Université Hadj-Lakhdar, Batna

Institut d'Hygiène & Sécurité Industrielle

Laboratoire de Recherche en Prévention Industrielle

THÈSE

Présentée pour obtenir le grade de

DOCTEUR

EN

Hygiène & Sécurité Industrielle

Option : Gestion des Risques

PAR

M^me^ OUAZRAOUI Nouara

Application des Techniques de l'Intelligence Artificielle aux Problèmes de Gestion des Risques Industriels

Soutenue le 22 Juin 2014 devant le Jury composé de :

M.KamelSarairi, Professeur à l'Université de Biskra,	Président
M. Rachid Nait-Said, Professeur à l'Université de Batna,	Rapporteur
Mme Fatiha Zidani, Professeur à l'Université de Batna,	Co-rapporteur
M Mebarak Djebabara, Professeur à l'Université de Batna.	Examinateur
M. Abdellah Tamrabat, Professeur à l'Université de Batna,	Examinateur
M. M. Kourichi, Maitre de Conférence à l'Université de Ouargla	Examinateur

❁2013-2014❁

À la mémoire de mes parents

À ma famille,

À mon mari

À mes adorables enfants

Safoua, Mohamed Anis et Rania

pour leur soutien, leurencouragements

et leur amour.

REMERCIEMENTS

Le travail présenté dans ce mémoire a été effectué au sein de l'équipe « Sureté de Fonctionnement » du Laboratoire de Recherche en Prévention Industrielle.

J'exprime mes profonds remerciements à mon encadreur le professeur Nait Said Rachid pour son aide et ses encouragements tout au long de ce travail. Sa compétence a été un atout à la réussite de ces travaux et m'a permis d'apprendre énormément durant ces années de collaboration.

Je suis très reconnaissante envers Madame Zidani Fatiha, Professeur à l'Université de Batna pour ses encouragements et l'intérêt qu'elle a accordé à ce travail.

J'exprime toute ma gratitude à Monsieur K. Sérairi, Professeur à l'université de Biskra pour avoir accepté la présidence de mon jury d'examen, monsieur M. Djebabra, Professeur à l'université de Batna, Monsieur M. Kourichi, Maître de Conférences à l'université de Ouargla ; Monsieur A. Tamerabat, professeur à l'université de Batna, pour avoir bien voulu me faire l'honneur de juger ce travail et de participer à ce jury.

Mes remerciements très particuliers s'adressent ***augroupe flou :*** *Melle Nouhed. Achouri, Mme L.Chergui, MrM. Bourareche, Mr R.Sal maîtres assistants à l'université de Batna, Mr I.Sellemi, Mr H.Touahar, Mr B.Rabah, , Mr S,Sekiou pour leur aide et leur soutien moral.*

Mes vifs remerciements vont également à mes amies qui m'ont accompagnées de leur affection, amitié et de leurs encouragements pendant toutes ces années, tout particulièrement à Fedali Yamina, Saadi Saadia, Nora Abdesselem, Leila Aouragh, Leila Boubaker, Houria Bencherif, Roukia Ouadai, Leila Mellal, Lylia Bahmed, Ghania Benbrahim, Samia Hariz.

Je remercie également tous mes collèges et personnel de l'institut d'Hygiène et Sécurité Industrielle de l'université de Batna.

Je remercie infiniment mon mari El Hadj Hamadi pour ses aides précieuses sa compréhension et ses encouragements réguliers.

Je remercie enfin tous ceux qui ont contribué de près ou de loin à l'aboutissement de ce travail de thèse.

Merci à toutes et à tous.

N. Ouazraoui

Résumé :

Un problème important auquel fait face les analystes de risque est comment traiter les incertitudes liées aux paramètres d'un scénario d'accident, tels que la fréquence des événements initiateurs, la probabilité de défaillance des barrières de sécurité, la gravité des conséquences et la fiabilité humaine. L'objectif principal assigné à cette thèse est de contribuer à la résolution de certains aspects problématiques de l'évaluation et de la réduction des risques inhérents aux systèmes industriels en présence d'informations incomplètes et/ou incertaines. Des modèles issus des techniques floues et possibilistes sont proposés. Le premier modèle consiste à proposer une approche floue d'évaluation du niveau d'intégrité de sécurité (SIL). Le modèle graphe de risque flou proposé tente d'améliorer le graphe conventionnel en le décrivant par un système d'inférence flou. Une approche LOPA floue permettant l'évaluation des éléments d'un scénario d'accident et les mesures de réduction des risques de manière plus souple et moins contraignante est l'objet du deuxième modèle proposé . Afin de mettre en valeur et valider ces modèles, ils ont été appliqués à un four rebouilleur dans un procédé de traitement de gaz.

Mots-clé : Analyse et évaluation du risque, Incertitudes, Techniques floues et possibilistes, Graphe de risque flou, LOPA flou.

Abstract:

An important problem that the analysts of risks faced is how to deal and treat uncertainties in different parameters of an accident scenario, the frequency of initiating events, the probability of failure of safety barriers, the severity of the consequences and human reliability.

The main objective of this thesis is to contribute to the resolution of certain aspects of the risks assessment and reduction inherent to the industrial systems, taking in consideration the presence of incomplete and/or uncertain data. In this context, two models of uncertainties treatment based on fuzzy and possibility techniques are proposed. The first model consists to propose a fuzzy approach of assessment of safety integrity level (SIL). The fuzzy risk graph model proposed attempts to improve conventional risk graph by describing it using fuzzy inference system. The second approach "Fuzzy LOPA" consists to assess the different elements of an accident scenario and risk reduction measures in a more flexible and less restrictive way. To enhance and validate these proposed models, they were applied in a reboiler system inside the gas treatment process.

Keywords: Risk assessment, Uncertainty, fuzzy and possibility techniques, fuzzy Risk graph, fuzzy LOPA.

ملخص:

يواجه محللو المخاطر مشكلة هامة في كيفية التعامل مع الارتيابات التي تصاحب عناصر سيناريو حادث صناعي، مثل :القيم الخاصة بتردد الأحداث الأولية،احتمال فشل الحواجز الأمنية، خطورة نتائج الحادث و موثوقية الإنسان.

الهدفالرئيسي لهذه الأطروحة هو المساهمة في حل بعض جوانب إشكالية تقييم المخاطر المرتبطة بالنظم الصناعيةو الحد منها خاصة في وجودمعلومات غير كاملة و/ أو غير مؤكدة و ذلك باقتراح نماذج مستمدة من تقنيات منطق الغموض و الاحتمالات . نحاول من خلال اقتراح نموذج أول لتقييم غامض لمستوى السلامة (SIL) تحسين نموذج المخطط البياني التقليدي للخطر و ذلك باستعمال نظام الاستدلالالغامض. الهدف من النموذج الثاني هو اقتراح منهج غامض لتحليل الطبقات الواقية بهدف تحسين النموذج التقليدي و تقييم أسهل و بسيط لعوامل سيناريو حادث صناعي و وسائل الحد منه. و في الأخير و من أجل إبراز أهمية هذين النموذجين و التحقق من صحتهما، تم تطبيقهما على نظام صناعي لمعالجة الغاز.

كلمات دلالية : تحليل و تقييم الأخطار، الارتيابات، تقنيات منطق الغموض و الاحتمالات، المخطط البياني الغامض للخطر ، التحليل الغامض للطبقات الواقية.

TABLE DES MATIERES

DEDICACE i
REMERCIEMENTS ii
RESUME iii
LISTE DES FIGURES viii
LISTE DES TABLEAUX ix
LISTE DES SYMBOLES ET ABREVIATIONS x

INTRODUCTION GENERALE 1

CHAPITRE I : ETAT DE L'ART SUR LES INCERTITUDES EN ANALYSE ET EVALUATION DES RISQUES INDUSTRIELS 5

Introduction 5
I.1 Incertitudes : Concepts, types et sources 6
I.1.1 Concept d'incertitude 6
I.1.2 Types et Sources d'incertitudes 7
I.1.2.1 Incertitudes paramétriques 8
I.1.2.2 Incertitudes de modèle 9
I.1.2.3 Incertitudes de complétude ou d'exhaustivité 9

I.2 Caractérisation de l'incertitude dans les différentes phases d'analyse et évaluationdes risques 9
I.2.1 Etape d'identification 10
I.2.2 Etape d'estimation de la fréquence d'occurrence des événements indésirables 13
I.2.3 Etape d'estimation des conséquences des événements indésirables 16
I.2.4 Etape estimation du risque 19

I.3 Théories de représentation de l'incertitude 19
I.3.1Théorie des probabilités 19
I.3.1.1 Notion de variable aléatoire, Notion de probabilité 20
I.3.1.2 Propriétés de comptabilité et d'incompatibilité d'évènements 21
I.3.1.3 Limitations de la théorie des probabilités 21
I.3.2 Théorie des ensembles flous 22
I.3.2.1 Caractéristiques d'un ensemble flou 23
I.3.2.2 Fonctions d'appartenance 24
I.3.2.3 Opérations sur les ensembles flous 26
I.3.2.4 Nombre et intervalle flous 28
I.3.2.5 Notion d'α-Coupe 29

I.3.2.6 Opérations arithmétiques sur les nombres flous 30
I.3.2.7 Principe d'extension.....31
I.3.3 Théorie des possibilités.....31
I.3.3.1 Mesure floue (Valuation) 32
I.3.3.2 Mesures de possibilité et de nécessité 32
I.3.3.3 Relation entre mesures de possibilité et de nécessité.....33

Conclusion.....34

CHAPITRE II : GRAPHE DE RISQUE FLOU POUR LA DETERMINATION DU NIVEAU D'INTEGRITE DE SECURITE.....35

Introduction 35
II.1 Notions de base relatives à la méthode Graphe de Risque 36
II.1.1 Notion de risque 36
II.1.2 Réduction du risque.....36
II.1.3Facteur de réduction du risque 37
II.1.4 Principe ALARP (As Low As Reasonably Practicable).....38
II.1.5 Systèmes Instrumentés de Sécurité (SIS) 39
II.1.6 Réduction nécessaire du risque 41
II.1.7 Niveau d'Intégrité de Sécurité (SIL).....41

II.2 Méthodes d'allocation du SIL 42
II.2.1 Méthodes qualitatives.....43
II.2.2 Méthodes semi-quantitatives.....43
II.2.3 Méthodes quantitatives 43

II.3 Graphe de risque Conventionnel.....44
II.4 Graphe de risque Etalonné.....47
II.5 Limites et alternatives.....48
II.6 Systèmes d'inférence floue.....51
II.6.1Fuzzification 51
II.6.2 Inférence floue 52
II.6.3 Défuzzification.....52

II.7 Graphe de Risque Flou : Modèle d'évaluation floue d'intégrité de sécurité 53
II.7.1 Sélection de variables d'entrée.....55
II.7.2 Développement des échelles floues 55
II.7.3 Définition des échelles des paramètres C, F, P, W et du SIL 58

II.7.4 Dérivation des règles de logique floue 63
II.7.5 Application de la base de règles floues 64
II.8Validation du modèle Graphe de Risque Flou proposé.....64
Conclusion.....67

CHAPITRE III : APPROCHE FLOUE D'ANALYSE DES COUCHES PROTECTION 69
Introduction 69
III.1 Notions de base relatives à la méthode LOPA.....70
III.1.1Couches de protection 70
III.1.2 Couches de protection indépendantes (IPLs).....73

III.2 Analyse des Couches de Protection (LOPA) conventionnelle.....76
III.2.1 Principe de la méthode LOPA.....77
III.2.2 Etapes d'élaboration de la méthode LOPA.....77
III.2.2.1 Établissement des critères d'acceptabilité des scénarios d'accidents 78
III.2.2.2 Développement et sélection d'un scénario d'accident 78
III.2.2.3 Identification de l'événement initiateur du scénario estimation de sa fréquence 78
III.2.2.4 Identification des IPLs et estimation de leurs PFD.....80
III.2.2.5 Calcul de la fréquence de la conséquence réduite 80
III.2.2.6Calcul de l'indice du risque 81
III.2.2.7 Evaluation du risque par rapport aux critères d'acceptabilité 82

III.3 Formalisme de la méthode LOPA.....85
III.4Avantages, limites de la méthode LOPA conventionnelle.....85
III.5 Apport de la logique floue à l'analyse du risque 90
III.6 Présentation du modèle LOPA floue proposé 92
III.6.1 Fuzzification.....93
III.6.2 Calcul de la fréquence floue de la conséquence réduite.....94
III.6.3 Comparaison avec la fréquence du risque maximum tolérable 95
III.6.4 Prise de décision et réduction du risque 97

Conclusion.....101

CHAPITRE IV : VALIDATION DES MODELES FLOUS PROPOSES 102
Introduction 102
IV.1 Description du processus 102
IV.2 Analyse fonctionnelle du système four rebouilleur H101 103
IV.3 Elaboration, sélection des scénarios d'accidents et analyse des barrières de Sécurité 106
IV.4 Détermination du SIL par la méthode graphe de risque conventionnel 107
IV.4.1 Données relatives aux paramètres C, F, P, W et au SIL 108
IV.4.2 Discussion des résultats 110
IV.5 Détermination du SIL par la méthode graphe de risque flou 111
IV.5.1 Etablissement des échelles floues 111
IV.5.2 Établissement des bases de règles floues 112
IV.5.2.1 Base de règles floues probabilité d'évitement (Prévit-FIS) 114
IV.5.2.2 Base de règles floues relative au paramètre SIL (SIL-SIF) 114
IV.5.3 Fuzzification 115
IV.5.4 Résultats et discussion 117
IV.6Validation du modèle LOPA floue 118
IV.6.1 Scénarios d'accidents retenus pour LOPA 118
IV.6.2 Identification des couches de protection indépendantes (IPL) 119
IV.6.3 Calcul de la fréquence de la conséquence réduite 121
IV.6.4 Application du modèle LOPA floue au système « Four Rebouilleur H101» 121
IV.6.4.1 Fuzzification des données relatives aux paramètres des scénarios d'accident 122
IV.6.4.2 Evaluation de la fréquence floue de la conséquence réduite 125
IV.6.4.3 Comparaison des fréquences floues à la fréquence maximale tolérable 125
IV.6.4.4 Réduction des fréquences des conséquences sous la contrainte de la nécessité 127
IV.6.4.5 Prise en compte des aspects pratiques 129
IV.7Comparaison des résultats des deux modèles flous proposés 131
Conclusion 132
Conclusion générale 134
Références Bibliographie 137

ANNEXES.....148
Annexe 1 :**Développement de scénarios d'accident par HAZOP** 148
Annexe 2 :**Exemple d'étalonnage du graphe de risque général** 151

LISTES DE FIGURES

Code	Titre	Page
Figure I-1	Relation simplifiée entre L'analyse, l'évaluation et la gestion du risque	10
Figure I-2	Eléments incertains liés au scénario d'accident issu de l'AMDEC	11
Figure I-3	Exemple d'un arbre de défaillances	15
Figure I-4	Exemple d'un AdE avec des barrières de sécurité	17
Figure I.5	Théorie classique par rapport à la théorie floue	23
Figure I-6	Caractéristiques d'un ensemble flou	24
Figure I-7	Présentation de quelques fonctions d'appartenance	26
Figure I-8	Illustration de quelques opérations sur les ensembles flous	28
Figure I-9	Intervalle flou trapézoïdal	29
Figure I-10	Description d'un ensemble flou triangulaire par ses α-coupes	30
Figure II-1	Réduction du risque	37
Figure II-2	Principe ALARP	38
Figure II-3	Système Instrumenté de Sécurité	40
Figure II-4	Modèle de réduction du risque	41
Figure II-5	Exemple de graphe de risque	46
Figure II-6	Graphe de risque avec une description qualitative des paramètres	47
Figure II-7	Procédure globale d'évaluation du SIL à base de règles floues	54
Figure II-8	Valeurs moyennes inférieure et supérieure de Q	57
Figure II-9	Transformation d'un intervalle ordinaire en un intervalle flou	58
Figure II-10	Transformation des intervalles ordinaires en intervalles flous	60
Figure II-11	Fonctions d'appartenance générées pour les paramètres du risque C, F, P et W	62
Figure II-12	Fonctions d'appartenance générées pour le SIL	63
Figure II-13	Surface floue du SIL	65
Figure II-14	Variation du SIL en fonction des paramètres du risque	66
Figure III-1	Les couches protection	71
Figure III-2	Couches de protection et déroulement d'un scénario d'accident	72
Figure III-3	Réduction du risque par les couches de protection	73
Figure III-4	Exemple d'une IPL non indépendante de l'événement initiateur	75
Figure III-5	Exemple d'Arbre d'Evénements avec trois couches de protection	77
Figure III-6	Données HAZOP exploitées par LOPA	79
Figure III-7	Procédure globale de LOPA floue	93
Figure III-8	Exemple de probabilité floue	94
Figure III-9	Comparaison de deux nombres flous	95
Figure III-10	Mesures de Possibilité et de nécessité de $\widetilde{f}_i^C \leq TR$	97
Figure III-11	Réduction de la fréquence sous une contrainte de nécessité	100
Figure IV-1	Four rebouilleur H101 : Organigramme flux du processus	103
Figure IV-2	Fonctions d'appartenance générées pour : (a) Vitesse d'évacuation, (b) PFD Alarme et (c) Possibilité d'évitement	113
Figure IV-3	Surface floue correspondant à la probabilité d'évitement du phénomène dangereux	113
Figure IV-4	Processus d'inférence des règles floues ($Pr_{évit}$-FIS)	115
Figure IV-5	Processus d'inférence des règles floues (SIL-FIS) : Cas du scénarioS1	116
Figure IV-6	Processus d'inférence des règles floues (SIL-FIS) : Cas du scénarioS2	116
Figure IV-7	Arbres d'Evénements relatifs aux scenarios d'accident retenus.	120

Figure IV-8	Représentation floue de la fréquence de l'événement initiateur, de la PFD et de la probabilité d'ignition (a) scénario 1, (b) scénario 2 et (c) scénario3.	123
Figure IV-9	Comparaison des fréquences floues des conséquences réduites au TR	126
Figure IV-10	Réduction de la fréquence de la conséquence, sous la contrainte de nécessité	128
Figure IV-11	Réduction de la fréquence des conséquences via des modifications pratiques	130

LISTE DES TABLEAUX

Code	Tableau	Page
Tableau II-1	Exemple de classification des risques d'accidents	39
Tableau II-2	Relation entre classes et zones de risque	39
Tableau II-3	Les niveaux de SIL	42
Tableau II-4	Paramètres du risque utilisés par le graphe de risque	45
Tableau II-5	Exemple de classification des paramètres du risque	46
Tableau II-6	Exemple de définitions qualitative et quantitative des paramètres du risque	48
Tableau II-7	Transformation des intervalles ordinaires en intervalles flous	59
Tableau II-8	Règles de combinaison des paramètres du risque	65
Tableau III-1	Tableau d'analyse de LOPA	87
Tableau III-2	Valeurs typiques des fréquences de l'événement initiateur	89
Tableau III-3	Valeurs typiques de PFD des IPLs	89
Tableau IV-1	Décomposition du système four rebouilleur H101	104
Tableau IV-2	Scénarios d'accident retenus relatifs au four rebouilleur H101	107
Tableau IV-3	Les fréquences d'occurrence des événements initiateurs	108
Tableau IV-4	Résultats d'application du graphe de risque conventionnel	110
Tableau IV-5	Règles relatives à la probabilité d'évitement du phénomène dangereux	114
Tableau IV-6	Comparaison des résultats de l'évaluation du SIL pour les différents scénarios	117
Tableau IV-7	Scénarios d'accidents retenus	119
Tableau IV-8	Fréquence des événements initiateurs	119
Tableau IV-9	Probabilités de défaillance à la demande des IPL	120
Tableau IV-10	Partition floue des intervalles des paramètres fréquence des EI et PFD des IPL	123
Tableau IV-11	Niveaux α des intervalles des fréquences floues	125
Tableau IV-12	Mesures de possibilité et de nécessité liées aux fréquences initiales	126
Tableau IV-13	MRRF pour λ=0.5 et TR=10-5/an	127
Tableau IV-14	Mesures de possibilité et de nécessité liées à la réduction théorique	129
Tableau IV-15	Modifications données par des experts du processus	129
Tableau IV-16	Mesures de possibilité et de nécessité relatives aux réductions pratiques	131

LISTE DES SYMBOLES ET ABREVIATIONS

AdD	Arbre de Défaillances
AdE	Arbre des Evénements
ALARP	As Low As Reasonably Practicable
AMDEC	Analyse des Modes de Défaillances, de leurs Effets et leur Criticité
BLEVE	Boiling Liquid Expanding Vapors Explosion
BPCS	Basic Process Control System
CCPS	Center for Chemical Process Safety
DCS	Distributed Control System
E/E/EP	Électrique / Électronique / Électronique Programmable
ESD	Emergency Shutdown
EUC	Equipment Under Control
FC	Fail Closed
FI	Flow Indicator
FICA	Flow Indicator Controller Alarm
FICAL	Flow Indicator Controller Alarm Low
FIS	Fuzzy Inference System
FO	Fail Open
FRA	Flow Recorder Alarm
FRAL	Flow Recorder Alarm Low
GPL	Gaz de Pétrole Liquifié
H	Heater
HAZOP	HAZard and OPerability study
HSE	Health and Safety Executive
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INERIS	Institut National de l'Environnement Industriel et des Risques
IPL	Independent Protection Layers
ISO	International Standard Organisation
LOPA	Layers of Protection Analysis
LS	Logic Solver
MPP3	Module Process Plant 3

MRRF	Minimum Risk Reduction Factor
OREDA	Offshore REliability DAta
PA	Pressure Alarm
PCV	Pressure Controller Valve
PFD	Probability of Failure on Demand
PFH	Probability of Failure on Hour
PHA	Process Hazard Analysis
PIA	Pressure Indicator Alarm
PLC	Programmable Logic Controller
RRF	Risk Reduction Factor
SAR	Scénarios d'Accidents Représentatifs
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SMS	Système de Management de la Sécurité
SONATRACH	Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures
SH/DP /HRM	SONATRACH/Division Production/ Hassi R'mel
TI	Temperature Indicator
TOR	Tout ou Rien

Introduction générale

Introduction générale

1- Problématique

La complexité des systèmes industriels ainsi que les risques inhérents à leurs utilisations ne cessent de croître à tel point qu'aujourd'hui les industriels ne devraient plus les ignorer s'ils veulent garantir la sécurité de leurs systèmes tout en respectant les objectifs de production. La survenue de plusieurs catastrophes industrielles ayant entraîné de graves conséquences socio-économiques, a confirmé la nécessité de maîtriser les nouveaux risques dont les effets ne concernent pas uniquement le système en question mais aussi son environnement. Ces nouvelles contraintes sont à l'origine d'une règlementation de plus en plus sévères (IEC 61508) et (IEC 61511) qui exigent aux propriétaires de procéder à des études concrètes et approfondies de leurs systèmes ou de leurs projets afin de mettre en évidence les points critiques au regard des risques et de montrer comment ils peuvent les maitriser.

Pour ce faire, une démarche de gestion des risques industriels s'avère indispensable. Cette démarche comporte trois étapes principales (ISO, 99), (Kum, 07), (Ave, 11) :

(i) L'analyse du risque qui consiste à identifier les événements dangereux et les situations dangereuses associées qui peuvent entraîner des accidents potentiels,

(ii) L'évaluation du risque, il s'agit d'estimer les risques identifiés en termes de probabilité d'occurrence et de gravité des conséquences. Le niveau de risque estimé sera comparé à un niveau de risque jugé acceptable. La définition des critères d'acceptabilité est une étape clé dans le processus de gestion des risques dans la mesure où elle va susciter la nécessité de considérer de nouvelles mesures de réduction du risque et, rétroactivement, influencer la façon de mener l'analyse et l'évaluation des risques,

(iii) La maitrise (ou la réduction) du risque qui désigne l'ensemble d'actions et dispositions entreprises en vue de diminuer la probabilité et/ou la gravité des dommages associés à un risque particulier (ISO 99). De telles mesures doivent être envisagées dès lors que le risque considéré est jugé inacceptable.

Il est à noter à ce propos que la qualité des résultats issus de ce processus de gestion dépend des données utilisées. En effet, pour beaucoup de systèmes industriels et en raison du manque de données sur les événements dangereux de base pouvant faire l'objet d'un

Traitement statistique fiable, il est souvent difficile de procéder à une estimation du risque, et donc à une éventuelle réduction, en se basant uniquement sur des méthodes quantitatives.

Le recours à l'évaluation semi quantitative semble être une alternative étant donné que des méthodes telles que la matrice de criticité, le RPN (Risk Piority Number), (Gui, 03), (Don, 07) (*le graphe de risque étalonné* (Bag, 13)*, l'analyse des couches de protection (LOPA), etc. ont connu une large utilisation dans ce domaine vu qu'elles sont moins exigeantes en termes de données précises sur les paramètres du risque* (Hau, 04), (Wei, 08).

Toujours dans le contexte de manque de données, si l'on prévoit des systèmes de sécurité sur la base d'une évaluation du risque, ces systèmes devraient effectuer la réduction nécessaire qui ramène le risque initial à un niveau minimum. La méthode graphe de risque et la méthode LOPA sont les plus utilisées pour déterminer le niveau d'intégrité de sécurité (CCP, 01), (IEC, 03), (Kir, 05). Ces méthodes utilisent des données issues de la littérature telles que les bases de données IEEE (IEE, 84), CCPS *(CCP, 89),* OREDA *(ORE, 02) ou de jugement d'experts sous forme de valeurs uniques (moyennes) ou d'intervalles de confiance (Sim,07).*

L'expérience a montré que ces données sont souvent imprécises et/ou incertaines (Ave, 11) et que dans le cas où elles sont disponibles, elles devraient être ajustées selon le système étudié et ses conditions opératoires pour qu'elles puissent ensuite être utilisées, (Zad, 65), (CCP, 00).

Par ailleurs, la définition des échelles de cotation relatives aux grandeurs du risque à savoir la fréquence et la gravité pose également un problème. Les catégories constituant 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 la fréquence et la gravité des situations réelles, particulièrement en présence d'événements rares ou de systèmes nouveaux en phase de conception(Nai,04), (Oua, 10).

De plus, cette cotation néglige les effets de confusion entre catégories (chevauchement des intervalles) qui reflète la nature du raisonnement humain. A ceci s'ajoute la discontinuité des échelles utilisées qui pose un problème d'interprétation des résultats de l'évaluation.

La prise de décision qui se traduit par des modifications de conception, de procédures de conduite ou de maintenance des installations, dépend de la disponibilité et de la nature de ces données. Leur élaboration et leur utilisation doivent donc faire l'objet d'une validation soigneuse afin de pouvoir effectivement prendre des décisions en toute connaissance de causes.

Le recours à des méthodes qualitatives et semi quantitatives, avec comme support les techniques floues et possibilistes, pour le traitement des données imprécises et/ou incomplètes et/ou incertaines, semble offrir un cadre adéquat pour la manipulation de ces données.

2- Objectif de l'étude

L'objectif principal de cette thèse étant de contribuer à la résolution de certains aspects problématiques de l'évaluation et de la réduction des risques inhérents aux systèmes industriels en présence d'informations incomplètes et/ou incertaines. Des modèles issus des techniques floues et possibilistes sont proposés. Le premier modèle consiste en une approche d'évaluationfloue du niveau d'intégrité de sécurité (SIL). Le modèle graphe de risque flou proposé tente d'améliorer le graphe de risque conventionnel en le décrivant par un système d'inférence floue.

Une approche LOPA floue permettant l'évaluation des éléments d'un scénario d'accident et les mesures de réduction des risques de manière plus souple et moins contraignante est l'objet du deuxième modèle proposé. L'intérêt de LOPA floue proposée est de tenir compte des données imparfaites selon un modèle offrant plus de souplesse lors de la prise de décision quant à la réduction du risque. La fréquence floue de la conséquence réduite est calculée en utilisant le principe d'extension et la méthode des α-coupes. Le résultat sera comparé à la fréquence du risque maximal tolérable, et la réduction exigée est obtenue par une prise de décision possibiliste sous une contrainte de nécessité.

3- Structure de la thèse

Ce mémoire de thèse comporte quatre chapitres :

- *Le premier chapitre a pour objectif de présenter un état de l'art sur les incertitudes et les théories de leur représentation en analyse et évaluation des risques industriels.*

- *Dans le deuxième chapitre, nous abordons d'abord les notions de base relatives à la méthode graphe de risque. Ensuite, nous exposons l'approche graphe de risque flou basée sur un système d'inférence floue.*

- *Le troisième chapitre est consacré à la présentation de l'approche LOPA floue. Cette présentation est précédée par un rappel des définitions des notions fondamentales utilisées par la méthode LOPA, ensuite la présentation de la méthode LOPA conventionnelle et une discussionde ses limites.*
- *Afin de valider les deux modèles flous proposés dans les chapitres précédents, le quatrième chapitre sera consacré à leur application à un système industriel opérationnel.*

Enfin, la présente thèse sera clôturée par une conclusion générale résumant le travail accompli, le bilan global de nos contributions et les perspectives envisagées.

CHAPITRE I :

Etat de l'art sur les incertitudes dans la gestion des risques industriels

---

Résumé : *Ce premier chapitre a pour objectif l'analyse et le traitement des incertitudes. Dans une première partie, nous nous focalisons sur les principaux types et méthodes de représentation des incertitudes. La démarche d'analyse des risques et l'implication de l'incertitude dans les différentes étapes de cette démarche font l'objet d'une seconde partie. En fin, la troisième partie a pour objet de présenter un état de l'art sur les travaux réalisés dans le cadre de l'analyse des risques.*

Introduction

L'évaluation quantitative des risques (QRA), appelée aussi l'évaluation probabiliste des risques, consiste à identifier tous les scénarios possibles pouvant conduire à des événements indésirables, à évaluer la gravité de leurs conséquences et à calculer leurs probabilités d'occurrence et les évaluer par rapport aux critères d'acceptabilité établis au préalable.

Or un problème crucial, auquel les analystes de risques sont confrontés, s'impose est celui de la crédibilité et l'utilisation des résultats obtenus. En effet, il s'agit de savoir comment traiter les incertitudes liées aux différentes étapes du processus d'évaluation des risques (Abr, 02), (Kum, 07), (Ave, 11), et comment les prendre en considération à des fins de prise de décision qui est la finalité du processus de gestion des risques.

Dans l'étape évaluation des risques, l'erreur de mesure et l'incertitude surgissent en raison de la limitation de l'outil de mesure, de la procédure de mesure, et de la personne effectuant la mesure (Nai, 04). La complexité de système augmente l'incertitude, puisque les modèles théoriques et empiriques ne prennent pas en considération certains phénomènes pertinents,y compris leurs régimes, les mécanismes et les valeurs des paramètres, et peuvent être basés sur un large éventail d'hypothèses sujettes à l'incertitude (Zad, 73), (Lee, 96), (Muh, 04). En outre, les conditions de fonctionnement et l'exploitation des systèmes changent constamment.

Les données historiques sur la fréquence de défaillance du système et de sa défense sont rares. Un exemple typique est celui les systèmes instrumentés de sécurité (SIS) fonctionnant en mode faible demande qui est le mode le plus commun dans les processus (Sal, O8). Les demandes ou sollicitations pour activer une fonction instrumentée de sécurité d'un SIS sont des événements rares (moins d'une fois par an) et les composants d'un SIS n'avaient pas fonctionné assez longtemps pour fournir des données fiables sur leurs défaillances. Ainsi, l'utilisation des expériences historiques n'est pas évidente dans le traitement de ces taux de défaillances (Lee, 96), (Abr, 02), (Ave, 08).

Certaines hypothèses sont utilisées dans l'établissement des scores de risque lorsque les données statistiques ne sont pas fiables ou non disponibles,

«le risque augmente l'incertitude» en est la plus connue. C'est une approche conservatrice exigeant que le risque soit surestimé en supposant des conditions défavorables.

Cette approche augmente la crédibilité d'évaluation des risques (particulièrement pour le public) mais elle implique des coûts d'exploitation et de maintenance plus élevés.

Le recours à une autre approche peut être justifié, il s'agit de traiter avec prudence l'état d'«absence ou d'information imparfaite» en considérant une gamme de scores de risque. Il semble que la robustesse suffisante dans l'estimation de la fréquence des conséquences ne peut être atteinte à l'aide des valeurs simples (souvent des moyennes ou des valeurs pessimistes). Pour beaucoup de systèmes, il est souvent difficile de traiter les fréquences des événements initiateurs et les PFD (ProbabilityFailure on Demand) des IPLs (Independent Protection Layer) en tant que valeurs précises à cause de l'incertitude liée aux données sur la défaillance des composants (Chu, 92). Ainsi, la prise de décision pourrait être basée sur des critères pessimistes et/ou optimistes selon le niveau global de la sécurité des systèmes (Zad, 83) (Lee, 96), (Man, 05).

Ce premier chapitre a pour objectif l'analyse et le traitement de l'incertitude. Pour atteindre cet objectif, nous rappelons dans une première partie, une définition de l'incertitude sera donnée ainsi qu'une présentation des principaux types et méthodes de présentation de l'incertitude. La démarche d'analyse des risques et l'implication de l'incertitude dans ses différentes étapes feront l'objet d'une seconde partie.Un état de l'art sur les travaux réalisés dans le cadre de l'analyse des risques constituera la troisième partie.

I.1 Incertitudes : concepts, types et sources

I.1.1 Concept d'incertitude

Malgré l'implication de l'incertitude dans tous les domaines, il n'existe pas une appréhension commune de ce concept (ICS, 11) :

- Bouchon-Meunier (Bou, 95) en Intelligence Artificielle, définit l'incertitude comme un doute sur la validité d'une information provenant d'une fiabilité relative de l'intermédiaire d'observation.

- Zadeh(ICS, 11) définit l'incertitude comme une propriété de l'information.
- Dubois (ICS, 11) propose une formalisation d'un problème de décision dans un contexte incertain :

Une décision est une application $d{:}S \rightarrow X,(s) = x$ conséquence de la décision d dans l'état s. Avec:

S : ensemble d'états possibles de l'univers de discours $s \in S$

D : ensemble de décisions (actions) : $d \in D$

X : ensemble de conséquences possibles : $x \in X$

Une connaissance partielle sur l'état de l'univers de discours implique de l'incertitude chez le décideur. Un éventail de situations d'incertitude, suivant le type d'information dont on dispose, se situe entre les situations extrêmes suivantes:

- le risque : une situation d'incertain probabilisé : il existe une unique distribution de probabilité P sur (S, X) et cette probabilité est connue de manière objective ;
- l'incertain total : caractérisé par l'absence de toute information sur les événements.

Entre deux cas extrêmes, il existe différentes situations présentant des niveaux d'incertitude différents, suivant que l'on a plus ou moins d'informations sur la probabilité des événements. L'incertitude est donc attribuée au manque d'informations parfaites à propos d'un phénomène, d'un processus ou des données nécessaires à la définition et la résolution du problème.

I.1.2 Types et Sources d'incertitudes

Dans la littérature, il est question de plusieurs types et sources d'incertitude. Dans le cadre de l'évaluation quantitative des risques, deux grands types d'incertitude ont été identifiés (Dub, 99a), (Abr, 02), (Kum, 07), (Mar, 10), (Le D, 11) :

- Incertitudes aléatoires (stochastiques ou objectives) associées à n'importe quel processus variable ou déduites d'une simple statistique. Ce type d'incertitudes est lié au caractère aléatoire inhérent aux phénomènes ou aux comportements propres aux

systèmes. On ne peut pas dans ce cas attribuer une valeur unique à un événement aléatoire, mais une distribution de valeurs associées à des probabilités.

- Incertitudes épistémiques (ou dues à la subjectivité) associées aux phénomènes et événements pour lesquels on ne dispose pas d'informations quantitatives.

  Ce typed'incertitudes est lié au manque de connaissances sur les valeurs à attribuer à certaines quantités.

La différence principale entre les deux types d'incertitude est d'ordre pratique ; l'incertitude aléatoire est par définition irréductible, alors que l'incertitude épistémique peut être réduite par une étude plus approfondie en rassemblant plus d'informations (Abr, 02), (Yeo, 05). Partant de cette distinction entre les types d'incertitudes dans le cadre de l'analyse des risques, on peut dire que la notion de risque est étroitement liée à la notion d'incertitude (Cay, 96). En se référant à la définition même du risque comme étant « une mesure de la probabilité et de la gravité d'un événement indésirable », on peut conclure que le caractère incertain est lié à l'apparition de cet événement (interprétation subjective des probabilités).

L'incertitude est donc, le résultat d'un manque de connaissances. D'autre part, l'incertitude aléatoire s'annule partiellement d'elle-même dans une analyse des risques. Dans un modèle d'évaluation probabiliste, le taux de défaillance en fonctionnement par exemple, est considéré sur une durée spécifique et la valeur obtenue est une valeur unique. Le caractère aléatoire du temps de défaillance n'est pas pris en considération. Plusieurs études (Wan, 04), (Sal, 08), (Mar, 10) (Le D, 11) ont montré que les résultats de l'évaluation quantitative des risques sont généralement affectés par des incertitudes épistémiques et doivent être pris en considération dans le processus décisionnel. Dans ce cadre, les incertitudes du type épistémique sont classées en trois catégories (Cay, 96) (Abr, 02), (Kum, 07), (Ave, 11) :

- Incertitudes liées aux paramètres ;
- Incertitudes liées au modèle ;
- Incertitudes d'incomplétude (information incomplète).

I.1.2.1 Incertitudes paramétriques : Apparaissent quand les valeurs des paramètres ne sont pas exactement connues. Souvent, on traite ce genre d'incertitudes en attribuant une distribution de probabilité ou une autre distribution pour le paramètre représentant les connaissances de l'analyste. Les paramètres utilisés dans un modèle peuvent aussi être sujet à une variabilité naturelle.Celle-ci est associée à l'incertitude inhérente aux processus physiques naturels dont l'occurrence varie d'un endroit à l'autre et d'un temps à l'autre (Abr, 02), (Yeo, 05). Ainsi, leur occurrence et leur ampleur (intensité) ne peuvent pas être prédis avec précision.Ce type d'incertitudes est fréquent car les données disponibles et utilisées dans le secteur industriel sont souvent incomplètes, incorrectes et entachées d'incertitudes. On a souvent tendance à utiliser des valeurs moyennes uniques ou des intervalles de confiance issus du retour d'expérience, de la littérature ou des jugements d'experts. Cependant, en plus de l'incertitude entachant ces données (intervalles larges, valeurs issues de statistiques non fiables), il y a une déclaration ferme (problème de rigidité) pouvant exclure d'autres valeurs possibles. Notons enfin que ce type d'incertitudes est facile à quantifier (Mar, 10) car il existe des méthodes mathématiques qui permettent leur traitement quantitatif (CCP, 00).

I.1.2.2 Incertitudes liées au modèle : Ce sont des incertitudes qui surviennent du fait que n'importe quel modèle, que ce soit de nature conceptuelle ou mathématique, n'est qu'une représentation simplifiée de la réalité du phénomène ou du système étudié (CCP, 00) (Abr, 02), (Mar, 10). Le niveau d'incertitude dépend à la fois de la bonne connaissance du phénomène physique étudié, du degré de simplification adopté et des hypothèses formulées par les experts pour le modéliser (Abr, 02), (Le D, 11).

I.1.2.3 Incertitudes de complétude ou (d'exhaustivité) : Ce type d'incertitudes provient du fait que le modèle d'évaluation des risques ne prend pas en considération tous les événements contribuant au risque (Abr, 02), (Mar, 10), (Le D, 11). Aucun modèle ne prend en considération par exemple, tous les événements initiateurs possibles. Ce type d'incertitudes est inhérent à la phase qualitative de l'analyse (l'identification) et il est difficile à quantifier.

I.2 Caractérisation de l'incertitude dans les différentes phases de gestion des risques

L'évaluation quantitative des risques consiste à quantifier, sur la base de l'analyse des scénarios, les niveaux de risques d'un système en termes de fréquences des événements indésirables et leurs conséquences. Cette approche s'appuie sur des méthodes d'analyse permettant d'identifier, aussi complètement que possible, les chemins ou les séquences susceptibles de conduire à des événements indésirables, de déterminer leurs causes et d'en évaluer les probabilités d'occurrence afin de juger de leur acceptabilité et définir les actions préventives et correctives nécessaires.

L'analyse quantitative des risques consiste en trois grandes phases : phase d'analyse, phase d'évaluation et phase de réduction (Fig. I.1).

L'incertitude dans ce cas, peut être présente à n'importe quelle étape de ce processus.

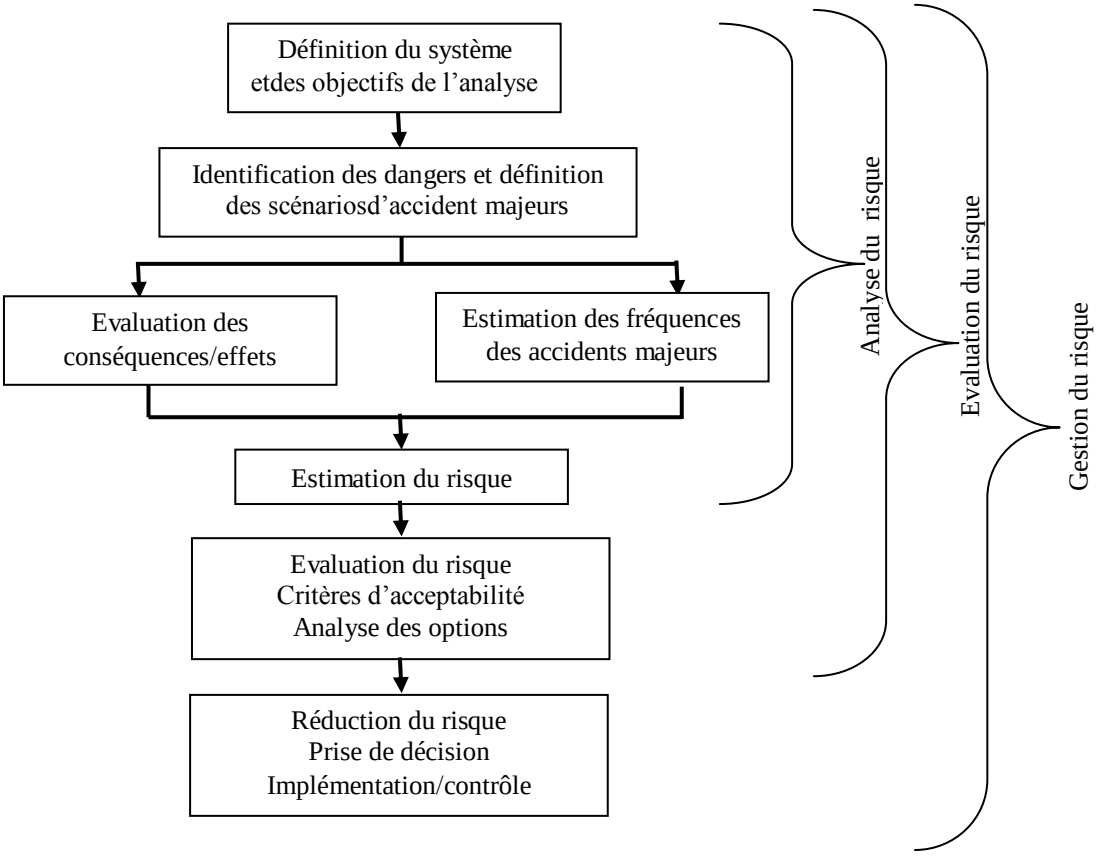


Fig. I.1 : Relation simplifiée entre l'analyse, l'évaluation et la maîtrise du risque (Abr, 02).

I.2.1 Étape d'identification

L'objectif de cette étape est de décrire le système et d'identifier les événements initiateurs ainsi que les scénarios d'accidents majeurs possibles. Ces scénarios désignent les séquences accidentelles qui devront être maîtrisées en priorité.

La démonstration de la maîtrise des risques doit être réalisée pour chacun des scénarios d'accidents majeurs, notamment par l'évaluation de leur gravité et de leur fréquence d'occurrence. Parmi les scénarios d'accidents majeurs identifiés, certains feront l'objet d'une estimation quantitative des conséquences afin de fournir des éléments pour démontrer l'efficacité de la maîtrise des risques. Plusieurs outils ou méthodes d'analyse peuvent être utilisés dans l'identification des événements indésirables. L'APR (Analyse Préliminaire des Risques), HAZOP (HAZardandOPerabilitystudy) (IEC, 01) et l'AMDEC (Analyse des Modes de Défaillances, de leurs Effets et leurs Criticité) en sont les plus répondus (FMC, 88).

L'AMDEC est une méthode inductive d'analyse utilisée pour l'étude systématique des modes de défaillances des composants et de leurs effets sur le système. Elle a pour objectifs (Vin, 06), (Lan, 07):

- d'évaluer les effets et la séquence de chaque mode de défaillance sur les différentes fonctions du système,
- d'identifier les modes de défaillance ayant d'importants effets sur la sureté de fonctionnement du système,
- de classer les modes de défaillances identifiées (suivant la facilité avec laquelle ces derniers peuvent être détectés) et de les diagnostiquer.
- Chaque mode de défaillance est étudié en termes de gravité des effets (S), de fréquence d'occurrence (O) et de détectabilité au cours du prochain test (D) (Fig. I.2). Cette méthode, en plus de son caractère d'analyse qualitatif, elle permet d'évaluer quantitativement les modes de défaillance en mesurant leur gravité, leur fréquence d'occurrence, et leur probabilité de détection.

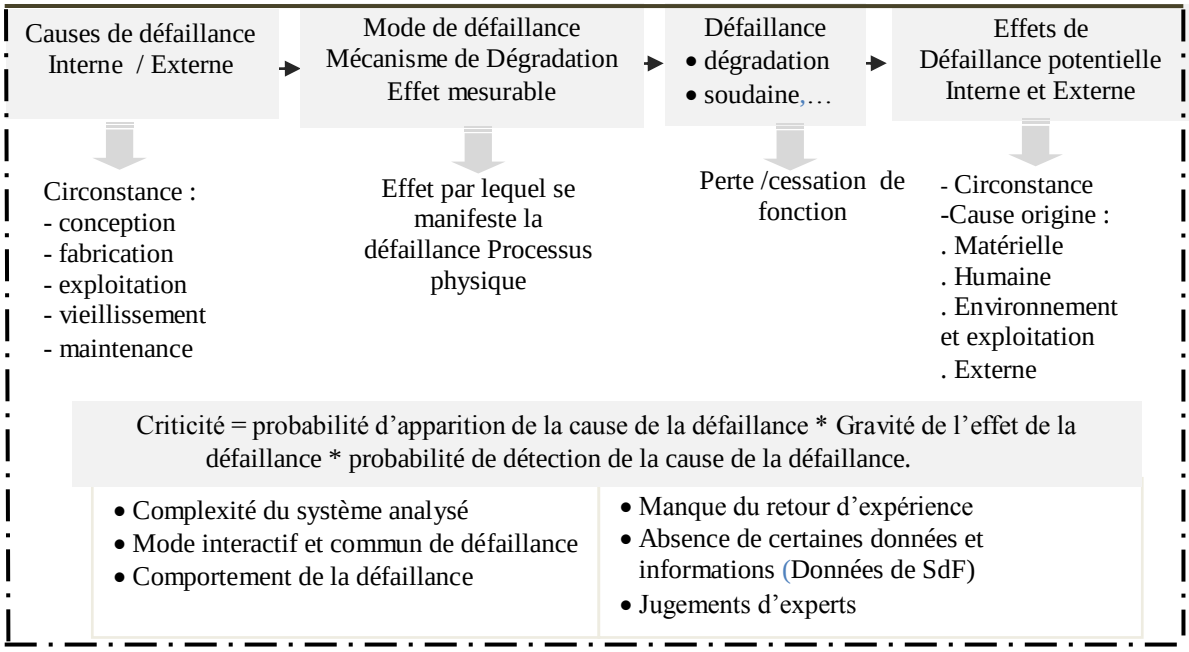


Fig. I.2 : Éléments incertains liés au scénario d'accident issu d'une AMDEC

La méthode la plus répondue dans l'évaluation de la criticité des modes de défaillances est le RPN (RiskPriorityNumber). Elle combine les paramètres cités ci-dessus selon la relation :

$$RPN = O.S.D \quad \text{(I.1)}$$

Chaque paramètre est représenté sur une échelle de 1 à 10 avec cinq niveaux pour la gravité et la fréquence et six niveaux pour la détectabilité ; à chaque classe est attribuée une description qualitative et/ou quantitative. Ainsi le RPN sera coté sur une échelle de 1 à 1000. Les modes de défaillances ayant les valeurs du RPN les plus élevées seront considérées comme les plus critiques (Bow, 03).

Malgré l'applicabilité de la méthode, le RPN reste sujet à un certain nombre d'inconvénients touchant à la fois la méthode de calcul et la manière d'interprétation des résultats (Bow, 98), (Bow, 03). En effet, dans le calcul du RPN, on utilise des échelles numériques (pour l'évaluation des paramètres S, O et D) dans le sens où la gravité 8 est deux fois plus importante que la gravité 4 alors que les scores de ces deux échelles expriment plutôt un ordre. Le produit des trois paramètres pose donc un sérieux problème d'interprétation et de classement. Par exemple, un mode de défaillance ayant une gravité 2,

une détectabilité 6 et une occurrence 9, et un autre mode de défaillance ayant une gravité 9, une détectabilité 3 et une occurrence 4, ont tous les deux un RPN de 108 alors qu'il est difficilement admissible qu'ils aient la même importance en termes de cout et d'actions préventives ou correctives.

Par ailleurs, cette évaluation est souvent difficile voire impossible surtout en présence des données et informations incertaines et incomplètes sur l'ensemble de composants, leurs modes interactifs de fonctionnement et de défaillance ainsi que les interdépendances entre les effets et modes de défaillance (Bra, 03), (Pil, 03), (kum, 05).

Il convient de noter que l'incertitude introduite à cette étape d'analyse est du type incertitudes de complétude qui est dans ce cas inhérente à l'identification : est-ce que tous les facteurs de risque et tous les scénarios pertinents ont été complètement et correctement identifiés ? A ceci s'ajoute le problème d'erreurs commises dans la prise en compte et l'évaluation des relations entre les facteurs de risque et les conséquences (Kli, 04), (Mar, 10). Ces erreurs sont dues aux incertitudes de modélisation. Enfin, l'utilisation de données issues des bases de données doit répondre à certaines exigences, telles que l'objectif de l'analyse et l'étape de l'analyse.

Pour remédier à ce type de problèmes, plusieurs travaux ont été développés (Pel, 94), (Bow, 95), (Xu, 02), (Sha, 05), (Cha, 07), (Don, 07),(Dar, 08) afin de mettre en évidence

l'intérêt du recours à la logique floue dans la résolution des problèmes liés à l'évaluation de la criticité du risque en présence de connaissances imparfaites.

Les premiers travauxsont dus à E. Peláez et J. B. Bowles, (Pel, 94) et (Bow, 95) où une nouvelle technique d'analyse et d'évaluation de la criticité, basée sur la logique floue, a été développée. La procédure proposée est similaire à celle utilisée dans les systèmes experts et les systèmes de contrôle flous (Lee, 90), (Pel, 94). L'analyse utilise les variables linguistiques pour décrire les inputs du système (gravité, fréquence et détectabilité). Ces variables (entrées) sont fuzzifiées à l'aide de fonctions d'appartenance pour déterminer le degré d'appartenance dans chaque classe.

Les entrées floues résultantes sont ensuite évaluées moyennant la base de règles linguistiques adoptée et les opérations de la logique floue pour produire une classification de la criticité du mode de défaillance, et un degré d'appartenance associé à la classe de risque.

La sortie floue est ensuite défuzzifiée par la méthode de la moyenne des maximums pour donner le degré de priorité du mode de défaillance considéré.

D'après les auteurs, cette approche présente les avantages suivants :

- Elle permet à l'analyste d'évaluer le risque associé au mode de défaillance de façon "naturelle" c'est-à-dire directement à partir des variables linguistiques habituellement employées dans le processus d'évaluation ;
- Les informations vagues, ambiguës, qualitatives et quantitatives peuvent être utilisées et traitées de manière souple et cohérente.
- Elle donne plus de flexibilité à la méthode de combinaison des variables du RPN.

I.2.2 Étape d'estimation de la fréquence d'occurrence des événements indésirables

Une fois les événements indésirables identifiés, il convient d'estimer leur fréquence d'occurrence en tenant compte de tous les facteurs potentiels qui peuvent y conduire. L'estimation de la fréquence d'occurrence des événements indésirables consiste à assigner une valeur numérique à ces événements. Les principales techniques, les plus utilisées (Zio, 07) pour estimer ou calculer ces fréquences, sont le retour d'expérience (données historiques), les Arbres de défaillances (AdD) et les Arbres d'Evénements (AdE).

Le recours aux données historiques et aux fréquences des incidents est largement connu dans l'évaluation des risques vue la simplicité relative de la méthode (Abr, 02).

Selon cette approche, une estimation de la fréquence d'un événement peut être faite en divisant le nombre d'incidents enregistrés par la période d'exposition. Cette approche exige que le nombre de cas soit important et l'applicabilité des données au processus. L'avantage de cette approche est qu'elle prend en considération la pluparts des circonstances pertinentes conduisant à l'événement indésirable, telles que les modes de défaillances intrinsèques difficiles à analyser (erreurs humaines, défaillances de causes communes, etc).

Les problèmes d'incertitudes liés à cette approche proviennent des questions de précision et d'applicabilité. En effet, les données issues du retour d'expérience peuvent être

imprécises, incomplètes ou inappropriées. Ce sont des données rarement recueillies d'une seule activité ou d'un seul cas. Par conséquent, il faut être prudent en appliquant ces données à un système spécifique car les conditions de fonctionnement et d'exploitation peuvent être carrément différentes de celles où les données génériques ont été recueillies (Wan, 04). Un autre inconvénient, est l'utilisation directe et inconditionnelle des données, ce qui ne permet pas la reconnaissance des changements dans le système (CCP, 00), (Abr, 02).

Deux autres techniques largement utilisées dans l'analyse et l'évaluation des risques à savoir ; l'AdD et l'AdE sont à citer (Kum, 93), (Man, 05). L'arbre de défaillances est une représentation graphique qui permet de rechercher l'ensemble des événements élémentaires, ou les combinaisons d'événements, qui conduisent à un événement redouté (Fig. I.3). L'objectif est de suivre une logique déductive en partant d'un événement redouté pour déterminer de manière exhaustive l'ensemble de ses causes jusqu'aux plus élémentaires(Lim, 91). Les objectifs de la méthode AdD sont résumés en quatre points (Det, 02):

- La recherche des événements élémentaires, ou leurs combinaisons, qui conduisent à un événement redouté.
- La représentation graphique des liaisons entre les événements. Remarquons qu'il existe une représentation de la logique de défaillance du système pour chaque événement redouté, ce qui implique qu'il y aura autant d'arbres de défaillances à construire que d'événement redouté retenus.
- Analyse qualitative : cette analyse permet de déterminer les faiblesses du système. Elle est faite dans le but de proposer des modifications afin d'améliorer la fiabilité du système. Larecherche des éléments les plus critiques se base sur la détermination des

- chemins qui conduisent à un événement redouté.Ces chemins critiques représentent des scénarios qui sont analysés en fonction des différentes modifications possibles d'apporter au système.

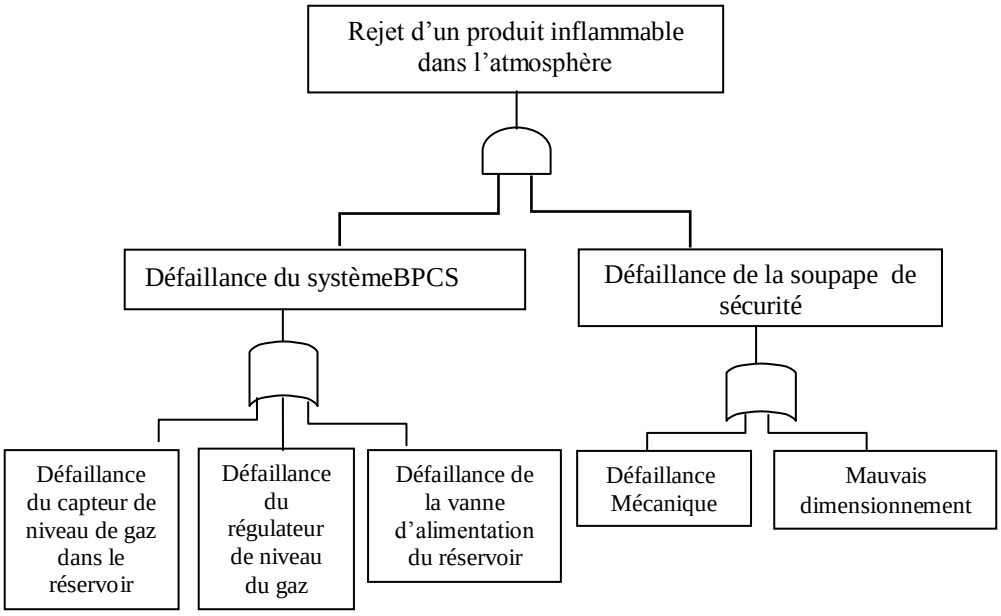


Fig. I.3 : Exemple d'un arbre de défaillances

- Enfin, il est possible d'évaluer la probabilité d'apparition de l'événement redoutéconnaissant la probabilité des événements élémentaires. C'est l'analyse quantitative qui permet de déterminer d'une manière quantitative les caractéristiques de fiabilité du système étudié. L'objectif est en particulier de définir la probabilité d'occurrence des divers événements analysés. Le calcul repose sur les équations logiques tirées de la structure de l'arbre et des probabilités d'occurrence des événements élémentaires.

Les problèmes relatifs à cette technique sont liés aux incertitudes d'exhaustivité et de simplification ainsi que les incertitudes liées aux paramètres du modèle. Par exemple, l'omission des modes de défaillances importants peut conduire à des résultats erronés.

D'autre part, dans l'AdD; les probabilités de défaillance des composants d'un système utilisées pour calculer la probabilité d'occurrence de l'événement redouté, sont considérées comme des valeurs exactes. Ces valeurs, comme déjà expliqué, sont issues du retour d'expérience, de jugement d'experts ou de la combinaison des deux.

Elles sont donc entachées d'incertitudes et devraient être ajustées au système étudié et à ses conditions de fonctionnement et d'exploitation (Tan, 83), (CCP, 00), (Sim, 07).

Le recours aux jugements d'experts présente également une difficulté majeure, notamment lorsque les experts ne s'entendent pas sur un problème donné. Pour surmonter cette difficulté, les analystes ont tendance à faire une agrégation des avis d'experts (Sim, 07). Or cette agrégation est source d'incertitude (CCP, 00), (Abr, 02).

Pour ces raisons, plusieurs approches ont été introduites dans l'analyse par l'AdD dont notamment l'approche floue(Lai, 88), (Nai, 96). Les premiers travaux d'analyse floue par arbres de défaillance sont dus à Tanaka et al (Tan, 83). Dans ces travaux, une nouvelle technique d'analyse basée sur la logique floue, a été proposée. La probabilité d'occurrence de l'événement sommet de l'arbre est calculée en représentant la probabilité d'occurrence des événements de base par des nombres flous trapézoïdaux et en utilisant le principe d'extension de Zadeh (Bou, 03). En 1990 Singer (Sin, 90) a développé un arbre de défaillance en représentant les probabilités d'occurrence des événements de base par des nombres flous du type L-R pour simplifier les opérations arithmétiques floues.

Pour traiter les arbres de défaillance comportant des événements répétés, Soman et Misra (Som, 93) ont proposé une méthode connue sous le nom de l'identité de résolution basée sur la méthode des α-coupes. Sallak et al (Sal, 07) ont proposé une comparaison des deux approches pour évaluer la probabilité d'occurrence de l'événement sommet de l'arbre.La première approche est basée sur les probabilités inférieures et supérieuresdes événements de base et laseconde approche utilise la théorie des ensembles flous. Les auteurs ont introduit également dans ces travaux, deux facteurs d'importance pour mettre en évidence les composants critiques de l'arbre et les composants qui contribuent le plus à l'imprécision entachant le taux de défaillance du système.

I.2.3 Étape d'estimation des conséquences des événements indésirables

Il s'agit de donner une dimension aux conséquences négatives des événements indésirables. Ceci peut être exprimé par le degré du dommage ou blessure, le coût de remise en état d'une installation, le nombre de victimes, etc. Cette évaluation se fait en utilisant la méthode d'arbre des événements (AdE) pour déterminer les résultats possibles d'un événement initiateur donné.

A partir d'un événement initiateur ou d'une défaillance d'origine, l'analyse par AdE permet d'estimer la dérive du système en envisageant de manière systématique le fonctionnement ou la défaillance des barrières de sécurité (Vil, 88) comme montré dans la figure I.4. La probabilité d'occurrence des conséquences indésirables est estimée en multipliant la fréquence d'occurrence de l'événement initiateur par les probabilités de défaillance des barrières de sécurité mises en place pour empêcher le scenario d'accident.

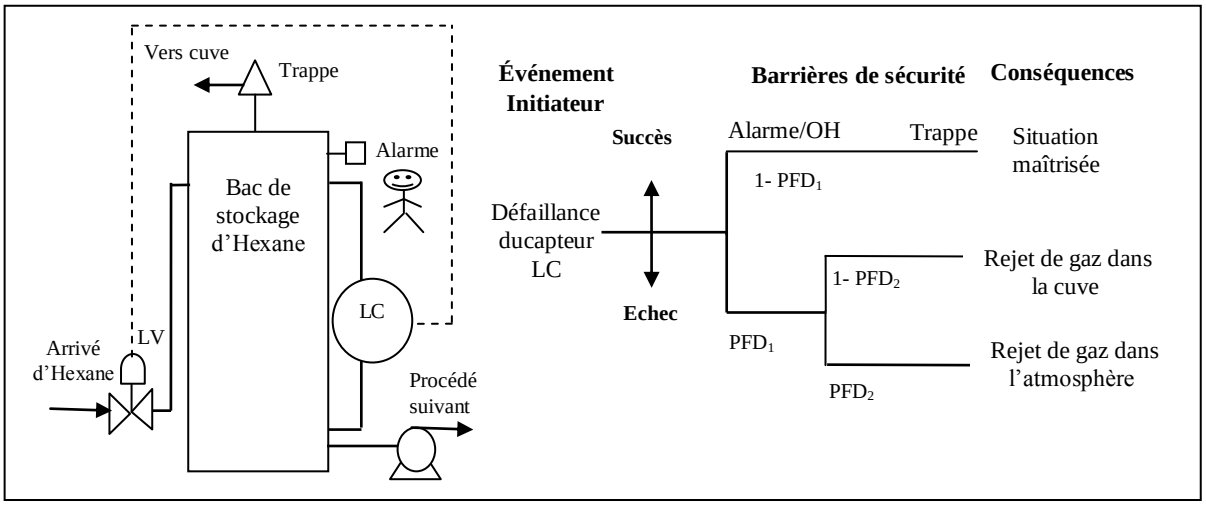


Fig. I.4 : Exemple d'un AdE avec des barrières de sécurité

Le caractère rigoureux d'analyse quantitative exigé par ce modèle, notamment en phase d'estimation de fréquences des événements initiateurs et de probabilités de défaillance des barrières de sécurité, rend les résultats inconsistants (Lai, 88). Ceci revient à l'incertitude et l'imprécision de données utilisées par la méthode. Dans ce contexte, plusieurs travaux basés sur une approche floue (Ras, 91), (Moo, 92), (Hau, 01), (Dum, 02) ont été développés pour surmonter le problème d'incertitude de données utilisées par l'arbre d'événements.

Des modèles physiques sont également utilisés pour estimer les conséquences du risque d'accidents majeurs tels que la dispersion de produits chimiques, la surpression et les effets thermiques causés par les explosions. L'estimation de ces conséquences est entachée d'incertitudes de types stochastiques et épistémiques. En effet, les modèles mathématiques utilisés pour modéliser les phénomènes physiques complexes ne sont qu'une approximation du processus réel, souvent avec des restrictions d'application (Abr, 02).

Bien que ce type d'incertitude soit difficile à quantifier, des tentatives ont été faites pour établir des marges d'incertitudes sur les estimations du modèle en utilisant une approche semi-quantitative. Citons à ce propos les travaux de Markowskiet col (Mar, 11) dans lesquels ils ont développés une approche floue modélisant la fréquence et la gravité des conséquences suivant l'approche classique « Nœud papillon ».Trois systèmes flous, permettant le traitement des incertitudes liées à l'évaluation de la fréquence, la gravité et la criticité du scénario d'accident, ont été proposés.

La fréquence floue est obtenue en appliquant la méthode AdD (arbre des défaillances) à partir des nombres flous des défaillances des d'événements de base suivant la méthode AdD. La représentation floue de ces paramètres d'entrée est faite moyennant les valeurs linguistiques exprimant leurs taux de défaillances à l'aide des nombres flous en utilisant des fonctions triangulaires. Les opérations arithmétiques floues telles que l'addition et la multiplication sont utilisées pour calculer les coupes minimales dans le scenario d'accident. Le résultat étant une fréquence floue du scénario d'accident qui est un nombre flou sous une forme possibiliste triangulaire.

Le deuxième système consiste à estimer et à modéliser la gravité des conséquences du scenario d'accident en prenant en considération les paramètres physiques et environnementaux tels que la température, la pression, la vitesse et la direction de l'air pouvantinfluencer sur la gravité de la conséquence. Les opérations arithmétiques floues sont aussi utilisées selon le modèle BLEVE, le résultat final est un nombre flou avec une distribution triangulaire de possibilité des effets de la conséquence qui correspond au scénario d'accident analysé.

Le troisième système flou, en se basant sur les résultats issus des modèles d'évaluation de la fréquence de la conséquence et de l'effet de la conséquence du scénario d'accident, permet de calculer l'indice de risque flou en multipliant la fréquence floue de la conséquence et la probabilité floue des effets létaux. Notons que cet indice flou de risque est calculé pardes règles floues. Le résultat final est un nombre flou décrivant l'indice de risque que présente le scénario d'accident analysé. L'indice de risque, après défuzzification, sera exploité pour la prise de décision en matière de barrières de sécurité assurant la réduction du

risque.Un facteur flou de correction de l'indice de risque obtenu est ensuite introduit en utilisantles règles d'inférence floues. Ce facteur prendenconsidération lesimprécisions

liées au modèle classique ainsi que les facteurs qui n'ont pas été pris en considération pour estimer les risques.

I.2.4 Étape d'estimation du risque

La dernière étape du processus d'évaluation quantitative des risques a pour but de quantifier le risque en termes de probabilité et de gravité. Plusieurs types de mesures de risque ont été proposés dans la littérature, telles que la mesure du risque individuel, la mesure du risque sociétal, la mesure de l'indice de risque, etc. (CCP, 00), (Hou, 02), (Mar, 10), (Ave, 11). Les incertitudes introduites au cours de cette étape que ce soit dans l'évaluation des probabilités ou des conséquences des scénarios, sont liées (Abr, 02), (Mar, 10) :

- au choix des scénarios majeurs à étudier et qui dépend des jugements d'experts,
- à l'ambigüité dans la définition des scénarios (différentes causes),
- au degré de simplification choisi pour modéliser un scénario (degré de complexité du logiciel utilisé pour modéliser un phénomène),
- au choix des hypothèses dans la modélisation des phénomènes qui requièrent toujours l'intervention du jugement d'expert,
- au niveau de conservatisme ou de prudence propre à chaque expert qui formule généralement des hypothèses plus au moins majorantes, selon son expérience et sa connaissance des phénomènes.

L'incertitude liée à l'estimation du risque est une fonction combinée du degré de finesse du modèle établi par l'analyste selon son expérience et sa connaissance des phénomènes qui lui permettent d'identifier l'ensemble des causes à l'origine des scénarios retenus afin de définir les hypothèses les plus réalistes pour le scénario à modéliser (Abr, 02).

Dans le but d'analyser, traiter et réduire ces incertitudes, différentes méthodes et théories qui prennent en considération la source et le type d'incertitude, ont été développées. Dans la section suivante une brève présentation de ces méthodes.

I.3 Théories de traitement de l'incertitude

I.3.1 Théorie des probabilités

La théorie des probabilités a été développée dans le but de "modéliser" les phénomènes aléatoires, elle constitue le plus ancien formalisme mathématique de la

modélisation des incertitudes à caractère aléatoire, dans un cadre purement probabiliste.

Les distributions probabilistes sont plus appropriées pour représenter les incertitudes aléatoires. Les incertitudes épistémiques, sont également modélisées par des distributions probabilistes mais d'une manière subjective (Dur, 07), (Vas, 11).

Rappelons que cette théorie de mesure fait appel dans son traitement, à des notions abstraites et aléatoires qui dépendent de l'expérience. Le but de cette approche probabiliste est de fournir un cadre alternatif permettant d'affecter, à l'issue de chaque expérience, une valeur numérique ou un nombre (probabilité) permettant de quantifier les résultats d'un très grand nombre d'expériences.

Dans ce qui suit, nous n'aborderons que les concepts de base de la théorie des probabilités. Ensuite, nous abordons ses limites en matière de représentation des incertitudes épistémiques.

I.3.1.1Notion de variable aléatoire, Notion de probabilité

La notion de variable aléatoire est liée à la notion d'expérience, ou de mesure, en supposant que cette expérience (la mesure) soit exprimée par une valeur numérique (probabilité). La notion de probabilité (ou mesure de probabilité), quant à elle, est une mesure positive P définie sur un espace probabilisable (Ω, A) tel que P(Ω)=1, elle est définie comme étant le résultat de l'expérience réalisée. C'est une grandeur numérique par laquelle on exprime le caractère aléatoire d'une variable aléatoire ou d'un événement (possible et non certain). La probabilité d'occurrence de cet événement est décrite par la mesure (Vil, 88) de probabilité par rapport à un ensemble référentiel (Ω) constituant l'ensemble de tous les événements observables possibles (univers). L'application de l'événement A dans l'espace des nombres réels est appelée probabilité de l'événement A [P(A)].

$$P : S(\Omega) \rightarrow [0,1] \qquad \text{(I.2)}$$

Pour tout événement A, sachant que : A ∈ S (Ω) Où S (Ω) est l'ensemble des parties de Ω, on admet que :

- A est impossible si $P(A) = 0$; (I.3)
- A est certain, si $P(A) = 1$; (I.4)
- Pour tout A dans Ω, son complémentaire $\bar{A}$ est dans Ω ;

- $P(\Phi) = 0 \leq P(A) \leq P(\Omega) = 1$ (I.5)

I.3.1.2Propriétés de comptabilité et d'incompatibilité d'évènements

Dans une expérience aléatoire, les événements A et B sont incompatibles (ou disjoints) si et seulement si la réalisation simultanée de A et B est impossible. Autrement dit, lorsqu'ils n'ont aucune éventualité en commun. Ceci implique que l'intersection des sous-ensembles A et B est vide :

$$P(A \cap B) = 0 \quad \text{(I.6)}$$

D'où :

$$P(A \cup B) = P(A) + P(B) \quad \text{(I.7)}$$

Et si les événements$A$ et B sont compatibles, alors on a :

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \quad \text{(I.8)}$$

L'axiome d'additivité (I.7) suppose que, si deux événements sont incompatibles (A∩B = Φ), alors la probabilité qu'au moins l'un d'entre eux ait lieu, est la somme de leurs probabilités individuelles. À noter que les événements A et B de probabilités non nulles ne peuvent être à la fois incompatibles et indépendants.

I.3.1.3Limites de la théorie des probabilités

Comme l'évaluation quantitative des risques traite des événements qui sont généralement rares, les probabilités manipulées ont deux interprétations : fréquentiste et subjectiviste. L'interprétation fréquentiste considère la probabilité d'un événement comme la limite de la fréquence de son occurrence lorsque l'expérience est répétée un grand nombre de fois. Par contre, dans l'interprétation subjectiviste (ou bayésienne), uneprobabilité mesure un degré de croyance ou un état de connaissances qu'un expert accorde à

l'occurrence d'un événement (Zou, 97), donnant ainsi un indicateur qui est manipulé suivant les règles mathématiques des probabilités (Sha, 76).

D'autre part, malgré que cette théorie a été largement utilisée dans l'analyse de risques (Dur, 07), (Vas, 11) et dans la prise en compte du caractère aléatoire inhérent aux phénomènes étudiés, cette approche présente des limites. En effet, toutes les méthodes basées sur l'approche probabiliste supposent que les paramètres d'un composant, comme les taux de défaillance parexemple, ou les probabilités de défaillance sont des variables aléatoires avec des distributions de probabilité connues pour inclure la variation dans les valeurs estimées (Ver, 07).

Cependant, en cas d'insuffisance de données sur les défaillances passées pour des inférences statistiques ou dans le cas où les données montrent une grande variation, il serait très difficile de déduire les distributions de probabilité. Dans ces cas, le recours à d'autres méthodes, telle que les techniques floues et possibilistes est nécessaire(Zad, 79), (Dub, 99b), (Els, 09). Dans cette approche, une fonction d'appartenance décrivant une distribution de possibilité est proposée pour l'analyse de l'incertitude. La fonction d'appartenance peut être obtenue en se basant seulement sur l'information disponible et, si elle est insuffisante, sur des avis d'experts (Gou, 03), (Ver, 07),(Le D, 11).

I.3.2Théorie des ensembles flous

La théorie des ensembles flous a été introduite par le professeur Lotfi Zadeh (Zad, 65) avec l'idée de pouvoir manipuler des informations exprimées en langage naturel. Cet objectif a nécessité d'étendre la théorie des ensembles et la logique propositionnelle classique. L'idée principale est facile à saisir par une comparaison avec la théorie des ensembles classiques. En théorie classique des ensembles, la valeur de vérité d'un énoncé peut être exprimée par la fonction caractéristique μ_A (x), comme suit :

$$\mu_A(x) = \begin{cases} 1 & si\ x \in A \\ 0 & si\ x \notin A \end{cases} \qquad \text{(I.9)}$$

Tandis que, la théorie floue attribue une valeur continue à μ_A avec des valeurs comprises entre 0 et 1, comme suit : *1*

$$\mu_A(x) = \begin{cases} 1 & si\ x \in A \\ 0 & si\ x \notin A \\ \alpha & 0 < \alpha < 1 \end{cases} \quad \text{(I.10)}$$

(appartient totalement)
(n'appartient nullement)
Si x appartient partiellement à A

Le concept d'ensemble classique a été étendu à celui d'ensemble flou grâce à l'idée d'appartenance partielle ou de vérité partielle. Les fonctions d'appartenance semblent être plus logiques et interprétables par un opérateur (Zad, 65), (Kau,77), en offrant unemodélisation souple et représentative de la réalité. La théorie des ensembles flous permet la représentation et le traitement des informations imprécises exprimées par des qualifications en langage naturel (Bou, 95).

Soit un ensemble référentiel U, soit x un élément quelconque de cet ensemble. Un ensemble flou Ã de U est caractérisé par une fonction μÃ(x) qui prend ses valeurs dans l'intervalle [0,1] (Zad, 65). Cette fonction, dite «d'appartenance», donne le «degré d'appartenance» de x à Ã. Un ensemble ordinaire est un cas particulier d'un ensemble flou (μÃ(x) ne prend que 0 ou 1). Formellement, Ã peut s'écrire comme :

$$\tilde{A} = \left\{ (x, \mu_{\tilde{A}}(x)) / x \in U \right\} \quad \text{(I.11)}$$

$$Avec : x \in U, \mu_{\tilde{A}}(x) \in [0,1]$$

À titre d'exemple, on désire classer un groupe d'individus par leurs tailles en définissant la catégorie des petits par une taille inférieure à 1,65 mètre et la catégorie des grands par une taille supérieure à 1,65 mètre.

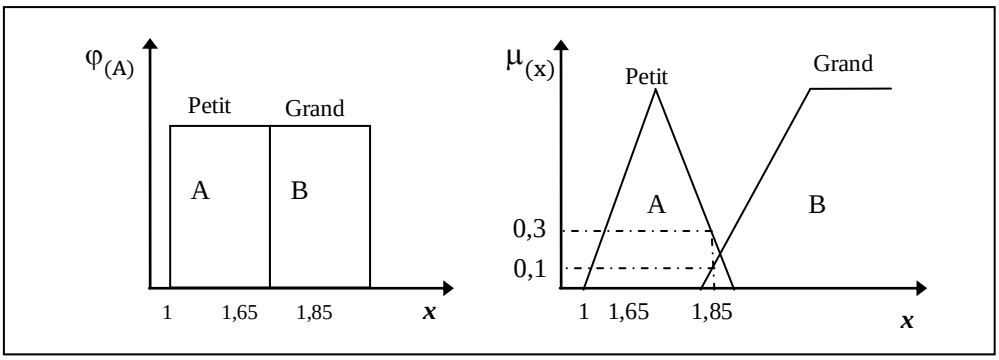


Fig. I.5 : Théorie classique par rapport à la théorie floue

En théorie des ensembles classiques, soient, une variable x (la taille) et un univers de discours U, un individu appartient totalement à un ensemble ou il ne lui appartient pas du

tout.Par contre, en théorie des ensembles flous,un individu de 1,65 mètre appartient à la fois, à l'ensemble grand et à l'ensemble petit mais avec des degrés d'appartenance différents (Fig. I.5).Il est à noter que les ensembles classiques sont considérés comme un cas particulier des ensembles flous.

I.3.2.1 Caractéristiques d'un ensemble flou

- **Support d'un ensemble flou :** Le support d'un ensemble flou noté, Sup(Ã), est défini comme l'ensemble des éléments qui lui appartiennent avec un degré d'appartenance non nul. Formellement:

$$Supp(\tilde{A}) = \{x \in U, \mu_{\tilde{A}}(x) > 0\} \quad \text{(I.12)}$$

- **Hauteur d'un ensemble flou :** La hauteur d'un ensemble flou Ã, notée h(Ã), est représentée par la valeur maximale (le plus fort degré) de sa fonction d'appartenance avec laquelle un élément de U appartient à Ã. Formellement:

$$h(\tilde{A}) = Sup_{x \in U} \mu_{\tilde{A}}(x) \quad \text{(I.13)}$$

Avec : $x \in U$

On dira alors qu'un ensemble flou est normalisé si sa hauteur h(Ã) est égale à 1.

- **Noyau d'un ensemble flou :** Le noyau d'un ensemble flou Ã, noté $Noy(\tilde{A})$ est défini comme l'ensemble de tous les éléments appartenant totalement à Ã (c'est-à-dire pour lesquels $\mu_{\tilde{A}}(x) = 1$). Formellement :

$$Noy(\tilde{A}) = \{x \in U, \mu_{\tilde{A}}(x) = 1\} \quad \text{(I.14)}$$

Les trois dernières propriétés sont illustréespar la figure I.6.

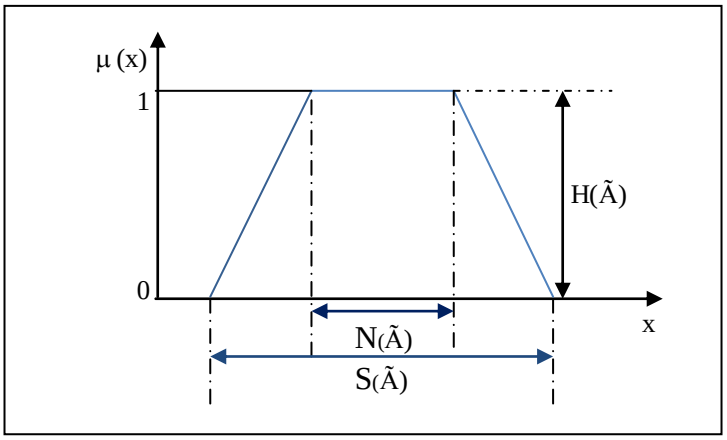


Fig. I.6: Caractéristiques d'un ensemble flou

I.3.2.2 Fonctions d'appartenance

Un ensemble flou peut être défini en lui affectant une fonction continue pour décrire analytiquement ou graphiquement l'appartenance. Ainsi, la représentation des ensembles flous dépend du type de la fonction d'appartenance retenu qui peut être représentée par plusieurs formes. Dans ce contexte, Zadeh a proposé une série de fonctions d'appartenance scindées en deux groupes : les fonctions d'appartenance «linéaires» et les fonctions d'appartenance «courbées» ou de forme «gaussienne ».

Lorsque l'univers du discours est défini par des segments de droite, exemple par des formes triangulaires ou trapézoïdales, cette partition est dite linéaire par morceaux. Ces dernières formes sont souvent utilisées car elles sont simples et comportent des zones où la notion est vraie et des zones où elle est fausse, ce qui rend plus naturelle l'acquisition de l'expertise. Lorsqu'une fonction d'appartenance est partout nulle, sauf en un point, on a un singleton.

- La fonction d'appartenance Triangulaire de la figure (I.7.i) est exprimée comme suit:

$$\begin{aligned} \mu(x) &= \frac{(x-a)}{(m-a)}; a \le x \le m, \\ &= 1; \ x = m, \\ &= \frac{b-x}{b-m}; \ m < x \le b. \end{aligned} \qquad \text{(I.15)}$$

- La fonction d'appartenance Trapézoïdale de la figure (I.7.ii) est exprimée comme suit :

$$\begin{aligned}\mu(x) &= \frac{(x-a)}{(m_1-a)}; a \le x < m_1, \\ &= 1;\ m_1 \le x \le m_2, \\ &= \frac{b-x}{b-m_2};\ m_2 < x \le b.\end{aligned} \tag{I.16}$$

- La fonction d'appartenance Gaussienne de la figure (I.7.iii) est exprimée comme suit :

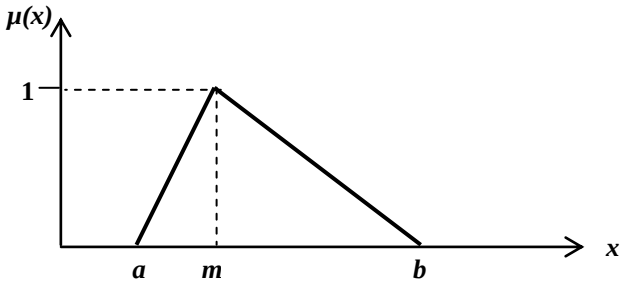
$$\mu(x) = exp\left(\frac{(-x-m)^2}{2\sigma^2}\right). \tag{I.17}$$

- La fonction d'appartenance singleton de la figure (I.7.iv) est exprimée comme suit **:**

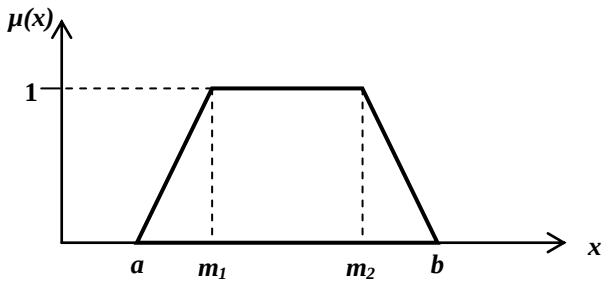
$$\mu(x) = \begin{cases} 1 & x = m \\ 0 & x \neq m \end{cases} \tag{I.18}$$

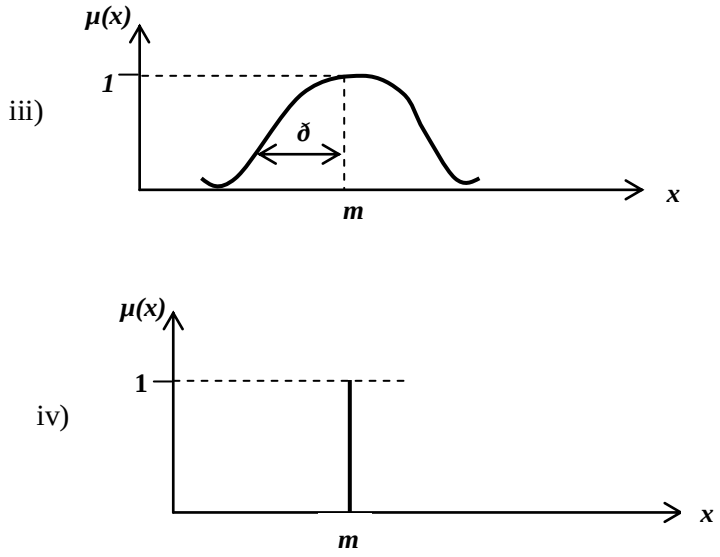
Les fonctions d'appartenance les plus répandues (Bom, 98), (Bil, 00), (Rog, 07) sont illustrées par la figure I.7.

i)



ii)





iii)

iv)

Fig. I.7 : Présentation de quelques fonctions d'appartenance :
i) Triangulaire ;
ii) Trapézoïdale ;
iii) Gaussienne ;
iv) Singleton.

I.3.2.3 Opérations sur les ensembles flous

Les opérations sur les ensembles flous sont généralement équivalentes aux opérations des ensembles classiques. On présente ici les principales opérations couramment utilisées (Kau, 77), (Dub, 00). Considérons les deux ensembles flous $\tilde{A}$ et $\tilde{B}$ définis sur l'univers de discours U ayant respectivement les fonctions d'appartenances $\mu_{\tilde{A}}(x)$ et $\mu_{\tilde{B}}(x)$.

- **Égalité des ensembles flous**

Les deux ensembles flous $\tilde{A}$ et $\tilde{B}$ de l'univers U sont dits égaux, si et seulement si leurs fonctions d'appartenance ont la même valeur en tout point x de U. Formellement, si et seulement si :

$$\tilde{A} = \tilde{B} \Leftrightarrow \forall x \in U, \mu_{\tilde{A}}(x) = \mu_{\tilde{B}}(x) \quad \text{(I.19)}$$

- **Complémentation des ensembles flous**

Le complément d'un ensemble flou $\tilde{A}$ dans un univers U, est un ensemble flou $\tilde{B}$ dont la fonction d'appartenance $\mu_{\tilde{A}}(x) = 1 - \mu_{\tilde{B}}(x)$. Formellement, si et seulement si:

$$\forall x \in U, \mu_{\tilde{A}}(x) = 1 - \mu_{\tilde{B}}(x) \quad \text{(I.20)}$$

- **Union des ensembles flous**

L'union de deux ensembles flous Ã et B̃est un ensemble flou dont la fonction d'appartenance est définie par:

$$\forall x \in X \ , \mu_{\tilde{A} \cup \tilde{B}}(x) = \max(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)) \qquad \text{(I.21)}$$

- **Intersection des ensembles flous**

L'intersection de deux ensembles flous Ã et B̃ de U est un ensemble flou dont la fonction d'appartenance est défini par:

$$\forall x \in U \ , \mu_{\tilde{A} \cap \tilde{B}}(x) = \min(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)) \qquad \text{(I.22)}$$

- **Inclusion des ensembles flous**

Dans un univers U, l'ensemble flou Ã est inclus dans B̃, si et seulement si, pour n'importe quel Élément x de U, x appartient moins à l'ensemble $\tilde{A}$ qu'à l'ensemble $\tilde{B}$. On dit alors que $\tilde{A}$ est inclus dans $\tilde{B}$ ($\tilde{A} \subseteq \tilde{B}$). Alors, $\tilde{A} \subseteq \tilde{B}$ si et seulement si :

$$\tilde{A} \subseteq \tilde{B} \Leftrightarrow \forall x \in U, \mu_{\tilde{A}}(x) \leq \mu_{\tilde{B}}(x) \qquad \text{(I.23)}$$

La figure I.8 illustre les opérations d'intersection, de réunion et de complémentation.

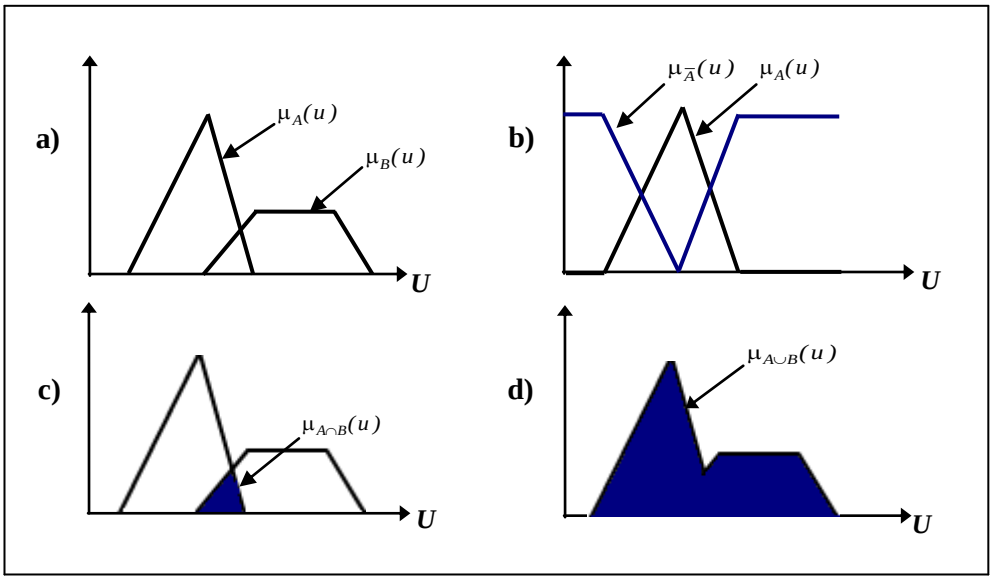


Fig. I.8 : Illustration de quelques opérations sur les ensembles flous:

a) Ensembles flous A et B
b) $\overline{A}$
c) A∩B
d) A∪B.

I.3.2.4 Nombre et intervalle flous

On appelle «nombre flou» tout ensemble flou $\tilde{A}$ du référentiel U, qui satisfait les deux propriétés suivantes (Dub, 88a):

- $\tilde{A}$ est normalisé : il existe au moins une valeur m $\in$ R telle que $\mu_A(m) = 1$;
- $\tilde{A}$ est convexe : $\forall\ (\alpha, \alpha') \in [0, 1]^2 : (\alpha \geq \alpha') \Rightarrow ([m_1 n_1] \leq [m_2 n_2])$.

Ainsi, un nombre flou peut être considéré comme une superposition d'intervalles auxquels correspondent des niveaux $\alpha=\mu_A(x)$ dits niveaux de « présomption »; $\alpha= 1$ étant le « maximum de présomption », il correspond à la valeur m. A mesure que α diminue, les intervalles obtenus s'emboîtent progressivement (emboîtement continu). Un nombre flou permet de modéliser une quantité approximativement égale à m.

Un intervalle flou généralise un nombre flou avec la présence d'un maximum de présomption sous forme d'intervalle (Fig. I.9). La représentation paramétrique d'un intervalle flou s'écrit : $\tilde{A} = (a_1, [a_2, a_3], a_4)$.

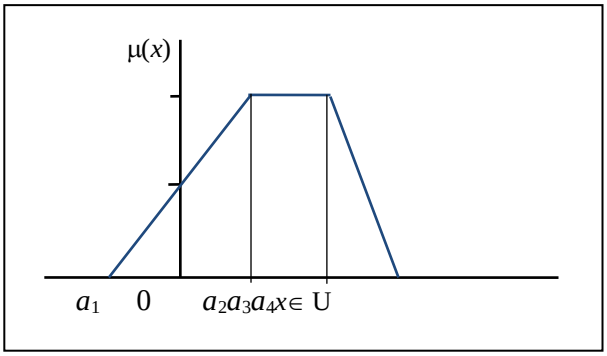


Fig. I.9 : Intervalle flou trapézoïdal

I.3.2.5 Notion d'α-Coupe

Un ensemble flou peut également être décrit comme une collection d'ensembles ordinaires emboîtés grâce à la notion de coupes de niveau α ou α-coupes. La coupe de niveau α de l'ensemble flou Ã est notée $\tilde{A}_\alpha$ (Zad, 75).Les coupes de niveau α établissent un lien naturel entre ensemble flou et ensemble ordinaire et permettent d'exprimer un ensemble flou par des interprétations plus ou moins souples en termes d'α-coupes. Comme mentionné ci-dessus, tout nombre ou intervalle flou Ã proportionne, à un niveau α

donné, un intervalle ordinaire appelé α-Coupe (Mar, 10), (Bou, 03). Une α-Coupe est définie alors comme suit :

$$\tilde{A}_\alpha = \{x \in U, \mu_{\tilde{A}}(x) \geq \alpha\}, \alpha \in [0,1] \quad \text{(I.24)}$$

Ou bien : $\tilde{A}_\alpha = [x_\alpha, y_\alpha]$

Où x_α et y_α sont les projections sur l'axe des abscisses des points appartenant à la courbe $y = \mu_{\tilde{A}}(x)$ et d'ordonnée α; ils représentent respectivement les extrémités gauche et droite de Ã, prises à un niveauα. Pour un nombre flou triangulaire (Fig. I.10), on a :

$$\tilde{A}_\alpha = [(m-\alpha_1)\alpha + \alpha_1, -(\alpha_2 - m)\alpha + \alpha_2] \quad \text{(I.25}$$

Certaines classes de nombres flous sont définies par une représentation paramétrique dite " L−R" afin de faciliter et rendre plus efficace leur manipulation. Un nombre flou du type "L-R", noté $(a^-, a^+, \gamma, \beta)_{LR}$est alors défini de la manière suivante :

$$\mu(x) = \begin{cases} L(\frac{\dot{a} - x}{\gamma}) & si \quad x \leq \dot{a} \\ 1 \quad si \quad a^- \leq x \leq a^+ \\ R(\frac{x - a^+}{\beta}) & si \quad x \geq a^+ \end{cases} \quad \text{(I.26)}$$

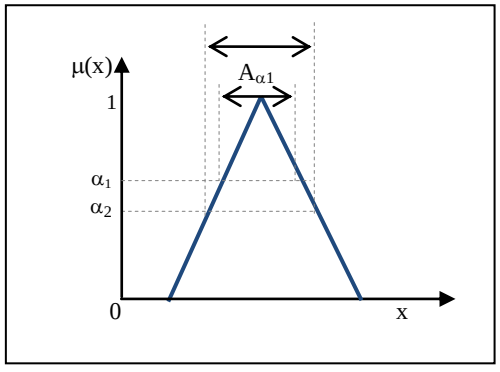


Fig.I.10 : Description d'un ensemble flou triangulaire par ses α-coupes

I.3.2.6 Opérations arithmétiques sur les nombres flous

Les opérations arithmétiques utilisées pour manipuler des nombres ou des intervalles flous requièrent beaucoup de ressources. Cependant, en utilisant la décomposition d'un nombre flou en α-coupes, ces opérations seront largement simplifiées en se réduisant à des opérations sur des intervalles de confiance.

Pour les deux ensembles flous $\tilde{A}$ et $\tilde{B}$ donnés définis par des α-coupes respectives:

$$\tilde{A}_\alpha = \left[A_\alpha^-, A_\alpha^+\right] \subset R^+ et \quad \tilde{B} = \left[B_\alpha^-, B_\alpha^+\right] \subset R^+$$

- Addition $(\tilde{A} + \tilde{B})_\alpha = [\, A_\alpha^- + B_\alpha^- , A_\alpha^+ + B_\alpha^+ \,] , \ \forall \alpha \in [0, 1]$ (I.27)
- Soustraction $(\tilde{A} - \tilde{B})_\alpha = [\, A_\alpha^- - B_\alpha^+ , a_\alpha^+ - b_\alpha^- \,] \ si B_\alpha^+ \leq A_\alpha^- \forall \alpha \in [0, 1]$ (I.28)
- Multiplication $(\tilde{A} \cdot \tilde{B})_\alpha = [\, min\, (A_\alpha^- \cdot B_\alpha^-, A_\alpha^- \cdot B_\alpha^+, A_\alpha^+ \cdot B_\alpha^-, A_\alpha^+ \cdot B_\alpha^+) ,$ (I.29)

  $max\, (A_\alpha^- \cdot B_\alpha^-, A_\alpha^- \cdot B_\alpha^+, A_\alpha^+ \cdot B_\alpha^-, A_\alpha^+ \cdot B_\alpha^+) \,] = [\, A_\alpha^- \cdot B_\alpha^-, A_\alpha^+ \cdot B_\alpha^+ \,] , \ \forall \alpha \in [0, 1]$ (I.30)
- Division $(\tilde{A} / \tilde{B})_\alpha = [\, min\, (A_\alpha^- / B_\alpha^-, A_\alpha^- / B_\alpha^+, A_\alpha^+ / B_\alpha^-, A_\alpha^+ / B_\alpha^+) ,$ (I.31)

  $max\, (A_\alpha^- / B_\alpha^-, A_\alpha^- / B_\alpha^+, A_\alpha^+ / B_\alpha^-, A_\alpha^+ / B_\alpha^+) \,] = [\, A_\alpha^- / B_\alpha^+, A_\alpha^+ / B_\alpha^- \,] , \ \forall \alpha \in [0, 1]$ (I.32)

I.3.2.7 Principe d'extension

Le principe d'extension, proposé à l'origine par Zadeh, est un des outils fondamentaux de la théorie des ensembles flous. Il permet d'étendre une fonction mathématique classique aux ensembles flous. Soit A un sous ensemble flou défini sur X. Le principe d'extension stipule que l'image par f de A, f(A), est un sous ensemble flou de Y dont la fonction d'appartenance est définie par :

$$\mu_B(y) = \sup_{x/y=f(x)} \mu A(x) \qquad \text{(I.33)}$$

La généralisation à des fonctions de plusieurs variables se fait comme suit :

Soit X un produit cartésien de l'univers X = x1, ……xr et soit $\tilde{A}$ 1, $\tilde{A}$ 2, ……, $\tilde{A}$ r, ensembles flous respectivement dans x1, ……xr. Si f est une fonction f de univers X vers l'univers Y, y = f (x1, ……xr), alors l'ensemble flou $\tilde{B}$ dans Y est défini par :

$$\tilde{B} = \left\{ (y, \mu_{\tilde{B}}(y)) \,|\, y = f\left(x_1, \ldots\ldots x_r\right), \left(x_1, \ldots\ldots x_r\right) \in X \right. \qquad \text{(I.34)}$$

I.3.3 Théorie des possibilités

En liaison avec la théorie des ensembles flous, la théorie des possibilités a été introduite par Zadeh (Zad, 78) et développée par Dubois (Dub, 87). La théorie des ensembles flous est considérée comme le cadre le plus adéquat permettant de traiter des données imprécises, alors que la théorie des possibilités offre un moyen de gérer les informations entachées d'incertitudes.

Dans la théorie des possibilités, les concepts des ensembles flous et des fonctions d'appartenance sont interprétés en tant que distributions linguistiques de possibilité (Cay, 96). Au lieu de parler de degrés d'appartenance, on perlera de degrés de possibilité, mais tous les outils et propriétés définis pour les ensembles flous sont également applicables aux distributions de possibilité (Zad, 78), (Dub, 99b).

Quant à la différence entre ces deux théories probabiliste et possibiliste, on s'en tiendra ici à l'exemple illustré par Zadeh (Zad, 78) où il éclaircit pour des degrés de possibilité et de probabilité qu'un faible degré de probabilité n'est pas synonyme d'un faible

degré de possibilité et un fort de degré de possibilité n'implique pas un fort degré de probabilité, seulement on peut dire qu'un degré de possibilité nul implique une probabilité nulle. Cette théorie se voit aussi comme un cas particulier de la théorie de croyances de Dempster-Shafer (Sha, 76) qui est étroitement liée à la théorie des probabilités. Cependant, la théorie des possibilités est liée à celle des ensembles flous.

Ci-après, nous présentons les concepts et définitions de base de la théorie des possibilités.

I.3.3.1 Mesure floue (Valuation)

Dans la théorie de possibilités, une mesure floue peut être de possibilité ou de nécessité. Cette mesure définie une représentation de l'incertitude attribuant des coefficients aux sous-ensembles d'un univers donné U. Chaque coefficient fournit le degré de certitude avec lequel un élément de U appartient à un ensemble flou correspondant. Il s'agit donc d'une application de $\vartheta(x)$ dans [0,1], où $\vartheta(x)$ est l'ensemble des parties de l'univers U qui doit satisfaire les conditions suivantes : cas limites, la monotonie et la continuité (Bou, 03).

- Limites: $\vartheta(\emptyset) = 0$ et $\vartheta(\Omega) = 1$ (I.35)
- Monotonie: ∀ A et B ∈ [0, 1] tels que $A \subseteq B \ alors, \ \vartheta(A) \leqslant \vartheta(B)$ (I.36)
- Continuité: Pour des sous-ensembles emboîtés :

$$A1 \subseteq A2 \ldots \subseteq An \text{ où } An \subseteq An\text{-}1 \ldots \subseteq A1 \quad \text{(I.37)}$$

On a: $\lim_{n\to\infty} \vartheta(An) = \vartheta\ (\lim_{n\to\infty} An)$

I.3.3.2 Mesures de possibilité et de nécessité

L'incertitude d'un événement quelconque, à la différence des probabilités, est donc caractérisée par deux valeurs : sa possibilité (Π) et sa nécessité (N), (Dub, 88a).

- **Mesure de possibilité :** Cette mesure peut être interprétée comme une mesure de la confiance accordée à l'occurrence d'un événement A. Elle permet d'évaluer à quel point la réalisation d'un événement est possible (Zad, 75), (Kau, 77), (Dub, 00), (Bou, 95). Si cet événement est possible de se réaliser, la mesure de possibilité est égale à 1. S'il est impossible de se réaliser, alors sa mesure de possibilité est égale à 0. C'est une fonction prenant ses valeurs dans l'intervalle [0, 1] telle que:

$$\Pi(U) = 1 \quad \text{(I.38)}$$

$$\Pi(\Phi) = 0 \quad \text{(I.39)}$$

Dans le cas de deux événements contraires A et Ā, la possibilité de réalisation de l'un n'implique pas l'impossibilité de réalisation de l'autre. Ceci est traduit par :

$$(MAX\ \Pi(A)\ ,\ \Pi(\bar{A})) = 1 \quad \text{(I.40)}$$

$$\Pi(A) + \Pi(\bar{A}) \geq 1 \quad \text{(I.41)}$$

- **Mesure de nécessité :** L'occurrence d'un événement A est quantifiée par son degré de possibilité avec lequel cet événement est possible mais cette mesure n'est pas suffisante pour décrire complètement l'incertitude existante sur cet événement. La mesure de nécessité donne une information complémentaire à la mesure de possibilité permettant de décrire cette incertitude (Bou, 95).

$$N(A) + N(\bar{A}) \leq 1 \quad \text{(I.42)}$$

I.3.3.3 Relation entre mesures de possibilité et de nécessité

La mesure de nécessité est une mesure duale à celle de possibilité, elle indique avec quel degré la réalisation de l'événement A est certaine. Cette mesure possède des propriétés spécifiques par rapport de celles de la mesure de possibilité. Ces deux degrés (de possibilité et de nécessité) nous permettent de décrire, dans une distribution de possibilité ou de nécessité, à la fois le degré avec lequel l'événement A est susceptible de se réaliser et le degré de certitude qu'on peut attribuer à cette réalisation.

Les deux mesures de possibilité et de nécessité sont liées par les relations suivantes :

$$N(A) = 1 - \Pi(\bar{A}) \quad \text{(I.43)}$$

$$N(A) > 0 \Rightarrow \Pi(A) = 1 \quad \text{(I.44)}$$

$$\Pi(A) < 1 \Rightarrow N(A) = 0 \quad \text{(I.45)}$$

Il en résulte, à partir de ces relations qui décrivent la dualité des deux mesures,que tout événement certain est tout à fait possible et qu'on ne peut avoir la moindre certitude sur un événement qui n'est pas relativement possible. On peut aussi tirer de ces relations qu'il n'est nécessaire de définir une distribution de nécessité et que la distribution de possibilité est largement suffisante pour déterminer une mesure de nécessité (Bou, 95).

Conclusion

La prise en compte des incertitudes dans la démarche d'analyse des risques s'impose en raison des imperfections des modèles et données manipulés. Dans cette partie, nous avons rappelé les différents cadres probabilistes et non probabilistes de représentation et de traitement des incertitudes et des imprécisions à savoir, la théorie des probabilités qui est destinée à traiter les incertitudes d'ordre aléatoire, la théorie des ensembles flous et la théorie des possibilités qui fournissent des outils simples et bien adaptés à la représentation des informations incertaines et imprécises. Nous avons évoqué l'importance de ces théories dans le cadre d'analyse des risques et comment le problème de l'analyse de données incertaines et imprécises en analyse des risques était abordé dans la littérature.

Ces rappels servent comme support de base pour l'évaluation de la criticité des risques moyennant des méthodes appropriées telles que la méthode graphe de risque flou, objet du chapitre suivant.

CHAPITRE II :

Graphe de risque flou pour la détermination du niveau d'intégrité de sécurité

Résumé *: Réduire le risque initial lié à un procédé industriel à un niveau acceptable est généralement atteint en utilisant une combinaison de systèmes relatifs à la sécurité, entre autres, les Systèmes Instrumentés de Sécurité (SIS).L'implémentation de ces derniers nécessite la détermination de leur niveau d'intégrité de sécurité (Safety Integrity Level :SIL). L'objectif de ce chapitre s'inscrit dans ce contexte et consiste à proposer une approche d'évaluation floue du SIL pour le SIS basée sur un système d'inférence floue. Cette proposition est précédée logiquement par des rappels des notions de base relatives à la méthode Graphe de risque, une présentation de l'approche conventionnelle ainsi que ses limites.*

Introduction

L'objectif d'une analyse de risques est de s'assurer que les risques comportant une source potentielle de préjudice, dommage aux propriétés et dégradation de l'environnement, soient suffisamment réduits en abordant toutes les étapes pertinentes du cycle de vie de la sécurité, y compris la conception, la réalisation, l'exploitation et l'entretien jusqu'au déclassement.

Réduire le risque initial à un niveau acceptable est généralement atteint en utilisant une combinaison de systèmes assurant la sécurité, entre autre, les Systèmes Instrumentés de Sécurité (SIS) (Systèmes d'arrêt d'urgence, d'incendie et de gaz,…).

Le SIS, qui représente souvent une partie intégrante du système de gestion de la sécurité (Tim, 04), est un système visant à maintenir le procédé en un état sûr (de sécurité) lorsqu'il se trouve dans une situation comportant un risque réel pour le personnel et l'environnement. Il est constitué d'une ou plusieurs Fonctions Instrumentées de Sécurité (SIF) qui y sont spécifiées pour s'assurer que les risques sont maintenus à un niveau acceptable par rapport à des événements dangereux spécifiques. Ceci est habituellement assuré en effectuant un arrêt partiel ou total du processus afin de prévenir l'événement redouté ou d'en atténuer les conséquences.

Les recommandations en matière de SIF sont abordées dans les normes internationales IEC 61508 (IEC, 98) et IEC 61511 (IEC, 03) qui sont largement reconnues comme étant la base quant aux prescriptions relatives à la spécification, la conception et le fonctionnement des SIS. Chaque SIF est spécifiée en termes d'action à réaliser et de probabilité de défaillance à la demande (PFD) requise. Cette dernière définit le niveau d'intégrité de sécurité (SIL) pour la SIF. Les normes IEC offrent un cadre pour la détermination du SIL et proposent différentes méthodes pour déterminer la PFD(Smi,11).

L'objectif de ce chapitre s'inscrit dans ce contexte et consiste à proposer une approche d'évaluation floue du SIL pour le SIS basée sur un système d'inférence floue. Cette proposition est précédée logiquement par des rappels des notions de base relatives à la méthode Graphe de risque, une présentation de l'approche conventionnelle ainsi que ses limites.

II.1 Notions de base relatives à la méthode Graphe de Risque

II.1.1 Notion de risque

Le risque est défini de nombreuses façons, dans un contexte d'ingénierie, les définitions les plus typiques sont les suivantes:

- Le risque est une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences (Vil, 88),
- Un risque est la combinaison de la probabilité et de la (des) conséquence(s) de la survenue, (OHS, 99),
- Le risque peut être défini par l'association des événements causes et conséquences d'une situation donnée (Gou, 03). Les événements-causes peuvent être caractérisés par leur occurrence (P) et les événements-effets par leur impact (I). La corrélation de ces grandeurs permet de construire un indicateur de risque R = f (occurrence, impact).

Qualitativement, le risque se caractérise par :

- L'ampleur des dommages potentiels causés suite à un événement redouté selon un critère de gravité (critique, marginale, mineure, insignifiante, etc.). Ce critère tient compte de l'appréciation des conséquences en termes de pertes humaines (blessures, mort) ou en termes de pertes économiques (coût liés aux dégradations, etc.) ;
- Le caractère incertain lié à l'apparition d'un événement redouté (fréquent, rare, improbable, etc.) provoquant le dommage à partir d'une situation dangereuse donnée.

II.1.2 Réduction du risque

Le risque inhérent aux opérations d'un processus industriel est souvent considéré comme élevé. En effet, la réglementation, les normes, les textes de lois des compagnies d'assurance et l'opinion publique peuvent exiger un niveau bas ou faible du risque. Ceci amène à la notion de « risque tolérable » (IEC, 98) comme illustré par la figure II.1. La réduction du risque consiste à mettre en œuvre les différentes mesures et barrières de sécurité afin de réduire la probabilité et/ou la gravité des dommages associés à un risque particulier (Kir, 99) et atteindre le risque tolérable (IEC, 98), (Smi, 11). Les mesures de réduction du risque doivent être envisagées et mises en œuvre tant que le risque est jugé

inacceptable. La détermination du risque tolérable pour un événement dangereux donné a pour but d'indiquer ce qui est jugé comme étant raisonnable par rapport à la fréquence de cet événement et ses conséquences (IEC, 98), (Faé, 00).

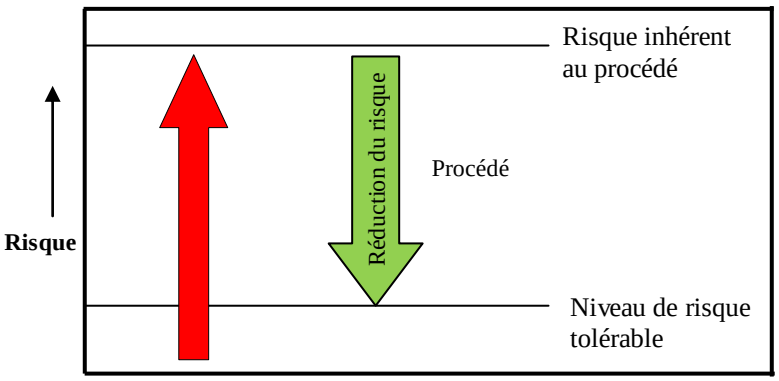


Fig. II.1 :Réduction du risque (Gob, *98)*

La détermination du risque tolérable revient donc, à préciser la fréquence tolérable de l'événement dangereux ainsi que les conséquences tolérables (Gob, 98) :

$$R_t = F * C \qquad \text{(II.1)}$$

Où R_t : est le risque tolérable (ou acceptable),

F : est la fréquence de l'événement dangereux (ou l'accident),

C : est la conséquence de l'événement dangereux (ou l'accident).

II.1.3 Facteur de réduction du risque

Bien que l'estimation du risque inhérent au procédé, à l'instar du risque tolérable, est très difficile à obtenir, l'estimation de la réduction du risque s'est avérée moins compliquée. Cela se fait en utilisant une mesure appelée « facteur de réduction du risque (ΔR) » (Gob, 98), (IEC, 98) défini par:

$$RRF = \Delta R = \frac{F_{np}}{F_t} \qquad \text{(II.2)}$$

Où :

ΔR : est le facteur de réduction du risque,

F_{np} : est la fréquence de l'événement dangereux sans protection,

F_t : est la fréquence tolérable de l'événement dangereux.

A titre d'exemple, quand la fréquence tolérable d'un événement dangereux F_t = 0,02/an et la fréquence de l'événement dangereux sans protection F_{np} = *1/an,* le facteur de réduction du risque *RRF* = 50.

II.1.4 Principe ALARP (As Low As Reasonably Practicable)

Le principe ALARP est un modèle établi par le Health and Safety Executive (HSE, 99), (Mer, 04) qui sert d'outil d'aide à la décision quant à l'évaluation des risques par la considération d'un niveau de risque tolérable. L'utilisation du principe ALARP signifie que le risque devrait être réduit à un niveau aussi bas que raisonnablement possible. Selon ce principe (IEC, 98), (Ave, 11), (Smi, 11), une mesure de réduction des risques devrait être mise en œuvre à condition qu'elle apporte un bénéfice par rapport au niveau d'investissement. On distingue pour cette structure trois niveaux de risque (Fig. II.2):

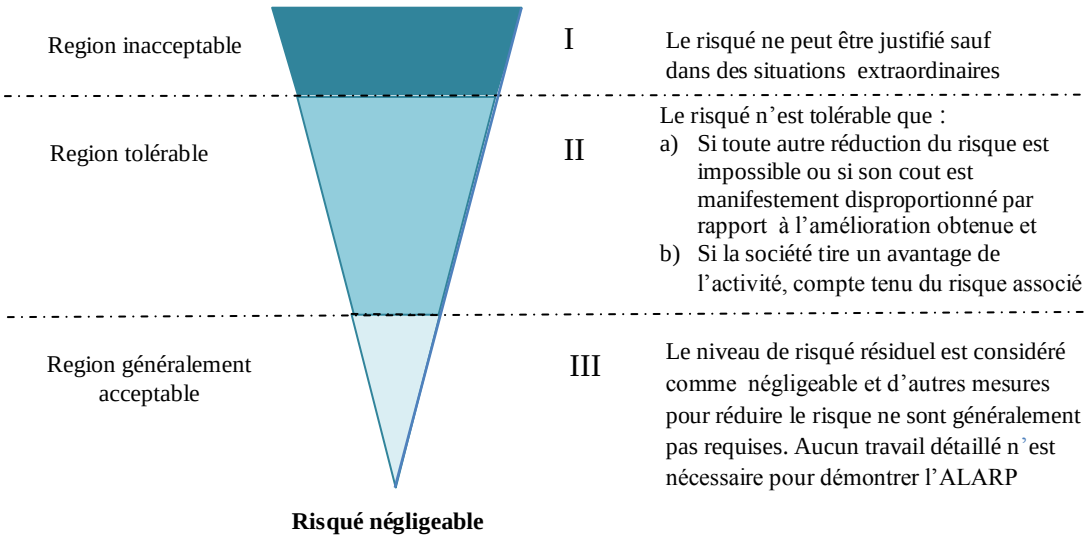


Fig. II.2 : Principe ALARP (IEC, 98)

1. Un niveau supérieur, dans lequel le risque est si élevé qu'il est intolérable (zone I),
2. Un niveau intermédiaire où le principe ALARA s'applique,
3. Un niveau inférieur dans lequel le risque résiduel est si faible qu'il devient négligeable ou encore acceptable sans réduction supplémentaire.

L'application du principe ALARP nécessite la définition d'une échelle de cotation du risque dont chacune des classes correspond à une zone de la structure ALARP (IEC, 98). Les tableaux II.1 et II.2 sont complémentaires, ils représentent respectivement, un exemple de classes de risque et leur correspondance aux zones.

Tableau II.1 : Exemple de classification des risques d'accidents (IEC, 98)

	Gravité			
Probabilité	Conséquence catastrophique	Conséquence critique	Conséquence marginale	Conséquence négligeable
Fortement probable	I	I	I	II
Probable	I	I	II	II
Possible	I	II	II	II
Peu probable	II	II	II	III
Improbable	II	III	III	III
Invraisemblable	II	III	III	III

Note 1 *:Se reporter au tableau II.2 pour l'interprétation des classes de risque I à III.*
Note 2*:Le renseignement réel de ce tableau avec les classes de risque I, II et III dépendra de l application et également de ce que sont effectivement les probabilités : fortement probable, probable, etc. De ce fait, il convient de regarder ce tableau plutôt que comme une spécification destinée àune utilisation ultérieure.*

Tableau II.2 : Relation entre classes et zones de risque (IEC, 98)

Classe de risque	**Interprétation**
Classe I	Risque intolérable
Classe II	Risque indésirable et uniquement tolérable si la réduction du risque est impossible ou si les couts sont manifestement disproportionnés par rapport aux améliorations obtenues.
Classe III	Risque négligeable

II.1.5 Systèmes Instrumentés de Sécurité (SIS)

Un SIS est un ensemble d'éléments permettant d'assurer la mise dans un état sûr lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu, …)(Gob, 05). L'objectif premier assigné à un SIS est la détection dessituations dangereuses (augmentation de température ou de pression, fuite de gaz, …) pouvant mener à un accident (incendie, explosion, rejet d'un produit dangereux, …) pourensuite mettre en œuvre un ensemble de réactions nécessaires à la mise en sécurité, en un temps spécifié, du procédé sous contrôle. Un SIS est constitué de trois sous-systèmes à savoir (Fig. II.3) (Gob, 05):

- ✓ sous-système de détection (capteurs, détecteurs) qui surveillent l'évolution des paramètres décrivant le comportement de l'équipement sous contrôle (EUC) (température, pression, débit, niveau, …).

- ✓ sous-système assurant la mise en œuvre de la logique de sécurité (système électronique programmable, reliage, …) : Unité Logique (LS) constituée d'un ensemble d'éléments logiques (PLC, API) qui reçoit l'information des éléments d'entrées (détection) et active la commande d'un ou plusieurs actionneurs à partir d'une fonction combinatoire des informations délivrées par différents capteurs,
- ✓ sous-système d'action (actionneurs, vannes, moteurs, …) agissant directement (Ex., vanne d'arrêt d'urgence) ou indirectement (Ex., vanne solénoïdes, alarme) pour neutraliser la dérive du système en le mettant dans un état sûr.

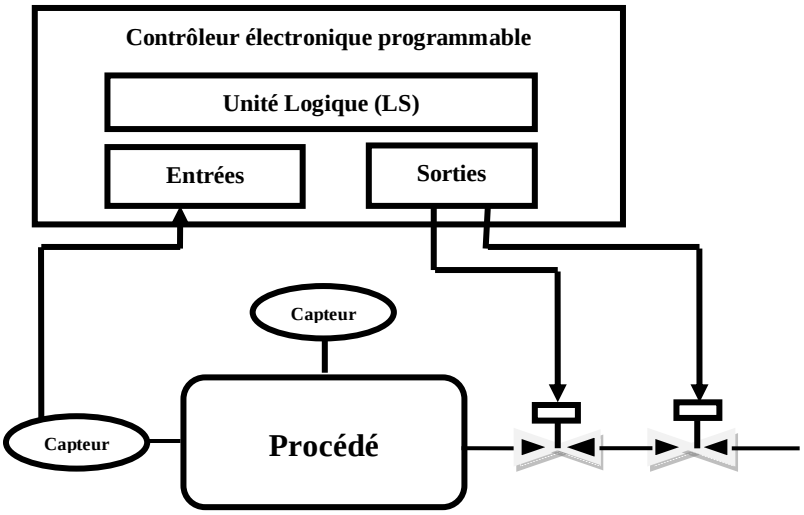


Fig. II.3 : Système Instrumenté de Sécurité (Gob, 98)

Un SIS peut avoir deux modes de fonctionnement :

- Mode de fonctionnement à la sollicitation : On s'intéresse dans ce cas à une activation de moins d'une fois par an et l'indisponibilité du SIS est exprimée par la probabilité de défaillance à la demande (PFD). On peut illustrer ce cas par un système d'arrêt d'urgence qui va commander l'ouverture d'une vanne de sécurité si la pression dans un ballon devient trop élevée.

- Mode de fonctionnement continu :On s'intéresse dans ce cas au taux de défaillance ou à la probabilité de défaillance rapportée à une unité de temps (taux de

défaillance/h ou probabilité/an). Ce cas peut être illustré par le contrôle de la vitesse d'une machine qui doit être maintenue à une vitesse très lente pendant que les opérateurs réalisent une opération de maintenance.

II.1.6 Réduction nécessaire du risque

Dans un procédé industriel, chaque couche de protection apporte une réduction du risque pour atteindre un niveau tolérable ou acceptable. Le modèle de la figure II.4 proposé par les normes IEC 61508-5 (IEC, 98) et IEC 61511-3 (IEC, 03) illustrent cette réduction. La réduction nécessaire du risque est celle qui doit être obtenue pour atteindre le risque tolérable défini au préalable dans une analyse de risques. Le concept de réduction nécessaire est fondamental pour le développement de la spécification des exigences de sécurité pour les systèmes instrumentés de sécurité. Cette réduction peut être obtenue en combinant un ou plusieurs systèmes instrumentés de sécurité et d'autres couches de protection (IEC, 98).

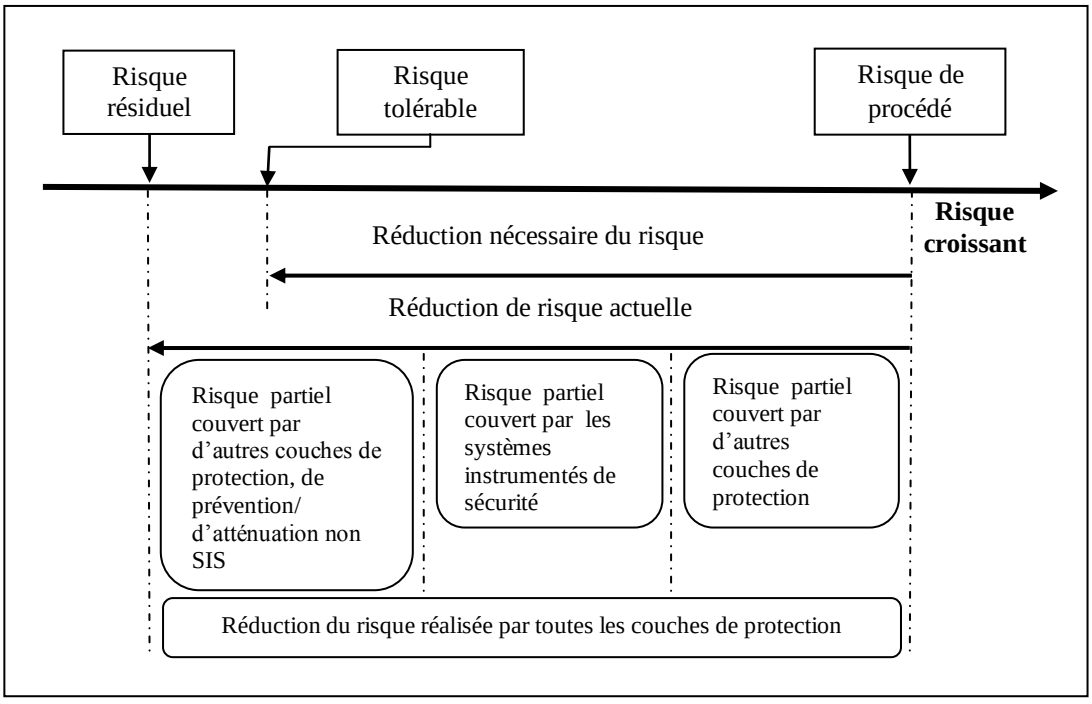


Fig. II.4 : Modèle de réduction du risque (IEC, 98)

II.1.7 Niveau d'Intégrité de Sécurité (SIL)

Les systèmes instrumentés de sécurité constituent donc, un des moyens de réduction du risque. Pour définir le niveau de réduction que doit apporter ou atteindre un SIS, les normes IEC 61508 (IEC, 98) et 61511 (IEC, 03) ont défini le concept du niveau d'intégrité de sécurité SIL (Safety Integrity Level) pour lequel il existe quatre niveaux possibles allant du SIL1 au SIL4, chacun d'eux dépend de la gravité et la fréquence du risque.

Plus le SIL a une valeur élevée, plus la réduction du risque est importante. Par exemple, un SIS de SIL4 apporte une réduction de risque entre 10 000 à 100 000 alors qu'un système de SIL1 comporte un facteur de réduction de risque compris entre 10 à 100 seulement.

Le SIL exigé pour une fonctioninstrumentée de sécurité (SIF) est déterminé en prenant en considération la réduction du risque requise de cette fonction. Selon le mode de fonctionnement d'un SIS, les normes IEC 61508 et IEC 61511ont fixé des exigences quantitatives que doit remplir un SIS afin de maintenir le processus dans un état non dangereux(Gob, 05):

- SIS a un mode de fonctionnement à la sollicitation: Dans ce cas, la mesure de performance appropriée de la fonction de sécurité estsa PFD ou son inverse le facteur de réduction du risque (RRF).
- SIS a un mode de fonctionnement continu : on s'intéresse dans ce cas au taux de défaillance, c'est-à-dire la probabilité de défaillance du SIS rapportée à une unité de temps (PFH).

Le tableau II.3 montre les niveaux du SIL et les exigences probabilistes correspondantes exprimées en termes de PFD moyenne (ou RRF) et PFH (ou RRF).

II.2 Méthodes d'allocation du SIL

La IEC 61508-5 et la IEC 61511-3 décrivent trois types de méthodes d'allocation du SIL requis pour une SIF : qualitatives, semi quantitatives et quantitatives.

Tableau II.3 : Les niveaux du SIL (I EC, 03)

Sollicitations du SIS			
SIL	**Rares PFD**	**Fréquente PFH**	**Facteur de réduction du risque (FRR= 1/PFD)**
4	$10^{-5} \leq PFD < 10^{-4}$	$10^{-9} \leq PFH < 10^{-8}$	$100000 \leq FRR < 10000$
3	$10^{-4} \leq PFD < 10^{-3}$	$10^{-8} \leq PFH < 10^{-7}$	$10000 \leq FRR < 1000$
2	$10^{-3} \leq PFD < 10^{-2}$	$10^{-7} \leq PFH < 10^{-6}$	$1000 \leq FRR < 100$
1	$10^{-2} \leq PFD < 10^{-1}$	$10^{-6} \leq PFH < 10^{-5}$	$100 \leq FRR < 10$

II.2.1 Méthodes qualitatives

Les méthodes qualitatives sont basées sur la vérification de la concordance du niveau de sécurité avec les spécifications des règlements et des normes (Mar, 08). Ces règles font référence à des dispositifs indépendants qui représentent les exigences minimales devant être satisfaites pour atteindre un certain niveau de sécurité acceptable(Dzi, 06). Parmi ces méthodes,le graphe de risque, la matrice de gravité des événements dangereux. Ces méthodes considèrent la contribution des facteurs de risques tels que la criticité de la conséquence, la fréquence des événements dangereux, l'occupation du personnel et la possibilité d'éviter l'événement dangereux (Kir, 05).

II.2.2 Méthodes semi-quantitatives

Les méthodes semi quantitatives permettent de quantifier le risque lié au processus et de déterminer la contribution nécessaire ou exigée du SIS à la réduction du risque (Sim, 07). Ces méthodes sont utilisées pour déterminer la fréquence des événements dangereux qui seront comparées à une fréquence tolérable prédéfinie. Toute insuffisance est exprimée en termes de SIL et cette valeur sera normalement prise en compte pour le développement d'une nouvelle couche de protection (Whi, 06). La méthode la plus répandue est la matrice de risque qui a la particularité de donner le niveau de SIL en fonction de la gravité du risque et de sa fréquence d'occurrence.

II.2.3 Méthodes quantitatives

Il s'agit des méthodes qui permettent de calculer le PFD des SIS à partir des probabilités de défaillances de leurs composants. Parmi les méthodes quantitatives les plus

utilisées, on trouve les équations simplifiées et les arbres de défaillances. La performance ainsi calculée permet de qualifier le niveau SIL du SIS selon les niveaux définis dans les normes IEC 61508 et IEC 61511.

Il convient de noter à ce niveau, que les méthodes qualitatives et semi-qualitatives sont généralement moins coûteuses que les méthodes quantitatives. Elles sont technologiquement moins exigeantes, relativement intuitives pour les opérateurs étant donné qu'elles ne demandent pas de formation qualifiante en évaluation des risques, et ne nécessitent pas un large usage des historiques liés aux données de défaillances comme base d'estimation des probabilités de défaillance.

Le graphe de risque comme méthode qualitative de détermination ou d'allocation du SIL, auquel nous nous intéressons dans le présent chapitre,est relativement facile à appliquer et permet une évaluation rapide des niveaux d'intégrité de sécurité.

II.3 Graphe de risque Conventionnel

Le graphe de risque décrit dans la partie 5 de l'IEC 61508 est l'une des méthodes les plus répandues, il permet de déterminer le SIL d'une SIF à partir de la connaissance des facteurs de risque liés au processus. Il a été largement appliqué en particulier pour déterminer les exigences en termes de SIL pour les fonctions instrumentées de sécurité (Hau, 01), (Kir, 05). Le principe de la méthode graphe de risque a été adopté dans les directives UKOOA concernant le contrôle des processus et des systèmes de sécurité des installations Offshore, et dans d'autres documents publiés par leurs opérateurs sur site (Dea, 99), (Smi, 04).

Le graphe de risque, comme méthode qualitative, peut être décrit comme un arbre de décision dans lequel quatre paramètres de risque, considérés comme suffisamment génériques pour traiter un large éventail d'applications, doivent être combinés pour arriver au SIL requis (IEC, 98). Ces paramètres sont :

- la conséquence de l'événement dangereux (C),
- la fréquence et la durée d'exposition au phénomène dangereux (F),
- la possibilité d'évitement de l'événement dangereux (P) et
- la probabilité d'apparition de l'événement dangereux (W).

Une description de ces paramètres est présentée dans le tableau II.4. Le processus du graphe de risque s'explique de la manière suivante : En combinant les paramètres de risque décrits ci-dessus, on peut développer une courbe de risque comparable à celle présentée dans la figure II.5.

L'utilisation des paramètres C, F et P aboutit à l'une des six sorties X1, X2, ..., X6. Chacune de ces sorties est liée a l'undes trois niveaux de échelles W (W1, W2 et W3). Chaque point d'intersection donne une indication sur le niveau de sécurité nécessaire qui doit être pris en charge par les systèmes E/E/PE (Electrique/Electronique/Electronique Programmable) relatifs à la sécurité du système :

Tableau II.4: Paramètres du risque utilisés par le graphe de risque (IEC, 98)

Paramètre		**Description**
Conséquence	C	Nombre d'accidents mortels et/ou de blessures graves pouvant résulter de l'occurrence de l'événement dangereux. Déterminé en calculant le nombre d'accidents dans la zone exposée lorsque celle-ci est occupée, en tenant compte de sa vulnérabilité à l'événement dangereux.
Occupation	F	Probabilité que la zone exposée soit occupée. Déterminée en calculant la fraction de temps d'occupation de la zone. Il convient de prendre en compte la possibilité d'avoir une probabilité accrue de présence de personnes dans la zone exposée afin de rechercher les situations anormales pouvant exister lors de la progression vers l'événement dangereux.
Possibilité d'éviter l'événement dangereux	P	Probabilité que des personnes exposées puissent éviter la situation de phénomène dangereux qui existe si la fonction instrumentée de sécuritééchoue à la sollicitation. Cela dépend du fait qu'il existe ou pas des moyens indépendants pour alerter les personnes exposées au phénomène dangereux et des issues pour y échapper.
Probabilité d'apparition de l'événement dangereux	W	Nombre de fois par an où l'événement dangereux se produit si aucun système instrumenté de sécurité n'a été adapté. Peut être déterminé en considérant toutes les défaillances pouvant générer l'événement dangereux et en estimant le taux global d'occurrence.

- Les numéros 1, 2, 3 et 4 représentent les quatre SIL,
- La lettre a : indique l'échelon faible sans exigences particulières de sécurité, ce qui correspond à une probabilité de défaillance inférieure à celle indiquée pour le SIL1,
- La lettre b : c'est le point de retour à des situations où, pour des conséquences spécifiques, un seul système de sécurité n'est pas suffisant pour assurer la réduction nécessaire du risque.

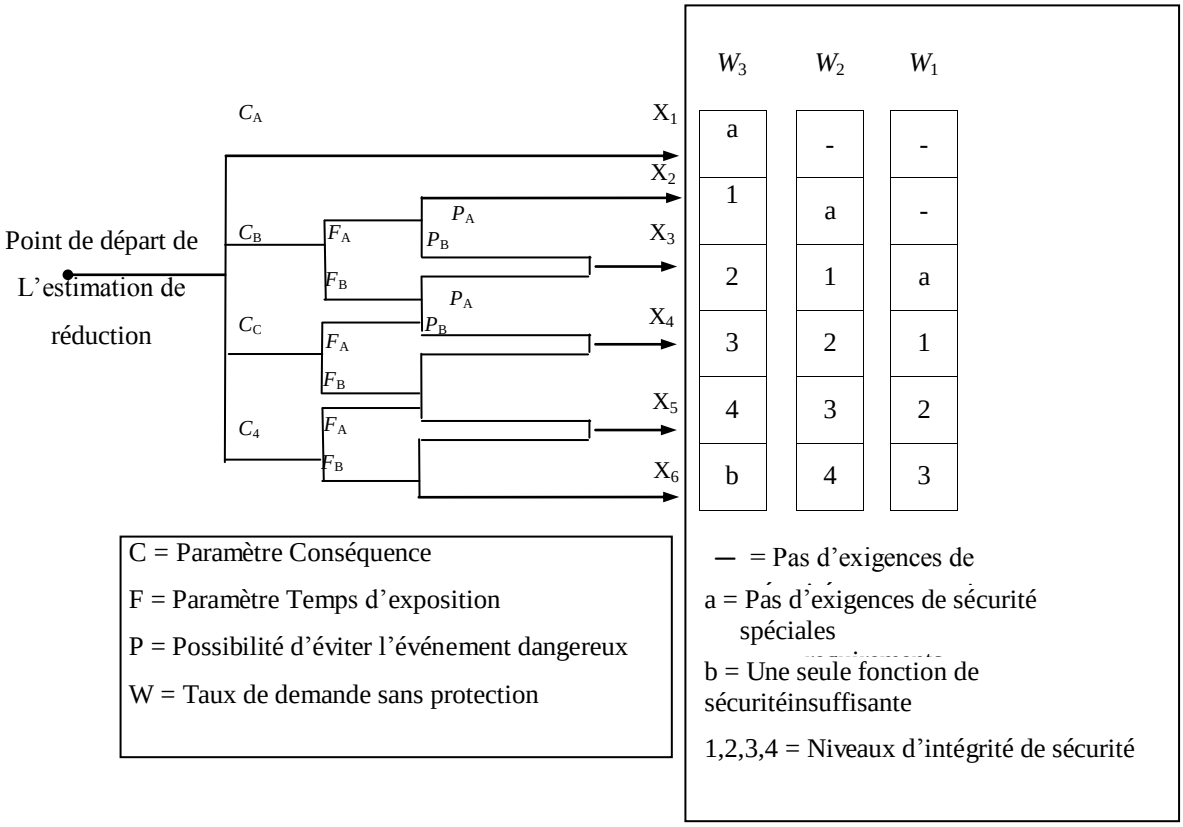


Fig. II.5 : Exemple de graphe de risque (IEC, 98)

Tableau II.5 : Exemple de classification des paramètres du risque(IEC, 98)

ParamètreClassification		
Gravité des conséquences	C_A	Blessure mineure
	C_B	Blessure sérieuse touchant une ou plusieurs personnes, mortel pour une personne
	C_C	Mort de plusieurs personnes
	C_D	Grand nombre de morts
Temps d'exposition (occupation)	F_A F_B	Rare Fréquent
Probabilité d'éviter le phénomène dangereux	P_A P_B	Possible Invraisemblable
Probabilité d'apparition d'un accident	W_1 W_2 W_3	Très faible probabilité Faible probabilité Forte probabilité

II.4 Graphe de risque Étalonné

La robustesse de la méthode graphe de risque repose fortement sur la définition des paramètres C, F, P et W afin d'avoir des résultats représentatifs. L'utilisation de cette méthode, comme toutes les méthodes qualitatives, nécessite un niveau d'expertise suffisant pour pouvoir calibrer les différents paramètres et les adapter au système étudié. Un bon calibrage implique la définition d'une échelle qui ne soit pas trop large pour garantir une précision suffisante dans le choix parmi les critères hiérarchisés C, F et P (IEC, 03).

En ce sens, la norme IEC 61511-Partie 3 (IEC, 03)propose une méthode semi-qualitative qui est le graphe de risque étalonné. Bien que n'étant pas spécifiquement et absolument fixé par la norme, le graphe de risque est habituellement étalonné de sorte que chaque décision diffère de l'autre par un facteur de dix (10^{-1}, 10^{-2}, ...).

La figure II.6 et le tableau II.6 montrent, respectivement, un exemple d'un graphe de risque tel qu'utilisé dans les directives d'UKOOA et les descriptions quantitatives des paramètres de risque (Dea, 99), (Gul, 04), (Smi, 04).

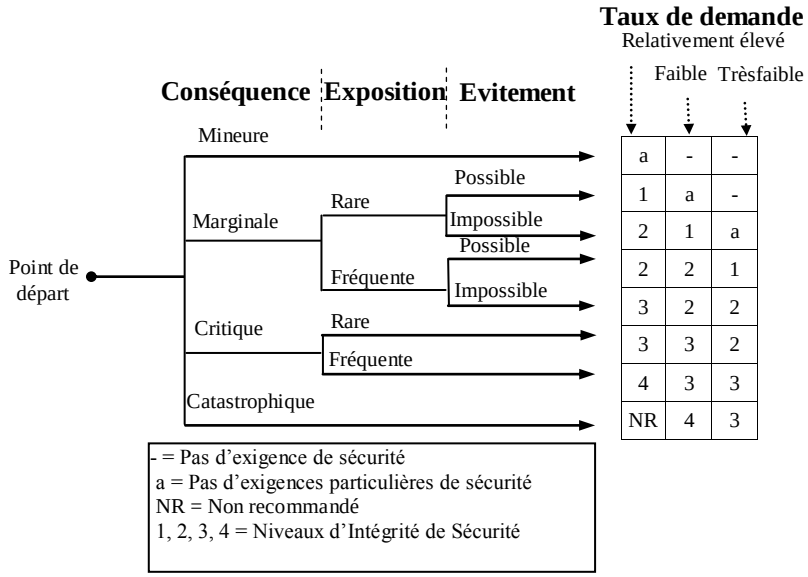


Fig. II.6 : Graphe de risque avec une description qualitative des paramètres

Tableau. II.6: Exemple de définition semi-quantitative des paramètres du risque

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	< 1dans 30 ans ≈<0.03/an
	Faible	1 dans [3, 30] ans ≈ [0.03, 0.3] par an
	Elevé	1 dans [0.3, 3] ans ≈ [0.3,3] par an

II.5 Limites et alternatives

Le graphe de risque, comme méthode qualitative de détermination ou d'allocation du SIL,est relativement facile à appliquer et permet une évaluation rapide des niveaux d'intégrité de sécurité. Cependant, le graphe de risque conventionnel tel que décrit dans la

norme IEC 61508(IEC, 98) est subjectif et sujet à un problème d'interprétation des paramètres du risque. Ainsi, il peut conduire à des résultats incohérents qui peuvent entraîner du conservatisme quant aux valeurs du SIL(Wan, 04). En effet, l'interprétation des termes linguistiques tels que « rare », « possible », « la mort de plusieurs personnes », etc., peut différer d'un évaluateur à un autre (résultat d'un jugement subjectif) ou d'un secteur d'activité à un autre (Red, 98), (Smi, 04), (Kir, 05), (Mar, 07).

Il semble donc nécessaire d'étalonner le graphe et de donner des indications sur la signification des termes linguistiques employés en utilisant des ordres de grandeur via des échelles numériques. Dans le cas contraire, la réduction du risque sera principalement subjective avec des restrictions importantes en matière de prise de décision liée à la sécurité (Kos, 06).

D'autre part, pour atteindre un risque tolérable, la gestion de l'incertitude inhérente aux catégories des paramètres de risque au sein du graphe de risque est problématique(Dea, 99), (Bla, 00),(Gul, 04). Bien que les intervalles comme étant des moyens de caractérisation de l'incertitude font partie acceptable des graphes de risque étalonnés conventionnels, la robustesse exigée (suffisante) dans la valeur du SIL ne peut être atteinte compte tenu de l'ambiguïté de l'information sur laquelle les analystes fondent leur jugement.

Ce type de licitation des connaissances présente deux inconvénients majeurs:

- d'abord, il est en discordance avec le passage progressif d'un intervalle à l'autre bien connu dans les applications du monde réel. En effet, une mesure qui se situe dans un voisinage proche de chacune des frontières précisément définie entre deux intervalles adjacents est prise comme support probant pour un seul d'entre eux en dépit de l'incertitude inévitable impliquée dans le calcul du SIL, c'est à dire que le niveau d'intégrité de sécurité sera plus ou moins le même avec bien sûr des exigences de sécurité différentes.

- Deuxièmement, il ne tient pas compte du fait que dans le raisonnement humain et la formation de l'idée, la décomposition de l'ensemble en deux parties est plutôtfloue que discrète (Mas, 92), (San, 95), (Zad, 79),(Wan, 04). En effet, il y a une incompatibilité entre l'incertitude qui caractérise la perception humaine et le caractère discret du mode

de réponse. Ainsi, nous avons besoin d'une représentation des nombres qui tolère des imprécisions et des connaissances partielles. Les termes linguistiques définis sur des univers numériques et représentés par des ensembles flous, fournissent un outil assez naturel pour les interfaces numériques/symboliques et seraient une alternative très appropriée lorsque l'information disponible est imprécise et/ou incertaine.

En outre, par rapport à C et W, les paramètres F et P n'ont que deux catégories chacun et c'est pourquoi le calibrage sera dominé par les deux premiers paramètres. Comme alternative, Blackmore (Bla, 00) a développé pour un projet Offshore un autre format du graphe de risque en introduisant quatre catégories pour F contre la réduction de ceux de C à deux seulement (blessures ou mort). Ainsi, l'approche proposée a montré une meilleure efficacité dans la détermination du SIL. Pour un meilleur étalonnage, Dean (Dea, 99) a également suggéré l'introduction de catégories supplémentaires pour la conséquence et la fréquence dans certains cas.

Récemment, Baybutt (Bay, 07) a développé un graphe de risque amélioré avec les quatre paramètres suivants: la fréquence de l'événement initiateur, les conditions d'exposition, la probabilité de défaillance des barrières de sécurité et les conséquences de l'événement dangereux. Il a introduit plus de deux niveaux pour les paramètres conséquence et taux de demande, pour maîtriser à la fois le choix conservatif et optimiste qui peut entraîner soit une surestimation ou bien une sous-estimation du SIL.

Une autre alternative proposée par Ormos et Ajtonyi (Orm, 04) concerne l'utilisation d'un système à base de règles floues pour déterminer la valeur du SIL en utilisant la matrice de gravité de l'événement dangereux et la théorie des catastrophes conditionnelles. En l'appliquant à trois sous-systèmes de production de vapeur, les résultats de cette approche, par rapport à ceux fournis par la méthode quantitative (telle que décrite par la norme IEC 61508) ont été très encourageants. Pour deux sous-systèmes le même résultat est obtenu, SIL1 et SIL2 et pour le troisième, le résultat est SIL1 obtenu par l'approche floue contre SIL2 par la méthode quantitative. Cette différence est expliquée par le fait que le paramètre gravité, qualitativement estimée comme faible, n'est pas pris en compte par la méthode quantitative.

De la même façon, Simon et al. (Sim, 07) ont proposé un modèle de graphe de risque à base de règles floues aussi bien qu'une évaluation subjective des paramètres de risque par agrégation de jugements d'experts. L'Affectation du SIL requis est déterminée en considérant le graphe comme un arbre de décision flou. Les paramètres de risque, comme le SIL, sont représentés par des partitions floues avec des descripteurs linguistiques définies sur des échelles de mesure ordinales. L'approche proposée est appliquée à un système test qui est un récipient contenant un liquide volatil inflammable. Une SIF est considérée comme une protection contre la fuite de gaz supérieure au taux admissible qui est de 10^{-4} par an. Chaque paramètre de risque est évalué par l'agrégation des jugements d'experts donnés comme des distributions de possibilité. Le système d'inférence floue fournit, après défuzzification, la valeur du SIL qui est SIL 2.

En se référant à ces travaux, nous tentons dans ce travail de développer un graphe de risque calibré plus flexible en utilisant un système flou, mais avec deux différences principales par rapport aux approches citées:

- Tout d'abord, le problème d'étalonnage est pris en compte et ainsi, les échelles de partitions floues du SIL et les paramètres C, F, P et W sont numériques plutôt qu'ordinales avec les ordres de grandeur donnés par le tableau II.5.

- Deuxièmement, les intervalles flous définis sur l'univers RRF permettent notamment à la valeur du SIL d'être comprise entre deux classes successives avec des degrés d'appartenancedifférents. En pratique, lorsque les données sur la disponibilité pour une SIF indiquent une exigence «juste entre» deux classes de SIL, généralement la plus stricte exigence en matière de SIL est choisie (Hau, 01).

II.6 Systèmes d'inférence floue

Les systèmes d'inférence floue ont connu de nombreuses applications dans des domaines tels que le contrôle automatique, la classification de données, l'analyse de décision, les systèmes experts, l'ingénierie de fiabilité et la sécurité des systèmes.

L'importance des règles floues réside dans le fait que la connaissance et l'expérience humaine peuvent, souvent, être représentées par ce type de règles (Sha, 05), (Siv, 07). Etant donné que les règles floues sont linguistiques plutôt que numérique,

associant les paramètres du risque (dans la prémisse) avec la valeur du risque (dans la conclusion), elles fournissent une structure naturelle pour exprimer ce type de connaissances. Ainsi, les experts trouvent souvent, les règles floues comme la manière la plus convenable pour exprimer leurs connaissances sur une situation donnée.

Parmi ces systèmes d'inférence, le contrôleur flou proposé par Mamdani et Assilian (Mam, 75) qui est le plus rencontré dans la résolution des problèmes à base de règles floues. C'est le premier modèle de réalisation dédié à la commande d'un moteur à vapeur par la synthèse d'un ensemble de règles floues fournies par expérience des opérateurs humains(Rog, 07). Basé sur une technique simple utilisant l'inférence min-max, la méthode de Mamdani a été appliquée avec succès dans de nombreux domaines allant du contrôle de processus jusqu'au diagnostic médical(Siv, 07). Les détails spécifiques de chaque étape de cette méthode sont expliqués brièvement ci-dessous (Dub, 99b).

Soit une base de règles floues constituée de n règles SI-ALORS avec plusieurs entrées et une seule sortie. Chaque règle $R_i (i = 1,...,n)$ est donc de la forme:

$$R_i : \text{SI } X_1 \text{ est } A_{i1} \text{ et } ... \text{ et } X_m \text{ est } A_{im} \text{ ALORS } \quad Y \text{ est } B_i \qquad \text{(II.3)}$$

Où X_j's $j = 1, ..., m$, et Y sont des variables linguistiques définies respectivement sur les univers $u^0 = \left(u_1^0, ..., u_m^0\right)$ et V. Les ensembles flous A_{ij} sont des éléments d'une partition linguistique $T_j \text{ de } U_j$ (univers de la variable X_j).

Pour un vecteur d'entrée discret $u^0 = \left(u_1^0, ..., u_m^0\right)$, la valeur de sortie est déterminée par la méthode à trois étapes suivante :

II.6.1 Fuzzification

La fuzzification des variables est une étape importante dont dépend la performance d'un système flou. Elle consiste à spécifier, pour une valeur réelle d'entrée, un degré d'appartenance aux ensembles flous. Les caractéristiques de cette étape sont habituellement déterminées par des experts ou des opérateurs qualifiés travaillant sur le processus (Fla, 94). Les étapes de la fuzzification sont:

1. L'établissement des variables linguistiques ;
2. L'établissement des quantificateurs flous (nombre de valeurs linguistiques) ;

3. L'attribution d'une signification numérique à chaque quantificateur flou : fonction d'appartenance.

C'est le processus de conversion d'une donnée d'entrée u_j^0 en sa représentation symbolique, c'est à dire un ensemble flou $A_{i_j}^*$ en utilisant la partition floue $T_j \text{ de } U_j$, en calculant le degré d'appartenance $\mu_{A_j}(u_j^0)$ de u_j^0 pour chaque A_{ij}. Puis, un degré de concordance $\alpha_i = \min_j \mu_{A_j}(u_j^0)$ est calculé pour chaque règle R_i.

II.6.2 Inférence floue

Le processus d'obtention de la sortie floue à l'aide de la méthode d'inférence max-min est constitué des sous-étapes suivantes (Rog, 07):

• **Trouver le niveau d'activation de chaque règle :** La valeur de vérité de la prémisse de chaque règle est calculée et appliquée à la partie de conclusion de cette règle. Le niveau d'activation de la règle est calculé comme suit:

$$\alpha_i = \min_j \mu_{A_{ij}}\left(u_j^0\right) \qquad \text{(II.4)}$$

Si la prémisse d'une règle a un degré de vérité non nul, c'est à dire lorsque l'entrée correspond partiellement à la prémisse de la règle, la règle est activée.

• **Inférencement :** Dans l'étape de déduction, la sortie B_i' de chaque règle R_i est calculée à l'aide d'un opérateur de conjonction (min). Ensuite, $B_i' = \alpha_i \wedge B_i$ est donnée par:

$$\mu_{B_i'}(v) = min\left(\alpha_i, \mu_{B_i}(v)\right) \qquad \text{(II.5)}$$

• **Agrégation:** Pour obtenir la sortie globale du système, toutes les règles individuelles de sortie sont combinées en utilisant l'opérateur d'union. Ainsi, $B' = \bigcup_i B_i' = \bigcup_i \alpha_i \wedge B_i$

Avec comme fonction d'appartenance:

$$\mu_{B'}(v) = max_{i=1,\ldots,n}\ \mu_{B_i'}(v) \qquad \text{(II.6)}$$

II.6.3 Défuzzification

L'étape de défuzzification permet de transformer la sortie floue en une valeur représentative v^0 de Y dans B'. Parmi les méthodes de défuzzification (Run, 97), le centre de gravité est la méthode la plus couramment utilisée. Selon cette dernière, la valeur représentative est donnée par :

$$v^0 = \frac{\int_{v \in V} \mu_{B'}(v).v.dv}{\int_{v \in V} \mu_{B'}(v).dv} \qquad \text{(II.7)}$$

II.7 Graphe de Risque Flou : Modèle d'évaluation floue d'intégrité de sécurité

La logique floue est un outil puissant de modélisation du comportement des systèmes qui sont trop complexes ou trop mal définis pour admettre des techniques quantitatives classiques ou lorsque les informations disponibles sur le système sont de nature qualitative, imprécise et/ou incertaine (Zad, 79), (Mar, 10). Contrairement aux systèmes logiques classiques, la logique floue vise à modéliser les modes de raisonnement imprécis qui jouent un rôle essentiel dans la capacité de l'homme de donner des jugements ou de prendre des décisions dans un contexte d'incertitude et d'imprécision (Zad, 73), (Kli, 04), (Mur, 09).

Comme mentionné auparavant et compte tenu des insuffisances constatées sur le graphe de risque conventionnel,un graphe de risque flou est développé pour la prise en charge de ces difficultés. Le modèle proposé tente d'améliorer le graphe de risque conventionnel en le décrivant par un système d'inférence floue. La figure II.7 montre l'ensemble de la procédure d'évaluation floue de l'intégrité de sécurité.

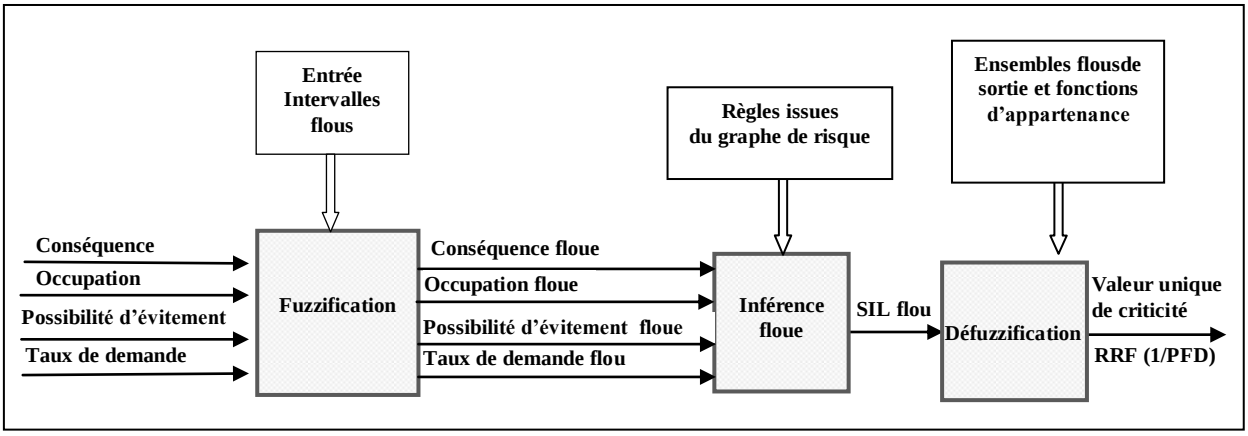


Fig. II.7 : Procédure globale d'évaluation du SIL à base de règles floues

Le modèle utilise des partitions floues pour décrire les paramètres du risque et les niveaux de SIL. Les fonctions d'appartenance sont déterminées par une opération de fuzzification (Zad, 79) des données relatives aux paramètres du graphe de risque calibré. Ainsi, les intervalles discrets sont remplacés par des intervalles flous avec des fonctions d'appartenance trapézoïdales. L'idée principale de cette transformation est de considérer les limites d'un intervalle ordinaire comme une valeur moyenne d'un nombre flou sous la forme d'espérance supérieure et inférieure (Dub, 87).

La mise en œuvre de la procédure d'évaluation du SIL à base de règles floues se fait selon trois grands modules:

- Le premier module traite les entrées du système (valeurs de C, F, P et de W). On définit tout d'abord un univers de discours, un partitionnement de cet univers en classes pour chaque entrée et des fonctions d'appartenance pour chacune de ces entrées. La première étape, appelée fuzzification, consiste à attribuer à chaque entrée sa fonction d'appartenance à chacune des classes préalablement définies, donc à transformer l'entrée réelle en un ensemble flou.

- Le deuxième module est constitué d'une base de règles et d'un moteur d'inférence permettant le calcul; il consiste en l'application de règles.
- Le troisième module décrit l'étape de défuzzification qui permet de passer d'un degré d'appartenance du SIL relatif au scénario à la détermination de la valeur précise à donner à ce SIL.

Les détails concernant les différentes étapes du modèle flou proposé sont présentés ci-dessous.

II.7.1 Sélection de variables d'entrée

En se référant aux normes IEC 61508 et IEC 61511, le système à base de règles floues associé au graphe de risque conventionnel considère les quatre paramètres de risque C, F, P et W comme variables d'entrée et le RRF comme l'unique variable de sortie. Les paramètres C, F, P et W permettent une graduation significative des risques et contiennent les principaux facteurs d'évaluation des risques. Évidemment, d'autres facteurs ou conditions

pourraient être envisagées, mais avec un nombre réduit parce que deux inconvénients majeurs peuvent apparaître: d'abord, plus le nombre de paramètres est élevé, plus des SIL supplémentaires devraient être nécessairement ajoutés, mais certainement sans exigences spécifiques. Deuxièmement, des variables d'entrée supplémentaires ne permettent pas au système flou d'avoir une taille raisonnable et peuvent rendre compliqué le test du modèle.

II.7.2 Développement des échelles floues

La logique floue utilise le concept de variable linguistique pour décrire la prémisse et la conclusion d'une règle floue (Zad, 75). Ce concept offre un outil de caractérisation approximative des situations qui sont trop complexes ou trop mal définies pour l'application des techniques classiques quantitatives. Une variable linguistique diffère d'une variable numérique en ce que ses valeurs ne sont pas des numéros mais des mots dans une langue naturelle(Bou, 03). Les ensembles flous, avec leurs limites pas nettement définis, représentent les valeurs de la variable linguistique et peuvent être considérés comme résumant les différentes sous-classes des éléments dans un univers de discours.

Rappelons que les ensembles flous considérés pour la description des paramètres C, F, P et W et le RRF sont issus des partitions discrètes correspondantes en se référant à un

modèle éprouvé ; le graphe risque calibré présenté dans la figure II.6. La transformation d'un intervalle ordinaire en un intervalle flou peut être considérée comme le problème inverse de la détermination de la valeur moyenne d'un intervalle flou. Toutefois, conformément à la définition bien connue de l'espérance dans la théorie des probabilités, Dubois et Prade (Dub, 87) ont proposé une définition pertinente de la valeur moyenne d'un intervalle flou comme suit: "la valeur moyenne d'un intervalle flou Q est un intervalle fermé délimité par les espérances mathématiques calculées à partir de fonctions de répartition supérieure et inférieure ", c'est-à-dire :

$$E(Q) = \left[E_*(Q),\ E^*(Q)\right] \qquad \text{(II.8)}$$

Où : $E_*(Q) = inf\ E(Q) = \int_{-\infty}^{+\infty} u\, dF^*(u)$ (II.9)

$$E^*(Q) = \sup E(Q) = \int_{-\infty}^{+\infty} u\, dF_*(u) \qquad \text{(II.10)}$$

F_* et F^* sont respectivement les fonctions de distribution supérieure et inférieure de P qui appartient à l'ensemble des mesures de probabilité P(Q),définie sur le support de Q. Soit Q un intervalle flou avec une fonction d'appartenance trapézoïdale μ_Q, et soient $S(Q)=[s_-, s_+]$et $C(Q)=[q_-, q_+]$respectivement, le support et le noyau de Q ; c'est-à-dire $\mu_{S(Q)}(u)>0$ et $\mu_{C(Q)}(u)=1$. Soient α et β respectivement, les écarts gauche et droit.

Sous la condition de :

$$\lim_{u\to-\infty} u^k F(u) = \lim_{u\to+\infty} u^k (1-F(u)) = 0 \ , \ k\geq 1,$$

il s'ensuit que :

$$E_*(Q) = \int_0^{+\infty} (1-F^*(u))du - \int_{-\infty}^{0} F^*(u)du = q_- - \int_{-\infty}^{q_-} \mu_Q(u)du \qquad \text{(II.11)}$$

$$E^*(Q) = \int_0^{+\infty} (1-F_*(u))du - \int_{-\infty}^{0} F_*(u)du = q_+ + \int_{q_+}^{+\infty} \mu_Q(u)du \qquad \text{(II.12)}$$

Le calcul de $E_*(Q)$ est comme suit (voir figure II.8) :

$$\begin{aligned} E_*(Q) &= q_- - \int_{-\infty}^{q_-} \mu_Q(u)du \\ &= q_- - \int_{-\infty}^{q_-} \left(1-\frac{q_- - u}{\alpha}\right)du \\ &= q_- - \int_{s_-}^{q_-} \left(1-\frac{q_- - u}{\alpha}\right)du \\ &= q_- - \left[\left(1-\frac{q_-}{\alpha}\right)u + \frac{u^2}{2\alpha}\right]_{s_-}^{q_-} \\ &= q_- - \frac{\alpha}{2} \end{aligned}$$

Ainsi,

Et $$E_*(Q) = q_- - \frac{\alpha}{2} \qquad \text{(II.13)}$$

$$E^*(Q) = q_+ + \frac{\beta}{2} \qquad \text{(II.14)}$$

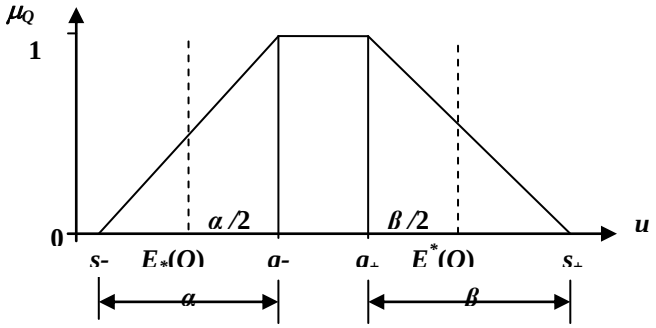


Fig. II.8 : Valeurs moyennes inférieure et supérieure de Q

Ces résultats sont en concordance avec le fait que la largeur de la valeur moyenne est une fonction linéaire des étalements α et β (Dub, 87). Dans notre cas, étant donné E_* et q_- (resp. E^* et q_+) d'un intervalle flou inconnu Q, α (resp.β) sera déterminée en utilisant l'équation II.12 (resp. l'équation II.13). E_* et E^*, comme valeurs moyennes, sont données par les bornes des intervalles précis. Le calcul de α et β se fait comme suit: d'abord on calcule la valeur moyenne m de l'intervalle $[E_*, E^*]$. Ensuite, les bornes q^- et q^+ du noyau en utilisant respectivement, la valeur moyenne des subdivisions [E*, m] et [m, E*]. Selon que l'univers de l'échelle soit, ou non, linéaire, la moyenne arithmétique ou la moyenne géométrique est utilisée à la fois pour calculer m, q^- et q^+. La figure II.9 illustre la transformation d'un intervalle ordinaire en un intervalle flou sur une échelle linéaire.A titre d'exemple, α et s- sont déterminés comme suit:

$$\begin{aligned}\alpha &= 2(q_- - E_*) = 2\left(\frac{E_* + m}{2} - E_*\right)\\ &= m - E_* = \frac{E_* + E^*}{2} - E_* \\ &= \frac{E^* - E_*}{2},\\ s_- &= q_- - \alpha.\end{aligned} \qquad \text{(II.15)}$$

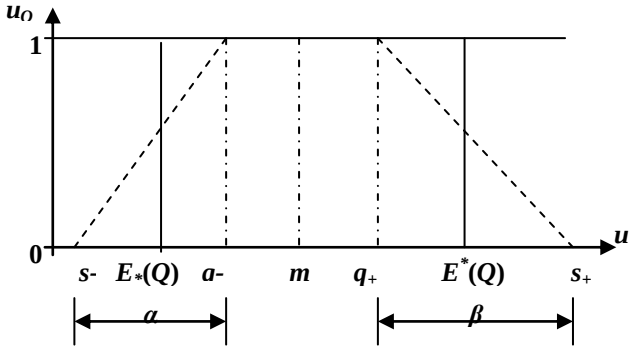


Fig. II.9 : Transformation d'un intervalle ordinaire en un intervalle flou.

Les ensembles flous extrêmes contenus dans la partition linguistique sont générés par la même transformation tout en supposant des étalements infinis, c'est-à-dire en prenant $\alpha = -\infty$, $\mu Q_{eg}(u)=1$ pour $u \leq q-$ et $\beta=+\infty$, $\mu Q_{ed}(u)=1$ pour $u \geq q+$ (eg et ed sont respectivement, l'extrême gauche et l'extrême droite).

En outre, transformer une partition ordinaire (discrète) irrégulière en une partition floue peut entraîner des libellés linguistiques avec des valeurs insignifiantes (problème d'incompatibilité). Dans ce cas, la pente de ces ensembles flous doit d'être raisonnablement modifiée.

Le tableau II.7 montre les résultats numériques des différentes transformations. A titre d'illustration, la transformation concernant le paramètre "Conséquence" est donnée par la figure II.10.

II.7.3 Définition des échelles des paramètres C, F, P, W et du SIL

Une définition qualitative et quantitative des paramètres C, F, P et W est donnée par le tableau II.6. Le graphe de risque utilisé pour déterminer le SIL en vue de maitriser les scenarios d'accident identifiés est celui proposé dans les directives d'UKOOA et représenté par la figure II.6.

Tableau II.7: Transformation des intervalles ordinaires en intervalles flous

Indices de transformation	**Valeur moyenne inférieure**	**Valeur moyenne supérieure**	**Moyenne géométrique de $[E_*, E^*]$**	**Borne inférieure du noyau $N(Q)$**	**Borne supérieure du noyau $N(Q)$**	**Étalement gauche de Q**	**Étalement droit de Q**	**Borne inférieure du support $S(Q)$**	**Valeur modifiée de S_-**	**Borne supérieure du support $S(Q)$**	**Valeur modifiée de S_+**
Symboles	E_*	E^*	m	q_-	q_-	α	β	S_-	S_-^*	S_+	S_+^*
Conséquence											
Mineure	1.0E-09	1.0E-07	1.0E-08	3.162E-09	3.162E-08	4.325E-09	1.368E-07	-1.162E-09	1.0E-09	1.684E-07	-
Modérée	0.01	0.1	3.162E-02	1.778E-02	5.623E-02	1.557E-02	8.753E-02	2.217E-03	-	1.438E-01	-
Critique	0.1	1	3.162E-01	1.778E-01	5.623E-01	1.557E-01	8.753E-01	2.217E-02	-	1.438E+00	-
Catastrophique	1	10	3.162E+00	1.778E+00	5.623E+00	1.557E+00	8.753E+00	2.217E-01	-	1.438E+01	10
Exposition											
Rare	0	10	5.0E+00	2.50E+00	7.50E+00	5.0E+00	5.0E+00	-2.50E+00	0	1.250E+01	-
Fréquente	10	100	5.50E+01	3.250E+01	7.750E+01	4.50E+01	4.50E+01	-1.250E+01	7.50E+00	1.225E+02	100
Evitement											
Impossible	0	90	4.50E+01	2.250E+01	6.750E+01	4.50E+01	4.50E+01	-2.250E+01	0	1.125E+02	9.250E+01
Possible	90	100	9.50E+01	9.250E+01	9.750E+01	5.0E+00	5.0E+00	8.750E+01	-	1.025E+02	100
Taux de demande											
Très faible	1.0E-05	0.03	5.477E-04	7.401E-05	4.054E-03	1.280E-04	5.189E-02	-5.401E-05	1.0E-05	5.595E-02	-
Faible	0.03	0.3	9.487E-02	5.335E-02	1.687E-01	4.670E-02	2.626E-01	6.652E-03	-	4.313E-01	-
Relativement élevé	0.3	1	5.477E-01	4.054E-01	7.401E-01	2.107E-01	5.198E-01	1.946E-01	-	1.260E+00	1
SIL (RRF=1/ PFD)											
NSSR (a)	1	10	3.162E+00	1.778E+00	5.623E+00	1.557E+00	8.753E+00	2.217E-01	1	1.438E+01	-
SIL 1	10	100	3.162E+01	1.778E+01	5.623E+01	1.557E+01	8.753E+01	2.217E+00	-	1.438E+02	-
SIL 2	1.0E+02	1.0E+03	3.162E+02	1.778E+02	5.623E+02	1.557E+02	8.753E+02	2.217E+01	-	1.438E+03	-
SIL 3	1.0E+03	1.0E+04	3.162E+03	1.778E+03	5.623E+03	1.557E+03	8.753E+03	2.217E+02	-	1.438E+04	-
SIL 4	1.0E+04	1.0E+05	3.162E+04	1.778E+04	5.623E+04	1.557E+04	8.753E+04	2.217E+03	-	1.438E+05	-
NR	1.0E+05	1.0E+06	3.162E+05	1.778E+05	5.623E+05	1.557E+05	8.753E+05	2.217E+04	-	1.438E+06	1.0E+06

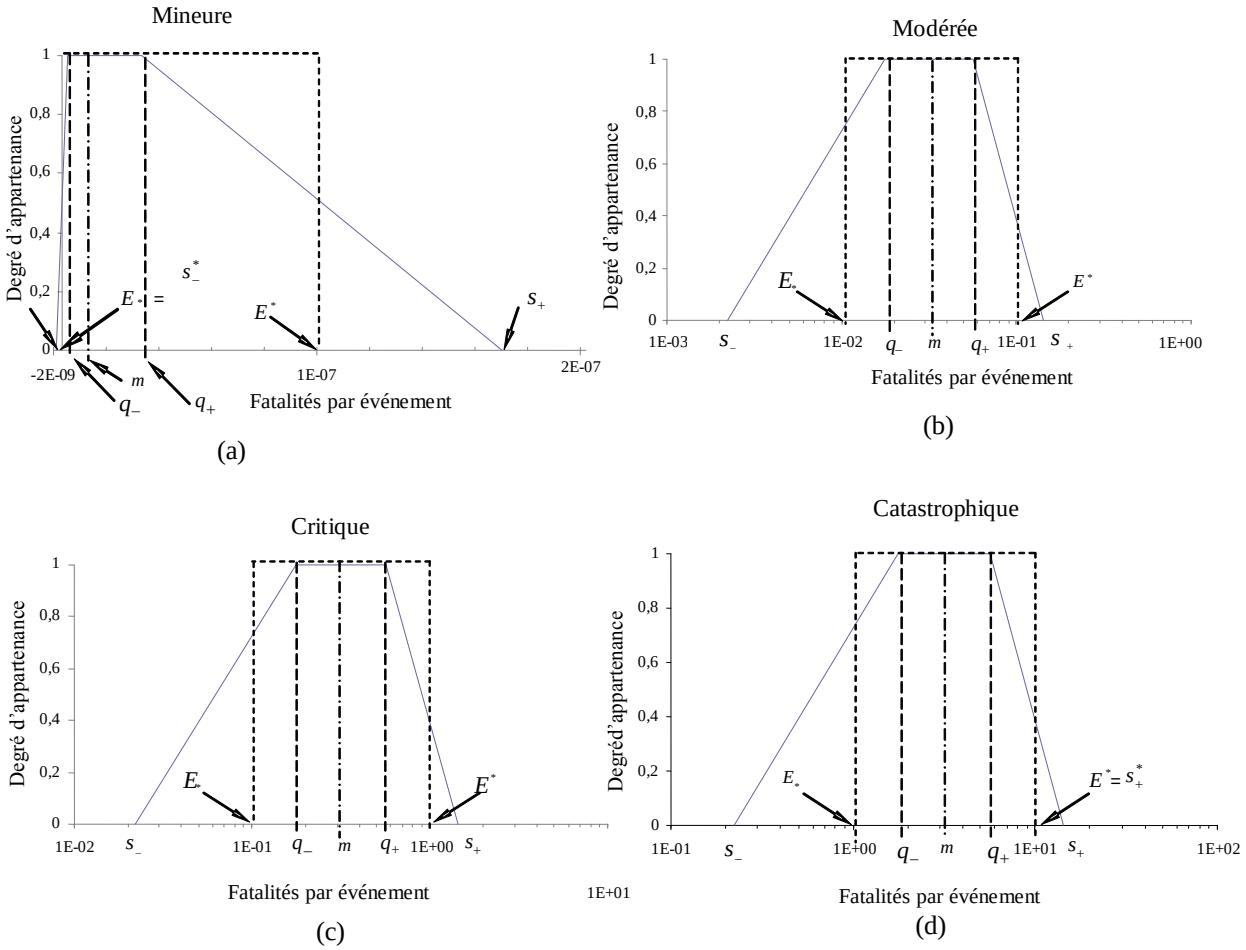


Fig. II.10 : Transformation des intervalles ordinaires en intervalles flous :
Cas du paramètre " Conséquence "
(a) Mineure, (b) Modérée, (c) Critique, (d) Catastrophique

Les partitions floues des paramètres du risque et du SILobtenues à partir des intervalles flous $Q = [q_-, [s_-, s_+], q_+]$ sont données par les figures II.11 et II.12. Une description plus détaillée de ces partitions est présentée ci après:

- **Conséquence :** Quatre ensembles flous à savoir «Mineure», «Modérée», «Critique» et «Catastrophique» ont été définis sur l'espace de cette variable d'entrée (Figure II.11: a). Les valeurs variant de 10^{-9} à 10 sont représentées sur une échelle logarithmique. A la valeur linguistique « mineure », définie dans le graphe de risque comme «pas de mort», est attribué l'intervalle [10^{-9}, 10^{-7}] qui représente convenablement un événement improbable. Cet intervalle est transformé en un intervalle flou avec l'omission de la partie négative. L'intervalle [1, 10] est choisi pour être la valeur moyenne de l'ensemble flou «catastrophique»avec la possibilité de modifier sa borne supérieure en fonction de la situation dangereuse. La partie croissante de «catastrophique» est ajustée en prenant la borne

supérieure du noyau de l'ensemble flou « critique » comme point de départ. Cet ajustement a un double objectif : d'une part, il supprime la partie négative de l'intervalle flou associé au terme «catastrophique» qui n'a pas de sens d'un point de vue 'nombre de décès'. Deuxièmement, il évite le chevauchement entre plus de deux ensembles flous, ce qui implique de nombreuses valeurs sans signification pour la catégorie «catastrophique». Par exemple, le degré d'appartenance de la valeur zéro à l'intervalle flou non-ajusté est 0,27.

-Fréquence et période d'exposition : Deux ensembles flous, à savoir «Rare» et «Fréquente» ont été définis sur une échelle linéaire allant de 0% à 100% (Figure II.11: b). Les bornes de leurs noyaux sont obtenues a partir des moyennes arithmétiques des subdivisions de l'intervalle discret. Comme pour le paramètre précédent, la partie négative du premier ensemble est omise et la borne supérieure de son noyau a servi de borne inférieure pour le support du second ensemble. La fonction d'appartenance de ce dernier est évidemment ouverte à droite.

- Possibilité d'éviter l'événement dangereux : Comme pour le paramètre d'entrée précédent, deux ensembles flous « Impossible» et «Possible» ont été définis sur l'univers [0, 100] (Figure II.11: c). Pour le premier ensemble, la partie négative est supprimée et la borne supérieure de son support prend la valeur de la borne inférieure du noyau de l'ensemble «possible». Les valeurs de ces derniers sont limitées à 100 avec une fonction d'appartenance ouverte à droite.

- Probabilité de l'apparition de l'événement 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 (Figure II.11: d). A l'instar du premier paramètre, les valeurs de probabilité sont représentées sur une échelle logarithmique. Le choix de la valeur 10^{-5}/an (soit 1,14 $\times 10^{-9}$/ h), comme borne inférieure de l'intervalle [10^{-5}, 0.03], se réfère à un événement improbable. Seuls le premier et les derniers ensembles flous ont été ajustés en supprimant la partie négative et les valeurs supérieures à 1. L'ensemble flou intermédiaire «faible» est demeuré inchangé.

- **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 l'intervalle [1, 10^6] avec une partition régulière d'un facteur de dix entre deux subdivisions successives.

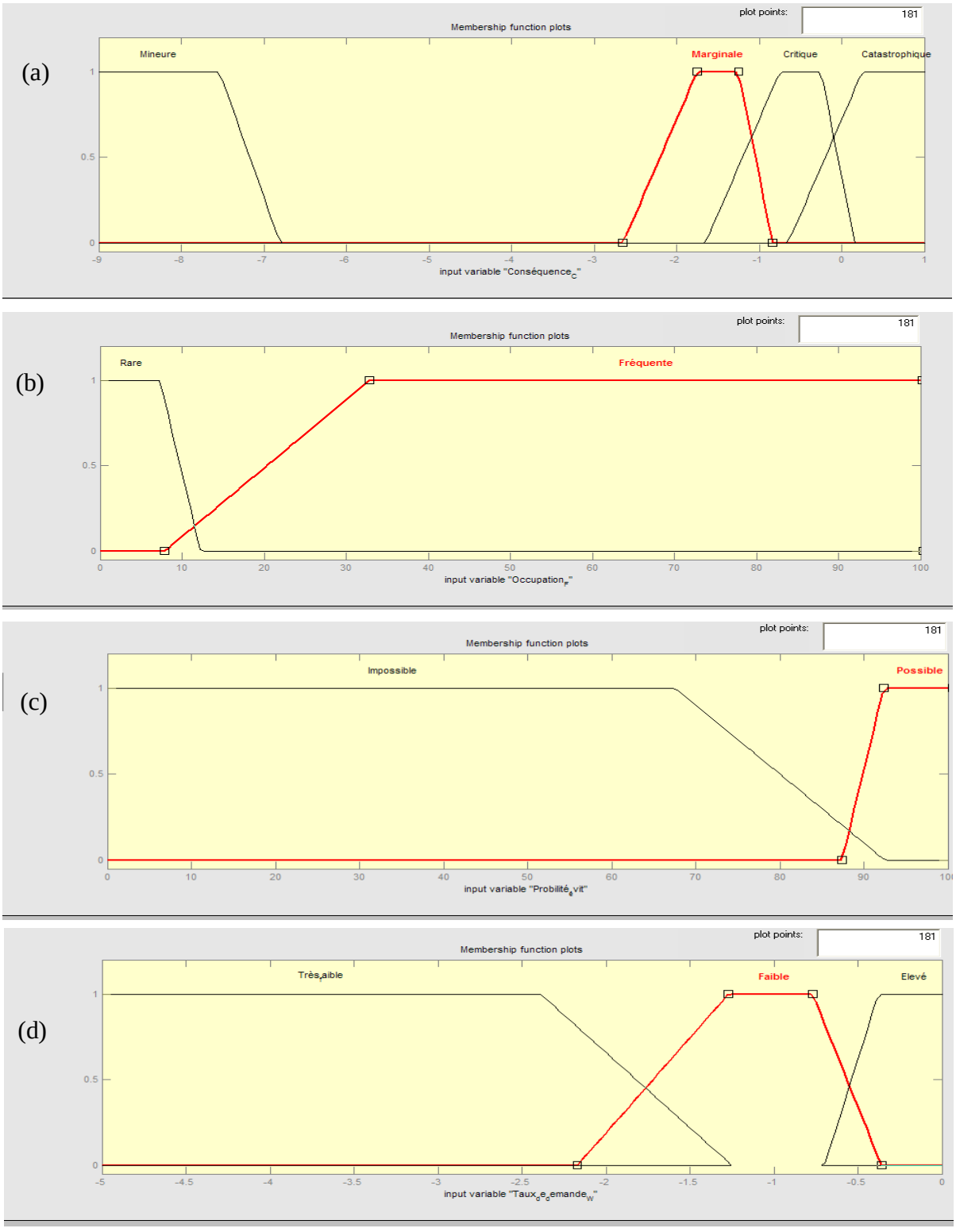


Fig. II.11 : Fonctions d'appartenance générées pour les paramètres du risque:
(a) Conséquence, (b) Exposition, (c) Evitement, et (d) Taux de demande.

Ainsi, six ensembles flous sont définis sur l'espace du SIL (Figure II.12): quatre ensembles sont associés à quatre SIL avec les mêmes nominations décrivant les niveaux eux mêmes, à savoir «SIL1», «SIL2», «SIL3» et «SIL4», et deux ensembles flous nommés «RNSS» et «NR» se référant, respectivement, aux cas «pas d'exigences particulières de sécurité», « un seul SRS non recommandé». Excepté la limitation de l'ensemble «NR», Aucun réajustement n'est effectué pour les autres ensembles.

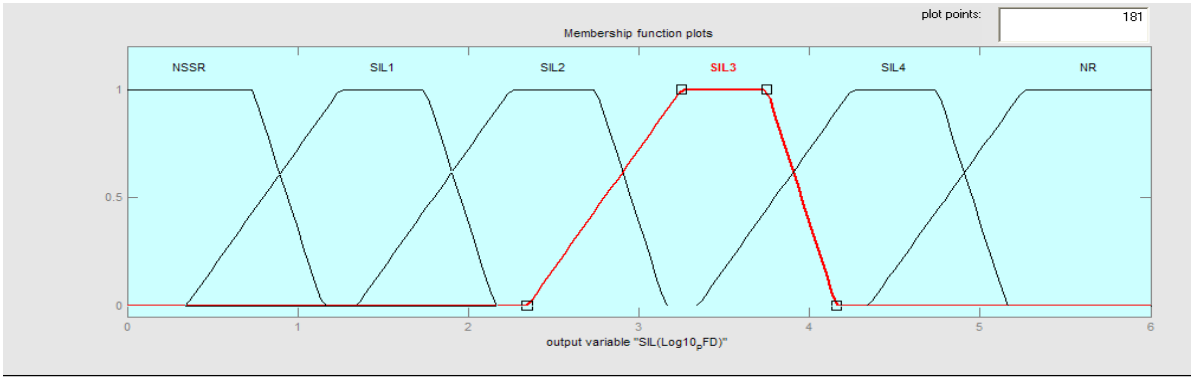


Fig. II.12 : Fonctions d'appartenance générées pour le SIL

II.7.4 Dérivation des règles floues

Un certain nombre de règles floues SI-ALORS sont extraites en suivant la logique du graphe de risque et en utilisant les descripteurs linguistiques associés aux paramètres de risque et au SIL. Dans ce cas, la base de règles peut être considérée comme une traduction du graphe principalement basée sur la connaissance et l'expérience des analystes quant à la nature du processus et à la réduction requise des risques. Le nombre de règles et des variables d'entrée figurant dans la prémisse des règles dépend de l'implémentation du graphe de risque, c'est-à-dire du niveau de décomposition du graphe. Dans les parties prémisse et conclusion des règles, la signification de la valeur linguistique des variables de sortie et d'entrée est décrite par les sous-ensembles flous définis dans l'étape 2. La forme générale des règles floues dérivées est:

$$R_i : \text{SI } C \text{ est } A_{iC} \text{ et } F \text{ est } A_{iF} \text{ et } P \text{ est } A_{iP} \text{ et } W \text{ est } A_{iW} \quad ALORS\ le\ SIL \text{ est } B_i \qquad \text{(II.16)}$$

où les paramètres C, F, P et W représentent les variables d'entrée ; A_{iC} , A_{iF} , A_{iP} , et A_{iW} qui sont respectivement leurs valeurs linguistiques. Le SIL est une variable de sortie avec B_i comme valeur linguistique.

Le vecteur flou $\left(A_{iC}, A_{iF}, A_{iP}, A_{iW}\right)$ et l'ensemble flou B_i sont respectivement, des éléments de l'univers $U_{RP} = U_C \times U_F \times U_P \times U_W$ (RP pour paramètres de risque) et l'univers U_{SIL}. Selon la réduction du graphe de risque, la partie prémisse de la règle (II.16) peut être réduite à deux ou trois variables d'entrée. En se référant au graphe de risque étalonné de la figure II.6, deux exemples de règles floues peuvent être présentés comme suit:

SI C est *Marginale* et F est *Fréquente* et P est *Possible*

et W est *F*aible A*LORS SIL* est *SIL2*

SI C est *Critiqe* et F est *Rare* et W est *F*aible

A*LORS SIL* est *SIL3*

II.7.5 Application de la base de règles floues

Comme expliqué dans la section II.6, lorsque le système d'inférence floue est appliqué à un ensemble de valeurs d'entrée, l'information suit le processus de fuzzification-inférence-défuzzification pour générer la valeur de sortie. Compte tenu de n'importe quelle combinaison de valeurs d'entrée qui couvrent le contexte spécifique de paramètres de risque, le graphe de risque à base de règles floues calcule la valeur du RRF que la SIF doit atteindre dans un contexte spécifique. La fuzzification transforme le vecteur d'entrée $u_{RP}^0 = \left(u_C^0, u_F^0, u_P^0, u_W^0\right)$ dans U_{RP} en des ensembles flous dans U_{RP}. Le moteur d'inférence permet l'obtention de la sortie floue (SIL flou) en utilisant le modèle Max-Min de Mamdani (voir les expressions (II.3), (II.4) et (II.5)) tandis que la défuzzification transforme les ensembles flous SIL sur U_{SIL}. Si un ou plusieurs paramètres ne sont pas pris en considération par une règle donnée, ils n'auront pas d'effet sur le degré de correspondance α_i.

L'ensemble des règles floues issues du graphe de la figure II.6 (chapitre 2) ainsi que la surface floue correspondante sont donnés respectivement par le tableau II.8 et la figure II.13.

II.8 Validation théorique du modèle Graphe de Risque Flou proposé

Pour valider le modèle graphe de risque flou que nous avons proposé, nous avons vérifié deux propriétés d'une base de règles floues, à savoir la cohérence et la consistance. La méthodologie de validation consiste à faire varier chaque paramètredu risque (C, F, P et W), indépendammentdes autres dans un sens croissant.

La vérification de la cohérence de la base de règles floues développée relative au SIL est faite en vérifiant la monotonie de celle-ci pour chaque paramètre. Les résultants de cette variation sont donnés par la figure II.14.

Tableau. II.8: Règles de combinaison des paramètres du risque

Règle	Conséquence	Occupation	Possibilité d'évitement	Taux de demande	SIL
1	Mineure	Néant	Néant	Elevé	A
2	Mineure	Néant	Néant	Faible	/
3	Mineure	Néant	Néant	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	Fréquente	Possible	Elevé	2
11	Marginale	Fréquente	Possible	Faible	2
12	Marginale	Fréquente	Possible	Très faible	1
13	Marginale	Fréquente	Impossible	Elevé	3
14	Marginale	Fréquente	Impossible	Faible	2
15	Marginale	Fréquente	Impossible	Très faible	2
16	Critique	Rare	Néant	Elevé	3
17	Critique	Rare	Néant	Faible	3
18	Critique	Rare	Néant	Très faible	2
19	Critique	Fréquente	Néant	Elevé	4
20	Critique	Fréquente	Néant	Faible	3
21	Critique	Fréquente	Néant	Très faible	3
22	Catastrophique	Néant	Néant	Elevé	NR
23	Catastrophique	Néant	Néant	Faible	4
24	Catastrophique	Néant	Néant	Très faible	3

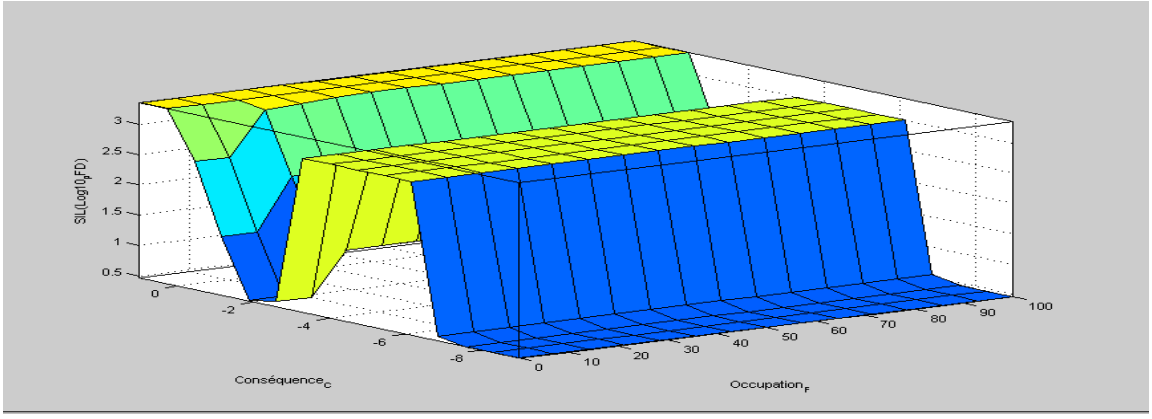
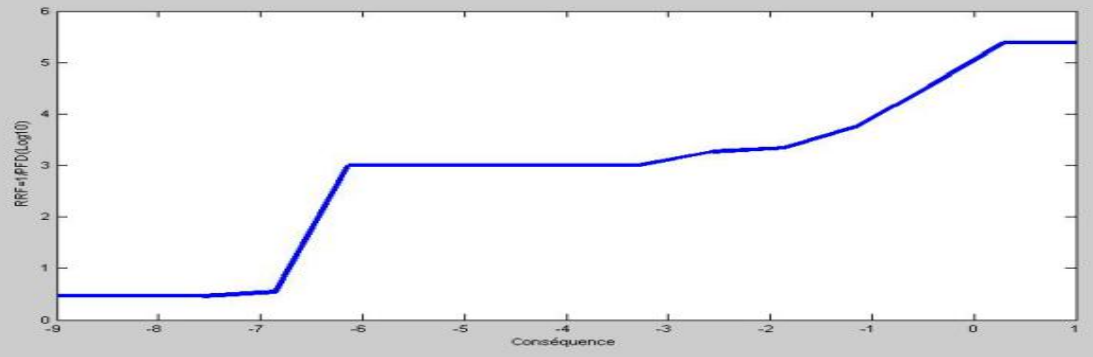
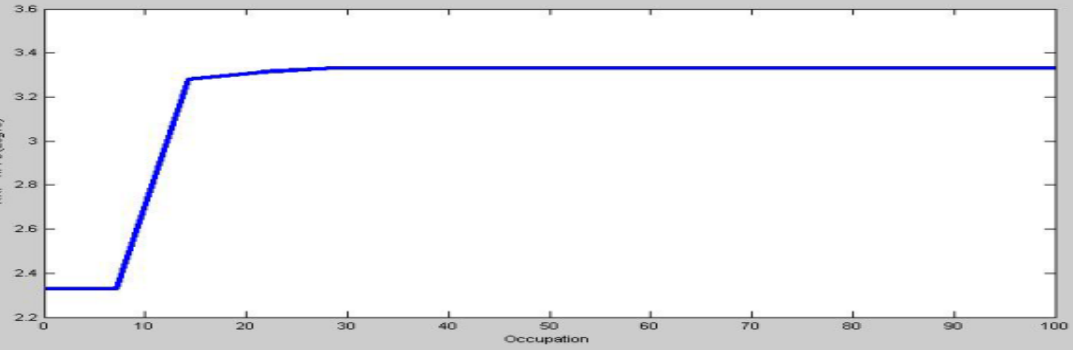


Fig. II.13: Surface floue du SIL

(a)



(b)



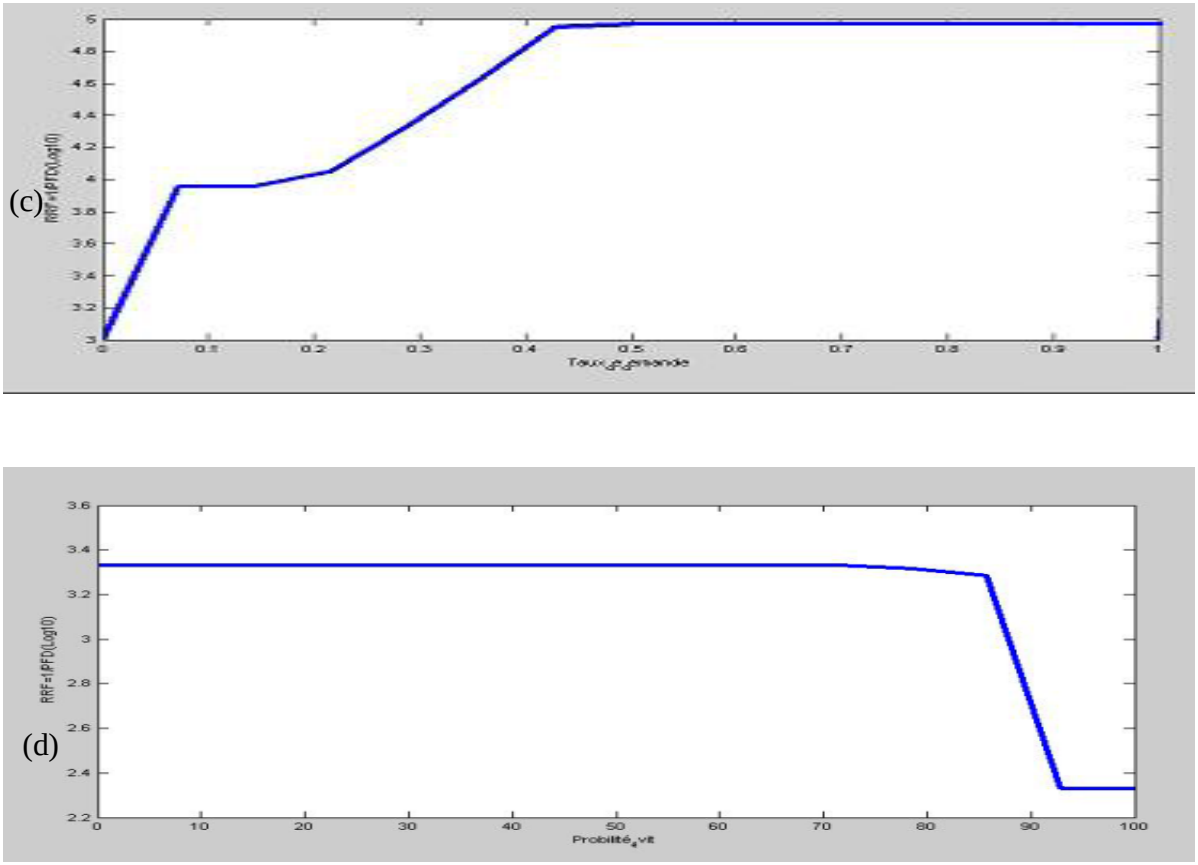


Figure II-14 : Variation du SIL en fonction des paramètres du risque

Nous remarquons d'après ces résultats qu'on faisant varier les paramètres C, F et W dans le sens croissant, le RRF augmente. Cependant, la variation du RRF est inversement proportionnelle par rapport à la probabilité d'évitement ce qui signifie que plus la probabilité d'évitement augmente, le SIL exigé est faible. La monotonie de la base de règles floues développée est vérifiée pour chaque paramètre.

Il ressort également de la comparaison de la variation des différents paramètres que la conséquence et le taux de demande sont prédominants par rapport aux deux autres paramètres,l'occupation et la possibilitéd'évitement.

Quant à la consistance de la base de règles floue développée, elle est également vérifiée en remarquant qu'il n'y a pas, parmi les règles floues établies, de règles redondantescar, comme il a été mentionné (§ II.7.3),notre base de règles floues est développée en se basant sur un modèle graphe de risque existant.

Les résultats obtenus confirment donc la cohérence et la consistance de la base de règles floues développée.

Conclusion

Bien que les graphes de risque classiques soient relativement simples à mettre en œuvre, ils peuvent conduire à des résultats incohérents et probablement au conservatisme qui peut entraîner une surestimation du SIL. En effet, l'utilisation de définitions qualitatives pour les paramètres de risque est très subjective et leur signification peut être mal comprise. D'autre part, l'interprétation numérique des paramètres de risque et du SIL à l'aide d'intervalles discrets viole la transition progressive entre les intervalles qui est plus réaliste.

En effet, comme il a été mentionné (§ II.5), quand la valeur par exemple du SIL, est comprise entre deux classes successives, la plus stricte exigence en matière de SIL est choisie. Cependant, cette solution conservatrice implique une augmentation plus substantielle de l'effort et de la compétence compte tenu de la différence notable survenant lors du passage du SIL2 au SIL3 (Smi, 04). Les niveaux d'intégrité flous peuvent être une alternative pour résoudre ce genre de problèmes. Par exemple, une valeur de RRF (1/PFD), en tant que résultat du modèle du graphe de risque flou, peut appartenir simultanément à deux SIL flous «SIL2» et «SIL3» mais avec un degré d'appartenance à ce dernier peu supérieur (par exemple égal à 0,7). Il serait donc, raisonnable de dire que nous sommes en présence de «plutôt SIL3», qui, selon la proportion donnée par le degré d'appartenance, implique clairement un coût et un temps moindres que «SIL3 conventionnel» (soit 70% par exemple du coût et du temps consacré au SIL3 conventionnel).

Le modèle flou proposé est un graphe à base de règles floues. Ses principaux avantages peuvent se résumer dans les points suivants :

- Il préserve les quatre paramètres utilisés dans le graphe de risque standard et peut être facilement adapté aux graphes de risque amélioré.

- Les échelles avec valeurs linguistiques floues sont utilisées pour évaluer les paramètres de risque et l'étalonnage du modèle peut être fait en faisant varier les valeurs associées aux paramètres de risque.

- Les résultats du modèle qui sont des valeurs numériques du RRF (1/PFD) peuvent être comparés directement avec ceux donnés par des méthodes plus raffinées comme l'AdD, le QRA et LOPA.

CHAPITRE III :

Approche floue d'analyse des couches de protection

Résumé : *L'objectif de ce chapitre consiste à proposer un modèle flou de LOPA qui permet à l'analyste d'évaluer les éléments d'un scénario d'accident et les mesures de réduction des risques de manière plus souple et moins contraignante. Avant de présenter l'approche proposée, nous rappelons quelques définitions fondamentales relatives à la méthode, ensuite nous présentons l'approche conventionnelle ainsi que le problème d'incertitudes qui y est lié. Enfin, le modèle flou proposé fera l'objet de la dernière section.*

Introduction

Partant de la définition du risque, on peut dire que la mauvaise gestion de ce dernier peut entraîner de graves conséquences socio-économiques ne touchant pas uniquement le système en question mais aussi son environnement. Le but principal de toute analyse liée à la sécurité des processus industriels est, en effet, la réduction des risques jugés inacceptables à un niveau acceptable ou au moins tolérable. Pour assurer cette réduction, plusieurs systèmes ou barrières de sécurité, de nature technique et/ou organisationnelle, peuvent être utilisés (Skl, 06), (Har, 09), (Sha, 10).. Chaque barrière de sécurité est caractérisée par une fonction de sécurité à laquelle est associé un Facteur de Réduction de Risque (RRF) qui est l'inverse de sa probabilité de défaillance à la demande (PFD) (IEC, 03). Les barrières de sécurité ont différents rôles selon qu'elles interviennent en prévention, en réduisant la probabilité d'occurrence d'un événement redouté, ou en protection en limitant la gravité de l'événement redouté dont on n'a pas pu empêcher l'occurrence (CCP, 00), (CCP, 01).

Pour l'analyse et l'évaluation de l'efficacité de ces barrières de sécurité, plusieurs méthodes ont été développées (Gul, 04), (Kir, 05), (Nai, 09):

- *Méthodes qualitatives telles le graphe de risque et la matrice de criticité des événements dangereux.*
- *Méthodes semi-quantitatives telles que l'Analyse des Couches de Protection (LOPA) et le graphe de risque étalonné.*
- *Méthodes quantitatives telles que l'Arbre de Défaillances (AdD) et l'Evaluation Quantitative de Risque (QRA).*

L'Analyse des couches de protection (LOPA : Layers Of Protection Analysis) décrite dans la norme IEC 61511 (IEC, 03) et développée par CCPS (Center for Chimical Process Safety) à la fin des années 1990 (CCP, 01), est l'une des méthodes les plus utilisées. Elle permet d'estimer la conséquence et la fréquence d'un événement redouté. Elle évalue la réduction du risque apportée par les différentes couches de protection et détermine le nombre nécessaire de ces dernières pour ramener le risque à un niveau tolérable.

L'Analyse des couches de protection (LOPA), bien que ce soit une méthode relativement récente (Art, 98), (CCP, 01), elle a trouvé un large domaine d'application comme étant une méthodologie d'évaluation des risques relativement simple (CCP, 00), (ARA, 04), (Fan, 07),

(Mar, 11), (Mye, 12), (Bay, 12). Cependant, en l'appliquant à des systèmes réels, il se pose le problème d'attribution des valeurs exactes aux éléments du scénario analysé, à savoir la fréquence de l'événement initiateur et les probabilités de défaillances à la demande des couches de protection indépendantes (IPLs : Independant Protection Layers). En effet, la complexité de certains systèmes, tels que les processus de transformation chimiques ou les systèmes où les accidents sont rares, fait que les données statistiques sur leurs défaillances sont faiblement fiables ou non disponibles (Kau, 91), (Chu, 92). Les systèmes Instrumentés de Sécurité (SIS), par exemple comme importante classe de barrières de sécurité hautement fiables, sont rarement sollicités et par conséquent, leurs défaillances sont des événements rares dont la valeur de probabilité est entachée d'incertitudes (Sal, 07), (Mar, 07), (Nai, 09).

De grands efforts sont déployés par les analystes du risque pour réduire les incertitudes qui surviennent durant chaque phase du processus d'évaluation des risques.

L'objectif du chapitre s'intègre dans cette perspective et consiste à proposer un modèle flou de LOPA qui permet à l'analyste d'évaluer les éléments d'un scénario d'accident et les mesures de réduction des risques de manière plus souple et moins contraignante. Avant d'aborder l'approche proposée, nous rappelons quelques définitions fondamentales relatives à la méthode, ensuite nous présentons le modèle conventionnel, ses avantages et limites. Nous évoquons particulièrement le problème d'incertitudes qui y est lié.

III.1 Notions de bases relatives à la méthode LOPA

III.1.1 Couches de protection

Pour éviter des phénomènes dangereux (incendies, explosions, les rejets de matières dangereuses, etc.) les industriels sont amenés à mettre en place des barrières de sécurité (ou couches de protection) dont le rôle est de prévenir l'apparition de tels phénomènes ou d'en limiter les conséquences. Le terme « couche de protection » est utilisé dans les industries de processus pour représenter le concept de défense en profondeur (Kum, 07). Il a été adopté depuis 1960 dans l'industrie nucléaire pour signifier le moyen qui atténue le dégagement des éléments radioactifs et leur dispersion dans l'atmosphère. Une défense en profondeur est la combinaison de plusieurs couches de protection indépendantes et redondantes pour compenser les défaillances potentielles humaines et mécaniques. Elle comprend aussi les

barrières de prévention et les mesures d'intervention d'urgence et de protection du publique (Ave, 11).

La bonne maitrise des risques industriels est assurée donc par différentes couches de protection qui interviennent soit en prévention, en minimisant la probabilité d'apparition de l'événement dangereux, soit en protection en limitant les conséquences de l'accident dont on n'a pas pu empêcher l'occurrence (ISO, 99), (Mar, 12). La figure III.1 présente les différentes couches de protection qui peuvent être utilisées dans un processus industriel (Gob, 98), (CCP, 01), à savoir :

- La conception des équipements et des procédés en respectant les codes et les normes de conception (limiter les quantités de produits dangereux stockés, prévoir des postes de travail ergonomiques, …) constitue la première couche de protection.

- La deuxième couche de protection est le système de conduite (ou contrôle- commande) qui comprend les opérations de contrôle élémentaires et d'alarmes. Cette couche intervient en cas d'anomalie sur le procédé. Des équipements appelés BPCS (Basic Process Control System) sont utilisés dans cette couche. Ce sont des systèmes manuels ou automatiques (systèmes de contrôle de température, de niveau, etc.) dont les exigences comportementales en termes de sécurité ne sont pas élevées.

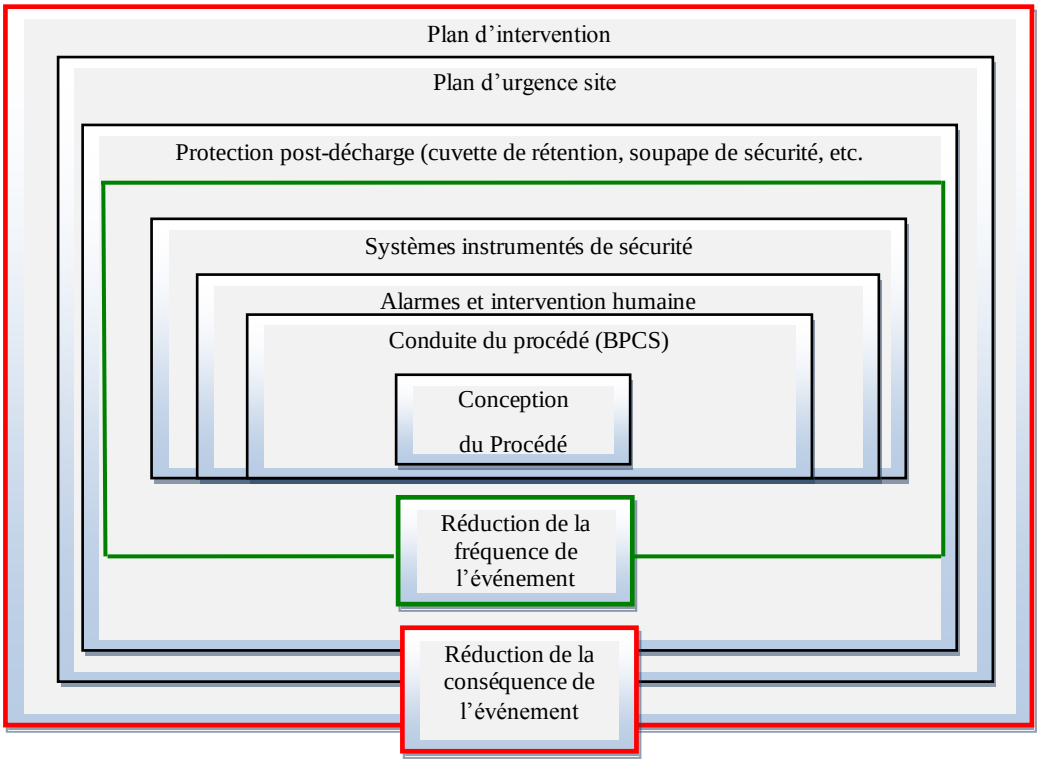


Fig. III.1 : Les couches protection (Gob, 98)

- En cas d'échec des matériels de surveillance de procédés, des dispositifs complémentaires de prévention tels que les systèmes d'alarmes interviennent pour alerter les opérateurs et induire des interventions manuelles, ils constituent la troisième couche de protection. A titre d'exemple, un capteur de pression pour initier une alarme de haute pression et alerter l'exploitant de prendre les mesures appropriées pour arrêter l'opération.

- Les Systèmes Instrumentés de Sécurité (SIS) représentent la quatrième couche de protection qui entre en action lorsque le processus se trouve dans des conditions anormales.

- La couche de protection suivante intervient après l'incident, il s'agit de limiter les conséquences par des dispositifs techniques tels que les soupapes, les disques de rupture, les systèmes d'extinction d'incendie, etc.

- L'éloignement et l'évacuation des zones dangereuses constituent la dernière couche de protection. Cette protection physique peut être assurée grâce à des moyens d'évacuation ou de rétention, des zones de dégagement, des zones de stockage clairement identifiées et différentiées, etc.

Toutes ces couches de protection ont donc pour objectif d'atteindre un niveau de sécurité ou de maîtrise des risques acceptable. Un phénomène dangereux ne peut se produire que si l'ensemble de ces couches de protection n'a pas rempli ses fonctions de sécurité. A titre d'illustration, la figure III.2 (CCP, 01) montre, dans le cadre d'une analyse probabiliste des risques, que la probabilité du phénomène dangereux est diminuée après le franchissement de chaque couche de protection (diminution de l'épaisseur des flèches sur le schéma de la figure III.2.

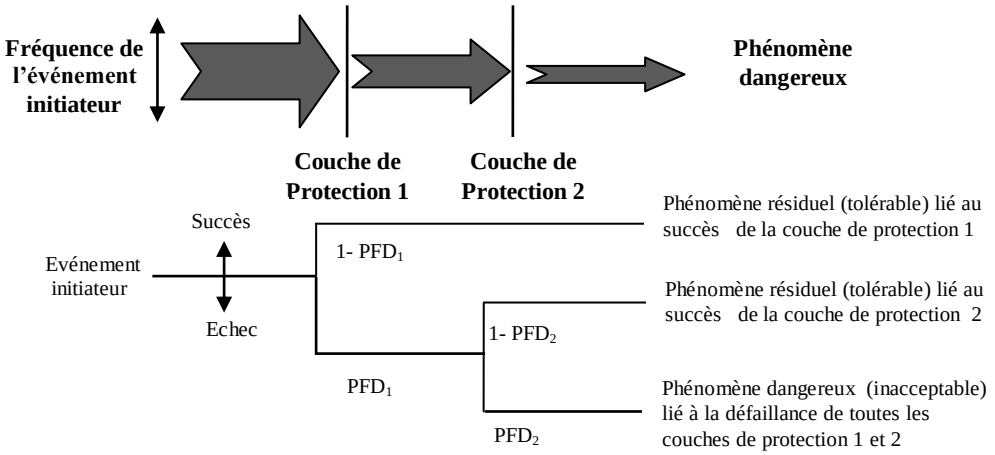


Fig. III.2 : Couches de protection et déroulement d'un scénario d'accident

Le franchissement de la couche de protection signifie sa défaillance (représentée par une probabilité de défaillance à la demande (PFD) qui se traduit, comme le montre la figure III.3, par une décote de la fréquence de l'événement initiateur d'un facteur de réduction égal à l'inverse de la probabilité de défaillance de la couche de protection (Art, 98), (CCP, 01).

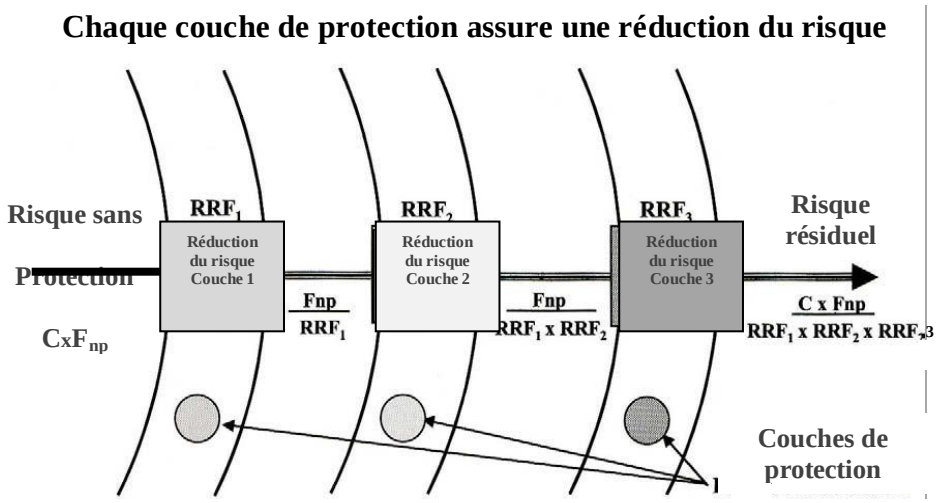


Fig. III.3 : Réduction du risque par les couches de protection *(Mac, 04)*

III.1.2 Couches de protection indépendantes (IPLs)

Une IPL est un dispositif, un système ou une action qui est capable de prévenir un scénario d'accident et/ou réduire ses effets, indépendamment de l'événement initiateur ou des composants des autres couches de protection conçues et prévues pour le même scénario. Elle doit être efficace pour remplir la fonction de sécurité pour laquelle elle a été conçue. L'efficacité d'une IPL est évaluée en termes de sa probabilité de défaillance à la demande (PFD) qui est la probabilité que l'IPL n'effectue pas correctement sa fonction de sécurité quand elle est sollicitée (CCP, 01), (ARA, 04). Cette défaillance peut être causée par :

- Un composant de la couche de protection qui se trouve dans un état de défaillance ou d'insécurité quand l'événement initiateur se produit ;
- Un composant qui devient défaillant durant l'accomplissement de sa fonction ;
- Une défaillance de l'intervention humaine.

- L'identification des IPL, parmi les barrières de sécurités existantes dans un procédé est une étape primordiale dans le processus d'analyse par LOPA. Une barrière de sécurité qualifiée d'IPL doit être :

i) ***Efficace :*** Une IPL est efficace si elle est :

- capable de détecter l'événement initiateur qui l'incite à agir,
- capable de détecter à temps cet événement initiateur ou dérive pour prendre l'action corrective qui devrait prévenir la conséquence indésirable associée à un scénario déterminé ;
- capable de remplir la fonction de sécurité à laquelle elle est dévolue pendant le temps disponible.

ii) ***Indépendante:*** La méthode LOPA utilise le critère d'indépendance pour s'assurer que les effets de l'événement initiateur ou des autres IPL n'interagissent pas avec une IPL spécifique ce qui dégrade sa capacité d'effectuer sa fonction de sécurité. L'indépendance exige que l'IPL soit indépendante de :

- L'occurrence d'un événement initiateur ;
- La défaillance des composants d'une autre IPL conçue et prévue pour maîtriser le même scénario.

Il est particulièrement important de déterminer les modes communs de défaillance lorsqu'on sélectionne une barrière de sécurité comme étant une IPL. Le mode commun de défaillance peut impliquer l'événement initiateur, une ou plusieurs barrières ou une interaction de plusieurs barrières. Toutes les barrières affectées par les modes communs de défaillance doivent être considérées comme une seule barrière (Cha, 04).

La figure III.4 illustre un cas où une barrière de sécurité peut être retenue, ou non, comme une IPL pour un scénario.

Deux approches sont développées pour évaluer l'indépendance des IPL (CCP, 01) :

Approche A : C'est une approche conservative puisqu'elle autorise seulement une seule IPL dans un BPCS (Basic Process Control System) et exige que cette IPL soit indépendante de l'événement initiateur. Cette approche élimine plusieurs défaillances de

causes communes en affectant la PFD aux IPLs existantes. L'approche A est simple à appliquer du fait que peu de jugement est laissé à l'analyste et que ses règles sont sans ambiguïté.

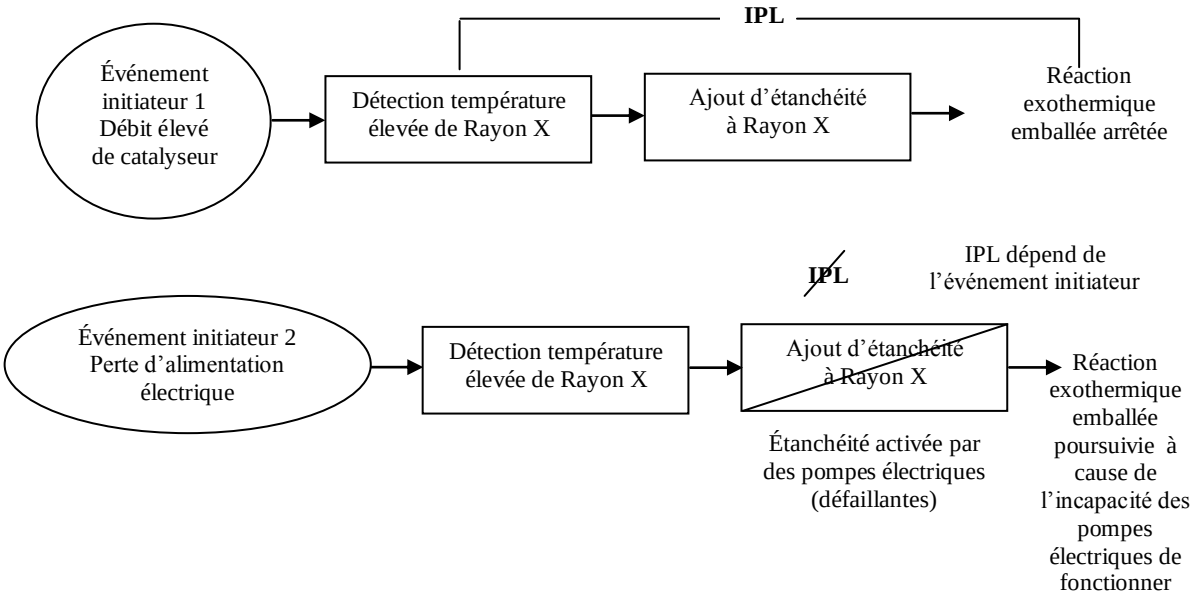


Fig. III.4 : Exemple d'une IPL non indépendante de l'événement initiateur (CCP, 01)

Approche B : Cette approche autorise soit plus d'une IPL dans la même boucle BPCS ou bien une seule IPL avec l'existence d'un événement initiateur lié à cette boucle (avec l'indépendance exigée pour certains composants). Cette approche est basée sur l'hypothèse que si une boucle de BPCS est défaillante, il est probable que le composant défaillant soit le système de détection ou bien l'élément final de contrôle, et que la défaillance de l'IPL est due à un défaut dans l'unité de traitement. L'approche B attribue un nombre limité de composants pour une boucle BPCS pour qu'elle puisse servir comme IPL dans un scénario. Cette approche est moins pratique, elle exige :

- Des informations sur la conception et la performance du BPCS,
- Une compréhension complète des modes communs de défaillance dans une IPL,
- Une analyse expérimentale permettant d'une part, d'identifier une IPL, et d'autre part de s'assurer qu'il s'agit effectivement d'une IPL selon les critères correspondants.

iii) ***Testable :*** Généralement, une barrière de sécurité est testable lorsqu'une opération manuelle ou automatique permet de vérifier ses fonctionnalités dans des conditions normales d'utilisation. Une IPL doit être donc conçue pour permettre périodiquement de s'assurer par test de son efficacité et de démontrer qu'elle répond aux exigences de réduction du risque.

Pratiquement les tests doivent être effectués afin de contrôler et de vérifier les performances des IPL (temps de réponse et niveau de confiance).

III.2 Analyse des Couches de Protection (LOPA) conventionnelle

L'analyse des couches de protection LOPA décrite dans la partie 3 de la norme IEC 61511 (IEC, 03) et développée par CCPS (Center for Chimical Process Safety) à la fin des années 1990 (CCP, 01) est une méthode semi-quantitative d'analyse et d'évaluation des risques. Elle peut être utilisée à n'importe quel moment du cycle de vie du processus ou de l'installation (système), mais de préférence durant la phase de conception ou quand des modifications pour un processus existant ou une amélioration de ses systèmes de sécurité sont exigées (CCP, 01). LOPA est un cas particulier de la méthode Arbre des Evénements (AdE) (Mar, 02), établie dans le but de déterminer la fréquence d'une conséquence indésirable pouvant être prévenue par une ou plusieurs couches de protection. Cette fréquence est, pour un scénario bien défini, une mesure du risque qui peut être comparée au risque maximum tolérable afin de décider si une réduction est nécessaire selon le principe ALARP « As Low As Reasonably Practicable ».

Le but principal de LOPA est de déterminer s'il y a suffisamment de couches de protection pour la maîtrise d'un scénario d'accident bien défini, c'est-à-dire de vérifier si le risque est réduit à un niveau au moins tolérable. Elle peut aussi être utilisée pour l'analyse d'un scénario s'il est si complexe et/ou ayant des conséquences aussi graves qu'on ne peut pas se contenter d'une décision basée uniquement sur un jugement qualitatif. C'est le cas par exemple où (CCP, 01) :

- L'événement initiateur n'est pas bien défini ;
- La séquence des événements n'est pas bien définie ;

- On ne sait pas identifier parmi les barrières de sécurité existantes, lesquelles sont vraiment des IPL.

Un scénario peut exiger une ou plusieurs couches de protection (Fig. III.2) selon la complexité du procédé et le potentiel de gravité de la conséquence (CCP, 01). Pour un scénario donné, une seule couche de protection qui fonctionne pour prévenir l'occurrence de la conséquence et dés qu'elle n'est pas efficace, d'autres couches doivent être prévues pour réduire le risque d'accident à un niveau tolérable.

Ces couches de protection comprennent des barrières passives (cuvette de rétention, mur coupe-feu, etc.) ou actives (soupape de décharge, SIS, etc.) (Sum, 03).

III.2.1 Principe de la méthode LOPA

Une autre façon de comprendre LOPA est de la considérer comme un cas particulier de la méthode de l'Arbre des Evénements (Mar, 02) qui est une méthode quantitative d'évaluation de risque. Un arbre d'événements analyse toutes les conséquences possibles d'un événement initiateur, alors que LOPA n'étudie qu'un seul scénario à la fois (couple cause- conséquence), ce qui représente un seul chemin sur l'arbre d'événements. Ce dernier peut servir de support pour LOPA puisqu'il facilite la représentation de l'ordre des IPL.

LOPA utilise un événement initiateur de la même façon que l'AdE, mais elle exige qu'il soit exprimé en termes de fréquence. Les couches de protection dans LOPA correspondent aux branches d'un AdE (Fig.III.5). Dans LOPA, chaque branche est souvent un ensemble d'événements complémentaires dans lequel la couche de protection accomplie sa fonction de sécurité avec succès ou se trouve défaillante (CCP, 01). LOPA estime la fréquence de la conséquence indésirable, de la même façon que fait l'AdE, en multipliant la fréquence de l'événement initiateur par le produit des PFD des IPL (Independent Protection Layers).

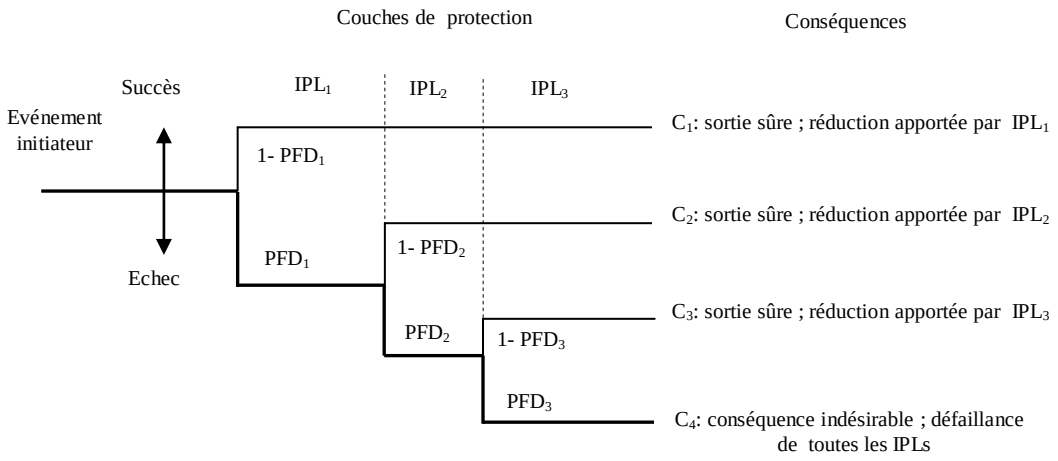


Fig. III.5 : Exemple d'Arbre d'Evénements avec trois couches de protection

III.2.2 Etapes d'élaboration de la méthode LOPA

Comme toutes les méthodes d'analyse de risques, LOPA possède ses propres règles d'élaboration et peut être décomposée en sept principales étapes (CCP, 01) :

III.2.2.1 Établissement des critères d'acceptabilité des scénarios d'accidents : Cette étape est préalable à l'analyse des risques, elle fournit un moyen de limiter la durée de l'étude en ne considérant que les scénarios significatifs en termes de conséquences. L'établissement des critères d'acceptabilité est fait en fonction du contexte de chaque établissement/entreprise concerné et aussi des objectifs poursuivis. Quelques que soient les critères d'acceptabilité retenus, il est indispensable qu'ils soient connus et explicites préalablement avant toute phase d'analyse des risques industriels (Mar, 02). L'estimation des conséquences des risques permet l'identification des scénarios d'accidents les plus importants. Pour les scénarios jugés inacceptables, une évaluation plus fine de gravité demeure indispensable.

III.2.2.2 Développement et sélection d'un scénario d'accident : Les scénarios d'accident sont développés par des méthodes préliminaires d'analyse telles que l'AMDEC et l'HAZOP (Fig. III.6). Le scénario développé par LOPA décrit un seul couple (cause-conséquence). IL est constitué d'un événement initiateur, de la défaillance des IPL et d'une conséquence indésirable. Ce scénario est représenté sous forme d'un AdE.

Selon la nature de la conséquence, est effectuée l'analyse ; dans le cas de l'industrie pétrochimique par exemple, on doit préciser pour le scénario la probabilité d'ignition du produit inflammable et la probabilité qu'une personne soit présente sur le lieu et être touchée par l'événement (CCP, 01).

III.2.2.3 Identification de l'événement initiateur du scénario estimation de sa fréquence : L'événement initiateur doit mener à la conséquence résultant de la défaillance de toutes les couches de protection. Cet événement peut être un événement externe, une défaillance d'un équipement ou une défaillance humaine. Quant à la fréquence de l'événement initiateur, elle peut être estimée, à partir des données de l'industrie, des données du concepteur, d'un jugement d'experts, etc. Cependant, ces données de défaillance devraient être sélectionnées en prenant soin quelles soient représentatives de l'industrie ou de l'opération analysée (CCP, 01).

A noter que, ces données sont parfois exprimées par une probabilité de défaillance à la demande (PFD). Dans ce cas, la fréquence de l'événement initiateur doit être déterminée en estimant combien de fois par an le system a été sollicité.

III.2.2.4 Identification des IPLs et estimation de leurs PFD : Comme mentionné auparavant, LOPA s'intéresse uniquement aux couches de protection qualifiées d'IPLs (Independent Protection Layers). Ces IPLs sont sélectionnées parmi les barrières de sécurité identifiées par une analyse qualitative telle que HAZOP (Fig. III.6). Une valeur de probabilité de défaillance à la demande (PFD) est ensuite affectée à chaque IPL. Déterminer ou spécifier la valeur appropriée de la PFD est un point important de LOPA. Les données disponibles pour évaluer la PFD d'une IPL peuvent être issues des bases de données, du retour d'expérience du secteur industriel concerné ou des données du constructeur

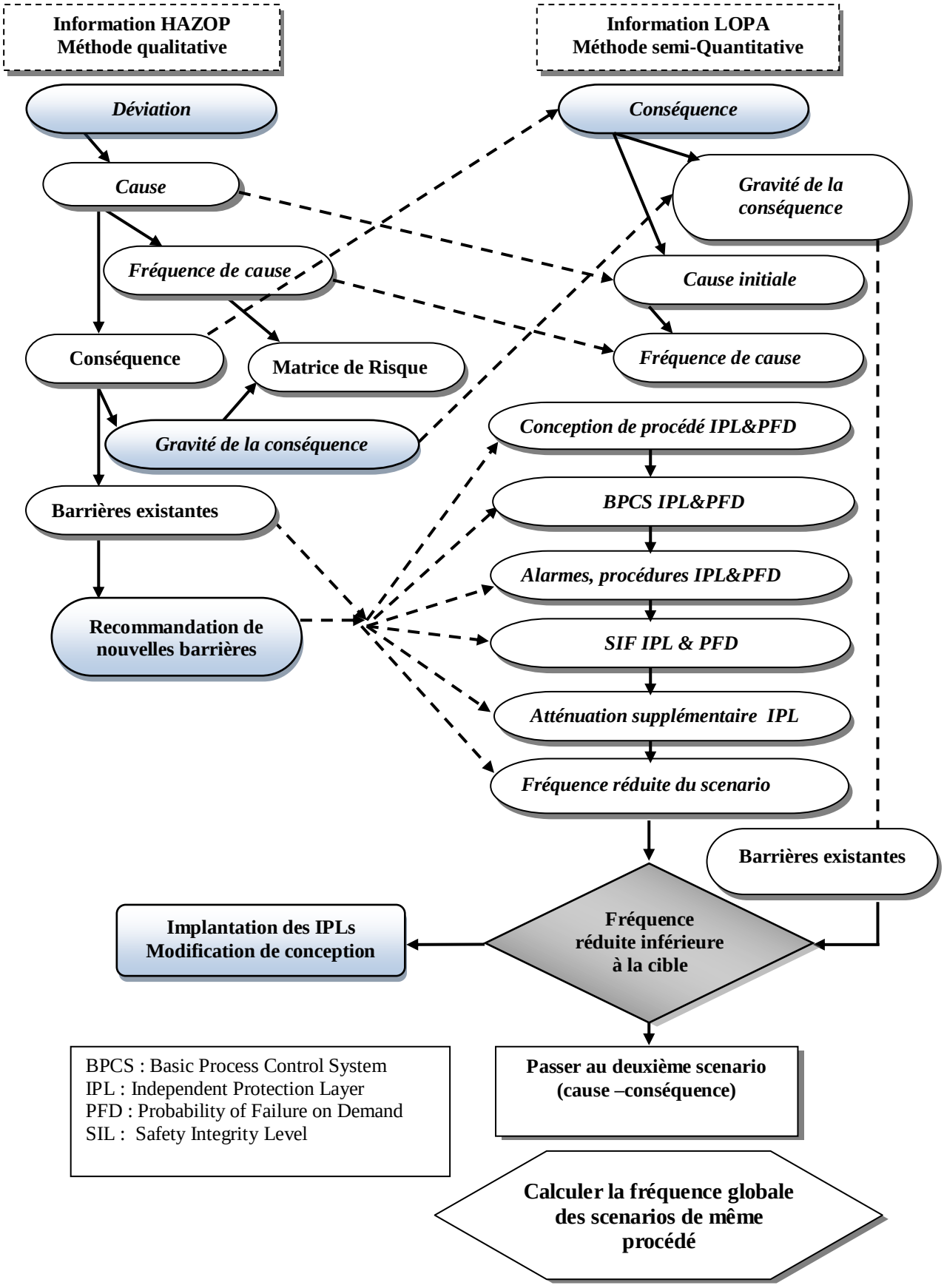


Fig. III.6 : Données HAZOP exploitées par LOPA (Zun, 08)

Cependant, et comme il a été mentionné précédemment, le contexte réel d'utilisation de l'IPL n'est pas toujours facile à prendre en compte, ce qui rend non évident l'utilisation de ces données. Par conséquent, il faut être prudent quant on estime la valeur appropriée de la PFD de l'IPL.

III.2.2.5 Calcul de la fréquence de la conséquence réduite : Cette étape constitue la synthèse des étapes précédentes. La procédure générale de calcul de la fréquence de la conséquence réduite est de combiner la fréquence de l'événement initiateur et les PFD des IPLs en utilisant l'équation suivante :

$$f_i^C = f_i^I \times \prod_{j=1}^{J} PFDmoy_{ij} \qquad \text{(III.1)}$$

Où f_i^C est la fréquence de la conséquence C pour l'événement initiateur i ;

f_i^I est la fréquence de l'événement initiateur i et $PFDmoy_{ij}$ est la probabilité de défaillance à la demande de la j^{éme} IPL qui protège contre la conséquence C de l'événement initiateur i.

Selon les conséquences aux limites, l'équation (III.1) sera modifiée en multipliant la fréquence de scénario d'accident par la probabilité de survenue appropriée à chaque conséquence.

Dans le cas par exemple, du rejet d'un produit toxique inflammable dans l'atmosphère, les effets d'inflammabilité tels que l'incendie sont aussi possibles. Ce dernier nécessite une source d'ignition pour sa réalisation. L'équation(III.1) devient :

$$f_i^{feu} = f_i^I .(\prod_{j=1}^{J} PFD_{ij}).P^{ignition} \qquad \text{(III.2)}$$

N.B : le produit $f_i^I .P^{ignition}$ peut être considéré comme un nouveau événement initiateur.

Notons à ce niveau que l'équation (III.1) est appliquée quand l'IPL est faiblement sollicitée. Le résultat de l'équation peut être utilisé pour comparer le risque calculé au critère d'acceptabilité retenu pour le scénario en question. Si la barrière fonctionne en mode continu, l'équation (III.1) est applicable pour calculer la fréquence de la conséquence d'un scénario pour lequel la fréquence de l'événement initiateur est deux fois inférieure à la fréquence du test.

Une sollicitation élevée survient quand la fréquence de défaillance pour une IPL est deux fois supérieure à la fréquence du test de cette IPL (Ex : IPL testée 1 fois/an et sollicitée plus de 2 fois/an). Ainsi, la fréquence de la conséquence ou la fréquence de défi contre l'IPL suivante peut être donnée par (CCP, 01):

$$f_i^C = 2 \times (\textit{ fréquence du test de IPL / an}) \times \textit{PFD de IPL} \qquad \text{(III.3)}$$

Dans le cas où on a des IPLs multiples, la fréquence de défaillance de la première IPL doit être comparée à la fréquence de test de l'IPL suivante et ainsi de suite.

La formule de Kletz peut être utilisée dans le cas d'une demande basse ou élevée :

$$f_i^C = f_i^{IPLi}(1 - e^{-DT/2}) \qquad \text{(III.4)}$$

Où :

f_i^C : la fréquence de la conséquence C pour l'événement initiateur i ;

f_i^{IPLi} : la fréquence de défaillance d'une IPL qui protège contre la conséquence C pour un événement initiateur i.

D : le taux de demande avec lequel l'IPL est appelée à agir (an^{-1}) pour un scénario avec une seule IPL, c'est la fréquence de l'événement initiateur.

T : l'intervalle du test de l'IPL (an).

III.2.2.6 Calcul de l'indice du risque (R_K^C): S'obtient en combinant la fréquence de la conséquence indésirable et sa gravité en utilisant l'équation :

$$\boldsymbol{R_K^C = f_K^C \cdot C_k} \qquad \text{(III. 5)}$$

Où :

R_K^C : Indice du risque, il est exprimé par l'amplitude de la conséquence K par unité de temps (ex., nombre de morts / an).

f_K^C : Fréquence de la conséquence K (an^{-1}, h^{-1}, etc.).

C_k : Gravité de la conséquence (nombre de morts /an, perte économique/mois, etc.)

Il est à souligner que la conséquence représentant la sortie indésirable doit être exprimée comme une mesure d'un seul nombre afin de pouvoir appliquer l'équation (III.5). Dans le cas de plusieurs scénarios affectant la même cible (géographique ou processus), les fréquences de ces scénarios doivent être additionnées pour avoir une fréquence globale, en utilisant l'équation suivante :

$$f^C = \sum_{i=1}^{K} f_i^C = f_1^C + f_2^C + f_3^C + f_4^C +, \ldots, f_k^C \qquad \text{(III.6)}$$

Où :

f^C : Fréquence globale des scenarios de même catégorie.

f_k^C : Fréquence de la conséquence C résultant de l'événement initiateur k.

Il faut noter que, dans le cadre de la méthode LOPA, chaque scénario (un couple événement initiateur- conséquence) doit être évalué séparément avec ses IPL respectives (CCP, 01).

Les résultats de calcul obtenus, en utilisant les équations (III.1) et (III.6), seront exploités pour comparer le risque évalué aux critères d'acceptabilité préalablement établis afin de juger s'il est acceptable ou non.

III.2.2.7 Evaluation du risque par rapport aux critères d'acceptabilité : La dernière étape de toute analyse de risques (qualitative ou quantitative) est la prise de décision sur l'acceptation du risque. Ce qui revient à s'assurer que le risque est bien maitrisé par rapport aux critères d'acceptabilité préalablement définis. Durant cette étape, on propose des alternatives et on choisit l'alternative la plus adéquate pour contrôler le risque. On prend des mesures de sécurité ou on réalise toute autre action qui aura pour but de ramener le risque à un niveau acceptable (Kum, 93), (Mar, 02).

La méthode LOPA est souvent utilisée pour juger si un scénario d'accident obéit aux critères d'acceptabilité du risque. Deux principales méthodes de prise de décision sur les risques sont utilisées dans le contexte de cette méthode :

- ***La méthode prédominante est de comparer le risque calculé à un critère de risque tolérable prédéfini :***

Pour cette méthode, l'occurrence d'un scénario d'accident est estimée par une fréquence appelée « fréquence d'occurrence » qui sera comparée aux critères d'acceptabilité établis préalablement par des établissements spécialisés. Ces critères sont fonction du contexte de chaque établissement concerné.

Bien entendu, les critères d'acceptabilité peuvent être explicites ou implicites. Les critères explicites incluent des valeurs pour le risque acceptable et/ou des valeurs pour réduire le risque à un certain niveau tolérable ALARP. Ces dernières peuvent être exprimées par une seule valeur, une zone sur un graphe ou bien une matrice de risque. Les critères implicites sont typiquement définis par des procédures pour sélectionner le nombre d'IPL nécessaire afin de réduire la gravité des conséquences potentielles.

Généralement, ces critères sont classés selon les catégories suivantes (CCP, 01), (Deb, 03):

- Critère défini par les matrices de risque en termes de fréquences et de gravité. Ces matrices contiennent généralement trois zones (par exemple, risque inacceptable, risque tolérable et risque acceptable). A chaque zone de la matrice est associé un degré de réduction de risque exigé pour un scénario qui se trouve dans cette zone.

- Critère qui spécifie le nombre minimal d'IPL exigé pour un scénario d'un certain niveau de conséquence et de fréquence. Chaque IPL est caractérisée par un nombre de crédit qui correspond à une réduction de la fréquence d'un événement de 10^{-2} (c.à.d. un facteur de réduction de 100).

- Critère numérique qui spécifie le risque maximum tolérable : vue la clarté et la simplicité de ce type de critères, il est préféré par certaines compagnies et exigé par certaines lois (Mar, 02), (HSE, 01) qui trouvent plus commode d'avoir un critère de risque numérique exprimé en termes de fréquence maximale tolérable(une valeur unidimensionnelle simple) par scénario, basé sur une variété de catégories de conséquences (CCP, 09).

En utilisant les critères quantitatifs de risque, les compagnies peuvent développer des directives pour la prise de décision qui répondent aux exigences d'ALARP (Mar, 02).

Certaines compagnies ont développé un critère global basé sur un risque tolérable maximum par unité de production, par zone géographique, ou risque cumulatif par personne (CCP, 00), (CCP, 01), (Mar, 02), (CCP, 09). La définition des critères de risque pour une usine nécessite l'établissement d'une base pour évaluer raisonnablement la contribution des différents scénarios de risque de l'installation entière. En supposant une contribution additive de tous les scénarios potentiels, on peut définir une valeur globale (intégrale) de risque comme étant la somme des contributions de ces scénarios de risque.

Le résultat de l'équation (III .1) peut être utilisé comme entrée pour comparer le risque calculé aux critères de risque pour des prises de décisions concernant la réduction de risque basée sur des critères quantitatifs. En se référant aux catégories de conséquences, certaines compagnies définissent des objectifs exprimés par la fréquence de risque incluant par exemple la fréquence tolérable des scénarios ayant un potentiel de causer des pertes humaines (PLL : Probable Loss of Life) (CCP, 01), (Mar, 02). Ainsi, la réduction du risque requise est proportionnelle à la différence entre la fréquence non atténuée et la fréquence tolérable maximum pour la conséquence considérée.

Réduire le risque réel à un niveau tolérable est assuré par un facteur de réduction de risque (*RRF*) associé à une couche de protection (IPL) et égal à la valeur inverse de sa *PFD*. Pour un scénario potentiel donné avec une conséquence indésirable C, pouvant conduire à une fatalité ou plus, lorsque la fréquence f_i^C dépasse la fréquence du risque maximum tolérable (qui est dans notre cas un critère global), noté *TR*, la PFD_{IPL} est une variable donnée par :

$$f_i^C \times PFD_{PL} \leq TR \qquad \text{(III.7)}$$

En utilisant l'équation : $$\mathrm{RRF} = \frac{1}{\mathrm{PFD}_{\mathrm{PL}}} \qquad \text{(III.8)}$$

On obtient : $$RRF_{PL} \geq \frac{f_i^C}{TR} \qquad \text{(III.9)}$$

Le rapport $\frac{f_i^C}{TR}$ correspond donc au *RRF* minimum exigé (M*RRF*) pour atteindre *TR*.

- ***La méthode de jugement d'expert :***

La méthode de jugement d'expert est nécessaire lorsque les critères spécifiques de risque tolérable ne sont pas disponibles en raison de la nouveauté du processus ou de sa complexité (CCP, 01), (Mar, 02). En outre, les décisions concernant des IPL supplémentaires et leur nature sont généralement basées sur les avis d'experts en évaluation des risques. En se référant à leurs propres expériences, les experts comparent les IPL et d'autres caractéristiques des scénarios aux pratiques de l'industrie ou aux procédés similaires.

III.3 Formalisme de la méthode LOPA

Un tableau de synthèse type est donné en annexe F de la norme IEC 61511-3 (IEC, 03) est et recommandé pour établir un compte rendu de l'analyse des risques par la méthode LOPA. Le tableau III.1 illustre une adaptation de ce formulaire type. Il s'agit d'un incendie résultant de l'inflammation d'une vapeur inflammable suite à un dégagement lors de la rupture d'une colonne de distillation.

La colonne 1 indique l'événement redouté et la colonne 2 permet de coter sa gravité. La colonne 3 décrit l'Evénement Initiateur (EI) et la colonne 4 cote sa fréquence. Les colonnes de 5 à 9 permettent de décrire les différentes couches de protection et d'indiquer leurs probabilités de défaillance à la demande (PFD). La colonne 10 indique le résultat de la combinaison de la fréquence de l'EI et les PFD des IPLs. La colonne 11 permet d'introduire une atténuation supplémentaire à l'aide d'un Système Instrumenté de Sécurité en indiquant son Niveau d'Intégrité de Sécurité (SIL). La colonne 12 indique le risque final réduit.

Tableau III.1 : Tableau d'analyse de LOPA (IEC, 03)

1	2	3	4	5	6	7	8	9	10	11	12	13
Événement *d'impact* (redouté)	Niveau de gravité	Causes initiales	Probabilité des causes initiales	Couches de protection					Fréquence *de l'événement* intermédiaire	Niveau *d'intégrité* SIF	Fréquence de *l'événement* réduit	Remarque
				Conception Procédé	BPCS	Alarmes	Barrières mitigation	Réduction Supplémen-taire IPL				La haute pression provoque la rupture de la colonne de distillation
Incendie colonne de distillation	S*	Perte de refroidi-ssement	0,1	0,1	0,1	0,1	0,1	PRV01	10^{-7}/an	10^{-2}	10^{-9}/an	

*Niveau de gravité : Sévère

III.4 Avantages, limites de la méthode LOPA conventionnelle

La méthode LOPA présente plusieurs avantages (CCP, O1), (Kir, 05), (Ken, 10) :

- C'est un outil performant et efficace d'évaluation des risques et de prise de décision quant aux mesures de protection et de réduction.
- C'est est un outil simple et flexible permettant de déterminer la réduction apportée par chaque mesure de réduction (IPL) en lui attribuant des probabilités de défaillance.
- Elle permet de déterminer le SIL associé au SIS.
- C'est un outil d'estimation des conséquences limites.
- C'est est un outil d'aide à la décision quant à l'acceptabilité du risque.
- En la comparant à d'autres méthodes d'analyse des risques telles que l'arbre de défaillance, la méthode LOPA exige moins du temps et moins de coûts pour sa réalisation. Cette caractéristique lui confère la possibilité d'être appliquée à un grand nombre de scénarios qui sont quantitativement difficiles à évaluer.

Cependant, la méthode LOPA présente également des limites (CCP, O1), (Kir, 05) :

- La limitation relative à la prise en compte d'un scénario résultant d'un simple couple cause-conséquence.

- LOPA est un outil qui ne peut pas être appliqué pour étudier tous les scénarios d'accidents surtout ceux qui présentent des combinaisons des défaillances.
- L'objectivité et l'efficacité des résultats de LOPA dépendent de la disponibilité des données, alors qu'en réalité on ne peut pas se passer des jugements d'experts et des bases de données.

LOPA utilise des données sous forme de grandeurs typiques pour la fréquence de l'événement initiateur, la gravité de la conséquence et les probabilités de défaillance à la demande des couches de protection pour évaluer le risque d'un scénario.

Les données sur les défaillances utilisées devraient être représentatives de l'industrie ou du système étudié et n'être utilisées que si elles sont statistiquement significatives. Autrement dit être disponibles sur une période de temps adéquate. Les tableaux III.2 et III.3 montrent un exemple de données issues de la littérature (CCP, 01), (IEC, 03), (ICS, 09).

Quand de telles données ne sont pas disponibles, le jugement d'experts devrait être utilisé pour estimer les données de défaillances (Lan, 07). Les analystes utilisent généralement la valeur moyenne pour évaluer les paramètres du risque. Or, cette moyenne n'étant pas généralement représentative à cause de la dispersion des données recueillies dans un environnement incertain et delà, ne donnant pas une idée précise sur la variation du paramètre de risque en question.

Tableau III.2 : Valeurs typiques des fréquences de l'événement initiateur (CCP, 01)

Evénement initiateur	Intervalle de fréquence (par an)	Exemple de valeurs choisies pour LOPA
Défaillance du séparateur due à la pression résiduelle	10^{-7} - 10^{-5}	10^{-6}
Défaillance du réservoir de stockage atmosphérique	10^{-5} - 10^{-3}	10^{-3}
Ouverture intempestive de la vanne de sécurité	10^{-4} - 10^{-2}	10^{-2}
Défaillance de la pompe (étanchéité)	10^{-2} - 1	10^{-1}
Défaillance du joint de la pompe	10^{-2} - 10^{-1}	10^{-1}
Défaillance du régulateur	10^{-1} - 1	10^{-1}
Incendie extérieur important	10^{-3} - 10^{-2}	10^{-2}
Défaillance humaine	10^{-3} - 10^{-1} Par opération	10^{-2} Par opération

Tableau III.3: Valeurs typiques de PFD des IPLs (CCP, 01)

IPL		PFD	Exemple de valeurs choisies pour LOPA
Digue		10^{-3} - 10^{-2}	10^{-2}
Système de drainage		10^{-3} - 10^{-2}	10^{-2}
Système d'ignifugeage		10^{-3} - 10^{-2}	10^{-2}
Arrêt Flamme et détonation		10^{-3} - 10^{-1}	10^{-2}
Soupape de sécurité		10^{-5} - 10^{-1}	10^{-2}
Disque de rupture		10^{-5} - 10^{-1}	10^{-2}
Système de contrôle (BPCS)		10^{-2} - 10^{-1}	10^{-1}
Fonctions instrumentées de sécurité (SIF)	SIL 1	10^{-2} - 10^{-1}	-
	SIL 2	10^{-3} - 10^{-2}	-
	SIL 3	10^{-4} - 10^{-3}	-

III.5 Apport de la logique floue à l'analyse du risque

Comme discuté dans la section précédente, le problème majeur rencontré en analyse de risques, notamment lorsque des méthodes semi-quantitatives et quantitatives sont appliquées, est l'indisponibilité des données fiables et objectives pour l'évaluation des différents paramètres du risque. Par ailleurs, les résultats de cette évaluation constitueront les critères principaux de prise de décisions sur l'acceptabilité ou la réduction des risques analysés. Ainsi, il s'avère nécessaire de pouvoir manipuler ces données subjectives pour rendre l'évaluation plus précise et plus fiable.

Selon l'approche conservative (voir introduction du chapitre I), qui exige qu'en cas d''absence de données significatives ou de possibilité d'assimiler toutes les données disponibles, le risque devrait être surestimé pour représenter les conditions défavorables afin de compenser l'incertitude. Bien que le résultat de cette approche soit conservatif conduisant à la conception d'une intégrité de sécurité suffisante, il entraine des coûts d'installation et de maintenance plus élevés (Nai, 09).

Une autre alternative est de considérer des intervalles de confiance avec les bornes inférieures et supérieures pour quantifier les probabilités de défaillances, avec la certitude que la valeur de la probabilité ou de la fréquence est à l'intérieur de cet intervalle. Cependant, cette approche n'est pas entièrement satisfaisante puisqu'on prétend que les valeurs en dehors de l'intervalle ne sont pas possibles, une déclaration ferme (problème de rigidité). A ceci s'ajoute l'utilisation d'intervalles larges et noyés dans l'incertitude, issus

d'une statistique non fiable ou fournie par des experts par peur d'être sanctionné en cas d'erreur (Ken, 91), (Chu, 92), (Bow, 95), (San, 95), (Sal, 07), (Mar, 09).

En outre, plusieurs bases de données comme celle du Center for Chemical Process Safety (CCP, 89), la norme IEEE 500 (IEE, 84) et OREDA (ORE, 02) fournissent des intervalles. Bien que cette approche est très bien adaptée pour mener l'analyse dans le sens du pire des cas avec la présence de limites inférieures moins pessimistes, il semble que les intervalles de probabilité de certaines défaillances devraient être réajustés (Abr, 02). En effet, pour l'utilisation de ces données, il faut avoir des précisions sur l'état de l'art du système ou du processus et sur la politique de sécurité du site.

Une alternative plus rassurante et soutenue par plusieurs spécialises en sécurité des systèmes (Zad, 78), (Dub, 88a), (Bow, 95) est l'utilisation de la théorie de possibilités. Des nombres flous et plus généralement des intervalles flous pourraient être des représentations robustes de l'imprécision et de d'incertitude lorsque des informations empiriques (ou des données précises) sont très rares (Tan, 83), (Bow, 95), (Abr, 02), (Mur, 09). Dans ce cas, au lieu d'utiliser des probabilités de défaillance, on peut utiliser des possibilités de défaillance autrement dit des probabilités de défaillance floues subjectivement attribuées aux partitions.

La logique floue semble offrir un cadre très adéquat pour l'évaluation des risques en présences de données imprécises et incertaines (Zad, 75), (Bou, 95), (Mar, 10). La théorie des ensembles flous (Zad, 65) a émergé comme outil très approprié pour le traitement de l'incertitude dans la fiabilité et l'analyse de sécurité. Dans cet objectif, plusieurs modèles flous (§ I.2, Chapitre I) ont été développés pour traiter les comportements des systèmes trop complexes ou trop mal définis pour admettre des techniques quantitatives conventionnelles (Tan, 83), (Ken, 91), (Bow, 95), (Nai, 09), (Mar, 11). Ces modèles sont proposés pour résoudre les problèmes liés à l'imperfection des connaissances impliquées dans ces méthodes en utilisant des systèmes d'inférence floue ou /et l'arithmétique floue.

Dans ce contexte, Markowski et Mannan (Mar, O6), (Mar, 07), (Mar, 09) ont développé une approche floue de LOPA basée sur la logique floue pour évaluer les risques majeurs inhérents à l'industrie de process. Ces modèles prennent en compte la fréquence de la conséquence réduite, la gravité des conséquences et le niveau du risque. La fréquence est calculée en utilisant la multiplication floue appliquée au scénario d'accident représenté par

un AdE. La gravité est considérée comme une variable en introduisant un indice de réduction de la gravité obtenu par un système d'inférence floue. Le niveau de risque est évalué à partir d'une matrice de risque floue à base d'inférence floue. Les résultats issus de ces modèles flous sont très encourageants, les valeurs de risque sont plus précises que ceux indiquées par LOPA classique.

En se référant au modèle de Markowski et de Mannan (Zun, 08), une LOPA floue a été adaptée pour représenter la connaissance disponible dans les normes et issue de la pratique de l'industrie pour les systèmes de réfrigération d'ammoniac. Des systèmes d'inférence floue sont développés pour le calcul de la gravité et du risque. Les indices de gravité et de risque ont été obtenus à partir de trois variables d'entrée : le nombre de vies menacées, de blessures ou de morts, nombre de blessures et le type de soins médicaux requis. La méthodologie est appliquée à quatre scénarios. Les indices de risque calculés sont comparés à ceux obtenus par LOPA conventionnelle. En concluant, on peut dire que LOPA floue a donné de bonnes approximations du risque pour les systèmes de réfrigération d'ammoniac.

Dans un travail récent, Khalil et al. (Kha, 12) ont développé une LOPA floue en cascade. Le modèle est constitué deux systèmes de base : le premier pour déterminer la gravité d'un scénario d'accident en se basant sur des aspects économique et de sécurité, le deuxième pour déterminer le niveau d'intégrité de sécurité (SIL) pour une fonction instrumenté de sécurité (SIF). Le résultat étant la gravité prédéterminée et la fréquence du scénario. Les deux modèles sont construits à l'aide de systèmes d'inférence floue. Les résultats expérimentaux ont montré que le modèle LOPA floue en cascade maintient le SIL à des limites acceptables.

Dans le même contexte, une autre approche LOPA floue, qui peut être considérée comme faisant partie d'une « analyse quantitative floue des risques (FQRA: Fuzzy Quantitative Risk Analysis) », est développée dans la présente thèse. La section suivante sera consacrée à la présentation de cette approche.

III.6 Présentation du modèle LOPA floue proposé

Une nouvelle approche LOPA floue est proposée dans cette thèse pour traiter les incertitudes associées aux valeurs de la fréquence de l'événement initiateur et les PFD des

IPLs (Oua,13). Le modèle LOPA floue proposé se distingue des modèles précédents par deux différences principales, en l'occurrence :

- Le risque est dans ce cas exprimé par la fréquence d'une conséquence indésirable. Ainsi, le critère d'acceptabilité se réfère à une fréquence de risque tolérable maximum plutôt qu'au score obtenu du croisement par matrice de criticité.
- La question de la réduction du risque par ce modèle est abordée en considérant une approche possibiliste.

Les différentes étapes de cette approche sont présentées dans ce qui suit (Fig. III.7).

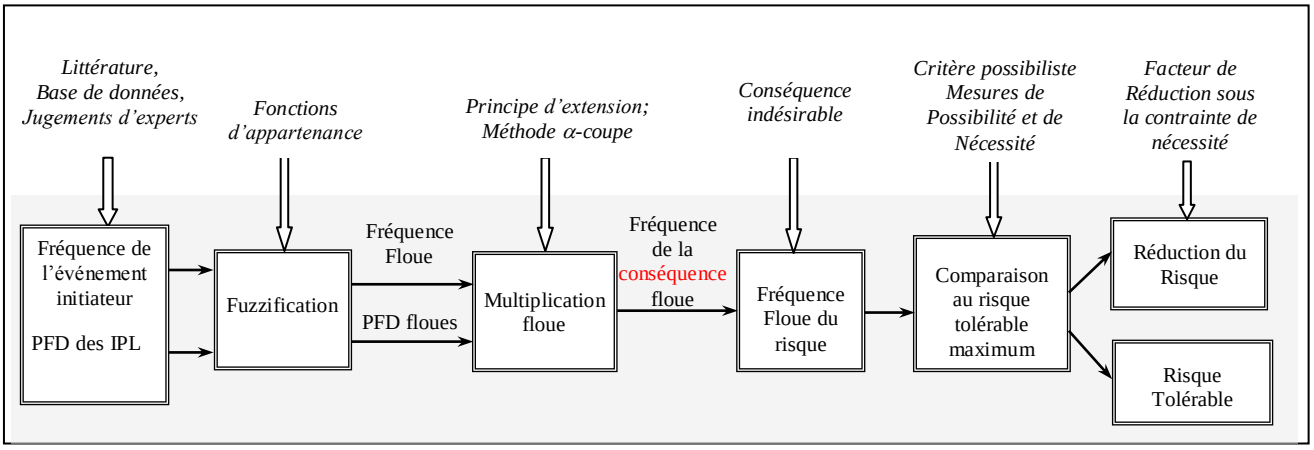


Fig. III.7 : Procédure globale de LOPA floue

III.6.1 Fuzzification

La première étape est de fuzzifier les valeurs et/ou les intervalles ordinaires, fournis par la littérature, les bases de données et/ou le jugement experts, en utilisant le concept de possibilité (ou de probabilité floue) (Zad, 78), (Tan, 83).

La possibilité est un ensemble flou défini dans un espace de probabilités. Dans ce travail, les possibilités de défaillance sont des nombres flous définis sur [0, 1] avec des fonctions d'appartenance triangulaires pour des raisons de simplification, c.à.d. un noyau avec une seule valeur modale au lieu d'un intervalle comme montré sur la figure III.8. La représentation triangulaire, comme il sera évoqué dans la dernière étape du modèle, mène à une approximation raisonnable de l'appartenance de la fréquence floue.

Comme déjà démontré (§ I.3.2.5 du chapitre I), un nombre flou peut être décomposé en α-coupes (Zad, 75). Soit $\tilde{P}$ et P_α, respectivement, un nombre flou et ses α-coupes. Donc $\tilde{P}$ peut être écrit comme l'union des produits α. P_α, avec α comprise entre 0 et 1:

$$\tilde{P} = \bigcup_{\alpha=0}^{\alpha=1} \alpha \cdot P_\alpha \qquad \text{(III.10)}$$

Avec :

$$P_\alpha = \left\{ p \in [0,1] \middle| \mu_{\tilde{P}}(p) \geq \alpha \right\} \qquad \text{(III.11)}$$

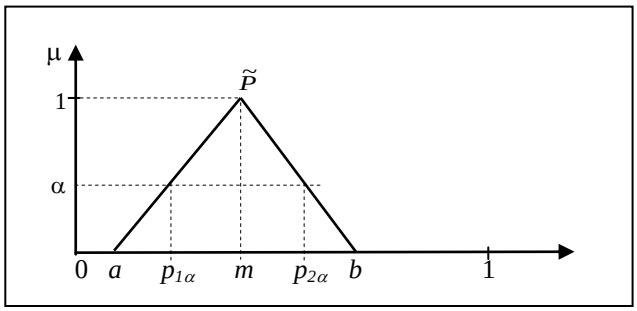


Fig. III.8 : Exemple de probabilité floue

La progression dans le degré d'appartenance donne un moyen commode de caractériser l'imprécision et l'incertitude qui peuvent affecter la fréquence de l'événement initiateur et les PFD des IPL. La valeur modale *m* où μ (m)=1 correspond à la valeur totalement possible.

III.6.2 Calcul de la fréquence floue de la conséquence réduite

La deuxième étape de ce modèle est l'évaluation floue de la fréquence de la conséquence réduite. Cette évaluation est basée sur l'utilisation du principe d'extension (§ I.3.2.7 du chapitre I) par lequel les opérations sur des nombres réels sont étendues aux opérations sur des nombres flous (Zad, 75). Dans la pratique, la mise en œuvre de la procédure de calcul n'est pas triviale car elle correspond à un problème de programmation non linéaire. Il est facile de montrer que les opérations arithmétiques floues sont équivalentes aux opérations arithmétiques d'intervalles correspondantes pour chaque α-coupe avec $0 \leq \alpha \leq 1$. Cette méthode fournit une solution discrète mais exacte pour étendre les opérations arithmétiques d'une manière très simple et efficace (Kau, 91). La fréquence

floue de la conséquence réduite est obtenue en utilisant l'équation (III.1) par la multiplication étendue, notée par ⊗, est donnée par :

$$\tilde{f}_i^C = \tilde{f}_i^I \otimes \prod_{j=1}^{J} \tilde{PFD}_{ij} \qquad \text{(III.12)}$$

Où :

$\tilde{f}_i^C$ est la fréquence floue de la conséquence C pour l'événement initiateur i;

$\tilde{f}_i^I$ est la fréquence floue de l'événement initiateur i;

$\tilde{PFD}_{ij}$ est la possibilité de défaillance à la demande de la j^{éme} IPL qui protège contre la conséquence C pour l'événement initiateur i.

En utilisant la méthode des α –coupes :

$$\tilde{f}_i^C = \bigcup_{\alpha=0}^{\alpha=1} \left(\alpha \cdot f_{\alpha i}^I \cdot \prod_{j=1}^{J} \alpha \cdot PFD_{\alpha ij} \right) \qquad \text{(III.13)}$$

Où : $f_{\alpha i}^I$ et $PFD_{\alpha ij}$ correspondent aux α-coupes.

III.6.3 Comparaison avec la fréquence du risque maximum tolérable

Comme il a été expliqué dans la section III.2.2 (étape 7), la prise de décision sur la réduction du risque est basée sur la comparaison de la fréquence calculée $\tilde{f}_i^C$ avec la fréquence du risque tolérable maximum *TR*. Lorsqu'il s'agit de valeurs uniques, cette comparaison est une question simple qui obéit à la relation (III.7). Cependant, ce n'est pas le cas lorsqu'on compare des quantités floues. En effet, il est parfois difficile de prétendre d'une manière absolue qu'une valeur floue est supérieure ou inférieure à une autre. Le seul cas où on peut dire qu'un nombre flou $\tilde{A}$ est inférieur ou égal à un nombre flou $\tilde{B}$ ($\tilde{A} \leq \tilde{B}$) c'est dans le cas où $a_1^\alpha \leq b_1^\alpha$ et $a_2^\alpha \leq b_2^\alpha$ pour chaque α-coupe, comme illustré par la figure III.9.

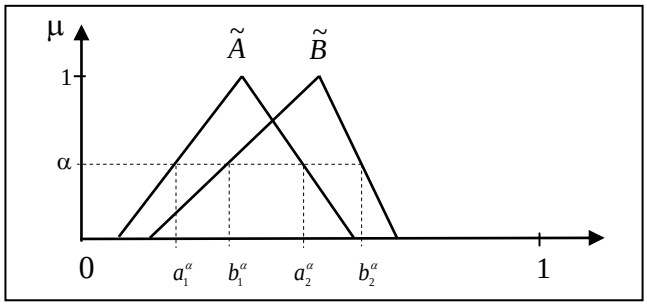


Fig. III.9 : Comparaison de deux nombres flous

Dans ce contexte, de nombreux travaux de recherche ont été consacrés au problème de classement de quantités floues. Une revue des différentes méthodes développées est donnée dans les références (Dub, 83), (Bor, 85), (Dub, 99a).

Dans le cadre de la théorie de possibilités (Zad, 78), ((Dub, 88a), à partir d'une distribution de possibilité, on peut définir différentes mesures d'incertitudes pour caractériser un événement donné. Une distribution de possibilité est une application π d'un univers de discours $U = \{u\}$ à l'intervalle unitaire [0, 1]. Elle représente une restriction floue sur les valeurs possibles d'une variable X. Soit $\tilde{F}$ un ensemble flou de U qui se caractérise par sa fonction d'appartenance $\mu_{\tilde{F}}$. Si $\tilde{F}$ décrit par exemple, le concept de label "élevé" qui signifie que les valeurs possibles pour X sont celles compatibles avec le concept "élevé", ce qui conduit à une distribution de possibilité $\pi_X = \mu_{\tilde{F}}$ avec $\pi_X(u)$est la possibilité que $X = u$.

Étant donné un ensemble flou $\tilde{A}$ de U et la possibilité de distribution π_X qui prend ses valeurs dans U, les mesures de possibilité et de nécessité (certitude) de $\tilde{A}$, désignées respectivement par Π et N, sont définies par (Dub, 88a) :

$$\Pi_{\tilde{F}}(\tilde{A}) = \sup_{u \in U} \min\left(\mu_{\tilde{A}}(u), \pi_X(u)\right) \qquad \text{(III.14)}$$

$$N_{\tilde{F}}(\tilde{A}) = 1 - \Pi_{\tilde{F}}(\overline{\tilde{A}}) = \inf_{u \in U} \max \left(\mu_{\tilde{A}}(u), 1 - \pi_X(u)\right) \qquad \text{(III.15)}$$

Où $\overline{\tilde{A}}$ est le complément de $\tilde{A}$, il évalue à quel point $\tilde{A}$ est compatible avec π_X qui représente l'état actuel des connaissances, et $N_{\tilde{F}}(\tilde{A})$ évalue à quel point $\tilde{A}$ est certainement impliqué par π_X (degré d'inclusion de $\tilde{F}$ dans $\tilde{A}$). Le degré de nécessité de $\tilde{A}$ est le degré d'impossibilité de $\overline{\tilde{A}}$.

Comme il existe une relation d'ordonnancement entre la fréquence de la conséquence et le risque tolérable maximum TR, il faut considérer le problème de comparaison d'une quantité floue à un nombre unique, en utilisant les mesures de possibilité et de nécessité. En considérant l'inégalité $p \le r$, où p est une variable possibiliste à l'intérieur d'un intervalle flou Q et r est un nombre unique, on peut définir l'ensemble des nombres possibles (respectivement nécessaires) supérieurs ou égaux aux valeurs de p. Ils sont désignés respectivement par $[Q, +\infty)$ et $]Q, +\infty[$, et définis par (Dub, 83) :

$$\mu_{[Q,+\infty)}(r) = \Pi_Q((-\infty, r]) = \sup\{\mu_Q(p) | p \le r\} \qquad \text{(III.16)}$$

$$\begin{aligned} \mu_{]Q,+\infty)}(r) &= N_Q((-\infty, r[) = \inf\{1 - \mu_Q(p) | p > r\} \\ &= 1 - \sup\{\mu_Q(p) | p > r\} \end{aligned} \qquad \text{(III.17)}$$

Où Π_Q et N_Q sont respectivement, les mesures de possibilité et de nécessité définies par la distribution μ_Q.

Considérons l'inégalité floue $\tilde{f}_i^C \le TR$, ces deux mesures comme indices de classement peuvent être écrites comme suit (Fig. III.10):

$$Pos(\tilde{f}_i^C \le TR) = \sup\left\{ \mu_{\tilde{f}_i^C}(p) | p \le TR \right\} \qquad \text{(III.18)}$$

$$Nes(\tilde{f}_i^C \le TR) = 1 - \sup\left\{ \mu_{\tilde{f}_i^C}(p) | p > TR \right\} \qquad \text{(III.19)}$$

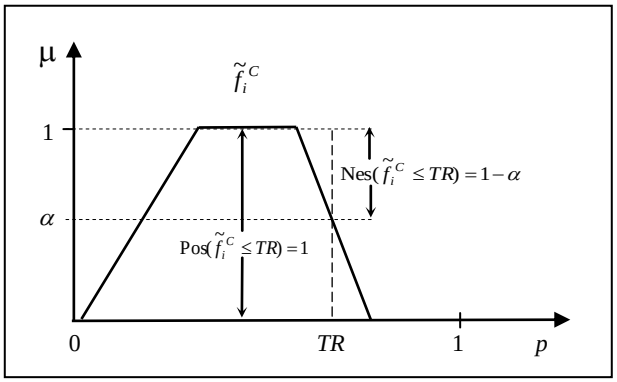


Fig. III.10 : Mesures de Possibilité et de nécessité de $\tilde{f}_i^C \le TR$

III.6.4 Prise de décision dans un environnement flou

La prise de décision concernant un risque revient à placer ce dernier dans une des catégories suivantes :

1- Maintenir le risque à son niveau actuel (supposé être tolérable) par le système de management de la sécurité (SMS),
2- Réduire le risque pour le rendre tolérable en ajoutant d'autres barrières de sécurité,
3- Le risque est si élevé qu'il exige des changements de la conception du processus ou l'élimination des procédures et des opérations. Ce type de décision est pris après une analyse approfondie comprenant l'évaluation quantitative des risques (QRA).

Une grande partie du processus de prise de décision dans les applications réelles a eu lieu dans un environnement flou (Bel, 70), (Mue, 07). Ceci se rapporte à un processus de décision dans lequel les objectifs et/ou les contraintes sont imprécis et/ou incertains. Dans l'évaluation quantitative des risques (QRA), le choix de n'importe quelle décision sur le risque dépend principalement des résultats issus de la comparaison du risque calculé avec le risque maximal tolérable. Cependant, les experts en matière de gestion des risques sont habituellement consultés quand les critères de risque ne sont pas disponibles ou mal définis (CCP, 01).

Dans le contexte de notre travail, l'utilisation de la théorie des ensembles flous comme outil d'aide à la décision quant à la réduction du risque se réfère à la fréquence floue de la conséquence dans la mesure où nous devons traiter l'inégalité floue $\tilde{f}_i^C \le TR$ où $\tilde{f}_i^C$ est une quantité floue. Un problème du type : « le risque par scénario doit être sensiblement

inférieur à TR » devrait être résolu. On cherche à déterminer des résultats satisfaisants plutôt qu'une solution optimale pour ce problème.

La programmation mathématique floue, basée sur la théorie des ensembles flous et la théorie des possibilités, est développée pour traiter des décisions dans un environnement flou. La prise de décision à base de logique floue fournit un cadre naturel pour traiter des représentations vagues comme plus grand, plus petit, satisfaisant, suffisant, etc.

La prise de décision floue a été initialement développée par Bellman et Zadeh (Bel, 70) qui ont considéré le problème de prise de décision sous des objectifs flous et les contraintes définies en tant qu'ensembles flous dans un espace d'alternatives.

En théorie de possibilité, un autre type de programmation floue a été développé (Inu, 00). Il traite des coefficients ambigus et imprécis des fonctions objectives et de contraintes.

La prise de décision possibiliste détermine, à partir d'un ensemble donné de distributions de possibilités, l'information disponible.

Une contrainte floue qui est un événement floue peut être satisfaite avec certains degrés de possibilité et / ou de nécessité prédéfinis (Inu, 00), (Das, 07). Dans LOPA, ces contraintes de possibilité et de nécessité peuvent être imposées conformément à la politique de sécurité de l'entreprise. La prise de décision possibiliste proposée vise à réduire la fréquence floue de la conséquence sous une contrainte de la nécessité.

Cette approche peut se référer au concept de «la réduction nécessaire du risque» comme défini par la norme IEC 61511 (IEC, 03).

Nous considérons la situation de risque dans laquelle $\tilde{f}_i^C > TR$. La fonction de risque à minimiser peut être écrite comme suit :

$$\tilde{f}_i^* = \tilde{f}_i^C . x_{PL} \qquad \text{(III.20)}$$

Où $\tilde{f}_i^C$ est un intervalle flou désigné par le quadruplet (a, b, c, d) et x_{PL} est la PFD d'une couche de protection, comme variable de décision. Le problème de prise de décision possibiliste à propos du risque peut s'écrire sous la forme suivante :

$$\begin{cases} \min \tilde{f}_i^* \\ Nes\left(\tilde{f}_i^* \le TR\right) \ge \lambda \\ 0 < x_{PL} < 1 \end{cases} \qquad \text{(III.21)}$$

Où λ est un niveau de confiance de la contrainte floue, dont les valeurs appartiennent à]0, 1]. Le choix de cet intervalle garantit une certaine réduction de la fréquence, puisque la contrainte de possibilité $Pos(\tilde{f}_i^* \le TR) = 1$ sera à chaque fois satisfaite. La contrainte floue peut être résolue par une défuzzication basée sur l'interprétation de la relation (III.19). D'après la figure III.11, il est clair que l'approximation trapézoïdale des résultats de $\tilde{f}_i^*$ est de la forme :

$$\begin{aligned} Nes(\tilde{f}_i^* \le TR) &= 1 - sup\left\{\mu_{\tilde{f}_i^*}(p) \middle| p > TR\right\} \\ &= 1 - \alpha \end{aligned} \qquad \text{(III.22)}$$

Avec :

$$\alpha = \frac{d^* - TR}{d^* - c^*}$$

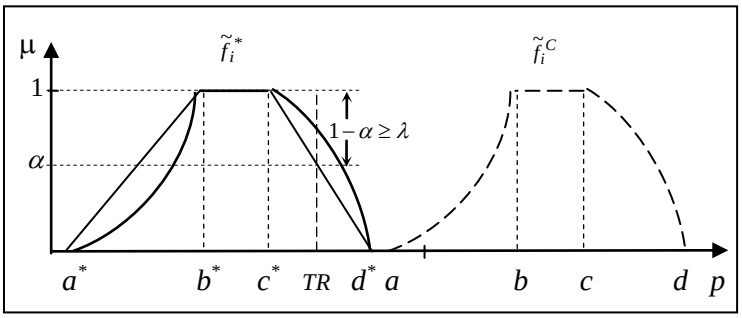


Fig. III.11 : Réduction de la fréquence sous une contrainte de nécessité

Les paramètres c^* et d^* sont obtenus de la relation (III.20) en considérant la méthode des α coupes pour α = 1 et α = 0, respectivement.

Ainsi, la relation (III.22) devient :

$$\alpha = \frac{d.x_{PL} - TR}{d.x_{PL} - c.x_{PL}} \qquad \text{(III. 23)}$$

En tenant compte de la contrainte floue (III.21), c'est-à-dire $1-\alpha \geq \lambda$, nous sommes arrivés à :

$$x_{PL} \leq \frac{TR}{d-(1-\lambda)(d-c)} \qquad \text{(III. 24)}$$

Le RRF peut être une variable de décision possible à déterminer. La relation (III.24) peut être écrite comme suit :

$$y_{PL} \geq \frac{d-(1-\lambda)(d-c)}{TR} \qquad \text{(III.25)}$$

Nous pouvons voir que le MRRF dépend de la valeur de λ. Plus cette valeur est élevée, plus l'investissement en termes de réduction des risques est important.

La fréquence réduite $\tilde{f}_i^*$ est calculée à partir de l'équation (III.20) en utilisant la méthode des α-coupes.

Conclusion

L'incertitude inhérente à l'analyse des risques constituent un sérieux problème dans la prise de décision concernant les risques. Avec peu d'informations et de statistiques, traiter les fréquences des événements initiateurs et les PFD des IPL comme des valeurs simples, est une manière controversée.

Nous avons proposé un modèle LOPA floue avec quatre principales caractéristiques:

- *L'utilisation des valeurs de possibilité, c.-à-d. probabilités floues ou fréquences floues, pour représenter les données d'entrée.*
- *L'utilisation de l'arithmétique floue pour calculer les fréquences floues des conséquences.*
- *La comparaison de ces fréquences avec la fréquence maximale tolérable à l'aide des mesures de possibilité et de nécessité.*

- *La mise en œuvre de la réduction nécessaire du risque par l'intermédiaire de la prise de décision possibiliste sur le risque. Pour ce dernier, nous avons traité un problème de réduction de risque sous une contrainte de nécessité. Étant donné que les fonctions d'appartenance des fréquences floues estimées pour les conséquences peuvent être non linéaires, cette résolution est largement facilitée à l'aide des approximations triangulaires ou trapézoïdales pour ces fonctions. La résolution a comme conséquence le MRRF qui dépend de la valeur d'un niveau de confiance qui sera appliquée aux fréquences floues (ou initiales) estimées.*

Pour vérifier et valider notre modèle, nous l'avons appliqué à un processus de traitement de gaz. Ceci fera l'objet du dernier chapitre de cette thèse.

Chapitre IV :

Validation des modèles flous proposés : Application à un système opérationnel

---

Résumé : *L'objectif de ce chapitre est de montrer l'opportunité des modèles flous proposés dans la gestion des risques industriels, en permettant d'une part, une prise en compte des aspects imprécis et incertains des données utilisées dans l'évaluation du risque. D'autre part, d'assurer une meilleure prise de décision en matière de prévention.*

Introduction

Dans le but d'illustrer l'applicabilité des modèles flous proposés et de montrer l'apport de la modélisation floue au traitement de l'incertitude liée aux données utilisées par les méthodes graphe de risque et LOPA, notre étude de cas s'est portée sur l'un des systèmes les plus sensibles de l'entreprise SONATRACH pouvant engendrer, en cas de défaillance, des conséquences humaines, matérielles, et environnementales critiques voire catastrophiques. Il s'agit du four rebouilleur destiné au traitement de gaz au niveau du complexe (SH/DP/HRM) Hassi R'Mel.

IV.1 Description du système

Le MPP3 est une station de compression qui permet de récupérer les hydrocarbures lourds (condensât et GPL) des gaz bruts recueillis à partir de nombreux puits et de produire des gaz traités (gaz de vente où gaz de réinjection). Le procédé de traitement de gaz est basé sur les éléments suivants :

• Gaz de refroidissement par échange thermique et simple relaxation (adiabatique).

• Détente supplémentaire par turbo-expander (isentropique).

• Température finale (- 40 °C).

La figure IV.1 représente un schéma simplifié du processus de production de gaz combustibles légers (gaz à vente). Ce procédé permet une meilleure récupération des hydrocarbures liquides, en commençant par la pré-séparation du gaz brut provenant des puits ensuite la compression au niveau de la station de pompage à une pression de 117 kg/cm^2 et une température de 62 °C. Dans la section de séparation à haute pression, les hydrocarbures liquides récupérés sont séparés en tant que gaz de pétrole liquéfié (GPL) et condensât dans le déethaniseur C101 de la section de fractionnement. Dès que les constituants légers sont extraits dans le déethaniseur C101 (composé de 28 clapets), le plateau accumulateur sépare le GPL du condensât. Pour éviter la formation des hydrates dans la partie supérieure de la colonne, on injecte une solution de glycol dans la conduite de reflux, cette solution est extraite à partir du plateau d'accumulation avec les hydrocarbures liquides. Les hydrocarbures liquides séparés sont envoyés en direction du plateau le plus élevé de la partie

inférieure du C101. Une partie de ces hydrocarbures est envoyée au moyen des pompes 31-P101 A et B vers le Four Rebouilleur H101 pour le réchauffage à 150 °C.

Le débit de l'hydrocarbure est régulé par la vanne de régulation motorisée FICA 136. Le fluide sortant du dispositif de chauffage à environ 180 °C est conduit vers le C101 de la colonne pour en extraire les gaz combustibles légers (gaz de vente).

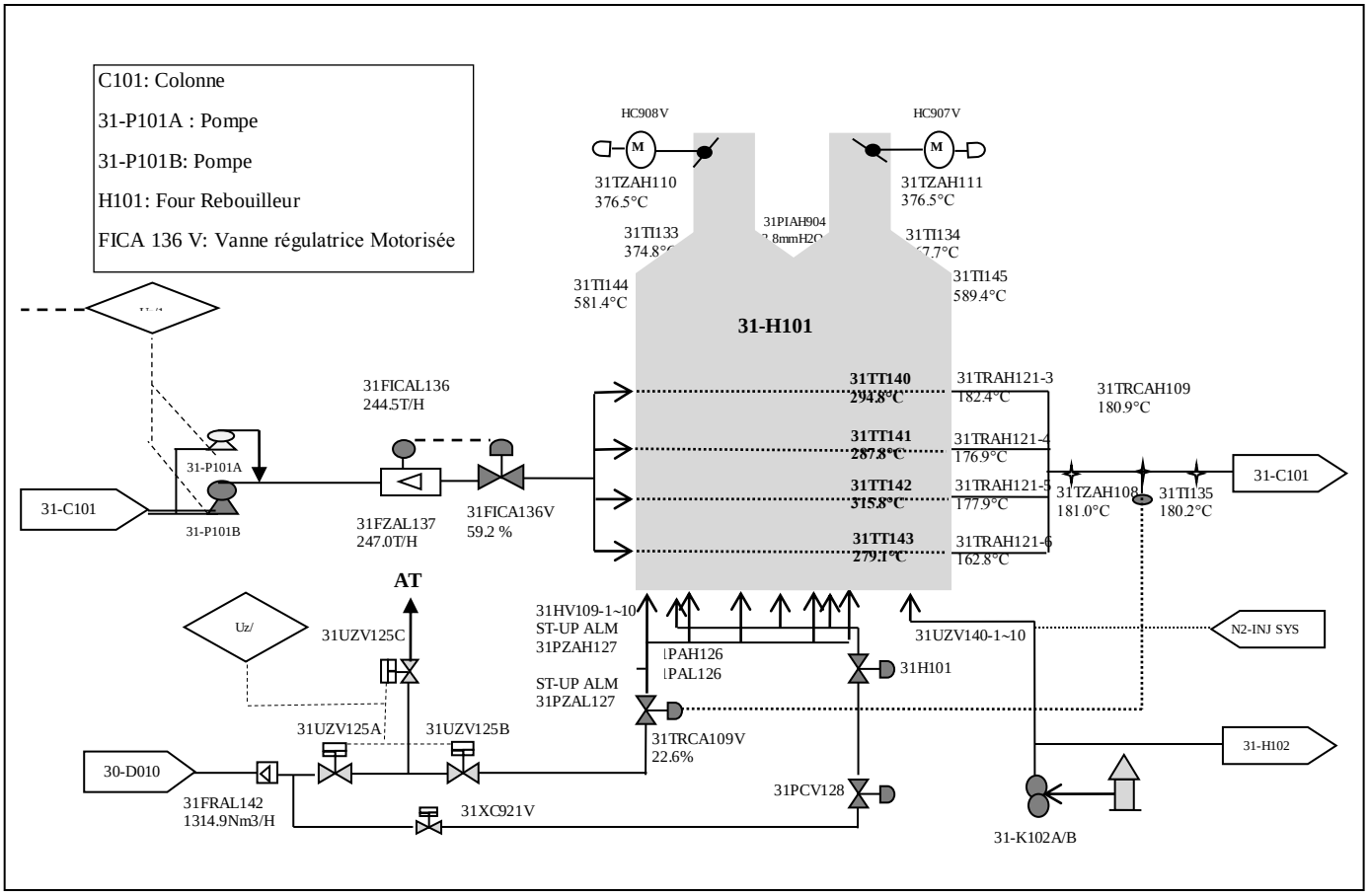


Fig. IV.1 : Four rebouilleur H101 : Organigramme flux du processus (SON, 08).

Notre étude se concentre particulièrement sur le H101 de chauffage qui est un équipement important dans la production de gaz combustibles légers qui sont composés de méthane et d'éthane.

IV.2 Analyse fonctionnelle du système four rebouilleur H101

Pour une meilleure description du système four rebouilleur H101, une analyse structurelle et fonctionnelle s'avère indispensable. Le but de cette analyse est de décomposer

le système et d'identifier ses différents composants ainsi que leurs fonctions. Les résultats de cette analyse (voir tableau IV.1) constitueront pour nous une base de données pour l'application de la démarche d'analyse proposée.

Tableau IV.1: Décomposition du système four rebouilleur H101

Sous système [Fonction Principale]	**Équipements** [Fonction Intermédiaire]	**Composant** [Fonction Elémentaire]
SS1 : Circuit d'alimentation [Alimentation du four rebouilleur]	E11 : Circuit Fuel Gaz [Assure l'alimentation en combustible]	C111 : Vanne TRCA-109V [Régulation du débit du combustible en fonction de la température du condensât]
		C112 : 10 Pilotes [Garantir une flamme continue pour l'amorçage du gaz]
		C113 : 10 Brûleurs [Assure le mélange air/combustible en vue d'obtenir une combustion complète]
	E12 : Circuit Liquide [Assure l'alimentation en liquide du fond de la colonne]	C121 : Vanne FICA-136V [Régulation du débit du condensât]
		C122 : Serpentin [Assure la circulation et l'échauffement du liquide]
SS2 : Sous-système de contrôle [contrôle les paramètres du procédés]	E21 : Équipement de contrôle (débit du condensât) [Contrôle le débit du condensât à l'entrée du four]	C211 : DCS (boucle de débit du condensât) [Adaptation du débit du condensât par action sur la vanne FICAL-136V] [Alerter l'opérateur quand le débit est insuffisant (≤ 150 t /h)]
		C212 : Débitmètre FICAL-136 [Mesure le débit du condensât à l'entrée du four]
		C213 : Indicateur de débit FI [Mesure le débit du liquide dans le four]
	E22 : Équipement de contrôle de dépression [Contrôle la dépression à l'intérieur du four]	C221 : DCS (boucle de dépression) [Adaptation de la dépression par action sur la vanne HC-908] [Alerter l'opérateur quand la dépression diminue (≥ 10 mmH_2O)].
		C222 : Vanne HXC-908 [Régulation de la dépression à l'intérieur du four par action sur le registre de tirage]
		C223 : Indicateur de dépression PIAH-904 [Mesure la dépression à l'intérieur du four]
	E23 : Équipement de contrôle de température [Contrôle la température du four]	C231 : DCS (boucles de température) [Adaptation de la température du condensât par action sur la vanne TRCAH-109 V], [Alerter l'opérateur quand la température augmente (≥ 295°C)].
		C232 : Thermocouple TRCAH-109 [Mesure la température du liquide à la sortie du four]
		C233 : Thermocouple TRAH-121 [Mesure la température à la sortie du serpentin]

		C334 : Indicateur de température TI [Mesure de température]
	E24 : Équipement de contrôle (débit du gaz combustible) [Contrôle le débit du gaz à l'entrée du four]	C241 : DCS (boucle de débit du gaz) [Alerter l'opérateur quand le débit du gaz diminue (≤ 1250 Nm^3/h)]
		C242 : Débitmètre FRAL-142 [Mesure le débit du gaz combustible à l'entrée du four]
	E25 : Équipement de contrôle (haute pression du gaz combustible) [Contrôle la pression du gaz à l'entrée du four]	C251 : DCS (boule de haute pression du gaz combustible) [Alerter l'opérateur quand la pression du gaz augmente (≥1,5 Kg/cm^2)]
		C252 : Switch de pression PAH-126 [Mesure la pression du fuel gaz]
	E26 : Équipement de contrôle (basse pression du gaz combustible) [Contrôle la pression du gaz à l'entrée du four]	C261 : DCS (boucle de basse pression du gaz combustible) [Alerter l'opérateur quand la pression du gaz diminue (≤0,4 Kg/cm^2)]
		C262 : Switch de pression PAL-126 [Mesure la pression du fuel gaz]
SS3: Sous-système de prévention [Assure la sécurité du procédé]	E31 : Équipement d'arrêt d'urgence. [Déclencher le four quand le débit du condensât est insuffisant (≤ 120 t /h)] [Déclencher le four quand la pression du gaz augmente (≥1,9 Kg/cm^2)] [Déclencher le four quand la pression du gaz diminue (≤0,4 Kg/cm^2)] [Déclencher le four quand la température des fumées augmente (≥ 600°C)] [Déclencher le four quand la température du condensât augmente (≥ 300°C)]	C311 : PLC (Programmable Logic Controller) [Assure les missions de mise en sécurité du four par action sur les vannes UZV 125 A, B et C]
		C312 : Débitmètre FZAL-137 [Mesure le débit du condensât à l'entrée du four]
		C313 : Switch de pression PZAH-127 [Mesure la pression du gaz combustible]
		C314 : Switch de pression PZAL-127[Mesure la pression du gaz combustible]
		C315 : Thermocouple TZAH-110/111[Mesure la température des fumées]
		C316 : Thermocouple TZAH-108 [Mesure la température à la sortie du four]
		C317 : Vannes UZV 125 A/B [Isolement de la ligne de gaz combustible]
		C318 : Vanne UZV 125 C [S'ouvre pour décomprimer la quantité de gaz qui reste entre les deux vannes UZV 125 A et B vers l'atmosphère]
SS4: Sous-système de protection [Maîtriser le feu]	E41 : Équipement de rideau d'eau [Réduire le rayonnement thermique de l'incendie aux adjacentes]	C411 : Vanne XC-901V [S'ouvre pour alimenter la couronne en eau]
		C412 : Couronne de refroidissement [Assurer la protection à l'eau pulvérisée pour le four]

	E42 : Équipement d'injection du N_2 [Fournir de l'azote pour l'étouffement et la maîtrise du feu]	C421 : Ballon D-450A/B [Stockage du N_2 sous pression] C422 : Vanne HXC-911V [S'ouvre pour fournir l'azote]

IV.3 Élaboration, sélection des scénarios d'accidents et analyse des barrières de sécurité

Identifier les scénarios d'accidents est une étape clé dans le processus d'analyse de risques. Les scénarios d'accidents représentatifs (SAR) sont sélectionnés en fonction des critères de risque établis par l'entreprise SONATRACH (SON, 07).

Nous nous intéressons, dans le cadre de cette thèse, aux scénarios ayant le potentiel d'entraîner des rejets de matières inflammables et, par conséquent, une perte de production.

Une analyse par la méthode HAZOP (HAZard and OPerabitity) (IEC, 01) est effectuée pour identifier les scénarios représentatifs. Les tableaux correspondants sont présentés en annexe (A1).

Le choix s'est porté sur trois scénarios résumés dans le tableau (IV.2).

IV.4 Détermination du SIL par la méthode graphe de risque conventionnel

Une fois les scénarios d'accident identifiés, il est alors à vérifier si une réduction est nécessaire pour chaque scénario retenu en utilisant, dans notre cas, la méthode graphe de risque qui a la particularité de donner des résultats sous forme d'exigence requise en termes de SIL.

Le four rebouilleur comporte, comme déjà décrit, un circuit d'arrêt d'urgence de nature instrumentée particulièrement conçu pour assurer la sécurité du personnel et protéger les appareillages contre tout incident ou accident. Les systèmes instrumentés de sécurité (indépendamment des systèmes de contrôle et de régulation (voir tableau IV.1)) pour lesquels il s'agit de déterminer le SIL, sont :

Tableau IV.2 : Scénarios d'accident relatifs au four rebouilleur H101

N°	Mot-guide	Élément	Déviation	Causes possibles	Conséquences	Protections
1	NE PAS FAIRE/ MOINS	Débit du condensât	Pas/ Moins de débit	Mauvais fonctionnement de la vanne FICA-136V (fermée)	Pas de liquide dans le H-101, endommagement du serpentin (incendie) & arrêt d'unité (arrêt possible du module)	- FICAL-136 : alarme (≤ 150 t/h) - Opérateurs - SIS -FZL-137 : (≤ 120 t/h) arrêt d'urgence du H-101
2	MOINS	Débit d'air	Moins de débit	Mauvais fonctionnement des HXC-908V/907V (trop fermés)	Combustion incomplète, pression élevée à l'intérieur du H-101, explosion possible & arrêt d'unité (arrêt possible du module)	-PIAH-904 : alarme (≥ 10 mmH_2O) - DG-130 : indication - Indicateur de position - Trappe d'explosion
3	NE PAS FAIRE/ MOINS	Débit de gaz combustible	Pas/ Moins de débit	Mauvais fonctionnement de la vanne UZ-125C (ouverte)	Pas de fuel gaz pour le H-101, baisse de pression et de température du fuel gaz à la sortie du H-101, Dégagement du fuel gaz en atmosphère, incendie & explosion possible & arrêt d'unité (arrêt possible du module)	- PAL-126 : alarme (≤ 0,4 Kg/cm^2) - PZL-127 : (≤ 0,2 Kg/cm^2) arrêt d'urgence du H-101 - FRAL-142 : alarme (≤ 1250 Nm^3/h) - TRCA-109 : indication

- le système d'arrêt d'urgence (FZAL-137, ESD, UZV-125V) qui déclenche le four quand le débit du condensat à l'entrée du four est insuffisant,

- le système d'arrêt d'urgence (PZAL-127, ESD, TRCA-109V) qui déclenche le four en cas de basses pression ou température du fuel gaz à l'intérieur du four.

Les scénarios d'accidents identifiés par la méthode HAZOP (Tab. IV.2) et qui seront analysés par la méthode graphe de risque sont:

- Incendie et Arrêt de l'unité de production, causé par la défaillance de la vanne de régulation du débit du condensât (FICA 136V) ou la défaillance de la vanne de sécurité (UZ-125C).

- Rejet de matières inflammables, causé par la défaillance de la vanne de sécurité (UZ-125C).

Notons à ce niveau, que nous nous intéressons en particulier dans ce travail aux SIS faiblement sollicités et que le modèle graphe de risque que nous allons utiliser pour déterminer le SIL des FIS sera celui proposé dans les directives d'UKOOA (Dea, 99), (Smi, 04), (Gul, 04) et représenté par la figure II.6 (Chap. 2).

IV.4.1 Données relatives aux paramètres C, F, P, W et au SIL

En se référant aux données du tableau II.6, une définition qualitative et quantitative des paramètres C, F, P et W est donnée.

Les résultats de cette analyse sont résumés dans le tableau IV.3.

Tableau. IV.3: Résultats d'application du graphe de risque conventionnel

Scenario	Conséquence (C)	Occupation (F)	Probabilité d'évitement (P)	Taux de demande (W)	SIL GRC
Scénario 1	C_b	F_B	P_A	W_2	SIL2
Scénario 2	C_c	F_A	P_A	W_1	SIL2

IV.4.2 Discussion des résultats

Au vu des résultats obtenus, on peut formuler le constat suivant :

Dans le cas du premier scénario, un débit faible du condensat résultant de la défaillance de la régulation (vanne FICA- 136) peut provoquer un incendie et, par conséquent, l'arrêt de l'unité de production. Il s'agit donc d'un événement initiateur qui peut être à l'origine d'un scénario d'accident selon la réponse des barrières de prévention disponibles. Le système instrumenté de sécurité installé a pour finalité, en cas de sollicitation, d'assurer la sécurité du procédé par action sur les vannes UZV-124 B et C, il doit répondre au moins aux prescriptions d'un SIL 2 afin de réduire le risque d'incendie à un niveau tolérable.

Quant au deuxième scénario, le rejet de matières inflammables dans l'atmosphère est provoqué par une diminution de pression et de température du fuel gaz à l'intérieur du four (ouverture de la vanne UZ-125C). Le SIS disponible sert à détecter cette dérive dangereuse (via TRCA 109) pour ensuite couper l'alimentation du four ; ce qui se manifeste par l'arrêt d'urgence du procédé.

Comme le montre les résultats de l'analyse et afin de réduire le risque de rejet de matières inflammables dans l'atmosphère à un niveau tolérable, le SIS étudié doit répondre aux prescriptions d'un SIL 2.

A noter que l'évaluation des paramètres du risque est faite en se basant, d'une part, sur le jugement d'experts et d'autre part sur l'utilisation des données issues de la littérature. Dans le cas, par exemple, de la conséquence (comme paramètre prédominant), l'estimation s'est appuyée sur le jugement d'experts présents sur site en faisant recours à leurs propres connaissances ainsi qu'au retour d'expériences.

L'évaluation du paramètre taux de demande (W) est faite en utilisant des valeurs de fréquence des événements initiateurs prises de la littérature. Cependant, un problème se pose concernant leur adaptation aux conditions réelles d'utilisation du système étudié. En effet, les données génériques utilisées ne permettent pas d'avoir un état de l'art sur l'installation de référence. De plus, à l'origine d'un événement initiateur, il y a souvent une erreur humaine directe ou indirecte (erreur d'exploitation, de maintenance, ...). La quantification probabiliste de l'erreur humaine reste toujours une grande source d'incertitude dans les résultats.

Quant à la probabilité d'évitement de l'événement dangereux, elle est estimée en prenant en considération la vitesse d'évacuation de l'opérateur et la disponibilité de l'alarme exprimée en termes de PFD prise également de la littérature.

Le paramètre Occupation est estimé en prenant la valeur maximale du temps d'occupation de la zone dangereuse, car ce temps varie entre 0 et 4h au cours de la période normale de travail.

L'estimation donc de ces paramètres est source importante d'incertitude et peut être à l'origine des incohérences des résultats et éventuellement du conservatisme qui peut se traduire par une sous ou surestimation du SIL. L'ensemble de ces arguments justifie la nécessité de faire recours à une évaluation floue du SIL, l'objet de la section suivante.

IV.5 Détermination du SIL par la méthode graphe de risque flou

IV.5.1 Établissement des échelles floues

Une description bien détaillée des partitions floues des paramètres du risque C, F, P, W et du SIL, a fait objet de la section (§II.7.2) du chapitre 2 et illustrées par les figures II.11et II.12.

Les résultats numériques des différentes transformations, basées sur les données des tableaux II.3 et II.6 du chapitre 2, sont donnés par le tableau II.7.

IV.5.2.2 Base de règles floues relative au paramètre SIL (*SIL-SIF*)

Comme il a été expliqué précédemment (§II.7.4 du chapitre II), en suivant la logique du graphe de risque et en utilisant les descripteurs linguistiques associés aux paramètres de risque C, F, P, W et au SIL, un certain nombre de règles floues Si-Alors est établi. Dans ce cas, la base de règle (SIL-SIF) peut être comprise comme une traduction du graphe de risque.

Le tableau II.8 (du chapitre 2) représente l'ensemble des règles de combinaison des paramètres C, F, P et W déduites du graphe de risque.

IV.5.3 Fuzzification des données des scénarios retenus

Les données d'entrée des deux scénarios étudiés ont été déjà obtenues dans les sections (§IV.4.1) et (§IV.5.2.1). Les échelles des parametres C ,F,P et W sot transformées en leurs représentations floues selon la méthode décrite dans la section (§II.7.3) du chapitre 2.

Les données sur les paramètres C, F, P et W sont introduites au système d'inférence floue de Mamdani (pour fuzzification) sous forme de valeurs uniques (singletons) afin d'obtenir la valeur du SIL flou pour les deux scénarios étudiés.

La figure IV.5 montre, la combinaison de toutes les règles pour le scénario S_2.

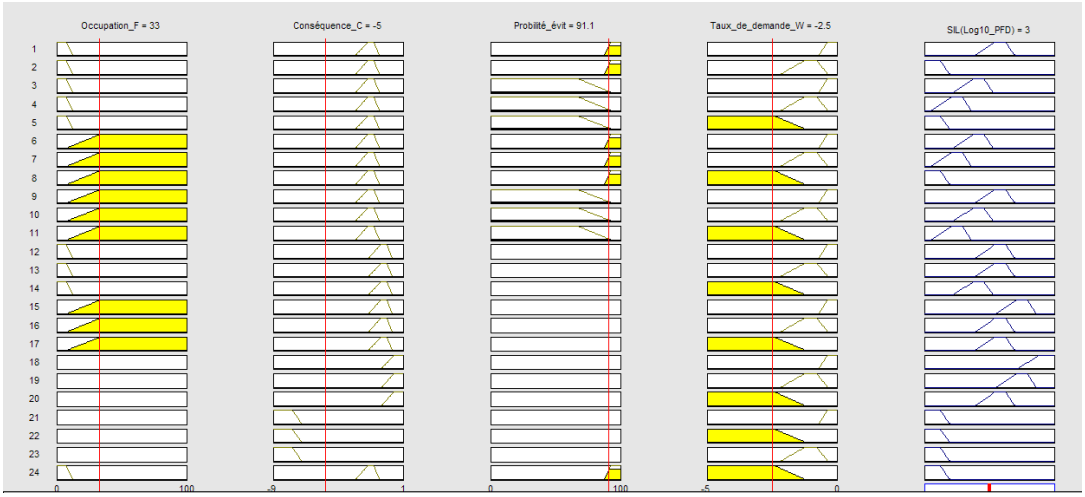


Fig. IV.5 : Processus d'inférence floue du SIL : Cas du scénario S_2

Les résultats de l'évaluation du SIL requis pour la fonction instrumentée de sécurité définie auparavant donnent pour le scénario 2, un SIL qui appartient à deux niveaux 2 et 3 avec des degrés d'appartenance respectivement 0,38 et 0,72.

IV.5.4 Résultats et discussion

En comparant les résultats obtenus par le graphe de risque conventionnel à ceux obtenus par le graphe de risque flou, une première conclusion peut être tirée ; une différence entre les deux approches est traduite par une sous estimation du SIL des FIS étudiés.

Le SIL flou obtenu pour les deux scénarios étudiés, est caractérisé par une appartenance graduelle à plus d'un niveau avec des degrés d'appartenance divergents. Dans le cas du premier scénario, le SIL conventionnel est de niveau 2, le SIL flou est de niveau 3 avec un degré d'appartenance de 82 %, de niveau 2 avec un degré d'appartenance de 33%. En ce qui concerne le scénario 2, le SIL flou est de niveau 3 avec un degré d'appartenance de 72 % et de niveau 2 avec un degré d'appartenance de 38%, sachant qu'il est jugé de niveau 2 par le graphe de risque conventionnel. Cette comparaison montre donc, qu'il ya sous estimation du niveau de SIL dans le cas des deux scénarios.

Au terme de cette application, une proposition d'amélioration du niveau d'intégrité de sécurité des SIS étudiés s'avère nécessaire. La section suivante sera, en effet, consacrée à l'application du modèle LOPA floue (proposé dans le chapitre trois section (§5)) sur le même système « four rebouilleur H101 ». Cette deuxième application nous permettra, d'une part, de s'assurer de la nécessité d'amélioration du niveau d'intégrité de sécurité de ces SIS et, d'autre part, de comparer les résultats issus des deux modèles flous proposés.

IV.6 Validation du modèle LOPA floue

Afin de démontrer l'intérêt de l'approche LOPA floue proposée dans le chapitre trois, nous avons mené une étude de cas sur le même système étudié dans la section précédente, à savoir le four rebouilleur H101.

IV.6.1 Scénarios d'accidents retenus pour LOPA

Comme il a été mentionné auparavant (§ III.1 du chapitre 3), la méthode LOPA s'intéresse aux conséquences les plus graves d'un scénario. L'identification de ces scénarios est une étape primordiale dans le processus de développement de la méthode LOPA. Les éléments de ces scénarios, à savoir les événements initiateurs et les conséquences sont identifiées par la méthode HAZOP (tableau IV.2).

Les scénarios d'accident représentatifs (SAR) retenus dans cette application (tableau IV.7) sont développés sous forme d'arbres d'événements (Figure IV.7).

Tableau IV.7 : Scénarios d'accidents retenus

Scénario	Événement initiateur	Conséquence
1	Défaillance de la vanne FICA-136V (fermée)	Endommagement du serpentin (incendie) & arrêt du processus
2	Erreur de l'opérateur : Mauvaise manipulation sur l'une des vannes manuelles HXC-907-V/908V (reste fermée)	Haute pression à l'intérieur du four H101, explosion & arrêt du processus
3	Défaillance de la vanne de sécurité (TOR) UZ-125C : Ouverture intempestive	dégagement du fuel gaz dans l'atmosphère, incendie & arrêt du processus

IV.6.2 Identification des couches de protection indépendantes (IPL)

Afin de réduire les risques générés par les scénarios d'accidents représentatifs retenus, plusieurs barrières de sécurité sont mises en œuvre. Ces dernières sont identifiées au préalable par la méthode HAZOP (Tableau IV.2). Parmi ces barrières, uniquement celles qualifiées d'IPL et répondant aux critères présentés en détails dans le chapitre 3 (§III.1.2) sont pris en considération dans cette application. Les couches de protection indépendantes prises en compte dans notre étude sont les suivantes:

- Alarme & Opérateur.
- Systèmes d'arrêt d'urgence PLC (SIS: système instrumenté de sécurité)
- Trappe d'explosion.

Les données utilisées pour estimer la fréquence des événements initiateurs et les PFD des barrières de sécurité (Tab.IV.8) et (Tab.IV.9) sont issues de la littérature (CCP, 98), (CCP, 01), (ORE, 02), (SON, O7), (ICS, 09), ou fournies par le concepteur du système.

Tableau IV.8 : Fréquence des événements initiateurs

Evénement initiateur	Code	Fréquence (/an)
Défaillance de la vanne de régulation (vanne FICA-136V) et (vanne HXC- 907V/908V)	EI_1	1,00E-01
Défaillance de l'opérateur (Mauvaise manipulation sur l'une des vannes HXC-907V/908V)	EI_2	3,16E-02
Défaillance d'une vanne de sécurité (TOR) (Ouverture intempestive de la vanne UZ-125C).	EI_3	3,16E-03

Tableau IV.9 : Probabilités de défaillance à la demande des IPL

IPL	Code	PFD
Réponse de l'opérateur à l'alarme	PFD_{11}	3,16E-01
SIS (PLC)	PFD_{21} PFD_{23}	SIL2
Trappe d'explosion	PFD_{22}	3,16E-03

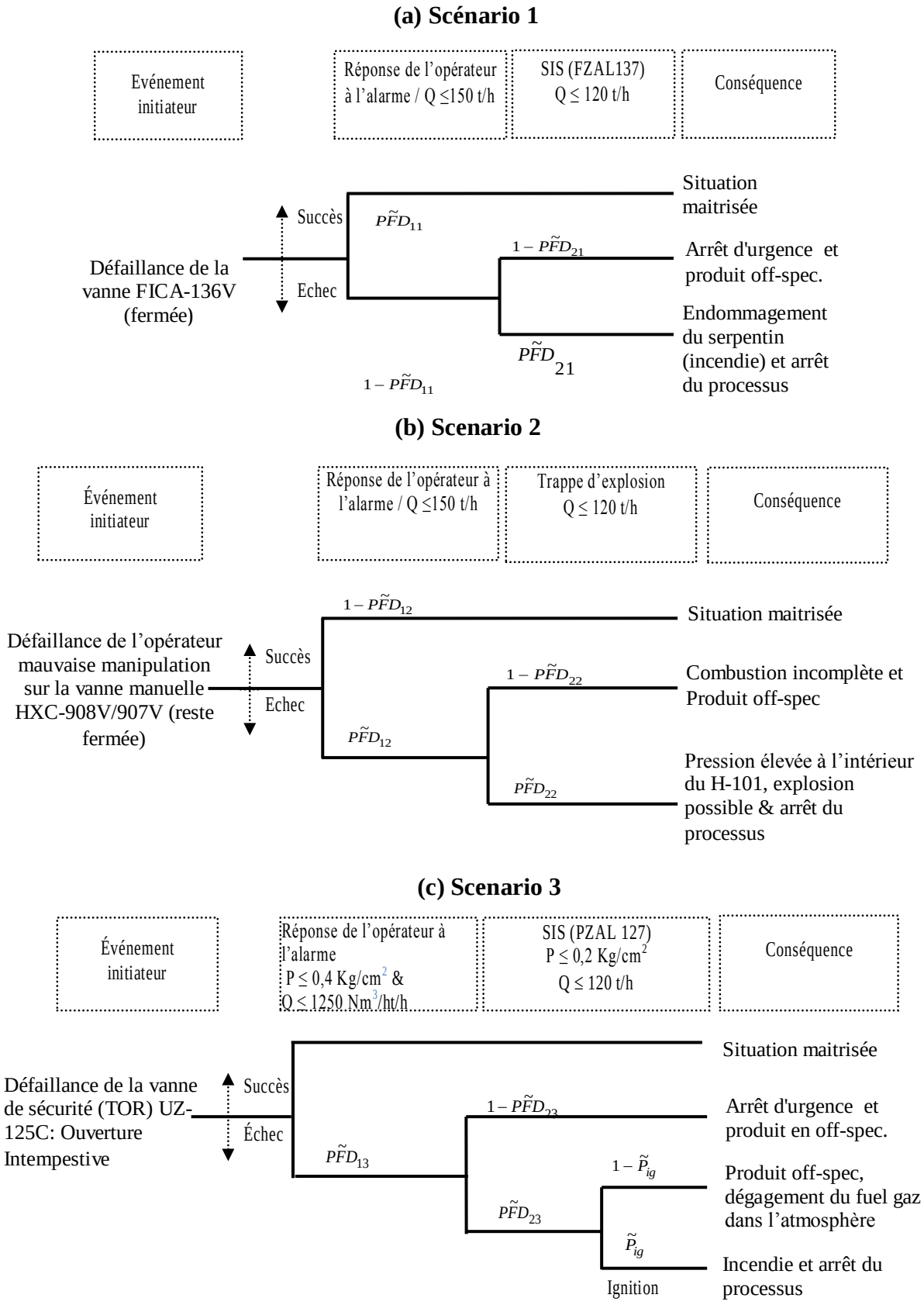


Fig. IV.7 : Arbres d'Événements relatifs aux scenarios d'accident retenus

6.3 Calcul de la fréquence de la conséquence réduite

La fréquence de la conséquence réduite des scénarios 1 et 2 est calculée en utilisant l'équation (III.1) et celle du scénario 3 est calculée en utilisant l'équation (III.2) (§III.2.2.5, chapitre 3). On trouve :

Scenario 1 : $f_1^{\,c}$ = EI_1. PFD_{11}. PFD_{21} = (1, 00E-01). (3,16E-01). (3,16E-03)
= 1, 00E-04 /an.

Scenario 2 : $f_2^{\,c}$ = EI_2. PFD_{12}. PFD_{22} = (3,16E-02). (3,16E-01). (3,16E-03)
= 3,6E-05/an.

Scenario 3: $f_3^{\,c}$ = EI_3. PFD_{13}. PFD_{23} .Pr_{ig} = (3, 16E-03). (3, 16E-03). (3, 00E-01).
= 3,16E-06 /an.

La valeur de fréquence calculée sera comparée à la fréquence du risque tolérable retenue par l'entreprise pour une prise de décision sur l'acceptabilité de ces scénarios.

A l'issue de l'application de la méthode LOPA conventionnelle, et en comparant les fréquences des conséquences réduites des scénarios étudiés à la fréquence du risque tolérable maximum (10^{-5}), nous constatons que la fréquence de la conséquence réduite f_1^c, relative au premier scénario, est jugée inacceptable.

La fréquence de la conséquence réduite f_2^c du deuxième scénario peut être considérée comme tolérable. Quant au troisième scénario, la fréquence de la conséquence réduite f_3^c est qualifiée d'acceptable.

Étant su que les données sur les fréquences des événements initiateurs et les PFD des IPL sont issues de la littérature, elles sont entachées d'incertitudes pouvant se répercuter sur les résultats obtenus, autrement dit les fréquences des conséquences réduites et sur la validité de la décision prise concernant leur acceptabilité. En effet, la valeur consistante exprimant la fréquence de la conséquence réduite, considérée comme critère principal de décision sur l'acceptabilité du scénario étudié, ne peut être obtenue en utilisant uniquement des valeurs uniques (souvent la valeur moyenne ou la valeur pessimiste d'un intervalle de

confiance). De plus, les intervalles de confiance sont souvent moins informatifs à cause de leur étendue.

Pour remédier à ce problème, le recours à la théorie des ensembles flous s'avère indispensable. La section suivante a pour objectif de mettre en œuvre le modèle LOPA floue proposé dans le chapitre trois.

IV.6.4 Application du modèle LOPA floue au système « Four Rebouilleur H101 »

IV.6.4.1 Fuzzification des données relatives aux paramètres des scénarios d'accident

En se référant aux données du tableau (IV.8) et (IV.9), les échelles de la fréquence des événements initiateurs et des PFD des IPL sont transformées en leurs représentations floues, selon la méthode décrite dans la section (§ III.6.1) du chapitre trois, en calculant la valeur moyenne quadratique des intervalles limites. Des fonctions d'appartenance triangulaires (figures IV.8) sont favorisées du moment qu'elles permettent le calcul simple des fréquences floues. Le tableau (IV.10) montre les résultats numériques de cette transformation.

Les paramètres a, b et m sont respectivement la borne inférieure, la borne supérieure et la valeur modale du nombre flou. Quand la probabilité de défaillance est une valeur unique, comme c'est le cas de la fréquence de l'événement initiateur dans le scénario 1 et la probabilité d'ignition dans le scénario 3, elles sont considérées comme des singletons.

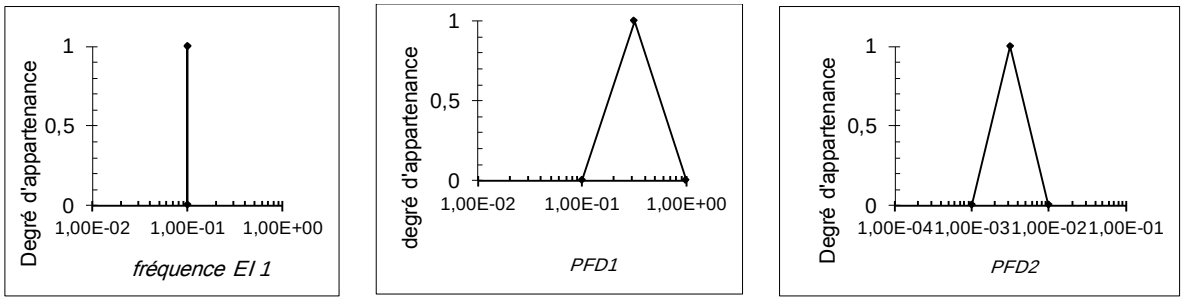
La PFD moyenne de la fonction de sécurité du SIS caractérise son SIL et elle est représentée par un intervalle selon la norme IEC61511 (IEC, 03). Autrement dit, les valeurs de la PFD complètement possibles sont celles appartenant à cet intervalle ($\mu_{\widetilde{PFD}}(p) = 1$. Pour le four rebouilleur H101, les SIS implémentés fonctionnent en mode faible sollicitation (moins d'une fois par an) et ils sont conçus pour atteindre un SIL 2.

La transformation des intervalles de confiance des paramètres d'entrée de la méthode LOPA fournis en nombres flous, offre une flexibilité dans la manipulation des données incertaines. En effet, avec des distributions de possibilité représentées par des ensembles flous triangulaires, la valeur de la fréquence de l'événement initiateur et celle de la PFD sont soumises à des degrés d'appartenance graduelle allant de la non appartenance à l'appartenance complète.

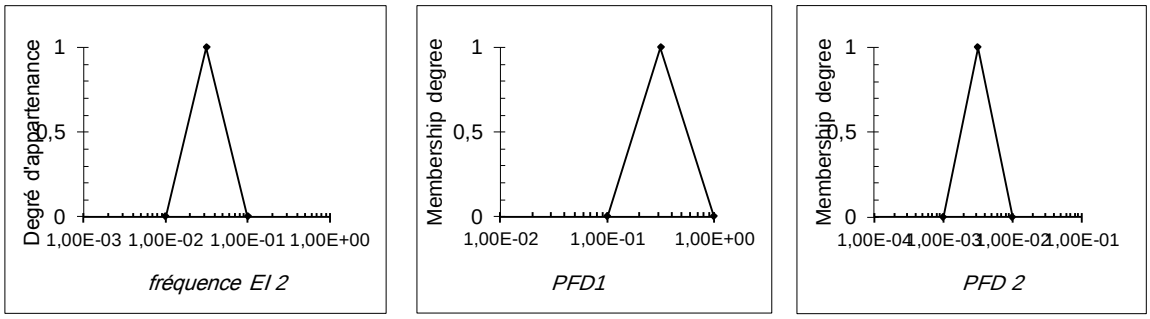
Tableau IV.10 : Supports et valeurs modales des fréquences floues des EI et PFD des IPL

(a) Scenario 1			
Probabilités floues des parameters	***a***	***m***	***b***
fréquence de la défaillance de la vanne (par an)	10^{-1}	10^{-1}	10^{-1}
$P\tilde{F}D_{11}$ Réponse de l'opérateur à l'alarme	10^{-1}	3.16×10^{-1}	1
$P\tilde{F}D_{21}$ (SIS FZAL137) (SIL2)	10^{-3}	-	10^{-2}
(b) Scenario 2			
Probabilités floues des parameters	***a***	***m***	***b***
Fréquence de l'erreur humaine (par an)	10^{-2}	3.16×10^{-2}	10^{-1}
$P\tilde{F}D_{12}$ Réponse de l'opérateur à l'alarme	10^{-1}	3.16×10^{-1}	1
$P\tilde{F}D_{22}$ Trappe d'explosion	10^{-3}	3.16×10^{-3}	10^{-2}
(c) Scenario 3			
Probabilités floues des parameters	***a***	***m***	***b***
fréquence de la défaillance de la vanne de sécurité (par an)	10^{-3}	3.16×10^{-3}	10^{-2}
$P\tilde{F}D_{13}$ Réponse de l'opérateur à l'alarme	10^{-1}	3.16×10^{-1}	1
$P\tilde{F}D_{23}$ (SIS FZAL 125) (SIL2)	10^{-3}	-	10^{-2}
$\tilde{P}_{ig}$ (Ignition)	3×10^{-1}	3×10^{-1}	3×10^{-1}

(a) **Scénario 1**



(b) Scénario 2



(c) Scénario 3

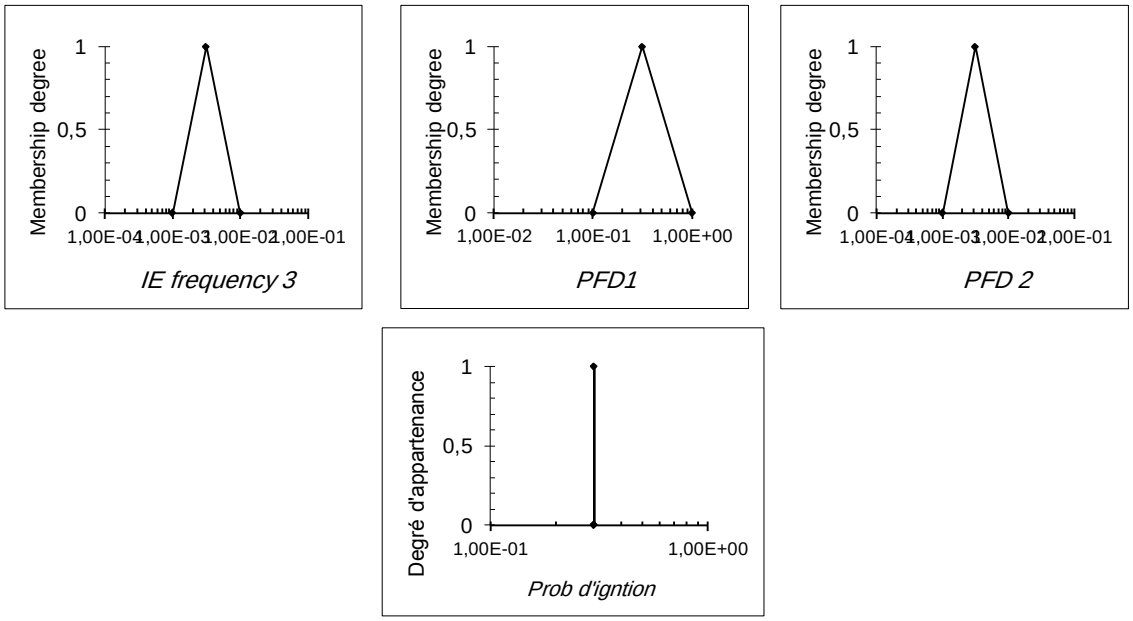


Fig. IV.8 : Représentation floue de la fréquence de l'événement initiateur, de la PFD et de la probabilité d'ignition (a) scénario 1, (b) scénario 2 et (c) scénario 3

IV.6.4.2 Évaluation de la fréquence floue de la conséquence réduite

L'évaluation de la fréquence floue de la conséquence réduite des scénarios est faite en utilisant l'équation (III.13). La fréquence floue de la conséquence réduite est obtenue en multipliant les intervalles flous des paramètres d'entrée à savoir les fréquences des événements initiateurs, les PFD des IPL et la probabilité d'ignition.

La multiplication est effectuée par α-coupes selon une discrétisation en décadaire, seulement onze niveaux de l'intervalle [0, 1] sont pris en considération (Kau, 91).

L'intervalle flou de la fréquence est obtenu en multipliant les bornes inférieures et supérieures des α-coupes des paramètres d'entrée. Le tableau IV.11 donne les bornes inférieures et supérieures associées à chaque niveau α.

Tableau IV.11: Niveaux α des intervalles des fréquences floues

Niveau-α	Scenario 1 (par an)		Scenario 2 (par an)		Scenario 3 (par an)	
0	10^{-5}	10^{-3}	10^{-6}	10^{-3}	3×10^{-8}	3×10^{-5}
0,1	$1,22\times10^{-5}$	$9,32\times10^{-4}$	$1,80\times10^{-6}$	$8,09\times10^{-4}$	$4,44\times10^{-8}$	$2,60\times10^{-5}$
0,2	$1,43\times10^{-5}$	$8,63\times10^{-4}$	$2,94\times10^{-6}$	$6,43\times10^{-4}$	$6,16\times10^{-8}$	$2,24\times10^{-5}$
0,3	$1,65\times10^{-5}$	$7,95\times10^{-4}$	$4,48\times10^{-6}$	$5,02\times10^{-4}$	$8,15\times10^{-8}$	$1,90\times10^{-5}$
0,4	$1,86\times10^{-5}$	$7,26\times10^{-4}$	$6,49\times10^{-6}$	$3,83\times10^{-4}$	$1,04\times10^{-7}$	$1,58\times10^{-5}$
0,5	$2,08\times10^{-5}$	$6,58\times10^{-4}$	$9,01\times10^{-6}$	$2,85\times10^{-4}$	$1,30\times10^{-7}$	$1,30\times10^{-5}$
0,6	$2,30\times10^{-5}$	$5,90\times10^{-4}$	$1,21\times10^{-5}$	$2,05\times10^{-4}$	$1,58\times10^{-7}$	$1,04\times10^{-5}$
0,7	$2,51\times10^{-5}$	$5,21\times10^{-4}$	$1,59\times10^{-5}$	$1,42\times10^{-4}$	$1,90\times10^{-7}$	$8,15\times10^{-6}$
0,8	$2,73\times10^{-5}$	$4,53\times10^{-4}$	$2,03\times10^{-5}$	$9,29\times10^{-5}$	$2,24\times10^{-7}$	$6,16\times10^{-6}$
0,9	$2,94\times10^{-5}$	$3,84\times10^{-4}$	$2,56\times10^{-5}$	$5,69\times10^{-5}$	$2,60\times10^{-7}$	$4,44\times10^{-6}$
1	$3,16\times10^{-5}$	$3,16\times10^{-4}$	$3,16\times10^{-5}$	$3,16\times10^{-5}$	3×10^{-7}	3×10^{-6}

IV.6.4.3 Comparaison des fréquences floues à la fréquence maximale tolérable

En comparant les fréquences floues des conséquences réduites à la fréquence du TR, on s'aperçoit qu'il existe une divergence d'un scénario à l'autre. Une représentation graphique de ces résultats est donnée par la figure IV.9.

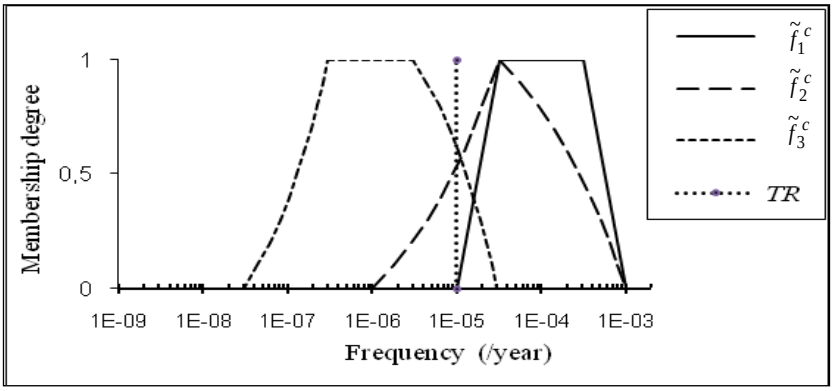


Fig. IV.9 : Comparaison des fréquences floues des conséquences réduites au TR

Pour $\tilde{f}_1^C$ (dont la fonction d'appartenance est trapézoïdale), à l'exception de la limite inférieure du support, toutes les valeurs de cet ensemble sont supérieurs à TR.

Cette remarque est compatible avec le respect de possibilité et de nécessité des mesures données par le tableau IV.12, c.à.d.:

$$\text{Pos}(\widetilde{f}_1^C \leq TR) = \text{Nes}(\widetilde{f}_1^C \leq TR) = 0$$

Par conséquent, $\widetilde{f}_1^C$ c'est une fréquence inacceptable. $\widetilde{f}_3^C$ du scénario 3 peut être considérée comme tolérable en se référant à la mesure de la possibilité qui est un critère optimiste :

$$\text{Pos}(\widetilde{f}_3^C \leq TR) = 1$$

Cependant, affirmant que $\widetilde{f}_3^C$ soit forcément tolérable n'est pas conforme avec la valeur de $\text{Nes}(\widetilde{f}_1^C \leq TR)$ qui est de 0,38. La fréquence floue $\widetilde{f}_2^C$ est comprise entre les deux fréquences précédentes mais elle tend beaucoup plus vers la zone intolérable puisque même le critère optimiste de comparaison n'est pas complètement vérifié, en effet :

$$\text{Pos}(\widetilde{f}_2^C \leq TR) = 0.53$$

Tableau IV. 12 : Mesures de possibilité et de nécessité liées aux fréquences initiales

Scénario	$\text{Pos}(\widetilde{f}_i^C \leq TR)$	$Nes(\widetilde{f}_i^C \leq TR)$
1	0	0
2	0.53	0
3	1	0.38

IV.6.4.4 Réduction des fréquences des conséquences sous la contrainte de la nécessité

En se référant à la relation (III.25), on peut constater que nous avons besoin de la valeur du niveau de confiance λ pour calculer MRRF. Cependant, λ= 0,5 semble être une valeur hypothétique raisonnable pour trois raisons principales:

- D'abord, en tant que valeur différente de zéro, il garantit parfaitement le critère optimiste basé sur la mesure de possibilité, c.à.d:

$$\text{Pos}(\widetilde{f}_i^* \leq TR) = 1$$

- Deuxièmement, il se réfère au point central dans l'intervalle [0, 1], ce qui correspond à 50% de certitude.

- Troisièmement, il permet à la contrainte de la nécessité, comme un critère pessimiste, d'être modérée et par conséquent, les deux contraintes technologiques et financières ne seraient pas un obstacle dans la réduction nécessaire des risques.

Les MRRF pour les scénarios spécifiques sont donnés par le tableau IV.13. Les fréquences réduites sous la contrainte de nécessité sont présentés sur la Fig. IV.10. A noter que $\tilde{f}_1^C$ et $\tilde{f}_1^*$ sont de forme trapézoïdale tracées sur une échelle logarithmique.

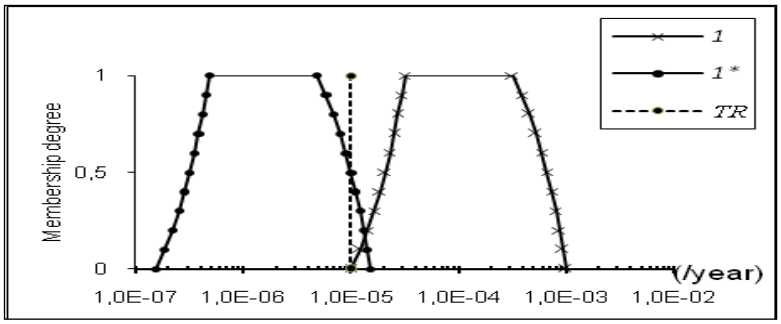
Tableau IV.13 : MRRF pour λ=0.5 et TR=10^{-5}/an

Scenario	MRRF
1	66
2	51.58
3	2

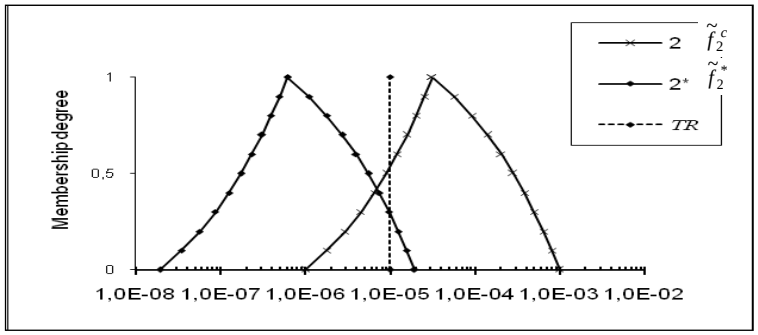
Comme nous pouvons le constater, les résultats sont en concordance avec les résultats du tableau IV.12 qui sont basées sur le positionnement des fréquences floues estimées par rapport à TR. En effet, plus la partie décroissante de la fréquence floue s'éloigne du TR, plus la valeur MRRF augmente. Le MRRF pour le scénario 1 est le plus élevé, le scénario 2 nécessite un MRRF non loin du premier. Le scénario 3 peut représenter le meilleur des trois scénarios, car il ne nécessite qu'un faible MRRF, à savoir MRRF égale à 2, pour répondre au TR.

Le tableau IV.14 montre les mesures de possibilité et de nécessité lorsqu'on considère les fréquences floues des conséquences réduites sous la contrainte de nécessité. Par rapport aux résultats du tableau IV.12, on peut voir que toutes les mesures de possibilité sont égales à 1 (comme mentionné ci-dessus) et toutes les mesures de première nécessité augmentent considérablement (valeur minimale = 0.5). Ce résultat pourrait être approprié pour la réduction nécessaire du risque.

(a) Scénario 1



(b) Scénario 2



(c) Scénario 3

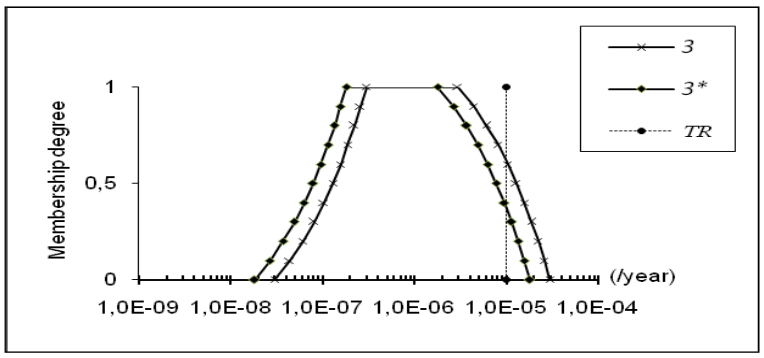


Fig. IV.10 : Réduction de la fréquence de la conséquence sous la contrainte de nécessité

Tableau IV.14: Mesures de possibilité et de nécessité liées à la réduction théorique

Scénario	$Pos(\tilde{f}_i^* \le TR)$	$Nes(\tilde{f}_i^* \le TR)$
1	1	0.5
2	1	0.71
3	1	0.62

IV.6.4.5 Prise en compte des aspects pratiques

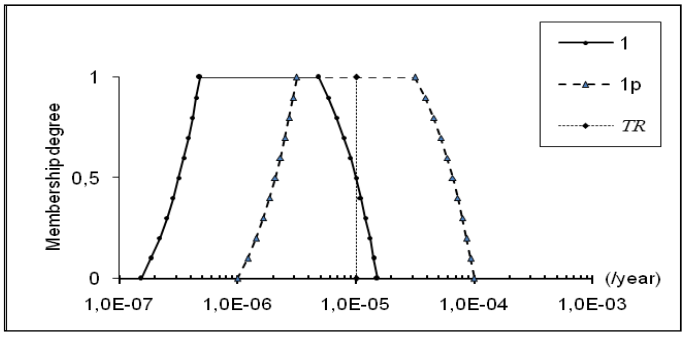
Pour une validation supplémentaire de l'approche proposée, nous avons essayé de tenir compte de certains aspects pratiques qui pourraient améliorer l'intégrité de la sécurité des couches de protection et donc de réduire les fréquences des conséquences.

Pour chaque scénario, il s'agit de minimiser soit la fréquence de l'événement initiateur ou bien la PFD d'une IPL en se basant sur le jugement d'experts en la matière. Le tableau IV.15 montre les modifications prévues par ces experts et leurs effets.

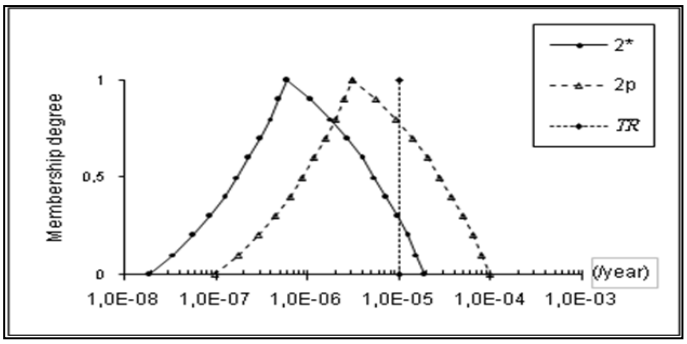
Tableau IV.15 : Modifications données par des experts du procédé

Scénario	Modifications suggérées	Effets
1	Pour le SIS FZAL137, comme une IPL, ajouter un autre capteur identique au premier pour modifier l'architecture de la partie capteur de 1oo1 à 1oo2	Augmentation de l'intégrité de sécurité de la SIF de SIL2 à SIL3 avec $P\tilde{F}D_{21}$ appartenant à $[10^{-4}, 10^{-3}]$
2	Se concentrer sur le facteur humain comme événement initiateur par une formation complémentaire	Augmenter la fiabilité humaine au moins d'un ordre de grandeur, soit : $\tilde{f}_2^I = (10\text{-}3, 3.16\times10\text{-}3, 10\text{-}2)$ (par an)
3	Pour le SIS PZAL127, comme une IPL, ajouter un autre capteur identique au premier pour modifier l'architecture de la partie capteur de 1oo1 à 1oo2	Augmentation de l'intégrité de sécurité de la SIF de SIL2 à SIL3 avec $P\tilde{F}D_{23}$ appartenant à $[10^{-4}, 10^{-3}]$

(a) Scénario 1



(b) Scénario 2



(c) Scénario 3

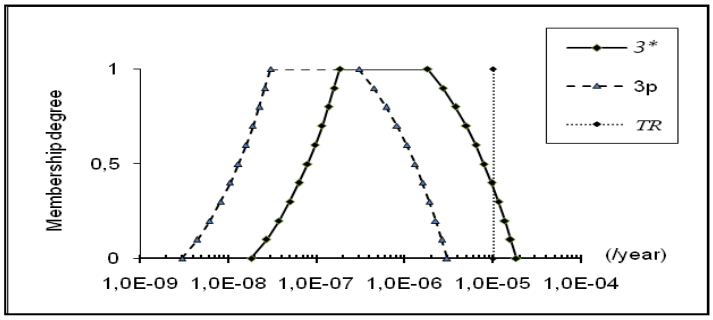


Fig. IV.11 : Réduction de la fréquence des conséquences via des modifications pratiques

Les fréquences des conséquences réduites sous la contrainte de nécessité (peuvent être qualifiées de théoriques) et celles issues des modifications pratiques sont représentées dans la figure (IV.11 a, b et c).

D'après les résultats du tableau (IV.16), on peut dire que pour les scénarios 1 et 2, les fréquences floues liées à des considérations pratiques se situent entre les fréquences floues estimées (ou initiales) et celles théoriques. Notons que la mesure de possibilité est toujours égale à 1 pour tous les scénarios. Ce résultat est compatible avec une réduction du risque optimiste.

D'autre part, la mesure de la nécessité a considérablement diminué, à savoir 0 et 0,22 contre, respectivement, 0,5 et 0,71. La réduction nécessaire des risques est un peu plus ou moins réalisée pour le scénario 2 et il pourrait être considéré que les deux valeurs modales et la borne inférieure du support de $\widetilde{f}_2^P$ sont inférieurs à TR.

Tableau IV.16 : Mesures de possibilité et de nécessité relatives aux réductions pratiques

Scénario	$Pos(\tilde{f}_i^{\,p} \leq TR)$	$Nes(\tilde{f}_i^{\,p} \leq TR)$
1	1	0
2	1	0.22
3	1	1

Pour le scénario 1, il semble cependant clairement que les modifications suggérées par les experts ne sont pas assez conséquentes et d'autres améliorations sont nécessaires.

En plus, pour l'amélioration du SIL de la SIF associée au SIS FZAL137, nous recommandons également la réduction de la fréquence de l'événement initiateur, c'est-à-dire la fréquence de la défaillance de la vanne, par l'ajout d'une vanne redondante. Pour le scénario 3 (Fig. VI.11c), des modifications pratiques ont abouti à une situation inverse dans le sens où la fréquence floue de la conséquence est inférieure à la valeur théorique, avec une mesure de nécessité égale à 1 (contre 0,62 pour la fréquence floue théorique). Par conséquent, nous pensons que le MRRF théorique est si faible (égale à 2) qu'il serait difficile de proposer une amélioration technique adéquate. Par conséquent, et par rapport au TR, la fréquence floue initiale $\tilde{f}_3^{\,C}$, peut être acceptée telle qu'elle est sans aucune action immédiate.

IV.7 Comparaison des résultats des deux modèles flous proposés

Rappelons que l'intérêt de ce chapitre réside dans l'application de modèles flous développés, à savoir le graphe de risque flou et LOPA floue au même procédé industriel ce qui nous a permet de comparer les résultats obtenus par ces modèles ainsi que de valider davantage ces derniers.

Cette comparaison nous incite à examiner en détail les résultats obtenus par les deux modèles en se référant aux tableaux (IV.6), (IV.14) et (IV.16). Nous constatons que la sous estimation du SIL, des SIS (FZAL 137) et (PZAL 127), comme résultat issu de d'application du graphe de risque flou, est confirmée par les résultats donnés par le modèle LOPA floue. En effet, Parmi les IPL étudiées par la méthode LOPA, on trouve les SIS (FZAL 137) et (PZAL 127), utilisés dans le système four rebouilleur (H-101) pour assurer

la réduction nécessaire du risque, autrement dit atteindre le risque tolérable et donc réduire les fréquences des conséquences des scénarios 1 et 3. Cependant, les PFD de ces SIS, correspondant au SIL 2, donnent des fréquences de conséquences jugées inacceptable et presque tolérable, respectivement pour les scénarios 1 et 3.

En prenant en considération les modifications suggérées par les experts du procédé analysé, les fréquences précédentes ont été réduites d'une manière optimiste. Ces modifications consistaient à reconfigurer les architectures des SIS (FZAL 137) et (PZAL 127) en vue d'augmenter l'intégrité de ces SIS de SIL2 à SIL3 (voir tableau IV.15), ce qui renforce les résultats donnés par le graphe de risque flou.

Conclusion

L'objectif de ce travail était de montrer la pertinence des modèles flous proposés dans la gestion des risques industriels, en permettant d'une part, une prise en compte des aspects imprécis et incertains des données utilisées dans l'évaluation de ces risques. D'autre part, d'assurer une meilleure prise de décision en matière de prévention de ces risques.

Une étude de cas portée sur un four rebouilleur dans un processus de traitement de gaz a montré la grande applicabilité des approches proposées en donnant des résultats encourageants. L'évaluation du SIL par le modèle graphe de risque flou, comme alternative du graphe de risque conventionnel nous a permet :

- d'utiliser des variables linguistiques associées à des intervalles flous à la place de nombres uniques généralement incompatibles avec l'imprécision de la perception humaine ;
- de relativiser les valeurs des intervalles de confiance aux bornes fixes en considérant des appartenances graduelles ;

- d'utiliser des échelles floues continues, ce qui résout le problème d'interprétation des résultats ;
- de donner une structure plus flexible pour combiner les paramètres du graphe de risque ;
- de prendre une décision sur la base d'un niveau d'intégrité précis et par conséquent, de mener à bien une démarche de réduction des risques dans le cadre d'un investissement rationnel.

L'application du modèle LOPA floue, nous a permet :

- D'utiliser, soit des valeurs de possibilité floues ou des fréquences floues, pour représenter les données d'entrée.
- D'utiliser l'arithmétique floue pour calculer les fréquences floues de conséquences.
- La comparaison de ces fréquences avec une fréquence maximale tolérable en utilisant les mesures de possibilité et de nécessité.

En se référant aux trois scénarios d'accidents avec des fréquences allant de « presque intolérable» jusqu'à « tolérable », nous avons vu comment le MRRF varie en fonction de la différence entre les fréquences floues et la fréquence tolérable. En outre, avec l'examen des modifications pratiques telles que proposées par les experts, nous avons pu mettre en évidence le potentiel de l'approche proposée dans l'évaluation des jugements d'experts.

Conclusion et perspectives

Conclusion générale

Le problème de réduction des risques que présente un système industriel reste au cœur des préoccupations des analystes des risques. Réduire un risque à un niveau acceptable ou tolérable, en utilisant plusieurs barrières de sécurité, revient à évaluer l'efficacité de ces barrières. Les normes IEC 61508 et IEC 61511, qui traitent de la sécurité fonctionnelle des systèmes relatifs à la sécurité, décrivent, entre autres, deux méthodes d'évaluation de ces barrières de sécurité ; le graphe de risque et l'analyse des couches de protection. Or, ces méthodes utilisent, pour évaluer les paramètres du risque, de données qui sont souvent imprécises et/ou incertaines car issues du retour d'expérience ou de jugement d'experts.

L'objectif de cette thèse était d'identifier, représenter et traiter les incertitudes liées aux paramètres du risque utilisés par les méthodes Graphe de Risque et LOPA mais également de proposer de nouvelles approches issues des techniques floues et possibilistes.

Bilan et apports de la thèse

Nous avons porté notre premier effort de recherche sur la distinction entre les différents types et sources d'incertitudes dans une démarche d'analyse et d'évaluation des risques. Nous avons ensuite présenté quelques théories de traitement des incertitudes telles que la théorie des probabilités, la théorie des ensembles flous et la théorie des possibilités. Cet état de l'art nous a permis d'examiner les limites de l'approche probabiliste (traditionnelle) pour le traitement des incertitudes, notamment dans le cas de manque d'un retour d'expérience fiable sur les défaillances ou dans le cas de données montrant une grande variabilité. Ceci implique une grande difficulté de déduction des distributions de probabilité suivies par ces données. Le recours à la théorie des ensembles flous et à la théorie de possibilité s'est avéré indispensable.

Notre deuxième effort a porté sur la révision des démarches traditionnelles empruntées par les méthodes Graphe de Risque et LOPA, plus précisément sur l'évaluation des paramètres du risque. Nous sommes arrivés au constat que ces démarches présentent des limites. La méthode graphe de risque utilisée pour déterminer le niveau d'intégrité de sécurité (SIL), malgré sa facilité de mise en œuvre et son applicabilité, elle présente des insuffisances quant à l'interprétation des termes linguistiques utilisés pour caractériser les paramètres C, F, P et W en raison de la subjectivité liée à la définition qualitative des

paramètres suscités. A ceci s'ajoute l'affectation ferme en termes de probabilités et de taux des paramètres C, F, P, W et le SIL. Le problème de rigidité des intervalles ordinaires utilisés pour la représentation quantitative des paramètres leur est imputable.

Quant à LOPA, il est souvent difficile d'affecter des valeurs exactes aux éléments du scénario analysé par cette méthode à savoir la fréquence de l'événement initiateur et les probabilités de défaillance à la demande (PFD) des couches de protection.

Les modèles flous proposés comme alternative aux méthodes Graphe de Risque et LOPA conventionnelles peuvent être considérés comme des compléments à ces dernières. Ils offrent une flexibilité pour la manipulation des données imprécises relatives aux paramètres du risque utilisés. Le modèle graphe de risque flou est basé sur un système d'inférence floue et prend en considération le problème d'étalonnage. Ainsi, les échelles de partitions floues du SIL et les paramètres C, F, P et W sont numériques plutôt qu'ordinales. Le modèle graphe de risque flou est validé en vérifiant les deux propriétés d'une base de règles floues à savoir la cohérence et la consistance. Le modèle LOPA floue permet de transformer la fréquence des événements initiateurs et la PFD des IPL en ensembles flous avec des fonctions d'appartenance graduelle. La fréquence floue de la conséquence réduite est calculée en utilisant le principe d'extension et la méthode des α-coupes. La fréquence calculée sera comparée avec la fréquence du risque maximal tolérable, et la réduction exigée est obtenue par une prise de décision possibiliste sous une contrainte de nécessité compatible avec le concept de réduction nécessaire de risque tel que décrit par la norme IEC 61508.

L'utilisation des concepts d'ensembles flous, de variables linguistiques, de possibilité, de nécessité et de règles floues issus de cette théorie nous a permis de :

- Prendre en compte le problème de représentation des données relatives aux paramètres du risque car les échelles floues ont la capacité de décrire la continuité des catégories via une appartenance graduelle ;
- Réduire l'incertitude relative aux intervalles de confiance larges par des valeurs modales

L'application de ces modèles à un four rebouilleur dans un système de traitement de gaz a montré la grande applicabilité et l'opportunité des modèles flous proposés dans la gestion des risques industriels en permettant, d'une part, une prise en compte des aspects imprécis et incertains des données utilisées dans l'évaluation des risques. D'autre part, d'assurer une meilleure prise de décision en matière de prévention de ces risques.

Perspectives

Comme perspective à cette recherche, nous pensons qu'il serait intéressant, pour améliorer le modèle Graphe de risque flou proposé, une caractérisation plus fine des paramètres fréquence d'exposition et probabilité d'évitement afin de se rapprocher davantage des situations réelles de risque. Une analyse des résultats obtenus montre que la caractérisation binaire de ces deux paramètres est insuffisante par rapport à la complexité des situations de danger étudiées. Il nous semble intéressant de prévoir d'autres catégories intermédiaires pour une caractérisation des échelles de ces paramètres permettant de renforcer l'utilité du graphe de risque flou en lui offrant une souplesse d'emploi.

Pour le modèle LOPA floue, en tenant compte de certains aspects non développés dans le modèle LOPA floue proposé, les résultats obtenus par ce modèle peuvent être considérés, dans un certain sens, comme partiels. Nous croyons que la phase de fuzzification a besoin de plus de développement concernant l'explication des connaissances d'experts et la représentation floue de l'information prise de la littérature et des bases de données. En particulier lorsqu'il s'agit de valeurs simples et/ou de grands intervalles. Un deuxième problème concerne le choix du niveau de confiance λ, la réduction nécessaire des risques et sa relation avec le principe ALARP. La question est de savoir quelle valeur de λ satisfait la démonstration du principe ALARP.

Enfin, il serait intéressant d'enrichir les deux modèles proposés en essayant d'une part, d'y intégrer les coûts de mise en œuvre et d'exploitation respectifs des différentes solutions proposées. D'autre part, de définir et d'intégrer les actions de surveillance et de maintenance afin de mener à bien une bonne démarche de maitrise des risques.

Au-delà de ce genre de questions, nous croyons que le modèle LOPA floue pourrait être une extension de LOPA conventionnelle qui peut être appliquée avec succès en dehors du cadre probabiliste. Néanmoins, d'autres développements doivent avoir lieu pour justifier et améliorer le modèle proposé.

Références bibliographiques

Références bibliographiques

(Abr 02)	M. Abrahamsson, « Uncertainty in Quantitative Risk Analysis-Characterisation and Methods of Treatment», Department of Fire Safety Eng., Lund University, Report no 1024, 2002.
(ARA 04)	ARAMIS, «Développement d'une méthode intégrée d'analyse des risques pour la prévention des accidents majeurs», rapport final, Septembre, INERIS, 2004.
(Art 98)	M.D. Arthur, «Layer of protection analysis for determining safety integrity level», ISA Transactions, vol. 37, N° 3, pp. 155-165, 1998.
(Ave 11)	T. Aven, « Quantitative risk assessment, the scientific platform », CAMBRIGE University press, 2011.
(Ave 08)	T. Aven, « Risk Analysis Assessing Uncertainties beyond Expected Values and Probabilities», John Wiley & Sons Ltd, 2008.
(Bag 13)	A. Baghaei, «3-Parameters SPW technique: A new method for evaluation of target safety integrity level », J. Loss Prev. Proc. Ind. 26, 1257-1261, 2013.
(Bay 07)	P. Baybutt, «An improved risk graph approach for determination of safety integrity levels (SILs) », Process Safety Progress Journal, vol. 26, no 1, pp. 66-76, 2007.
(Bay 12)	P. Baybutt, «Using risk tolerance criteria to determine safety integrity levels for safety instrumented functions», J. Loss Prev. Proc. Ind. 25, 1000-1009, 2012.
(Bel 70)	R.E. Bellman, L.A. Zadeh, «Decision-Making in a Fuzzy Environment», Manag. Sci. 17, 141-164, 1970.
(Bil 00)	T. Bilgic and I. Turksen, «Measurement of membership functions : theoretical and empirical work», In D. Dubois and H. Prade, editors, Fundamentals of Fuzzy sets, pages 195–228, Kluwer Academic Publishers, Boston, 2000.
(Bla 00)	L. Blackmore, «IEC 61508-Practical experience in increasing the effectiveness of SIL assessments», ISA EXPO, ISBN/ID TP00ISA6023, 2000.
(Bom 98)	P. Bome, « Introduction à la commande floue», Collection Sciences et technologies, 6, Paris: Technip, 1998.
(Bor 85)	G. Bortolan, R. Degani, «A review of some methods for ranking fuzzy substs», Fuzzy Sets and Syst. 15, 1-19, 1985.
(Bou 95)	B. Bouchon - Meunier, « La logique floue et ses applications-Vie artificielle », Ed. Addison - Wesley France, Paris, 1995.
(Bou 03)	B. Bouchon – Meunier et C. Marsala, «Logique floue, principes, aide à la décision », Hermes Science, LAVOISIER, 2003.

(Bow 98)	J.B. Bowles, «The new SAE FMEACA Standard», IEEE proceeding annual Reliability and Maintenability symposium, 1998.
(Bow 95)	J. B. Bowles and C. E. Peláez, « Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis », Reliability Engineering & System Safety, vol. 50, N° 2, pp. 203–213, 1995.
(Bow 03)	J.B. Bowels, « An assessment of RPN Prioritization in a Failure Modes Effects and Criticality Analysis », Proceeding of Annual Reliability and Maintenability Symposium, pp. 380-386,2003.
(Bra 03)	M.Braglia, M. Frosolini and R. Montanari, «Fuzzy criticality assessment model for failure modes and effets analysis», International Journal of Quality & Reliability Management, vol. 20, no. 4, pp. 503-524, 2003.
(Cay 96)	D.Cayrac, D. Dubois, «Handing Ucertainty with possibility theory and fuzzy sets in a satellite fault diagnosis application», IEEE Trans.on Fuzzy Systems, vol 4, N° 3, 1996.
(CCP 89)	Center for Chemical Process Safety (CCPS), «Guidelines for Process Equipment Reliability Data with Data Tables», American Inst. of Chem. Eng. (AIChE), 1989.
(CCP 00)	Guidelines for Chemical Process Safety Quantitative Risk, second edition, American Institute of Chemical Engineers, New York, 2000.
(CCP 01)	Center for Chemical Process Safety, « Layer of Protection Analysis-Simplified Process Risk Assessment », American Institute of Chemical Engineers, New York, 2001.
(CCP 09)	Center for Chemical Process Safety (CCPS), «Guidelines for Developing Quantitative Safety Risk Criteria», American Inst. of Chem. Eng. (AIChE), 2009.
(Cha, 04)	S. Chaumette, «Méthodes systématiques de détermination d'ensemble de scénarios et exigences pratiques en termes de barrières de sécurité», INERIS, DRA 34 décembre 2004.
(Cha 07)	A.Chan, J.B. Yang and K.S. Chin., « Development of fuzzy FMEA based product design system», International Journal of Advanced Manufacturing Technology, 2007.
(Chu 92)	M.H. Chun, K.I. Ahn, « Assessment of the potential applicability of fuzzy set theory to accident progression event trees with phenomenological uncertainties», Reliab. Eng. Syst. Safety, 37, 237-252, 1992.
(Dar 08)	R.M. Darbra, M. Demichela and S. Murè, « Preliminary risk assessment of ecotoxic substances accidental releases in major risk installations through fuzzy logic», J. Process safety and environmental protection, 86, 103-111,

	2008.
(Das 07)	B. Das, K. Maity and M. Maiti, «A two warehouse supply-chain model under possibility/necessity/credibility measures», Math. Comp. Mod. 46, 398-409, 2007.
(Dea 99)	S. Dean, IEC 61508-Assessing the hazard and risk, Sauf Consulting Ltd. Available: http://www.sauf.co.uk, April, 1999.
(Deb 03)	Debray, « Méthodes d'analyse des risques générés par une installation industrielle. Technical Report Omega 7, DRA 35 INERIS, 2003.
(Don 07)	C. Dong, « Failure mode and effects analysis based on fuzzy utility cost estimation », International Journal of Quality & Reliability Management, vol. 24, no. 9, pp. 958-971, 2007.
(Dub 83)	D. Dubois, H. Prade, «Ranking Fuzzy Numbers in the Setting of Possibility Theory», Inf. Sci. 30,183-224, 1983.
(Dub 87)	D. Dubois and H. Prade, «The mean value of a fuzzy number», *Fuzzy Sets and Syst.*, vol.24, pp. 279-300, 1987.
(Dub 88a)	D. Dubois and H. Prade, « possibility theory», Plenum Press, New –York, 1988.
(Dub 88b)	D. Dubois and H. Prade, «Representation and combination of uncertainty with belief functions and possibility measures», Comput. Intell., 4 :244–264, 1988.
(Dub 99a)	D. Dubois, H. Prade, A unified view of ranking techniques for fuzzy numbers, Proc. IEEE Conf. on Fuzzy Syst, 3,1328-1333, 1999.
(Dub 99b)	D. Dubois, H. Prade and L. Ughetto, « Fuzzy logic, control engineering and artificial intelligence», in H.B. Verbruggen, H.J. Zimmerman and R. Babuska (Eds), Fuzzy algorithms for control, Kluwer Academic Publishers, pp. 17-57, 1999.
(Dub 00)	D. Dubois and H. Prade, editors, Fundamentals of Fuzzy sets, pages 195–228. Kluwer Academic Publishers, Boston, 2000.
(Dum 02)	Dumitrescu .M, Munteanu. A. Ulmeanu. P. «Fuzzy Logic System for Fuzzy Event Tree, Computing», First international IEEE symposium 'intelligent systems', September 2002.
(Dur 07)	R. Durga , K. Kushwaha, H. Verm and A. Srividya, «A. Quantification of epistemic and aleatory uncertainties in level-1 probabilistic safety assessment studies», Reliability Engineering and System Safety, 92, 947- 956, 2007.
(Dzi 06)	M. Dziubiñski, M. Frątczak, A. S. Markowski, « Aspects of risk analysis associated with major failures of fuel pipelines », Journal of Loss Prevention in the process industries, vol. 19, pp.399-408, 2006.

(Els 09)	T. Elsayed, « Fuzzy inference system for the risk assessment of liquefied naturel gas carriers during loading/offloading at terminals», J. Applied Ocean Research, 31, 179-185, 2009.
(Faé 00)	E. Faé et J.L. Durka, « Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de process industriels », Rapport Final INERIS, 2000.
(Fan 07)	J. S. Fang, M. S. Mannan, D. M. Ford, J. Logan, and A. Summers, «Value at risk perspective on layers of protection analysis», Process Safety and Environmental Protection, Trans IChemE, Part B, January 2007.
(Fla 94)	J.M. Flaus, « La régulation industrielle : régulateurs PID, prédictifs et flous », Coll. Traité des nouvelles technologies, Paris-Hermès, p.348, 1994.
(Gob 98)	W.M. Goble, «The use and development of quantitative reliability and safety analysis in new product design», University Press Facilities, Eindhoven, 1998.
(Gob 05)	M.W. Goble and H. Cheddie, «Safety Instrumented Systems Verification:Practical Probabilistic Calculations», ISA-The Instrumentation, Systems and Automation Society, 2005.
(Gou 03)	R. Gouriveau, « Analyse de risques, formalisation des connaissances et structuration des données pour l'intégration des outils d'étude et de décision », PhD thesis, Institut National Polytechnique de Toulouse, 2003.
(Gui 03)	Guidelines for Failure Mode and Effects Analysis for Automotive, Aerospace and General Manufacturing Industries, Dyadem Press, Co-Published and distributed by CRC Press, 2003.
(Gul 04)	W.G. Gulland, "Methods of determining safety integrity level (SIL) requirements Pros and Con, in Proc. of the 12th Annual Safety-Critical Systems Symp., February 17-19, pp. 105-122, 2004.
(Har 09)	L. Harms-Ringdal, « Analysis of Safety Functions and barriers in accidents», Safety Sci. 47, 353-363, 2009.
(Hau 01)	S. Hauge, P. Hokstad and T. Onshus, «The introduction of IEC 61511 in Norwegian offshore industry», in Proc. of ESREL, Torino, September 16-20, pp. 483-490, 2001.
(Hau 04)	U. Hauptamanns, «Semi quantitative fault tree analysis for process plant safety using frequency and probability ranges», J. Loss. Prev. Proc. Ind. 17, 339-345, 2004.
(Hou 02)	D. Hourtoulou, « ASSURANCE - ASSessment of the Uncertainties in Risk

	ANalysis of Chemical Establishments», Rapport final INERIS-DRA-007 472, 2002.
(HSE 01)	Health and Safety Executive (HSE), Reducing Risks, Protecting People-HSE Decision-making Process, Her Majesty's Stationery Office, London, 2001.
(HSE 99)	Health and Safety Executive (HSE) », Reducing Risk, Protecting People », Discussion Document. HMSO, London, 1999.
(FMC 88)	Potential Failure Mode and Effects Analvsis In Design (Design FMEA) and For Manufacturing and Assembly Processes (Process FMEA) Instruction Manual, Ford Motor Company, Dearborn, Michigan, 1988.
(ICS 09)	Institue pour une Culture de Sécurité Industrielle (ICSI), «Fréquence des événements initiateurs et disponibilité des barrières de protection et de prévention», disponible sur : http://www.icsi-eu.org/, 2009.
(ICS 11)	Institue pour une Culture de Sécurité Industrielle (ICSI), «Pratiques de la décision en situation d'incertitude- approche de l'incertitude», disponible sur : http://www.FonCSI.org/fr/, 2011.
(IEC 98)	Functional safety of electrical/electronic/programmable electronic safety related systems, IEC 61508 Standard, Parts 1-6, First edition, 1998.
(IEC 01)	IEC61882. Hazard and Operability Studies (HAZOP studies) –Application Guide, International Electrotechnical Commission (IEC), 2001.
(IEC 03)	IEC 61511 Standard, Functional Safety-Safety Instrumented Systems for the Process Industry Sector, Parts 1 and 3, First edition, 2003.
(IEE 84)	IEEE-Std-500, IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Station, 1984.
(ISO 99)	ISO, « Aspects liés à la sécurité : Principes directeurs pour les inclure dans les normes », Organisation internationale de normalisation, 1999.
(Inu 00)	M. Inuiguchi and J. Ramik, «Possibilistic linear programming: a brief review of fuzzy mathematical programming and a comparison with stochastic programming in portfolio selection problem», Fuzzy Sets and Syst. 111, 3-28, 2000.
(Kau 77)	A. kaufmann, « Introduction à la théorie des sous ensembles flous à l'usage des ingénieurs, Tome I : Eléments théoriques de base », 2ème édition, Ed. Masson, Paris, 1977.
(Kau 91)	A. Kaufman, M.M. Gupta, «Introduction to Fuzzy Arithmetic Theory and Application», Van Nostrand Reinhold, New York, 1991.
(Ken 91)	R. Kenarangui, «Event tree Analysis by fuzzy probability», IEEE Trans. on Reliab.40 (1991).120-124.
(Ken 10)	F. Kenneth, «Scenario identification and evaluation for layers of protection

	analysis», J. Loss Prev. Proc. Ind. 23, 705-718, 2010.
(Kha 12)	M. Khalil, M.A. Abdou, M.S. Mansour, H.A. Farag, M.E. Ossman, «A cascaded fuzzy- LOPA risk assessment model applied in natural gas industry», J. Loss Prev. Proc. Ind. 25, (2012) 877-882.
(Kir 99)	C. Kirchsteiger, «On the use of probabilistic and deterministic methods in risk analysis», Journal of Loss Prevention in the Process Industrials 12.PP 399-419.1999.
(Kir 05)	D. Kirkwood and B. Tibbs, «Developments in SIL determination», Comput. & Cont. Eng. J., vol. 16, pp. 21-27, 2005.
(Kli 04)	Z.H. Klim, « Preliminary hazard analysis for the design alternatives based on fuzzy methodology», IEEE Annual Meeting of the fuzzy information, processing NAFIPS' 04, Vol.1, 27-30 June, 46-50, 2004.
(Kum 93)	H. Kumamoto, «Fault tree analysis», New trends in system reliability evaluation, K.B. Misra editor, Elsevier Science Publischer, 1993.
(Kum 05)	E. Kumar, P. Kumar and R.S. kumar, Systemic failure mode effect analysis (FMEA) using fuzzy linguistic medelling. International Journal of Quality and Reliability Management. Vol.22 No.9, 2005.
(Kum 07)	H. Kumamoto, « Satisfying Safety Goals by Probabilistic Risk Assessment», Spriger – Verlag London, 2007.
(Lai 88)	F.S.Lai, S.Shenoi, and L.T Fan, «Fuzzy Fault Tree Analysis: Theory and Application», In Engineering risk and hazard Assessment, vol. I, CRC Press, Inc. Florida, (Eds) A. Kandel and E. Avni, pp.117-137, 1988.
(Lan, 07)	G. Landy, «AMDEC Guide pratique», Edition AFNOR, 2007.
(Le D 11)	T.D. Le Duy, «Traitement des incertitudes dans les applications des Études Probabilistes de Sûreté Nucléaire», Université de Technologie, Troyes, 2011.
(Lim 91)	N. Liminios, «Arbres de défaillances», Edition Hermes, Paris, 1991.
(Lee 90)	C.C. Lee, « Fuzzy logic in control systems: fuzzy logic controller », IEEE Transactions on Systems, Man and Cybernetics, vol. 20, pp. 404-435, 1990.
(Lee 96)	F.P. Lees, « Loss Prevention in the Process Industries», Volume1, Butterworth-Heinmann, Oxford, Second edition, 1996.
(Mac 04)	D. Macdonald, «Practical Industrial Safety, Risk Assessment, and Shutdown Systems», Elsevier Science & Technology Books, 2004.
(Mam 75)	E. H. Mamdani and S. Assilian, « An experiment in linguistic synthesis with a fuzzy logic controller», Int. J. of Man-Machine Studies, Vol. 7, pp. 1-13, 1975.

(Man 05)	S. Mannan « Lee's Loss Prevention in the Process Industries, Hazard Identification», Assessment and Control Volume 1, Third edition, 2005.
(Mar 06)	A.S. Markowski, M.S. Mannan, «Fuzzy logic application for LOPA», Proceedings of the 5th European Meeting on Chemistry and Environment (EMChIE), Vienna, Austria, May, 2006.
(Mar 12)	C.R. Marengo, J. Flores, A.L. Molina, R. Román, V. C. Vázquez, M. S. Mannan, «A formulation to optimize the risk reduction process based on LOPA», J. Loss Prev. Proc. Ind., 1-6, 2012.
(Mar 07)	A.S. Markowski, M.S. Mannan and A. Bigoszewska, « Fuzzy logic for process safety analysis», International Symposium of Process Sagety Center, 2007.
(Mar 08)	A. S. Markowski, M. Mannan, « Fuzzy Risk Matix », Journal of Hazardous Materials, 159, 152–157, 2008.
(Mar 09)	A.S. Markowski, M.S. Mannan, «Fuzzy logic for piping risk assessment (pfLOPA) », J. Loss. Prev. Proc. Ind. 22, 921-927, 2009.
(Mar 10)	A.S. Markowski, M.S. Mannan, A. Kotynia, D. Siuta, « Uncertainty aspects in process safety analysis», J. Loss. Prev. Proc. Ind. 23, 446-4542010.
(Mar 11)	A.S. Markowski, M. S. Mannan, A. Kotynia, H. Pawlak, «Application of fuzzy logic to explosion risk assessment», Journal of Loss Prevention in the Process Industries 24, 780-790, 2011.
(Mar 02)	E.M. Marszal, E.W. Scharpf, «Safety Integrity Level selection-Systematic Methods Including Layer of Protection Analysis», Instrumentation Syst. and Automation Society (ISA), 2002.
(Mas 92)	D.W. Massaro, « Broadening the domain of the fuzzy logical model of perception», in H.L. Pick, JR. P. Van Den Broek and D.C. Knill (Eds), Cognition: Conceptual and methodological issues, APA, Washington, DC, 1992.
(Mer 04)	M. M. Merad, « Analyse de l'état de l'art sur les grilles de criticité », rapport INERIS-DRA638, 16 Mars 2004.
(Moo 92)	H.C, Moon and I.A, Kwang, «Assessment of the potential applicability of fuzzy set theory to accident progression event trees phenomenological uncertainties», Reliability Engineering and System Safety 37, 237-252, 1992.
(Mue 07)	E. Muela, G. Schweickardt, F. Garcés, «Fuzzy possibilistic model for medium-term power generation planning with environmental criteria», Energy Pol. 35, 5643- 5655, 2007.
(Muh 04)	W.K. Muhlbauer, «Pipeline Risk Management Manual: Ideas, Techniques and Resources», Elsevier Inc. 2004.
(Mur 09)	S. Murè and M. Demichela, «Fuzzy application procedure (PAP) for the risk

	assessment of occupational accidents», J. Loss. Prev. Proc. Ind. 22, 593-599, 2010.
(Mye 12)	P.M. Layers, «Layer of Protection Analysis e Quantifying human performance in initiating events and independent protection layers», Journal of Loss Prevention in the Process Industries, 1-13,Available at http: //dx.doi.org/10.1016/j.jlp.2012.07.003,2012.
(Nai, 96)	R. Nait-Said, «Apport de la théorie des ensembles flous à la quantification des arbres de défaillance», Mémoire de Magister en Hygiène de Sécurité Industrielle, Université de Batna, 1996.
(Nai, 04)	R. Nait-Said, «Contribution subjective de la charge de travail par la théorie des ensembles flous», Thèse de doctorat, Institut d'Hygiène de Sécurité Industrielle, Université de Batna, 2004.
(Nai, 09)	R. Nait-Said, F. Zidani, N. Ouazraoui, «Modified risk graph method using fuzzy rule-based approach», J. Haz. Mat. 164, 651-658, 2009.
(Nie, 02)	E. Niel et E. Craye, «Maitrise des risques et sûreté de fonctionnement des systèmes de production», Hermes Science, LAVOISIER, 2002.
(OHS, 99)	OHSAS 18001, Système de management de la santé et de la sécurité au travail- Spécification -BSI, Afnor, 1999.
(Oua, 10)	N. Ouazraoui, N. Achouri, R. Nait Said et M. Bourareche «Apport de la logique floue à l'analyse de criticité des risques industriels», 17e Congrès de Maitrise des Risques et de Sûreté de Fonctionnement, 5-7 Octobre , La Roochelle 2010.
(Oua, 13)	N. Ouaztraoui, R. Nait Said, M. Bourareche and I. Sellami, «Layers of protection analysis in the framework of possibility theory», J. Haz. Mat. 262, 168– 178, 2013.
(ORE 02)	Offshore Reliability Data (OREDA), Offshore Reliability Data Handbook, 4th edition, 2002.
(Orm 04)	L. Ormos and I. Ajtonyi, « Soft computing method for determining the safety of technological system by 1EC 61508», presented at the First Romanian-Hungarian Joint Sympsiom on Applied computational Intelligence, Timisoara, May 25-26, 2004.
(Pel 94)	C.E. Peláez and J.B. Bowles, « Using fuzzy logic for system criticality analysis », In Proceedings Annual Reliability and Maintainability Symposium, Anaheim, California, pp. 449-455, January 24-27 1994.
(Pil 03)	Pillay and J. Wang, « Modified failure mode and effets analysis using approximate reasoning », Reliability Engineering & System Safety, 79, pp. 69-85, 2003.
(Ras 91)	K.Rasool, «Event Tree Analysis by Fuzzy Probability», IEEE Transaction On Reliability, Vol. 40, N0.1, 1991.

(Red 98)	F. Redmill, «IEC 61508: Principles and use in the management of safety», Comput. & Cont. Eng. J., pp. 205-213, 1998.
(Rog, 07)	J.-S. Roger Jang, N. Gulley, «MATLAB, Fuzzy Logic Toolbox», April 1997.
(Run 97)	T.A. Runkler, «Selection of appropriate defuzzification methods using application specific properties», IEEE Trans. on Fuzzy Syst., 5, 72-79, 1997.
(Sal 07)	M. Sallak, «Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception: application aux Systèmes Instrumentés de Sécurité », thèse de doctorat de l'institut national polytechnique de Lorraine, France, 2007.
(Sal 08)	M. Sallak, C. Simon, J.F. Aubry, « A Fuzzy Probabilistic for Determining Safety Integrity Level», IEEE Trans. on Fuzzy Syst., 16, 239-248, 2008.
(San 95)	S.A. Sandri, D. Dubois and H.W. Kalfsbeek, "Elicitation, Assessment, and pooling of expert judgments using possibility theory», IEEE Tran. on Fuzzy Syst., vol. 3, No 3, pp. 313-335, 1995.
(Sha 76)	G. A Shafer, «Mathematical Theory of Evidence», Princeton University Press, 1976.
(Sha 05)	R. K. Sharma, D. Kumar and P. Kumar, « Systemic failure mode effect analysis (FMEA) using fuzzy linguistic modeling », International Journal of Quality & Reliability Management, vol. 22, no 9, pp. 986-1004, 2005.
(Sha 10)	M. Shahrokhi and A. Bernard, «A development in energy flow/barrier analysis», J. Safety Science, 48, 598–606, 2010.
(Sim 07)	C. Simon, M. Sallak and J.F. Aubry, «SIL allocation of SIS by aggregation of experts opinions», Safety and Reliability Conference, June 25-27, Stavanger (Norway), 2007.
(Smi 11)	D. J. Smith and K.G. L. Simpson, «Safety Critical Systems Handbook», A Straightforward Guide to Functional Safety: IEC 61508 and Related Standards, Published by Elsevier Ltd 2011.
(Sin 90)	D. Singer , « A fuzzy set approach to fault tree and reliability analysis», Fuzzy Sets and Systems, 34:145–155, 1990.
(Siv, 07)	S. N. Sivanandam, S. Sumathi and S. N. Deepa, «Introduction to Fuzzy Logic using MATLAB», Springer-Verlag Berlin Heidelberg, 2007.
(Skl 06)	S .Sklet, «Safety barriers: Definition, classification, and performance», J. Loss Prev. Proc. Ind. 19 (2006) 494-506.
(Smi 04)	D.J. Smith and K.J.L Simpson, «Functional safety: A straightforward guide to applying IEC 61508 and related standards», 2nd edition, Elsevier Butterworth-

	Heinemann, 2004.
(Som 93)	K.P Soman. and K.B. Misra, «Fuzzy fault tree analysis using resolution identity 1», page 193, 1993.
(SON 07)	Methodology for Layer Of Protection Analysis, SONATRACH Company, Hassi-R'Mel, Rep. S-30-1240-140, 2007.
(SON, 08)	SONATRACH, Document SONATRACH DP HRM, 2008.
(Sum 03)	A.E. Summers, «Introduction to layers of protection analysis», J. Haz. Mat. 104, 163-168, 2003.
(Tan 83)	L.T. F. Tanaka, F. S. Lai, and K. Toguchi., «Fault tree analysis by fuzzy probability», IEEE Transactions on Reliability, 32: 453–457, 1983.
(Tim 04)	C.R. Timms, «IEC 61511-an aid to COMAH and safety case regulations compliance», Measurement & Cont. J., Vol. 37, Part 4, pp. 115-122, 2004.
(Vas 11)	D.Vasseur, T. Le Duy, A. Dieulle, and C.Bérenguer, Uncertainty analysis in probabilistc risk assessment : Comparison of probabilistic and non probabilistic approach, In *Proceeding of the ESREL 2011 Conference* Troyes, France, 2011.
(Ver 07)	A.K Verma, A.Srividia and R.S.P Gaonar, «Fuzzy-Reliability Engineering, concepts and application», Narosa Publishing House, Nez Delhi, 2007.
(Vil 88)	A. Villemeur, «Sûreté de fonctionnement des systèmes industriels », Eyrolles, 1998.
(Vin 06)	W. J. Vincoli, «Basic Guide to System Safety», WILLEY- INTERSCIENCE, Second Edition, 2006.
(Wan 04)	Y.Wan, H.H. West and M.S. Mannan, «The impact of data uncertainty in determination safety integrity level», Trans Institution of Chemical Engineers, 2004.
(Wei 08)	C.Wei, W.J. Rogers and M.S. Mannan, «Layers of protection analysis for reactive chemical risk assessment», J. Haz. Mat. 159, 19-24, 2008.
(Whi 06)	White Paper Report, «SIL Determination Technique », ACM Facility Safety, 2006.
(Xu 02)	K. Xu, L. C. Tang, M. Xie, S. L. Ho, and M. L. Zhu, « Fuzzy assessment of FMEA for engine systems », Reliability Engineering & System Safety, vol. 75, no. 1, pp. 17–29, 2002.
(Yeo 05)	K.T. Yeou and B.C. Yen, «Hydrosystems engineering uncertainty analysis», McGraw-Hill, 2005.

(Zad 65)	L. Zadeh, « Fuzzy sets », Information and Control, vol. 8, pp. 338–353, 1965.
(Zad 73)	L. Zadeh, «Outline of a New Approach to the Analysis of Complex Systems and Decision Processes», IEEE Trans. Syst. Man Cyb. 3 (1973) 28-44.
(Zad 75)	L. Zadeh, « The concept of a linguistic variable and its application to approximate reasoning-I-II», Information Sciences, vol. 8, no. 3, pp. 199-249, 301-357, 1975.
(Zad 78)	L. Zadeh, « Fuzzy sets as a basis for a theory of possibility », Fuzzy Sets and Systems, vol. 1, pp. 3–28, 1978.
(Zad 79)	L. Zadeh, « A theory of approximate reasoning», I, J. Hayes, D. Michie, and L.I. Mikulich, Eds, Machine Intelligence, vol.9, New York: Halstead press, pp. 149-194, 1979.
(Zad 83)	L. Zadeh, « The role of fuzzy logic in the management of uncertainty in expert systems», Fuzzy sets and systems, 11, PP. 199-227, 1983.
(Zad 92)	L.A., Zadeh, « The calculus of fuzzy if/then rules », AI Expert, vol. 7, pp.23-27, 1992.
(Zio 07)	E. Zio, «An introduction to the basics of reliability rho risk analysis», World Scientific Publishing Co. Re. Ltd., 2007.
(Zou 97)	L. M. Zouhal, «Contribution à l'application de la théorie des fonctions de croyance en reconnaissance des formes», PhD thesis, Université de Compiègne, France, 1997.
(Zun 08)	G.A. Zuniga, «Layer of protection analysis applied to ammonia refrigeration systems», Master's thesis, Texas A&M University, Available at http : //hdl .handle .net /1969 .1 /ETD -TAMU -3133, 2008.

Annexes

ANNEXE 1 :
Développement de scénarios d'accident par HAZOP

Tab. A.1 : Etude de HAZOP appliquée au système industriel « Four rebouilleur H101 »

TITRE DE L'ÉTUDE : Four Rebouilleur H-101									
N° du dessin (P&ID) : 9345.10-A1-006-B				N° de RÉVISION : 1					DATE : 15-30/03/2008
PARTIE CONSIDERÉE : Serpentin du four depuis l'admission du condensât (avant la mesure du débit), jusqu'à la sortie (après contrôle de la température)					INTENTION DE CONCEPTION :	Entrées :	Alimentation en condensât, chaleur du four		
						Activités :	Vaporisation partielle, surchauffe et transfert du condensât au processus		
N°	Mot-guide	Élément	Déviation	Causes possibles	Conséquences	Protection	Commentaire	Mesures à prendre	Responsable des mesures
1	NE PAS FAIRE/ MOINS	Débit du condensât	Pas/ Moins de débit	Mauvaise manipulation sur la vanne manuelle à l'entrée/sortie de la vanne FICA-136V (fermée)	Pas du liquide dans H-101, endommagement de serpentin (incendie) et arrêt d'unité (possible arrêt module)	. Opérateurs . FICAL-136 : alarme (≤ 150 t/h) . FZL-137 : (≤ 120 t/h) arrêt d'urgence de H-101			
				Mauvais fonctionnement de la vanne FICA-136V (fermée)	Pas du liquide dans H-101, endommagement de serpentin (incendie) et arrêt d'unité (possible arrêt module)	. FICAL-136 : alarme (≤ 150 t/h) . FZL-137 : (≤ 120 t/h) arrêt d'urgence de H-101			
				Mauvaise manipulation sur l'une des vannes manuelles à l'entrée de H-101 (fermée)	Pas de débit dans l'un des pass. du H-101, température élevée, endommagement de serpentin (incendie) et arrêt d'unité (possible arrêt module)	. FI-138 : indication . TRAH-121-3: alarme (≥ 295°C) . FICAL-136 : alarme (≤ 150 t/h) . FZL-137 : (≤ 120 t/h) arrêt d'urgence de H-101 . Opérateurs			

Tab. A.1 : Etude de HAZOP appliquée au système industriel « Four rebouilleur H101 » (Suite).

TITRE DE L'ÉTUDE : Four Rebouilleur H-101									
N° du dessin (P&ID) : 9345.10-A1-006-B			N° de RÉVISION : 1					DATE : 15-30/03/2008	
PARTIE CONSIDERÉE : Serpentin du four depuis l'admission du condensât (avant la mesure du débit), jusqu'à la sortie (après contrôle de la température)					INTENTION DE CONCEPTION :	Entrées : Alimentation en condensât, chaleur du four Activités : Vaporisation partielle, surchauffe et transfert du condensât au processus			
N°	Mot-guide	Élément	Déviation	Causes possibles	Conséquences	Protection	Commentaire	Mesures à prendre	Responsable des mesures
2	PLUS	Température du condensât	Plus de température	Mauvais fonctionnement de la vanne TRCA-109V (ouverte), combustion importante dans le H-101	Température élevée à la sortie du H-101, endommagement possible du serpentin (incendie) et arrêt de l'unité (possible arrêt module)	. Opérateurs . FICAL-136 : alarme (≤ 150 t/h) . FZL-137 : (≤ 120 t/h) arrêt d'urgence du H-101			
3	MOINS		Moins de température	Mauvais fonctionnement de la vanne TRCA-109V (fermée), faible combustion dans H-101	Basse température à la sortie du H-10, passage possible de produit en OFF-SPEC	. TI-135 : indication			
4	NE PAS FAIRE/ MOINS	Débit du gaz combustible	Pas/ Moins de débit	Mauvais fonctionnement des vannes UZ-125/B (fermées)	Pas de fuel gaz pour le H-101, basse pression du fuel gaz, basse température à la sortie du H-101, passage possible de produit en OFF-SPEC	. PAL-126 : alarme (≤ 0,4 Kg/cm^2) . FRAL-142 : alarme (≤ 125 Nm^3/h) . TRCA-109 : indication			
				Mauvais fonctionnement de la vanne UZ-125C (ouverte)	Pas de fuel gaz pour le H-101, basse pression de fuel gaz, basse température à la sortie du H-101, passage possible de produit en OFF-SPEC Dégagement de fuel gaz en atmosphère, explosion possible et arrêt de l'unité (possible arrêt module)	. PAL-126 : alarme (≤ 0,4 Kg/cm^2) . PZL-127 : (≤ 0,2 Kg/cm^2) arrêt d'urgence du H-101 . FRAL-142 : alarme (≤ 125Nm^3/h) . TRCA-109 : indication			

Tab. A.1 : Etude de HAZOP appliquée au système industriel « Four rebouilleur H101 » (Suite).

TITRE DE L'ÉTUDE : Four Rebouilleur H-101									
N° du dessin (P&ID) : 9345.10-A1-006-B			N° de RÉVISION : 1					DATE : 15-30/03/2008	
PARTIE CONSIDERÉE : Serpentin du four depuis l'admission du condensât (avant la mesure du débit), jusqu'à la sortie (après contrôle de la température)			INTENTION DE CONCEPTION :		Entrées : Alimentation en condensât, chaleur du four Activités : Vaporisation partielle, surchauffe et transfert du condensât au processus				
N°	Mot-guide	Élément	Déviation	Causes possibles	Conséquences	Protection	Commentaire	Mesures à prendre	Responsable des mesures
4	NE PAS FAIRE/ MOINS	Débit du gaz combustible	Pas/ Moins de débit	Mauvaise manipulation sur la vanne manuelle à l'entrée/sortie de la vanne TRCA-109V (fermée)	Pas de fuel gaz pour le H-101, basse pression du fuel gaz, basse température à la sortie du H-101, passage possible de produit en OFF-SPEC	. Opérateurs (locaux) . AL-126 : alarme ($\leq$ 0,4 Kg/cm^2) . PZL-127 : ($\leq$ 0,2 Kg/cm^2) arrêt d'urgence du H-101 . FRAL-142 : alarme ($\leq$ 1250 Nm^3/h) . TRCA-109 : indication			
				Mauvais fonctionnement de la vanne TRCA-109V (fermée)	Pas de fuel gaz pour le H-101, basse pression de fuel gaz, basse température à la sortie du H-101, passage possible de produit en OFF-SPEC	. PAL-126 : alarme ($\leq$ 0,4 Kg/cm^2) . PZL-127 : ($\leq$ 0,2 Kg/cm^2) arrêt d'urgence du H-101 . FRAL-142 : alarme ($\leq$ 1250 Nm^3/h)			
5	PLUS	Débit du gaz combustible	Pas/ Moins de débit	Mauvaise manipulation sur la vanne manuelle à l'entrée/sortie de la vanne TRCA-109V (fermée)	Haut débit du fuel gaz pour le H-101, haute pression du fuel gaz pour les brûleurs, haute température à la sortie du H-101, (incendie) et arrêt de l'unité (possible arrêt module)	. FRA-142 : indication . PA H-126 : alarme ($\geq$ 1,5 Kg/cm^2) . PZ H-127 : ($\geq$ 1,9 Kg/cm^2) arrêt d'urgence de H-101 . TI-135 : indication . TZ H-108 : ($\geq$ 300°C) arrêt d'urgence			
6	MOINS	Débit d'air	Moins de débit	Mauvais fonctionnement de HXC-908V/907V (trop fermés)	Combustion incomplète, pression élevée à l'intérieur de H-101, explosion possible & arrêt d'unité (possible arrêt module)	. PIA H-904 : alarme ($\geq$ 10 mmH_2O) . Trappe d'explosion			

ANNEXE 2 :
Exemple d'étalonnage du graphe de risque général (IEC, 03)

Tableau D.2 – Exemple d'étalonnage du graphe de risque général

Paramètre de risque		Classification	Commentaires
Conséquence (C) Nombre d'accidents mortels Ce paramètre peut être calculé en déterminant le nombre de personnes présentes lorsque la zone exposée au danger est occupée et en multipliant par la vulnérabilité au danger identifié. La vulnérabilité est déterminée par la nature du danger contre lequel la protection est assurée. Les facteurs suivants peuvent être utilisés: V=0,01 Faible déversement ou dégagement de matériau inflammable ou toxique V=0,1 Important déversement ou dégagement de matériau inflammable ou toxique V=0,5 Comme ci-dessus, mais aussi une haute probabilité d'incendie ou matériau très toxique V=1 Rupture ou explosion	C_A C_B C_C C_D	Lésion mineure Plage de 0,01 à 0,1 Plage de >0,1 à 1,0 Plage > 1,0	1 Le système de classification a été établi pour traiter les blessures infligées aux personnes ou les décès. 2 Pour l'interprétation de C_A, C_B, C_C et C_D, il convient de tenir compte des conséquences de l'accident et du rétablissement normal
Occupation (F) Ce paramètre est calculé en déterminant la durée proportionnelle pendant laquelle la zone exposée au danger est occupée pendant les périodes normales de travail. NOTE 1 Si le temps de séjour dans la zone dangereuse est différent selon l'équipe d'exploitation, il convient alors de choisir le temps maximal. NOTE 2 L'utilisation du paramètre F_A n'est appropriée que s'il est possible de démontrer que le taux de sollicitation est aléatoire et qu'il n'est pas lié à la période durant laquelle l'occupation est supérieure à la normale. C'est habituellement le cas avec des sollicitations qui se produisent au moment du démarrage des équipements ou pendant la recherche d'anomalies.	F_A F_B	Exposition rare à plus fréquente dans la zone dangereuse. L'occupation est inférieure à 0,1 Exposition fréquente à permanente dans la zone dangereuse	3 Voir commentaire 1 ci-dessus.
Probabilité (P) pour que l'événement dangereux soit évité en cas de défaillance du système de protection.	P_A P_B	Adoptée si toutes les conditions de la colonne 4 sont remplies Adoptée si toutes les conditions ne sont pas remplies	4 Il convient de choisir P_A uniquement si toutes les conditions suivantes sont vraies: – des moyens sont prévus pour avertir l'opérateur de la défaillance du SIS ; – des moyens indépendants sont prévus pour arrêter le procédé afin d'éviter le danger ou pour permettre aux personnes d'être évacuées vers une zone sûre ; – le temps, entre le moment où l'opérateur est averti et le moment où un événement dangereux se produit, dépasse 1 h ou est finalement suffisant pour entreprendre les actions nécessaires.
Taux de sollicitation (W) Le nombre de fois par an où l'événement dangereux est susceptible de se produire en l'absence d'un SIS. Pour déterminer le taux de sollicitation, il est nécessaire de considérer toutes les sources de défaillance susceptibles de provoquer un événement dangereux. Lors de la détermination du taux de sollicitation, il faut accorder une confiance limitée aux performances et à l'intervention du système de commande. Les performances, qui peuvent être revendiquées si le système de commande n'est pas conçu et entretenu conformément à la CEI 61511, sont limitées à des valeurs inférieures aux plages de performances associées au niveau d'intégrité de sécurité SIL1	W_1 W_2 W_3	Taux de sollicitation inférieur à 0,1D par an Taux de sollicitation entre 0,1D et D par an Taux de sollicitation entre D et 10D par an Pour des taux de sollicitation supérieurs à 10D par an, une intégrité plus élevée est nécessaire	5 Le but du facteur W est d'estimer la fréquence du danger qui apparaît sans l'ajout du SIS. Si le taux de sollicitation est très élevé, le SIL doit être déterminé par une autre méthode ou le graphe de risque doit être étalonné une nouvelle fois. Il convient de noter qu'il est possible que les méthodes utilisant des graphes de risques ne constituent pas la meilleure approche dans le cas d'applications fonctionnant en mode continu, se reporter au paragraphe 3.2.43.2 de la CEI 61511–1. 6. Il convient de déterminer la valeur de C à partir de critères propres à la société concernant le risque tolérable en tenant compte d'autres risques auxquels des personnes peuvent être exposées.
NOTE Il s'agit d'un exemple destiné à illustrer l'application des principes pour la conception des graphes de risques. Les graphes de risques relatifs à des applications particulières et à des dangers particuliers devront faire l'objet d'un accord entre les parties concernées, en tenant compte du risque tolérable, se reporter aux Articles D.1 à D.6.			