détection
Variable linguistique	Lointain	Très élevé	Faible
Fonction d'appartenance	[1 ; 2 ;3]	[9.09 ; 9.99 ; 10.1]	[2.051 ; 3.566 ; 5.081]
Valeur affectée	2	9.99	3.566

La sortie du système d'inférence est égale au rang 5 ce qui correspond au centre de la fonction d'appartenance du niveau 'majeur' de la variable linguistique HazOp-RPN.

L'application dans la toolbox Fuzzy Logic Designer de matlab pour ce scénario est illustrée dans la figure 16.

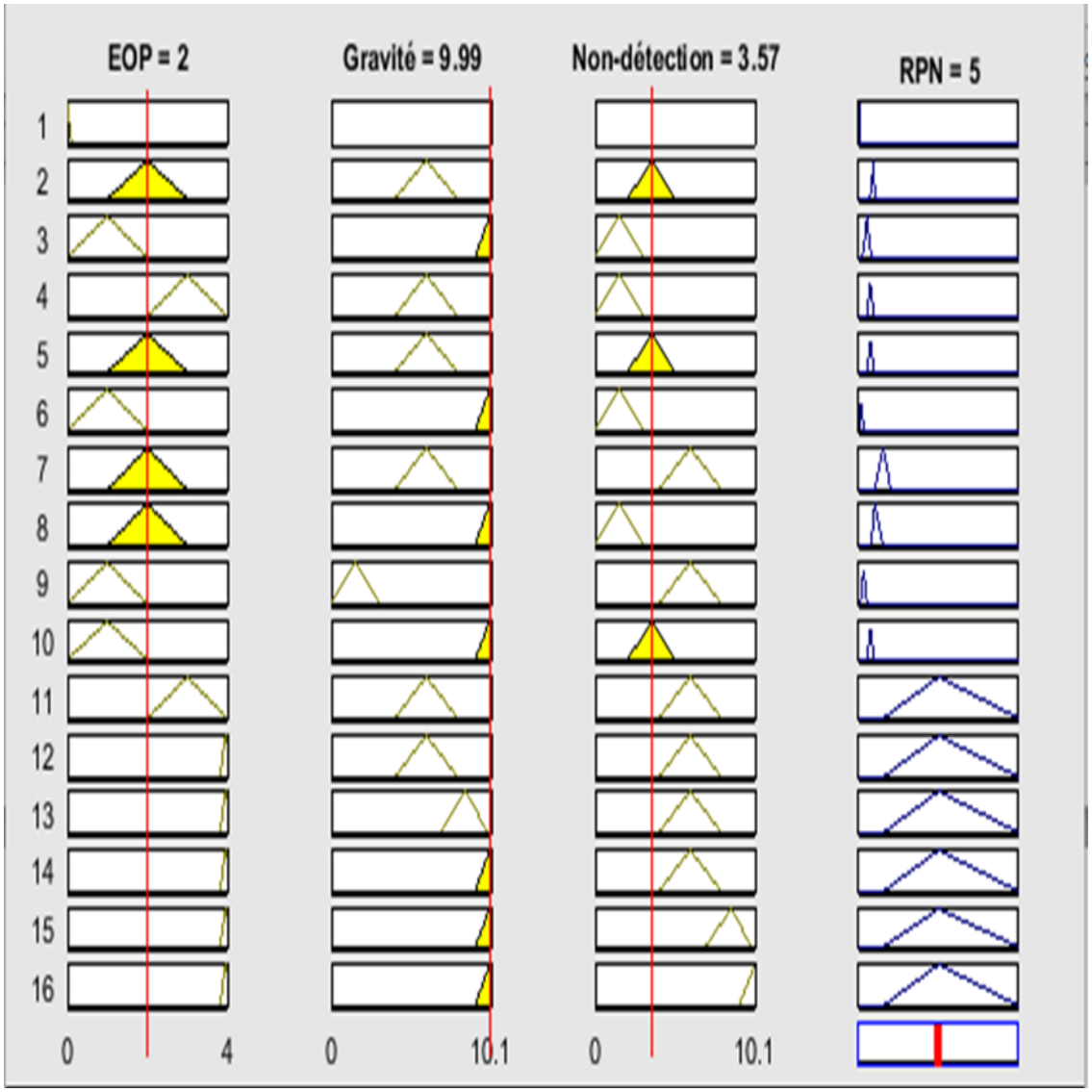


Figure 16 Résultats sous matlab de l'application de la HazOp_RPN sur le scénario 2.4

2.2.3.Analyse des résultats

Une fois la construction des scénarios et leurs estimations faites, nous avons sélectionné les scénarios à étudier, ç'est à dire les scénarios pouvant mener à des accidents majeurs : incendie et explosion. Les autres évènements non souhaités étudiés sont : la baisse du rendement, la détérioration et l'arrêt de l'installation.

Les scénarios de risques majeurs sont caractérisés par des niveaux de risque différents et qui prend en compte les différents paramètres de risques. Nous avons pris en compte dans la suite de notre étude les scénarios ayant un niveau de risque modéré jusqu'au niveau de risque majeur, c'est-à-dire le niveau 5 et plus.

Nous avons relevé 44 scénarios d'accident pour l'ensemble des systèmes étudiés et sélectionné 9 scénarios d'accidents majeurs : 4 pour le système fuel, 3 pour le système de refroidissement à hydrogène et 2 pour le système gaz.

Conclusion

L’application de la méthode HazOp_RPN nous a permis de faire ressortir les risques majeurs qu’encoure chaque système critique étudié, c’est à dire le risque d’explosion et d’incendie en se basant sur les données et les informations fournies par les opérateurs dont l'expérience assure une certaine confiance dans les résultats obtenus.

L’évaluation des scénarios faite avec des intervalles flous nous a permis de mieux caractériser chaque scénario en prenant en compte l’incertitude sur les facteurs de risques.

Chapitre 3 : Analyse des barrières

Introduction

Un risque ne pouvant être supprimé, on tente de le rendre acceptable du point de vue des conséquences qu'il peut amener et de la fréquence à laquelle il se manifeste. En effet dans chaque industrie, des seuils bien définis permettent de classer les risques selon leur criticité. Pour atteindre ces seuils, des barrières de sécurité sont mises en place. Ces dernières doivent être *sûres*, c'est-à-dire qu'elles doivent être en état de fonctionner lorsqu'elles sont sollicitées. Leur fiabilité détermine la réduction de risque qu'elles apportent.

Dans ce chapitre nous nous intéresserons aux barrières de sécurité actives mises en place dans les systèmes critiques étudiés afin de réduire les risques d'accidents majeurs identifiés. Nous déterminerons d'abord, les exigences de sécurité auxquelles doivent répondre les barrières. Ensuite, les barrières de sécurité sont analysées de point de vue de leur intégrité et de leur fiabilité de déterminer leur adéquation à leur fonction.

Nous avons introduit, aussi, dans ce chapitre des notions de la théorie de la logique floue afin de prendre en compte les incertitudes de l'analyse. Une autre méthode appelée BORA qui permet de corriger les probabilités de défaillances des équipements a été appliquée. Les résultats obtenus grâce à l'intelligence artificielle et la méthode BORA vont être comparés aux résultats obtenus par les méthodes conventionnelles de l'analyse des barrières.
Avant d'entamer l'étude des barrières de sécurité, nous présenterons les notions essentielles sur les barrières de sécurité active.

3.1. Introduction aux barrières de sécurité active

On distingue les mesures de sécurité par leurs modes d'action : la sécurité passive et la sécurité active.
La sécurité passive désigne tous les éléments mis en jeu afin de réduire les conséquences d'un accident lorsque celui-ci n'a pas pu être évité. Elle agit par sa seule présence, sans intervention humaine ni besoin en énergie (exemple : bâtiment de confinement, cuve de rétention, etc.).
La sécurité active désigne tous les éléments mis en jeu afin d'éviter les accidents. Elle nécessite une action, une énergie et un entretien (exemple : détecteur, vannes, SIS, etc.).

3.1.1. Système instrumenté de sécurité

Selon la norme CEI 61511 (CEI 61511, 2003), les systèmes instrumentés de sécurité (SIS) sont l'ensemble de matériels utilisés pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Ils se composent de n'importe quelle combinaison de capteur (s), d'unités logique (s) et d'élément (s) terminal (aux).

Un système instrumenté de sécurité vise à mettre le procédé en un état stable ne présentant pas de risque pour l'environnement et les personnes lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu…). (Mkhida, 2009)

Les SIS (figure 17) 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.

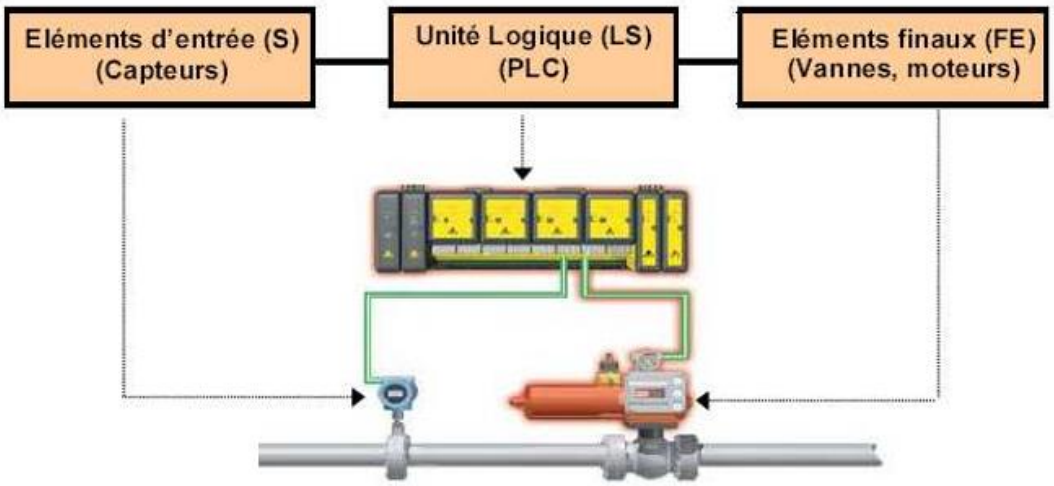


Figure 17 Schéma générale d'un SIS

a. **Capteur :** Est un équipement qui délivre, à partir d'une grandeur physique (température, débit,...), une autre grandeur, souvent électrique (tension, courant, résistance), fonction de la première et directement utilisable pour la mesure ou la commande.
b. **Unité de traitement :** Sa fonction consiste à activer la commande d'un ou plusieurs actionneurs à partir d'une fonction combinatoire des informations délivrées par différents capteurs.
c. **Actionneurs** : Un actionneur peut être une vanne, un servomoteur ou tout autre équipement qui transforme un signal (électrique ou pneumatique) en phénomène

physique qui permet de commander le démarrage d'une pompe, la fermeture ou l'ouverture d'une vanne… Selon l'énergie motrice, on parle d'actionneur pneumatique, hydraulique ou électrique.

Enfin, l'unité de traitement est reliée aux capteurs et aux actionneurs par des moyens de transmission. Il peut s'agir de câbles électriques, de lignes téléphoniques, d'ondes hertziennes (transmission par talkie-walkie…), ou de tuyauteries (transmission pneumatique ou hydraulique).

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

- Les SIS nécessitent une énergie extérieure pour remplir leur fonction de sécurité.
- Plusieurs capteurs ou actionneurs peuvent être reliés à une même unité de traitement ou plusieurs unités de traitement.
- Toutes les combinaisons de capteurs, d'unités de traitement et d'actionneurs qui sont exigées pour accomplir des fonctions de sécurité sont considérées comme une partie de SIS.

L'ensemble des sous-fonctions de sécurité contribue à assurer la sécurité fonctionnelle. Cette dernière constitue la sécurité relative aux équipements et aux systèmes de contrôle-commande associés, qui dépend du fonctionnement correct de systèmes électriques, électriques programmables, électroniques (E/E/PE) concernés par la sécurité (CEI61508, 2011).

3.1.2. Fonction instrumenté de sécurité

Une fonction instrumentée de sécurité (SIF, *Safety Instrumented Function*) est utilisée pour décrire les fonctions de sécurité implémentées par un SIS. Une SIF peut être considérée comme une barrière de protection fonctionnelle lorsque le SIS est considéré comme un système réalisant cette barrière de sécurité (Sklet, 2005). Le but de la SIF est d'atteindre ou de maintenir dans un état sûr les équipements contrôlés, dans le cadre d'un évènement dangereux particulier. La figure 18 illustre la définition d'un SIS et des SIF qui sont exécutées. Cette figure illustre, entre autres, une fonction instrumentée de sécurité (SIF n°1) qui surveille la température du procédé et fait fermer une vanne d'isolement en cas de dérive de température de procédé vers un état dangereux. Les autres SIF exécutées dans cet exemple de SIS sont la surveillance du débit et du niveau et leurs actionneurs associés.

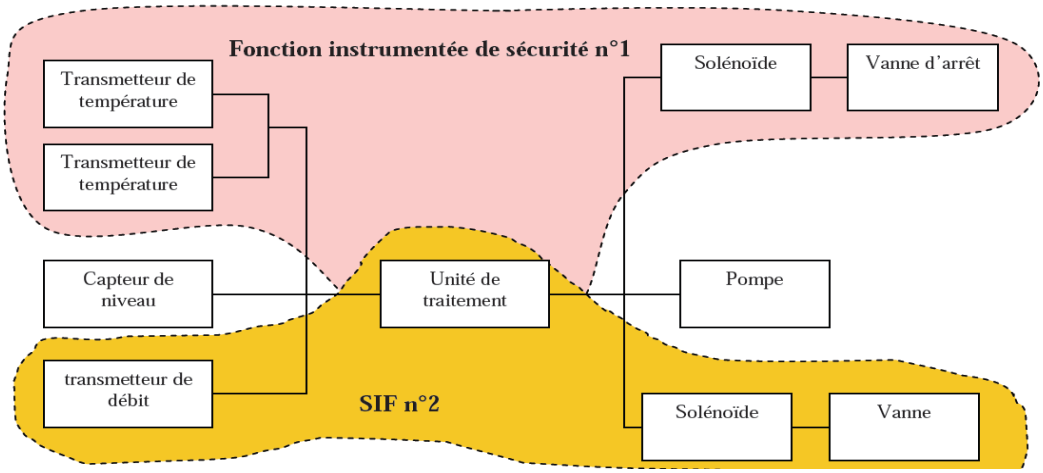


Figure 18 Fonctions instrumentées de sécurité (Mkhida, 2009)

3.1.3. Niveaux d'intégrité de sécurité

Les normes CEI 61508 et CEI 61511 spécifie le niveau d'intégrité de sécurité des systèmes de protections (SIL, *Safety Integrity Level*) qui représente le niveau de réduction du risque qu'ils doivent apporter. Plus le SIL à une valeur élevée, plus la réduction du risque n'est pas importante. Par exemple un système de SIL 4 apporte un facteur réduction de la probabilité du risque (RRF, *Risk Reduction Factor*) entre 10^4 à 10^5 alors qu'un système de SIL 1 comporte un RRF compris entre 10 à 10^2 seulement.

Les SILs se caractérisent par des indicateurs discrets positionnés sur une échelle à quatre niveaux. Le SIL 4 désigne le degré de sécurité le plus élevé du fait de l'exigence forte de sécurité imposée et le SIL 1 désigne l'exigence la plus faible. Les SILs sont employés pour spécifier les exigences de SIF selon la norme CEI 61508 et CEI 61511.

L'étude des barrières de sécurité permet de déterminer le SIL des SIFs (allocation des SILs) et l'analyse des risques permet de déterminer le SILs requis, c'est-à-dire la réduction qu'il faut avoir pour rendre le risque acceptable. La comparaison entre ces deux valeurs, permet d'apprécier l'adéquation des barrières de sécurité.

L'étude des défaillances des SIFs permet de prendre en compte les défaillances aléatoires, c'est à dire les défaillances résultant de divers mécanismes de dégradation au sein du matériel (CEI 61511, 2003) mais ne prend pas en compte les défaillances systématiques, c'est à dire les défaillances liées aux erreurs de conception, défauts logiciels ainsi que certaines défaillances matérielles liées à l'environnement.

La différence entre les défaillances aléatoires du matériel et les défaillances systématiques est que les taux de défaillances du système, engendrés par les défaillances aléatoires du matériel

peuvent être prédits et quantifiés alors que les défaillances systématiques ne peuvent pas être prédites ou quantifiés.

La norme CEI s'applique aussi bien aux systèmes de sécurité qui fonctionnent sur sollicitation que ceux qui travaillent en permanence pour maintenir un procédé dans un état non dangereux. Le mode de fonctionnement à faible sollicitation est considéré lorsque la fréquence de demande n'est pas plus grande qu'une par an et est au plus égale à deux fois la fréquence des tests périodiques (CEI61508, 2011). Le SIL est attribué pour ce cas par rapport à la moyenne de sa probabilité de défaillance à la demande (PFD_{avg}, *Average Probability of Failure On Demand*) évaluée sur un intervalle [0, t].

Le mode de fonctionnement continu ou à forte sollicitation implique une forte demande du système instrumenté de sécurité. Il est considéré lorsque la fréquence de demande est élevée ou continue, c'est-à-dire qu'elle plus grande qu'une par an ou supérieure à deux fois la fréquence des tests périodiques. (CEI61508, 2011) Ce mode concerne généralement les systèmes de prévention. Le SIL est attribué pour ce mode par rapport à sa probabilité de défaillance dangereuse par heure (PFH, *Probability of a dangerous Failure per Hour*) qui est un intervalle de temps [0, t].

Pour chaque fonction instrumentée de sécurité fonctionnant en mode de sollicitation respectivement en mode continu, le SIL doit être spécifié en accord avec le tableau 3.1 respectivement le tableau 13. (CEI 61511, 2003)

Il est à noter que le concept de SIL s'applique au système instrumenté de sécurité (SIS) dans son intégralité et pas à un sous-ensemble (par exemple un capteur).

Tableau 13 Niveaux d'intégrité de sécurité, Fonctionnement à la sollicitation

SIL	PFD_{avg}	RRF(Risk Reduction Factor)
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$100000 \leq RRF < 10000$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10000 \leq RRF < 1000$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$1000 \leq RRF < 100$
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$100 \leq RRF < 10$

3.1.4. Méthode de détermination des SIL

La détermination du SIL requis se fait par des méthodes qualitative et semi-quantitative alors que l'allocation des SILs des SIS doit se faire par des méthodes quantitatives (Sellak, 2007). Les normes CEI 61508 et CEI 61511 décrivent les méthodes suivantes pour la détermination du SIL requis :

a. **Méthodes qualitatives** : Elles permettent de déterminer le SIL à partir de la contribution des facteurs de risques (Kirkwood & Tibbs, 2005). Parmi ces méthodes : le graphe de risque et la matrice de gravité des événements dangereux.

b. **Méthodes semi-quantitatives** : Elles permettent de quantifier le risque lié au processus et de déterminer la contribution nécessaire ou exigée du SIS à la réduction du risque (Simon, Sallak, & Aubry, 2007). La méthode la plus utilisé est la méthode LOPA.

Les méthodes permettant l'allocation des SILs des SIS permettent de calculer le PFD à partir des probabilités de défaillances de leurs composants. Parmi les **méthodes quantitatives** citées, on trouve les équations simplifiées, les arbres de défaillance, les blocs diagramme fiabilité, les réseaux de Pétri ainsi que les chaines de Markov

3.2. Détermination du SIL requis

Nous avons choisi d'utiliser dans cette section la méthode du graphe du risque pour la détermination du SIL requis. Malgré le caractère qualitatif des résultats de cette méthode, l'introduction des concepts de la logique floue permet de donner de résultats quantitatifs et se révèle ainsi plus adaptée à l'environnement incertain où les données d'entrée sont insuffisantes et incertaines. (Lanternier & Adjadj, 2008)

3.2.1. Graphe de risque

Nous allons présenter dans ce qui suit l'enchainement logique qui a conduit à la construction de la méthode du graphe du risque flou, à partir du graphe de risque conventionnel et du graphe de risque étalonné

3.2.1.1. Graphe de risque conventionnel

La méthode de graphe de risques est une méthode qualitative très utilisée lors de la conception des systèmes de sécurité de par sa facilité d'application et sa rapidité de résolution. Elle est dédiée au SIS et permet de définir le niveau de SIL requis en fonction de certains paramètres.
La démarche de cette méthode s'appuie sur la formule (3.1) caractérisant le risque R sans considérer les moyens instrumentés de sécurité. (CEI61508, 2011)

$$R = C * f \qquad (3.1)$$

Où R est le risque en l'absence de système relatif à la sécurité ; C est la conséquence de l'événement dangereux ; f est la fréquence de l'évènement dangereux en l'absence des systèmes relatifs à la sécurité. Cette dernière est le résultat de trois facteurs : F, le pourcentage de la durée d'exposition dans une zone dangereuse par rapport à la fréquence du risque, P, la possibilité

d'éviter l'évènement dangereux et W, la possibilité que l'évènement dangereux se reproduise en l'absence de système relatif à la sécurité (la probabilité de l'occurrence non souhaitée)
Donc, on aboutit aux 4 paramètres C, F, P et W qui seront divisés en plusieurs niveaux définis dans le tableau 14.

Tableau 14 Exemple de classification des paramètres du risque (CEI61508, 2011)

Paramètre	Hiérarchisation	Critère d'évaluation
Gravité des conséquences	C_A	Blessure mineure
	C_B	Blessure sérieuse touchant une ou plusieurs personnes, mortelle pour une personne
	C_C	Mort de plusieurs personnes
	C_D	Grand nombre de morts
Temps d'exposition (occupation)	F_A	Rare
	F_B	Fréquent
Probabilité d'éviter le phénomène dangereux	P_A	Possible
	P_B	Impossible
Probabilité d'apparition d'un accident	W_A	Très faible probabilité
	W_B	Faible probabilité
	W_C	Forte probabilité

À partir des critères choisis pour chacun des paramètres C, F, P et W, il suffit de suivre l'arborescence pour déterminer le SIL requis.
La figure 19 montre un exemple d'un graphe de risque tel qu'utilisé dans les directives d'UKOOA (Gulland, 2004) .

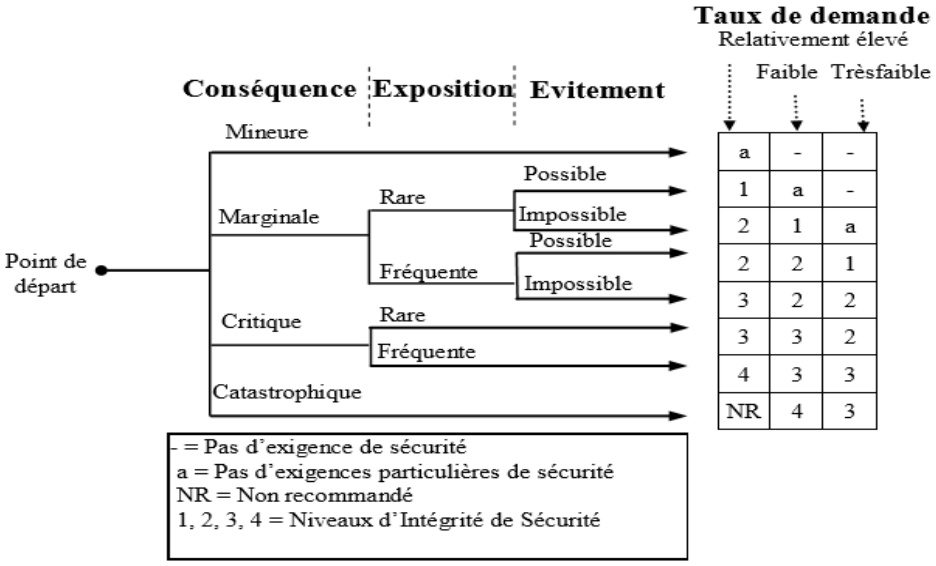


Figure 19 Graphe de risque avec une description qualitative des paramètres (Gulland, 2004)

La méthode du graphe de risque conventionnelle est jugée comme subjective, car l'interprétation des termes linguistiques tels que « rare » ou « possible » peut différer d'un évaluateur à un autre. (Redmil, 1998)

La norme CEI 61511 propose une méthode semi-qualitative « le graphe de risque étalonné ».

3.2.1.2. Graphe du risque étalonné

L'étalonnage du graphe de risque est une procédure qui consiste à attribuer une plage de valeurs numériques aux différents paramètres.

Le tableau 15 montre la description quantitative des paramètres du graphe de risque utilisés dans les directives d'UKOOA (Gulland, 2004).

Tableau 15 Description quantitative et qualitative des paramètres du graphe de risque (Gulland, 2004)

Paramètre	Description qualitative	Description quantitative
Conséquence (C)	Mineure	Blessures mineures
	Marginale	$[10^{-2},10^{-1}]$
	Critique	$[10^{-1},1]$
	Catastrophique	>1
Occupation (F)	Rare	< 10 % de temps
	Fréquente	≥ 10 % de temps
Possibilité d'évitement (P)	Possible	90 % probabilité d'évitement du danger
	Impossible	≤ 90 % probabilité d'évitement du danger
Taux de demande (W)	Très faible	< 1 dans 30 ans ≈< 0.03/ans
	Faible	1 dans [3,30] ans ≈ [0.03, 0.3] par an
	Elevé	1 dans [0.3, 3] ans ≈ [0.3, 3] par ans

Les intervalles utilisés dans le graphe du risque étalonné représentent un moyen de caractérisation de l'incertitude mais cette approche ne tient pas compte du fait que dans le raisonnement humain et la formation de l'idée, la décomposition d'un ensemble en deux parties est plutôt floue que discrète (Massaro, 1992). En d'autres termes, il existe une incompatibilité entre l'incertitude qui caractérise la perception humaine et le caractère discret du mode de réponse.

Afin de palier à ces difficultés, un nouveau modèle de graphe de risque à base de règles floues a été développé.

3.2.1.3. Graphe du risque flou

Le graphe de risque flou est un modèle basé sur les mêmes paramètres du graph de risque standard. Il est établi selon trois principales étapes présentées dans la Figure 20 et expliquées auparavant dans la §2.1.

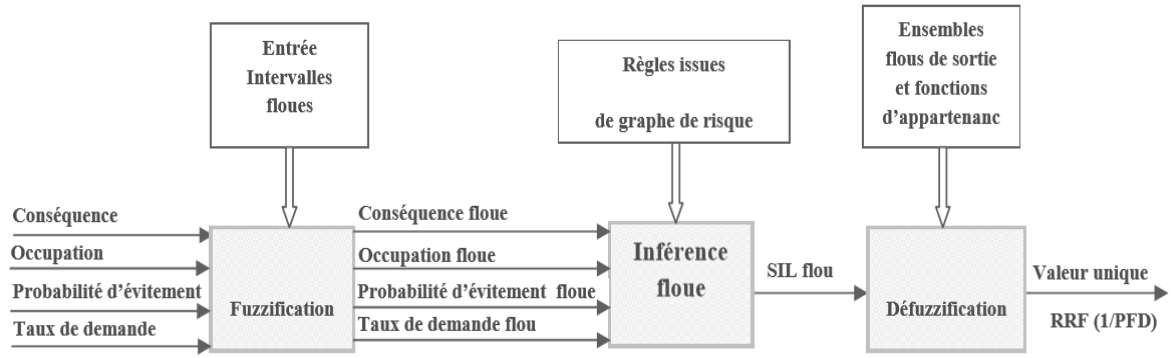


Figure 20 Procédure globale d'évaluation de SIL à base de règles floues

3.2.1.3.1. Détermination des intervalles flous

Les intervalles floues des paramètres du graphe du risque ont été présentés par (Nait-Said, Zidani, & Ouazraoui, 2009) et ((Simon, Sallak, & Aubry, 2007) et sont inspirés des intervalles utilisés par le graphe du risque étalonné. Les fonctions d'appartenance pour chaque niveau de paramètre est de type trapézoïdale (figure 21) tels que :

- E_* : Valeur de la borne inférieure de l'intervalle correspondant dans le graphe du risque étalonné ;
- E^* : Valeur de la borne supérieure de l'intervalle correspondant dans le graphe du risque étalonné ;
- q_- : Borne inferieure du noyau de la fonction d'appartenance ;
- q_+ : Borne supérieure du noyau de la fonction d'appartenance ;

- S_- : Borne inferieure du support de la fonction d'appartenance ;
- S_+ : Borne inferieure du support de la fonction d'appartenance.

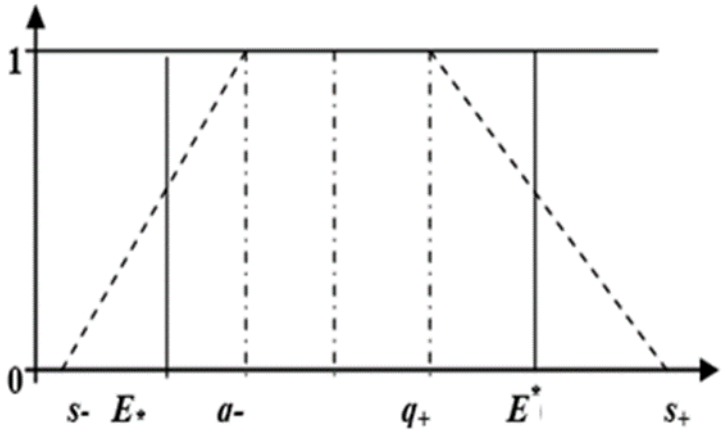


Figure 21 transformation de l'intervalle ordinaire en intervalle flou

Les fonctions d'appartenance pour les différents paramètres sont présentées ci-dessous.

- **Conséquence** (C):

On définit sur l'espace de cette variable 4 ensembles flous «Mineure», «Modérée», «Critique» et «Catastrophique» telles que ces valeurs varient de 10^{-9} à 10 et ils sont représentées sur une échelle logarithmique (tableaux 16 et 17) (figure 22).

A la valeur linguistique « mineure », définie dans le graphe de risque étalonné comme «Blessures mineures», est attribué l'intervalle [10^{-9}, 10^{-7}]. Cet intervalle est transformé en un intervalle flou.

Tableau 16 les fonctions d'appartenance pour le paramètre Conséquence

Symboles	E_*	E^*	q_-	q_+	S_-	S_+
Mineur	10^{-9}	10^{-7}	$3{,}16.10^{-9}$	$3{,}16.10^{-8}$	$1{,}0.10^{-9}$	$1.68.10^{-7}$
Marginal	0,01	0,1	$1{,}77.10^{-2}$	$5{,}62.10^{-2}$	$2{,}211.10^{-3}$	$1.43.10^{-1}$
Critique	0,1	1	$1{,}77.10^{-1}$	$51{,}62.10^{-1}$	$2{,}21.10^{-2}$	1.43
Catastrophique	1	10	1,77	5,62	$2{,}21.10^{-2}$	10

Tableau 17 Echelle log_{10} des fonctions d'appartenance pour le paramètre Conséquence

Log10(Symboles)	E_*	E^*	q_-	q_+	S_-	S_+
Mineur	-9	-7	-8,50	-7,50	-9	-6,77
Marginal	-2	-1	-1,75	-1,25	-2,65	-0,84
Critique	-1	0	-0,75	-0,25	-1,66	0,15
Catastrophique	0	1	0,25	0,75	-0,65	1

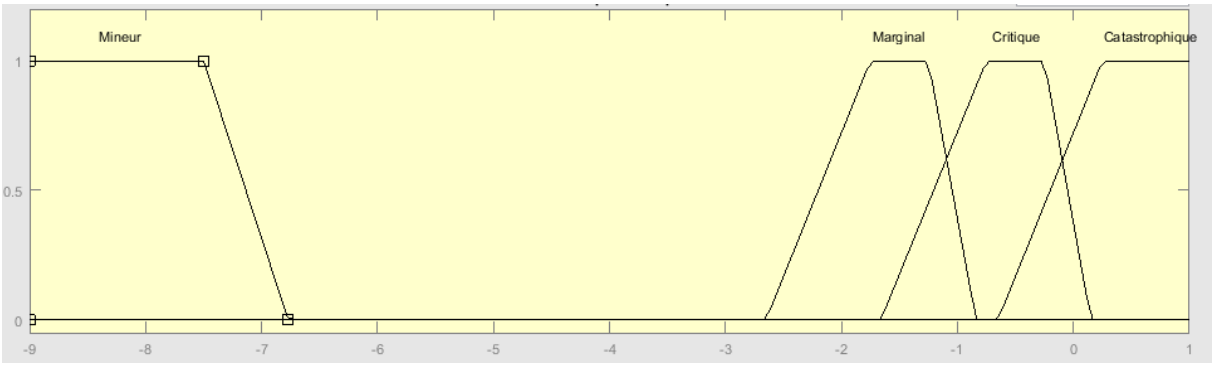


Figure 22 Fonctions d'appartenance du paramètre Conséquence

- **Fréquence et période d'exposition :**

Deux ensembles flous «Rare» et «Fréquente» ont été définis sur une échelle allant de 0% à 100% (tableau 18).

Tableau 18 Les fonctions d'appartenance pour le paramètre Fréquence

Symboles	E_*	E^*	q_-	q_+	S_-	S_+
Rare	0	10	2,50	7,50	0	12,5
Fréquente	10	100	32,5	77,5.	7,50	100

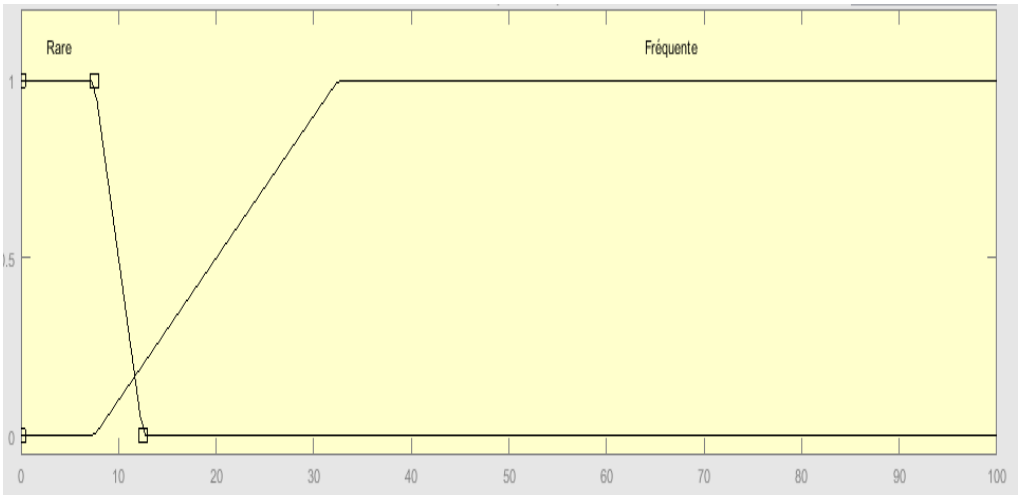


Figure 23 Fonctions d'appartenance du paramètre Fréquence

- **Possibilité d'éviter l'événement dangereux**

Deux ensembles flous « Impossible» et «Possible» ont été définis sur l'intervalle [0, 100] (tableau 19).

Tableau 19 Fonctions d'appartenance du paramètre Possibilité d'évitement

Symboles	E_*	E^*	q_-	q_+	S_-	S_+
Impossible	0	90	22,5	67,50	0	92,50
Possible	90	100	92,50	97,50	87,50	100

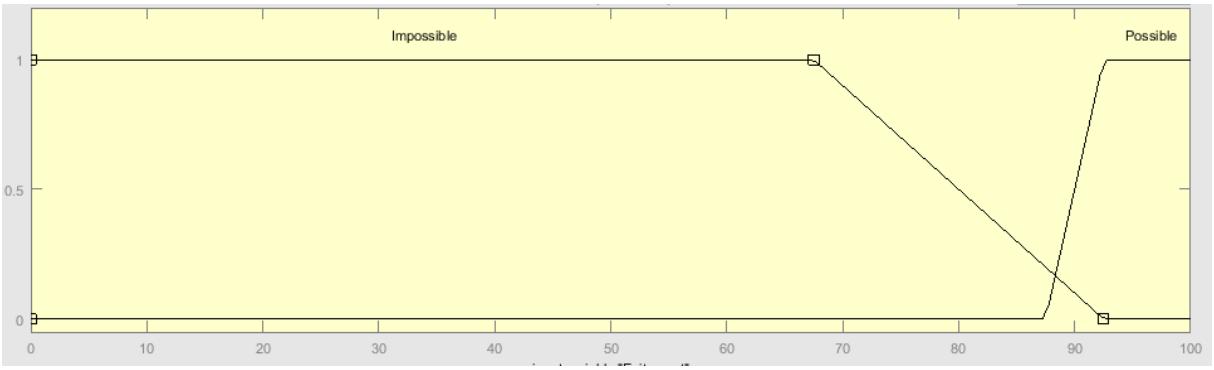


Figure 24 Fonctions d'appartenance du paramètre Possibilité d'évitement

- **Probabilité de l'apparition de l'évènement indésirable** :

Trois ensembles flous, à savoir «Très faible», «Faible» et «Relativement élevée» ont été définis sur un espace de probabilité allant de 10-5⁄an à 1⁄an.

A l'instar du premier paramètre, les valeurs de probabilité sont représentées sur une échelle logarithmique. La valeur 10^{-5} ⁄an est choisi comme la borne inférieure de l'intervalle correspondant au terme "très faible".

Les tableaux 20 et 21 montrent les bornes des fonctions d'appartenance de la probabilité d'apparition de l'évènement indésirable et leurs correspondances sur l'échelle logarithmique.

Tableau 20 Fonctions d'appartenance du paramètre Probabilité d'apparition de l'événement indésirable

Symboles	E_*	E^*	q_-	q_+	S_-	S_+
Très faible	10^{-5}	0.03	$7{,}401.10^{-5}$	$4{,}054.10^{-3}$	$1{,}0^{e}$-05	$5{,}595.10^{-2}$
Faible	0.03	0.3	$5{,}335.10^{-2}$	$1{,}687.10^{-1}$	$6{,}652.10^{-3}$	0,4.313
Elevé	0.3	1	0,4054	$7{,}401.10^{-1}$	0,1946	1

Tableau 21 Echelle log_{10} des fonctions d'appartenance du paramètre Probabilité d'apparition de l'événement indésirable

Log_{10} (Symboles)	E_*	E^*	q_-	q_+	S_-	S_+
Très faible	-5	-1,52	-4,13	-2,39	-5	-1,25
Faible	-1,52	-0,52	-1,27	-0,77	-2,17	-0,36
Elevé	-0,52	0	-0,39	-0,13	-0,71	0

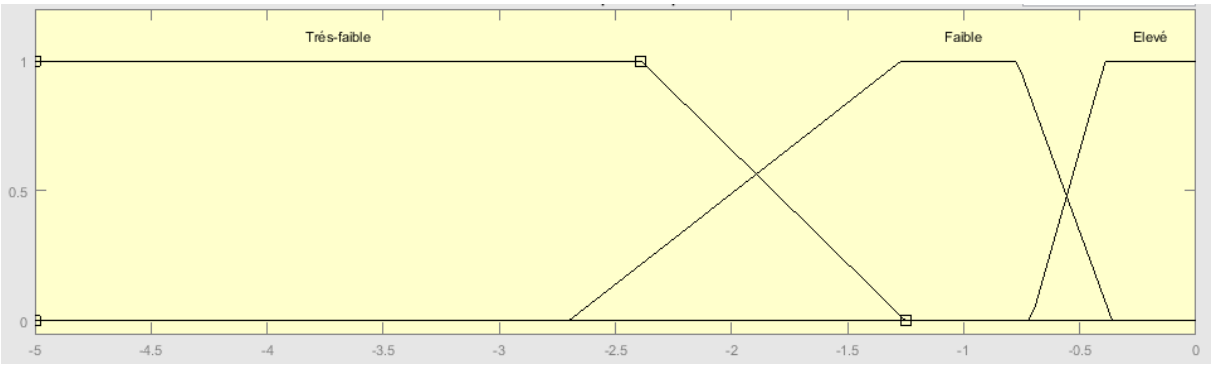


Figure 25 Fonctions d'appartenance du paramètre Probabilité d'apparition de l'événement indésirable

Le paramètre de sortie est le niveau du SIL requis

- **Niveau d'intégrité de sécurité (SIL) :**

Le SIL, comme variable de sortie unique, est définie sur une échelle de RRF. L'univers de discours est défini sur l'intervalle [1, 10^6] avec une partition régulière d'un facteur de dix entre deux subdivisions successives.

Ainsi, six ensembles flous sont définis sur l'espace du SIL : quatre ensembles sont associés aux SILs avec les mêmes nominations décrivant les niveaux eux-mêmes, et deux ensembles flous nommés «a» et «b» se référant, respectivement, aux cas «pas d'exigence particulière de sécurité», « un seul SIS non recommandé».

Le tableau 22 et 23 montres les bornes des fonctions d'appartenances des niveaux SIL et leurs correspondances sur l'échelle logarithmique.

Tableau 22 Les fonctions d'appartenance pour le paramètre SIL

Symboles	E_*	E^*	q_-	q_+	S_-	S_+
A	1	10	1,778	5.623	1	14,38
SIL 1	10	10^2	17,78	56,23	2,217	$1{,}438.10^{2.}$
SIL 2	10^2	10^3	$1{,}778.10^{2.}$	$5{,}623.10^{2.}$	22,17	$1{,}438.10^{3.}$
SIL 3	10^3	10^4	$1{,}778.10^3$	$5{,}623.10^3$	$2{,}217.10^{2.}$	$1{,}438.10^{4.}$
SIL 4	10^4	10^5	$1{,}778.10^{4.}$	$5{,}623.10^4$	$2{,}217.10^3$	$1{,}438.10^{5.}$
B	10^5	10^6	$1{,}778.10^5$	$5{,}623.10^5$	$2{,}217.10^4$	$10^{6.}$

Tableau 23 Echelle log10 des fonctions d'appartenance pour le paramètre SIL

Log10 (Symboles)	E*	E*	q-	q+	S-	S+
A	0	1	0,25	0,75	0	1,16
SIL 1	1	2	1,25	1,75	0,35	2,16
SIL 2	2	3	2,25	2,75	1,35	3,16
SIL 3	3	4	3,25	3,75	2,35	4,16
SIL 4	4	5	4,25	4,75	3,35	5,16
B	5	6	5,25	5,75	4,35	6

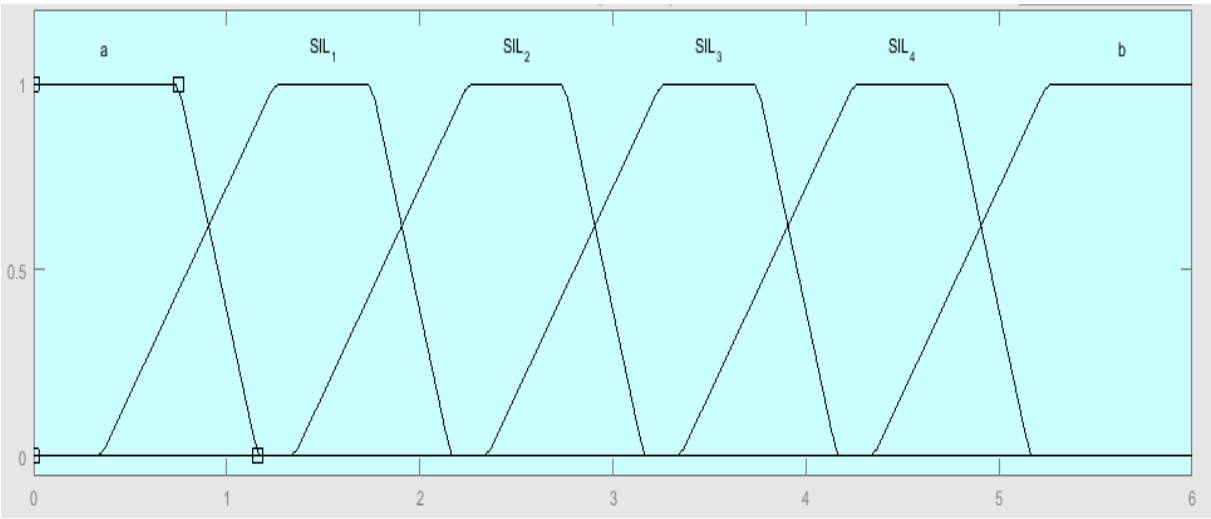


Figure 26 Fonctions d'appartenance du paramètre SIL

3.2.1.3.2. Construction de la base de règles

Pour prendre en considération l'incertitude des données, le graphe de risque flou utilise le système d'inférence pour établir la relation entre les variables d'entrées flou et la sortie flou.

Dans notre cas, la base de règles est établie suivant la logique du graphe de risque. Donc, la combinaison des valeurs des variables d'entrée C, F, P et W permet de décrire le niveau de SIL. Le tableau 24 résume les règles utilisées.

Une règle est formulée de la manière suivante : Si la conséquence (C) est «marginale » et si l'Occupation (F) est « rare » et si la Possibilité d'évitement (P) est « possible » et si le Taux de demande (W) est « élevé » alors le SIL est 1.

Tableau 24 Règles d'inférence du graphe de risque flou

Règle	Conséquence	Occupation	Possibilité d'évitement	Taux de demande	SIL
1	Mineure	/	/	élevé	/
2	Mineure	/	/	Faible	/
3	Mineure	/	/	Très faible	/
4	Marginale	Rare	possible	Elevé	1
5	Marginale	Rare	possible	Faible	A
6	Marginale	Rare	possible	Très faible	/
7	Marginale	Rare	Impossible	Elevé	2
8	Marginale	Rare	Impossible	Faible	1
9	Marginale	Rare	Impossible	Très faible	A
10	Marginale	Fréquent	Possible	Elevé	2
11	Marginale	Fréquent	Possible	Faible	2
12	Marginale	Fréquent	Possible	Très faible	1
13	Marginale	Fréquent	Impossible	Elevé	3
14	Marginale	Fréquent	Impossible	Faible	2
15	Marginale	Fréquent	Impossible	Très faible	2

16	Critique	Rare	/	Elevé	3
17	Critique	Rare	/	Faible	3
18	Critique	Rare	/	Très faible	2
19	Critique	Fréquent	/	Elevé	4
20	Critique	Fréquent	/	Faible	3
21	Critique	Fréquent	/	Très faible	3
22	Catastrophique	/	/	Elevé	B
23	Catastrophique	/	/	Faible	4
24	Catastrophique	/	/	Très faible	3

En utilisant la méthode du centre de gravité la valeur défuzzifiée correspond à l'abscisse du centre de gravité de la surface sous la courbe résultante de l'agrégation des règles C'est une valeur numérique de SIL comparable à celle donnée par le graphe conventionnel.

Les calculs de la mémoire du système d'inférence floue FIS générés avec Matlab sont présentés dans l'Annexe 5.

3.2.2.Application de la méthode du graphe de risque flou aux scénarios étudiés

Pour chaque système étudié, il y a lieu de sélectionner les scénarios qui mènent à des phénomènes dangereux afin d'appliquer la méthode du graphe de risque qui nous permettra de déterminer le niveau du SIL des SIF à mettre en place pour assurer une réduction adéquate du risque

L'évaluation des paramètres du risque est faite en se basant, d'une part, sur le jugement des opérateurs et d'autre part sur l'utilisation des données issues de la littérature.

- **Conséquence (C)** : l'estimation s'est appuyée sur le jugement des opérateurs présents sur le site.
- **Taux de demande (W)** : L'évaluation du paramètre est faite en utilisant des valeurs de fréquence des événements initiateurs prises des bases de données (OREDA, 2002) et (EXIDA, 2005).
- **La probabilité d'évitement de l'événement dangereux (P)** : elle est estimée en prenant en considération la vitesse d'évacuation de l'opérateur et la disponibilité de l'alarme.
- **Occupation (F)** : Ce paramètre est estimé en prenant la valeur maximale du temps d'occupation de la zone dangereuse, et ce temps varie entre 0 et 8h au cours de la période normale de travail.

3.2.2.1. Application du graphe de risque conventionnel

Le travail est effectué pour les trois systèmes étudiés, Tel que le choix des scénarios est basé sur les résultats de la HazOp_RPN.

a. Système N°1 : Système fuel

Concernant le système fuel, l'étude portera sur les scénarios qui mèneront à un incendie D'après la HazOp_RPN floue on dénombre 4 scénarios développés ci-après.

Scénarios N°1.1 (tableau 25)**:** La corrosion du bac de stockage entraine une fuite du fuel et la présence d'une source chaude conduira à un incendie

Tableau 25 Paramètres du graphe de risque relatifs au scénario N°1.1

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_B	Marginale : Blessure sérieuse touchant une ou plusieurs personnes, mortelle pour une personne	$[10^{-2}, 10^{-1}]$
Occupation	F_B	Fréquente	≥ 10 % de temps
Possibilité d'évitement	P_B	Impossible	< 90 % probabilité d'évitement du danger
Taux de demande	W_B	Faible	1 dans [3,30] ans

Scénarios N°1.3 (tableau 26)**:** L'ouverture intempestive de la vanne d'alimentation des bacs va entrainer le débordement du fuel et la présence d'une source chaude conduira à un incendie

Tableau 26 Paramètres du graphe de risque relatifs au scénario N°1.3

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_B	Marginale : Blessure sérieuse touchant une ou plusieurs personnes, mortelle pour une personne	$[10^{-2}, 10^{-1}]$
Occupation	F_B	Fréquente	≥ 10 % de temps
Possibilité d'évitement	P_B	Impossible	< 90 % probabilité d'évitement du danger
Taux de demande	W_B	Faible	1 dans [3,30] ans

La défaillance de la vanne elle est de 10^{-1} par an ce qui veut dire qu'elle peut survenir une fois tous les 10 ans ce qui la situe dans l'intervalle [3,30] ans.

Scénario N°1.5 (tableau 27) : La rupture de la ligne entre les nœuds du système fuel va entrainer l'épandage du fuel et la présence d'une source chaude conduira à un incendie

Tableau 27 Paramètres du graphe de risque relatifs au scénario N°1.5

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_C	Critique : Mort de plusieurs personnes	$[10^{-1}, 1]$
Occupation	F_B	Fréquente	≥10 % de temps
Possibilité d'évitement	P_B	Impossible	< 90 % probabilité d'évitement du danger
Taux de demande	W_C	Très faible	< 1 dans 30 ans

Scénario N°1.6 (tableau 28) : Le défaut d'étanchéité de l'installation va entrainer une fuite du fuel et la présence d'une source chaude conduira à un incendie.

Tableau 28 Paramètres du graphe de risque relatifs au scénario N°1.6

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_B	Marginale : Blessure sérieuse touchant une ou plusieurs personnes, mortelle pour une personne	$[10^{-2}, 10^{-1}]$
Occupation	F_B	Fréquente	≥10 % de temps
Possibilité d'évitement	P_B	Impossible	< 90 % probabilité d'évitement du danger
Taux de demande	W_C	Très faible	< 1 dans 30 ans

b. Système N°2 : Système de refroidissement à hydrogène de l'alternateur

Pour le skid Hydrogène l'étude portera sur les scénarios qui mèneront à une explosion. D'après la HazOp RPN floue on dénombre 3 scénarios développés ci-après.

Scénario N°2.2 (tableau 29) **:** Le défaut d'étanchéité de l'installation va entrainer une fuite du gaz d'Hydrogène susceptible de créer un mélange ATEX

Tableau 29 Paramètres du graphe de risque relatifs au scénario N°2.2

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_C	Critique : Mort de plusieurs personnes	$[10^{-1}, 1]$
Occupation	F_B	Fréquente	≥10 % de temps
Possibilité d'évitement	P_B	Impossible	≤ 90 % probabilité d'évitement du danger
Taux de demande	W_C	Très faible	< 1 dans 30 ans

Scénario N°2.4 (tableau 30) **:** La défaillance de la boucle de régulation de la pression de l'huile d'étanchéité va entrainer une fuite du gaz hydrogène susceptible de créer un mélange ATEX

Tableau 30 Paramètres du graphe de risque relatifs au scénario N°2.4

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_C	Critique : Mort de plusieurs personnes	$[10^{-1}, 1]$
Occupation	F_B	Fréquente	≥10 % de temps
Possibilité d'évitement	P_B	Impossible	≤ 90 % probabilité d'évitement du danger
Taux de demande	W_B	Faible	1 dans [3,30] ans

Le taux de demande et obtenue à partir du calcul de la probabilité de défaillance de la boucle par la méthode de l'arbre de défaillance flou expliqué dans la section suivante tel que PFD_{avg}= 0.19 par an.

Scénario N°2.9 (tableau 31) **:** L'évacuation incomplète de l'hydrogène avant les opérations de maintenances donnera lieu à la formation d'un mélange air / H2 susceptible de conduire à une explosion.

Tableau 31 Paramètres du graphe de risque relatifs au scénario N°2.9

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_B	Marginale : Blessure sérieuse touchant une ou plusieurs personnes, mortelle pour une personne	$[10^{-2}, 10^{-1}]$
Occupation	F_A	Rare	< 10 % de temps
Possibilité d'évitement	P_B	Impossible	≤ 90 % probabilité d'évitement du danger
Taux de demande	W_B	Faible	1 dans [3,30] ans

c. Système N°3 : Poste gaz

Pour le poste gaz l'étude portera sur les scénarios qui mèneront à une explosion D'après la HazOp RPN floue on dénombre 2 scénarios développés ci-après.

Scénario N°3.1 (tableau 32) **:** L'augmentation de la température ambiante entrainera une augmentation de la pression dans le circuit gaz naturel et peut conduire à une fuite du gaz, susceptible de créer un mélange ATEX.

Tableau 32 Paramètres du graphe de risque relatifs au scénario N°3.1

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_C	Critique : Mort de plusieurs personnes	$[10^{-1}, 1]$
Occupation	F_B	Fréquente	≥10 % de temps
Possibilité d'évitement	P_B	Impossible	≤ 90 % probabilité d'évitement du danger
Taux de demande	W_C	Très faible	< 1 dans 30 ans

Scénario N°3.4 (tableau 33) **:** Le défaut d'étanchéité de l'installation va entrainer une fuite du gaz naturel, susceptible de créer un mélange ATEX.

Tableau 33 Paramètres du graphe de risque relatifs au scénario N°3.4

Paramètre	Hiérarchisation	Description qualitative	Description quantitative
Conséquence	C_C	Critique : Mort de plusieurs personnes	$[10^{-1}, 1]$
Occupation	F_B	Fréquente	≥10 % de temps
Possibilité d'évitement	P_B	Impossible	≤ 90 % probabilité d'évitement du danger
Taux de demande	W_B	Faible	1 dans [3,30] ans

L'estimation de ces paramètres est source d'importante incertitude et peut être l'origine des incohérences des résultats. Cela peut se traduire par une sous ou surestimation du SIL. L'ensemble de ces arguments justifie la nécessité d'avoir recours à une évaluation du SIL par l'approche floue.

3.2.1.1. Détermination du SIL par la méthode graphe de risque flou

Les données sur les paramètres C, F, P et W sont introduites au système d'inférence floue de Mamdani afin d'obtenir la valeur du SIL flou pour les scénarios étudiés.

Le système d'inférence correspondant au graphe du risque flou a été implémenté dans la toolbox Fuzzy Logic Design de matlab[3]. La figure 27 représente une illustration de la méthode pour le scénario N° 1.1 du système fuel.

[3] Matlab R2015a

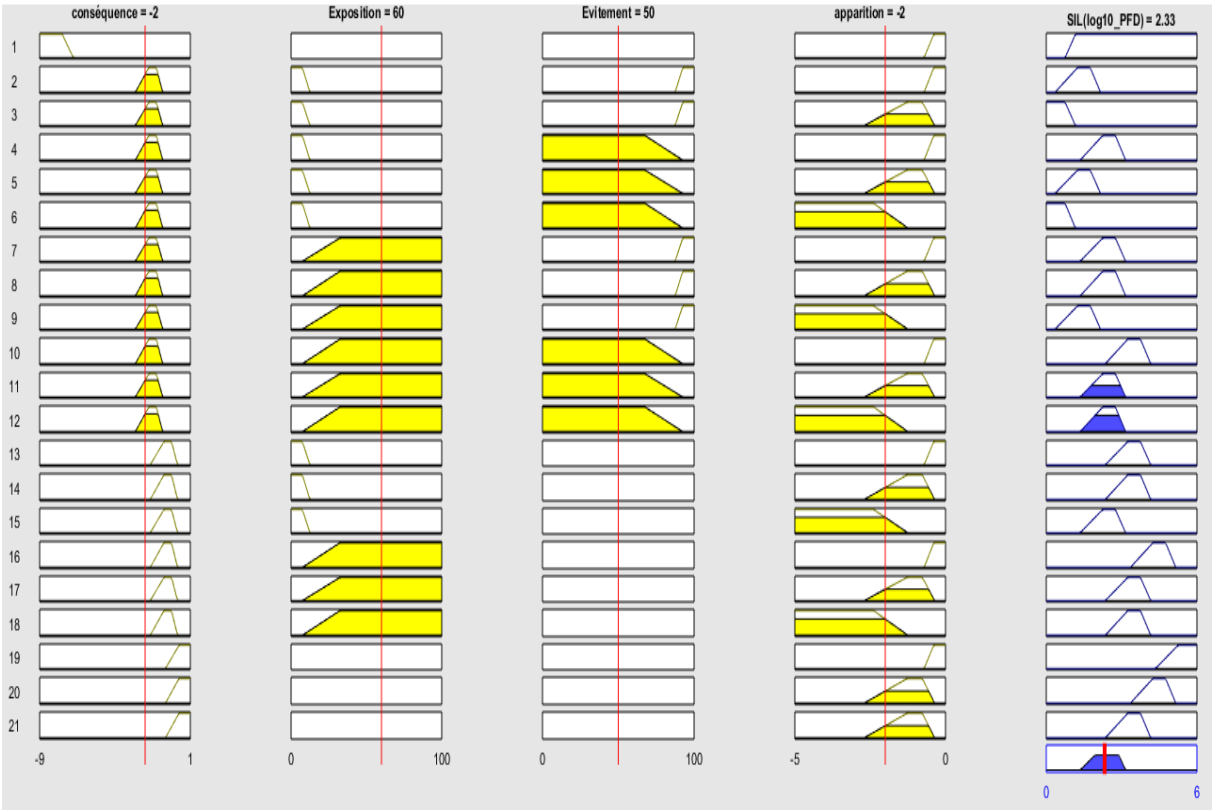


Figure 27 Processus d'inférence floue pour le scénario N° 1.1 du système fuel

Le tableau 34 représente un récapitulatif des résultats obtenus avec la méthode du graphe de risque conventionnel et flou appliqués sur les trois systèmes étudiés.

Tableau 34 Récapitulatif des résultats de l'évaluation du SIL des scénarios.

Système	Scénario	Entrée				SIL		
		C	F	P	W	Modèle conventionnel	modèle Flou	RRF
Système fuel	N°1.1	-2	60	50	-2	SIL 2	SIL 2	2.33
	N°1.3	-2	60	50	-1	SIL 2	SIL 2	2.33
	N°1.5	-1.5	60	50	-4	SIL 2	0.5-SIL3 / 0.9-SIL 2	2.52
	N°1.6	-2.5	60	50	-2.5	SIL 1	SIL 2	2.27
Skid Hydrogène	N°2.2	-1.2	70	30	-2	SIL 2	0.46-SIL 3 / 0.96-SIL 2	2.77
	N°2.4	-1.2	70	30	-0.72	SIL 3	0.38-SIL 3 / 1-SIL 2	2.73
	N°2.9	-2.5	20	10	-1.6	SIL 1	SIL 2	2.27
Poste gaz	N°3.1	-1.6	30	40	-4	SIL 2	0.09-SIL 3 / 1-SIL 2	2.42
	N°3.4	-1.6	30	40	-1	SIL 3	0.09-SIL 3 / 1-SIL 2	2.42

3.3. Allocation des SILs des SIS

Dans cette étape, nous avons opté pour l'utilisation de deux méthodes d'allocation du SIL. La premières et la méthode BORA dans laquelle on introduit le concept de facteur de risque et la deuxième est celle l'arbre de défaillance flou qui prend en compte l'incertitude des PFD_{avg}.

3.3.1. Méthodologie BORA (Barrier and Operational Risk Analysis)

La méthodologie BORA ou l'analyse des barrières et des risques opérationnels (Barrier and Operational Risk Analysis) a été développée à l'Université Norvégienne de Sciences et Technologies (NTNU) (Aven, Sklet, & Vinnem, 2003). Son objectif est de faire une analyse détaillée et quantitative de la performance des barrières. BORA permet de quantifier la probabilité de défaillance (PFD_{avg}) des barrières de sécurité mais permet également de prendre en compte les facteurs techniques, opérationnels et organisationnels, qui influent sur la performance des barrières. Ces derniers sont utilisés pour ajuster la probabilité des défaillances de base conduisant à l'échec de la barrière.

La méthodologie BORA combine plusieurs outils : le bloc diagramme barrière (BDD) qui permet de situer la fonction de la barrière de sécurité dans le scénario d'accident, l'arbre de défaillance (AdD) utilisé pour identifier les défaillances et la séquence de ces derniers qui conduisent à l'échec de la barrière et finalement, le diagramme d'influence qui permet d'identifier les facteurs influençant la performance et de corriger la probabilité des évènements de base. La méthode BORA est implémentée selon les étapes explicitées ci-après.

3.3.1.1. Développement d'un modèle base de risque

La première étape consiste à illustrer un modèle de base de risque par un Diagramme Bloc Barrière (DBB). Il permet de représenter graphiquement la séquence du scénario d'accident et il peut être assimilé à un arbre d'évènement (Aven, Sklet, & Vinnem, 2006). Il est constitué de :

- Evènement initiateur : la première déviation significative conduisant à un évènement redouté ;
- Fonctions barrière : mises en place pour contrôler, prévenir ou mitiger un évènement indésirable ou un accident ;
- Flèches : montrent la séquence des évènements, telle qu'une flèche horizontale indique le bon fonctionnement du système de barrières et une flèche verticale son échec.

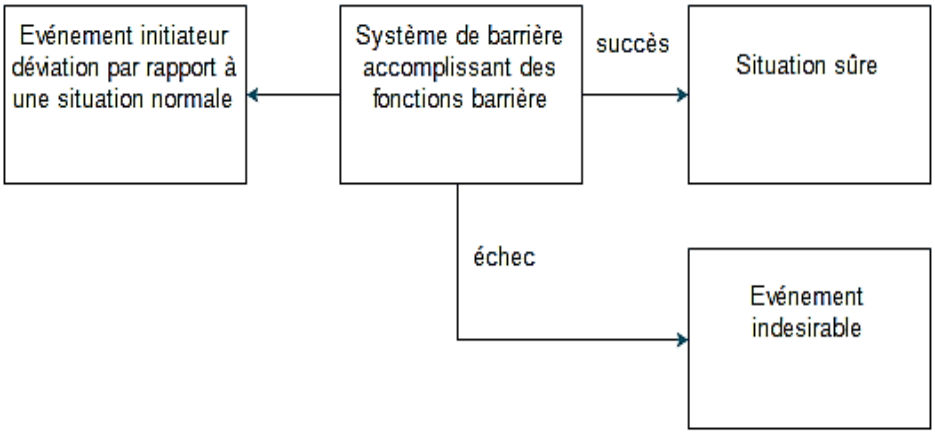


Figure 28 Diagramme Bloc Barrière

3.3.1.2.Modélisation de la performance des barrières de sécurité

Cette modélisation a pour but d'analyser la performance des barrières de sécurité. Elle est établie à l'aide de l'arbre de défaillance (AdD) en prenant en compte comme évènement de tête l'échec du système de barrière à accomplir une fonction de barrière spécifique.

L'arbre de défaillance est une méthode d'analyse déductive basée sur la réalisation d'une arborescence qui permet d'identifier les combinaisons (conjonction ou disjonction) de défaillances ou de causes primaires conduisant à la réalisation d'un évènement redouté (dans notre cas : l'échec de la fonction de sécurité) en passant par les évènements intermédiaires.

La méthode de l'arbre de défaillance comprend un traitement qualitatif (figure 29) qui correspond à la construction de l'arbre et la recherche des évènements de base et un traitement quantitatif qui vise à évaluer la probabilité de la survenance de l'évènement de tête en combinant les probabilités de la survenance des évènements de base et des évènements intermédiaires. Cette combinaison se fait avec des connecteurs logiques. Les plus utilisés sont :

- Porte ET :

L'évènement de sortie *A* de la porte ET est généré si et seulement si toutes les entrées A_i sont présentes. La probabilité de défaillance de *A* est égale à :

$$P(A) = \prod_{i=1}^{n} P(A_i) \qquad (3.2)$$

- Porte Ou :

L'évènement de sortie *A* de le porte OU est généré si et seulement si un ou plusieurs entrées A_i de la porte sont présentes. La probabilité de défaillance de *A* est égale à :

$$P(A) = 1 - \prod_{i=1}^{n}(1 - P(A_i)) \qquad (3.3)$$

L'attribution de la probabilité de la survenance des évènements de bases se fait en se référant aux bases de données.

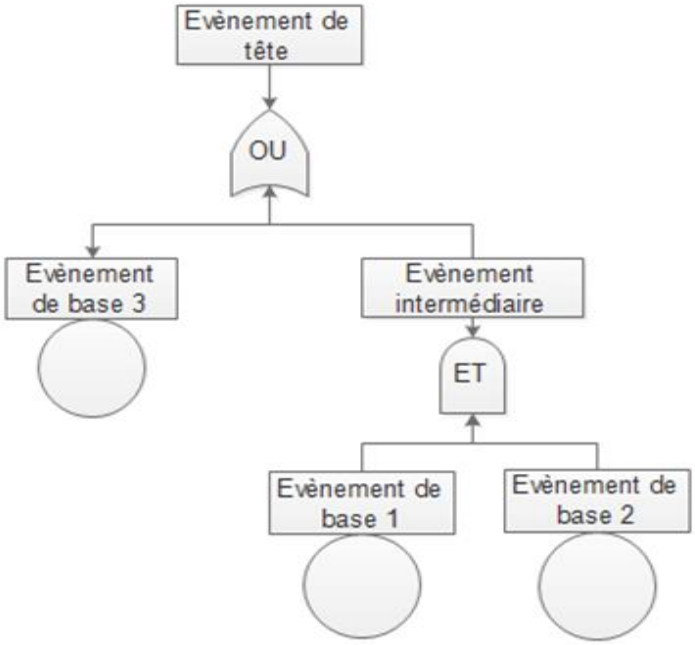


Figure 29 Arbre de défaillance

3.3.1.3.Elaboration des diagrammes d'influence

Cette étape consiste à construire un diagramme qui permet d'intégrer l'effet des conditions du système sur les probabilités des évènements de base de l'arbre de défaillance et les performances de la barrière.

Les conditions du système sont représentées par des facteurs influençant le risque ou RIF *(*RIF, *Risk Infuencing Factors*). Il existe 5 catégories de RIFs : système technique, tâche, contrôle administratif, facteur organisationnel et personnel, détaillées dans l'annexe 6.

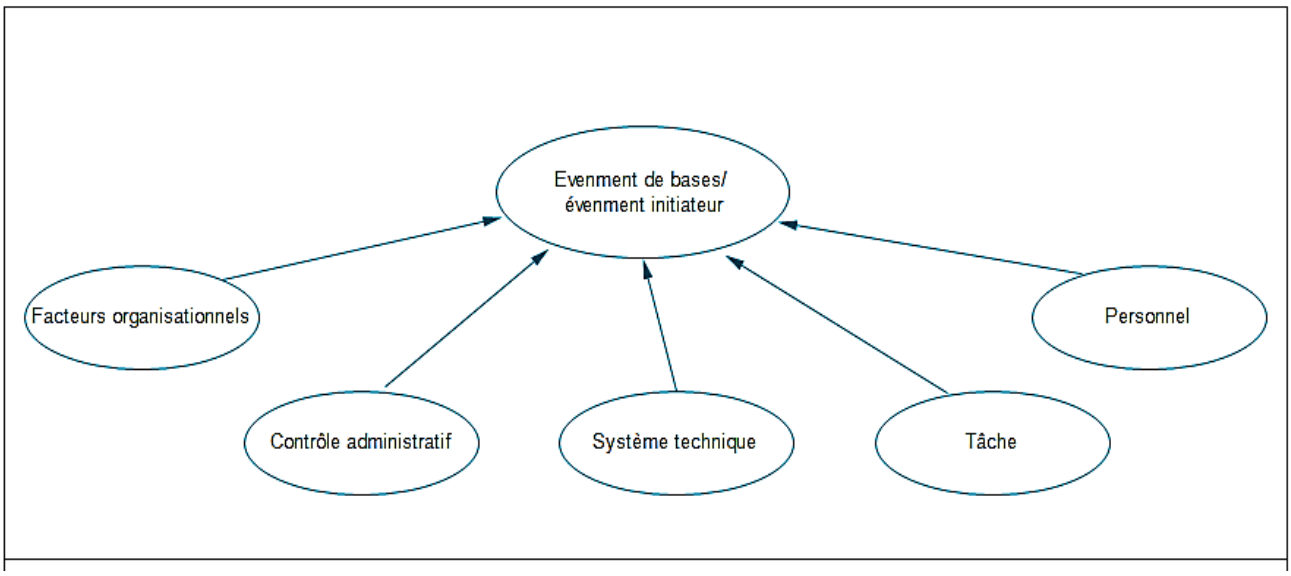


Figure 30 Diagramme d'influence de risque

3.3.1.4.Etablissement des scores de RIF

Un score doit être attribué pour chaque RIF identifié. Il varie de A à F tel que A correspond aux meilleures pratiques par rapport au standard (norme) de l'industrie et F au pire. Le score nous renseigne sur l'état du RIF pour l'installation étudiée. Le tableau 35 donne la signification des scores.

Système générique pour le score des RIFs (Aven, Sklet, & Vinnem, 2006)

Tableau 35 Explication des scores

Score	Explication
A	Etat qui correspond à la meilleure norme dans l'industrie
B	Etat qui correspond à un niveau supérieur à la moyenne de l'industrie
C	Etat qui correspond à la moyenne de l'industrie
D	Etat qui correspond à un niveau légèrement inférieur à la moyenne de l'industrie
E	Etat qui correspond à un niveau nettement inférieur à la moyenne de l'industrie
F	Etat qui correspond au pire pratique dans l'industrie

3.3.1.5. Affectation des poids des RIFs

Dans cette étape, on détermine les poids de l'influence des RIFs sur la fréquence ou la probabilité des évènements de base. Un grand poids implique une forte influence et un poids faible, une faible influence.

Une échelle de cinq points (de grande importance à la faible importance) est appliquée. Quantitativement, les RIF sont donnés en fonction des poids relatifs sur l'échelle de 10 - 8 - 6 - 4 - 2.

Les poids des RIFs sont normalisés à la somme des poids pour les RIF influençant un seul événement de base. La somme des poids normalisés doit être égale à 1.

L'identification des RIFs et l'attribution de leurs poids et de leurs scores, se fait à partir des résultats des interviews effectués auprès des personnes chargées de l'exploitation.

3.3.1.6.Ajustement des valeurs de probabilité

Dans cette étape, les probabilités des évènements de base vont être corrigées en tenant compte des scores et des poids des RIFs identifiés pour chaque évènement (Aven, Sklet, & Vinnem, Barrier and operational risk analysis of hydrocarbon releases (BORARelease); part I Method description, 2006).

$$P_{rev}(A) = P_{moy}(A).\sum_{i=1}^{n} W_i.Q_i \qquad (3.4)$$

Où :

A : évènement de base

$P_{rev}(A)$: Probabilité ajustée

$P_{moy}(A)$: Probabilité moyenne de l'occurrence de l'évènement *A* Donnée par la base de données

W_i : Poids normalisé du RIF *i* pour l'évènement *A*

Q_i : Mesure du score de RIF et *n* est le nombre des RIFs impliqués pour l'évènement *A*

Avec :

$$\sum_{i=1}^{n} W_i = 1 \qquad (3.5)$$

Des valeurs numériques doivent être attribuées pour les poids Q_i des RIFs. Pour ce faire, on utilise les valeurs limites des probabilités des évènements de base $P_{low}(A)$ et $P_{high}(A)$, limite inférieure et supérieure respectivement. En effet, les bases de données assignent non pas une valeur unique pour la probabilité des évènements de base, mais des intervalles avec des valeurs moyennes. Ces données sont issues du retour d'expérience.

Les formules utilisées pour calculer numériquement les poids des RIFs sont données ci-dessous :

$$Q_i(S) = \begin{cases} {P_{low}}/{P_{moy}} & , S = A \\ \frac{P_{low}}{P_{moy}} + \frac{(S_B - S_A)(1 - \frac{P_{low}}{P_{moy}})}{S_C - S_A} & , S = B \\ 1 & , S = C \\ 1 + \frac{(S_D - S_C)(\frac{P_{high}}{P_{moy}} - 1)}{S_F - S_C} & , S = D \\ 1 + \frac{(S_E - S_C)(\frac{P_{high}}{P_{moy}} - 1)}{S_F - S_C} & , S = E \\ {P_{high}}/{P_{moy}} & , S = F \end{cases} \quad (3.6)$$

Avec : $S_A = 1$, $S_B = 2$, $S_C = 3$, $S_D = 4$, $S_E = 5$ et $S_F = 6$.

3.3.1.7.Calcul de la probabilité de l'événement de tête et allocation du SIL

L'évaluation de l'arbre de défaillance se fera avec les probabilités ajustées des évènements de bases. La probabilité obtenue pour l'évènement de tête va être situé dans les intervalles correspondant au tableau 13 afin de déterminer le degré d'intégrité du SIS étudié.

3.3.2. Arbre de défaillance flou

Une autre manière de prendre en compte les incertitudes sur les probabilités de défaillance des composants d'un système induites par les conditions d'exploitation dont ils sont soumis, est d'utiliser la logique floue. Contrairement à la méthode BORA développée ci-dessus, l'utilisation de la logique floue dans les arbres de défaillances ne prend pas en compte l'état des RIFs mais la dispersion des probabilités données par les bases de données. En effet, la dispersion des données traduites par des intervalles de probabilités avec une valeur moyenne, résulte de la différence des états des RIFs des situations qui on servies à la construction de ces bases de données.

Parmi le grand nombre des publications proposant différentes approches pour intégrer la logique floue dans les arbres de défaillances, nous avons choisi d'utiliser l'arbre de défaillance floue proposé par Liang et Wang (Liang & Wang, 1993). Cet arbre utilise des fonctions d'appartenance de type triangulaire (Figure 31) pour représenter les probabilités des évènements de bases, ce qui correspond intuitivement le plus aux valeurs de probabilité données par les bases de données avec une valeur moyenne et des valeurs limites supérieures et inférieures.

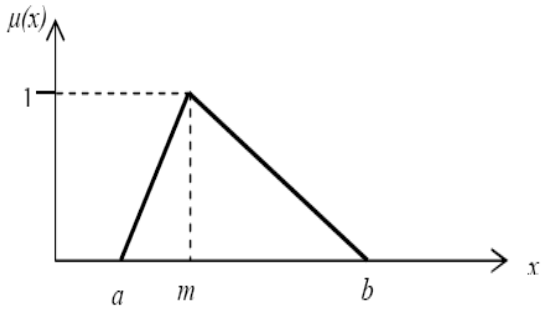


Figure 31 Fonction d'appartenance de probabilité de défaillance

Où *m* est la valeur moyenne, *a* la limite inférieure et *b* la limite supérieur, de la probabilité donnée par les bases.

Les calculs des portes logiques ET et OU deviendront :

Porte logique ET :

$$P(A) = \prod_{i=1}^{n} P(A_i) = (\prod_{i=1}^{n} a_i \,, \prod_{i=1}^{n} m_i \,, \prod_{i=1}^{n} b_i) \tag{3.7}$$

Avec :

$$P(A_i) = (a_i, m_i, b_i\,) \tag{3.8}$$

Et

$$P(A) = (a, m, b\,) \tag{3.9}$$

Porte logique OU :

$$\begin{aligned} P(A) &= 1 - \prod_{i=1}^{n} (1 - P(A_i)) \\ &= 1 - (\prod_{i=1}^{n}(1 - b_i)\,, \prod_{i=1}^{n}(1 - m_i)\,, \prod_{i=1}^{n}(1 - a_i)) \\ &= (1 - \prod_{i=1}^{n}(1 - b_i)), (\,1 - \prod_{i=1}^{n}(1 - m_i))\,, (1 - \prod_{i=1}^{n}(1 - a)) \end{aligned} \tag{3.10}$$

La probabilité de l'évènement de tête est aussi un nombre flou avec une fonction d'appartenance triangulaire. (Liang & Wang, 1993) Cependant, pour trouver le SIL du SIS analysé, on doit avoir non pas un nombre flou mais une valeur ordinale. Passer d'un nombre flou à un nombre ordinal est appelé défuzzification. La méthode utilisée est celle du centre de gravité. Il suffirait de calcul l'abscisse du centre de gravité :

$$P(A) = \frac{a+m+b}{3} \tag{3.11}$$

3.3.3. Application des méthodes d'allocation des SILs des SIS

D'aprés les résultats de la HazOp_RPN, nous avons déterminé les SIS implémentés dans la centrale électrique Hamma II pour mitiger les risques des scénarios conduisant à un incendie ou une explosion. Tel que pour le système fuel, nous avons sélectionné le système déluge et pour le système de refroidissement de l'alternateur, le système d'arrêt d'urgence

3.3.3.1.Système déluge

Le système déluge est composé de 8 capteurs de température, un traitement logique et comme actionneurs et d'une vanne déluge reliée au réseau d'eau d'incendie.

3.3.3.1.1. Application de la méthode BORA

a. Modèle base de risque

Le système déluge est utilisé dans le but de contenir et d'éteindre les feux qui peuvent survenir dans le système fuel à cause de plusieurs évènements initiateurs.

Nous avons relevé 4 scénarios (N°1.1 N°1.3 N°1.5 N°1.6) faisant intervenir le système déluge comme une barrière de protection. La figure 32 représente le diagramme bloc barrière correspondant au scénario N°1.3 correspondant à l'ouverture intempestive de la vanne d'alimentation des bacs qui va entrainer le débordement du fuel avec la présence d'une énergie d'activation qui peut conduire à un incendie.

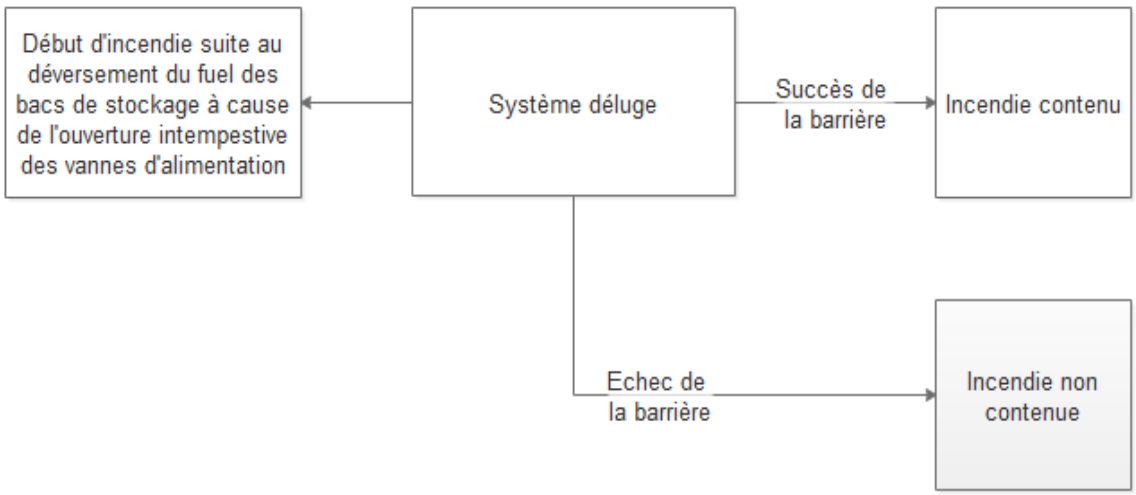


Figure 32 Barrière Bloc Diagramme système déluge

b. Arbre de défaillance du système déluge

L'arbre de défaillance correspondant au système déluge est présenté dans la Figure 32

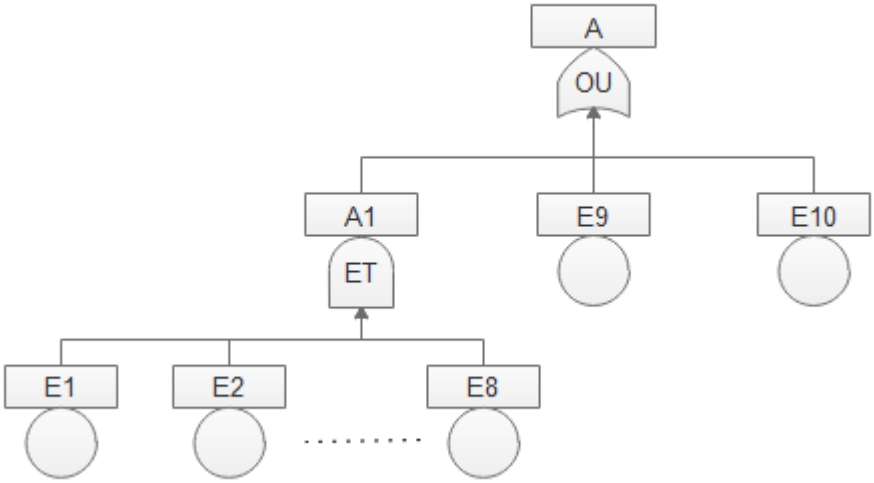


Figure 33 Arbre de défaillance du système déluge

Le calcul de la probabilité de défaillance de l'évènement de tête selon l'équation (3.2) de la porte logique ET et (3.3) pour la porte logique OU est le suivant :

$$P(A) = 1 - (1 - P(A_1)) \times (1 - P(E_9)) \times (1 - P(E_{10}))$$

$$P(A_1) = P(E_1) \times P(E_2) \times P(E_3) \times P(E_4) \times P(E_5) \times P(E_6) \times P(E_7) \times P(E_8)$$

Les évènements de base ainsi que les probabilités de défaillances (OREDA, 2002) qui leur correspondent sont présentés dans le Tableau 36. Pour la méthode de l'arbre de défaillance flou on ne prend en compte que les valeurs moyennes des intervalles.

Tableau 36 Probabilités de défaillances des événements de base

	Evènement	**P_{low}**	**P_{moy}**	**P_{high}**
E1, E2, E3, E4, E5, E6, E7, E8	Défaillance du capteur de température	0	0,005782	0,02225
E9	Défaillances traitement logique du système déluge	0,0033691	0,06822113	0,2054623
E10	Défaillance de la vanne	0,0022776	0,008322	0,0213744

La probabilité de défaillance du système déluge obtenue par la méthode de l'arbre de défaillance conventionnel est égale à :

$$P(A) = 0.075975394$$

c. Ajustement des valeurs de probabilité par l'intégration des facteurs d'influence du risque (FIS)

Les diagrammes d'influence du risque (figures 34, 35, 36) des évènements de bases pouvant menées à la défaillance de la barrière de sécurité sont représentés ci-dessous :

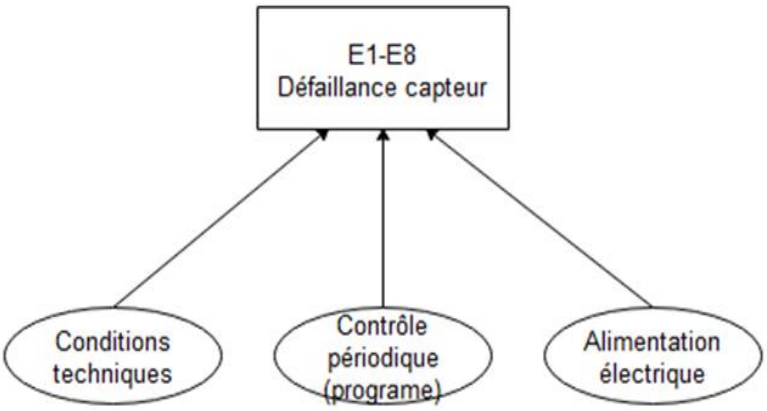


Figure 34 Diagramme d'influence de la défaillance du capteur

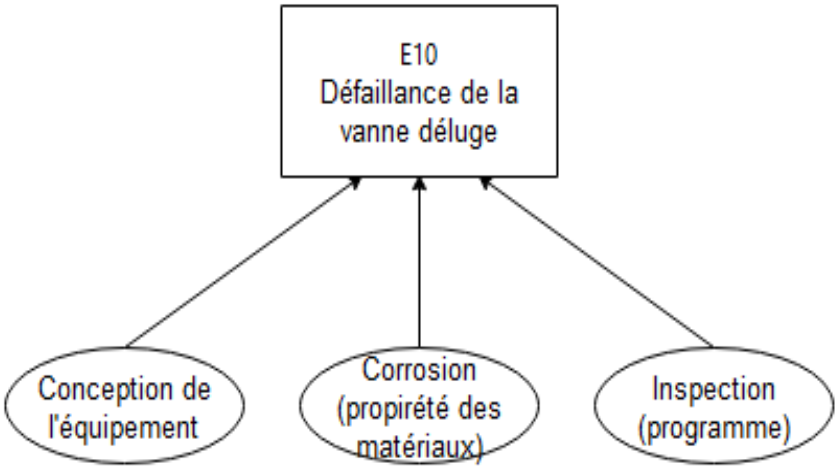


Figure 35 Diagramme d'influence de la défaillance de la vanne déluge

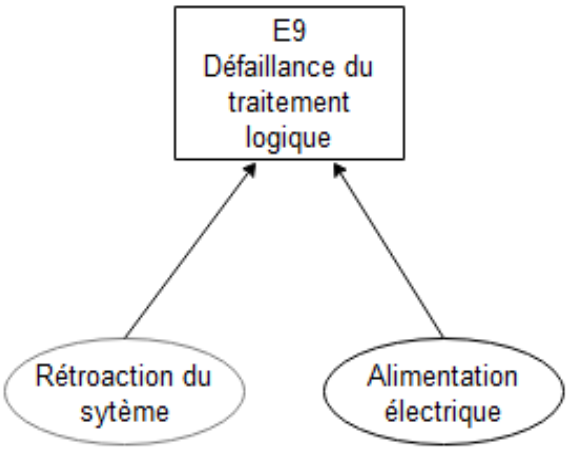


Figure 36 Diagramme d'influence de la défaillance du traitement logique

L'affectation des scores et des poids des FISs ainsi que les valeurs ajustées des probabilités de défaillances sont présentées dans le tableau 37.

Telle que la probabilité de défaillance du système déluge après la prise en compte des conditions d'exploitation est égale à

$$P(A) = 0.112635$$

Ce qui correspond à un SIL 1

Tableau 37 Résumé des résultats de la méthode BORA pour le système déluge

Evènement intermédiaire/évènement de tête	Evènement de base	Plow	Pmoy	Phigh	RIFs	Wi	Wi normalisé	Si	Qi	MF	Prév
	Défaillance vanne déluge	0,0022776	0,008322	0,0213744						1,377	0,01146392
					Conception de l'équipement	4	0.2	A	0,273		
					Propriété des matériaux (corrosion)	10	0.5	E	2,045		
					Inspection (programme)	6	0.3	C	1		
	Défaillance traitement logique du système déluge	0,0033691	0,06822113	0,2054623						1,2465	0,08504415
					Rétroaction du système	10	0.63	D	2,341		
					Alimentation électrique	6	0.37	B	0,524		
	Défaillance capteur de température	0	0,005782	0,02225						1,1882	0,00687073
					Conditions techniques	8	0.33	D	1,945		
					Contrôle périodique	10	0.42	C	1		
					Alimentation électrique	6	0.25	B	0,502		
Défaillance de la détection d'incendie (8 capteurs de températures	$1{,}249.10^{-18}$										$4{,}9.10^{-18}$
Défaillance du système déluge	0,075975394										0.112635

3.3.3.1.2. Méthode de l'arbre de défaillance flou

La méthode de l'arbre de défaillance flou utilise la même représentation graphique que l'arbre de défaillance flou (figure 33) prend en compte toutes les valeurs des probabilités de défaillance données par les bases de données représentées dans le tableau 36. Tel que les valeurs limites des PFD représentent les points de base des fonctions d'appartenance triangulaires et la moyenne, leur hauteur.

En utilisant les formules (3.7) et (3.10) pour le calcul des portes logiques ET respectivement OU, nous avons calculé les fonctions d'appartenance représentant l'évènement intermédiaire A1 et l'évènement de tête A. Les résultats sont présentés dans le tableau 38 avec :

$$P(A) = (P_{low}(A), P_{low}(A), P_{low}(A))$$

$$P_{low}(A) = (1 - (1 - P_{low}(A_1)) * (1 - (1 - P_{low}(E_9)) * (1 - (1 - P_{low}(E_{10}))$$

$$P_{moy}(A) = (1 - (1 - P_{moy}(A_1)) * (1 - (1 - P_{moy}(E_9)) * (1 - (1 - P_{moy}(E_{10}))$$

$$P_{high}(A) = (1 - (1 - P_{high}(A_1)) * (1 - (1 - P_{high}(E_9)) * (1 - (1 - P_{high}(E_{10}))$$

$$Avec : P(A_1) = (P_{low}(A_1), P_{low}(A_1), P_{low}(A_1))$$

$$P_{low}(A_1) = P_{low}(E_1) \times P_{low}(E_2) \times P_{low}(E_3) \times P_{low}(E_4) \times P_{low}(E_5) \times P_{low}(E_6) \times P_{low}(E_7) \times P_{low}(E_8)$$

$$P_{moy}(A_1) = P_{moy}(E_1) \times P_{moy}(E_2) \times P_{moy}(E_3) \times P_{moy}(E_4) \times P_{moy}(E_5) \times P_{moy}(E_6) \times P_{moy}(E_7) \times P_{moy}(E_8)$$

$$P_{high}(A_1) = P_{high}(E_1) \times P_{high}(E_2) \times P_{high}(E_3) \times P_{high}(E_4) \times P_{high}(E_5) \times P_{high}(E_6) \times P_{high}(E_7) \times P_{high}(E_8))$$

Tableau 38 Fonctions d'appartenance des événements intermédiaires et l'événement de tête

	Evènement	P_{low}	P_{moy}	P_{high}
A1	Défaillance de la détection d'incendie	0	$1{,}25.10^{-18}$	$6{,}01.10^{-14}$
A	Défaillance du système déluge	0,005639027	0,075975394	0,222445067

En défuzzifiant la fonction d'appartenance de l'évènement de tête, nous trouverons la probabilité de l'évènement de tête est égale à :

$$P(A) = \frac{P_{low}(A) + P_{moy}(A) + P_{high}(A)}{3} = 0{,}101353162$$

Ce qui correspond à un SIL de niveau 1.

3.3.3.2.Système d'arrêt d'urgence du système hydrogène

La boucle de surveillance des fuites d'hydrogène est composée de 3 détecteurs d'hydrogène, d'un traitement logique et d'une vanne d'arrêt d'urgence comme actionneur.

3.3.3.2.1. Application de la méthode BORA

a. Modèle base de risque

Nous avons relevé 5 scénarios faisant intervenir la boucle de surveillance des fuites d'hydrogène comme une barrière de sécurité. Le diagramme bloc barrière correspondant au scénario N°2.4 est présenté dans la figure 37.

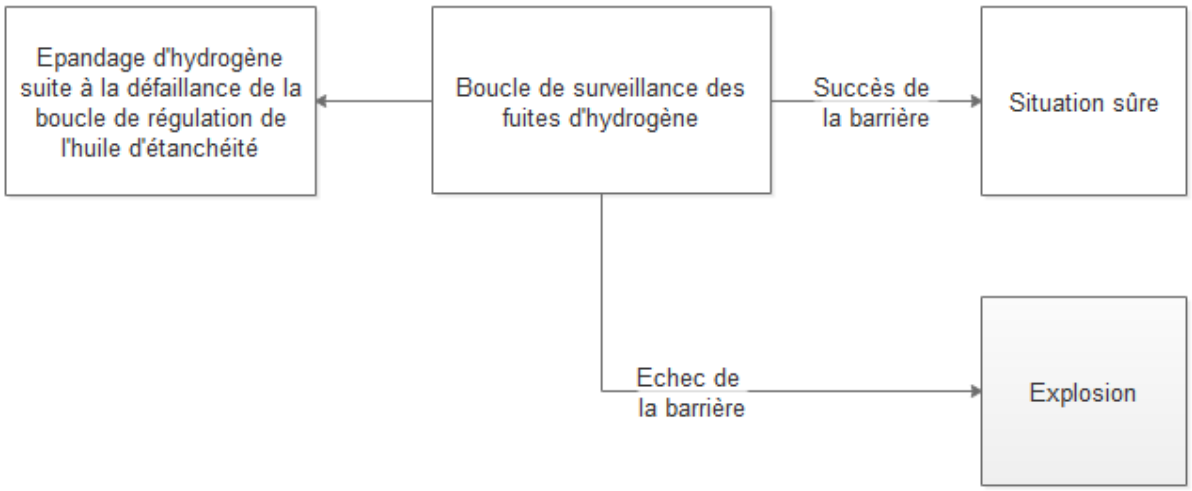


Figure 37 Barrière Bloc Diagramme du système d'arrêt d'urgence

b. Arbre de défaillance du système d'arrêt d'urgence

L'arbre de défaillance correspondant à la défaillance du système d'arrêt d'urgence du système hydrogène est présenté dans la figure 38.

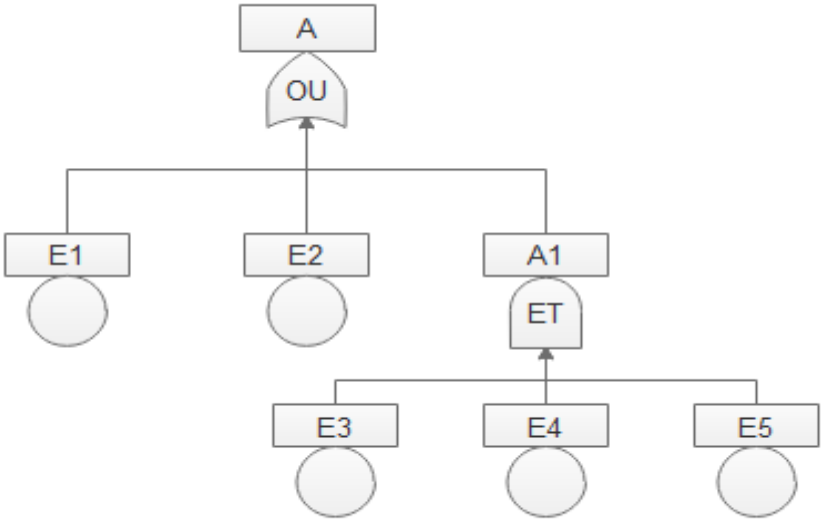


Figure 38 Arbre de défaillance du système d'arrêt d'urgence

Les évènements de base ainsi que les probabilités de défaillances (OREDA, 2002) qui leur correspondant sont présentés dans le tableau 39.

Tableau 39 Probabilités de défaillances des événements de base

Symboles	Composants	P_{low}	P_{moy}	P_{high}
E1	Traitement logique	0,0033691	0,0682211	0,2054623
E2	Défaillance de la vanne d'arrêt d'urgence du système d'H2	0,0038544	0,0097236	0,0204108
E3	Détecteur 1	0,0007008	0,0032412	0,0071832
E4	Détecteur 2	0,0007008	0,0032412	0,0071832
E5	Détecteur 3	0,0007008	0,0032412	0,0071832

L'évènement intermédiaire A1 représente la défaillance de la détection d'hydrogène. L'évènement de tête A représente la défaillance de la boucle de surveillance des fuites d'hydrogène.

Les résultats obtenus par la méthode de l'arbre de défaillance conventionnel pour le système d'arrêt d'urgence sont présentés dans le tableau 40.

Tableau 40 Probabilités de défaillances du système d'arrêt d'urgence

Symboles	Composant	P_{moy}
A1	Détection H2	$3{,}405.10^{-8}$
A	Défaillance de la boucle de surveillance des fuites d'H2	0,07728138

c. Ajustement des valeurs de probabilité par l'intégration des facteurs d'influence du risque (FIS)

Les diagrammes d'influence de risque des évènements de base pouvant mené à la défaillance de la barrière de sécurité sont représentés dans les figures 39, 40 et 41.

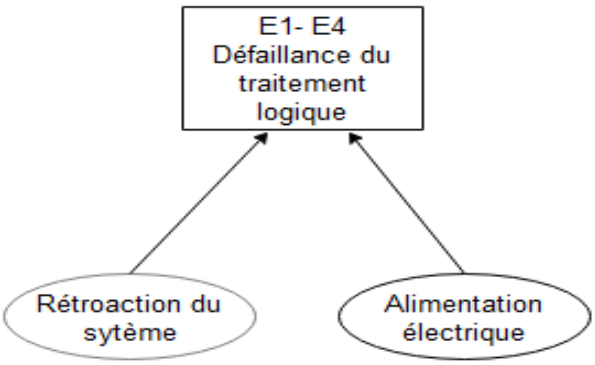


Figure 39 Diagramme d'influence de défaillance du traitement logiquement du système

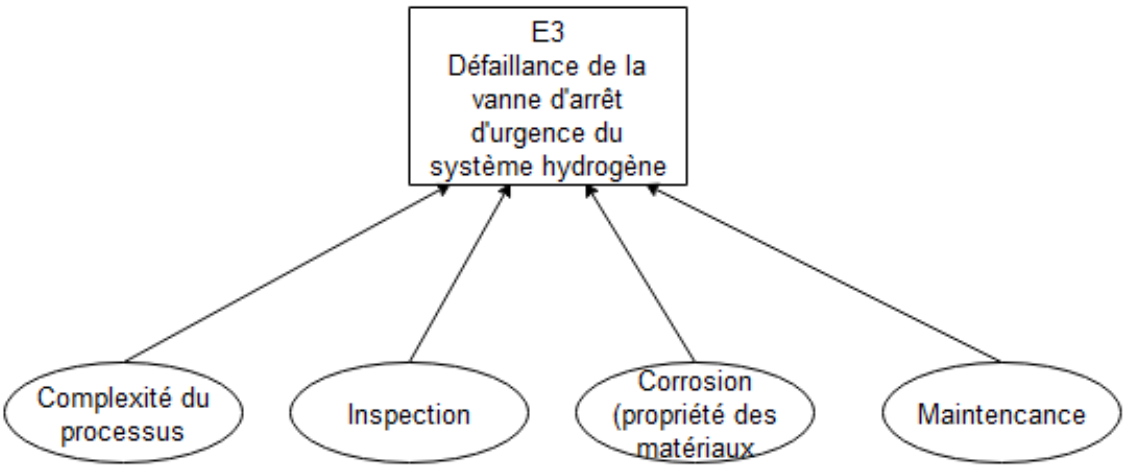


Figure 40 Diagramme d'influence de la défaillance de la vanne d'arrêt d'urgence du système hydrogène

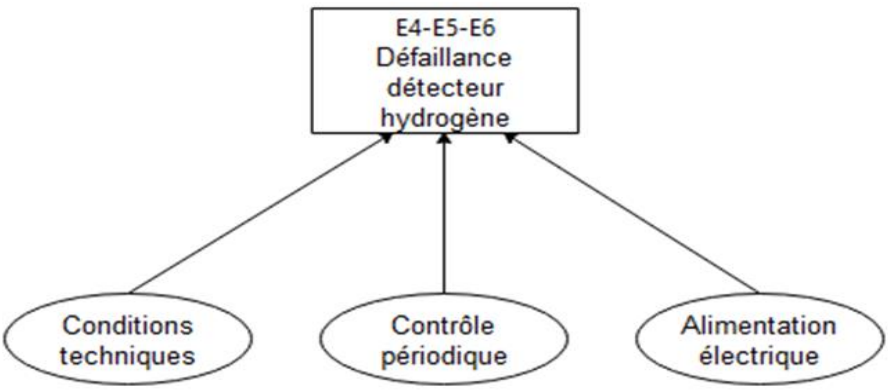


Figure 41 Diagramme d'influence de la défaillance du détecteur d'hydrogène

L’affectation des scores et des poids des FISs ainsi que les valeurs ajustées des probabilités de défaillances sont présentés dans tableau 41.

Tableau 41 Résumé des résultats de la méthode BORA pour le système d'arrêt d'urgence

Evènement intermédiaire/évènement de tête	Evènement de base	Plow	Pmoy	Phigh	RIFs	Wi	Wi normalisé	Si	Qi	MF	Prév
	Défaillance de la vanne d'arrêt d'urgence du système d'H2	0,0038544	0,0097236	0,0204108						1,211	0,01677826
					Complexité du processus	6	0.25	B	0,698		
					Propriété des matériaux (corrosion)	8	0.33	D	1,366		
					Inspection	6	0.25	E	1,732		
					Maintenance	4	0.17	C	1		
	Défaillances détecteur d'hydrogène	0,0007008	0,0032412	0,0071832						1.510	0,00489465
					Conditions techniques	8	0.33	E	1,810		
					Contrôle périodique	10	0.42	E	1,810		
					Alimentation électrique	6	0.25	B	0,608		
Défaillance de la détection hydrogène	3,405E-08										$1{,}17264.10^{-7}$
	Traitement logique	0,0033691	0,06822113	0,2054623						1,246	0,0846862
					Rétroaction du système	10	0.63	C	2,341		
					Alimentation électrique	6	0.37	B	0,524		
Défaillance de la boucle de surveillance des fuites d'H2	0.07728138										0.100043678

3.3.3.2.2. Application de la méthode Arbre de défaillances flou pour le système d'arrêt d'urgence

Les fonctions d'appartenance représentant l'évènement intermédiaire A1 et l'évènement de tête A sont présentées dans le tableau 42.

Tableau 42 Fonctions d'appartenance des événements intermédiaires et l'événement de tête

Symboles	Composants	P_{low}	P_{moy}	P_{high}
A1	**Détection H2**	$3{,}4418.10^{-10}$	$3{,}405.10^{-8}$	$3{,}7064.10^{-7}$
A	**Défaillance de la boucle de surveillance des fuites d'H2**	0,007210882	0,07728138	0,22167945

En défuzzifiant la fonction d'appartenance de l'évènement de tête, nous trouverons la probabilité de l'évènement de tête est égale à :

P(A) = 0,102057236

3.3.4. Discussion des résultats obtenus

3.3.4.1. Détermination des SILs requis

La comparaison entre les deux approches (conventionnel et flou) montre des différences dans les valeurs du SIL obtenues.

On remarque que le SIL déterminé par le model flou est caractérisé par une appartenance à deux niveaux successive mais avec un degré d'appartenance différent. Le choix du SIL requis dépend de ce dernier tel qu'on choisit le niveau ayant le plus grand degré d'appartenance.

Nous avons obtenu un SIL requis de niveau 2 pour l'ensemble des scénarios sélectionnés.

3.3.4.2. Allocation des SILs des SIS existants

a. Système déluge

Les probabilités de défaillances du système déluge (évènement de tête A), obtenues par les différentes méthodes sont :

- AdD conventionnel : P(A) =0,075975394 qui correspond au SIL 2 ;
- BORA : P(A) = 0.112635, correspondant au SIL 1,
- AdD Flou : P(A) = 0,101353162, correspondant au SIL 1.

Avec P(A) représente la probabilité moyenne de défaillance sur demande (PFD_{avg}) du système déluge.

La norme CEI 61511-1 spécifie dans sa section 11, qu'un SIS de niveau 2 ou plus doit avoir une unité de traitement logique indépendante de celle utilisée pour la conduite du procédé. On peut déduire que le SIL du système déluge est de niveau 1.

Nous remarquons que les résultats des PFD_{avg} obtenus par la méthode BORA et AdD flou sont très rapprochés. Cela est dû au fait que la méthode BORA prend en compte les conditions d'implantation et d'exploitation du SIS, et la méthode AdD flou, dispersion des probabilités données par les bases de données.

b. Système d'arrêt d'urgence du système Hydrogène

Les probabilités de défaillances du système d'arrêt d'urgence du système Hydrogène (évènement de tête A), obtenues par les différentes méthodes sont :

- AdD conventionnel : P(A) = 0.07728138 avec un SIL de niveau 2 ;
- BORA : P(A) = 0.100043678 correspondant au SIL 1 ;
- AdD Flou : P(A) = 0.102057236, ce qui correspond au SIL 1.

La norme CEI 61511-1 recommande dans sa section 11 d'assigner un SIL 1 aux SIS possédant une unité de traitement logique commune avec une boucle de régulation utilisée dans le procédé et qui peut être l'origine d'une défaillance faisant intervenir le SIS. Ce qui correspondant dans notre cas, au scénario N°2.4, où la boucle de régulation de l'huile d'étanchéité qui est à l'origine de l'évènement redouté possède le même traitement logique que le système d'arrêt d'urgence. Cela nous conduit à attribuer un SIL 1 au système d'arrêt d'urgence et de considérer la pertinence des résultats convergents de la méthode BORA et de l'AdD flou.

Conclusion

En faisant appel à différents concepts comme l'intelligence artificielle et à des méthodes permettant de prendre en compte les conditions d'exploitation des barrières de sécurité, nous avons proposé une nouvelle démarche d'analyse des barrières.

L'analyse des barrières qui s'est faite en deux étapes nous a permis de déterminer les objectifs de sécurité devant être atteints pour rendre le risque d'accidents majeurs acceptable et d'analyser ensuite les barrières de sécurité mises en place du point de vue de leur intégrité et

Chapitre 4 : Optimisation et conception des SIS

Introduction

Les résultats de l'analyse des barrières ont clairement démontré que les barrières de sécurité mises en place par l'entreprise ne sont pas suffisantes du point de vue de leur fiabilité par rapport aux scénarios d'accidents majeurs identifiés dans l'étape de l'évaluation.
Nous allons proposer dans ce chapitre des modifications des SIS mis en place dans le système fuel et le système de refroidissement de l'alternateur ainsi qu'un nouveau SIS pour le système gaz naturel afin d'atteindre l'objectif de la fiabilité visé des SIS et ainsi la réduction adéquate des risques.

Pour ce faire, il faudrait définir au départ une structure simple pour les sous-systèmes des SIS et leur allouer des redondances. En introduisant le coût comme un paramètre dans nos propositions, nous aurons un problème d'optimisation du coût des SIS sous la contrainte du SIL requis. Les résultats de cette optimisation seront des architectures de type structure simple. Ces dernières impliquent un nombre élevé de connexions entre les composants du SIS. Pour pallier à ce problème, des structures complexes vont être utilisées, impliquant moins de connexions et satisfaisant la contrainte du SIL requis. Afin d'évaluer la fiabilité des nouvelles structures proposées, nous utiliseront le concept de réseau de fiabilité.

Ce chapitre est organisé en trois parties. Dans la première partie nous citerons les différentes structures de systèmes ainsi que les formules permettant d'obtenir leur fiabilité. Dans la seconde partie, des notions de base sur la théorie des graphes et les réseaux de fiabilité vont être présentées. Dans la dernière partie, nous appliqueront ces concepts afin d'optimiser et de concevoir la structure des SIS.

4.1. Structure des systèmes

Le développement d'un système se fait par le recensement de tous ses composants et la connaissance de l'agencement et les connexions qui les rassemblent.
Dans cette section nous allons définir les différentes configurations que peut présenter un système.

4.1.1. Système à configuration simple

4.1.1.1. Système série

Le système en série (Figure 42) est un système caractérisé par un enchaînement linéaire de *n* éléments. D'après cette structure la défaillance de l'un des *n* composants entraînera la défaillance du système complet car le fonctionnement de chaque élément dépend du fonctionnement de celui qui le précède (Christiane, 1997).

Figure 42 Système série

La fiabilité du système complet R_s est égale au produit des fiabilités de chaque composant :

$$R_S = \prod_{i=1}^{n} R_i \quad (4.1)$$

4.1.1.2. Système parallèle

Le système parallèle (Figure 43) est caractérisé par une association parallèle de tous les composants. Dans cette structure la défaillance de l'un ou de plusieurs éléments n'entraîne pas la panne du système. Ce dernier n'est défaillant que si l'ensemble des éléments tombent en panne.

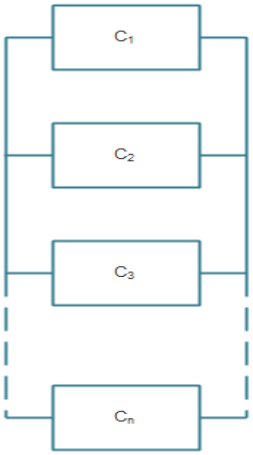


Figure 43 Système parallèle

La probabilité de panne du système F_S est égale au produit de la probabilité de panne de chaque composant.

$$F_S = \prod_{i=1}^{n} F_i \quad (4.2)$$

Alors la fiabilité R_s du système est :

$$R_S = 1 - \prod_{i=1}^{n} (1 - R_i) \quad (4.3)$$

Avec :

$$R_S = 1 - F_s \quad (4.4)$$

Et :

$$R_i = 1 - F_i \quad (4.5)$$

4.1.1.3. Système série parallèle

C'est un système constitué de *n* sous-systèmes connectés en parallèle tel que chaque sous-système est composé de *k* éléments placée en série. C'est le résultat de l'association des deux systèmes série parallèle (Figure 44) (Christiane, 1997).

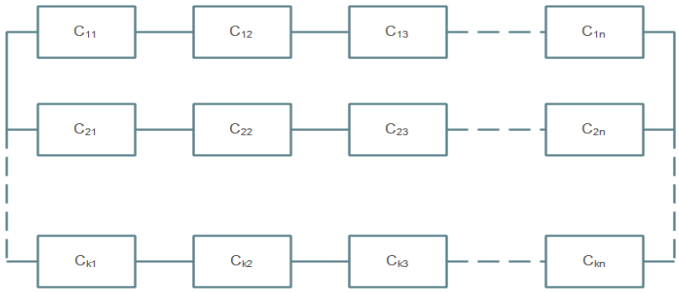


Figure 44 Système série-parallèle

Pour le calcul de la fiabilité, on doit modéliser chaque sous-système en série par un seul composant, tel que la fiabilité d'un sous-système en série *i* est égale à :

$$R_i = \prod_{j=1}^{n} R_{ij} \tag{4.6}$$

Alors la fiabilité R_S du système complet est

$$R_S = 1 - \prod_{i=1}^{k}(1 - R_i) \tag{4.7}$$

$$R_S = 1 - \prod_{i=1}^{k}\left(1 - \prod_{j=1}^{n} R_{ij}\right) \tag{4.8}$$

4.1.1.4. Système parallèle-série :

C'est un système constitué de *n* sous-système connectés en série tel que chaque sous-système est composé de *k* éléments placés en parallèle. Cette configuration est le résultat de l'association des deux systèmes série et parallèle (Christiane, 1997) (Figure 45).

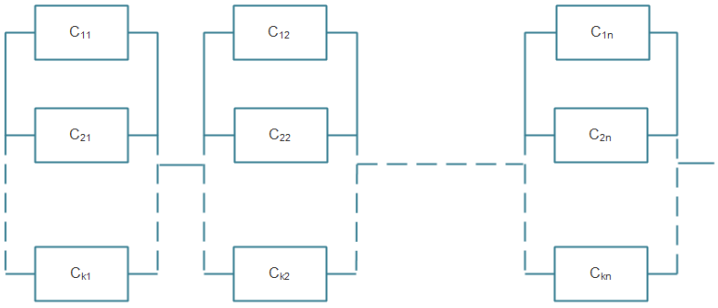


Figure 45 Système parallèle-série

Le calcul de la fiabilité se fait en réduisant le système complet en un système série tel que chaque sous système en parallèle est modélisé par un seul composant.

La fiabilité d'un sous-système en parallèle *j* est égale à :

$$R_j = 1 - \prod_{i=1}^{k} 1 - R_{ij} \quad (4.9)$$

Alors que la fiabilité R_S du système complet est égale à :

$$R_S = \prod_{j=1}^{n} R_{ij} \quad (4.10)$$

$$R_S = \prod_{j=1}^{n} [1 - \prod_{i=1}^{n} (1 - R_{ij})] \quad (4.11)$$

4.1.1.5. Système mixte

C'est une combinaison de structures séries et de structures parallèles (Figure 46). La fiabilité du système global est évaluée en décomposant le système en plusieurs sous-systèmes séries et sous-système parallèles ensuite chaque sous système est réduit en un seul composant.

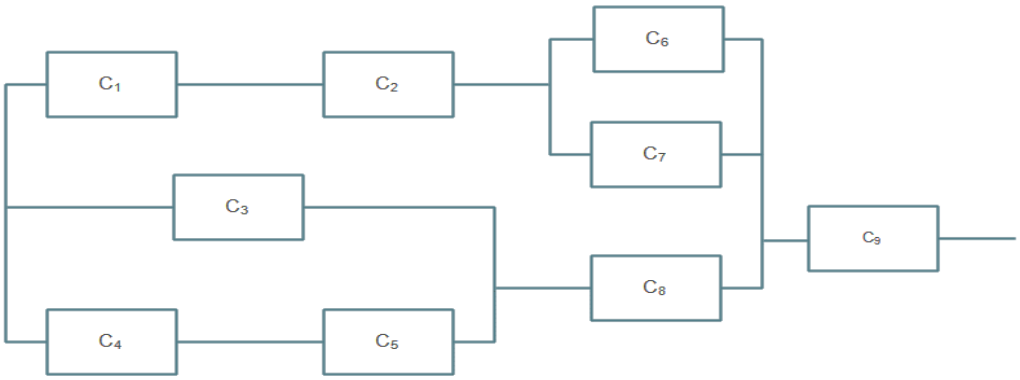


Figure 46 Système mixte

4.1.2. Systèmes à configuration quelconques

4.1.2.1. Système redondant k/n (redondance majoritaire)

C'est un système en parallèle à *n* composants qui fonctionnent seulement si au moins *k* composants de *n* fonctionnent (Figure 47).

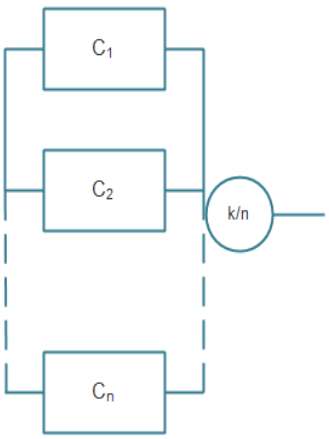


Figure 47 Système k parmi n

Si tous les composants du système ont le même taux de défaillance la fiabilité du système est la suivante (Basile & Dehombreux, 2006) :

$$R_S(k,n) = \sum_{i=k}^{n} C_n^i R^i (1-R)^{n-i} \quad (4.12)$$

Avec :

$$C_n^i = \frac{n!}{i!(n-i)!} \quad (4.13)$$

4.1.2.2. Autres types de redondance

Pour améliorer le niveau de confiance d'un système, il est possible, entre autres, de le doubler totalement (redondance totale), ou de doubler une partie de ses composants (redondance partielle de ses sous-système). A noter que la redondance peut être réalisée avec du matériel identique ou avec du matériel de technologie différente, ce dernier type de redondance permet de limiter les modes communs de défaillance. On peut distinguer plusieurs types de redondance (Chergui, 2010):

- **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 (exemple : système by-pass).
- **la redondance M/N** (ou architecture en MooN) avec M≤N, 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. La redondance majoritaire k/n est un cas particulier de la redondance M/N, où M est différent de N (ou k≠n). Dans le cas ou M est égale à 1, on se retrouve avec un système à configuration simple de type parallèle.

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

- 1oo1 (M=N=1) : Cette architecture comprend un seul élément, et toute défaillance dangereuse de cet élément empêche le traitement correct de tout signal d'alarme valide.
- 1oo2 (M= 1 et N= 2) : Cette architecture comprend deux éléments connectés en parallèle de façon que chacun puisse traiter la fonction de sécurité. Ainsi, il faudrait la défaillance dangereuse des deux éléments pour qu'un signal d'alarme valide ne soit pas traité correctement.

- 2oo2 (M= 2 et N= 2) : Cette architecture comprend deux éléments connectés en parallèle de sorte qu'il est nécessaire que les deux éléments demandent la fonction de sécurité avant que celle-ci ne survienne. La défaillance dangereuse d'un seul élément empêche le traitement correct de tout signal d'alarme valide.
- 2oo3 (M= 2 et N = 3) : Cette architecture comprend trois éléments connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie de telle sorte que l'état de sortie n'est pas modifié lorsqu'un seul élément donne un résultat différent des deux autres éléments. Il faudrait la défaillance dangereuse des deux éléments pour qu'un signal d'alarme valide ne soit pas traité correctement.

4.1.2.3. Structure pont

C'est un système qui ne peut pas être décomposé en des combinaisons séries et parallèles. Ce système fonctionne en mode parallèle-série sous le contrôle du composant pont (Figure 48).

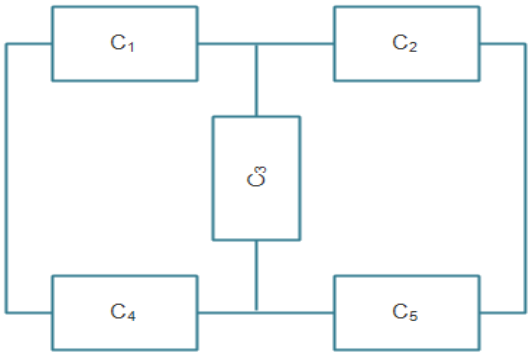


Figure 48 Structure de pont

La fiabilité du système R_S est calculée en utilisant les probabilités conditionnelles en tenant compte des deux configurations relatives à l'état du composant pont (Figure 49).

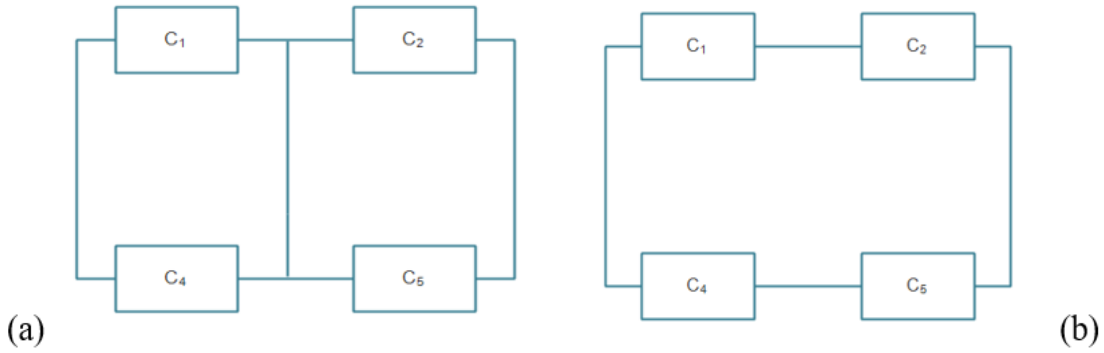


Figure 49 Décomposition d'un système en pont

Le composant pont est en marche alors

$$R_a = [1 - (1 - R_1)(1 - R_4)].[1 - (1 - R_2)(1 - R_5)] \quad (4.14)$$

Le composant pont est défaillant

$$R_b = 1 - (1 - R_2R_1)(1 - R_5R_4)] \quad (4.15)$$

Donc

$$R_S = R_3.R_a + (1 - R_3).R_b \quad (4.16)$$

4.1.3. Système à configurations complexes

C'est un système (Figure 50) qui ne contient pas de sous-systèmes placés en série, parallèle ou pont (Sellak, 2007).

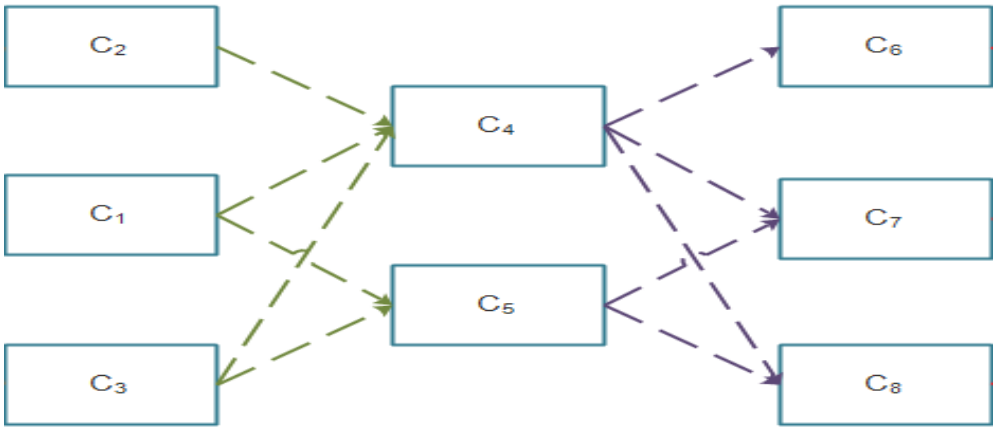


Figure 50 Exemple de configuration complexe

Les systèmes complexes englobent toutes les autres configurations et architectures de systèmes. Ces derniers ne sont que des cas particuliers de systèmes complexes.

L'évaluation de la fiabilité des systèmes complexes qui ne peuvent pas être ramené à des systèmes à configurations simples ou quelconques est difficile et compliqué. Cela exige l'utilisation de méthodes permettant la modélisation de son fonctionnement.

4.2. Théorie des graphes et réseaux de fiabilité

Un réseau de fiabilité c'est une représentation d'un système qui se base sur la théorie des graphes. Nous introduirons quelques notions de base de la théorie des graphes afin de pouvoir introduire les réseaux de fiabilité.

4.2.1. Théorie des graphes

De manière générale, un graphe permet de représenter la structure et les connexions d'un ensemble complexe en exprimant les relations entre ses éléments : réseaux de communication,

réseaux routiers, circuit électrique, etc. (Cogie & Robert , 2003). Les graphes constituent une méthode qui permet de modéliser une grande variété de problème en se ramenant à l'étude de sommets et d'arcs.

Il existe deux types de graphes, le graphe non orienté, c'est-à-dire ne présentant pas un sens dans les liaisons entre ses éléments et le graphe orienté ou digraphe. Dans notre étude, nous utiliserons les digraphes.

4.2.1.1. Définition

Un diagraphe G(V,E) est défini par l'ensemble fini V={v_1,v_2,...,v_n}, dont les élément sont appelés sommets et par l'ensemble fini E{e_1,e_2,...,e_n}, dont les élément sont appelés arcs et e = (u,v) est définis par une paire ordonnée de sommets. L'arc e va de l'extrémité initiale u à l'extrémité finale v.

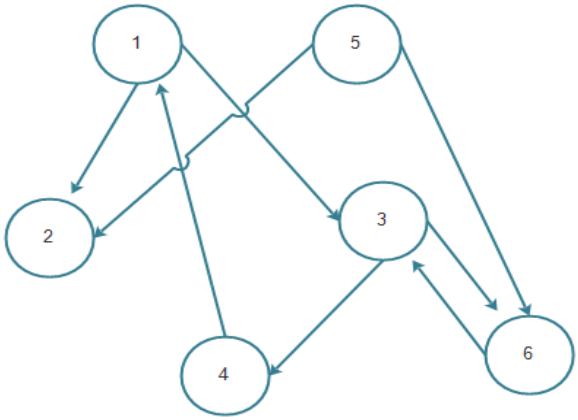


Figure 51 Graphe orienté

L'ensemble des arcs et des sommets dans le graphe de la figure 51 sont :V={1,2,3,4,5,6} et E={(1,2),(1,3),(3,4),(3,6),(4,1),(5,2),(5,2),(6,3)}.

Un chemin conduisant d'un sommet a au sommet b est une suite ayant pour élément alternativement des sommets et des arcs commençant et se terminant par un sommet. Le chemin conduisant de l'élément 1 à l'élément à l'élément 6 est : {1, (1, 3), 3, (3, 6), 6}.

4.2.1.2. Représentation matricielle

Un graphe peut être représenté par une matrice d'adjacences (n x n) tel que les lignes et les colonnes représentent les sommets du graphe. Un "1" à la position (i, j) signifie qu'un arc part de i pour rejoindre j.

C'est une matrice booléenne, carrée et non symétrique. La représentation matricielle de l'exemple de la figure 51 est comme suit :

$$M = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \quad (4.17)$$

4.2.2. Réseaux de fiabilité

Un réseau est un système dans lequel les entités communiquent entres elles, en envoyant un flux qui circule d'un nœud source à un nœud cible ce qui correspond à un diagraphe dont les nœuds et les arcs peuvent tomber en panne suivant une certaine probabilité.

4.2.2.1. Définition

Un réseau de fiabilité R est un graphe orienté G=(V,E) dont les arcs représentent les composants E={C_1,C_2,...,C_n}et les sommets V={V_1,V_2,...,V_n}représentent les nœuds.

Un réseau de fiabilité est caractérisé par deux sommets $S \in V$ et $T \in V$ qui sont appelés respectivement « origine » et « extrémité ». Tous arcs reliés à l'origine sont sortant et rentrant dans le cas de l'extrémité du sommet (Kaufmann, Grouchko, & Cruon, 1975).

Chaque arc $U_i \in U$ est noté $(V_jV_k)_{C_l}$ Tel que $V_jV_k \in V$ et $C_l \in E$ avec U, l'ensemble des arcs du graphe.

L'application $\Omega : U \longrightarrow V \times V$ fait correspondre à chaque arc du graphe un couple de ses extrémités. Le même couple d'extrémités peut représenter plusieurs arcs tels que chaque ars correspond à un composant.

L'application $\Delta : V \times V \longrightarrow E$ fait correspondre à chaque arc du graphe représenté par ses extrémités initiale et finale un composant. Plusieurs ars peuvent représenter le même composant.

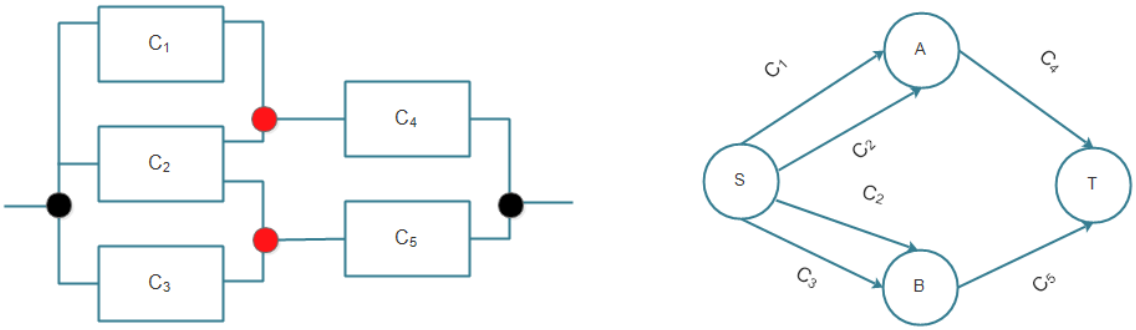


Figure 52 Exemple de schéma de connexion et de son réseau de fiabilité

La figure 52 représente un schéma de connexion d'un système avec une structure mixte et le réseau de fiabilité lui correspondant. Tel que les points de connexion (en rouge) dans le schéma

de connexion sont présenté par les sommets A et B et les points noirs sont présentés par les sommets origine S et extrémité T. L'ensemble des nœuds est $V = \{S, A, B, T\}$. L'ensemble des composants est $E = \{C_1, C_2, C_3, C_4, C_5\}$

L'application oméga est définie tel que :

$$\Omega : U \longrightarrow V \times V \tag{4.18}$$

$$\Omega\ (C_1) = (S, A)$$

L'application delta est définie tel que :

$$\Delta : V \times V \longrightarrow E \tag{4.19}$$

$$\Delta\ (A, T) = C_4$$

Le couple (S, A) est représenté par deux arcs $(SA)_{C_1}$ et $(SA)_{C_2}$(c'est-à-dire 2 composants relient ces deux points dans le schéma de connexion) et il existe deux arcs représentés par le couple (S, A) et (S, B) qui sont générés par le même composant C_2 (Rhazali, 2015).

4.2.2.2. Lien minimal et coupe minimale

Un lien C d'un réseau R est chemin conduisant du point d'origine à l'extrémité du réseau, c'est-à-dire, un sous ensemble d'arc $U' \subset U$ connectant le point S au point T.

Un lien est dit minimal lorsque aucun sous-ensemble $U'' \subset U'$ ne peut présenter un lien, tel que U' est l'ensemble des arcs du lien C.

Une coupe D d'un réseau E d'un réseau R est un sous ensemble de composants $E' \subset E$, tel que l'élimination de ces composants déconnecterait les deux extrémités du réseau, et par conséquent, il n'existerait aucun chemin reliant le point d'origine S au point d'extrémité T.

Une coupe D est dite minimale lorsque aucun sous ensemble de composant $E'' \subset E'$ ne peut présenter une coupe, tel que E' est l'ensemble des composants de la coupe D.

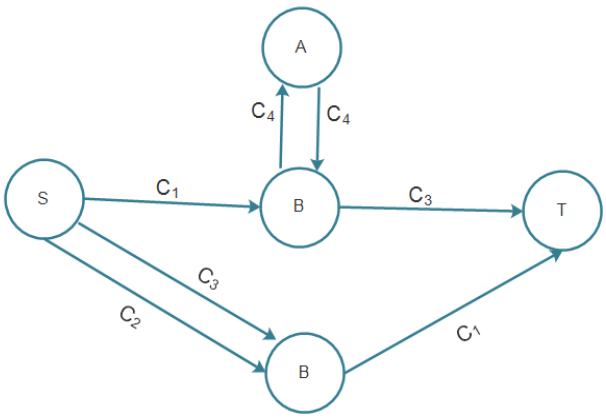


Figure 53 Exemple d'un réseau de fiabilité

Il existe 5 chemins entre le point S et le point T dans le réseau de la figure 53 et qui sont :

$$C_1 = \{(SB)_{C_1}, (BA)_{C_2}, (AB)_{C_4}, (BT)_{C_3}\}$$

$$C_2 = \{(SB)_{C_1}, (BT)_{C_3}\}$$

$$C_3 = \{(SB)_{C_1}, (BC)_{C_4}, (CT)_{C_1}\}$$

$$C_4 = \{(SC)_{C_3}, (CT)_{C_1}\}$$

$$C_5 = \{(SC)_{C_2}, (CT)_{C_1}\}$$

Les liens C_2, C_3, C_4 et C_5 sont des liens minimaux du réseau de fiabilité par contre C_1 n'est pas un lien minimal car l'ensemble des arcs du lien C_2 sont inclus dans l'ensemble des arcs du lien C_1.

$\{C_1, C_2, C_3\}$ et $\{C_1, C_3\}$ sont des coupes du réseau mais elles ne sont pas minimales alors que $\{C_1\}$ et $\{C_2, C_3, C_4\}$ sont des coupes minimales.

Toutes les architectures d'un SIS peuvent être modélisées par des réseaux de fiabilité. En effet, les réseaux de fiabilité est l'une des méthodes qui permettant l'évaluation de la fiabilité des systèmes complexes (Rhazali, 2015).

4.2.3. Evaluation de la fiabilité des systèmes complexes modélisés par un réseau de fiabilité

Il existe dans la littérature plusieurs méthodes qui traitent l'évaluation des systèmes complexes modélisés par un réseau de fiabilité :

- La technique d'énumération des états
- La technique de la table de vérité booléenne
- La méthode d'inclusion exclusion

Nous allons nous intéresser dans ce qui suit à la méthode d'inclusion-exclusion (Rhazali, 2015). L'évaluation de la fiabilité du système est basée sur la formule de Poincaré. Au départ, Nous devons déterminer tous les liens minimaux et les coupes minimales du réseau étudié. Ensuite par le biais de la formule de Poincaré, la fiabilité est exprimée par la probabilité de la réunion de l'ensemble des coupes minimales ou liens minimaux en fonction de leur nombre et leurs probabilités d'intersection.

L'adaptation de l'approche coupes minimale ou liens minimaux est conditionné par leurs nombres, tel que plus le nombre est faible plus le calcul et allégé.

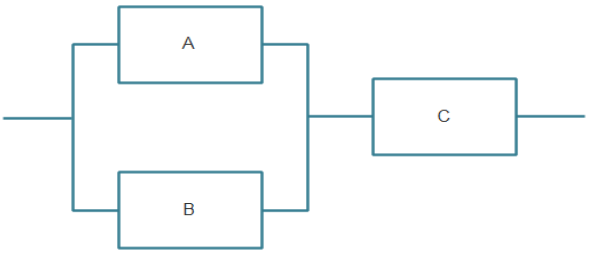


Figure 54 Exemple de diagramme de fiabilité d'un système

Les liens minimaux de la structure présentée dans la figure 54, sont $C_1 = \{AC\}$ et $C_2 = \{BC\}$.

Les coupes minimales sont $D_1 = \{AB\}$ et $D_2 = \{C\}$.

L'évaluation de la fiabilité avec la méthode d'inclusion exclusion est donnée par :

$$R_s = P(C_1 \cup C_2)$$

$$R_s = P(C_1) + P(C_2) - P(C_1 \cap C_2)$$

$$R_s = P_A P_C + P_B P_C - P_A P_B P_C$$

L'évaluation de la fiabilité à partir des coupes minimales se fait par le calcul de la probabilité que le système soit défaillant.

$$F_s = 1 - R_s$$

$$F_s = P(D_1 \cup D_2)$$

$$F_s = P(D_1) + P(D_2) - P(D_1 \cap D_2)$$

$$F_s = (1 - P_A)(1 - P_B) + (1 - P_C) - (1 - P_A)(1 - P_B)(1 - P_C)$$

La formule de Poincaré généralisée pour m liens minimaux s'écrit comme suit :

$$P(\cup_{i=1}^{m} C_i) = \sum_{i=1}^{m} P(C_i) - \sum_{1 \le i < j \le m} P(C_i \cap C_j) + \sum_{1 \le i < j < k \le m} P(C_i \cap C_j \cap C_k) + \cdots + (-1)^{m+1} P(C_1 \cap \ldots \cap C_m) \quad (4.20)$$

4.3. optimisation des architectures des SIS des systèmes critique étudiés

Dans l'étude des barrières faite dans le chapitre précédent, nous avons relevé deux systèmes instrumentés de sécurité à savoir le système déluge implanté dans le système fuel et le système d'arrêt d'urgence dans le circuit de refroidissement à hydrogène de l'alternateur. Après l'analyse de ces SIS (allocation de leur SIL) et leur comparaison avec les objectifs de sécurité qui doit être atteint (SIL requis), nous avons conclu qu'ils sont insuffisants du point de vue de leur fiabilité.

Nous allons essayer dans cette section d'optimiser leurs architectures afin d'atteindre l'objectif du SIL requis tout en minimisant le coût à allouer. Pour ce faire, nous avons divisé la résolution de ce problème en deux étapes :

- L'allocation de la redondance des sous-systèmes des SIS sous la contrainte du SIL requis et la minimisation du coût;

- Les architectures obtenues dans la première étape seront de type parallèle-série, ce qui veut dire que chaque composant d'un sous-système *n* est relié par des connexions à tous les composants du système *n-1* et du système *n+1*. Ce genre d'architecture implique un coût de connexion. En utilisant les réseaux de fiabilité et la méthode d'exclusion et d'inclusion pour l'évaluation de la fiabilité, nous allons optimiser l'architecture des SIS avec des architectures de type complexe, impliquant moins de connexions tout en satisfaisons la contrainte du SIL requis.

4.3.1. Optimisation de l'architecture du système d'arrêt d'urgence du circuit hydrogène

La configuration initiale de ce SIS est donnée dans la figure 55.

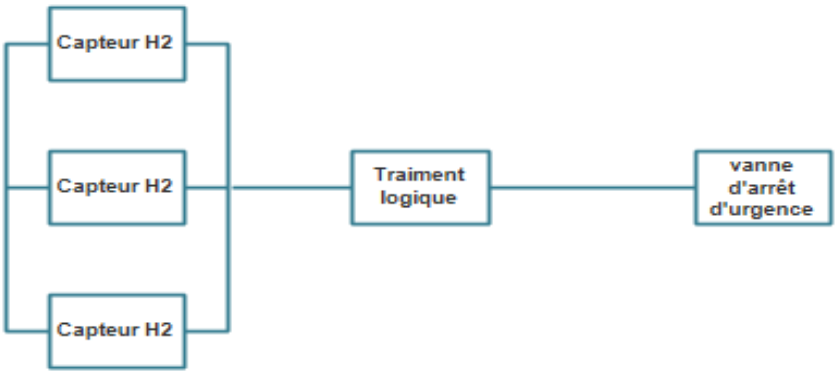


Figure 55 Schéma de connexion initiale du système d'arrêt d'urgence

Les données sur les composants de ce SIS sont présentées dans le tableau 43. En raison de l'indisponibilité des données financières sur les composants actuels du SIS, nous avons pris une moyenne des prix des composants qui sont sur le marché. Nous avons utilisé les probabilités de défaillance corrigées par la méthode BORA.

La fiabilité de chaque composant est donnée par :

$$R_i = 1 - PFD_{avg_i} \tag{4.21}$$

Tableau 43 Données sur les composants du système d'arrêt d'urgence

Composant	**PFD*avg***	**Fiabilité *R***	**Prix ($)**
Capteur Hydrogène	0,00489465	0.995105	300
Traitement logique	0,0846862	0.9153138	100
Vanne d'arrêt d'urgence	0,01677826	0.98322174	1000

Si on pose n(1) le nombre de détecteurs d'hydrogène, n(2) le nombre des cartes de traitement logique, et n(3) le nombre des vannes d'arrêt d'urgence, la fonction à optimiser, c'est-à-dire la fonction coût est donnée par :

$$F(n(i)) = 300 * n(1) + 100 * n(2) + 1000 * n(3) \quad (4.22)$$

Sous la contrainte du SIL, qui doit être de niveau 2 :

$$10^{-3} \leq PFD_{avg_{sys}} < 10^{-2} \quad (4.23)$$

La fiabilité du système est donnée par :

$$R_{sys} = 1 - PFD_{avg_{sys}} \quad (4.24)$$

Donc la contrainte sera exprimé par :

$$0.99 < R_{sys} \leq 0.999 \quad (4.25)$$

Sachant que la fiabilité du système est calculée comme suit :

$$R_{sys} = R_{sous-système_1} \times R_{sous-système_2} \times R_{sous-système_3} \quad (4.26)$$

Alors la fiabilité du système en fonction de la fiabilité de ses composants est donnée par :

$$R_{sys} = (1 - (1 - R_{capteur})^{n(1)}) \times (1 - (1 - R_{traitement})^{n(2)}) \times (1 - (1 - R_{Actionneur})^{n(3)} \quad (4.27)$$

La fonction à optimiser et la fonction contrainte écrites sur matlab[4] sont données en annexe 7. En utilisant la fonction *fmincon* de matlab, nous trouverons les résultats suivants :

$$n(1) = 3.99\,, n(2) = 2, n(3) = 2$$

Puisque les n (i) représentent le nombre de composants dans chaque sous-système, nous ne prendrons que les parties entières de chaque résultat.

La fiabilité de cette architecture est égale à :

$$R_{sys} = 0.9925$$

C'est-à-dire :

$$PFD_{avg_{sys}} = 7{,}5.10^{-3}$$

Cette probabilité correspond à un SIS de SIL 2. Le coût de l'installation est égal à 3400 $. En ne considérons pas le coût des composants déjà existants dans l'installation, le coût est égale à 1100$.

Le schéma de connexion de la nouvelle architecture du SIS est présentée dans la figure 56.

[4] Matlab R2015a

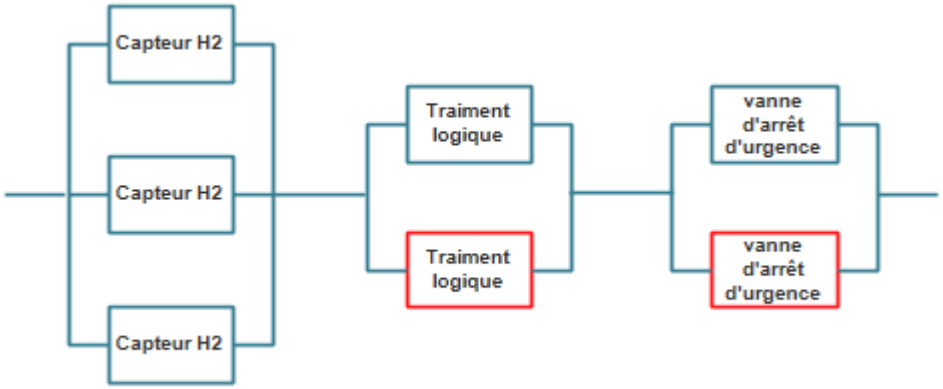


Figure 56 Le nouveau schéma de connexion du système d'arrêt d'urgence

Le réseau de fiabilité correspondant à cette architecture est donné dans la figure 57.

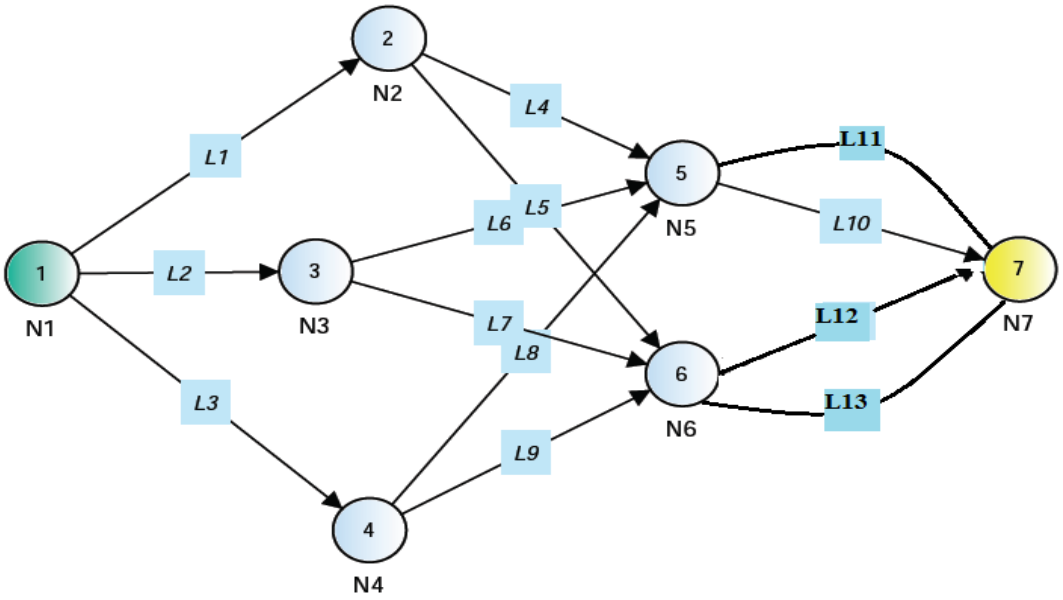


Figure 57 Réseau de fiabilité du nouveau système d'arrêt d'urgence

Les arcs de L1 à L3 représentent les détecteurs d'hydrogène. Les arcs de L4 à L19 représentent les traitements logiques. Les arcs de L10 à L13 représentent les vannes d'arrêt d'urgence. Les nœuds représentent les connexions entre les différents composants du SIS.

Nous avons construit un algorithme (annexe 7) qui permet de déterminer les liens minimaux pour les différentes architectures possibles de ce SIS. L'évaluation de la fiabilité de chaque architecture se fera par la formule de Poincaré.

En essayant plusieurs architectures, nous sommes arrivés à une architecture complexe ayant 4 connexions en moins, tout en satisfaisant la contrainte du SIL. La fiabilité de la nouvelle architecture est à égale 0.991. Le réseau de fiabilité de cette architecture est donné dans la figure 58 et son schéma de connexion dans la figure 59.

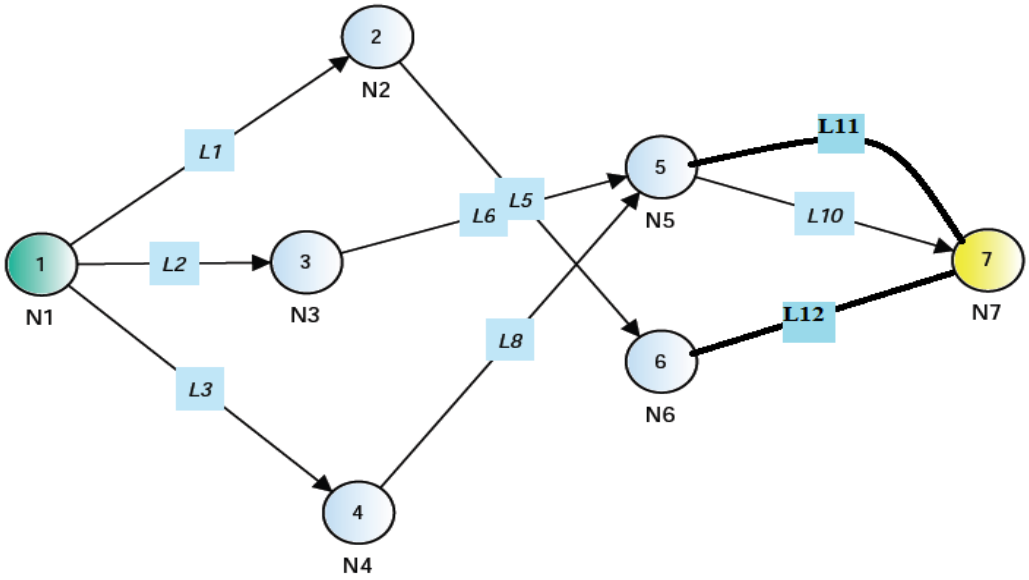


Figure 58 Réseau de fiabilité du système complexe du système d'arrêt d'urgence

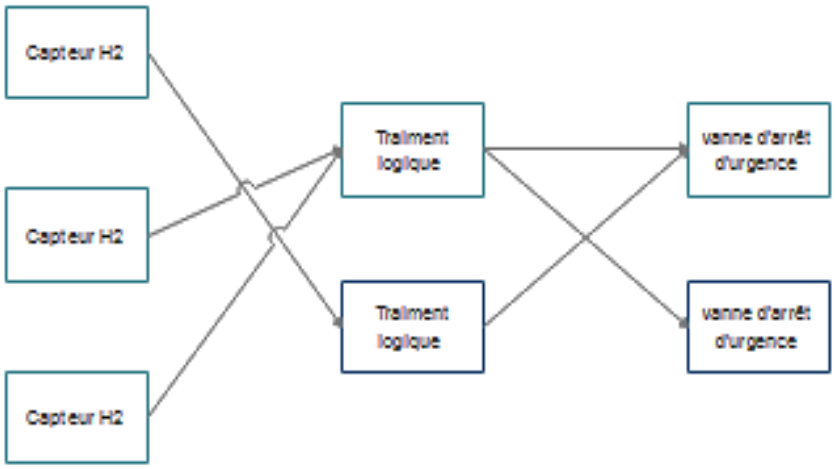


Figure 59 Schéma de connexion du système complexe du système d'arrêt d'urgence

4.3.2. Optimisation de l'architecture du système déluge

La configuration initiale de ce SIS est donnée dans la figure 60. Cette structure a une configuration simple de type parallèle série. Les données sur les composants de ce SIS sont présentées dans le tableau 44.

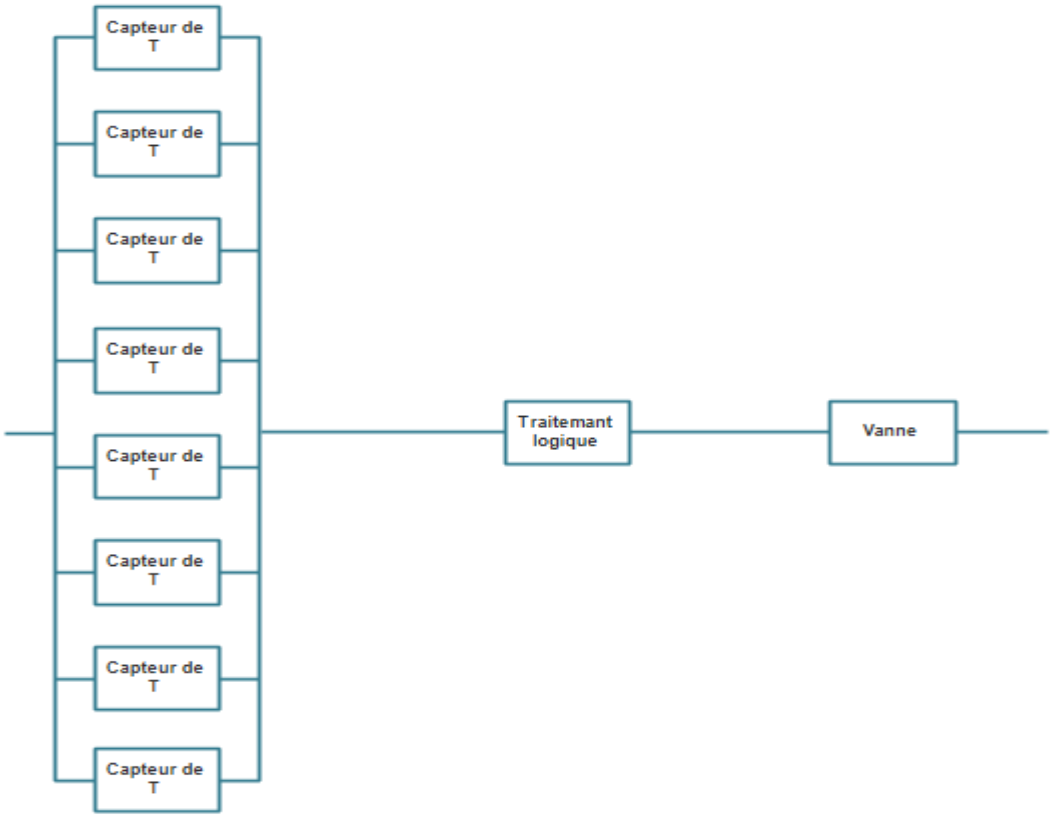


Figure 60 Schéma de connexion initial du système déluge

Tableau 44 Données sur les composants du système déluge

Composant	PFDavg	Fiabilité R	Prix ($)
Capteur de température	0,00687073	0,99312927	300
Carte traitement logique	0,08504415	0.91495585	100
Vanne déluge	0,01146392	0,98853608	1000

Si on pose n(1) le nombre de capteur, n(2) le nombre de carte de traitement et n(3) le nombre de vanne déluge, la fonction à optimiser est :

$$F\big(n(i)\big) = 300 \times n(1) + 500 \times n(2) + 1000 \times n(3) \tag{4.28}$$

sous la contrainte du SIL du SIS qui doit être de niveau 2 :

$$10^{-3} \leq PFD_{avg_{sys}} < 10^{-2} \tag{4.29}$$

La fiabilité du système est donnée par :

$$R_{sys} = 1 - PFD_{avg_{sys}} \quad (4.30)$$

Donc la contrainte sera exprimé par :

$$0.99 < R_{sys} \leq 0.999$$

(4.31)

Sachant que la fiabilité du système est calculée comme suit :

$$R_{sys} = R_{sous-sys_1} \times R_{sous-sys_2} \times R_{sous-sys_3} \quad (4.32)$$

Alors la fiabilité du système en fonction de la fiabilité de ses composants est donnée pas :

$R_{sys} = (1 - (1 - R_{capteur})^{n(1)}) \times (1 - (1 - R_{traitement})^{n(2)}) \times (1 - (1 - R_{Actionneur})^{n(3)}$
(4.33)

En utilisant la fonction *fmincon* de matlab, nous trouverons les résultats suivants :

$$n(1) = 8.5664, n(2) = 2, n(3) = 2.1065$$

En prenant que les parties entières des résultats, la nouvelle architecture est donnée dans la figure 61 et le réseau de fiabilité lui correspondant dans la figure 62. La fiabilité de cette architecture est égale à :

$$R_{sys} = 0.9926$$

C'est-à-dire :

$$PFD_{avg_{sys}} = 7{,}4.10^{-3}$$

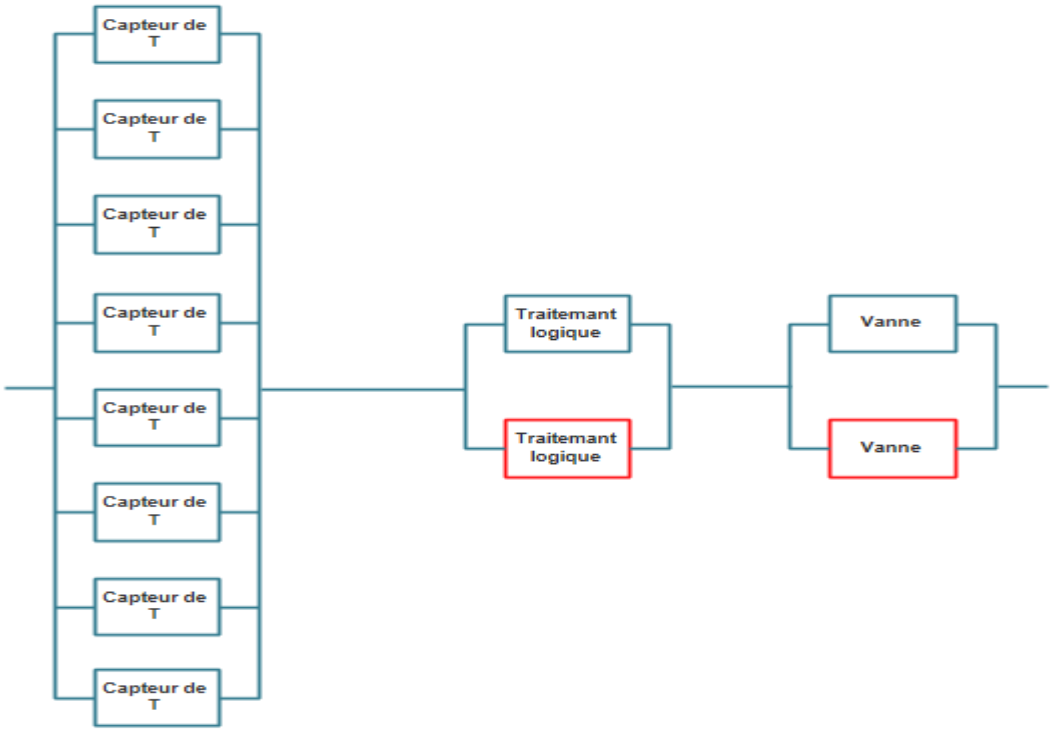


Figure 61 Le nouveau schéma de connexion du système déluge

Cette probabilité correspondant à SIS de SIL 2. Le coût de l'installation est égal à 4600 $.

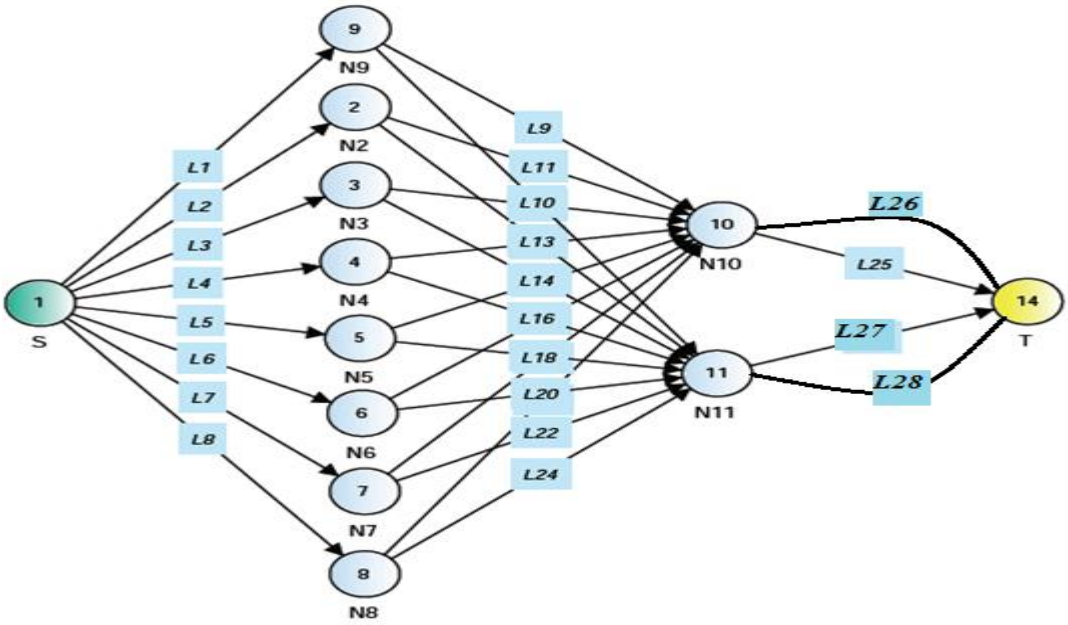


Figure 62 Réseau de fiabilité du nouveau système déluge

Les arcs de L1 à L9 représentent les capteurs. Les arcs de L9 à L24 représentent les traitements logiques. Les arcs de L25 à L28 représentent les vannes déluge. Les nœuds représentent les connexions entre les différents composants du SIS.

En essayant plusieurs combinaisons, nous sommes arrivés à une architecture complexe ayant 5 connexions en moins qu'une architecture parallèle série, tout en satisfaisant la contrainte du SIL. La fiabilité de la nouvelle architecture est égale à : 0.9901**.**

Le réseau de fiabilité de la nouvelle architecture est donné dans la figure 63 et son schéma de connexion dans la figure 64.

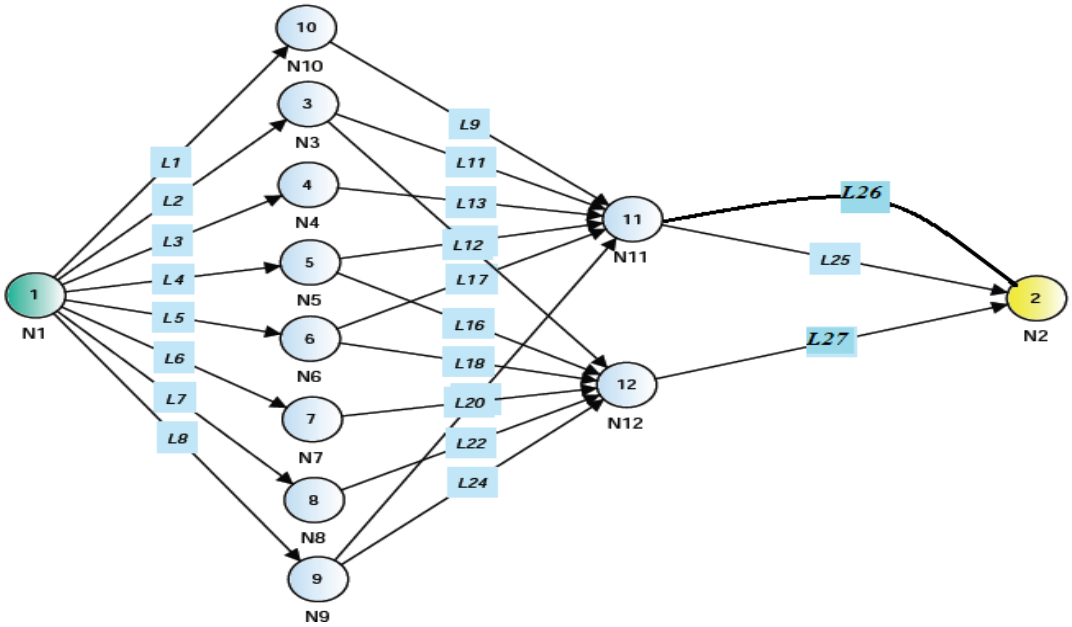


Figure 63 Réseau de fiabilité du système complexe du système déluge

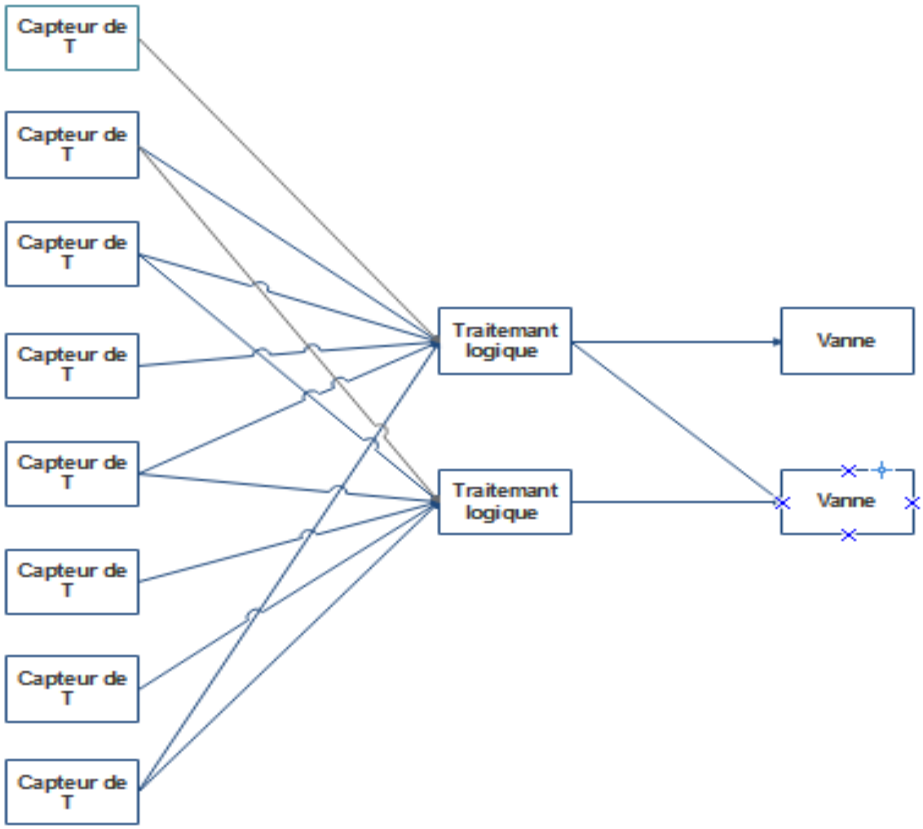


Figure 64 Schéma de connexion du système complexe du système déluge

4.3. Conception optimale de l'architecture d'un SIS dans le poste gaz

Dans le système gaz, on a noté l'existence d'un SIS qui est le système déluge. Il est composé de 4 capteurs UV, d'un traitement logique et d'une vanne déluge. Ce SIS se déclenche quand il détecte dans le champ couvert par les détecteurs une énergie d'activation.

Dans le cas du risque d'accident majeur identifié dans ce système en l'occurrence le risque d'explosion, ce SIS s'avère moins adapté pour mettre en repli le système. Pour qu'il ait explosion on a besoin d'au moins un comburant qui est l'oxygène de l'air, d'un carburant qui est dans ce cas le gaz naturel et d'une énergie d'activation. En l'absence de confinement dans notre cas, l'explosion sera de type *flash fire*.

Lors d'une fuite de gaz et en absence du vent, le gaz naturel va s'accumuler près du sol. Cela est dû au fait que sa densité est supérieure à celle de l'air. Si on a une fuite de gaz qui n'a pas été détecté à temps par les rondiers, le déclenchement du système déluge peut être en retard par rapport à la présence d'une énergie d'activation dans la zone présentant un domaine d'explosivité.

Voulant traiter les deux conditions pouvant mener à une explosion, nous proposerons de relier le système déluge au système de contrôle de la pression dans le circuit de gaz.

Le poste gaz contient 14 capteurs de pressions, placés en aval de chaque équipement le composant. Une vanne de tête pneumatique (figure 65) est placée en amont du poste gaz.

Figure 65 Vanne de tête du poste gaz de la centrale électrique Hamma II

Le SIS proposé pour maîtriser le risque d'explosion dans le poste gaz est composé de :

- Partie capteur : des capteurs de pression en parallèle et des capteurs UV en parallèle, et sont placés dans une structure de type 2oo2. C'est-à-dire qu'il suffit qu'un capteur UV et qu'un capteur de pression donnent le signal pour que le SIS se déclenche. L'architecture 2oo2 a été choisi afin d'éviter le déclenchement intempestif du SIS à cause de la défaillance d'un seul capteur et pour respecter la contrainte de la disponibilité de la centrale.
- Partie traitement logique.
- Partie actionneur : composé des vannes déluges reliées au circuit d'anti-incendie et des vannes de tête placées en amont du poste gaz afin d'arrêter les fuites de gaz.

Suite à l'analyse des barrières de sécurité effectuée dans le chapitre précédent, le SIS requis dans le poste gaz est de SIL 2. Pour satisfaire cette contrainte, nous devons optimiser l'architecture de ce SIS par l'ajout de redondance.

Les données sur les composants du SIS sont présentées dans le tableau N°40.

Tableau 45 Données sur les composants du SIS du poste gaz

Composants	**PFD*avg***	**Fiabilité R**	**Coût**
Capteur UV	0,0057816	0,9942184	300
Capteur de pression	0,04847959	0,95152041	250
Traitement logique	0,08504415	0,91495585	100
Vanne déluge	0,01146392	0,98853608	1000
Vanne de tête	0,047742	0,952258	5000

Les capteurs et les actionneurs placés dans une architecture de type 2oo2 peuvent se ramener à l'étude de système en série. La fiabilité du système donnée par :

$$R_{sys} = R_{sous-système_1} \times R_{sous-système_2} \times R_{sous-système_3} \times R_{sous-système_4} \times R_{sous-système_5} \quad (4.34)$$

Avec :

- Sous-système 1 : capteurs UV placés en parallèle ;
- Sous-système 2 : capteurs de pression placés en parallèle ;
- Sous-système 3 : cartes de traitement logique placées en parallèle ;
- Sous-système 4 : vannes déluges placées en parallèle ;
- Sous-système 5 : vannes de tête.

Si on pose n(1) le nombre de capteurs UV, n(2) le nombre de capteurs de pression, n(3) le nombre de cartes de traitement logique, n(4) le nombre de vannes déluge et n(4) le nombre de vannes de tête, la fonction du coût à optimiser est :

$$C\big(n(i)\big) = 300 \times n(1) + 250 \times n(2) + 100 \times n(3) + 1000 \times n(4) + 5000 \times n(5) \quad (4.35)$$

Sous la contrainte du SIL qui doit être :

$$0.99 < R_{sys} \leq 0.999 \quad (4.36)$$

Avec la fiabilité du système en fonction de la fiabilité de ses composants est donnée par :

$$R_{SYS} = \Big(1 - \big(1 - R_{capteurUV}\big)^{n(1)}\Big)\Big(1 - \big(1 - R_{capteurPression}\big)^{n(2)}\Big)\big(1 - (1 - R_{traitement})^{n(3)}\big)\big(1 - \big(1 - R_{vanneDéluge}\big)^{n(4)}\big)\big(1 - (1 - R_{vanneTête})^{n(5)}\big) \quad (4.37)$$

En utilisant la fonction *fmincon* de matlab, et en spécifiant la borne inférieure comme étant le nombre de composants déjà existant, nous trouverons les résultats suivants (sans les parties fractionnaires) :

$$n(1) = 4, n(2) = 16, n(3) = 2, n(4) = 2, n(5) = 2$$

La fiabilité de cette architecture est égale 0.9904 c'est-à-dire que son PFD_{avg} est égale à $9{,}6.10^{-3}$, ce qui correspond à un SIL 2. Le coût du SIS est égal à 17400 $. En ne comptant pas les composants déjà existants, le coût de l'optimisation de ce SIS est égal à 6100 $.

Le schéma de connexion de l'architecture finale du SIS proposé pour mitiger le risque d'explosion dans le poste gaz est présenté dans la figure 66.

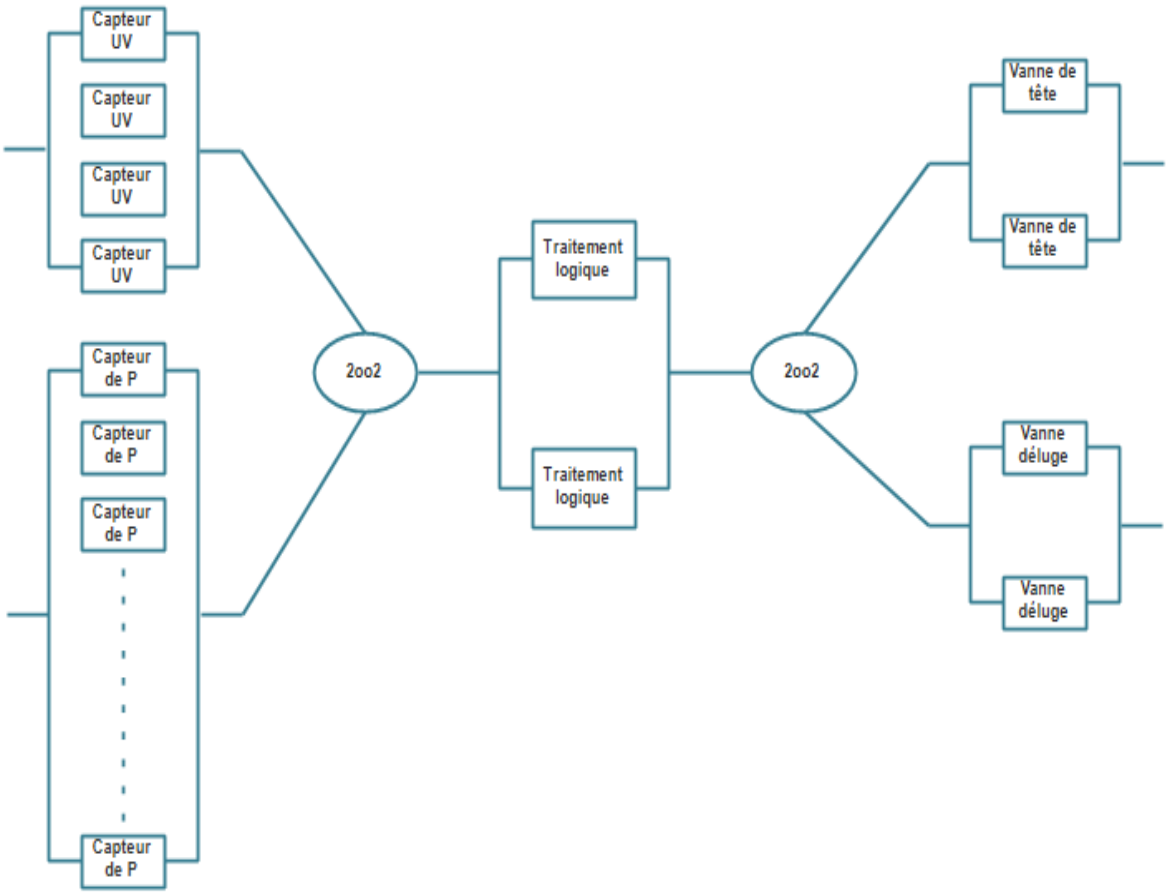


Figure 66 Schéma de connexion de SIS proposé pour le poste gaz

Conclusion

Dans ce chapitre, nous avons pu améliorer les SIS mis en place dans les systèmes critiques de la centrale électrique Hamma II dans le but de maîtriser les risques majeurs. Ce faisant, nous avons fiabiliser ces systèmes en vue d'améliorer la sécurité de l'installation et sa disponibilité. L'utilisation de l'optimisation mathématique et des réseaux de fiabilité nous a permis de proposer des architectures des SIS respectant les exigences de sécurité à moindre coût.

Conclusion générale

Le travail présenté a porté sur la problématique de la fiabilisation de systèmes critiques de la centrale électrique Hamma II, en vue de la maîtrise des risques majeurs qu'ils induisent. Pour ce faire, une nouvelle approche a été développée, utilisant la théorie de la logique floue, de l'analyse fonctionnelle, la théorie des graphes et les méthodes classiques d'analyse des risques et des barrières de sécurité.

Bilan

Nous avons d'abord, utilisé la méthode SADT pour faire une analyse fonctionnelle par la décomposition des systèmes critiques, sujets de notre étude. Cela nous a permis de les appréhender du point de vue des flux de matières et d'informations qui les traversent, ainsi que les fonctions qu'ils doivent assurer. Les représentations graphiques obtenues nous ont aidés à mieux les comprendre et de pouvoir identifier les évènements qui peuvent les rendre inopérants ou dangereux.

La méthode HazOp présentant des insuffisances, nous avons estimé la nécessite d'intégrer la logique floue à cette méthode pour pallier à ces insuffisances.

Suite à l'application de la méthode HazOp-RPN flou, nous avons sélectionné les scénarios d'accidents majeurs pouvant survenir dans les systèmes critiques de la centrale électrique Hamma II. Nous avons dénombré 9 scénarios d'accidents majeurs ayant un niveau de risque modéré jusqu'à majeur.

Dans une troisième étape, nous avons procédé à l'analyse des barrières de sécurité mises en place pour contrôler les scénarios identifiés. Nous avons d'abord, appliqué la méthode du graphe de risque flou pour la détermination de leur niveau d'intégrité (SIL) requis. L'ensemble des scénarios d'accidents majeurs identifiés requiert des SIS ayant un niveau d'intégrité 2.

Puis, nous avons analysé les SIS mis en place par l'entreprise pour sécuriser ces systèmes critiques, afin de leur allouer un SIL, c'est-à-dire le niveau de réduction de risque qui leur est associé. L'application de la méthodologie BORA, nous a permis de corriger les valeurs de probabilité de défaillance des composants du SIS prises des bases de données par rapport aux conditions d'exploitation réelles dans lesquelles évoluent ces SIS. Dans le même but nous avons utilisé l'arbre de défaillance flou afin de modéliser la dispersion des probabilités de défaillances

des SIS données par les bases de données par des fonctions d'appartenance triangulaires. Les valeurs obtenues par les deux méthodes sont très proches. Le SILs trouvés pour les deux SIS existants dans la centrale sont de niveau 1, contrairement au SIL obtenu par la méthode de l'arbre de défaillance conventionnel, qui est de niveau 2. En se référant aux exigences de la norme CEI 61511 sur les caractéristiques que doivent avoir les SIS de différents niveaux, nous avons pu valider les résultats de la méthode BORA et de l'arbre de défaillance flou. Ce qui nous amène à statuer que les barrières de sécurité existantes sont insuffisantes pour réduire les scénarios d'accidents majeurs présents.

La dernière étape de notre travail a consisté en l'amélioration des SIS existants dans le système fuel et le système de refroidissement de l'alternateur et à proposer un nouveau SIS pour le poste gaz. Cela s'est fait par l'allocation de redondances dans les sous-systèmes des SIS afin d'atteindre l'objectif du SIL requis, tout en optimisant le coût de ces modifications. En introduisant les réseaux de fiabilité pour modéliser les structures complexes et la méthode d'inclusion et d'exclusion de Poincaré, nous avons pu réduire le nombre de connexions, tout en satisfaisant le niveau d'intégrité requis des SIS. Un algorithme a été écrit afin de pouvoir déterminer les liens minimaux permettant le fonctionnement des SIS et utiliser la formule de Poincaré.

Perspective

Les probabilités de défaillances données par les bases de données concernent seulement une seule phase de vie des SIS qui est celle de la maturité. Par contre la méthode BORA permet de prendre en compte les facteurs qui puissent influencer les valeurs de la probabilité de défaillance d'un composant tout au long de son exploitation.

Nous estimons donc, qu'une suite à ce travail permettra de déterminer à quel moment, les résultats obtenus par la méthode BORA et la méthode de l'arbre de défaillance, qui sont corrélés durant la phase de maturité, vont diverger.

Références bibliographiques

Aven, T., Sklet, S., & Vinnem, J. E. (2003). Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). *Journal of Hazardous Materials, A137*, 692-708.

Aven, T., Sklet, S., & Vinnem, J. E. (2006). Barrier and operational risk analysis of hydrocarbon releases (BORARelease); part I Method description. *Journal Of Hazardous Materials, A137*, 681-691.

Basile, O., & Dehombreux, P. (2006). Modélisation de la fiabilité d'un système soumis à des sollicitations variables. *Journal de la fiabilité des systèmes*, 12-25.

Boutelis, O. (2015). *"Etude de l'applicabilité de la méthode BORA (Barrier and Operational Risk Analysis) dans le contexte de l'industrie pétrolière algérienne" mémoire de magistère.* Batna: Institut d'Hygiène & Sécurité Industrielle - Université de Batna.

CEI 61511. (2003). *Sécurité fonctionnelle-Système instrumenté de sécurité pour le domaine de la production par processus.*

CEI 61882. (2001). *Études de danger et d'exploitabilité (études HAZOP) - Guide d'application -.*

CEI61508. (2011). *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.*

Chergui, L. (2010). *Diagnostic des défaillances et optimisation des architectures des systèmes instrumentés de sécurité : apport de la logique flou, mémoire de magistère.* Batna: Institut d'Hygiène et Sécurité Industrielle de Batna.

Christiane, C.-T. (1997). *Processus stochastiques et fiabilité des systèmes.* Berlin: Springer-Verlag Berlin Heidelberg.

Cogie, O., & Robert , C. (2003). *Théorie des graphes : Au delà des ponts de Königsberg, Problèmes, théorêmes, algorithme* . Paris: Vuibert.

Daoud, H. (2015). *Evaluation du risque d'explosion au niveau de la centrale électrique El-Hamma II.* Alger: Ecole Nationale Polytechnique.

Dubois, H., & Prade, H. (1988). *Possibiliy theory : An approach to computerized processing of uncertainty.* Plenum Press: Berlin.

EXIDA. (2005). *Safety Equipment Reliability Handbook, 2nd Edition.*

Guimaraes, A. C., & Lapa, C. F. (2006). Hazard and operability study using appromimate reasoning in light-water reactors passive systems. *Original Research Article*, 1256-1263.

Gulland, W. G. (2004). Methods of determing safety intergrity level (SIL) requirements. *12th Annual Safety-Critical Systems Symp* (pp. 105-122). Frankfurt: Pros and Con.

ISO 12100. (2010). *Sécurité des machines - Principes généraux de conception - Appréciation du risque et réduction du risque.*

Kaufmann, A., Grouchko, D., & Cruon, R. (1975). *Modèles mathématiques pour l'étude de la fiabilité des systèmes.* . Paris: Masson et Cie.

Kirkwood, D., & Tibbs, B. (2005). Developments in SIL determination. *Comput. & Cont. Eng. J, Vol. 16*, 21-27.

Klir, G. J., & Yuan, B. (1995). *Fuzzy Sets and Fuzzy Logic.* New Jersey: Prentice Hall.

Lanternier, B., & Adjadj, A. (2008). Allocation de niveau d'intégrité de sécurité (SIL) requis conformément à la norme CEI 61511. *Revue internationale sur l'ingénierie des Risques Industriels, Vol. 1*, 34-45.

Liang, G. S., & Wang, M.-J. J. (1993). Fuzzy fault-tree analysis using failure possibility. *Microelectronics and reliability, 33*, 583-597.

Mamdani, H. E., & Assilian, S. (1975). An experiment in lingusitic synthesis with a fuzzy logic controller. *International Journal of Man-Machines Studies, vol. 7*, 1-13.

Massaro, D. W. (1992). *Broadening the domain of the fuzzy logical model of perception.* Washington: Knill (Eds).

Meunier, B. B. (1995). *La logique floue et ses applications - Vie artificielle.* Paris: Ed. Addisson - Wesley France.

Michel, L. (1990). *Maîtriser SADT.* Paris: Colin .

Mkhida, A. (2009). *"Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence", thèse de doctorat* . Lorraine : Ecole Doctorale IAEM Lorraine.

Nait-Said, R., Zidani, F., & Ouazraoui, N. (2009). Modified risk graph method using fuzzy rule-based approach. *Haz. Mat.*, 651-658.

NF 50-150. (1990). *Analyse de la valeur - Analyse fonctionnelle. Vocabulaire* . NF.

Noyes, D. e. (2007). *Analyse des systèmes - Sûreté de fonctionnement.* Paris: Techniques de l'Ingénieur.

OREDA. (2002). *Offshore Reliability Data Handbook, 4th Edition.*

Redmil, F. (1998). IEC 61508 : Principles and use in the management of safety. *Comput. & Cont. Eng. J, Vol. 8*, 205-213.

Rhazali, K. (2015). *Optimisation de la disponibilité des systèmes multi-Etats, mémoire d'ingénieur.* Compiègne: UTC.

Sellak, M. (2007). *"Evaluation de parametres de sureté de fonctionnement en présence d'incertitude et aide à la conception : application aux systèmes instrumentés de sécurité" Thèse de doctorat.* Lorraine: Ecole Doctorale IAEM Lorraine.

Simon, C., Sallak, M., & Aubry, F. (2007). SIL allocation of SIS by aggregation of experts opinions. *Safety and reliability Conference*, 25-27.

Sindjui, C. (2014). *Le grand guide des systèmes de contrôle commande industriels - automatisme - instrumentation réseaux locaux - régulation automatique* . Paris: Lexitis Edition.

Sklet, S. (2005). Safety barriers : Definitions, classification and performance. *Journal of Loss Prevention in the process industries*, 494-506.

Thierry, H. (2008). *"Analyse statique et preuve de programmes industriels critiques" Thèse de doctorat.* Paris : Université Paris XI.

Wang, Y., West, H. H., & Mannan, M. S. (2004). The impact of data uncertainty in determing Safety Intregrity Level. *Process Safety and Environmental Protection, 82*, 393-397.

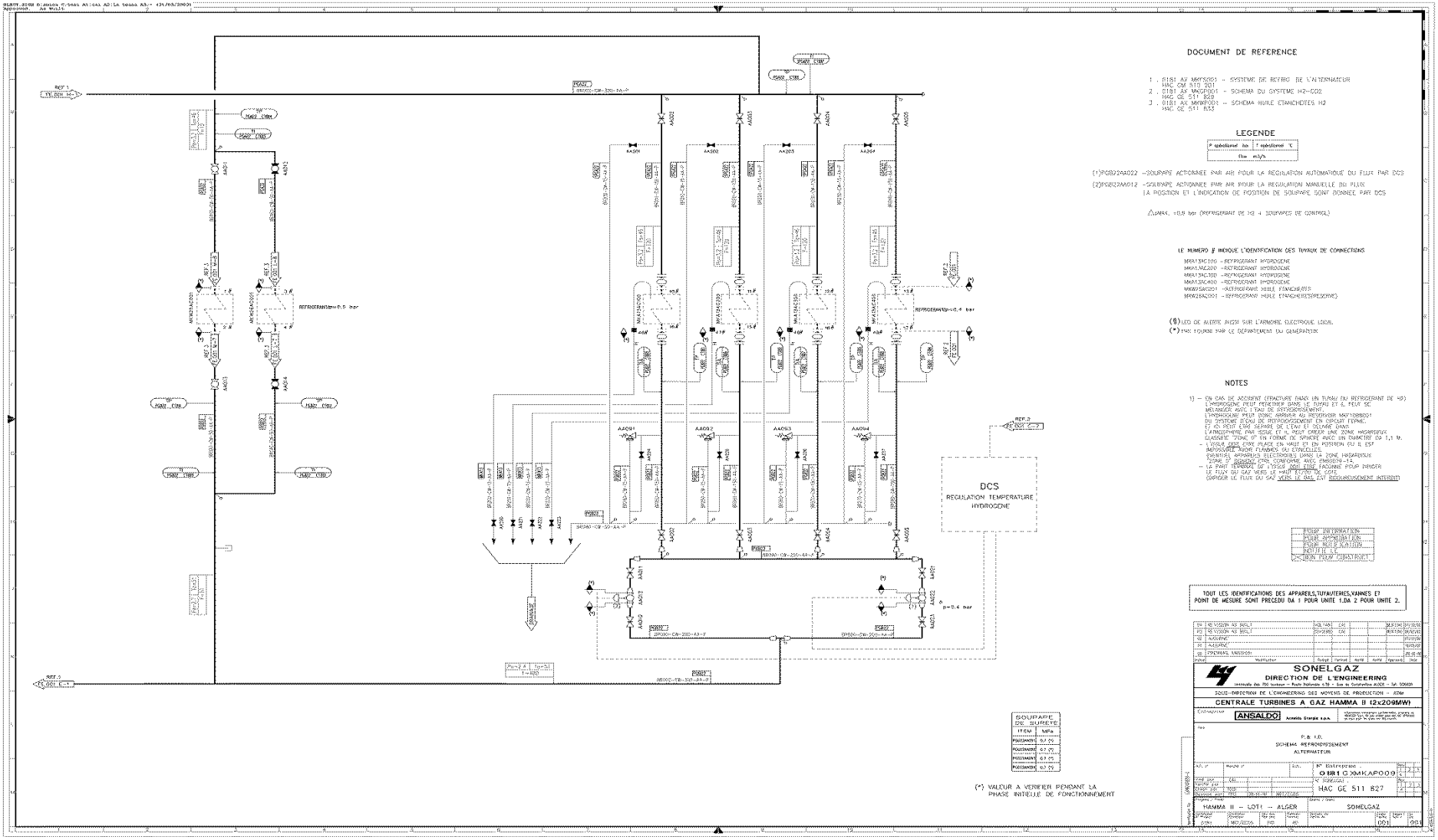
Zadeh, L. (1965). Fuzzy sets. *Information and Control, vol. 8*, 338-353.

Zadeh, L. (1975). The concept of a linguistique variable, applicaion to approximate reasoning . *Information Sciences, vol. 8*, 301-357.

Zadeh, L. (1978). Fuzzy sets as a basis for a theory of possibility. *Fuzzy sets and Systems, vol. 1*, 3-28.

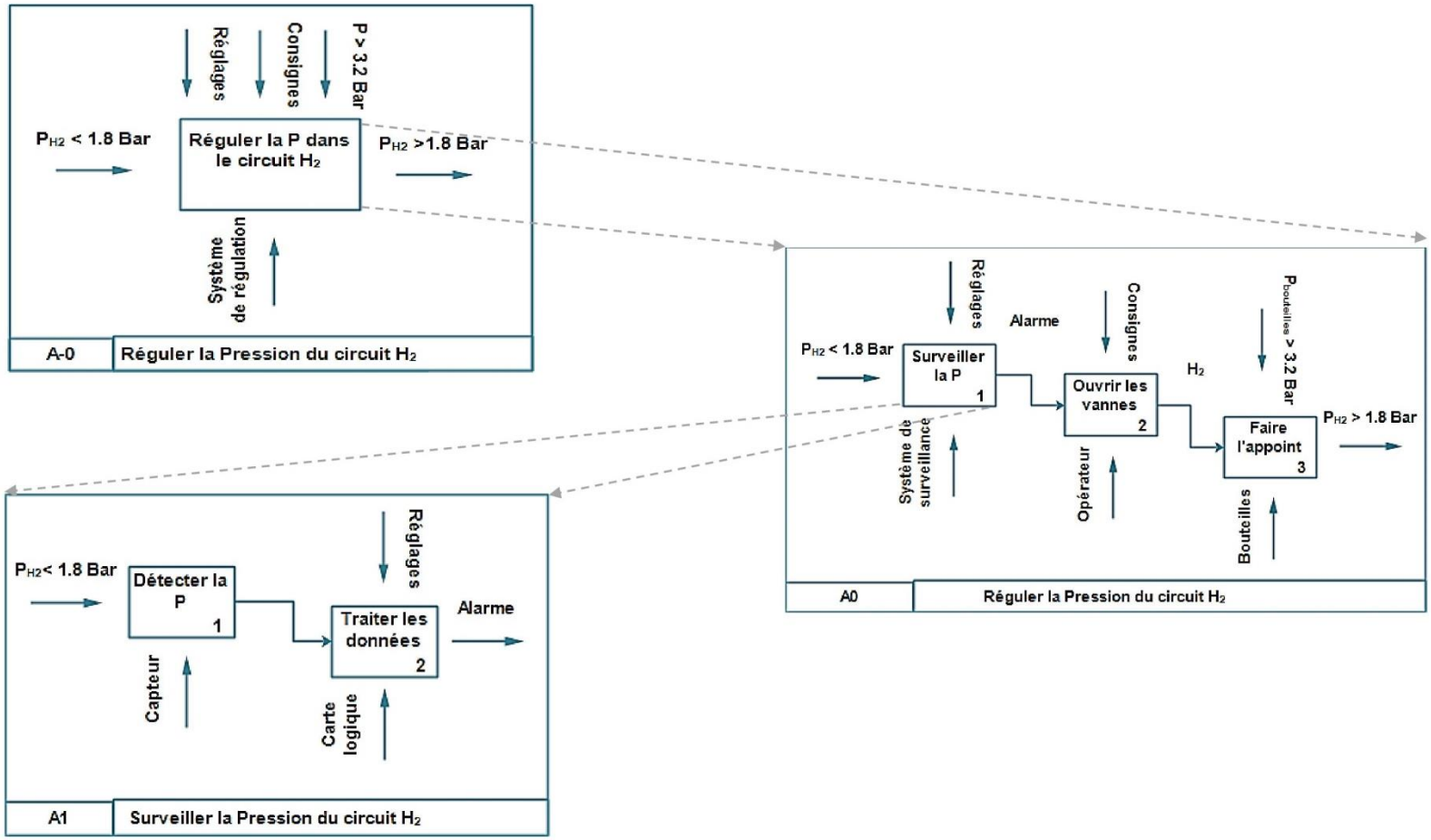
Annexes

Annexe 1 : Schéma P&ID du système de refroidissement à hydrogène de l'alternateur

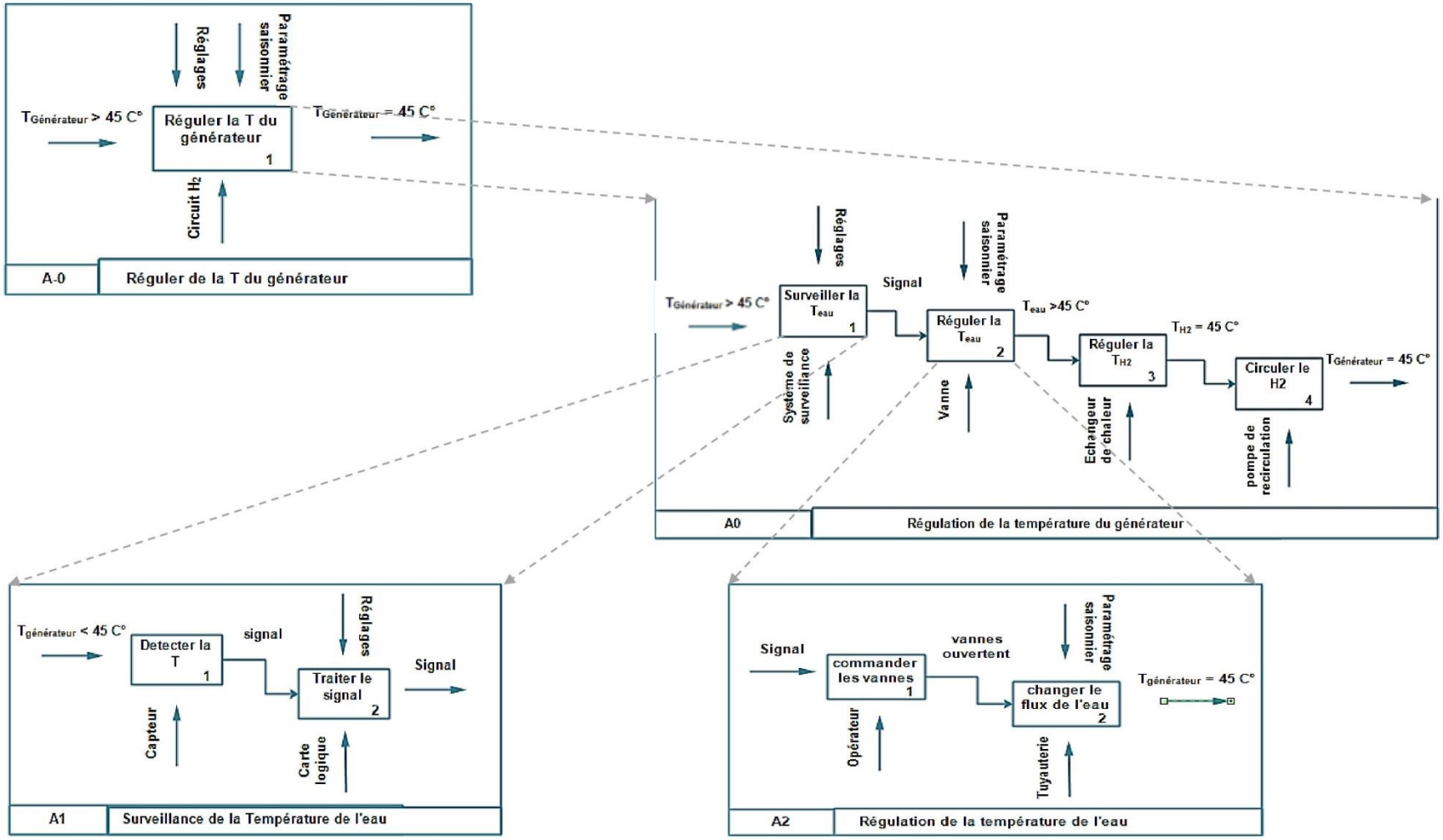


Annexe 2 : Actigrammes et datagrammes obtenus par la méthode SADT

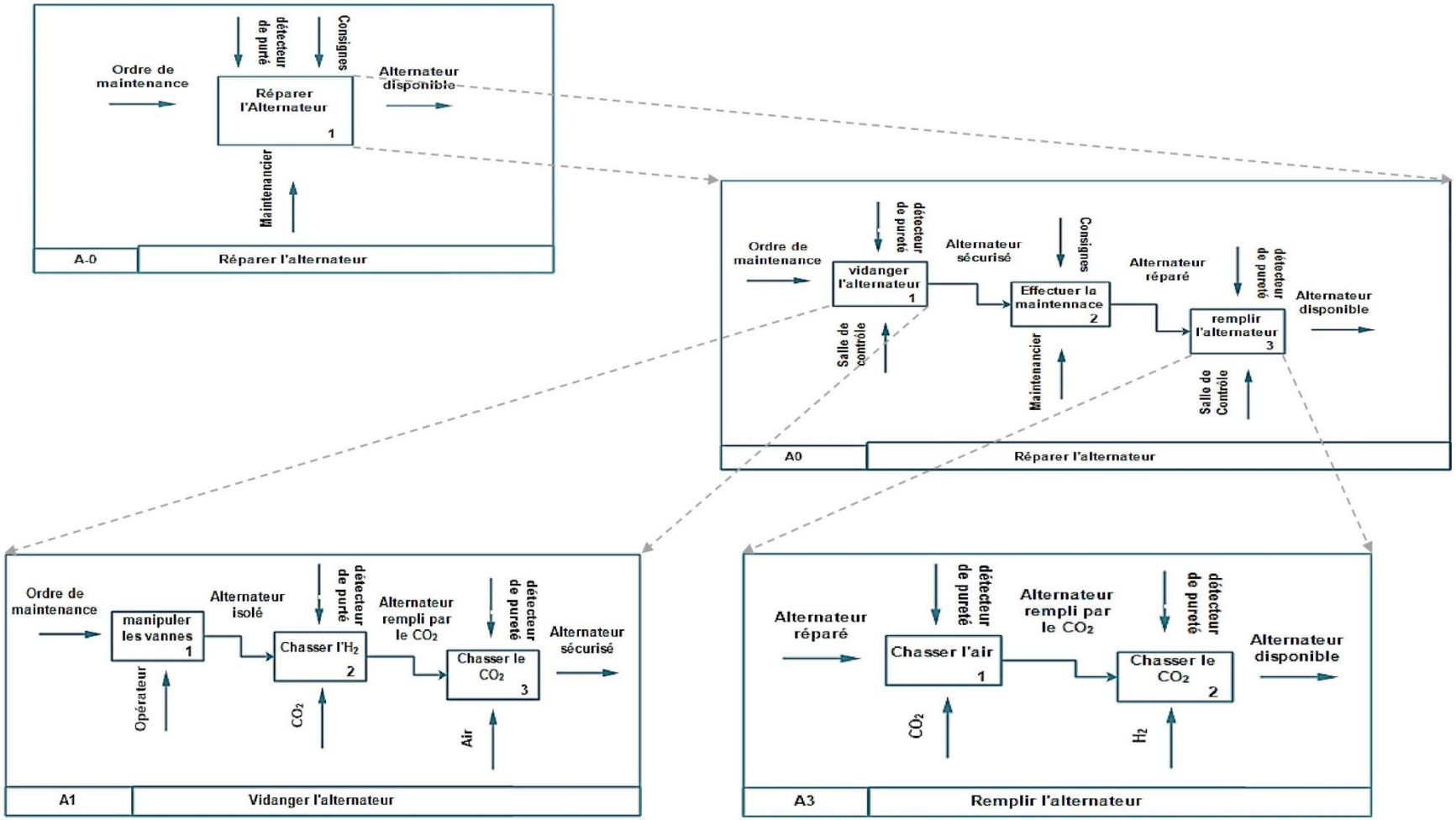
Système : Système de refroidissement de l'alternateur	**Schéma :** Actigramme
Fonction : Réguler la pression du circuit H_2	



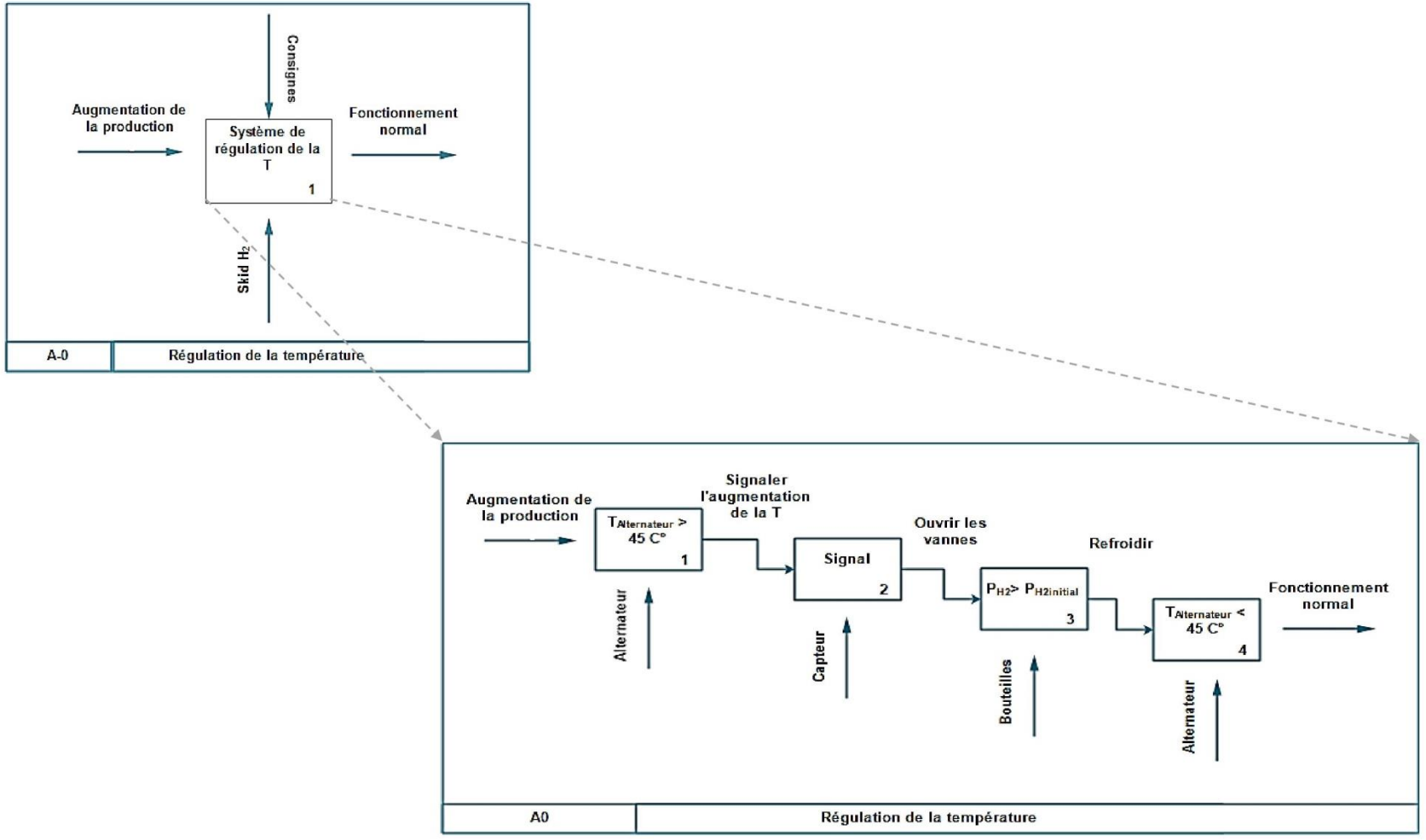
Système : Système de refroidissement de l'alternateur	**Schéma :** Actigramme
Fonction : Réguler la température de l'alternateur	



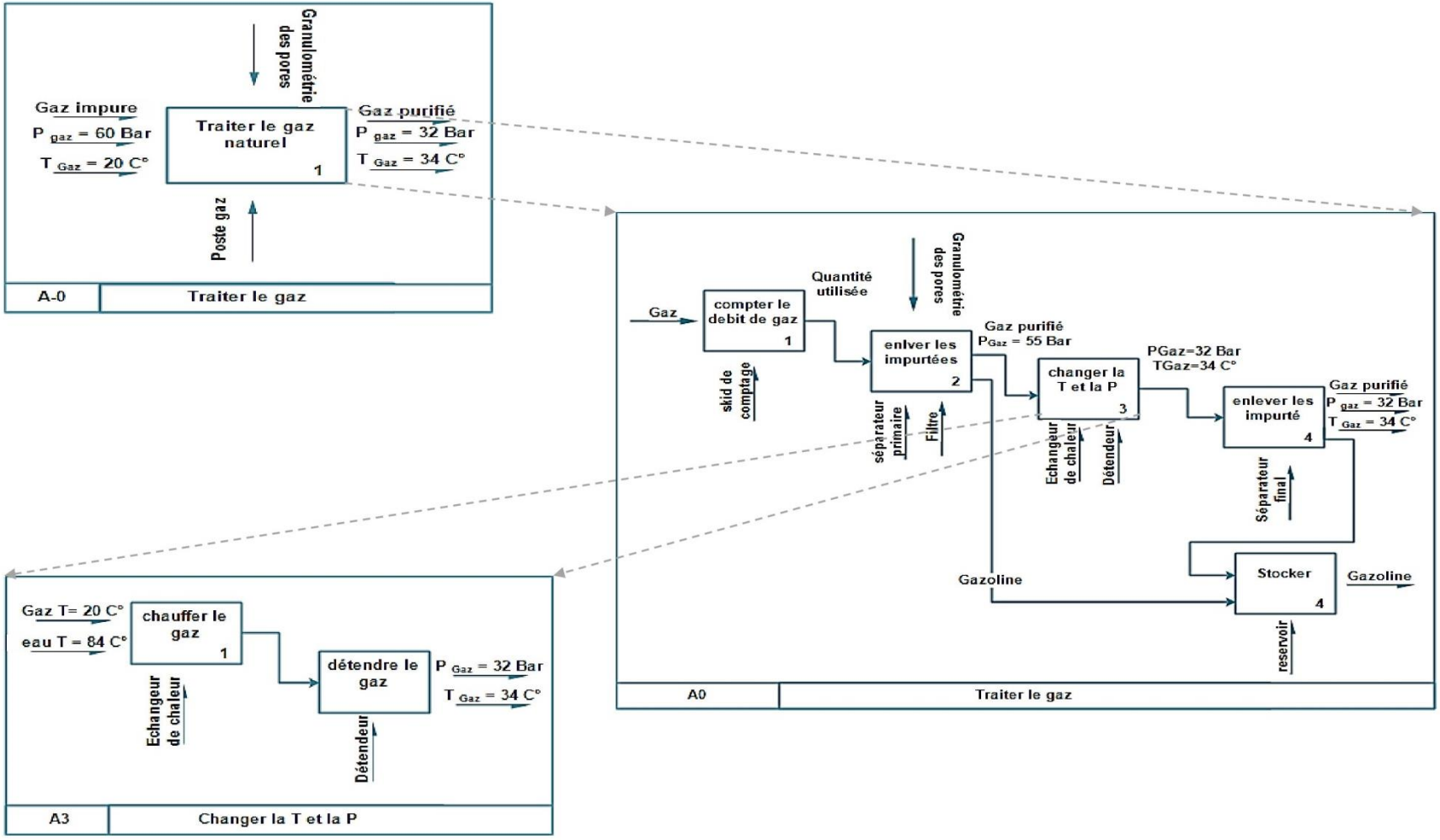
Système : Système de refroidissement de l'alternateur	**Schéma :** Actigramme
Fonction : Réparer l'alternateur	



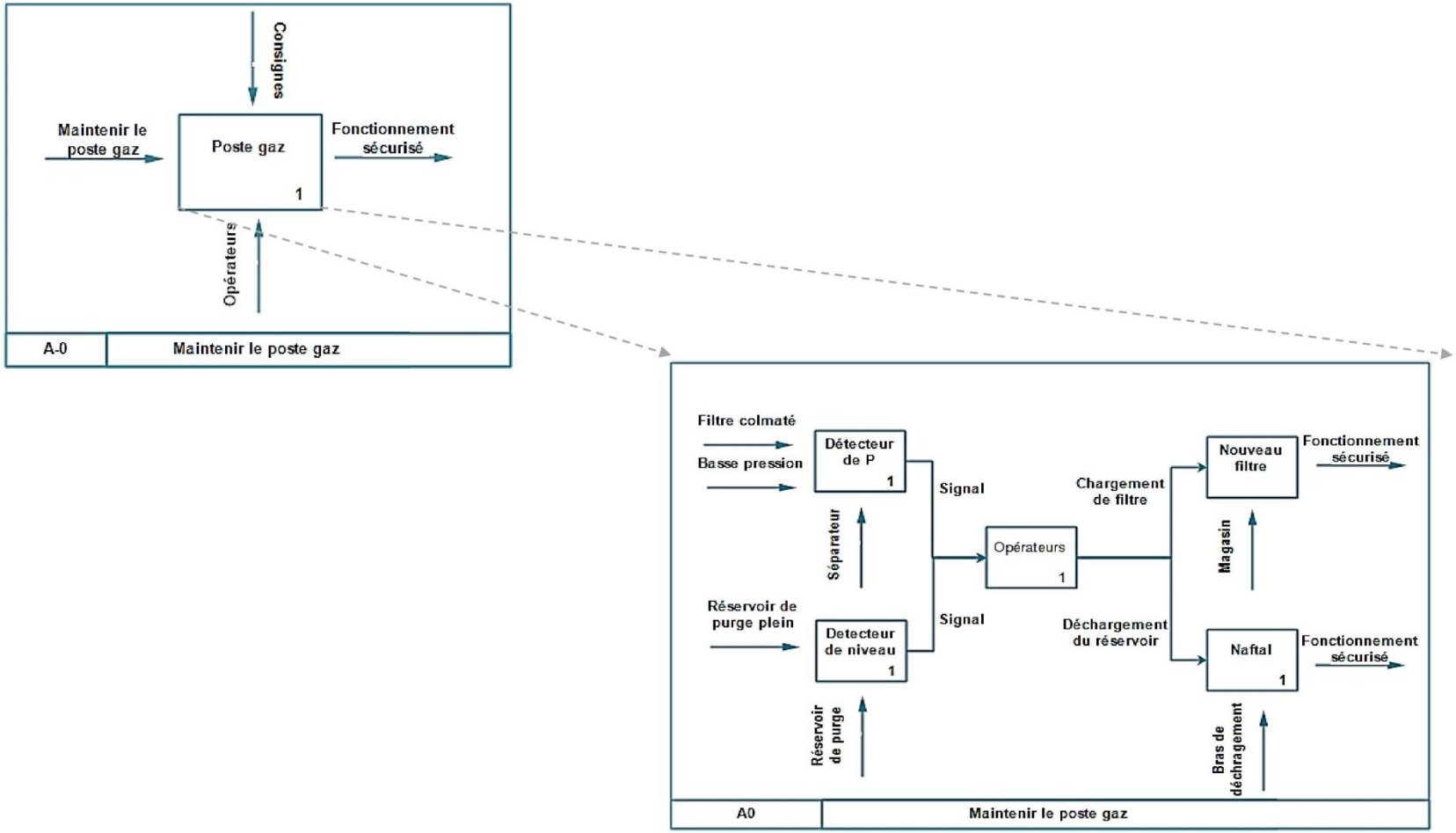
Système : Système de refroidissement de l'alternateur	**Schéma :** Datagramme
Fonction : Refroidir l'alternateur	



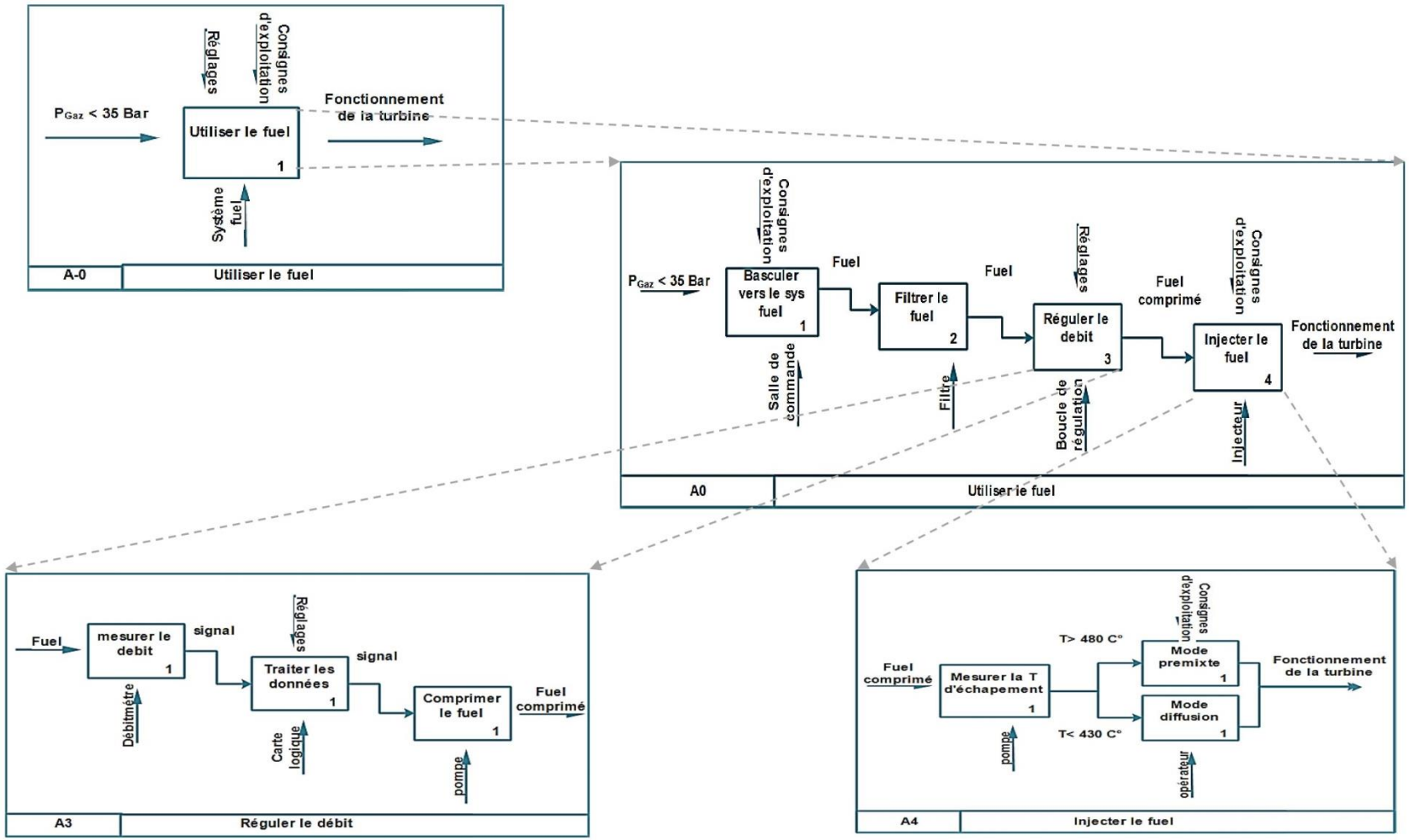
Système : Poste gaz	**Schéma :** Actigramme
Fonction : Traiter le gaz naturel	



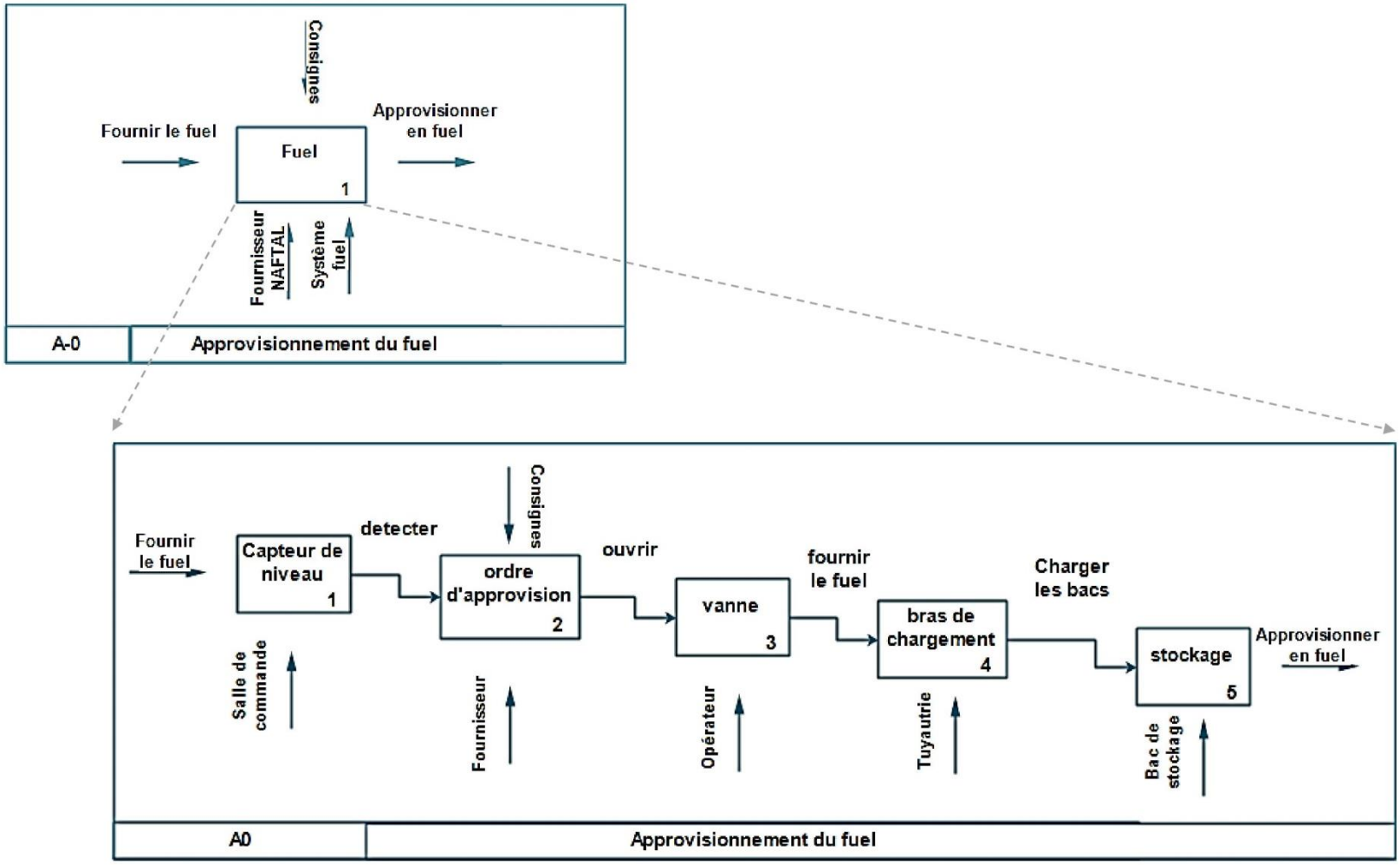
Système : Poste gaz	**Schéma :** Datagramme
Fonction : Maintenir le poste	



Système : Système fuel	**Schéma :** Actigramme
Fonction : Utiliser le fuel comme combustible de secours	



Système : Système fuel	**Schéma :** Datagramme
Fonction : Approvisionnement en fuel	



Annexe 3 : Calcul de la mémoire du système d'inférence floue sous matlab de la HazOp-RPN

```
[System]
Name='finale'
Type='mamdani'
Version=2.0
NumInputs=3
NumOutputs=1
NumRules=16
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='EOP'
Range=[0 4]
NumMFs=5
MF1='Impossible':'trimf',[0 0 0.1]
MF2='Trés_lointain':'trimf',[0 1 2]
MF3='Lointain':'trimf',[1 2 3]
MF4='faible':'trimf',[2 3 4]
MF5='Modéré':'trimf',[3.81 3.96 4.2]

[Input2]
Name='Gravité'
Range=[0 10.1]
NumMFs=5
MF1='mineure':'trimf',[0 1.515 3.03]
MF2='faible':'trimf',[2.02 3.535 5.05]
MF3='Modérée':'trimf',[4 6 8]
MF4='Elevée':'trimf',[6.931 8.5 9.902]
MF5='Très_élevée':'trimf',[9.09 9.99 10.1]

[Input3]
Name='Non-détection'
Range=[0 10.1]
NumMFs=5
MF1='mineure':'trimf',[0 1.515 3.03]
MF2='faible':'trimf',[2.051 3.566 5.081]
MF3='modérée':'trimf',[4 6 8]
MF4='Elevée':'trimf',[6.931 8.615 9.902]
MF5='Trés_élevée':'trimf',[9.059 10.1 10.1]

[Output1]
Name='RPN'
Range=[0 10]
NumMFs=9
MF1='Non-existant':'trimf',[0 0 0.1]
```

MF2='Négligeable':'trimf',[0 0.15 0.25]
MF3='Moins_faible':'trimf',[0.15 0.25 0.5]
MF4='Faible':'trimf',[0.25 0.5 0.75]
MF5='modéré':'trimf',[0.5 0.75 0.9]
MF6='Moins_fort':'trimf',[0.75 0.9 1]
MF7='Fort':'trimf',[0.75 1 1.5]
MF8='Très fort':'trimf',[1 1.5 2]
MF9='Majeur':'trimf',[1.5 5 10]

[Rules]
1 0 0, 1 (1) : 1
3 3 2, 6 (1) : 1
2 5 1, 4 (1) : 1
4 3 1, 5 (1) : 1
3 3 2, 5 (1) : 1
2 5 1, 2 (1) : 1
3 3 3, 8 (1) : 1
3 5 1, 7 (1) : 1
2 1 3, 3 (1) : 1
2 5 2, 5 (1) : 1
4 3 3, 9 (1) : 1
5 3 3, 9 (1) : 1
5 4 3, 9 (1) : 1
5 5 3, 9 (1) : 1
5 5 4, 9 (1) : 1
5 5 5, 9 (1) : 1

Annexe 4 : Résultats de la méthode HazOp-RPN

Tableau N°1 : HazOp-RPN du système fuel, nœud : réservoir fuel											
1.1	Niveau	Bas	Corrosion du bac	Fuite du fuel	Incendie	Bac de rétention Système déluge Capteur de niveau	3	3	2	0.7791	5
1.2			Fermeture intempestive des vannes d'alimentation de la chaudière	Pas d'alimentation de la chaudière	Arrêt de l'installation	Capteur de niveau 2éme bac	3	3	2	0.7791	5
1.3		Haut	Ouverture intempestive des vannes d'alimentation des bacs	Débordement des bacs de stockage du fuel	Incendie	Bac de rétention Système déluge Capteur de niveau	3	3	2	0.7791	5

Tableau N°2 : HazOp-RPN du Système fuel, nœud : circuit fuel											
N°	Paramètre	Mot-clé	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie floue	Hazop-rpn
1.4	Débit	Pas de	Fermeture intempestive des vannes	Pas d'alimentation de la chaudière	Arrêt de l'installation	Débitmètre Ouverture by-pass	3	3	2	0.7791	5
1.5			Rupture ligne entre nœud	Epandage du fuel	Incendie	Système déluge Capteur UV	2	5	2	0.7143	5
1.6		Peu de	Défaut d'étanchéité	Fuite du fuel	Incendie	Réseau anti incendie Capteur UV	3	3	2	0.7791	5
1.7			Filtres colmatés	Baisse de rendement	Arrêt de l'installation	By passe Maintenance Débitmètre Accumulateur	3	3	2	0.7791	5

Tableau N°3 : HazOp-RPN du système fuel, nœud : pompes											
N°	Paramètre	Mot-clé	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie floue	Hazop-rpn
1.10	Débit	Pas de	Défaillance de la pompe	Pas d'alimentation de la chaudière	Arrêt de l'installation	Pompes de secours Maintenance	3	3	2	0.7791	5
1.11		Peu de	Défaillance du système de régulation de débit du fuel	Mauvaise alimentation de la chaudière	Baisse de rendement		3	3	2	0.7791	5

Tableau N°4 : HazOp-RPN du système de refroidissement, nœud : circuit d'hydrogène											
N°	Paramètre	Mot-clé	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie flou	HazOp rpn
2.1	Pression	Pas de	Défaillance des pompes permettant la circulation de l'hydrogène dans le circuit	Accumulation de l'hydrogène dans les coins du corps de l'alternateur et Mauvais refroidissement du bobinage.	Usure et détérioration des anneaux d'étanchéité	Capteur de pression Capteur de température de l'alternateur	3	3	2	0.791	5
2.2		Faible <120m^3/h	Défaut d'étanchéité	Fuite d'H2 et création d'un mélange facilement explosif	explosion	Système de surveillance des fuites d'hydrogène Capteur de pression Alarme Vanne manuelle d'arrêt d'urgence	3	5	1	1.0789	7
2.3			Mauvaise ventilation Régulation du débit d'hydrogène défectueuse	Mauvais refroidissement de l'alternateur	Usure et détérioration des anneaux d'étanchéité	Capteur de débit Alarme Système automatique d'appoint d'hydrogène	3	3	2	0.791	5
2.4		Basse pression de l'huile d'isolation <<5 Bar	Défaillance de la boucle de régulation de la pression d'huile	Fuite de gaz d'H2 Création d'un mélange détonant	Explosion	Système de surveillance des fuites d'hydrogène Alarme	3	5	2	5	9
2.5			Défaut de fonctionnement des aéro-réfrigérant	Mauvais refroidissement des	Usure et détérioration des	Capteur de température Alarme	3	3	2	0.791	5

2.6	Tem pérat ure	Haute température >>46 C°	Défaillance de la boucle de régulation du débit d'eau de refroidissement	composants du générateur	composants du générateur	Capteur de débit Capteur de température Alarme	3	3	2	0.7 791	5

Tableau N°5 : HazOp-RPN du système de refroidissement, nœud : stockage d'hydrogène											
N°	Paramètre	Déviations	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie floue	Hazop rpn
2.7	Pression	Basse pression	Fuite d'hydrogène au niveau des bouchons, usure, corrosion de la bouteille	Formation d'un mélange air/H2 explosif	Explosion	Détecteur de gaz d'H2 Alarme Tournée opérateur	2	5	1	0.3894	4
2.8		Haute pression	Canicule	Surpression dans les bouteilles (fuite ou éclatement de la bonbonne)	Explosion	Surveillance à partir de la salle de commande	2	5	1	0.3894	4

Tableau N°6 : HazOp-RPN du système de refroidissement, nœud : Générateur H2/CO2											
N°	Paramètre	Déviations	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie floue	Hazop rpn
2.9	Composition des gaz dans l'alternateur	Présence d'air et d'hydrogène en même temps	Évacuation incomplète de l'hydrogène avant les opérations de maintenances	Formation d'un mélange air/H2 explosif	Explosion	Détecteur de gaz d'H2. Capteur de proportion d'inertage Alarmes Matériels antidéflagrants	3	5	1	1.0789	7

Tableau N°7 : HazOp-RPN du poste gaz, nœud : circuit de gaz											
N°	Paramètre	Déviations	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie floue	Hazop rpn
3.1	Température	haute	canicule	Augmentation de pression dans le circuit gaz ce qui favorise les fuites	Explosion	Contrôle de la T et P Décharge vers soupape Calorifuge (séparateur final)	2	5	1	0.3894	4
3.2				Détérioration des filtres (séparateur final/ filtre)	Bouchage des bruleurs	Maintenance	2	1	3	0.2941	3
3.3		Basse	Hiver	Givrage des vannes et pertes d'étanchéité des joints et fuite du gaz	Explosion	Contrôle de la T Calorifuge	4	3	1	0.7143	5
3.4	Pression	Basse	Défaut d'étanchéité	Fuite du gaz naturel	explosion	Manomètre	3	5	1	1.0789	7
3.5		pas de	Pas d'alimentation en gaz en amont Rupture de ligne	Arrêt de l'installation		Système fuel	3	3	2	0.7791	5
3.6		Plus de	Augmentation	Rupture ligne	Explosion	Manomètre	2	5	1	0.3894	4

			de la température en été et augmentation de la pression dans le circuit	et épandage du gaz		Capteur de T					
3.7			Vannes fermée et alimentation forcée	Fuite du gaz dans les points fragiles du circuit (défaillance, corrosion)	Explosion	Décharge vers soupapes	2	5	2	0.7143	5
3.8	Débit	Pas de	Pas d'alimentation en gaz par gazoduc	Pas d'alimentation en gaz des chaudières	Arrêt installation	Système fuel	3	3	2	0.7791	5
3.9			Fermeture intempestive des vannes	rupture de la ligne	Explosion	Redondance des vannes	2	5	1	0.3894	4
3.10		Peu de	Défaut d'étanchéité et baisse du débit gaz	Fuite du gaz naturel	Explosion	Système déluge	3	5	1	1.0789	7
3.11			Vanne partiellement ouverte	Mauvaise alimentation de la chambre de combustion	Arrêt de l'installation	Possibilité de manœuvre de la vanne manuellement	3	3	2	0.7791	5

Tableau N°8 : HazOp-RPN du filtre du Système poste gaz											
N°	Paramètre	Déviations	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie floue	Hazop rpn
3.12	Débit	Peu de	Colmatage des filtres (Seuil de filtration 5µm)	Mauvaise alimentation de la turbine et	Baisse de production	Basculement vers la deuxième ligne Maintenance	3	3	2	0.7791	5

Tableau N°9: HazOp-RPN du poste gaz, nœud : Echangeur de chaleur											
N°	Paramètre	Déviations	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie floue	Hazop rpn
3.13	Température	Peu	Défaillance des brûleurs de la chambre de combustion de réchauffeur d'eau	Gaz à énergie calorifique basse	Baisse du rendement	Circuit By-pass des réchauffeurs	3	3	2	0.7791	5
3.14			Mauvaise alimentation de la chaudière du système de chauffage du gaz			Capteur de pression dans le circuit d'alimentation des chaudières	3	3	2	0.7791	5
3.15			Défaut d'étanchéité dans le circuit d'alimentation des chaudières	Epandage du gaz	Explosion	capteur de pression	2	5	2	0.7143	5
3.16			rupture de la ligne d'alimentation des chaudières				2	5	2	0.7143	5

3.17	Débit (eau)	Pas	Défaillance pompes de circulation d'eau	Givrage des vannes du circuit gaz	Arrêt de l'installation	3 pompes de secours	3	3	2	0.7791	5
3.18			Rupture de lignes eau			Vérification périodique	3	3	2	0.7791	5
3.19			Fermeture intempestive des vannes de la ligne d'eau de réchauffage				3	3	2	0.7791	5
3.20		Peu de	Défaillance de la pompe de la pompe de circulation d'eau				3	3	2	0.7791	5
3.21			Vannes de la ligne d'eau de réchauffage partiellement ouvertes				3	3	2	0.7791	5
3.22			Défaut d'étanchéité	Epandage du gaz	Explosion		2	5	2	0.7143	5

Tableau N°10 : HazOp-RPN du poste gaz, nœud : Détendeur

N°	Paramètre	Déviations	Causes	Conséquences	Risque potentiel	Barrières	EOP	Gravité	Non-détection	Sortie floue	Hazop rpn
3.23	Débit	pas de	Fermeture intempestive de la vanne dans la ligne gaz	arrêt de l'installation		3 rampes de secours.	3	3	2	0.7791	5
3.24		Faible	Ouverture incomplète de la vanne (défaillance)	Baisse de pression de service.	Arrêt de l'installation.	Contrôle des vannes, maintenances. 3 rampes de secours.	3	3	2	0.7791	5

Annexe 5 : Calcul de la mémoire du système d'inférence floue sous matlab du graphe de risque flou

```
[System]
Name='Untitled2'
Type='mamdani'
Version=2.0
NumInputs=4
NumOutputs=1
NumRules=21
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='consÃ©quence'
Range=[-9 1]
NumMFs=4
MF1='Mineur':'trapmf',[-9 -8.5 -7.5 -6.77]
MF2='Marginal':'trapmf',[-2.65 -1.75 -1.25 -0.84]
MF3='Critique':'trapmf',[-1.66 -0.75 -0.25 0.15]
MF4='Catastrophique':'trapmf',[-0.65 0.25 0.75 1]

[Input2]
Name='Exposition'
Range=[0 100]
NumMFs=2
MF1='Rare':'trapmf',[0 2.5 7.5 12.5]
MF2='FrÃ©quente':'trapmf',[7.5 32.5 100 100]

[Input3]
Name='Evitement'
Range=[0 100]
NumMFs=2
MF1='Impossible':'trapmf',[0 22.5 67.5 92.5]
MF2='Possible':'trapmf',[87.5 92.5 100 100]

[Input4]
Name='apparition'
Range=[-5 0]
NumMFs=3
MF1='TrÃ©s-faible':'trapmf',[-5 -4.13 -2.39 -1.25]
MF2='Faible':'trapmf',[-2.7 -1.27 -0.77 -0.36]
MF3='ElevÃ©':'trapmf',[-0.71 -0.39 0 0]

[Output1]
Name='niveauSIL'
Range=[0 6]
NumMFs=6
```

MF1='a':'trapmf',[0 0.25 0.75 1.16]
MF2='SIL_3':'trapmf',[2.35 3.25 3.75 4.16]
MF3='b':'trapmf',[4.35 5.25 6 6]
MF4='SIL_1':'trapmf',[0.35 1.25 1.75 2.16]
MF5='SIL_2':'trapmf',[1.35 2.25 2.75 3.16]
MF6='SIL_4':'trapmf',[3.35 4.25 4.75 5.16]

[Rules]
1 0 0 3, -1 (1) : 1
2 1 2 3, 4 (1) : 1
2 1 2 2, 1 (1) : 1
2 1 1 3, 5 (1) : 1
2 1 1 2, 4 (1) : 1
2 1 1 1, 1 (1) : 1
2 2 2 3, 5 (1) : 1
2 2 2 2, 5 (1) : 1
2 2 2 1, 4 (1) : 1
2 2 1 3, 2 (1) : 1
2 2 1 2, 5 (1) : 1
2 2 1 1, 5 (1) : 1
3 1 0 3, 2 (1) : 1
3 1 0 2, 2 (1) : 1
3 1 0 1, 5 (1) : 1
3 2 0 3, 6 (1) : 1
3 2 0 2, 2 (1) : 1
3 2 0 1, 2 (1) : 1
4 0 0 3, 3 (1) : 1
4 0 0 2, 6 (1) : 1
4 0 0 2, 2 (1) : 1

Annexe 6 : Catégorie des facteurs d'influence de risque RIF et leurs descriptifs

Tableau : Description des facteurs d'influence de risque RIF		
Groupe de RIF	RIF	Couvrant les aspects liés à
Personnel	Compétence	Compétence, expérience, connaissance du système de formation du personnel
	Charge de travail/stress	Charge de travail générale sur les personnes (la somme de toutes les tâches et activités)
	Milieu de travail	environnement de travail physique (bruit, vibration, lumière, utilisation de substances chimiques
	Fatigue	fatigue de la personne, par exemple en raison du quart de nuit et une vaste utilisation des heures supplémentaires
Tâche	Méthodologie	méthodologie utilisée pour effectuer une tâche spécifique
	supervision de la tâche	Supervision des tâches spécifiques par un superviseur (p. ex., par le gestionnaire des opérations ou supervision mécanique
	Complexité de la tâche	Complexité d'une tâche spécifique.
	Pression du temps	Pression du temps dans la planification, l'exécution et la finition d'une tâche spécifique
	Outils	Disponibilité et efficacité opérationnelle des outils nécessaires pour effectuer une tâche.
	Pièces de rechange	Disponibilité des pièces de rechange nécessaires pour effectuer la tâche.
Système technique	Conception de l'équipement	Conception d'équipements et de systèmes tels que le type de bride (ANSI ou compact), type de vanne, etc.
	Propriétés des matériaux	Propriétés du matériau sélectionné en ce qui concerne la corrosion, l'érosion. fatigue, joint propriétés des matériaux, etc.
	Complexité du processus	Complexité générale de l'usine de processus dans son ensemble.

	HMI (Interface homme-machine)	Interface homme-machine comme facteurs ergonomiques, étiquetage du matériel, positionner les commentaires des soupapes, des alarmes, etc.
	Maintenabilité /accessibilité	Maintenabilité des équipements et des systèmes tels que l'accessibilité aux valves et brides, espace pour utiliser les outils nécessaires, etc.
	Rétroaction du système	Comment les erreurs et les échecs sont instantanément détectés, à cause de l'alarme, défaut de démarrage, etc.
	Condition technique	Condition de l'installation technique.
Contrôle administratif	Procédures	Qualité et disponibilité des procédures permanentes et des descriptions de tâche/projet
	Permis de travail	Système de travail permet, comme la demande, examen, approbation, suivi et contrôle
	Instructions de travail	Qualité et disponibilité de descriptions de travail comme analyse de sécurité des tâches et plans d'isolement
	Documentation	Qualité, disponibilité et mise à jour des dessins, P & ID, etc.
Facteurs organisationnels	Programmes	Étendue et la qualité des programmes de maintenance préventive (PM), surveillance (CM), inspection, 3ème contrôle du parti du travail, utiliser des listes de contrôle/commande libre, etc. Un aspect important est si PM, CM, etc., est spécifié
	Pratique de travail	Pratique courante au cours de l'accomplissement d'activités professionnelles. Facteurs comme s'il procédures et listes de contrôle sont utilisés et suivi, si les raccourcis sont acceptées, se concentrent sur le temps avant la qualité, etc.
	Supervision	Supervision sur la plateforme comme le suivi des activités, suivi de plans, délais, etc.
	Communication	Communication entre les différents acteurs comme directeur de plateforme secteur, superviseurs, zone techniciens, entrepreneurs de maintenance, techniciens, etc.
	Propreté et nettoyage	Nettoyage général et l'ordre dans différents zones sur la plate-forme.

	Système de soutien	Qualité des systèmes de support de données, etc.
	Critères d'acceptation	Définitions des critères d'acceptation spécifiques associés par exemple : État de surveillance, inspection, etc.
	Activités simultanées	Quantité d'activités simultanées, soit prévu (comme les maintenances et modifications) et imprévus (comme arrêt)
	Gestion des changements	Changements et modifications des changements

Annexe 7 : Programmes MATLAB utilisés pour l'optimisation de l'architecture du système d'arrêt d'urgence

1. Fonctions utilisées pour l'allocation de redondance

Fonction objective pour le système d'arrêt d'urgence :

```
function px = costAvg(n)
n=floor(n); % signifier que les variables utilisées seront transformées en des variables entières
px = 300*n(1)+100*n(2)+ 1000*n(3);
end
```

La contrainte du SIL est écrite comme suit :

```
function [c, ceq] = contrainte(n)
n=floor(n);
c(1)=-(1-(1-0.995105)^n(1))*(1-(1-0.9153138)^n(2))*(1-(1-
0.98322174)^n(3))+0.99;
c(2)=(1-(1-0.995105)^n(1))*(1-(1-0.9153138)^n(2))*(1-(1-0.98322174)^n(3))-
0.999;
ceq=[];
end
```

2. Fonction d'évaluation de la fiabilité des architectures complexes du système d'arrêt d'urgence

```
function f = poincare(x)
f=0;
Psys=0;%c'est la fiabilité du système
P(1:1:3)=0.995105;%fiabilité des détecteurs d'hydrogène
P(4:1:9)=0.9153138;%fiabilité des traitements logiques
P(10:1:13)= 0.98322174;%fiabilité des pompes de recirculation
n=0;%n est le nombre de liens minimaux

for i=1:1:3%détermination des liens  minimales
    if x(i)==1
        for j=i*2+2:1:i*2+3
            if x(j)==1
              if mod(j, 2)==0
                for z=10:1:11
                   if x(z)==1
                       n=n+1;
                       c(n,:)=[i, j, z]; %création de la matrice contenant
les liens minimaux
                   end
                end
                       else
                           for z=12:1:13
                               if x(z)==1
                               n=n+1;
                               c(n,:)=[i,  j,  z];  %création  de  la  matrice
contenant les liens minimaux
                               end
                           end
              end
            end
        end
    end
```

```
end

%développement de la formule de Poincaré pour l'évaluation de la
%disponibilité par la disjonction des liens minimaux
%Si toutes les connexions sont présente, le réseau de fiabilité présente 12
%liens minimaux et autant de termes dans la formule de poincaré
if n>0
    for i=1:n
            Psys=Psys+prod(P(c(i,:)));% 1er terme de Poincaré
    end
end
if n>1
  for i=1:n-1
    for j=i+1:n
         Psys=Psys-prod(P(union(c(i,:), c(j,:))));%2eme terme
    end
  end
end
if n>2
    for i=1:n-2
        for j=i+1:n-1
            for z=j+1:n
                   r1=union(c(i,:),  c(j,:));  %La  fonction  union  n'accepte
%que deux vecteurs comme entrée
                   r2=union(r1,c(z,:));
                   Psys=Psys+prod(P(r2));%3eme terme
            end
        end
    end
end
if n>3
    for i=1:n-3
        for j=i+1:n-2
            for z=j+1:n-1
                for s=z+1:n
                    r1=union(c(i,:), c(j,:));
                    r2=union(r1,c(z,:));
                    r3=union(r2,c(s,:));
                    Psys=Psys-prod(P(r3)); %4eme terme
           end
        end
     end
  end
end
if n>4
    for i=1:n-4
        for j=i+1:n-3
            for z=j+1:n-2
                for s=z+1:n-1
                    for m=s+1:n
                        r1=union(c(i,:), c(j,:));
                        r2=union(r1,c(z,:));
                        r3=union(r2,c(s,:));
                        r4=union(r3,c(m,:));
                        Psys=Psys+prod(P(r4)); %5eme terme
           end
                end
             end
     end
  end
end
```

```
if n>5
    for i=1:n-5
        for j=i+1:n-4
            for z=j+1:n-3
                for s=z+1:n-2
                    for m=s+1:n-1
                        for h=m+1:n
                             r1=union(c(i,:), c(j,:));
                             r2=union(r1,c(z,:));
                             r3=union(r2,c(s,:));
                             r4=union(r3,c(m,:));
                             r5=union(r4,c(h,:));
                            Psys=Psys-prod(P(r5)); %6eme terme
                        end
                    end
                end
            end
        end
     end
end
%les autres termes de la formule de poincaré ont été ignoré afin de réduire
%le temps d'execution du programme
f = Psys;
```