



**HAL**  
open science

# Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis

Walid Mechri

► **To cite this version:**

Walid Mechri. Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis. Automatique / Robotique. Université de Tunis El-Mana, 2011. Français. ⟨NNT : ⟩. ⟨tel-00653078⟩

**HAL Id: tel-00653078**

**<https://theses.hal.science/tel-00653078v1>**

Submitted on 17 Dec 2011

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization



Université de Tunis El Manar



# THÈSE

présentée à

**l'Ecole Nationale d'Ingénieurs de Tunis**

pour l'obtention du

**Doctorat en Génie Electrique**

par

**Walid MECHRI**

Ingénieur en Génie Electrique de l'ENIM

---

## Évaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis

---

Soutenue le 11 Avril 2011 devant le Jury d'Examen :

MM.

*Président :* Moncef GUESMI

*Rapporteurs :* Mohamed Naceur ABDELKRIM  
Faouzi BEN AMMAR

*Examineurs :* Dhaou SOUDANI  
Kamel BEN OTHMAN (Directeur de Thèse)  
Christophe. SIMON (Co-encadreur)

---

Unité de recherches LARA Automatique 99/UR/11-08 ENIT



# Evaluation de la performance des systèmes instrumentés de sécurité à paramètres imprécis

## Mots Clés :

Systèmes instrumentés de sécurité, arbre de défaillances, chaînes de Markov, imprécision, incertitudes, nombres flous, probabilités imprécises, niveau d'intégrité de sécurité.

## Résumé :

Dans ce travail, le problème d'imprécision dans l'évaluation de la performance des systèmes instrumentés de sécurité est traité. Deux méthodes d'évaluation sont appliquées à un SIS. La première méthode d'évaluation utilise les arbres de défaillances, la seconde se base sur les chaînes de Markov.

L'imperfection des données concerne les paramètres caractéristiques des SIS, tels que le taux de défaillance et le facteur de défaillance de cause commune. Les probabilités élémentaires sont remplacées par des modèles mathématiques permettant aux experts fiabilistes d'exprimer leur incertitude dans l'énoncé des valeurs de probabilités de défaillances et d'autres paramètres des systèmes. Nous montrons comment l'imprécision sur la valeur de taux de défaillance induit des variations particulièrement significatives sur la qualification du niveau d'intégrité de sécurité du système.

Ce travail peut avoir beaucoup d'intérêt pour le décideur de connaître l'imprécision sur les paramètres de performance des systèmes.

# Performance evaluation of safety instrumented systems to imprecise parameters

## **Keywords :**

Safety instrumented systems, fault tree, Markov chains, imprecision, uncertainty, fuzzy numbers, imprecise probabilities, safety integrity level.

## **Abstract :**

This work analyses the problem of epistemic uncertainty in assessing the performance evaluation of safety instrumented systems (SIS). Two evaluation methods are applied to an SIS. The first evaluation method uses the faults trees; the second method is based on the use of the Markov chains.

The imperfect knowledge concerns the parameters characteristic of the SIS, such as such as the failure rate and common cause failure factor. The elementary probabilities of fault trees are replaced by mathematical models allowing experts to express their uncertainty in the unreliability values and other system parameters. We show how the imprecision on the characteristic parameter values, such as the common cause failure factor, induces significant changes on the safety integrity level of a safety instrumented systems.

This work shows how it interests the decision maker knowing the uncertainty on the performance parameters.

# Performance evaluation of safety instrumented systems to imprecise parameters

## **Keywords :**

Safety instrumented systems, fault tree, Markov chains, imprecision, uncertainty, fuzzy numbers, imprecise probabilities, safety integrity level.

## **Abstract :**

This work analyses the problem of epistemic uncertainty in assessing the performance evaluation of safety instrumented systems (SIS). Two evaluation methods are applied to an SIS. The first evaluation method uses the faults trees; the second method is based on the use of the Markov chains.

The imperfect knowledge concerns the parameters characteristic of the SIS, such as such as the failure rate and common cause failure factor. The elementary probabilities of fault trees are replaced by mathematical models allowing experts to express their uncertainty in the unreliability values and other system parameters. We show how the imprecision on the characteristic parameter values, such as the common cause failure factor, induces significant changes on the safety integrity level of a safety instrumented systems.

This work shows how it interests the decision maker knowing the uncertainty on the performance parameters.

*A mon cher père  
A ma chère mère  
A mon frère et mes soeurs  
A tous mes amis  
A ceux qui m'aiment  
A ceux que j'aime*

## Avant propos

Le travail présenté dans ce mémoire a été effectué à l'Unité de Recherche LARA Automatique de l'ENIT, dirigée par Monsieur le Professeur Mohamed BENREJEB, sous la direction de Monsieur Kamel BEN OTHMAN, Maître de conférences, en collaboration avec le Centre de Recherche en Automatique de Nancy, CRAN de l'INPL, sous la responsabilité de Monsieur Christophe SIMON. Qu'ils trouvent ici l'expression de ma gratitude pour l'aide et les conseils qu'ils m'ont prodigué tout au long de la réalisation de ce travail.

J'exprime mes plus vifs remerciements à Monsieur Moncef GUESMI, Professeur à l'Institut National des Sciences Appliquées et de Technologie de Tunis, qui a bien voulu me faire l'honneur de présider ce jury.

Je remercie Monsieur Mohamed Naceur ABDELKARIM, Professeur à l'Ecole Nationale d'Ingénieurs de Gabès et Monsieur Faouzi BEN AMMAR, Professeur à l'Institut National des Sciences Appliquées et de Technologie de Tunis, pour l'intérêt qu'ils ont manifesté à l'égard de mon travail et d'en être les rapporteurs.

J'exprime ma reconnaissance à Monsieur Dhaou SOUDANI, Maître de conférences à l'Ecole Nationale d'Ingénieurs de Tunis, qui a accepté d'examiner ce travail.

Je tiens à exprimer ma profonde reconnaissance à Monsieur Christophe SIMON, Co-encadreur de thèse, Maître de conférences à l'Ecole Supérieure des Sciences et Techniques d'Ingénieurs de Nancy, qui m'a suivi et guidé durant l'élaboration de ce travail. Je le remercie pour son aide et sa disponibilité.

J'exprime mes profonds remerciements et ma reconnaissance à Monsieur Kamel BEN OTHMAN, directeur de thèse, Maître de conférences à l'Institut Supérieur des Sciences et de Technologie de l'Energie de Gafsa, pour son aide inestimable, sa patience, sa disponibilité et son encouragement tout au long de ce travail.

Enfin, qu'il me soit permis d'exprimer mes remerciements à tous les membres de l'Unité de Recherche LARA Automatique et du groupe thématique SURFDIAG du CRAN, pour leur assistance amicale.

# Table des matières

<b>Table des figures</b>	<b>xi</b>
<b>Liste des tableaux</b>	<b>xiii</b>
<b>Production personnelle</b>	<b>xiv</b>
<b>Liste des acronymes</b>	<b>xvi</b>
<b>Introduction générale</b>	<b>xvii</b>

## Chapitre 1

### Normes et méthodes pour l'évaluation des performances des systèmes instrumentés de sécurité

1.1	Introduction . . . . .	3
1.2	Principaux concepts de sécurité . . . . .	3
1.2.1	Notion de sécurité . . . . .	4
1.2.2	Notion de danger . . . . .	4
1.2.3	Notion de risque . . . . .	4
1.2.4	Sécurité fonctionnelle . . . . .	5
1.2.5	Systèmes E/E/EP relatifs aux applications de sécurité . . . . .	6
1.3	Normes relatives aux Systèmes Instrumentés de Sécurité . . . . .	6
1.3.1	Norme IEC 61508 et ses normes filles . . . . .	6
1.3.1.1	La norme IEC 61511 . . . . .	8
1.3.1.2	La norme IEC 62061 . . . . .	9
1.3.1.3	La norme IEC 61513 . . . . .	9
1.3.1.4	La norme EN 50126 . . . . .	9
1.3.2	Le Concept de Système Instrumenté de Sécurité . . . . .	9
1.3.2.1	Constitution d'un SIS . . . . .	10

1.3.2.2	Systèmes de protection à intégrité élevée (HIPS) . . . . .	11
1.3.2.3	Fonction Instrumentée de Sécurité . . . . .	11
1.3.3	Paramètres de performance de sécurité des SIS . . . . .	12
1.3.3.1	Probabilité moyenne de défaillance à la demande . . . . .	12
1.3.3.2	Probabilité de défaillance dangereuse par heure (PFH) . . . . .	12
1.3.4	Notion de niveau d'intégrité de sécurité (SIL) . . . . .	12
1.3.5	Classification des défaillances dans la norme IEC 61508 . . . . .	14
1.3.6	Tests et stratégies des tests des SIS . . . . .	15
1.3.7	Les facteurs caractéristiques des SIS . . . . .	16
1.3.7.1	Taux de couverture de diagnostic . . . . .	16
1.3.7.2	Défaillances de causes communes . . . . .	17
1.3.8	Limites de la norme IEC 61508 . . . . .	17
1.4	Détermination des niveaux de sécurité des SIS . . . . .	18
1.4.1	Les méthodes qualitatives . . . . .	18
1.4.1.1	Graphe de risque . . . . .	18
1.4.1.2	Matrice de risque . . . . .	19
1.4.2	Les méthodes quantitatives . . . . .	19
1.4.2.1	Les équations simplifiées . . . . .	19
1.4.2.2	Blocs diagramme de fiabilité . . . . .	20
1.4.2.3	Arbres de défaillance . . . . .	20
1.4.2.4	Chaînes de Markov . . . . .	24
1.4.2.5	Chaînes de Markov multiphase . . . . .	28
1.5	Conclusion . . . . .	29

<p><b>Chapitre 2</b></p> <p><b>Méthodes et techniques pour l'évaluation</b></p> <p><b>des systèmes à paramètres imprécis</b></p>
--

2.1	Introduction . . . . .	32
2.2	Terminologie des informations imparfaites . . . . .	32
2.3	Représentation des connaissances imparfaites . . . . .	32
2.3.1	Théorie des probabilités . . . . .	33
2.3.2	Théorie des intervalles . . . . .	35
2.3.2.1	Opérations logiques sur les intervalles . . . . .	35
2.3.2.2	Opérations arithmétiques sur les intervalles . . . . .	36
2.3.3	Théorie des sous-ensembles flous . . . . .	37

---

2.3.3.1	Opérations de base des sous-ensembles flous . . . . .	38
2.3.3.2	Nombres flous . . . . .	39
2.3.3.3	Nombres flous de type $L - R$ . . . . .	39
2.3.3.4	Notion d' $\alpha$ -coupe . . . . .	40
2.3.4	Théorie des possibilités . . . . .	41
2.3.5	Théorie des fonctions de croyance . . . . .	42
2.3.6	Théorie de familles de probabilités cumulées : p-boxe . . . . .	42
2.3.6.1	Propagation de l'incertitude dans le cadre des P-boxes . . . . .	43
2.3.6.2	Discrétisation d'une P-box . . . . .	44
2.3.6.3	Opérations mathématiques des p-boxes . . . . .	45
2.4	Méthodes pour l'évaluation des performances des systèmes en présence d'informations imprécises . . . . .	47
2.4.1	Méthodes d'évaluations par arbres de défaillances à paramètres imprécis . . . . .	47
2.4.1.1	Méthode de Singer . . . . .	48
2.4.1.2	Méthode des $\alpha$ -coupes . . . . .	49
2.4.2	Evaluation par les chaînes de Markov des systèmes à paramètres imprécis . . . . .	51
2.4.2.1	Chaînes de Markov à probabilités de transitions floues . . . . .	52
2.4.2.2	Méthode des $\alpha$ -coupes . . . . .	53
2.4.2.3	Modèle de Markov avec un système d'inférence flou (MMF) . . . . .	53
2.5	Conclusion . . . . .	58

### Chapitre 3

#### Contribution à l'évaluation par arbres de défaillances des performances des SIS à paramètres imprécis

3.1	Introduction . . . . .	61
3.2	Paramètres de performance des SIS . . . . .	61
3.2.1	Défaillances de Causes Communes (DCC) . . . . .	62
3.2.2	Les différents modèles des DCC . . . . .	62
3.2.2.1	Modèle du facteur $\beta$ . . . . .	63
3.2.2.2	Méthode des lettres grecques multiples (MGL) . . . . .	63
3.2.2.3	Méthode du facteur $\alpha$ . . . . .	63
3.2.2.4	Méthode PDS . . . . .	64
3.2.3	Mise en œuvre du facteur $\beta$ . . . . .	64

3.3	Eléments théoriques de l'approche d'évaluation probabiliste floue . . . . .	67
3.3.1	Nombres flous triangulaires . . . . .	67
3.3.1.1	Probabilités floues . . . . .	68
3.3.1.2	Intervalles flous . . . . .	70
3.3.1.3	Facteurs de DCC flous . . . . .	70
3.3.2	Proposition d'évaluation par arbres de défaillances flous . . . . .	71
3.3.3	Application : Etude d'un HIPS . . . . .	73
3.3.3.1	Proposition de l'évaluation de la $PF D_{avg}$ par une approche probabiliste floue . . . . .	75
3.3.3.2	Validation de l'approche proposée par simulation de Monte Carlo . . . . .	79
3.3.3.3	Importance des sources d'informations . . . . .	82
3.3.4	Conclusion partielle . . . . .	84
3.4	Evaluation des performances des SIS à l'aide des P-boxes . . . . .	84
3.4.1	Les P-boxes . . . . .	85
3.4.2	Modélisation de l'imprécision des DCC à l'aide des P-boxes . . . . .	87
3.4.2.1	Evaluation imprécise de la $PF D_{avg}$ . . . . .	88
3.5	Conclusion . . . . .	91

## Chapitre 4

### Contribution à l'évaluation des performances des SIS à paramètres imprécis par chaînes de Markov

4.1	Introduction . . . . .	94
4.2	Evaluation quantitative des SIS . . . . .	94
4.2.1	Les paramètres caractéristiques des SIS . . . . .	95
4.2.1.1	Taux de couverture de diagnostic DC . . . . .	95
4.2.1.2	Défaillances de mode commun . . . . .	95
4.2.2	Evaluation de la $PF D_{avg}$ à l'aide des Chaînes de Markov . . . . .	96
4.3	Proposition d'évaluation de la $PF D_{avg}$ par l'approche intervalles . . . . .	98
4.3.1	Chaînes de Markov à intervalles . . . . .	98
4.3.2	Modélisation des paramètres caractéristiques des SIS par intervalles . . . . .	99
4.3.3	Application à un HIPS . . . . .	101
4.3.3.1	Présentation du système . . . . .	101
4.3.3.2	Utilisation des chaînes de Markov multiphases à intervalles . . . . .	102
4.3.3.3	Validation par une approche aléatoire . . . . .	110

---

4.3.3.4	Conclusion partielle . . . . .	111
4.4	Chaînes de Markov multiphases floues pour l'évaluation de la $PFD_{avg}$ . . .	111
4.4.1	Présentation des chaînes de Markov floues . . . . .	112
4.4.2	Modélisation des paramètres caractéristiques des SIS par des nombres flous . . . . .	114
4.4.3	Application au HIPS . . . . .	115
4.4.3.1	Approche des chaînes de Markov multiphase floue . . . . .	115
4.4.3.2	Validation de l'approche floue par une approche aléatoire .	118
4.4.3.3	Comparaison entre l'approche proposée et l'approche aléa- toire . . . . .	120
4.5	Conclusion . . . . .	121
	<b>Conclusion générale</b>	<b>123</b>
	<b>Bibliographie</b>	<b>125</b>

# Table des figures

1.1	Courbe de Farmer [35]	5
1.2	Les normes sectorielles de l'IEC 61508 [98]	7
1.3	Utilisateurs de l'IEC 61508 et l'IEC 61511 [79]	8
1.4	Structure d'un SIS [55]	10
1.5	Classification des défaillances [58]	15
1.6	Composant périodiquement testé [99]	28
2.1	Nombre flou triangulaire du type $L - R$	40
2.2	Représentation d'une p-boxe	43
2.3	Discrétisation d'une P-boxe	44
2.4	La p-boxe de la variable $X$	45
2.5	La p-boxe de la variable $Y$	46
2.6	La p-boxe résultante $Z = X.Y$	47
2.7	Exemple d'arbre de défaillances	50
2.8	Probabilité d'occurrence de l'évènement indésirable (EI)	51
2.9	Schéma général de construction de Modèle de Markov Flou	54
2.10	Bloc diagramme de fiabilité de l'exemple	55
2.11	Graphe de Markov du système	55
2.12	La température $T$ en fonction de la saison	56
2.13	Les taux de défaillance $\lambda_A$ et de réparation $\mu_A$	56
2.14	L'indisponibilité du système en fonction de la température pour $T=30^\circ\text{C}$	58
3.1	Machines A et B en parallèle exposé à la DCC	65
3.2	Arbre de défaillances du système exposé à la DCC	66
3.3	$\alpha$ -coupes d'une probabilité floue $\tilde{p}_X$	69
3.4	Schéma fonctionnel du HIPS	73
3.5	Bloc-Diagramme de fiabilité du HIPS	74
3.6	Arbre de défaillances relatif au HIPS	75
3.7	La $P\tilde{F}D$ et $P\tilde{F}D_{avg}$ du HIPS dans le cas 1, pour $\alpha = 0$ and $\alpha = 1$	77
3.8	$P\tilde{F}D_{avg}$ floue du HIPS pour le cas 1	77
3.9	Variation de la $PFD$ et la $P\tilde{F}D_{avg}$ du HIPS pour le cas 2	78
3.10	$P\tilde{F}D_{avg}$ floue du HIPS pour le cas 2	79
3.11	Densité de probabilité de la loi uniforme	80
3.12	Densité de probabilité de la loi triangulaire	81
3.13	Histogrammes des résultats de la simulation de Monte Carlo	82

---

3.14	Distribution cumulée supérieure et inférieure de la $PFD_{avg}$ . . . . .	83
3.15	Représentation d' une p-boîte de type uniforme . . . . .	86
3.16	Représentation du facteur de DCC par une p-boîte de type uniforme. . . . .	87
3.17	P-boîte résultante de la $PFD_{avg}$ du HIPS . . . . .	90
4.1	Schéma fonctionnel d'un HIPS . . . . .	101
4.2	Bloc-diagramme de fiabilité du HIPS . . . . .	102
4.3	Modèle de Markov multiphases relatif au sous système capteurs en architecture 2oo3 . . . . .	104
4.4	Enchaînement des phases de l' architecture 2oo3 . . . . .	105
4.5	Modèle de Markov multiphases relatif au sous système unité logique de traitement . . . . .	106
4.6	Modèle de Markov multiphases relatif au sous système actionneurs . . . . .	107
4.7	Enchaînement des phases dans l' architecture 1oo2 . . . . .	108
4.8	Variation de la $[PFD]$ et $[PFD_{avg}]$ du HIPS . . . . .	109
4.9	Distribution de la $PFD_{avg}$ . . . . .	110
4.10	Variation de la $P\tilde{F}D$ du HIPS ainsi que sa $P\tilde{F}D_{avg}$ pour ( $\alpha = 0$ et $\alpha = 1$ ) . . . . .	117
4.11	La $P\tilde{F}D_{avg}$ floue du HIPS étudié . . . . .	118
4.12	Histogramme de la $PFD_{avg}$ du tirage de Monte Carlo . . . . .	119
4.13	Convergence des bornes estimées de la $PFD_{avg}$ en fonction du nombre de tirage . . . . .	120
4.14	Comparaison entre l'approche floue et aléatoire . . . . .	121

# Liste des tableaux

1.1	Les différents niveaux de SIL définis par la norme IEC 61508 . . . . .	13
1.2	Représentation des portes logiques . . . . .	22
2.1	Expression des principales caractéristiques d'un intervalle . . . . .	35
2.2	Produit de $X$ et $Y$ (cas $X$ est indépendante de $Y$ ) . . . . .	46
2.3	Paramètres des probabilités floues des événements de base . . . . .	50
2.4	Base des règles . . . . .	57
3.1	Paramètres caractéristiques du HIPS . . . . .	76
3.2	Paramètres caractéristiques du HIPS sous forme de p-boxes . . . . .	89
4.1	Paramètres caractéristiques sous forme d'intervalles . . . . .	103
4.2	Paramètres caractéristiques des composants du HIPS . . . . .	116

# Production personnelle

## Publications

- ***Approche par intervalles pour l'évaluation imprécise des Systèmes Instrumentés de Sécurité.***  
Mechri W., Simon Ch., Ben Othman K.  
*e-STA, Revue des Sciences et Technologie de l'Automatique, vol. 8, n° 1, pp 44-52, 2011.*
- ***Uncertainty analysis of common cause failure in Safety Instrumented Systems.***  
Mechri W., Simon Ch., Ben Othman K.  
Accepté, *au Proceeding of the institution of Mechanical Engineers, Part O-Journal of Risk and Reliability*, À paraître en 2011.
- ***Probabilistic fuzzy approach for the imprecise evaluation of Safety Instrumented Systems.***  
Mechri W. and Ben Othman K.  
*International Review of Modeling and Simulation, IReMos, vol. 3, n° 3, pp. 388-400, 2010.*

## Communications

- ***Chaînes de Markov multiphases à intervalles pour l'évaluation de performance imprécise des SIS.***  
Mechri W., Simon Ch., Ben Othman K., Aubry J-F., Benrejeb M.  
*8 ème Congrès international pluridisciplinaire en Qualité et Sûreté de Fonctionnement, Qualita 2009, Besançon, France, Mars 2009.*
- ***Evaluation imprécise de l'indisponibilité des systèmes par chaînes de Markov floues.***  
Mechri W., Simon Ch., Ben Othman K., Aubry J-F., Benrejeb M.  
*Performances et Nouvelles Technologies en Maintenance, PENTOM 2009, Autrans*

---

Grenoble, France, Décembre 2009.

- ***Analyse de l'imprécision de taux de défaillance de cause commune pour l'évaluation des performances des SIS***  
Mechri W., Simon Ch., Ben Othman K., Aubry J-F., Benrejeb M.  
*8 ème Conférence Internationale de Modélisation et Simulation Modélisation, Hammamet, Mai 2010.*
- ***Chaînes de Markov floues multi-phases pour l'évaluation de la performance imprécise des Systèmes Instrumentés de Sécurité.***  
Mechri W., Simon Ch., Ben Othman K., Aubry J-F., Benrejeb M.  
*Sixième Conférence Internationale Francophone d'Automatique Nancy, CIFA 2010, Nancy, France, 2-4 juin 2010.*
- ***Evaluation des performances imprécises des SIS par des familles de densités de probabilités.***  
Mechri W., Simon Ch., Ben Othman K., Benrejeb M.  
*9 ème Congrès international pluridisciplinaire en Qualité et Sûreté de Fonctionnement, Qualita 2011, Angers, France, Mars 2011.*
- ***Uncertainty evaluation of Safety Instrumented Systems by using Markov chains.***  
Mechri W., Simon Ch., Ben Othman K., Benrejeb M.  
*Accepté in 18<sup>th</sup> IFAC World Congress, Milan, Italy - August 28 - September 02, 2011.*

# Liste des acronymes

**AMDE** : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité

**API** : American Petroleum Institute

**APD** : Analyse Préliminaire de Dangers

**CCF** : Common Cause Failure

**CM** : Coupe minimale

**DCC** : Défaillance de Cause Commune

**DDB** : Diagramme de Décision Binaire

**DC** : Diagnostic Coverage

**E/E/PE** : Electriques/Electroniques/Electroniques programmables de sécurité

**EI** : Evènement Indésirable

**IEC** : International Electrotechnical Commission

**LS** : Logic Solver

**HIPS** : High Integrated Protection System

**MGL** : Multiple Greek Letters

**MTTR** : (Mean Time To Repair ), Durée moyenne de réparation

**PDS** : Reliability and availability of computer based systems

**PF<sub>D</sub>** : Probability of Failure on Demand

$PF_{D_{avg}}$  : Average probability of Failure on Demand

**PFH** : Probability of dangerous Failure per Hour

**SIL** : Safety Integrity Level

**SIS** : Safety Instrumented System

**SIF** : Safety Instrumented Function

# Introduction générale

Les industries s'occupent non seulement des performances des systèmes en termes de qualité et de rentabilité mais aussi en termes de sécurité. Les moyens à mettre en oeuvre pour réduire les risques sont nombreux et variés. La conception du procédé, le choix des équipements participent à la réduction du risque. On peut aussi agir sur le système de contrôle commande du procédé, en prévoyant par exemple des redondances et des solutions de repli en cas des conditions anormales de fonctionnement. Ces approches ne sont pas toujours suffisantes.

Des systèmes spécifiques appelés Systèmes Instrumentés de Sécurité (SIS) sont utilisés ayant pour objectif de réduire les risques d'occurrence d'événements dangereux tout en garantissant la protection ; des personnes, des équipements matériels et de l'environnement.

Les SIS sont utilisés pour exécuter des fonctions de sécurité, ils sont aussi appelés boucles de sécurité. Ils comprennent les matériels et logiciels nécessaires pour obtenir la fonction de sécurité désirée. Ces systèmes peuvent atteindre un niveau d'intégrité de sécurité important en conformité avec les normes en vigueur telles que ; la norme IEC 61508 [54] et la norme IEC 61511 [55], qui traitent de la sécurité fonctionnelle des systèmes. Les SIS ont pour objectif de mettre le procédé qu'ils surveillent en position de repli de sécurité lorsqu'il évolue vers une voie comportant un risque réel (explosion, feu, . . .), c'est-à-dire dans un état stable ne présentant pas de risque pour les opérateurs humains et équipements.

Les normes IEC 61508 [54] et IEC 61511 [55], spécifient pour une fonction de sécurité, quatre niveaux possibles de performance de la sécurité. Ils sont appelés niveaux d'intégrité de la sécurité (SIL). Ces deux normes de sécurité fonctionnelle introduisent une approche probabiliste pour l'évaluation quantitative de la performance du système instrumenté de sécurité et la qualification de cette performance par des niveaux de sécurité référencés. L'utilisation des probabilités pour la mesure du niveau d'intégrité a entraîné la mise en place de concepts tels que la probabilité de défaillance à la sollicitation ou la probabilité de défaillance par unité de temps.

La performance des SIS doit être prouvée par l'utilisation de modèles adaptés. Toutefois l'IEC 61508 [54] ne définit pas ces modèles. Différentes techniques sont néanmoins préconisées dans les annexes de la norme sans toutefois exclure toute méthode pertinente de calcul probabiliste. Parmi les méthodes citées, on trouve les blocs diagrammes de fia-

---

bilité, les arbres de défaillances, les réseaux de Petri ainsi que les chaînes de Markov. La performance ainsi calculée permet de qualifier le niveau d'intégrité de sécurité (SIL) du SIS selon les niveaux définis dans la norme. Cette évaluation consiste à calculer l'indisponibilité moyenne de la fonction de sécurité ou encore la probabilité moyenne de défaillance à la demande ( $PFD_{avg}$  : Average Probability of Failure on Demand) pour les SIS faiblement sollicités.

Les méthodes usuelles de calcul de l'indisponibilité des systèmes tels que, les arbres de défaillances, les chaînes de Markov ou encore les réseaux de Petri... sont des méthodes probabilistes. Ces méthodes issues des études traditionnelles de la sûreté de fonctionnement où les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation...) peuvent être connues avec précision et validées par le retour d'expérience. Dans certains cas, le retour d'expérience est malheureusement insuffisant pour valider avec précision les paramètres de défaillance. En plus l'évolution constante de l'environnement et de la complexité des installations industrielles, les conditions d'utilisation des composants des SIS utilisés dans les installations peuvent changer pour un même composant et réduit notre connaissance de leurs processus de dégradation. L'idéal est de disposer d'une quantité d'information suffisante concernant les défaillances des composants pour pouvoir estimer avec précision leur paramètres de défaillance.

Les SIS sont des dispositifs sur lesquels nous n'avons pas forcément de retour de données en quantité. Ceci est d'autant plus vrai lorsque ces dispositifs sont faiblement sollicités, et pour lesquels le retour d'expérience est naturellement faible. De fait, le constat est que si dans les études d'indisponibilité des systèmes, les probabilités manipulées sont souvent considérées précises et parfaitement déterminables, dans les systèmes instrumentés de sécurité, leur précision est soumise à questionnement. Ce problème de précision dans la connaissance des valeurs de probabilités est connu et appréhendé de diverses manières. La modélisation des probabilités par un intervalle est une forme simple et séduisante de l'imprécision. Mais, cela peut être généralisé par d'autres représentations et associé à des diverses théories de manipulation de l'incertain comme, la théorie des sous-ensembles flous, la théorie de possibilités, la théorie de l'évidence ou la théorie des probabilités imprécises qui peuvent être utilisées pour prendre en compte l'imprécision (qu'on appelle aussi incertitude de type épistémique) liée aux paramètres de défaillance et estimer les probabilités de défaillance des composants ainsi que les  $PFD_{avg}$  des SIS.

Le premier chapitre concerne la présentation de la problématique de la sécurité dans les installations industrielles, ainsi que les principales normes de sécurité fonctionnelles utilisées pour la conception des systèmes de sécurité. Nous insistons en particulier sur les difficultés auxquelles les industriels sont confrontés lors du déploiement des normes de sécurité fonctionnelle. On s'intéresse aussi aux systèmes instrumentés de sécurité et aux différentes notions utiles pour calculer la probabilité moyenne de défaillance dangereuse, notamment l'explication des différents paramètres intervenants dans ce calcul.

Le deuxième chapitre permet, au travers de la définition des principales théories utilisées pour la représentation des connaissances imparfaites (théorie des probabilités, théorie

---

d'intervalle, théorie des ensembles flous, théorie des P-boxes . . . ), d'introduire et d'expliquer leur utilisation (en particulier la théorie des ensembles flous) dans les méthodes d'évaluation de la sûreté de fonctionnement des systèmes complexes. Une étude basée sur la méthode des arbres de défaillances flous est présentée pour évaluer la performance des systèmes, et qui permet, en outre, de prendre en compte les incertitudes des paramètres de défaillance et de caractériser l'incertitude des résultats obtenus. Les bases théoriques concernant l'étude des chaînes de Markov à probabilités de transitions floues sont présentées [137]; [16]; [70]; [13].

Dans Le troisième chapitre le problème d'imprécision dans l'évaluation des performances des SIS à l'aide des arbres de défaillance est traité. Deux approches probabilistes sont proposées. La première approche d'évaluation se base sur l'utilisation des nombres flous pour représenter l'incertitude épistémique. La seconde approche s'intéresse à étendre les calculs à une représentation plus générale de l'imprécision et à intégrer la modélisation des paramètres par des familles de probabilités (p-boxes) dans les arbres de défaillance. Une application support [30] illustre l'utilisation de l'approche proposée. Les résultats obtenus sont comparés à ceux obtenus par simulation de Monte Carlo. L'influence de l'indépendance des sources d'information sur l'imprécision du résultat est également montrée. La dernière partie de ce chapitre s'intéresse à la modélisation de l'imprécision de la connaissance des paramètres imprécis des SIS, à l'aide des familles de probabilités imprécises (P-boxes). L'imprécision du facteur de défaillance de cause communes (DCC) est modélisée et propagée dans un arbre de défaillances.

Le quatrième chapitre concerne l'évaluation imprécise des performances des SIS faiblement sollicités et périodiquement testés à l'aide des chaînes de Markov multiphases. La première partie de ce chapitre s'intéresse à la présentation d'une approche basée sur l'utilisation de la théorie d'intervalles au sein des chaînes de Markov multi-phases, à partir des valeurs imprécises de taux de couverture de diagnostic et du facteur de DDC. Cette approche est utilisée pour évaluer la performance imprécise des SIS et pour montrer l'impact de cette imprécision sur la qualification de performance d'un SIS.

La dernière partie porte sur une approche floue basée sur l'intégration du formalisme flou dans les chaînes de Markov multiphases [30] pour la détermination de la  $PF D_{avg}$  des SIS et l'évaluation des SIL. Les probabilités de transition des chaînes de Markov sont remplacées par des nombres flous [17] permettant aux experts fiabilistes d'exprimer leurs incertitudes dans l'énoncé des valeurs des probabilités des défaillances et autres paramètres caractéristiques des systèmes. L'approche floue proposée est appliquée à un exemple [110] qui met en évidence la conformité des résultats avec une approche purement aléatoire de la modélisation de l'imprécision.

# 1

## Normes et méthodes pour l'évaluation des performances des systèmes instrumentés de sécurité

### Sommaire

---

<b>1.1</b>	<b>Introduction</b>	<b>3</b>
<b>1.2</b>	<b>Principaux concepts de sécurité</b>	<b>3</b>
1.2.1	Notion de sécurité	4
1.2.2	Notion de danger	4
1.2.3	Notion de risque	4
1.2.4	Sécurité fonctionnelle	5
1.2.5	Systèmes E/E/EP relatifs aux applications de sécurité	6
<b>1.3</b>	<b>Normes relatives aux Systèmes Instrumentés de Sécurité</b>	<b>6</b>
1.3.1	Norme IEC 61508 et ses normes filles	6
1.3.1.1	La norme IEC 61511	8
1.3.1.2	La norme IEC 62061	9
1.3.1.3	La norme IEC 61513	9
1.3.1.4	La norme EN 50126	9
1.3.2	Le Concept de Système Instrumenté de Sécurité	9
1.3.2.1	Constitution d'un SIS	10
1.3.2.2	Systèmes de protection à intégrité élevée (HIPS)	11
1.3.2.3	Fonction Instrumentée de Sécurité	11
1.3.3	Paramètres de performance de sécurité des SIS	12
1.3.3.1	Probabilité moyenne de défaillance à la demande	12
1.3.3.2	Probabilité de défaillance dangereuse par heure (PFH)	12

---

1.3.4	Notion de niveau d'intégrité de sécurité (SIL) . . . . .	12
1.3.5	Classification des défaillances dans la norme IEC 61508 . . . . .	14
1.3.6	Tests et stratégies des tests des SIS . . . . .	15
1.3.7	Les facteurs caractéristiques des SIS . . . . .	16
1.3.7.1	Taux de couverture de diagnostic . . . . .	16
1.3.7.2	Défaillances de causes communes . . . . .	17
1.3.8	Limites de la norme IEC 61508 . . . . .	17
<b>1.4</b>	<b>Détermination des niveaux de sécurité des SIS . . . . .</b>	<b>18</b>
1.4.1	Les méthodes qualitatives . . . . .	18
1.4.1.1	Graphe de risque . . . . .	18
1.4.1.2	Matrice de risque . . . . .	19
1.4.2	Les méthodes quantitatives . . . . .	19
1.4.2.1	Les équations simplifiées . . . . .	19
1.4.2.2	Blocs diagramme de fiabilité . . . . .	20
1.4.2.3	Arbres de défaillance . . . . .	20
1.4.2.4	Chaînes de Markov . . . . .	24
1.4.2.5	Chaînes de Markov multiphase . . . . .	28
<b>1.5</b>	<b>Conclusion . . . . .</b>	<b>29</b>

---

## 1.1 Introduction

Généralement les systèmes industriels peuvent présenter des risques pour les personnes et l'environnement, diverses sécurités doivent être mises en oeuvre. Ces types de sécurité utilisent des moyens contribuant soit à la prévention soit à la protection pour minimiser les conséquences d'un dysfonctionnement. Les Systèmes Instrumentés de Sécurité (SIS) sont utilisés comme moyens de protection pour réaliser des Fonctions Instrumentées de Sécurité (SIF) afin de mettre le procédé surveillé dans une position de repli de sécurité. La Commission Internationale d'Electronique (CEI), ou "International Electrotechnical Commission" (IEC), a normalisé les systèmes de sécurité; Norme IEC 61508 en 1998 [54] et IEC 61511 en 2000 [55].

Certains termes et concepts de base utilisés dans ce chapitre sont ambigus tels que danger, risque, sécurité, sécurité fonctionnelle,... Afin de clarifier la signification de ces termes, il est important de présenter les définitions précises pour chacun de ces concepts. Par la suite, nous citons les principales normes de sécurité utilisées pour concevoir les systèmes de protection. La définition des SIS et les paramètres caractéristiques (taux de défaillance, défaillance de cause commune,...) qui interviennent dans l'évaluation de ses performances en fonction des événements rencontrés (défaillance, test) sont détaillés. La dernière partie s'intéresse aux différentes méthodes, citées par les normes de sécurité, utilisées pour déterminer les niveaux SIL des SIS.

## 1.2 Principaux concepts de sécurité

Les industries déploient beaucoup d'efforts pour éviter les accidents. Malgré ces efforts, de nombreux accidents se produisent dans le monde et causent des dégâts sur les plans; humains et matériels. La fréquence de ces accidents conduit à des études de sécurité afin de mieux maîtriser les risques.

Dans les études de sécurité, l'utilisation d'une des méthodes conventionnelles est recommandée afin d'identifier les sources ou les situations dangereuses. Une analyse préliminaire des dangers (APD) permet de déterminer les risques qu'un système peut entraîner. Elle conduit à une série de mesures d'analyse de risques mises en oeuvre peut mener l'installation à un niveau de sécurité jugé acceptable par l'exploitant [88].

### 1.2.1 Notion de sécurité

La sécurité est généralement définie par l'absence de phénomènes dangereux, de risque inacceptable, d'accident ou de situations catastrophiques [34].

Selon Villemeur [129], " *la sécurité est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques* ".

D'après Desroches [24], *la sécurité concerne la non occurrence d'événements pouvant diminuer ou porter atteinte à l'intégrité du système, pendant toute la durée de l'activité du système, que celle-ci soit réussie, dégradée ou ait échoué.*

Dans le cadre des systèmes industriels, la sécurité consiste à mettre en oeuvre des moyens évitant l'apparition de dangers. Elle s'énonce alors par l'absence de risque inacceptable, selon la norme IEC 61508 [54].

### 1.2.2 Notion de danger

La norme IEC 61508 [54] définit le danger comme *une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes.*

Selon la norme OHSAS 18001 [94] : " *un danger est une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments* ". Les dangers liés à un système sont inhérents au fonctionnement ou au dysfonctionnement du système, soit extérieur au système.

Selon Mazouni [79], *le danger se définit comme une propriété intrinsèque inhérente à un type d'entité ou un type d'événement qui a la potentialité de provoquer un dommage.*

### 1.2.3 Notion de risque

Selon Villemeur [130], " 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."

Le risque peut être considéré comme une certaine quantification du danger associant une mesure de l'occurrence d'un événement redouté à une estimation de la gravité de ses conséquences [58]. Le risque donne une mesure de la combinaison de deux facteurs qui sont la gravité d'un danger (ou sa conséquence) et la fréquence d'occurrence. Sa réduction peut être obtenue par la prévention (réduction de la fréquence d'occurrence) ou la protection (réduction de la gravité).

Le risque est caractérisé d'une part par l'ampleur des dommages, suite à l'occurrence d'un événement redouté, selon un critère de gravité, et d'autre part par son caractère

incertain lié à l'apparition de l'événement redouté provoquant le dommage à partir d'une situation critique ou dangereuse [88].

Le risque peut être modélisé d'une façon générale et élémentaire par la mesure de sa criticité  $C$ , qui est fonction de sa gravité  $G$  et de sa probabilité d'occurrence  $P$  :

$$C = P \times G \quad (1.1)$$

En général, le risque se rapporte au couple (gravité, probabilité). Le plus souvent cela quantifie le produit de la gravité d'un accident par sa probabilité d'occurrence. Farmer [35] a classifié les risques en deux catégories ; risque acceptable et risque inacceptable en se basant sur la fonction  $G = f(P)$ , comme le montre la courbe représentée à la figure 1.1.

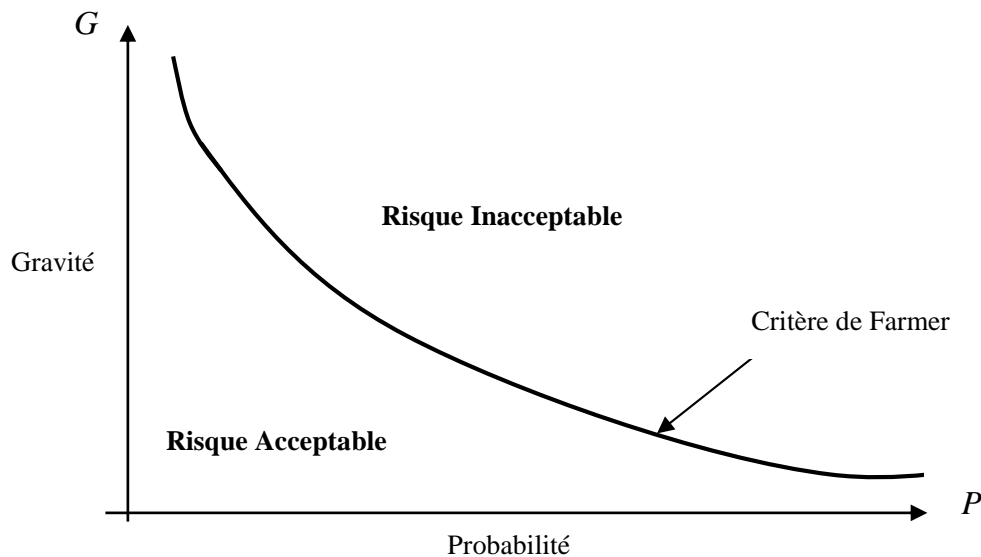


FIGURE 1.1 – Courbe de Farmer [35]

La courbe de Farmer permet une classification du risque en deux sous-ensembles disjoints, correspondants au domaine du risque acceptable et à celui du risque inacceptable.

#### 1.2.4 Sécurité fonctionnelle

La sécurité fonctionnelle a pour objet de contrôler les risques inacceptables qui pourraient provoquer des accidents dangereux. Elle couvre les systèmes mettant en oeuvre des solutions de protection appliquées dans plusieurs domaines : mécanique, électrique, électronique, électronique programmable, hydraulique, optique, ...

- La sécurité fonctionnelle, selon la norme IEC 61508 [54], est un sous ensemble de la sécurité globale qui se rapporte au système commandé et qui dépend du bon fonctionnement des systèmes relatifs à la sécurité basée sur une autre technologie et des dispositifs externes de réduction de risque.
- Selon la norme IEC 61511 [55], la sécurité fonctionnelle est un sous-ensemble de la sécurité globale qui se rapporte à un système de commande de processus de base (BPCS, Base Process Control System) et qui dépend du fonctionnement correct du système instrumenté de sécurité et d'autres couches de protection [88].

### 1.2.5 Systèmes E/E/EP relatifs aux applications de sécurité

Les systèmes de sécurité sont définis en termes d'absence de risque inacceptable de blessure ou de préjudice à la santé des personnes et à la dégradation de l'environnement. Les dommages aux personnes peuvent être directs ou indirects, comme des dommages aux biens ou à l'environnement par exemple [58]. Certains systèmes peuvent être principalement conçus pour se prémunir contre des pannes ayant des implications économiques majeures. Ceci signifie que dans l'esprit, à objectifs techniques comparables ou identiques, il n'y a pas une grande différence entre un système de sécurité et un système de contrôle.

Un système E/E/EP (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité, c'est-à-dire, depuis le capteur, en passant par l'unité logique de traitement, jusqu'à l'élément final (la partie actionneur), tout en tenant compte des actions de l'opérateur du système.

La norme IEC 61508 [54] peut être utilisée pour développer n'importe quel système E/E/EP comportant des fonctions critiques, telles que la protection des équipements, des biens ou de l'environnement.

## 1.3 Normes relatives aux Systèmes Instrumentés de Sécurité

La norme internationale de sécurité IEC 61508 est une des dernières normes dédiées à la sécurité fonctionnelle. Elle est devenue avec ses normes filles les plus récentes et les plus connues des acteurs de la sécurité dans les secteurs industriels.

### 1.3.1 Norme IEC 61508 et ses normes filles

La norme IEC 61508 [54] est un ensemble de règles et de recommandations permettant l'amélioration de la sécurité par l'utilisation des systèmes électriques, électroniques programmables E/E/EP. Cette norme orientée performances, propose une démarche opérationnelle permettant de mettre en place un système E/E/EP à partir de l'étude des

exigences de sécurité issues notamment d'une analyse des risques. L'avantage de cette norme est qu'elle propose des moyens de justification sur l'ensemble du cycle de vie d'un produit en fonction du niveau de sécurité que l'on souhaite atteindre.

La norme IEC 61508 [54] se compose de sept volets comme suit :

- 61508-1 présente les définitions des prescriptions générales.
- 61508-2 traite les prescriptions spécifiques aspect matériel des systèmes E/E/EP.
- 61508-3 dédiée à la présentation des prescriptions spécifiques, aspect logiciel, des Systèmes E/E/EP. Elle est développée dans la troisième partie de la norme.
- 61508-4 présente les définitions et les abréviations utilisées.
- 61508-5 donne des exemples de méthode pour la détermination des niveaux d'intégrité de sécurité.
- 61508-6 fournit les guides d'application des parties 2 et 3 de la norme.
- 61508-7 présente les techniques et les mesures recommandées lors de la validation des systèmes E/E/EP.

La complexité de la norme IEC 61508 [54] a conduit ses concepteurs à développer des normes relatives à des secteurs bien précis (ex : machines, processus industriels, ferroviaire, centrales nucléaires ...). La figure 1.2 montre la norme IEC 61508 générique ainsi que ses normes filles selon le secteur d'activité concerné. Elle influence le développement des systèmes E/E/EP et les produits concernés par la sécurité dans tous les secteurs [101].

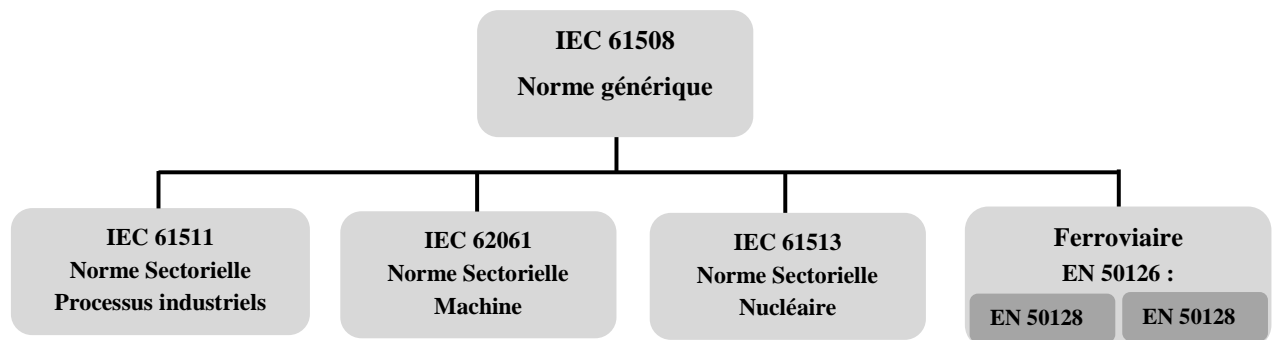


FIGURE 1.2 – Les normes sectorielles de l'IEC 61508 [98]

### 1.3.1.1 La norme IEC 61511

L'IEC 61511, s'intéresse à la sécurité fonctionnelle des SIS pour le secteur de l'industrie des procédés continus. Les remarques faites ci-dessus pour l'IEC 61508 [54] s'appliquent également à l'IEC 61511 [55]. Cette norme est composée de trois grandes parties :

- 61511-1 présente les définitions et les exigences des systèmes (matériel et logiciel).
- 61511-2 traite les lignes directrices pour l'application de la première partie de la norme.
- 61511-3 fournit des conseils pour la détermination des niveaux d'intégrité de sécurité.

L'IEC 61511 [55] détaille les définitions et les prescriptions relatives au cycle de vie en sécurité contenant la spécification, la conception, l'exploitation et la maintenance d'un système instrumenté de sécurité, afin de maintenir le procédé dans une position de sécurité convenable.

La norme IEC 61511 est l'une des déclinaisons de la norme IEC 61508. Les SIS constituent l'objet principal de ces deux normes, mais ils y sont considérés différemment selon les métiers auxquels elles s'adressent (cf.figure 1.3) [58].

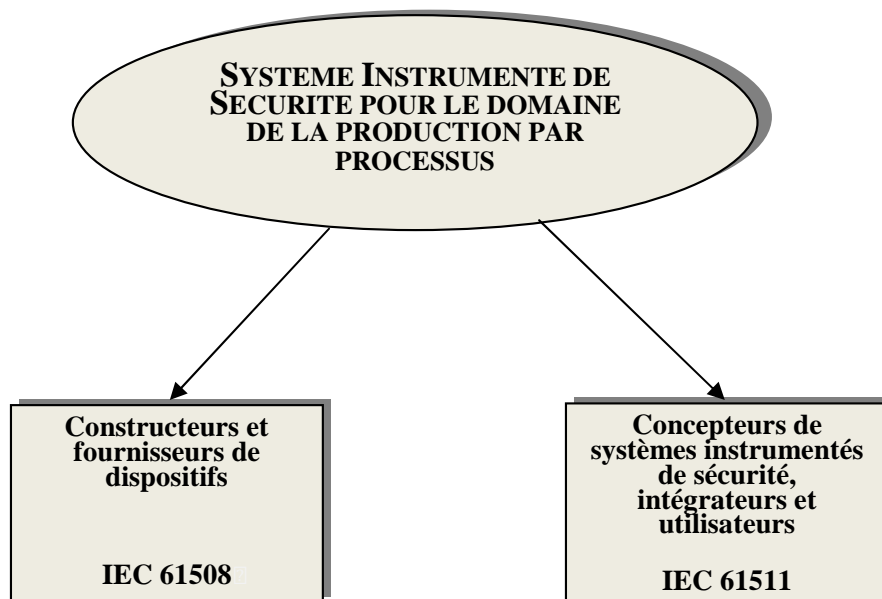


FIGURE 1.3 – Utilisateurs de l'IEC 61508 et l'IEC 61511 [79]

L'IEC 61508 [54] est une norme complexe, difficile à mettre en oeuvre, elle est destinée surtout aux fabricants et fournisseurs de systèmes E/E/EP [101], alors que la norme

IEC 61511 est plus facile à utiliser, elle présente une simplification de l'IEC 61508, en se limitant aux éléments nécessaires pour l'industrie de process [101].

#### 1.3.1.2 La norme IEC 62061

L'IEC 62061 [57] repose sur les mêmes concepts que ceux de l'IEC 61508 [54]. Elle est destinée à être utilisée par les concepteurs de machines et les fabricants de systèmes de commande électroniques relatifs à la sécurité de machines [57]. Elle concerne la spécification des prescriptions et fait des recommandations pour la conception, l'intégration et la validation de ces systèmes [101].

#### 1.3.1.3 La norme IEC 61513

L'IEC 61513 [56] concerne le secteur de la sûreté des centrales nucléaires. Elle présente les prescriptions relatives aux systèmes de contrôle commande utilisés pour accomplir les fonctions de sécurité des centrales nucléaires. La conception des systèmes de contrôle commande peuvent être réalisés à l'aide d'une combinaison de composants traditionnels câblés à des composants informatiques. La conformité à l'IEC 61513 facilite la compatibilité avec les exigences de l'IEC 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire.

#### 1.3.1.4 La norme EN 50126

La norme EN 50126 [31] s'intéresse essentiellement aux applications ferroviaires. Elle permet de spécifier les principaux concepts de la sûreté de fonctionnement des systèmes tels que : la fiabilité, la disponibilité et la sécurité, . . . Cette norme est constituée de deux normes filles. L'EN 50128 [32] est destinée à la partie logicielle des systèmes de protection ferroviaire. L'EN 50129 [33] concerne les systèmes électroniques de sécurité pour la signalisation [101].

### 1.3.2 Le Concept de Système Instrumenté de Sécurité

Les SIS sont une composante essentielle des dispositifs de prévention des installations industrielles. La définition des fonctions de sécurité, la conception, la maintenance, et la modification des systèmes doivent assurer la disponibilité et la fiabilité de la fonction de sécurité en toute circonstance. Les meilleures pratiques disponibles dans le management des SIS ont été décrites dans la norme IEC 61511 [55] pour les industries de procédé.

La norme IEC 61508 [54] définit quand à elle les systèmes relatifs aux applications de sécurité par : *un système E/E/EP (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.*

La norme IEC 61511 [55] définit les systèmes instrumentés de sécurité de la façon suivante : *système instrumenté utilisé pour mettre en oeuvre une ou plusieurs fonctions*

instrumentées de sécurité (SIF). Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux).

### 1.3.2.1 Constitution d'un SIS

Un SIS est un système visant à mettre le procédé en un état stable lorsque le procédé s'engage dans une voie comportant un risque réel (explosion, feu, ...), [58]. Un SIS se compose de trois couches comme le montre la figure 1.4 :

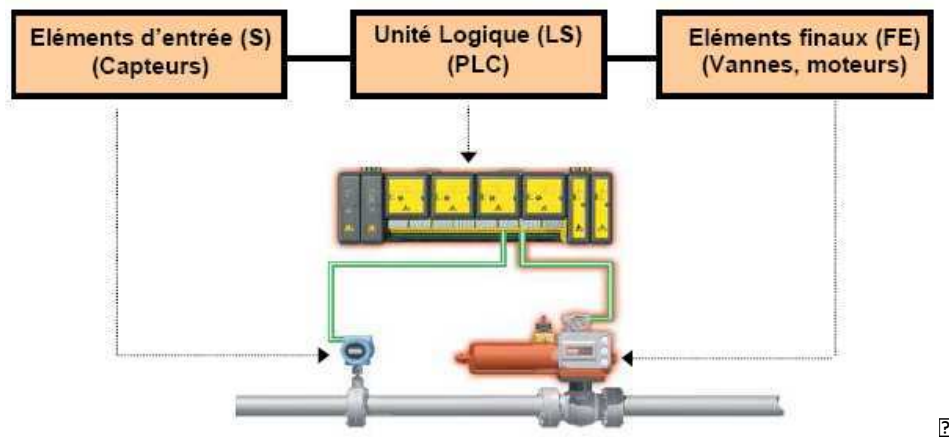


FIGURE 1.4 – Structure d'un SIS [55]

- Une couche capteur (Sensor) : elle est constituée d'un ensemble d'éléments d'entrée (ex : capteurs, détecteurs) qui surveillent l'évolution des paramètres physico-chimiques représentatifs du comportement du procédé (température, pression, niveau ...).
- Une couche unité logique LS (Logic Solver) : ce sous-ensemble d'éléments logiques réalise le processus de prise de décision qui s'achève par l'activation du troisième sous-système FE (Final Element) [58]. Le sous-système LS peut être un automate programmable ou un micro-ordinateur doté de logiciels spécifiques.
- Une couche actionneur FE : Elle agit directement (ex : vannes d'arrêt d'urgence) ou indirectement (ex : vannes solénoïdes) sur le procédé pour neutraliser sa dérive en mettant, en général, le système à l'arrêt (état sûr) au terme d'un délai qui doit être spécifié pour chaque fonction de sécurité [58].

Un des principaux objectifs de la norme IEC 61508 [54] est d'assurer la sécurité d'une installation lorsqu'elle s'engage dans une voie comportant un risque réel pour les personnes et l'environnement [101]. Autrement dit, une analyse de risque correcte du comportement du SIS permet d'étudier son aptitude à répondre à une demande sécuritaire [58], [71].

### 1.3.2.2 Systèmes de protection à intégrité élevée (HIPS)

Dans l'industrie pétrolière, les systèmes de protection traditionnels comme définis dans l'institut américain du pétrole (API : American Petroleum Institute), sont le plus souvent remplacés par des systèmes de protection d'intégrité élevée (High Integrity Protection Systems HIPS) [109]. Comme les SIS, les HIPS doivent être analysés par les méthodes formelles décrites dans les normes IEC 61508 et IEC 61511 afin d'évaluer leur niveau d'intégrité de sécurité SIL (Safety Integrity Level) [110], [111], [112].

Les HIPS sont des SIS à niveau d'intégrité élevé (niveau SIL 3 ou 4), mis en application pour s'adresser aux scénarios de surpression [109], [111]. Les HIPS fournissent un outil de réduction du risque alors que les SIS sont conçus pour empêcher ces scénarios. Les applications des HIPS sont généralement la protection contre la surpression dans les canalisations [111].

Comme tout SIS, un HIPS est constitué d'une partie capteur, une partie unité logique de traitement et une partie actionneur destinée à mettre un procédé industriel en position de repli de sécurité, lorsque le procédé présente un risque réel pour le personnel et l'environnement. La mise en oeuvre des HIPS doit être basée sur une analyse de risque suivant une approche structurée et systématique. Cette analyse permet d'identifier les causes et les conséquences des scénarios de risque, notamment les scénarios de surpressions.

L'ensemble capteurs, unité logique de traitement et actionneurs sont des équipements permettant de réaliser la fonction de sécurité à partir de la fonction de sécurité de chaque élément du SIS.

### 1.3.2.3 Fonction Instrumentée de Sécurité

Les principales étapes de la norme IEC 61508 [54] et ses normes filles sont déclinées dans ce qu'on appelle le cycle de vie, c'est-à-dire que ces normes traitent depuis l'analyse des risques jusqu'à l'exploitation des fonctions de sécurité instrumentées SIF (Safety Instrumented Functions).

Une SIF est définie pour obtenir un facteur de réduction du risque mise en oeuvre pour un SIS. Lorsque le SIS est considéré comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une fonction de sécurité [88], [20].

Un SIS contient généralement plus qu'une SIF. Si les exigences d'intégrité de la sécurité pour ces SIF diffèrent, alors les exigences applicables au niveau d'intégrité de la sécurité le plus élevé s'appliquent au SIS. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à la réduction de la fréquence d'occurrence du danger.

L'architecture fonctionnelle d'un SIS est un ensemble de SIF qui comprend trois fonctionnalités de base, la détection, le traitement (ou la décision) et l'actionnement.

### 1.3.3 Paramètres de performance de sécurité des SIS

La norme IEC 61508 [54] spécifie deux indicateurs de la sécurité relatifs aux systèmes électroniques programmables dédiés aux applications de sécurité. Ces deux paramètres utilisés pour l'évaluation des performances des SIS suivant les deux modes de défaillance cités par les normes de sécurité. Ces modes sont le mode de défaillances dangereuses et le mode de défaillances sûres. Ces indicateurs sont donnés sous forme de probabilités de défaillance dangereuse ( $PFDD$ ) et de défaillance en sécurité ( $PFHS$ ).

#### 1.3.3.1 Probabilité moyenne de défaillance à la demande

Il est utile de rappeler certains principes et hypothèses de base largement utilisés dans la norme IEC 61508 [54] et ses normes filles.

La probabilité moyenne de défaillance à la demande, notée  $PFDD_{avg}$  n'est pas définie dans le volume 4 de la norme IEC 61508, malgré son utilisation dans plusieurs définitions et abréviations. Cette probabilité représente tout simplement l'indisponibilité moyenne d'un système E/E/EP relatif à la sécurité, qui rend ce dernier incapable d'effectuer correctement sa fonction de sécurité, lorsqu'il est faiblement sollicité [76].

La dénomination  $PFDD$  utilisée dans la norme est d'autant moins adéquate. Elle désigne la probabilité de défaillance dangereuse à la sollicitation. La  $PFDD_{avg}$  (Average Probability of Failure on Demand) est la mesure d'une indisponibilité moyenne sur une période spécifiée.

Cette probabilité se distingue formellement d'une indisponibilité asymptotique (quand elle existe) ou stationnaire [58]. Cette distinction s'impose notamment pour les systèmes testés périodiquement et ne possédant pas de régime stationnaire. Elle est systématiquement ignorée, aussi bien dans la norme que par certains auteurs d'articles traitant du calcul des différentes architectures de base des SIS [58], [104], [111], [76].

#### 1.3.3.2 Probabilité de défaillance dangereuse par heure (PFH)

La probabilité d'une défaillance dangereuse par heure ( $PFH$ ) :Probability of a dangerous Failure per Hour, est parfois appelée " fréquence des défaillances dangereuses ", ou " taux de défaillances dangereuses ", ou nombre de défaillances dangereuses par heure ".

La probabilité de défaillance par heure n'est pas aussi citée dans la partie 4 de la norme IEC 61508-4 destinée aux définitions. Elle est indiquée dans le tableau 1.1 pour le mode de fonctionnement continu ou à demande élevée [54], [76].

### 1.3.4 Notion de niveau d'intégrité de sécurité (SIL)

Les normes de sécurité fonctionnelle IEC 61508 et IEC 61511 définissent une démarche d'analyse du niveau d'intégrité de sécurité (SIL) d'un système. Elles permettent de définir

le niveau SIL qui doit être atteint par un SIS qui réalise la fonction de sécurité suite à une analyse de risque, [102] [133], [106]. Plus le SIL a une valeur élevée plus la réduction du risque est importante.

Les SIS sont classés en quatre niveaux SIL qui se caractérisent par des indicateurs discrets positionnés sur une échelle de un à quatre niveaux (cf. Tableau 1.1). Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisées par des systèmes E/E/EP relatifs à la sécurité selon la norme IEC 61508 [54]. Le SIL "quatre" désigne le degré de sécurité le plus élevé du fait de l'exigence forte de sécurité imposée et le niveau SIL "un" désigne l'exigence la plus faible [106].

TABLE 1.1 – Les différents niveaux de SIL définis par la norme IEC 61508

Sollicitation	Demande faible	Demande élevée
Niveau d'intégrité		
<i>SIL</i>	<i>PFD<sub>avg</sub></i>	<i>PFH</i>
1	$PFD_{avg} \in [10^{-2}, 10^{-1}]$	$PFH \in [10^{-6}, 10^{-5}]$
2	$PFD_{avg} \in [10^{-3}, 10^{-2}]$	$PFH \in [10^{-7}, 10^{-6}]$
3	$PFD_{avg} \in [10^{-4}, 10^{-3}]$	$PFH \in [10^{-8}, 10^{-7}]$
4	$PFD_{avg} \in [10^{-5}, 10^{-4}]$	$PFH \in [10^{-9}, 10^{-8}]$

L'utilisation des niveaux SIL permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel, menant aux événements dangereux identifiés pendant l'analyse de risque [54], [106]. Les SILs sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances [54].

Un SIS est en mode de fonctionnement à faible demande lorsque la fréquence de sollicitation est inférieure à une fois par an ( $1/an$ ) ou inférieure au double de la fréquence des tests périodiques auxquels il est soumis. A partir de l'architecture du SIS réalisant la SIF faiblement sollicitée, la  $PFD_{avg}$  est évaluée sur un intervalle  $[0, t]$ .

Un SIS en mode de fonctionnement continu ou à forte demande implique une forte sollicitation du SIS. Il est considéré lorsque la fréquence de sollicitation est élevée ou continue, c'est-à-dire qu'elle est supérieure à une fois par an ( $1/an$ ) ou supérieure à deux fois la fréquence des tests périodiques [54]. A partir de l'architecture du système instrumenté de sécurité réalisant la fonction instrumentée de sécurité fortement sollicitée, la  $PFH$  est évaluée sur un intervalle de temps  $[0, t]$  [54].

La norme IEC 61508 relative à l'évaluation de performance des SIS établit la classification des systèmes étudiés selon des niveaux de sécurité à partir du calcul de la  $PFD_{avg}$ , pour les SIS faiblement sollicités (moins d'une sollicitation par an) ou de la  $PFH$  dans le cas des SIS fortement sollicités) [54], [88].

La norme IEC 61508 [54] détaille les prescriptions nécessaires pour répondre aux exigences de chaque niveau d'intégrité de sécurité. Ces prescriptions deviennent plus rigoureuses à mesure que le niveau de SIL s'élève en vue d'obtenir la probabilité d'une défaillance dangereuse de plus en plus faible.

### 1.3.5 Classification des défaillances dans la norme IEC 61508

Généralement un système peut se trouver dans l'un des quatre états suivants :

- état normal : la fonction de sécurité du système est valide et il n'existe pas de défaillance.
- état normal dégradé : La fonction de sécurité est valide, des composants du système pouvant être défaillants. Le système peut réagir dès l'apparition d'un évènement dangereux [71], [109].
- état de sécurité : Il s'agit d'un état du système pour lequel la sécurité est réalisée [71]. Le système peut converger vers cet état dès qu'une défaillance par exemple d'un ou plusieurs composants se produit. Dans ce cas la défaillance peut être : soit détectée, soit non détectée, mais elle n'a pas d'action néfaste vis-à-vis de la sécurité [54].
- état de défaillance dangereuse : C'est un état du système où la fonction de sécurité n'est plus réalisée, un ou plusieurs composants sont défaillants. Le système entre dans cet état dès qu'un risque d'accident apparaît et le système ne répond pas à une demande d'activation de la fonction de sécurité [54], [71].

La norme IEC 61508 [54] distingue les défaillances aléatoires du matériel des défaillances systématiques. Seules les premières sont prises en compte dans ce document. La norme distingue, à la page 40 de son volume 4, les défaillances dangereuses des défaillances sûres (cf. figure 1.5). Toutes les défaillances détectées en ligne par test de diagnostic sont qualifiées de défaillances détectées [76], [65]. Celles qui ne sont pas détectées sont qualifiées de défaillances non détectées [71], [61]. Les défaillances peuvent être comme suit :

- Les défaillances sûres et détectées font passer le système de l'état normal à l'état de sécurité, leur taux de défaillance est noté  $\lambda_{SD}$ .
- Les défaillances sûres et non détectées font passer le système de l'état normal à l'état dégradé, leur taux de défaillance est noté  $\lambda_{SU}$ .
- Les défaillances dangereuses détectées auraient la potentialité de faire passer le système de l'état normal à l'état de défaillance dangereuse mais leur détection associée à une stratégie sécuritaire (arrêt, alarme) permet au système de passer à l'état de sécurité, leur taux de défaillance est noté  $\lambda_{DD}$  [71], [61].
- Les défaillances dangereuses non détectées font passer le système de l'état normal à l'état de défaillance dangereuse, leur taux de défaillance est noté  $\lambda_{DU}$ , [61].

La somme des taux des défaillances sûres détectées et non détectées représente le taux de défaillances sûres, noté  $\lambda_S$  :

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \quad (1.2)$$

La somme des taux des défaillances dangereuses détectées et non détectées donne le taux de défaillances dangereuses, noté  $\lambda_D$  :

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \quad (1.3)$$

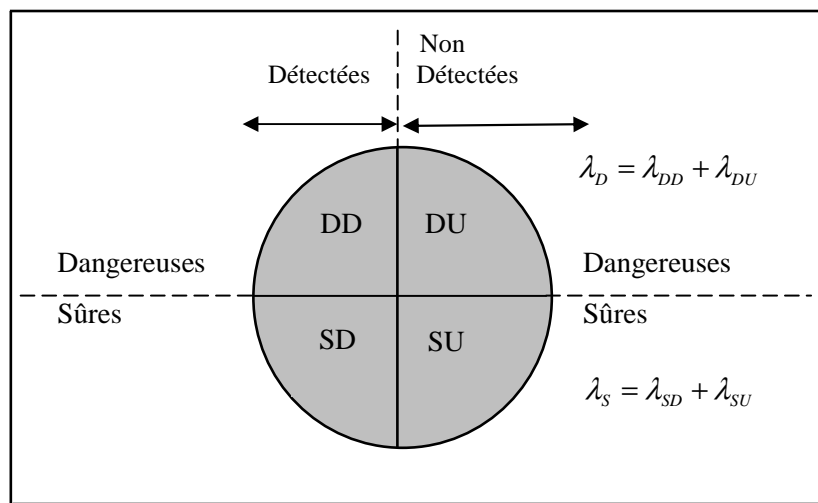


FIGURE 1.5 – Classification des défaillances [58]

**Remarque :**

L'IEC 61508 n'est dédiée qu'à la sécurité, elle traite essentiellement les défaillances dangereuses. Il en résulte que les formules analytiques citées dans la norme ne concernent que ce type de défaillances, alors qu'en général un SIS peut subir deux modes de défaillance : les défaillances dangereuses et les défaillances sûres [71], [20], [58].

### 1.3.6 Tests et stratégies des tests des SIS

Pour la vérification des SIS plusieurs tests ont été définis et peuvent être classés en fonction de leur mode de sollicitation (en ligne ou hors ligne) [20]

- Les tests de diagnostic en ligne (on-line diagnostic), sont des tests en ligne qui détectent essentiellement les défaillances aléatoires d'un composant, d'un module de système [71]. Ils sont le plus souvent exécutés dès la mise sous tension, puis

périodiquement [123]. Ils sont caractérisés par un taux de couverture  $DC$ , défini comme étant la probabilité qu'une défaillance soit détectée dès son apparition [128].

- Les tests périodiques ou tests d'inspection (proof tests), sont exécutés hors ligne et doivent être différenciés des tests de diagnostic [60], [71]. Ils sont destinés à détecter les défaillances d'un système non détectées en fonctionnement, de telle sorte que le système puisse être rétabli dans une condition 'aussi bon que neuf' ou aussi proche que possible de celle-ci [20], [71].

Le temps de mission noté  $T_i$ , est considéré comme égal au temps entre deux proof tests consécutifs [18], [20], [71].

Le proof test peut être mis en application en utilisant plusieurs stratégies de test différentes. Tores-Echeveria [123] énumère une classification des stratégies de test :

- Le test simultané où tous les composants sont testés en même temps. Ceci exige d'avoir un nombre de réparateurs suffisant pour tester tous les composants du système.
- Le test séquentiel, où tous les composants redondants sont testés consécutivement l'un après l'autre. Juste après qu'un composant est testé et mis en service, le prochain composant est testé et ainsi de suite jusqu'à finir avec tous les composants du sous-système [19].
- Le test indépendant, dans cette stratégie, la durée de test, des composants testés, ne suit pas un programme spécifique, l'intervalle de temps de test entre deux composants est aléatoire [123].

Généralement, on considère un seul intervalle de test pour vérifier la fonction de sécurité de l'ensemble du système mais certaines applications exigent l'utilisation d'intervalles de test différents propres à chaque sous système du SIS voire à chaque composant [110], [71].

### 1.3.7 Les facteurs caractéristiques des SIS

La norme IEC 61508 [54] permet d'estimer la probabilité de défaillance de la fonction de sécurité due à des défaillances matérielles aléatoires. Les calculs font intervenir un grand nombre de paramètres : architecture, taux de défaillance des composants, intervalle des tests, taux de couverture de diagnostic  $DC$  et le facteur  $\beta$  qui caractérise les défaillances de cause commune) [43], [51], [71].

#### 1.3.7.1 Taux de couverture de diagnostic

La norme IEC 61508 [54] définit le taux de couverture comme étant le rapport du taux de défaillance des pannes dangereuses détectées  $\lambda_{DD}$  (par un test de diagnostic) et du taux de défaillance totale des pannes dangereuses  $\lambda_D$  (détectées et non détectées), [71], [58], [20].

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dangereuses}} \quad (1.4)$$

L'évaluation du taux de couverture  $DC$  se fait par une Analyse des Modes de Défaillances et de leurs Effets (AMDE) au niveau des différents composants d'un système [42]; [124]. On cherche ainsi à déterminer les défaillances possibles et à savoir si elles peuvent être détectées [65].

Le taux de couverture  $DC$  intervient dans la détermination des taux de défaillances dangereuses; détectées et non détectées.

### 1.3.7.2 Défaillances de causes communes

La norme IEC 61508 introduit également des défaillances de causes communes (DCC) pour les architectures redondantes qui peuvent apparaître dans les canaux suite à une même cause. L'étude des modes communs ont été réalisés par différents auteurs [41]; [91]; [47].

Dans le cas de structure redondante (multiple canaux), les modes communs représentent les défaillances qui peuvent apparaître dans les canaux suite à une même cause. L'introduction des défaillances de mode commun est généralement modélisée par le modèle du facteur  $\beta$ .

Les défaillances de mode commun peuvent être introduites dans les calculs de la  $PFD_{avg}$  des SIS de façon directe. On évalue les paramètres de calcul à partir de données issues du retour d'expérience.

### 1.3.8 Limites de la norme IEC 61508

Les limites de la norme IEC 61508 sont liées à la complexité et à la difficulté de son utilisation. Plusieurs utilisateurs de l'IEC 61508 ont mentionné la nécessité d'être guidés, tant que ses notions paraient complexes, et difficiles à mettre en oeuvre.

Beaucoup de prescriptions ne sont pas assignées à une certaine gamme des niveaux d'intégrité de sécurité ou à la complexité de la conception. Ceci rend la norme difficile à utiliser pour de petits projets et rend la gestion de la sécurité fonctionnelle trop chère pour des petites et moyennes entreprises.

La norme IEC 61508 [54] définit l'intégrité de sécurité comme propriété de l'installation complète de sécurité, du capteur à l'actionneur. En outre, les parties 2 et 3 de cette norme entrent dans le détail dans; la conception et validation des systèmes E/E/EP de sécurité. Pour réaliser la fonction de sécurité, l'utilisateur met en oeuvre plusieurs sous-systèmes: capteur, unité de traitement, actionneur. Dans chacun des sous-systèmes, des composants peuvent être mis en redondance. La  $PFD_{avg}$  de l'ensemble doit être calculée à partir des caractéristiques des composants et des architectures du système de sécurité [101].

Rappelons également que les données des entrées spécifiées dans la norme sont bien souvent difficiles à obtenir et sont souvent des approximations (taux de couverture de diagnostic, modes communs de défaillances, ...). La  $PF D_{avg}$  devrait être aussi renommée, car sa dénomination prête à confusion. Il ne s'agit nullement d'une défaillance à la sollicitation classique, mais d'une indisponibilité moyenne sur un intervalle de temps spécifié [58], [112].

## 1.4 Détermination des niveaux de sécurité des SIS

Un élément majeur développé dans les normes en question est l'évaluation quantitative de la performance du système de sécurité mis en oeuvre et la qualification de cette performance par des niveaux référencés (cf. Tableau 1.1) [101], [102], [58], [109], [111], [113].

L'évaluation du niveau d'intégrité de sécurité d'un SIS est déterminée par des méthodes qualitatives et quantitatives [103], [104]. Elles permettent ; d'examiner les différents dangers provenant du système opérationnel et de déterminer le SIL de la SIF pour réduire la criticité du danger analysé. L'objectif global de ces méthodes est de décrire une procédure d'identification des SIF, d'établir les niveaux de sécurité correspondant et de les mettre en oeuvre dans un SIS afin de ramener le procédé dans l'état de sécurité attendue [102].

### 1.4.1 Les méthodes qualitatives

La norme IEC 61508 introduit des méthodes qualitatives qui permettent d'allouer le SIL à partir de la connaissance des risques associés au procédé. Les méthodes les plus utilisées sont la méthode du graphe de risque [12] [101], [113] et la méthode de la matrice de gravité des événements dangereux [102].

#### 1.4.1.1 Graphe de risque

Il s'agit de la méthode qualitative la plus répandue, elle permet de déterminer le niveau d'intégrité de sécurité d'une SIF à partir de l'analyse des risques associés au procédé [11], [102], [88].

La méthode du graphe de risque s'appuie sur l'équation 1.5 :

$$R = f \times C \tag{1.5}$$

$R$  est le risque en l'absence de systèmes relatifs à la sécurité,  $f$  est la fréquence de l'événement dangereux en l'absence de systèmes relatifs à la sécurité et  $C$  est la conséquence de l'événement dangereux.

La méthode du graphe de risque analyse quatre facteurs de risque relatifs aux dangers et partagés en catégories selon leur importance :

- La conséquence d'un évènement dangereux ( $C$ ),
- La fréquence et le temps d'exposition au danger ( $F$ ),
- La possibilité d'évitement du danger ( $P$ ),
- La probabilité d'apparition d'un accident ( $W$ ).

La structure du graphe de risque dépend du domaine d'activité, d'où l'emploi de différents graphes dans les normes. La prise en compte de dégâts matériels et de dommages causés à l'environnement nécessite l'utilisation de graphes additionnels.

#### 1.4.1.2 Matrice de risque

Contrairement à la méthode du graphe de risque qui ne prend en compte qu'une fonction de sécurité, la matrice de risque intègre plusieurs fonctions de sécurité sous réserve de leur indépendance [54]. La matrice possède trois dimensions : la gravité, la probabilité d'occurrence de l'accident potentiel et le nombre de dispositifs de sécurité qui sont déjà mis en place pour empêcher le développement du danger en un accident [11]. Comme déjà mentionné pour la méthode de graphe de risques, la structure de la matrice de risque dépend du domaine spécifique d'activité [12].

### 1.4.2 Les méthodes quantitatives

Les normes de sécurité fonctionnelle, l'IEC 61508 [54] et l'IEC 61511 [55], introduisent une approche probabiliste pour l'évaluation quantitative de la performance du SIS et la qualification de cette performance par des niveaux de sécurité référencés [111]. L'introduction de probabilité dans la mesure du niveau d'intégrité a entraîné la mise en place de concepts tels que les notions de calcul de probabilité de défaillance à la sollicitation ou de défaillance par unité de temps [112].

L'évaluation de la performance des SIS doit être réalisée par l'utilisation de modèles adaptés. Différentes techniques sont néanmoins préconisées dans les annexes de la norme IEC 61508 [54]. Parmi les méthodes quantitatives citées, on trouve les équations simplifiées, les arbres de défaillances [111], les blocs diagramme fiabilité, les réseaux de Petri [58] ainsi que les chaînes de Markov [58], [107], [139]; [101]. La performance ainsi calculée permet de qualifier le niveau SIL du SIS selon les niveaux définis dans la norme (Tableau 1.1).

#### 1.4.2.1 Les équations simplifiées

Les normes de sécurité fonctionnelle n'imposent cependant pas l'utilisation de modèles particuliers mais fournissent des formules approchées pour les architectures courantes. En effet, la communauté des fiabilistes s'est rendue compte que certaines équations citées dans la norme IEC 61508-6 [54] ne sont valables que sous plusieurs hypothèses qui ne sont pas citées dans la norme [111]. En outre, ces formules ne sont valables que pour certains types d'architecture  $k$  parmi  $n$ . D'après Innal [58], les équations simplifiées sont utilisées

pour l'étude d'architectures de SIS dont les canaux sont mutuellement indépendants et homogènes [58], [111].

Les équations simplifiées donnent la  $PF D_{avg}$  du SIS en fonction de l'architecture des composants (1001 : un parmi un, 1002 : au moins un parmi deux), ... ) et des paramètres de fiabilité utilisés (taux de défaillances des composants  $\lambda$ , taux de couverture de diagnostic  $DC$  et le facteur  $\beta$  qui caractérise les défaillances des causes communes) [58].

Comme mentionné par plusieurs chercheurs dans le domaine de la fiabilité des systèmes [101], [58], il est nécessaire d'utiliser des méthodes de sûreté de fonctionnement classiques telles que les diagrammes de fiabilité [96], les arbres de défaillances [101], ou les approches markoviennes [58] pour évaluer les performances des SIS (la  $PF D_{avg}$  et le SIL), plutôt que d'utiliser les équations simplifiées données dans la partie six de la norme IEC 61508 [54].

#### 1.4.2.2 Blocs diagramme de fiabilité

La méthode de diagramme de fiabilité est une représentation de la logique de fonctionnement des systèmes. Cette méthode est basée sur l'utilisation de blocs pour représenter les composants, les sous-systèmes ou les fonctions. La modélisation consiste à rechercher les liens existants entre ces blocs [96]. Elle permet une analyse quantitative qui a pour objectif en particulier de définir la probabilité de bon fonctionnement d'un système. Les calculs reposent sur les probabilités de réussite des missions des éléments constituant le système. Cette méthode est utilisée dans l'évaluation des performances des SIS par le calcul de la  $PF D_{avg}$  résultante et la détermination du son niveau SIL [44].

La méthode de bloc diagramme de fiabilité a ses limites d'application : il faut s'assurer de l'indépendance entre les différents états de fonctionnement, elle ne permet pas de modéliser des systèmes dynamiques, sauf sous certaines conditions.

#### 1.4.2.3 Arbres de défaillance

La méthode des arbres de défaillance est l'une des méthodes les plus utilisées dans les analyses des performances des SIS [98], [112]. Elle a pour objectif le recensement des causes entraînant l'apparition de l'événement indésirable d'un système et le calcul de sa  $PF D_{avg}$ . Elle constitue un moyen de représentation de la logique des défaillances, cette méthode est adaptée aussi pour l'étude des systèmes élémentaires présentant des défaillances de mode commun [130].

L'arbre de défaillances est une méthode déductive, qui commence par l'événement indésirable et détermine ses causes. L'analyse par l'arbre de défaillances nécessite deux phases ; une qualitative, où on détermine la fonction logique du système en terme de l'ensemble de ses coupes minimales, et l'autre est dite quantitative, où on calcule la probabilité d'occurrence de l'événement indésirable (sommet).

L'évaluation quantitative de la probabilité de l'événement sommet qui représente la défiabilité du système lorsque cet événement est la défaillance d'un système non répa-

nable [97], [109]. La méthode de l'arbre de défaillances consiste à rechercher toutes les combinaisons possibles d'événements entraînant la réalisation de l'événement indésirable. On représente graphiquement ces combinaisons au moyen d'une structure arborescente dont l'événement non désiré est le sommet (ou racine).

Pour décrire la relation entre les événements et la logique d'un système, l'arbre de défaillances utilise des portes logiques. Ces portes indiquent les types des événements et les types de relation qui sont impliquées.

L'arbre de défaillances peut mener à des évaluations quantitatives de la probabilité d'occurrence de l'événement indésirable qui représente la défiabilité lorsque cet événement est la défaillance d'un SIS non réparable [130], [97].

### a) Constitution

L'arbre de défaillances est constitué de trois types d'événements : les événements de base, l'événement non désiré (indésirable) et les événements intermédiaires. La combinaison d'événements de base mène vers l'événement non désiré. Les événements sont combinés par les portes classiques "ET" et "OU", ou les portes  $k/n$  ( $k$  parmi  $n$ ).

Les portes logiques lient les événements par des relations de causalité. Les principales portes logiques sont représentées dans le tableau 1.2.

Dans un arbre de défaillances constitué uniquement de portes 'OU' (respectivement 'ET'), la probabilité d'occurrence de l'événement indésirable (Sommet) est donnée par l'équation 1.6 (respectivement 1.7) :

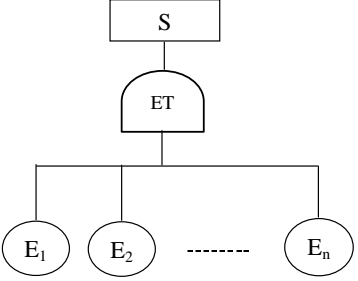
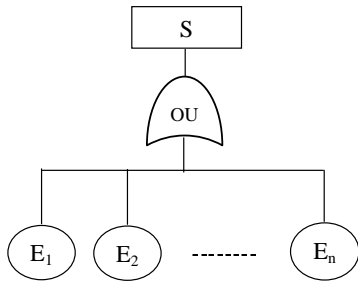
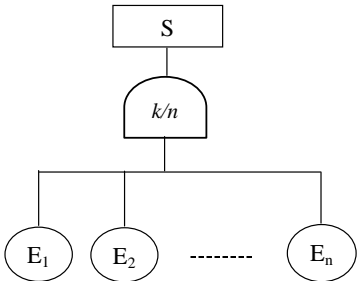
$$P_S(t) = 1 - \prod_{i=1}^n (1 - P_i(t)) \quad (1.6)$$

$$P_S(t) = \prod_{i=1}^n P_i(t) \quad (1.7)$$

$n$  est le nombre d'évènement de base,  $P_i(t)$  la probabilité de défaillance du  $i^{ime}$  composant à l'instant  $t$  et  $P_S(t)$  la probabilité de défaillance du système.

Les systèmes ne répondent pas exclusivement aux équations (1.6) et (1.7) mais à une combinaison de ces deux équations en relation avec leur structure généralement de type parallèle-série ou série-parallèle. Si leur structure est complexe les équations précédentes ne sont plus exploitables directement [130].

TABLE 1.2 – Représentation des portes logiques

Symbole	Nom	Signification
 <p>The diagram shows a rectangular box labeled 'S' at the top. Below it is a semi-circular gate labeled 'ET'. Three lines connect the bottom of the gate to three circles labeled 'E1', 'E2', and 'En'. A dashed line between 'E2' and 'En' indicates multiple inputs.</p>	Porte 'ET'	L'événement sommet S de la porte 'ET' est généré si tous les événements d'entrée sont présents simultanément.
 <p>The diagram shows a rectangular box labeled 'S' at the top. Below it is a semi-circular gate labeled 'OU'. Three lines connect the top of the gate to three circles labeled 'E1', 'E2', and 'En'. A dashed line between 'E2' and 'En' indicates multiple inputs.</p>	Porte 'OU'	L'événement sommet S de la porte 'OU' est généré si l'un au moins des événements d'entrée est présent.
 <p>The diagram shows a rectangular box labeled 'S' at the top. Below it is a semi-circular gate labeled 'k/n'. Three lines connect the bottom of the gate to three circles labeled 'E1', 'E2', and 'En'. A dashed line between 'E2' and 'En' indicates multiple inputs.</p>	Porte ' $k/n$ '	L'événement sommet S est généré si au moins $k$ parmi $n$ événements d'entrée sont présents.

## b) Méthodes de réduction des arbres de défaillance

L'analyse des systèmes complexes par les arbres de défaillance conduit généralement à des arbres de taille importante ce qui rend le calcul des probabilités difficile, d'où la nécessité des méthodes de réduction comme la méthode des coupes minimales (CM) et celle des diagrammes de décision binaire (DDB) [97].

### b-1) Méthode des coupes minimales

Une coupe est un ensemble d'événements qui entraîne l'événement indésirable, c'est-à-dire, la panne de l'élément de la coupe entraîne la panne du système. Une coupe minimale

est la plus petite combinaison d'événements entraînant l'événement indésirable. Ainsi, par définition, si un des événements d'une coupe minimale ne se produit pas, l'événement indésirable ne se réalise pas, donc c'est une coupe qui ne contient aucune autre coupe.

L'expression booléenne de l'événement indésirable est obtenue sous la forme :

$$S = C_1 + C_2 + \dots + C_n = \sum_{i=1}^n C_i \quad (1.8)$$

où  $C_i$  est le produit de  $m$  événements de base :

$$C_i = B_i^1 \cdot B_i^2 \cdot \dots \cdot B_i^m = \prod_{j=1}^m B_i^j \quad (1.9)$$

Quand l'expression de  $S$  est réduite, les événements  $C_i$  sont les coupes minimales, la coupe  $C_i$  est dite d'ordre  $m_i$ .

La probabilité d'occurrence de l'événement indésirable est :

$$P(S) = P[C_1 + C_2 + \dots + C_n] = P\left[\sum_{i=1}^n C_i\right] \quad (1.10)$$

## b-2) Méthode de diagramme de décision binaire (DDB)

Le diagramme de décision binaire est une représentation des fonctions booléennes basée sur le théorème de Boole, en particulier la décomposition de Shannon. Cette dernière est définie par la conjonction ternaire " Si Alors Sinon " 'If-Then-Else' (ITE).

En 1993, Rauzy [97] a proposé un codage binaire des arbres de défaillances. Chaque événement est transformé en une variable booléenne  $x$  qui vaut 1 si l'évènement s'est produit et 0 sinon. Les portes logiques sont directement traduites en connecteurs logiques.

Soit  $f$  une formule booléenne dépendant d'une variable  $x$ . L'égalité suivante est vérifiée :

$$F = \text{iet}(x, f_1, f_0) = x \cdot f_1 + \bar{x} \cdot f_0 \quad (1.11)$$

$x$  est l'une des variables de décision. Les fonctions  $f_1$  et  $f_0$  sont des fonctions Booléennes évaluées respectivement à  $x = 1$  et  $x = 0$ .

En choisissant un ordre total sur les variables et en appliquant récursivement la décomposition de Shannon, la table de vérité de toute formule peut être représentée graphiquement par un arbre binaire. Chaque noeud interne de cet arbre code une formule  $f$  et peut se lire comme un opérateur *si-alors-sinon*.

Le DDB est une structure de données qui permet de représenter de façon compacte les relations entre variables booléennes [99]. Il est devenu incontournable pour les outils de vérification. Il permet d'analyser l'arbre et de déterminer les coupes minimales.

Le DDB utilisé pour l'analyse d'un arbre de défaillances est connu plus correctement sous le nom d'un DDB Rangé Réduit ; Réduit indique le DDB est dans sa forme minimale, et Rangé indique que les variables apparaissent dans le même ordre sur chaque trajectoire [99], [53].

#### 1.4.2.4 Chaînes de Markov

Les chaînes de Markov apportent une bonne formalisation de tous les états que peuvent prendre les systèmes en fonction des événements rencontrés (défaillance, réparation, ...) et des paramètres étudiés (taux de défaillance, défaillance de cause commune, ...) [139]. Les chaînes de Markov apportent une finesse de modélisation pertinente au regard du comportement des SIS étudiés notamment les SIS faiblement sollicités et périodiquement testés [112]. Compte tenu de la relative complexité des SIS, l'explosion combinatoire du nombre des états est l'inconvénient majeur des chaînes de Markov. Cet inconvénient est généralement surmontable.

L'évaluation de la performance du SIS est obtenue grâce à une chaîne de Markov synthétique représentant les différents états du SIS tout en tenant compte des différents types de défaillance. Elle permet de déterminer la probabilité de défaillance à la demande du SIS et de calculer sa valeur moyenne par intégration dans le temps. La détermination du niveau de sécurité du SIS est obtenue par référence aux données du tableau 1.1, [58], [101], [112].

La méthode des chaînes de Markov est souvent utilisée pour analyser et évaluer les performances des systèmes réparables et avec des composants à taux de défaillance constant. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et à chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une action de réparation. Elle permet ainsi de faire une analyse dynamique du système.

Dans l'évaluation des performances des systèmes par les chaînes de Markov on utilise le processus d'analyse constitué de trois parties. La première partie est consacrée au classement de tous les états du système en états de fonctionnement, états dégradés ou états de panne. La deuxième partie concerne la détermination de toutes les transitions possibles entre ces différents états, tout en tenant compte des actions de réparations. Enfin on calcule les probabilités de se trouver dans les différents états du système étudié.

Pour l'étude des systèmes par chaînes de Markov, on distingue deux représentations possibles, chaînes de Markov à temps discret et chaînes de Markov à temps continu.

**a) Chaînes de Markov à temps discret**

Un système Markovien est un système qui transite de l'état  $S_i$  à l'état  $S_j$  avec une probabilité  $a_{ij}$  qui ne dépend que des états  $S_i$  et  $S_j$  (système sans mémoire).

La matrice  $A = (a_{ij})$  de dimension  $(r \times r)$  est la matrice de transition élaborée à partir des probabilités de transition  $a_{ij}$ . Cette matrice est caractérisée par le fait que la somme de chacune de ses lignes est égale à un et chaque coefficient  $a_{ij}$  est positif.

**a-1) Equation de Chapman-Kolmogorov**

Soient  $p^{(n)}$  le vecteur de probabilités des différents états et  $A$  la matrice des probabilités de transition supposées connues, les vecteurs  $p^{(n)}$  vérifient la formule suivante :

$$(p_0^{(n+1)}, p_1^{(n+1)}, \dots, p_r^{(n+1)}) = (p_0^{(n)}, p_1^{(n)}, \dots, p_r^{(n)}) \cdot \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,r} \\ a_{2,1} & a_{2,2} & \dots & a_{2,r} \\ \cdot & \cdot & \dots & \cdot \\ a_{r,1} & a_{r,2} & \dots & a_{r,r} \end{bmatrix} \quad (1.12)$$

L'équation 1.12 peut s'écrire sous la forme compacte :

$$p^{(n+1)} = p^{(n)} \cdot A \quad (1.13)$$

où  $p^{(n)}$  de dimension  $(1 \times r)$ , est la distribution de probabilités des différents états à l'instant  $n$ .

Quand les coefficients sont constants et indépendants du temps, le processus de Markov est dit homogène.

Une chaîne de Markov est dite irréductible quand tous les états communiquent. Le système passe d'un état à un autre soit directement soit par l'intermédiaire d'autres états.

En appliquant l'équation 1.13 aux différents instants. L'équation de Chapman Kolmogorov peut être formulée, elle représente l'état du système à l'instant  $n$  en fonction de son état initial, comme suit :

$$p^{(n)} = p^{(0)} \cdot A^n \quad (1.14)$$

**a-2) Remarques**

- La distribution  $p^{(n)}$  converge vers une distribution limite, notée  $p^{(\infty)}$ , lorsque  $n$  tend vers l'infini.

- Si une certaine puissance de la matrice de transition  $A$  n'a que des composantes strictement positives alors il existe une distribution limite lorsque  $n \rightarrow \infty$ .  $p^{(\infty)}$  est indépendante du vecteur stochastique initial  $p^{(0)}$ .
- De même, la suite des matrices  $A$  lorsque  $n \rightarrow \infty$ , converge vers la matrice  $A^\infty$  dont toutes les lignes sont égales au vecteur  $\omega$  qui n'est autre que  $p^{(\infty)}$ .

$$\lim_{t \rightarrow \infty} A^n = A^\infty = \begin{bmatrix} w_1 & w_2 & \dots & w_r \\ w_1 & w_2 & \dots & w_r \\ \cdot & \cdot & \dots & \cdot \\ w_1 & w_2 & \dots & w_r \end{bmatrix} \quad (1.15)$$

où les coefficients  $\omega_i > 0$ , vérifiant  $\sum_{i=1}^r \omega_i = 1$  pour tout  $i$ , .

$\omega$  est l'unique vecteur propre gauche de la matrice de transition  $A$  pour la valeur propre 1, vérifiant  $\omega.A = \omega$ .

### b) Processus de Markov : Cas continu

Dans ce cas, le temps  $t$  est un nombre réel positif ou nul. Les concepts introduits dans le cas discret ont leurs équivalents dans le cas continu.

#### Définition 1.1

On appelle générateur stochastique infinitésimal toute matrice  $A = (a_{ij})$  vérifiant les conditions suivantes :

- La somme des éléments d'une ligne quelconque de la matrice  $A = (a_{ij})$  est nulle.
- les termes diagonaux  $a_{ii}$  de la matrice sont négatifs et égaux à l'opposé de la somme des taux de transition faisant sortir le système de l'état  $S_i$  ;

$a_{ij}$  représente le taux de transition de l'état  $S_i$  vers l'état  $S_j$ .

#### b-1) Equation de Chapman-Kolmogorov en temps continu

Un processus est dit processus de Markov si et seulement si son vecteur stochastique  $p(t)$  vérifie l'équation différentielle suivante :

$$\frac{d}{dt}P(t) = P(t).A \quad (1.16)$$

$A$  est une matrice de dimension  $(r \times r)$ , appelée générateur stochastique infinitésimal.

L'équation (1.16) est l'équation d'état du processus de Markov. Cette equation admet pour solution le vecteur :

$$p^{(t)} = p^{(0)}.e^{A.t} \quad (1.17)$$

La résolution de cette équation se ramène à un calcul des exponentielles des matrices de transition. Dans le cas continu, le calcul de l'exponentielle est basé sur le calcul des valeurs propres de  $A$ .

Si  $A$  est une matrice diagonale alors l'exponentielle de la matrice  $A$  est donnée par la relation :

$$e^{A.t} = \text{Diag}(e^{\lambda_1.t}, e^{\lambda_1.t}, \dots, e^{\lambda_r.t}) \quad (1.18)$$

Si  $A$  n'est pas une matrice diagonale, il existe une matrice de passage  $P$  réversible telle que :

$$A = P^{-1}.D.P \quad (1.19)$$

où  $D$  est une matrice diagonale.

L'exponentielle de la matrice  $A$  est déterminée par la relation suivante :

$$e^{A.t} = P.e^{D.t}.P^{-1} \quad (1.20)$$

**b-2) Remarques :**

Comme dans le cas discret, pour qu'une distribution limite existe et ne dépende pas de la distribution initiale  $p(0)$  il suffit qu'au moins une puissance de la matrice de transition  $A$  n'ait que des composantes strictement positives.

La distribution stochastique stationnaire  $p = (p_0, p_1, \dots, p_r)$  est donnée par l'équation suivante :

$$p.A = 0 \quad (1.21)$$

Cette condition traduit le fait que si la chaîne de Markov est initialisée avec la distribution  $p(0)$ , alors le vecteur stochastique  $p(t)$  est constant à chaque instant.

### 1.4.2.5 Chaînes de Markov multiphase

Les graphes de Markov précédents permettent de décrire le comportement du système dans chaque type de phase. Pour pouvoir réaliser des calculs dans les phases proprement dites, il est nécessaire d'évaluer les conditions initiales [107], [112]. Les probabilités des états à la fin d'une phase permettent de calculer les conditions initiales de la phase suivante. Bien entendu, à chaque phase est attribué un graphe de Markov modélisant le comportement du système (réparable/non réparable) [58].

Lors de l'application des chaînes de Markov dans l'analyse de performance des systèmes, on considère généralement que le comportement du système étudié était le même tout au cours du temps. Dans la réalité, il arrive souvent que cela ne soit vérifié, par exemple le cas des systèmes périodiquement testés [112], [111].

L'état du SIS est connu à ces instants de test et les probabilités des différents états sont également connues. En présence d'une chaîne de Markov multiphases où les phases sont constituées par les intervalles entre tests,  $T$ , successifs [107], [112], [58]. Il existe une matrice de passage  $M$  permettant l'affectation de la distribution des probabilités d'être dans les différents états  $S_j$  aux instants d'inspection  $t_1$ , par exemple, vers la distribution de probabilités aux instants  $t_2$ .

La figure 1.6 illustre un système périodiquement testé proposé par Signoret dans [108], [112]. Un composant unique caractérisé par son taux de défaillance  $\lambda$  et son taux de réparation  $\mu$ . Il peut être dans l'un des états suivants [107] :

- Etat de marche à partir duquel il peut tomber en panne cachée,  $M$  ;
- Etat de panne cachée  $P$  où il reste jusqu'au test suivant,  $P$  ;
- Etat de réparation  $R$  dû à la détection d'une panne lors d'un test,  $R$ .

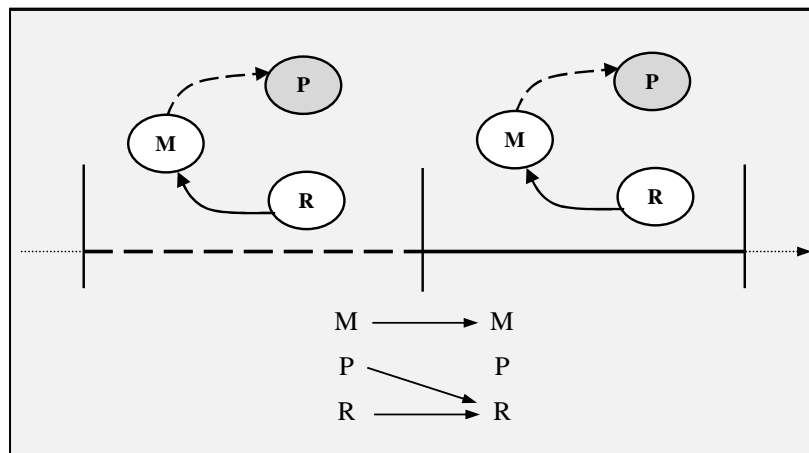


FIGURE 1.6 – Composant périodiquement testé [99]

Pour le système de la figure 1.6. Il y a un seul type de phase modélisé par le graphe à trois états décrits ci-dessus et les phases s'enchaînent au moment du test de la manière suivante :

- si le système fonctionne, il y reste.
- si le système est en panne, il passe en réparation.
- si le système est en réparation, il y reste.

Cette analyse permet de décoller une matrice de passage interphases  $M_i$ , ce qui permet d'évaluer la disponibilité moyenne du système étudié, qui est en général le paramètre recherché pour les systèmes de sécurité périodiquement testés [107], [112]; [58]; [30].

L'approche des chaînes de Markov multiphase est particulièrement bien adaptée au traitement des systèmes de sécurité périodiquement testés et qu'elle permet de prendre en compte des contraintes difficiles à modéliser avec une approche du type arbre de défaillances. Les calculs d'indisponibilité moyenne permis par cette approche correspondent très exactement aux calculs de la  $PFD_{avg}$  introduits dans les normes internationales IEC 61508 et IEC 61511 [54], [55] pour l'évaluation des SIL des SIS.

## 1.5 Conclusion

La norme IEC 61508 est la norme de référence pour la spécification et la conception des SIS. Sa déclinaison sectorielle dans le domaine du process industriel [55] est destinée aux concepteurs et utilisateurs de ce domaine. Ces normes de sécurité fonctionnelle introduisent une approche probabiliste pour l'évaluation quantitative de la performance du SIS et la qualification de cette performance par des niveaux de sécurité référencés (cf. Tableau 1.1).

L'introduction de probabilité dans la mesure de niveau d'intégrité a entraîné la mise en place de nouveaux concepts tels que les notions de calculs de probabilité moyenne de défaillance à la sollicitation  $PFD_{avg}$  ou de défaillance par unité de temps. Différentes techniques sont néanmoins préconisées dans les annexes de la norme sans toutefois exclure toute méthode pertinente de calcul probabiliste. Parmi les méthodes citées, on trouve les arbres de défaillances, les blocs diagramme fiabilité ainsi que les chaînes de Markov. La performance ainsi calculée permet alors de qualifier le niveau SIL du SIS selon les niveaux définis par la norme qui en sont l'un des points clés. Cette évaluation s'apparente à un calcul d'indisponibilité de la fonction de sécurité.

# 2

## Méthodes et techniques pour l'évaluation des systèmes à paramètres imprécis

### Sommaire

---

<b>2.1</b>	<b>Introduction</b>	<b>32</b>
<b>2.2</b>	<b>Terminologie des informations imparfaites</b>	<b>32</b>
<b>2.3</b>	<b>Représentation des connaissances imparfaites</b>	<b>32</b>
2.3.1	Théorie des probabilités	33
2.3.2	Théorie des intervalles	35
2.3.2.1	Opérations logiques sur les intervalles	35
2.3.2.2	Opérations arithmétiques sur les intervalles	36
2.3.3	Théorie des sous-ensembles flous	37
2.3.3.1	Opérations de base des sous-ensembles flous	38
2.3.3.2	Nombres flous	39
2.3.3.3	Nombres flous de type $L - R$	39
2.3.3.4	Notion d' $\alpha$ -coupe	40
2.3.4	Théorie des possibilités	41
2.3.5	Théorie des fonctions de croyance	42
2.3.6	Théorie de familles de probabilités cumulées : p-boxe	42
2.3.6.1	Propagation de l'incertitude dans le cadre des P-boxes	43
2.3.6.2	Discretisation d'une P-box	44
2.3.6.3	Opérations mathématiques des p-boxes	45
<b>2.4</b>	<b>Méthodes pour l'évaluation des performances des systèmes en présence d'informations imprécises</b>	<b>47</b>
2.4.1	Méthodes d'évaluations par arbres de défaillances à paramètres imprécis	47

---

2.4.1.1	Méthode de Singer . . . . .	48
2.4.1.2	Méthode des $\alpha$ -coupes . . . . .	49
2.4.2	Evaluation par les chaînes de Markov des systèmes à paramètres imprécis . . . . .	51
2.4.2.1	Chaînes de Markov à probabilités de transitions floues	52
2.4.2.2	Méthode des $\alpha$ -coupes . . . . .	53
2.4.2.3	Modèle de Markov avec un système d'inférence flou (MMF) . . . . .	53
<b>2.5</b>	<b>Conclusion . . . . .</b>	<b>58</b>

---

## 2.1 Introduction

Dans les études d'indisponibilité des systèmes, les connaissances manipulées concernant les paramètres de défaillances des composants sont généralement imparfaites [126]; [101]. L'incertitude sur des paramètres peut avoir deux origines [4]. La première source d'incertitude provient du caractère aléatoire de l'information qui est dû à une variabilité naturelle résultant de phénomènes stochastiques. On parle alors d'incertitudes de variabilité ou d'incertitudes stochastiques [105]. La seconde source d'incertitude est liée au caractère imprécis et incomplet de l'information en raison d'un manque de connaissance. On parle alors d'incertitudes épistémiques. Plusieurs théories ont été développées pour modéliser et manipuler l'incertitude et l'imprécision.

Dans ce chapitre, on introduit, les différentes notions de base concernant les théories et les modèles mathématiques de représentation l'imprécision et l'incertitude; théorie des probabilités, théorie d'intervalles, théorie des sous-ensembles flous, théorie des familles de probabilités p-boxes,...

## 2.2 Terminologie des informations imparfaites

Les natures de l'imperfection de l'information sont divisées en trois types [14] :

- L'incertitude concerne un doute sur la validité d'une connaissance. Celui-ci peut provenir d'une fiabilité relative de l'intermédiaire d'observation, peu sûr de lui ou susceptible de commettre des erreurs ou de donner intentionnellement des informations erronées, ou encore d'une difficulté dans l'obtention ou la vérification de la connaissance.
- L'imprécision correspond à une difficulté dans l'énoncé de la connaissance, soit parce que les valeurs numériques des connaissances sont mal connues, soit parce que les termes du langage naturel sont utilisés pour qualifier une caractéristique du système de façon vague [48].
- L'incomplétude présente une absence de connaissances sur les paramètres caractéristiques du système. Elle peut être due à l'impossibilité d'obtenir certains renseignements ou à un problème au moment de la mesure de la connaissance [28], [26].

## 2.3 Représentation des connaissances imparfaites

La modélisation des imperfections de l'information amène à considérer les langages disponibles à cet effet [1]. On en retrouve un grand nombre et parmi ces langages, la théorie des probabilités est la plus ancienne et certainement encore la plus utilisée. Elle s'adresse aux incertitudes de nature aléatoire, ce qui renvoie aux concepts d'expérience aléatoire, d'ensemble fondamental ...

Dans le cas particulier de données numériques approximatives, la modélisation par

des intervalles [90], [67] peut être utile et efficace. Le calcul d'intervalles est fréquemment utilisé pour réaliser des calculs d'erreur. Les incertitudes sont alors représentées sous la forme d'intervalles de valeurs.

Bien que la théorie des sous-ensembles flous [136]; [17], [118] soit un outil séduisant, permettant de traiter autant des données numériques que des données en langage naturel, elle ne traite pas l'imprécision et l'incertitude qui peut les entacher dans le même formalisme. En revanche, la théorie des possibilités permet la manipulation de l'incertitude sur des connaissances imprécises ou vagues [26]; [5]. L'association de la théorie des possibilités à la théorie des sous-ensembles flous permet de traiter les connaissances à la fois imprécises et incertaines [26].

La théorie de l'évidence, encore appelée la théorie des fonctions de croyance, est assez proche de la théorie des probabilités mais offre la possibilité de formaliser l'incertitude épistémique. Les fonctions de croyance sont parfois utilisées pour calculer la crédibilité attribuée dans le cas où, on ne connaît pas la probabilité d'occurrence. Les fonctions de croyance sont issues de la théorie de l'évidence développée par Dempster et Shafer [23]. Elle permet également le traitement des connaissances à la fois imprécises et incertaines [23].

Cependant, tous ces modèles de représentation des informations imparfaites définissent des familles de probabilité (p-boxes), [134], [38]. La représentation de l'imprécision par une famille de probabilités est utilisée quand le type de modèle stochastique est connu, ou bien dans le cas où seules certaines informations statistiques descriptives sont disponibles. Ainsi, cette théorie permet de représenter l'information probabiliste incomplète [21], c'est à dire de l'information à la fois aléatoire et imprécise ou incomplète.

### 2.3.1 Théorie des probabilités

La théorie des probabilités offre le plus ancien formalisme permettant de gérer de façon itérative l'incertitude dans les données. Dans ce cadre, la relation entre l'information issue des données et les différentes hypothèses envisagées est représentée par une distribution de probabilités conditionnelles [4]. Les probabilités reposent sur des fondements mathématiques et une expérience solide, ce qui explique son utilisation courante pour représenter l'incertain. Rappelons quelques éléments utiles.

#### Définition 2.1

Dans la théorie des probabilités, il est considéré un espace mesurable  $(\Omega, \Upsilon)$ , où  $\Omega$  est l'ensemble de tous les résultats possibles (événements) d'une expérience et  $\Upsilon$  est un sous-ensemble des parties de  $\Omega$  représentant un ensemble d'événements.

Dans cet espace mesurable  $(\Omega, \Upsilon)$ , une mesure de probabilité est définie, comme étant une fonction vérifiant les axiomes suivants :

$$P(\Omega) = 1 \tag{2.1}$$

$$\forall A, B \in \Upsilon, A \cap B = \emptyset \Rightarrow P(A \cup B) = P(A) + P(B) \quad (2.2)$$

$P(A)$  représente dans quelle mesure l'évènement  $A$  est probable.

### Propriété 2.1

Si  $A$  et  $B$  deux éléments de  $\Upsilon$ , on a :

– Union (formule générale) :  $A \cup B$  représente la réalisation de  $A$  ou de  $B$ .

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \quad (2.3)$$

– Si  $\bar{A}$  représente l'évènement contraire de  $A$ .

$$P(\bar{A}) = 1 - P(A) \quad (2.4)$$

– Inclusion : si  $A \subset B$  alors  $P(A) \leq P(B)$

### Propriété 2.2

Dans le cas où  $A$  est fini, la distribution de probabilité  $p$  est définie comme étant une fonction définissant la mesure de probabilité :

$$P(A) = \sum_{w \in A} p(w) \quad (2.5)$$

Lorsque  $A$  est infini, une distribution de probabilité est une fonction  $p$  définissant la mesure de probabilité  $P$  :

$$P(A) = \int_{w \in A} p(w) dw \quad (2.6)$$

La théorie de probabilités permet de prendre en compte le caractère aléatoire d'expériences, mais pas le caractère imprécis de leur résultat. En effet, aucune incertitude résultant de l'imprécision de la valeur d'un résultat observé d'une expérience n'est prise en compte : une fois la distribution de probabilité connue (ou choisie), il n'y a plus d'imprécision sur les résultats, mais une incertitude, liée uniquement au caractère aléatoire et reproductible [4].

Pour rendre compte du caractère imprécis des observations d'expériences aléatoires, il est possible d'utiliser non pas une distribution de probabilité unique pour décrire le comportement d'une variable aléatoire, mais à l'aide d'une famille de probabilités [4].

## 2.3.2 Théorie des intervalles

Le calcul des intervalles est fréquemment utilisé pour réaliser des calculs d'erreur. Les incertitudes sont représentées sous la forme d'intervalles de valeurs et le calcul d'erreur revient à faire un calcul de pire cas et de meilleur cas. L'intérêt de cette méthode réside dans sa simplicité [90]; [67]; [92]; [62], [132].

### Définition 2.2

Par définition, un intervalle est un ensemble fermé et borné de nombres réels [89], [92], [132]. Si  $x$  désigne une variable réelle bornée alors l'intervalle  $[x]$  auquel elle appartient est défini par :

$$[x] = [x_L, x_R] = \{x \in \mathbb{R} / x_L \leq x \leq x_R\} \quad (2.7)$$

où  $x_L$  et  $x_R$  sont des nombres réels représentant respectivement les bornes inférieure et supérieure de  $x$ .

Les caractéristiques d'un intervalle dont les plus courantes sont fournies dans tableau 2.1. Elles concernent notamment le centre, la longueur et le rayon ...

TABLE 2.1 – Expression des principales caractéristiques d'un intervalle

Description	Représentation	Valeur
Milieu de l'intervalle $[x]$	$\text{mid}([x])$	$(x_L + x_R)/2$
Longueur ou taille $[x]$	$w([x])$	$(x_R - x_L)/2$
Rayon $[x]$	$\text{rad}([x])$	$(x_R - x_L)/2$
Magnitude de $[x]$	$\text{mig}([x])$	$\min_{x \in [x]} x$

### 2.3.2.1 Opérations logiques sur les intervalles

Les intervalles peuvent être vus comme des ensembles sur lesquels s'appliquent des opérateurs logiques (égalité, intersection, union, relation d'ordre, inclusion) permettant de les comparer.

Deux intervalles  $[x]$  et  $[y]$  sont égaux si et seulement si leurs bornes sont égales :

$$[x] = [y] \Leftrightarrow x_L = y_L \quad \text{et} \quad x_R = y_R \quad (2.8)$$

L'intersection de deux intervalles  $[x]$  et  $[y]$  est vide si l'une des conditions  $x_L > y_R$  ou  $x_R < y_L$  est vérifiée. Sinon, cette intersection est aussi un intervalle défini par :

$$[x] \cap [y] = [\max(x_L, y_L), \min(x_R, y_R)] \quad (2.9)$$

L'union de deux intervalles est définie si et seulement si leur intersection est non-vide. Dans ce cas, c'est aussi un intervalle :

$$[x] \cup [y] = [\min(x_L, y_L), \max(x_R, y_R)] \quad (2.10)$$

L'opérateur d'inclusion peut être défini par :

$$[x] \subseteq [y] \Leftrightarrow x_L \geq y_L \quad \text{et} \quad x_R \leq y_R \quad (2.11)$$

### 2.3.2.2 Opérations arithmétiques sur les intervalles

Les intervalles peuvent être vus comme des couples de réels, et non plus seulement en tant qu'ensembles. Les opérations arithmétiques (addition, soustraction, multiplication, division) sur les variables réelles peuvent donc être reformulées dans le cadre de l'analyse par intervalles [67]. Les opérateurs élémentaires de l'arithmétique des intervalles sont définis comme suit :

$$[z] = [x] + [y] = [z_L, z_R] \rightarrow \begin{cases} z_L = x_L + y_L \\ z_R = x_R + y_R \end{cases} \quad (2.12)$$

$$[z] = [x] - [y] = [z_L, z_R] \rightarrow \begin{cases} z_L = x_L - y_R \\ z_R = x_R - y_L \end{cases} \quad (2.13)$$

$$[z] = [x] \times [y] = [z_L, z_R] \text{ avec } : \begin{cases} z_L = \min(x_L \times y_L, x_L \times y_R, x_R \times y_L, x_R \times y_R) \\ z_R = \max(x_L \times y_L, x_L \times y_R, x_R \times y_L, x_R \times y_R) \end{cases} \quad (2.14)$$

$$[z] = [x]/[y] = [z_L, z_R] \text{ avec } : \begin{cases} z_L = \min(x_L/y_L, x_L/y_R, x_R/y_L, x_R/y_R) \\ z_R = \max(x_L/y_L, x_L/y_R, x_R/y_L, x_R/y_R) \end{cases} \quad (2.15)$$

et  $0 \notin y$

Les propriétés de l'arithmétique des intervalles sont des conséquences directes des définitions des opérations qu'elles utilisent [67] ; [62] ; [93].

Tout d'abord, la soustraction n'est pas la réciproque de l'addition. Par exemple, si  $[x] = [2, 4]$  , en utilisant l'équation 2.13, on obtient :  $[x] - [x] = [2, 4] - [2, 4] = [-2, 2] \neq [0, 0]$ , même s'il le contient. En effet :

$$[x] - [x] = \{x - y \mid x \in [x], y \in [y]\} \supset \{x - x \mid x \in [x]\} = [0, 0] \quad (2.16)$$

Le résultat est correct au sens où il vérifie la propriété d'inclusion, mais il est plus grand que le résultat attendu. De la même façon, on peut montrer que la division n'est pas la réciproque de la multiplication.

Une autre propriété algébrique perdue dans le calcul d'intervalles est la distributivité de la multiplication par rapport à l'addition. Moore [89] définit la sous-distributivité en observant que pour les intervalles  $[x]$ ;  $[y]$  et  $[z]$  la relation suivante est toujours satisfaite :

$$[x].([y] + [z]) \subset [x].[y] + [x].[z] \quad (2.17)$$

Cet exemple illustre clairement le fait que des expressions équivalentes en arithmétique conventionnelle ne le sont plus en arithmétique par intervalles.

Les propriétés algébriques de l'arithmétique des intervalles se déduisent de celles rencontrées dans le cas de variables conventionnelles. Néanmoins, certaines propriétés diffèrent à cause de la surestimation (ou un encadrement trop large) des résultats qui a été observé dans les exemples précédents, il s'agit du problème de dépendance ou de décorrélation des données [90], [92].

L'arithmétique des intervalles ne conserve pas la corrélation entre les occurrences de la même variable. Plusieurs techniques ont été développées pour améliorer les résultats de l'arithmétique d'intervalles. Des solutions reposent sur la méthode de fonctions d'inclusion (extension d'intervalle) proposée par Moore [89], développée par Jaulin [63]. L'objectif est d'obtenir un intervalle qui soit le plus proche possible du domaine image de la fonction réelle lorsque le domaine de définition de la fonction réelle est un intervalle [132].

L'intérêt de la théorie des intervalles réside dans sa simplicité [90]. L'inconvénient majeur de ce type de calcul est son caractère peu informatif en termes de quantification de l'incertitude ; notamment il ne permet pas de quantifier dans quelle mesure, un seuil risque d'être dépassé [63].

### 2.3.3 Théorie des sous-ensembles flous

Zadeh [136] a introduit l'idée des sous-ensembles flous en 1965 afin de manipuler des informations exprimées en langage naturel [136]. Dans la théorie des ensembles classiques, une proposition est soit vraie soit fausse [137]. En théorie des ensembles flous une proposition peut être partiellement vraie et fausse.

#### Définition 2.3

Un sous-ensemble usuel  $A$  d'un ensemble de référence  $\Omega$  peut être déterminé à partir de sa fonction caractéristique :

$$\mu_A : \Omega \rightarrow [0, 1] \quad (2.18)$$

Un élément  $x$  de  $\Omega$  est un élément de l'ensemble  $A$  si et seulement si  $\mu_A(x) = 1$ . Un élément  $y$  n'appartient pas à  $A$  si et seulement si  $\mu_A(y) = 0$ .

Une autre définition celle de "fonction caractéristique"  $\mu_A(z)$  dont la valeur indique si, oui ou non  $z$  appartient à  $A$ .

$$\mu_A(z) = \begin{cases} 1 & \text{si } z \in A \\ 0 & \text{sinon} \end{cases} \quad (2.19)$$

#### Définition 2.4

Un sous-ensemble flou  $\tilde{A}$  est caractérisé par sa fonction d'appartenance  $\mu_{\tilde{A}}(x)$  [136], et a pour définition : *un sous-ensemble flou  $\tilde{A}$  sur un référentiel  $\Omega$  est caractérisé par une fonction d'appartenance  $\mu_{\tilde{A}}$  qui associe à chaque élément  $x$  de  $\Omega$  un nombre réel dans l'intervalle  $[0, 1]$  :*

$$\mu_{\tilde{A}} : \Omega \rightarrow [0, 1] \quad (2.20)$$

Le terme  $\mu_{\tilde{A}}(x)$  représente le degré d'appartenance de  $x$  à  $A$ .

Si  $\mu_{\tilde{A}}(x) = 0$ ,  $x$  n'appartient pas à  $\tilde{A}$ . Si  $\mu_{\tilde{A}}(x) = 1$ , il lui appartient totalement. Si  $0 < \mu_{\tilde{A}}(x) < 1$ , alors l'appartenance de  $x$  à  $\tilde{A}$  est plus ou moins complète.

#### Définition 2.5

Le noyau de  $\tilde{A}$  représente l'ensemble des éléments qui appartiennent complètement à l'ensemble flou  $\tilde{A} : \{x \in \Omega / \mu_{\tilde{A}}(x) = 1\}$ . Le support de  $\tilde{A}$  est défini par les éléments pour lesquels le degré d'appartenance n'est pas nul. Si le noyau de  $\tilde{A}$  est non vide,  $\tilde{A}$  est dit normalisé.

##### 2.3.3.1 Opérations de base des sous-ensembles flous

On peut définir les opérations ensemblistes de base qui sont ; l'union, l'intersection et la complémentarité. A partir de sous-ensembles flous  $\tilde{A}$  et  $\tilde{B}$  sur  $\Omega$  définis par leurs fonctions d'appartenance  $\mu_{\tilde{A}}$  et  $\mu_{\tilde{B}}$ . Ces opérations sont définies comme suit :

$$\mu_{\tilde{A} \cup \tilde{B}}(x) = \max(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)) \quad (2.21)$$

$$\mu_{\tilde{A} \cap \tilde{B}}(x) = \min(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)) \quad (2.22)$$

$$\mu_{\tilde{C}}(x) = 1 - \mu_{\tilde{A}}(x) \quad \text{si } C = \bar{A} \quad (2.23)$$

Ces définitions sont les plus utilisées, mais ne sont pas les seules possibles : les opérateurs *max* et *min* peuvent être remplacés par d'autres opérateurs, donnant lieu à d'autres modèles de l'incertain.

L'image d'un ensemble classique  $E$  par une fonction  $f$  est l'ensemble des valeurs que prend  $f$  sur le domaine  $E$ .

La définition de l'image de  $\tilde{B}$  d'un ensemble flou  $\tilde{A}$  par une fonction  $f$  réalisée selon le principe d'extension énoncé par Zadeh [136] est :

$$\mu_{\tilde{B}}(y) = \sup_{x/y=f(x)} \mu_{\tilde{A}}(x) \quad (2.24)$$

### 2.3.3.2 Nombres flous

#### Définition 2.6

Soit  $x$  une variable réelle continue de fonction d'appartenance  $\mu_{\tilde{A}}(x) \in [0, 1]$ , un nombre flou  $\tilde{A}$  est un sous-ensemble flou, qui satisfait aux conditions suivantes :

- $\mu_{\tilde{A}}(x)$  est continue par morceau.
- $\mu_{\tilde{A}}(x)$  est convexe.
- $\mu_{\tilde{A}}(x)$  est normale (il existe au moins une valeur  $x_0$  telle que  $\mu_{\tilde{A}}(x_0) = 1$ ).

### 2.3.3.3 Nombres flous de type $L - R$

Les nombres flous de type  $L - R$  sont une classe particulière de nombres flous puisqu'ils sont définis à partir de deux fonctions  $L$  et  $R$ . On considère trois paramètres réels,  $a$  et  $b$  étant strictement positifs (cf.figure 2.1).  $L$  et  $R$  sont deux fonctions, définies sur l'ensemble  $IR_+$  des réels positifs à valeurs dans  $[0, 1]$  telles que :

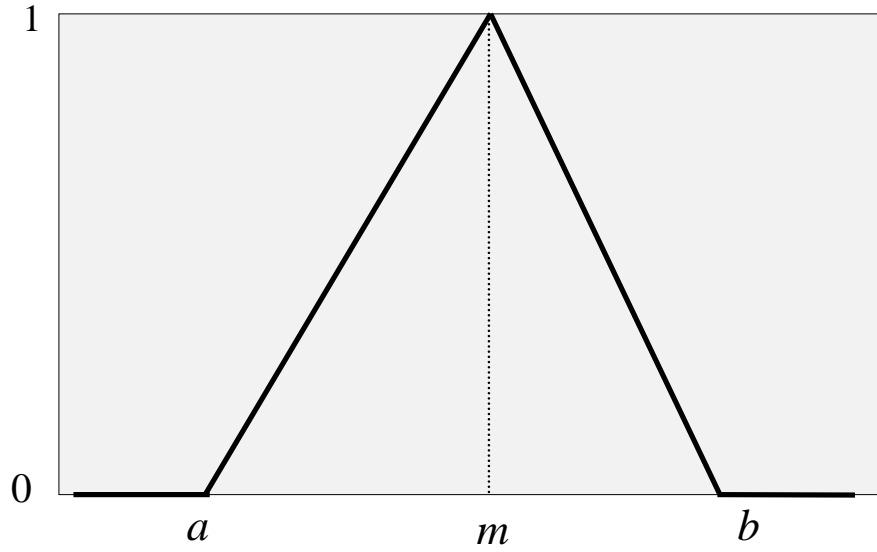
$$L(0) = R(0) = 1, L(1) = 0 \quad \text{où} \quad L(x) > 0 \quad (2.25)$$

avec

$$\lim_{x \rightarrow \infty} L(x) = 0, R(1) = 0, \quad \text{où} \quad R(x) > 0 \quad \text{avec} \quad \lim_{x \rightarrow \infty} R(x) = 0 = 0 \quad (2.26)$$

Un nombre flou  $\tilde{M}$  est de type  $L - R$  si sa fonction d'appartenance  $f_{\tilde{M}}$  est définie par :

$$f_{\tilde{M}}(x) = \begin{cases} R[(x - m)/b] & \text{si } x > m \\ L[(m - x)/a] & \text{si } x \leq m \end{cases} \quad (2.27)$$


 FIGURE 2.1 – Nombre flou triangulaire du type  $L - R$ 

#### 2.3.3.4 Notion d' $\alpha$ -coupe

Un nombre flou  $\tilde{M}$  peut être représenté généralement, soit pas sa fonction d'appartenance, soit par ses coupes de niveau  $\alpha$  :

$$\forall \alpha \in [0, 1], \quad M_\alpha = \{x / \mu_{\tilde{M}}(x) \geq \alpha\} \quad (2.28)$$

Un intervalle flou est un outil adapté à la représentation des quantités imprécises [66]. Dans la plupart des situations où l'on doit évaluer un paramètre (dont la vraie valeur n'est pas connue avec précision) [26].

Comme les opérations arithmétiques utilisées pour traiter les nombres flous requièrent beaucoup de ressources, Kaufman et Gupta [68]. La décomposition des fonctions d'appartenance des nombres flous en  $\alpha$ -coupes a largement simplifié la manipulation des opérateurs arithmétiques flous [101].

Un nombre flou peut être caractérisé par un intervalle de confiance à un certain niveau  $\alpha$ . En effet, si on considère un nombre flou  $\tilde{A}$  de fonction d'appartenance  $\mu_{\tilde{A}}(x)$ , en utilisant la méthode des  $\alpha$ -coupes, on obtient une série d'intervalles emboîtés. Les termes  $A_L^{(\alpha)}$  et  $A_R^{(\alpha)}$  représentent respectivement les limites gauche et droite de la fonction d'appartenance  $\mu_{\tilde{A}}(x)$  à chaque  $\alpha$ -coupe [26], [101].

En utilisant la méthode des  $\alpha$ -coupe, un nombre flou peut être représenté par l'expression suivante :

$$\tilde{A} \rightarrow [A^{(\alpha)}] = [A_L^{(\alpha)}, A_R^{(\alpha)}], 0 \leq \alpha \leq 1 \quad (2.29)$$

En outre, les nombres flous répondent à la propriété d'inclusion monotone spécifiant qu'à un niveau de connaissance donné plus une proposition est imprécise plus elle est certaine [26]. Ainsi, si une information  $X$  est plus spécifique que  $Y$  (et donc l'implique), l'agent qui possède ces informations ne peut pas avoir plus confiance en  $X$  qu'en  $Y$  [29]. Ainsi, la monotonie de l'inclusion pour un nombre flou peut être écrit comme suit :

$$[A^{(\alpha_1)}] \subseteq [A^{(\alpha_2)}] \Rightarrow (1 - \alpha_1) \leq (1 - \alpha_2) \quad (2.30)$$

Soient  $\tilde{X}$  et  $\tilde{Y}$  deux nombres flous, représentés respectivement par les intervalles  $[X_L^{(\alpha)}, X_R^{(\alpha)}]$  et  $[Y_L^{(\alpha)}, Y_R^{(\alpha)}]$  pour chaque  $\alpha$ -coupe. Les opérations arithmétiques appliquées aux intervalles (cf. equations 2.12, 2.13, 2.14) donnent les expressions suivantes :

$$\tilde{Z} = \tilde{X} + \tilde{Y} \rightarrow [Z_L^{(\alpha)}, Z_R^{(\alpha)}] = [X_L^{(\alpha)} + Y_L^{(\alpha)}, X_R^{(\alpha)} + Y_R^{(\alpha)}] \quad (2.31)$$

$$\tilde{Z} = \tilde{X} - \tilde{Y} \rightarrow [Z_L^{(\alpha)}, Z_R^{(\alpha)}] = [X_L^{(\alpha)} - Y_R^{(\alpha)}, X_R^{(\alpha)} - Y_L^{(\alpha)}] \quad (2.32)$$

$$\begin{aligned} \tilde{Z} &= \tilde{X} \cdot \tilde{Y} \rightarrow [Z_L^{(\alpha)}, Z_R^{(\alpha)}] \\ \text{avec : } &\begin{cases} Z_L^{(\alpha)} = \min(X_L^{(\alpha)} \cdot Y_L^{(\alpha)}, X_L^{(\alpha)} \cdot Y_R^{(\alpha)}, X_R^{(\alpha)} \cdot Y_L^{(\alpha)}, X_R^{(\alpha)} \cdot Y_R^{(\alpha)}) \\ Z_R^{(\alpha)} = \max(X_L^{(\alpha)} \cdot Y_L^{(\alpha)}, X_L^{(\alpha)} \cdot Y_R^{(\alpha)}, X_R^{(\alpha)} \cdot Y_L^{(\alpha)}, X_R^{(\alpha)} \cdot Y_R^{(\alpha)}) \end{cases} \end{aligned} \quad (2.33)$$

### 2.3.4 Théorie des possibilités

La théorie des possibilités, appelée comme telle par opposition à la théorie des probabilités est très proche de la théorie des sous-ensembles flous [26], [29] [5].

Une distribution de possibilités est un outil mathématique permettant de représenter l'information incomplète et imprécise. Elle reflète naturellement le format des informations fournis par un expert lorsque celui-ci propose un intervalle de valeurs dans lequel il est sûr que la valeur recherchée s'y trouve. Cet intervalle est choisi de préférence aux intervalles qui lui sont vraisemblables [26]. Ces préférences permettent alors de définir des intervalles emboîtés de plus en plus restreints qui définissent une information plus précise mais au demeurant moins certaine.

Une distribution de possibilités peut être vue comme une fonction d'appartenance de l'ensemble flou des éléments possibles solutions d'un problème donné. Dans ce cas on peut considérer que le degré d'appartenance  $\mu_{\tilde{A}}$ , d'un élément  $x$  à un sous ensemble flou  $\tilde{A}$ , comme un degré de possibilité  $\pi_{\tilde{A}}$  [27], [29]. La fonction d'appartenance est donc considérée comme une distribution de possibilités, notée  $\pi_{\tilde{A}}$ . Cette distribution permet de définir la mesure de possibilité, et de nécessité, d'un évènement.

Comme déjà mentionné dans le paragraphe précédent, une fonction d'appartenance  $\mu(x)$ , d'un élément  $x$ , est considérée comme une distribution de possibilités  $\pi(x)$ . Par analogie à la théorie des ensembles flous, une distribution de possibilité  $\pi$  peut être vue comme un ensemble d'intervalles emboîtés qui représentent les coupes de  $\pi$ .

$$[x_L^{(\alpha)}, x_R^{(\alpha)}] = \{x, \pi(x) \geq \alpha\} = \pi_\alpha \quad (2.34)$$

### 2.3.5 Théorie des fonctions de croyance

La théorie des fonctions de croyance fournit des outils mathématiques permettant à la fois de traiter de l'information de nature aléatoire et imprécise [23], [4]. Les informations sont alors représentées comme des masses (poids de probabilité) affectées à des intervalles. L'ensemble de la connaissance est synthétisé par une distribution de masse appelée aussi fonction de croyance.

Toute distribution de probabilité et toute distribution de possibilité peuvent être représentées à l'aide d'une telle fonction ce qui a pour avantage de travailler dans un cadre commun pour traiter l'information quelle que soit sa nature aléatoire ou imprécise (jugement d'expert) [5].

### 2.3.6 Théorie de familles de probabilités cumulées : p-boxe

Une distribution de probabilités peut aussi être définie par sa fonction de répartition  $F$  [131], appelée aussi probabilité cumulée. Un modèle naturel pour donner une approximation d'une distribution de probabilités mal connue est alors de considérer une paire des fonctions de répartition haute et basse ( $\underline{F}, \overline{F}$ ). Cette paire de fonction permet d'encadrer la distribution de probabilités mal connue et définit une famille de probabilités comme le montre la figure 2.2.

La théorie de familles de probabilités p-boxes  $[\underline{F}, \overline{F}]$  généralise l'idée de l'intervalle d'une paire de points à une paire de probabilités cumulées.

L'intervalle  $[\underline{F}, \overline{F}]$  est nommé p-boxe [38]. Il correspond à une extension du calcul d'intervalle et représente la classe de mesure de probabilité dont les probabilités cumulées sont bornées par  $\underline{F}$  et  $\overline{F}$  telles que :

$$\underline{F}(x) \leq F(x) \leq \overline{F}(x) \quad (2.35)$$

Les p-boxes apparaissent comme un choix naturel pour les modèles paramétriques avec des paramètres imprécis. Par exemple, un modèle gaussien, où la moyenne et/ou l'écart type se situent dans un intervalle prescrit, peut naturellement engendrer une p-boxe étroite [4].

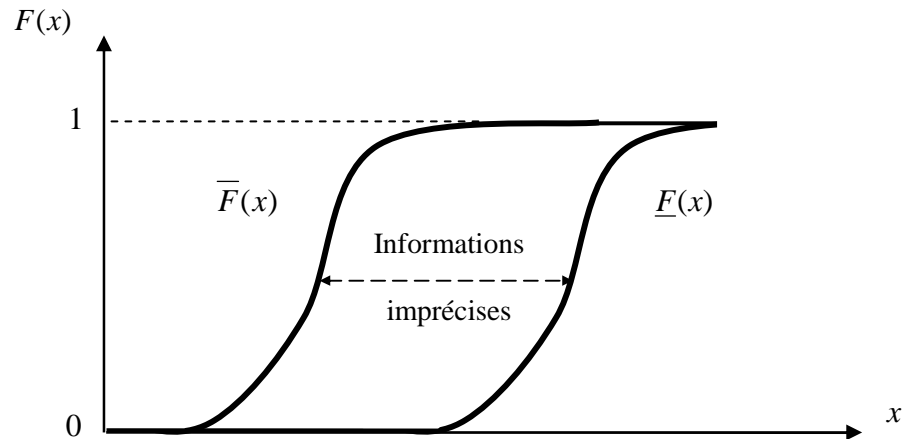


FIGURE 2.2 – Représentation d'une p-boxe

La théorie des p-boxes a été particulièrement étudiée par Ferson [37]. Dans ce qui suit, on rappelle ses propositions pour représenter des distributions de probabilité connaissant le type de modèle stochastique mais on n'a pas une connaissance complète sur ses paramètres, ou bien dans le cas où on dispose de certains paramètres caractéristiques, (min, max, moyenne, mode, . . .), fournis par experts.

### 2.3.6.1 Propagation de l'incertitude dans le cadre des P-boxes

Le calcul avec des probabilités imprécises est une généralisation du problème de calcul du produit de convolution des fonctions de densité de probabilités où les fonctions de densité de probabilités s'avèrent justement être imprécises [134], [7], [38], [39], [25].

La première approche numérique efficace de la propagation des quantités incertaines a été présentée par Williamson et Downs [134]. Le travail de Williamson consiste à développer des méthodes numériques pour l'arithmétique probabiliste précise, mais ses méthodes sont étendues pour les appliquer à l'arithmétique probabiliste imprécise. Les méthodes de Williamson permettent de calculer les bornes résultantes de la fonction de sortie sur la véritable distribution de probabilité pour n'importe quelle relation possible de la dépendance entre les quantités d'entrées incertaines.

Une approche très semblable a été développée indépendamment par Berleant [7]; [8]. Elle consiste à discrétiser les fonctions de distribution de probabilité et à employer les opérations de minimisation et de maximisation pour déterminer les bornes de la probabilité résultante. Berleant appelle son approche '*détermination de l'enveloppe de probabilités*' (ou DEnv) [9]. Regan, [100] a prouvé que la méthode de DEnv et l'approche de produit de convolution sont équivalentes pour des fonctions de distribution cumulées pour les réels positifs [125]. Ces deux approches sont entièrement suffisantes pour la propagation des quantités incertaines dans le cas des opérations binaires, mais elles sont insuffisantes pour

d'autres opérations mathématiques complexes.

### 2.3.6.2 Discrétisation d'une P-box

L'algorithme du produit de convolution des p-boxes, dans le cas d'indépendance, [134] ; [6] ; [7] est essentiellement identique au produit cartésien de Yager [135]. Les p-boxes d'entrée sont discrétisées dans des structures de Dempster-Shafer. Le produit cartésien est calculé et la p-boxe de la sortie résultante est reconstituée à partir de la théorie de Dempster-Shafer [135]. Ferson [37] a amélioré cet algorithme pour calculer les produits de convolution dans d'autres prétentions au sujet de la dépendance entre les quantités incertaines [10].

Soit une quantité incertaine  $X$  discrétisée en  $m$  intervalles, supposons que les intervalles de discrétisation pour l'entrée  $X$  sont également distribués le long de l'axe des probabilités cumulées.

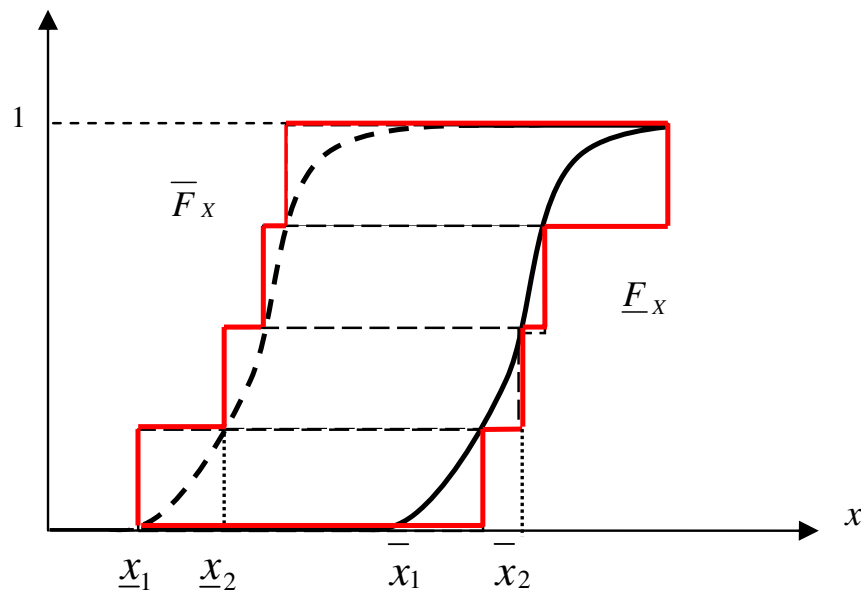


FIGURE 2.3 – Discrétisation d'une P-boxe

Chaque P-boxe  $[F_X, \bar{F}_X]$  est représentée par une série de paire de probabilités de la forme (intervalle, masse), où l'intervalle correspond à une section horizontale de la p-boxe et la masse correspond à son poids de probabilités :  $\{(x = [\underline{x}_i, \bar{x}_i], p_i)\}$ , pour  $i, \dots, m$ . Il s'agit d'une discrétisation canonique. Chaque intervalle de probabilités est alors propagé par un produit cartésien à travers une fonction [135], [134], [7].

### 2.3.6.3 Opérations mathématiques des p-boxes

Soit une fonction binaire des quantités incertaines  $X$  et  $Y : Z = f(X, Y)$ . Les entrées incertaines,  $X$  et  $Y$ , sont discrétisées respectivement en  $m$  et  $n$  intervalles, alors le produit cartésien résultant est  $(m \times n)$  éléments de l'intervalle des paires de masses.

Pour chaque p-box  $[\underline{F}_X, \overline{F}_X]$ , on obtient une série d'intervalles :

$[x_i] = [\underline{x}_i, \overline{x}_i]$ ,  $i = 1, \dots, m$  de même pour  $[\underline{F}_Y, \overline{F}_Y]$ , on récupère une série d'intervalles

$[y_j] = [\underline{y}_j, \overline{y}_j]$ ,  $j = 1, \dots, n$ .

Chaque intervalle de probabilités est alors propagé par un produit cartésien à travers la fonction  $f$ .

La p-boxe résultante  $[\underline{F}_Z, \overline{F}_Z]$ , dans le cas d'indépendance entre les variables d'entrées, est alors ordonnée comme suit :  $(f(x_i, y_j), \frac{1}{m} \times \frac{1}{n})$  pour  $i = 1, \dots, m$  et  $j = 1, \dots, n$ .

Par exemple :  $Z = X \times Y$ , le cas où les entrées  $X$  et  $Y$  sont indépendantes. La figure 2.4 représente la p-boxe  $[\underline{F}_X, \overline{F}_X]$ .

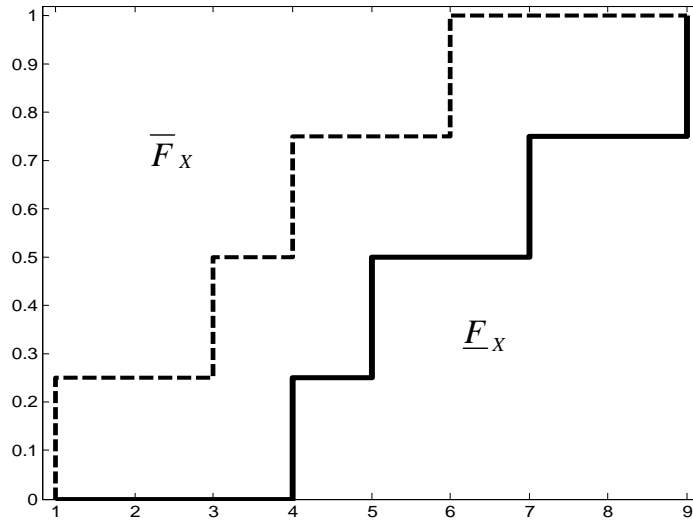


FIGURE 2.4 – La p-boxe de la variable  $X$

$$[\underline{F}_X, \overline{F}_X] = \{([1, 4], \frac{1}{4}); ([3, 5], \frac{1}{4}); ([4, 7], \frac{1}{4}); ([3, 5], \frac{1}{4})\}$$

La p-boxe  $[\underline{F}_Y, \overline{F}_Y]$  est représentée par la figure 2.5.

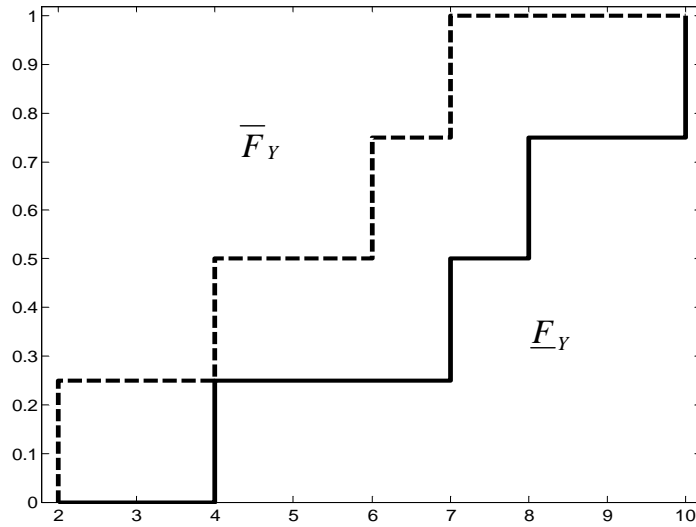


FIGURE 2.5 – La p-boite de la variable  $Y$

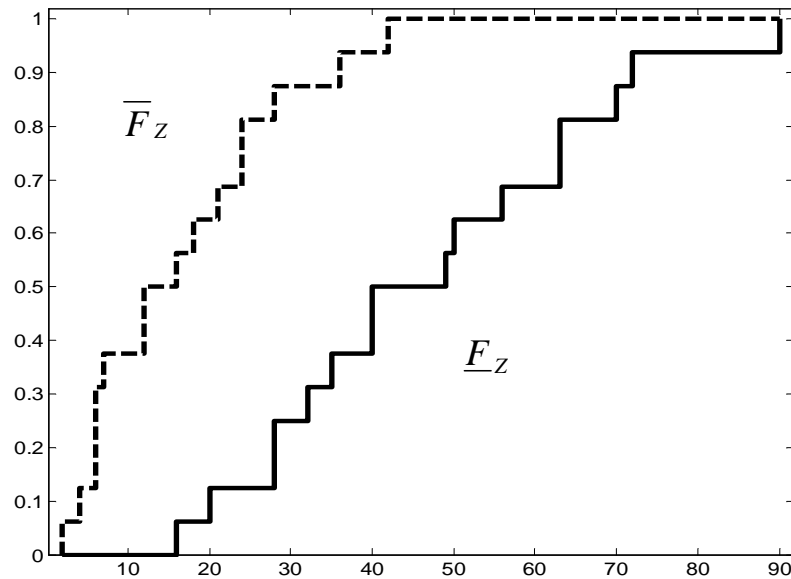
$$[E_Y, \bar{F}_Y] = \{([2, 4], \frac{1}{4}); ([4, 7], \frac{1}{4}); ([6, 8], \frac{1}{4}); ([7, 10], \frac{1}{4})\}$$

Les bornes de la distribution des probabilités cumulées du produit de  $X$  et  $Y$  sont déterminées à partir des données du tableau 2.2. Il s'agit d'une discrétisation canonique. Chaque intervalle de probabilités est propagé sur la base du produit cartésien à travers une fonction mathématique.

TABLE 2.2 – Produit de  $X$  et  $Y$  (cas  $X$  est indépendante de  $Y$ )

		$X$			
		$[1, 4], \frac{1}{4}$	$[3, 5], \frac{1}{4}$	$[4, 7], \frac{1}{4}$	$[6, 9], \frac{1}{4}$
$Y$	$[2, 4], \frac{1}{4}$	$[2, 16], \frac{1}{16}$	$[6, 20], \frac{1}{16}$	$[8, 28], \frac{1}{16}$	$[12, 36], \frac{1}{16}$
	$[4, 7], \frac{1}{4}$	$[4, 28], \frac{1}{16}$	$[12, 35], \frac{1}{16}$	$[16, 49], \frac{1}{16}$	$[24, 63], \frac{1}{16}$
	$[6, 8], \frac{1}{4}$	$[6, 32], \frac{1}{16}$	$[18, 40], \frac{1}{16}$	$[24, 56], \frac{1}{16}$	$[36, 72], \frac{1}{16}$
	$[7, 10], \frac{1}{4}$	$[7, 40], \frac{1}{16}$	$[21, 50], \frac{1}{16}$	$[28, 70], \frac{1}{16}$	$[42, 70], \frac{1}{16}$

La p-boite résultante du produit de  $X$  par  $Y$  est donnée par la figure 2.6

FIGURE 2.6 – La p-boxe résultante  $Z = X.Y$ 

Il semble naturel de considérer une famille de mesures de probabilités p-boxe lorsque nous sommes confrontés à l'information probabiliste incomplète ou encore quand les paramètres d'un modèle probabiliste tels que la moyenne ou l'écart type sont mal connus.

## 2.4 Méthodes pour l'évaluation des performances des systèmes en présence d'informations imprécises

Il existe dans la littérature plusieurs méthodes quantitatives d'évaluation dans le domaine du sûreté de fonctionnement intégrant les théories de représentation des informations imprécises (théorie de probabilité, théorie des intervalles, théorie des sous ensembles flous, ...). On s'intéresse particulièrement à la méthode des arbres de défaillances, la plus utilisée pour l'évaluation des systèmes non réparables et la méthode des chaînes de Markov qui permet de traiter l'aspect dynamique des systèmes.

### 2.4.1 Méthodes d'évaluations par arbres de défaillances à paramètres imprécis

Des nombreux travaux concernent l'étude de l'imprécision dans les arbres de défaillances [121]; [117]; [104]; [75], [36]. Les premiers travaux d'analyse des arbres de défaillance intégrant le formalisme appartiennent à Tanaka [121]. Il utilise dans ses travaux le principe d'extension de Zadeh [136] pour calculer la probabilité d'occurrence de

l'événement sommet de l'arbre. Les probabilités d'occurrence des événements de base sont représentées par des nombres flous trapézoïdaux. Par contre Singer [115] a choisi de modéliser l'imprécision des probabilités d'occurrence des événements de base à l'aide des nombres flous du type  $L - R$ . Soman et Misra [117] ont aussi analysé les arbres de défaillances flous. Dans leurs travaux, ils proposent une méthode connue sous le nom de l'identité de résolution basée sur la méthode des  $\alpha$ -coupes pour traiter les arbres contenant des événements répétés.

Sallak [104] a également appliqué la méthode des  $\alpha$ -coupes pour l'étude de l'imprécision dans les arbres de défaillances [103]. Ses travaux sont basés sur la représentation des taux de défaillances des composants par des nombres flous de type  $L - R$  et concernent l'évaluation imprécise des performances des systèmes et particulièrement les SIS. Limbourg [75] a traité aussi la problématique de l'imprécision dans l'évaluation de la probabilité de défaillance des systèmes. Leur travaux sont basés sur l'utilisation de la théorie de Dempster Shafer pour la modélisation de l'incertitude dans les arbres de défaillances [114]. Ils ont étudié la propagation de la fonction de masses résultantes du modèle du système analysé à partir de son arbre de défaillances [75].

#### 2.4.1.1 Méthode de Singer

Le traitement des arbres de défaillance floue selon Singer [115] est basé sur la représentation les probabilités d'occurrence des événements de base par des nombres flous. Il calcule les fonctions d'appartenance des différents événements intermédiaires de l'arbre en appliquant le principe d'extension flou de Zadeh [136]. Il remplace les probabilités d'occurrence des événements de base comme des probabilités floues du type  $L - R$ . Puis, il utilise les deux opérateurs de base (portes 'ET' et 'OU') afin de calculer la probabilité de défaillance floue du système [115]; [104].

La forme floue d'une association d'opérateurs 'ET' est :

$$\tilde{p}_S = AND(\tilde{p}_0, \tilde{p}_1, \dots, \tilde{p}_n) = \prod_{i=1}^n \tilde{p}_i \quad (2.36)$$

où  $\tilde{p}_i$  est la probabilité floue d'occurrence de l'évènement  $i$  et  $\tilde{p}_S$  est la probabilité floue d'occurrence de l'évènement indésirable (sommet).

De même, la forme floue d'une association d'opérateurs 'OU' est :

$$\tilde{p}_S = OR(\tilde{p}_0, \tilde{p}_1, \dots, \tilde{p}_n) = 1 - \prod_{i=1}^n (1 - \tilde{p}_i) \quad (2.37)$$

La probabilité d'occurrence de l'évènement indésirable peut être déterminée en appliquant les équations (2.36) et (2.37). La méthode de Singer [115] permet d'évaluer la probabilité de défaillance d'un système à partir de son arbre de défaillances à paramètres

fous. Cette méthode, limite le choix de la probabilité floue de l'événement de base uniquement aux nombres fous de type  $L - R$ .

### 2.4.1.2 Méthode des $\alpha$ -coupes

La méthode des  $\alpha$ -coupes, traite les arbres de défaillances intégrant le formalisme flou. Pour appliquer cette méthode les probabilités d'occurrence des événements de base sont considérées comme des nombres fous [104]. Chaque nombre flou est décrit par un ensemble d'intervalles emboîtés défini par l' $\alpha$ -coupe. Les travaux de Sallak [104] sont basés sur l'approximation des événements rares et le facteur des défaillances de cause commune est considéré nul. Cependant, il n'est pas toujours possible d'éliminer les répétitions d'évènements et l'hypothèse d'évènements rares n'est pas toujours vérifiée.

Sallak applique les opérateurs de *multiplication* pour les portes "ET" (cf. equation 2.38) et *d'addition* pour les portes "OU" de l'arbre (cf. equation 2.39) afin calculer la probabilité d'occurrence de l'événement sommet à chaque  $\alpha$ -coupe [101]. La distribution de la probabilité floue d'occurrence de l'événement sommet est construite à partir des probabilités d'occurrence calculées à chaque  $\alpha$ -coupe.

$$\tilde{p}_S = \prod_{i=1}^n \tilde{p}_i \Rightarrow [p_S^{(\alpha)}] = \prod_{i=1}^n ([p_i^{(\alpha)}]) \quad (2.38)$$

$$\tilde{p}_S = \sum_{i=1}^n \tilde{p}_i \Rightarrow [p_S^{(\alpha)}] = \sum_{i=1}^n ([p_i^{(\alpha)}]) \quad (2.39)$$

$\tilde{p}_i$  est la probabilité floue d'occurrence de l'événement de base  $i$ .

$[p_i^{(\alpha)}]$  et  $[p_S^{(\alpha)}]$  représentent respectivement l'ensemble d'intervalles emboîtés des probabilités floues  $\tilde{p}_S$  et  $\tilde{p}_i$ .

La méthode des  $\alpha$ -coupes est très intéressante, mais elle nécessite une grande puissance de calcul [68]. Cette méthode présente un autre avantage, elle permet d'utiliser d'autres formes de probabilités floues (trapézoïdales, gaussiennes, ...) pour représenter les probabilités d'occurrences des événements de base [101], [104].

#### Exemple 2.1 :

Considérons un système dont l'arbre de défaillances est représenté par la figure 2.7. La méthode des  $\alpha$ -coupes proposée par Sallak [104] est appliquée pour calculer la probabilité floue d'occurrence de l'événement indésirable.

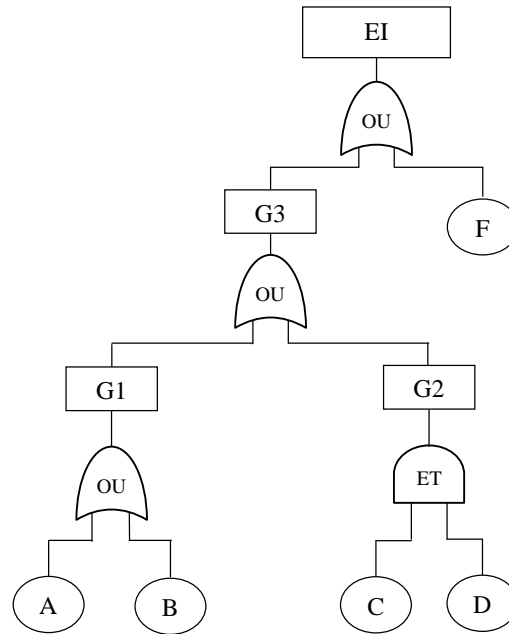


FIGURE 2.7 – Exemple d'arbre de défaillances

Les probabilités floues d'occurrence des événements de base sont des nombres flous  $\langle m_i, a_i, b_i \rangle_{L-R}$  du type  $L - R$  caractérisés par trois paramètres réels. Le tableau 2.3 présente les valeurs des trois paramètres  $m_i$ ,  $a_i$  et  $b_i$  pour chaque événement de base [101].

TABLE 2.3 – Paramètres des probabilités floues des événements de base

Événements de base	$\langle m_i, a_i, b_i \rangle_{LR}$
A	$\langle 0.009, 0.008, 0.0125 \rangle_{LR}$
B	$\langle 0.0035, 0.002, 0.005 \rangle_{LR}$
C	$\langle 0.0075, 0.005, 0.0095 \rangle_{LR}$
D	$\langle 0.0075, 0.005, 0.0095 \rangle_{LR}$
E	$\langle 0.007, 0.006, 0.0115 \rangle_{LR}$

L'approche de Sallak est appliquée pour déterminer la probabilité d'occurrence de l'événement indésirable (EI) de l'arbre de défaillances de la figure 2.7. La probabilité d'occurrence floue de l'évènement indésirable est donnée à la figure 2.8.

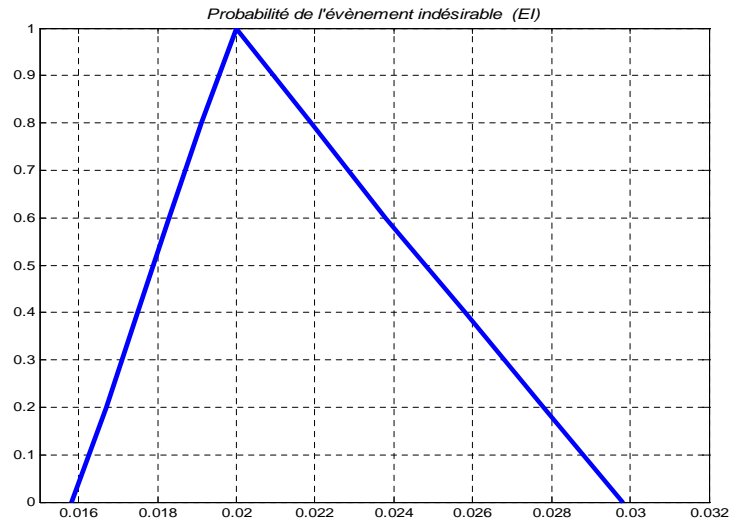


FIGURE 2.8 – Probabilité d'occurrence de l'évènement indésirable (EI)

L'analyse par arbre de défaillances est largement utilisée dans les études de fiabilité des systèmes car elle caractérise de façon claire les liens entre les composants d'un système [101]. Bien que cette méthode soit efficace, elle présente des limites. L'une de ses limites est que l'ordre d'occurrence des événements conduisant à l'évènement indésirable n'est pas pris en compte.

### Remarque

Dans le formalisme flou la méthode des  $\alpha$ -coupes est la plus utilisée, cependant il existe d'autres méthodes qui permettent de traiter les arbres de défaillance en présence des informations imparfaites [46]; [114]; [75].

## 2.4.2 Evaluation par les chaînes de Markov des systèmes à paramètres imprécis

Des nombreux travaux s'intéressent à l'étude du problème de l'imprécision dans les chaînes de Markov [70], [13], [22], [69], [122], [16], [116]. Il s'agit des méthodes intégrant les théories de représentation de l'imprécision sur les probabilités de transition des chaînes de Markov. Le problème de précision dans la connaissance des valeurs de probabilités de transition est traité de diverses manières. La modélisation de l'imprécision dans la connaissance des probabilités est traitée par Kozine sous forme d'intervalles [69], [116]. Le problème de précision est considéré, par d'autres auteurs [70], [13], [17], à l'aide des nombres flous.

Les premiers travaux d'analyse floue des chaînes de Markov appartiennent à Kruse [70]. Ces travaux présentent les chaînes de Markov floues comme une extension des chaînes

de Markov classiques basées sur des probabilités floues pour représenter les éléments des matrices de transition afin de calculer la puissance efficace d'un processeur. En 1998, Zadeh a proposé des algorithmes de Markov flous [138] utilisant des chaînes de Markov floues. Bhattacharyya [13] a prouvé par la suite que, si une chaîne de Markov est irréductible alors la chaîne de Markov floue qui lui est associée est également irréductible. Il a utilisé ce résultat pour étudier des processus décisionnels flous. Buckley en 2002 [17] a proposé une méthode connue sous le nom de multiplication restreinte des matrices floues basée sur la méthode des  $\alpha$ -coupes pour traiter les chaînes de Markov floues. En 2004, Symeonaki [120] a défini des conditions de convergence des chaînes de Markov non homogènes à états flous. En même temps, Tanrioven [122] a réalisé plusieurs applications des chaînes de Markov floues en se basant notamment sur les systèmes d'inférences et les probabilités de transitions floues [16].

### 2.4.2.1 Chaînes de Markov à probabilités de transitions floues

Les états que peut prendre un système, sont définis d'une manière claire et précise. Les probabilités des matrices de transition sont imprécises représentées par des nombres flous. Dans ce cas, il s'agit des chaînes de Markov à états non flous et à probabilités de transition floues [70], [13], [122], [16].

A tout instant  $n$ , l'état d'un système est complètement décrit par la distribution floue. La loi de transition de la chaîne de Markov floue est donnée par la relation floue suivante :

$$p_j^{(n+1)} = \max_{i \in S} \{p_i^{(n)} \wedge a_{ij}\}, \quad S_j \in S \quad (2.40)$$

$p^{(0)}$  désigne le vecteur d'état flou initial et  $S$  représente l'ensemble des états de la chaîne de Markov.

A partir de cette équation, les chaînes de Markov floues sont déterminées à partir des chaînes de Markov classiques en remplaçant les opérateurs " *produit* et *somme* " par les opérateurs '*min*' et '*max*', et les probabilités sont remplacés par des mesures de possibilités.

L'état flou  $S_k$  d'une chaîne de Markov peut être caractérisé à tout instant  $n$ , par la formule de récurrence :

$$p(S_j)^{(n)} = p_j^{(n)} = \max_{i \in S} \{p_i^{(0)} \wedge a_{ij}^n\}, \quad S_j \in S \quad (2.41)$$

où  $a_{ij}^n$  représente le terme de la matrice de transition floue  $A^n$ .

L'équation (2.41) peut s'écrire en utilisant la notation matricielle sous la forme [70], [2] :

$$p^{(n)} = p^{(0)} \circ A^n \quad (2.42)$$

L'opérateur  $\circ$  désigne la composition des deux opérateurs min et max, c'est à dire :

$$A \circ B = \max\{\min(A, B)\} \quad (2.43)$$

avec  $A$  et  $B$  deux matrices floues quelconques.

Dans le cas des chaînes de Markov classiques, les puissances des matrices de transition convergent vers une solution stationnaire quand  $n$  tend vers l'infini [2]. L'étude des chaînes de Markov floues montre que les puissances des matrices de transition à états non flous et probabilités de transition floues convergent en un nombre fini d'étapes.

#### 2.4.2.2 Méthode des $\alpha$ -coupes

Dans cette partie, une partie des  $a_{ij}$  est supposée imprécise, cette incertitude peut être modélisée en utilisant des nombres flous [17]. Ainsi, à chaque  $a_{ij}$  est associée une valeur floue  $\tilde{a}_{ij}$  et la matrice de transition floue  $\tilde{A}$ , est définie comme suit :

$$\tilde{A} = \begin{bmatrix} \tilde{a}_{11} & \tilde{a}_{12} & \dots\dots\dots & \tilde{a}_{1r} \\ \tilde{a}_{21} & \tilde{a}_{22} & \dots\dots\dots & \tilde{a}_{2r} \\ \cdot & \cdot & \dots\dots\dots & \cdot \\ \tilde{a}_{r1} & \tilde{a}_{r2} & \dots\dots\dots & \tilde{a}_{rr} \end{bmatrix} \quad (2.44)$$

où  $\tilde{a}_{ij}$  est la probabilité de transition floue de l'état  $S_i$  vers l'état  $S_j$ .

Les chaînes de Markov à états non flous et probabilités de transitions floues sont traitées aussi par une méthode proposée par Buckley [17] appelée multiplication restreinte des matrices floues. Les probabilités de transition de la matrice de la chaîne de Markov sont remplacées par des nombres flous et découpées en  $\alpha$ -coupes. Chaque  $\alpha$ -coupe d'une probabilité floue est utilisée pour calculer l' $\alpha$ -coupe correspondante à la matrice de transition de la chaîne de Markov ce qui permet de déterminer la probabilité floue d'être dans les différents états du système. La fonction d'appartenance de la probabilité floue des états de défaillances est construite à partir des  $\alpha$ -coupes calculées [16].

#### 2.4.2.3 Modèle de Markov avec un système d'inférence flou (MMF)

Les modèles de Markov basés sur les systèmes d'inférence flous peuvent être présentés, en se basant sur les travaux de Tanrioven [122].

La figure 2.9, illustre les différentes étapes qui permettent de construire le modèle de Markov flou.

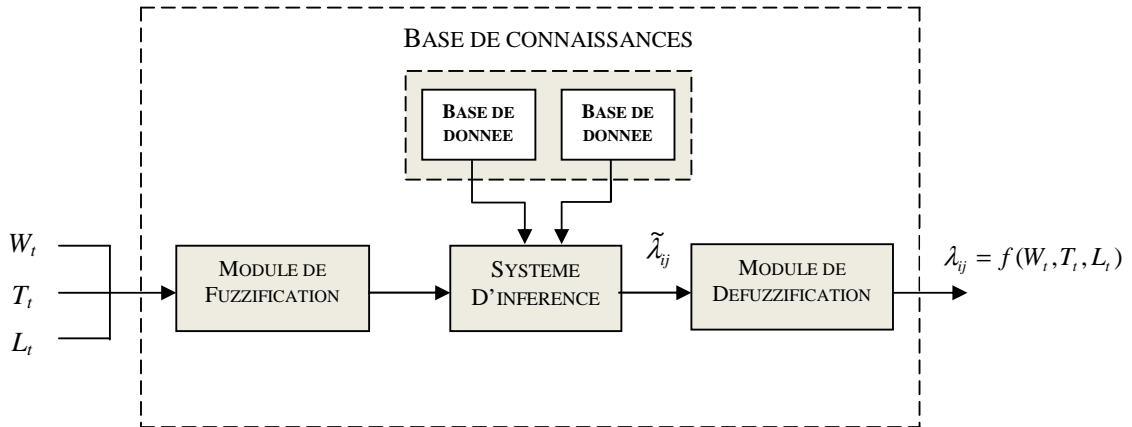


FIGURE 2.9 – Schéma général de construction de Modèle de Markov Flou

Le taux de transition  $\lambda_{ij}$  représente le taux de transition entre les états  $S_i$  et  $S_j$  (cf. figure 2.9). Il est en fonction des termes ;  $T_t, L_t$  et  $W_t$  :

$$\lambda_{ij} = f(T_t, L_t, W_t) \quad (2.45)$$

$T_t$  représente la température du système ;  $L_t$  représente le niveau de sollicitation du système et  $W_t$  désigne les conditions climatiques (climat normal, orageux, chaud, ...).

Pour l'obtention du modèle de Markov flou, les différentes étapes sont :

- Fuzzification : L'étape de fuzzification permet de définir les fonctions d'appartenance de toutes les variables des entrées, et le passage des grandeurs physiques aux variables linguistiques (nombres flous).
- Système d'inférence : Cette étape exprime la relation qui existe entre les variables d'entrées (exprimées comme variables linguistiques) et la variable de sortie (également exprimée comme variable linguistique). La base des règles fournies par les experts est appliquée sous forme de relations entre les variables linguistiques des paramètres des entrées et des sorties. La combinaison des différentes fonctions conduit à plusieurs méthodes d'inférences.
- Défuzzification : L'inférence fournit une fonction d'appartenance floue résultante pour la variable de sortie. La défuzzification consiste à transformer cette information floue en une valeur précise. On peut utiliser plusieurs méthodes de défuzzification. La plus utilisée est la méthode du centroïde qui permet de prendre le centre de masse de la fonction d'appartenance résultante de la sortie.
- Obtention des valeurs singulières pour la matrice des taux de transition  $A$ .

L'équation d'état du système est alors donnée par :

$$\frac{dp(t)}{dt} = A.p(t) \quad (2.46)$$

**Exemple 2.2** : Application de l'algorithme de Tanrioven [122].

Le système considéré est composé de cinq composants. Son digramme bloc de fiabilité est représenté à la figure 2.10. Cet exemple est utilisé comme support d'application du modèle de Markov avec système d'inférence flou [122].

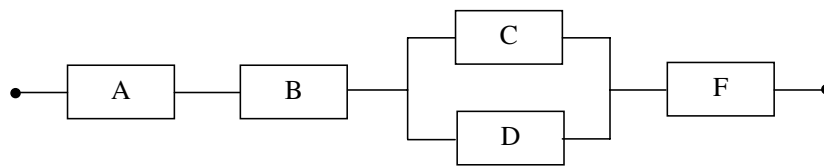


FIGURE 2.10 – Bloc diagramme de fiabilité de l'exemple

Le graphe de Markov de ce système est représenté à la figure 2.11. L'objectif est de calculer les performances de disponibilité en utilisant la méthode du modèle d'inférence flou proposée par Tanrioven [122].

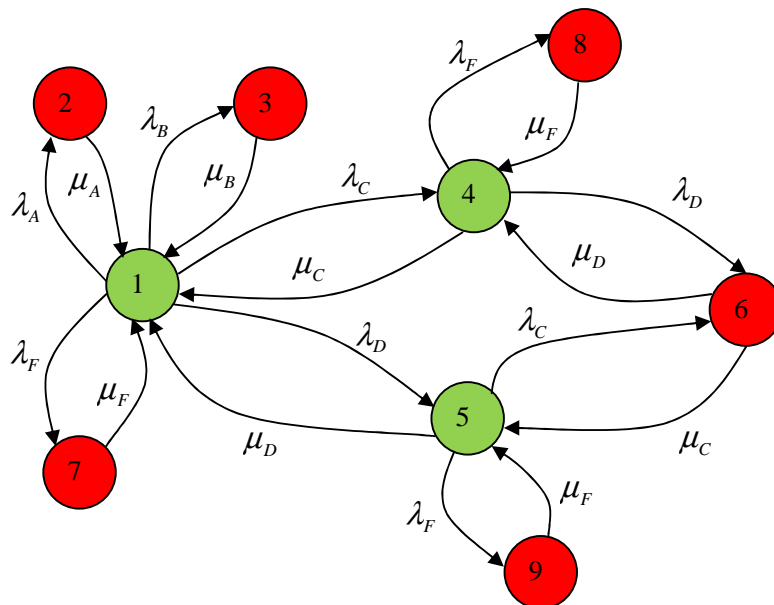


FIGURE 2.11 – Graphe de Markov du système

**a) Fuzzification**

La température est en fonction du climat suivant la saison. Elle peut être représentée par trois formes trapézoïdales : hiver, printemps/automne et été (cf. figure 2.12).

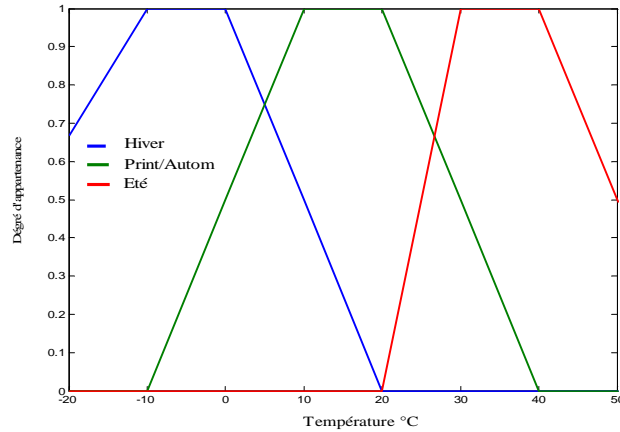


FIGURE 2.12 – La température  $T$  en fonction de la saison

Les taux des transitions sont représentés par trois formes triangulaires (cf. figure 2.13) :

- Petit ( $P$ ),
- Moyen ( $M$ ),
- Grand ( $G$ ).

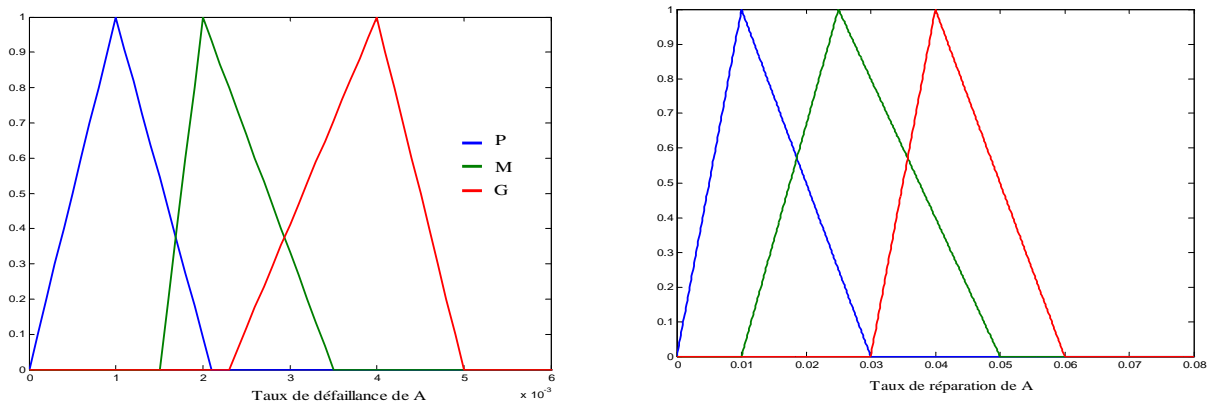


FIGURE 2.13 – Les taux de défaillance  $\lambda_A$  et de réparation  $\mu_A$

**b) Etape d'inférence**

Cette étape exprime la relation qui existe entre les variables d'entrées et les variables de sorties. La combinaison des différentes fonctions conduit à plusieurs méthodes d'inférences. Pour cet exemple la méthode utilisée est celle du Max-Min. Les résultats de cette étape sont donnés par le tableau 2.4.

TABLE 2.4 – Base des règles

Saison	taux de défaillance et de réparation					
	$\lambda_A$	$\mu_A$	.....	$\lambda_n$	$\mu_n$	
Print/Auto	$M_1$	$M_2$				
Eté	$P_1$	$G_2$				
Hiver	$G_1$	$P_2$				
.....			.....			
Print/Auto				$M_n$	$M_n$	
Eté				$P_n$	$G_n$	
Hiver				$G_1$	$P_2$	

Les méthodes d'inférence fournissent une fonction d'appartenance résultante pour la Variable de sortie.

**c) Etape de Défuzzification**

Il s'agit d'une information floue qu'il faut transformer en grandeur physique. Il existe plusieurs méthodes de défuzzification [122]. Dans cet exemple la méthode de centroïde est utilisée. La sortie correspond à l'abscisse du centre de gravité de la surface de la fonction d'appartenance résultante.

L'indisponibilité du système peut être déterminée en utilisant la l'équation d'état de la chaîne de Markov (cf. équation 2.46).

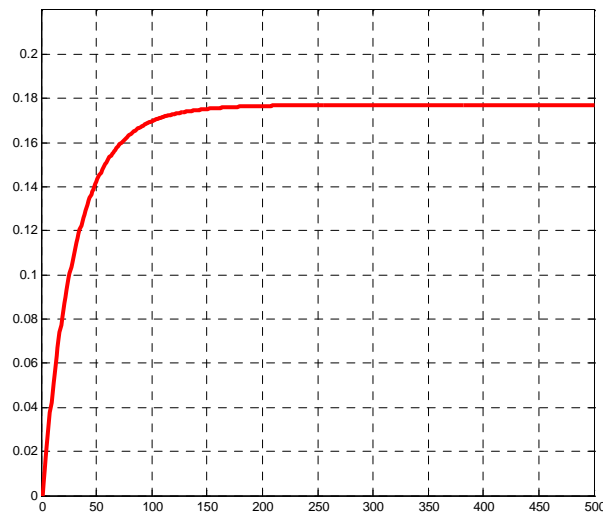


FIGURE 2.14 – L’indisponibilité du système en fonction de la température pour  $T=30^{\circ}\text{C}$

## 2.5 Conclusion

La représentation des informations imparfaites pour leur quantification peut se faire par l’utilisation de l’une des théories suivantes ; probabilités, intervalles, ensembles flous, familles des probabilités cumulées (p-boxes) . . .

Les méthodes d’évaluation développées se basent particulièrement sur l’arbre de défaillances (systèmes non réparables) et sur les chaînes de Markov (systèmes réparables).

L’évaluation des performances des systèmes à paramètres imprécis à partir de l’arbre de défaillances, peut se faire dans le formalisme flou selon la méthode de Singer ou la méthode des  $\alpha$ -coupe. Dans le cadre des systèmes réparables l’évaluation de leurs performances, à partir de leur modélisation par les chaînes de Markov, peut être obtenue par la méthode  $\alpha$ -coupe ou par l’utilisation du modèle de Markov avec système d’inférence flou.

# 3

## Contribution à l'évaluation par arbres de défaillances des performances des SIS à paramètres imprécis

### Sommaire

---

<b>3.1</b>	<b>Introduction</b>	<b>61</b>
<b>3.2</b>	<b>Paramètres de performance des SIS</b>	<b>61</b>
3.2.1	Défaillances de Causes Communes (DCC)	62
3.2.2	Les différents modèles des DCC	62
3.2.2.1	Modèle du facteur $\beta$	63
3.2.2.2	Méthode des lettres grecques multiples (MGL)	63
3.2.2.3	Méthode du facteur $\alpha$	63
3.2.2.4	Méthode PDS	64
3.2.3	Mise en œuvre du facteur $\beta$	64
<b>3.3</b>	<b>Eléments théoriques de l'approche d'évaluation probabiliste floue</b>	<b>67</b>
3.3.1	Nombres flous triangulaires	67
3.3.1.1	Probabilités floues	68
3.3.1.2	Intervalles flous	70
3.3.1.3	Facteurs de DCC flous	70
3.3.2	Proposition d'évaluation par arbres de défaillances flous	71
3.3.3	Application : Etude d'un HIPS	73
3.3.3.1	Proposition de l'évaluation de la $PFD_{avg}$ par une approche probabiliste floue	75

---

3.3.3.2	Validation de l'approche proposée par simulation de Monte Carlo . . . . .	79
3.3.3.3	Importance des sources d'informations . . . . .	82
3.3.4	Conclusion partielle . . . . .	84
<b>3.4</b>	<b>Evaluation des performances des SIS à l'aide des P-boxes . .</b>	<b>84</b>
3.4.1	Les P-boxes . . . . .	85
3.4.2	Modélisation de l'imprécision des DCC à l'aide des P-boxes . .	87
3.4.2.1	Evaluation imprécise de la $PFD_{avg}$ . . . . .	88
<b>3.5</b>	<b>Conclusion . . . . .</b>	<b>91</b>

---

## 3.1 Introduction

Dans ce chapitre, deux approches probabilistes d'évaluation sont proposées. La première approche d'évaluation se base sur l'utilisation des nombres flous, pour représenter l'incertitude des facteurs de défaillance de cause commune (DCC). On montre la validité des résultats de cette approche en les comparant à ceux déterminés par l'approche aléatoire, tirage de Monte Carlo. La seconde approche s'intéresse à étendre les calculs à une représentation plus générale de l'imprécision (p-boxes) et à intégrer la modélisation des paramètres par des familles de probabilités (p-boxes) dans les arbres de défaillances. Ces deux approches sont utilisées pour l'évaluation imprécise des performances des SIS. Une application support est proposée afin de montrer l'intérêt des approches proposées pour l'évaluation de la  $PF D_{avg}$  en présence d'informations imparfaites.

La dernière partie s'intéresse à la modélisation de l'imprécision du facteur de DCC à l'aide des familles de probabilités (p-boxes). On montre comment l'imprécision de ce paramètre est modélisée et propagée dans un arbre de défaillances, ce qui induit une incertitude sur la probabilité de défaillance à la sollicitation des SIS et ainsi l'intérêt pour le décideur de connaître l'imprécision sur le paramètre de performance.

## 3.2 Paramètres de performance des SIS

On s'intéresse uniquement aux SIS faiblement sollicitée d'où le besoin d'évaluer leurs  $PF D$ . Dans ce cas, la  $PF D$  instantanée n'est que l'indisponibilité instantanée de la fonction de sécurité du SIS étudié. C'est pourquoi on utilise les paramètres caractéristiques de défaillance des composants, tels que le taux de défaillance, et le facteur des DCC. Ces paramètres peuvent être introduits de façon directe dans les calculs de probabilité de défaillance des SIS.

La  $PF D_{avg}$ , est calculée lorsque la fonction de sécurité est faiblement sollicitée. Elle est égale à l'indisponibilité moyenne calculée sur la durée de mission  $T$  ou éventuellement sur l'intervalle de test  $[0, T_i]$ .

Dans le calcul de la performance, on fait l'hypothèse que toute l'information sur le comportement du système et de ses composants est disponible. En outre, ce calcul se base sur les hypothèses suivantes :

1. L'évaluation probabiliste des boucles de sécurité s'applique à des composants ayant des défaillances aléatoires et modélisées par une distribution exponentielle [72].
2. Les taux de défaillance sont présumés être constants et indépendants du temps.
3. Le système est cohérent.

Le calcul de la  $PF D_{avg}$  fait intervenir le taux de défaillance des composants et le facteur de DCC. Les défaillances de mode commun peuvent être introduites dans les calculs de probabilité de défaillance de façon directe. Les paramètres de calcul sont évalués à partir

des données issues du retour d'expérience ou de données constructeurs. Les valeurs des facteurs de DCC étant difficiles à obtenir des modèles paramétriques ont été développés à cet effet.

### 3.2.1 Défaillances de Causes Communes (DCC)

La probabilité de défaillance du SIS est déterminée par le calcul et la combinaison des probabilités de défaillances de ses composants. Ces probabilités dépendent des paramètres de sûreté des composants tels que le taux de défaillance et aussi du facteur qui caractérise les DCC.

#### Définition 3.1

Lilleheier [73] considère que les défaillances de cause commune (DCC) constituent un sous-ensemble de l'ensemble des défaillances dépendantes. Mosleh [91] en a proposé une définition très explicite : *"Ensemble d'événements dépendants affectant deux composants ou plus, au même moment ou dans un petit intervalle de temps et résultant directement d'une cause partagée"*.

#### Classifications de DCC

De manière pratique, les fiabilistes utilisent une classification basée sur des causes génériques pour analyser ce type de défaillance des systèmes importants pour la sûreté des centrales nucléaires [95]. Ils considèrent que les défaillances qui affectent les composants d'un système résultent soit d'agressions externes, soit d'erreurs humaines commises à la conception, à la fabrication ou bien en exploitation. Les défaillances peuvent être divisées, selon la nature de leurs causes, en quatre grandes classes :

- Les agressions de l'environnement : événements liés à l'environnement externe ou interne à l'installation mais extérieurs au système élémentaire considéré.
- Les erreurs de conception : erreurs commises au cours des études des composants et du système élémentaire qui compromettent ses missions.
- Les erreurs de fabrication : erreurs commises au cours de la fabrication des composants et du système élémentaire.
- Les erreurs d'exploitation : erreurs commises au cours de l'exploitation des composants et du système élémentaire reconnus aptes à fonctionner auparavant.

### 3.2.2 Les différents modèles des DCC

Les défaillances de mode commun peuvent être introduites dans l'évaluation des performances des systèmes de sécurité [15], [74]. Les paramètres de calcul peuvent être déterminés à partir de données issues du retour d'expérience [52], [119], [49]. Étant donné la difficulté à obtenir de telles données, des méthodes paramétriques de modélisation et de

quantification des DCC ont été développées, tels que ; le modèle du facteur  $\beta$ , [41] ; [73], la méthode PDS [47], La méthodes des lettres grecques multiples (MGL) [49], ou bien le modèle du facteur  $\alpha$  [91].

### 3.2.2.1 Modèle du facteur $\beta$

Cette méthode a été introduite par Fleming [41]. C'est probablement le modèle le plus répandu pour traiter les DCC. La principale raison de son succès est son extrême simplicité d'utilisation [96]. Bien qu'elle puisse servir à modéliser des dépendances entre des équipements différents et non nécessairement redondants, dans la pratique, elle est le plus souvent appliquée aux systèmes redondants formés de composants identiques.

Cette méthode considère les possibilités suivantes :

- un seul composant tombe en panne du fait d'une défaillance indépendante,
- tous les composants du groupe de DCC tombent en panne simultanément, avec une seule et même cause de défaillance.

Le facteur  $\beta$  caractérisant une défaillance en fonctionnement peut ne pas être le même que celui relatif à une défaillance à la sollicitation pour le même groupe de composants. Le paramètre  $\beta$  est défini comme étant égal au pourcentage de défaillances résultant d'une cause commune [96].

### 3.2.2.2 Méthode des lettres grecques multiples (MGL)

Cette méthode est une extension du modèle du facteur  $\beta$  lorsque l'on considère plusieurs composants en redondance. Des paramètres supplémentaires sont ajoutés au facteur  $\beta$  pour traiter des niveaux élevés de redondance [41]. La probabilité totale de défaillance tient compte de l'effet de toutes les contributions indépendantes et de causes communes des différents composants. Les probabilités conditionnelles des défaillances de mode commun qu'un composant peut partager avec les composants d'un groupe de cause commune sont aussi considérées.

Les paramètres de cette méthode, sont constitués par :

- des taux de défaillance des composants qui tiennent compte des contributions des causes indépendantes et communes,
- des probabilités conditionnelles.

### 3.2.2.3 Méthode du facteur $\alpha$

La méthode du facteur  $\alpha$  constitue une amélioration par rapport à la méthode MGL, car les paramètres peuvent être estimés à partir de statistiques d'événements observés et plus particulièrement à partir des données sur les défaillances du système et non des composants [91].

L'estimation des paramètres de la méthode du facteur  $\alpha$ , est assez difficile à obtenir malgré l'existence et l'utilisation de méthodes d'approximations. L'estimation de ces paramètres peut être obtenue en introduisant un paramètre intermédiaire basé sur les événements des défaillances de cause commune qui est plus facile à estimer à partir des données observées plutôt qu'à partir des défaillances du système. Cette estimation est à la base du modèle du facteur  $\alpha$  [91], [127].

#### 3.2.2.4 Méthode PDS

La méthode PDS a initialement été développée dans l'industrie pétrolière [47]. PDS est un acronyme norvégien pour la *fiabilité et la disponibilité des systèmes gérés par informatique* [74]. Contrairement au modèle du facteur  $\beta$ , la méthode PDS cherche à modéliser les causes communes de défaillance partielles, ce qui a pour conséquence d'adapter la probabilité de cause commune en fonction de l'architecture du système [47].

Un nouveau paramètre est alors introduit, noté  $\beta_k$ , qui est la probabilité d'une défaillance additionnelle d'un composant  $i$  spécifique, sachant que  $k$  composants sont défaillants ( $k$  n'inclut pas le composant  $i$ ).

#### 3.2.3 Mise en œuvre du facteur $\beta$

Le modèle du facteur  $\beta$  utilisé est le modèle le plus répandu pour introduire les défaillances de mode commun dans les analyses de fiabilité [3], [50], [52], [73], [96] et pour calculer la part de ces défaillances sur la probabilité de défaillance d'un système [73], [15].

Le modèle du facteur  $\beta$  est utilisé pour la modélisation des causes communes de défaillance [41], [3], [15], [73]. L'hypothèse principale du modèle du facteur  $\beta$  est que chaque composant  $i$  du système (avec  $i = 1, \dots, N$ ) peut être défaillant à cause de :

- circonstances n'ayant eu un effet que sur le composant en question. Le taux des défaillances correspondantes, dites " *indépendantes* ", est noté  $\lambda_i^{(i)}$ .
- l'occurrence d'un événement qui a provoqué la défaillance des  $N$  composants du système simultanément. Le taux des défaillances correspondantes, dites " *de cause commune* ", est noté  $\lambda_i^{(ccf)}$ .

Le taux de défaillance total de chaque composant  $i$  du système (avec  $i = 1, \dots, N$ ), noté  $\lambda_i$ , est alors :

$$\lambda_i = \lambda_i^{(i)} + \lambda_i^{(ccf)} \quad (3.1)$$

Le facteur  $\beta$  de DCC est défini comme la probabilité d'une DCC sachant la présence d'une défaillance. Le facteur  $\beta$  est déterminé comme suit :

$$\beta = \frac{\lambda_i^{(ccf)}}{\lambda_i^{(ccf)} + \lambda_i^{(i)}} = \frac{\lambda_i^{(ccf)}}{\lambda_i} \quad (3.2)$$

Le facteur  $\beta$  est défini comme étant égal au pourcentage de défaillances résultant d'une cause commune. La quantification de  $\lambda_i^{(ccf)}$  est assez délicate à réaliser. C'est en général une valeur estimée. Le choix de  $\beta$  induit donc les valeurs de  $\lambda_i^{(i)}$  et  $\lambda_i^{(ccf)}$  :

$$\lambda_i^{(i)} = (1 - \beta) \cdot \lambda_i \quad \text{et} \quad \lambda_i^{(ccf)} = \beta \cdot \lambda_i \quad (3.3)$$

Pour évaluer la performance des SIS, un arbre de défaillances peut être utilisée pour modéliser les événements de base du SIS tout en tenant compte des différents types de défaillances et des DCC [51], [77], [87].

La DCC est caractéristique d'un ensemble d'événements qui provoquent la défaillance concomitante de tous les composants d'un système ou d'un sous-système sur lesquels la cause peut avoir un effet [74], [15]. Cette cause commune n'a de sens que si au minimum deux composants sont concernés.

### Exemple 3.1 : Un système exposé à la DCC

On considère une couche d'un SIS composé de deux machines en parallèle exposées à la DCC. Une DCC peut être considérée sur cette couche. La DCC peut être matérialisée comme un composant en série avec les composants redondants [73] comme le montre la figure 3.1.

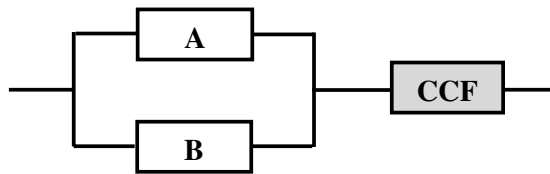


FIGURE 3.1 – Machines A et B en parallèle exposé à la DCC

La cause commune peut être introduite dans le calcul de la probabilité de défaillance  $P(t)$ . On caractérise la probabilité indépendante de défaillance, notée  $P^i(t)$  et la probabilité de DCC, notée  $P^{ccf}(t)$ .

Dans le cas de la figure 3.1, les deux composants d'une couche d'un SIS  $A$  et  $B$  sont identiques, placés en redondance. L'arbre de défaillances du système précédant est donné par la figure 3.2.

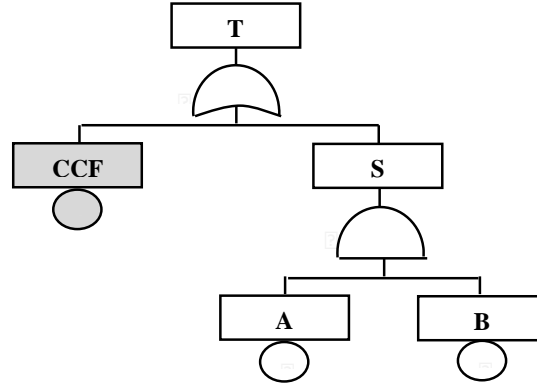


FIGURE 3.2 – Arbre de défaillances du système exposé à la DCC

$P^i(t)$  s'exprime en fonction de l'architecture du système et avec les taux  $\lambda^i$  des défaillances indépendantes des composants.

$$P^i(t) = P_A(t).P_B(t) \quad (3.4)$$

$$P^i(t) = (1 - e^{-\lambda^{(i)}.t})^2 = (1 - e^{-(1-\beta).\lambda.t})^2 \quad (3.5)$$

D'après le modèle du facteur  $\beta$ , une DCC provoque la défaillance de tous les composants du système.  $P^{(ccf)}(t)$  s'exprime selon une architecture 1oo1, quelque soit l'architecture du système, et en fonction du taux des DCC  $\lambda^{(ccf)}$ .

$$P^{(ccf)}(t) = 1 - e^{-\lambda^{(ccf)}.t} = 1 - e^{-\beta.\lambda.t} \quad (3.6)$$

La probabilité d'occurrence de l'événement sommet de l'arbre est donnée par :

$$P_T(t) = 1 - (1 - P^i(t)).(1 - P^{(ccf)}(t)) \quad (3.7)$$

L'exemple précédant peut être étendue à l'ensemble des couches du SIS, l'arbre de défaillances permet l'établissement de la relation logique entre l'état du système et celui de ses composants. Le calcul de la  $PF D_{avg}$  du SIS est alors immédiat. Cette méthode permet de déterminer la  $PF D_{avg}$  du SIS et calculer la performance moyenne par intégration dans le temps de la probabilité d'occurrence de l'évènement indésirable.

Dans certains cas, les données de fiabilité (par exemple le taux de défaillance  $\lambda$ ) trouvées dans la littérature ou dans les bases de données des constructeurs ne sont pas des valeurs précises. Ce problème se pose, en particulier, pour les SIS faiblement sollicités, le retour d'expérience est faible. En effet, ceux-ci présentent des défaillances très rares ne

permettant pas de valider statistiquement les calculs prévisionnels à partir des paramètres de défaillance de leurs composants. Il est donc intéressant de proposer d'autres approches pour analyser les arbres de défaillances en présence de données de fiabilité imparfaites .

Les experts fiabilistes peuvent dans certains cas fournir plus d'informations qu'un simple intervalle. Ils peuvent par exemple fournir une série d'intervalles emboîtés liés au niveau de confiance  $\alpha$  qu'ils ont sur chaque intervalle de valeurs fournies. Il s'agit en fait d'un nombre flou au sens de Zadeh [136]. L'expert fiabiliste peut éventuellement préciser le nombre flou directement sous une forme linguistique. Dans ce cas, les limites extérieures des intervalles emboîtés indicés par les niveaux  $\alpha$  peuvent être reliées à l'aide d'une interpolation linéaire. Il s'agit d'une extrapolation de connaissance minimale si on doit combiner avec finesse des nombres flous à des niveaux de confiance différents.

### 3.3 Éléments théoriques de l'approche d'évaluation probabiliste floue

L'approche proposée s'appuie sur les travaux de Sallak [104] et ceux de Buckley [16] pour traiter le problème de l'incertitude dans l'évaluation de la  $PFD_{avg}$  des SIS. Le premier défi est de propager l'incertitude sans faire l'hypothèse des événements rares et le deuxième est de réduire l'imprécision des résultats, due aux événements répétés, en employant l'arithmétique floue contrainte proposée par Buckley [16]. nous traitons le problème d'imprécision sur la connaissance de la valeur du facteur de DCC. Le manque de connaissance est exprimé par des nombres flous de type trinagulaire.

L'approche peut être étendue à d'autre forme de nombres flous (trapézoïdale, rectangulaire,...). Les arbres de défaillances flous sont utilisés pour évaluer la  $PFD_{avg}$  et le niveau SIL du SIS. Les fonctions d'appartenance représentant les probabilités floues des événements de base sont découpées en  $\alpha$ -coupes [68]. Chaque  $\alpha$ -coupe d'une probabilité floue d'un événement de base est utilisée pour calculer l' $\alpha$ -coupe de la probabilité de l'événement indésirable résultante qui représente la probabilité floue de défaillance du SIS lors de sa sollicitation. La fonction d'appartenance de la probabilité floue de l'événement indésirable est déterminée à partir des  $\alpha$ -coupes calculées [101].

#### 3.3.1 Nombres flous triangulaires

Pour un composant dont le paramètre de défaillance est obtenu à partir d'une base de données de fiabilité, l'expert fiabiliste peut éventuellement préciser le nombre flou directement à partir des bornes minimale, maximale et la valeur modale  $m$ . Le taux de défaillance du composant est d'environ  $m$  défaillances /an prés.

Dans ce cas, l'information sur le facteur de DCC est incertaine. Cette information est considérée comme une imprécision qui sera estimée par expert et représentée par exemple, sous forme d'un nombre flou de valeur modale  $m$ .

Bien qu'un nombre flou puisse avoir des formes très variées, dans ce travail, on ne manipule que les nombres flous de type triangulaire. L'intérêt de cette représentation est double. D'une part, il s'agit d'une représentation conforme à l'expression linguistique 'environ', d'autre part, le nombre flou triangulaire joue le rôle de la distribution uniforme dans le domaine des probabilités [26].

L'avantage d'utiliser une forme triangulaire pour modéliser les paramètres de défaillance réside dans le fait qu'elle est la forme de représentation la plus adéquate au sens de l'engagement minimum, elle joue le rôle de la loi normale [26]. Un autre avantage inhérent aux nombres flous triangulaires est la facilité d'utilisation grâce à la simplification des opérations arithmétiques floues [68].

La fonction d'appartenance d'un nombre flou triangulaire  $\tilde{\beta}_i$  est donnée ci après :

$$\mu(\tilde{\beta}_i) = \begin{cases} 0 & \text{si } \beta_i < a_i \\ \frac{\beta_i - a_i}{m_i - a_i} & \text{si } a_i \leq \beta_i \leq m_i \\ \frac{b_i - \beta_i}{b_i - m_i} & \text{si } m_i \leq \beta_i \leq b_i \\ 0 & \text{si } \beta_i > b_i \end{cases} \quad (3.8)$$

Les nombres flous triangulaires modélisés par l'équation (3.8), sont caractérisés par trois paramètres  $m_i$ ,  $a_i$  et  $b_i$  (qui sont donnés par les experts),  $m_i$  représente la valeur modale de la fonction d'appartenance. Elle représente la valeur la plus probable du facteur de défaillance ( $\mu(m_i) = 1$ );  $a_i$  est la limite à gauche de  $m_i$ , et  $b_i$  est la limite à droite de  $m_i$ .

### 3.3.1.1 Probabilités floues

Une probabilité floue est un ensemble flou défini dans l'espace des probabilités. Elle représente un nombre flou entre 0 et 1 qui est affecté à la probabilité d'occurrence d'un événement. La prise en compte de l'imprécision par des probabilités floues peut-être résolue par le principe d'extension de Zadeh [136].

Soit  $y = f(p_1, p_2, \dots, p_n)$  une fonction déterministe qui associe une variable numérique de sortie  $y$  à  $n$  variables numériques d'entrée, combinées entre elles par des opérateurs algébriques classiques (ex : +, -, ×, ÷). Le principe d'extension de Zadeh consiste à considérer chacune des variables d'entrée comme un nombre flou ( $\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_n$ ) et à les combiner entre elles par une extension max-min des opérateurs algébriques classiques.

Si  $\tilde{B}$  est l'image par une fonction  $f$  des sous-ensembles flous ( $\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_n$ ), alors la

fonction d'appartenance de  $\tilde{B}$  est donnée par :

$$\mu_{\tilde{B}}(y) = \sup_{(p_1, p_2, \dots, p_n)} \{ \{ \min \{ f(\mu_{\tilde{A}_1}(p_1), \mu_{\tilde{A}_2}(p_2), \dots, \mu_{\tilde{A}_n}(p_n)) \} \} \} \quad (3.9)$$

La formulation 3.9 est très consommatrice en temps de calcul. Il est possible de combiner la notion d' $\alpha$  coupe et le calcul d'intervalles [90] pour obtenir le même résultat que le principe d'extension de Zadeh avec les opérateurs algébriques précédemment cités (voir section 2.2.3.4) [16].

Une probabilité floue  $\tilde{p}_X$  peut être caractérisée par une fonction d'appartenance de type triangulaire, par un ensemble d'intervalles de confiance à un certain niveau  $\alpha$ . On obtient ainsi, plusieurs intervalles emboîtés en utilisant la méthode des  $\alpha$ -coupes.

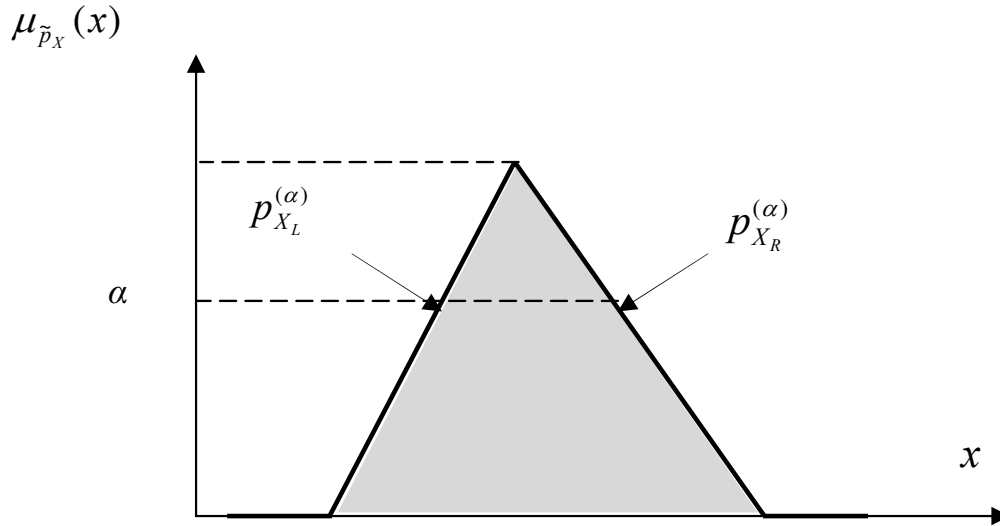


FIGURE 3.3 –  $\alpha$ -coupes d'une probabilité floue  $\tilde{p}_X$

A partir de la figure 3.3, une probabilité floue peut être représentée en utilisant l'expression suivante :

$$\tilde{p}_X \rightarrow [p_X^{(\alpha)}] = [p_{X_L}^{(\alpha)}, p_{X_R}^{(\alpha)}], 0 \leq \alpha \leq 1 \quad (3.10)$$

$p_{X_L}^{(\alpha)}$  et  $p_{X_R}^{(\alpha)}$  représentent respectivement les limites gauche et droite de la fonction d'appartenance  $\mu_{\tilde{p}_X}(x)$  à chaque  $\alpha$ -coupe.

### 3.3.1.2 Intervalles flous

Lorsque l'on utilise des intervalles pour modéliser l'incertitude, la répétition d'une même variable dans une expression revient à comptabiliser plusieurs fois l'imprécision sur cette variable dans le résultat final. Le calcul d'intervalles étant sous distributif, le résultat d'un calcul est bien plus imprécis qu'il ne pourrait l'être [90]. Buckley a précisé dans [16] que si  $f$  était monotone alors le calcul de l'intervalle de sortie peut être mené en choisissant de manière adéquate les bornes des entrées  $p_i$  [16].

Soit  $y = f(p_1, p_2, \dots, p_n)$ , où chaque  $p_i$  varie dans l'intervalle  $[p_{iL}^{(\alpha)}, p_{iR}^{(\alpha)}]$ . Si les conditions suivantes sont vérifiées [87] :

- $f$  est localement monotone par rapport à chaque argument .Une fonction dérivable est localement monotone par rapport à  $p_i$  si le signe de sa dérivée  $\frac{\partial f}{\partial p_i}$  ne dépend pas de  $p_i$ . Le signe de la dérivée est alors constant et la restriction est donc monotone.
- $\forall j \in E_1$ ,  $f$  est croissante par rapport à  $p_j$ .
- $\forall j \in E_2$ ,  $f$  est décroissante par rapport à  $p_j$ .

$E_1$  et  $E_2$  sont deux ensembles disjoints, mais ne forment pas nécessairement une partition de  $\{1, \dots, n\}$ .

Il vient  $y^{(\alpha)} = [y_L^{(\alpha)}, y_R^{(\alpha)}]$

$$y_L^{(\alpha)} = \min \begin{cases} f(w) | \forall j \in E_1, w_j = p_{jL}^{(\alpha)} \\ f(w) | \forall j \in E_2, w_j = p_{jR}^{(\alpha)} \end{cases} \quad (3.11)$$

$$y_R^{(\alpha)} = \max \begin{cases} f(w) | \forall j \in E_1, w_j = p_{jR}^{(\alpha)} \\ f(w) | \forall j \in E_2, w_j = p_{jL}^{(\alpha)} \end{cases} \quad (3.12)$$

Le choix des bornes sur les intervalles d'entrée est fait suivant le signe de la dérivée partielle de la fonction de sortie  $y$  par rapport aux variables d'entrée  $p_i$  (suivant le signe  $\frac{\partial f}{\partial p_i}$ ), de manière à obtenir en sortie l'intervalle le plus petit garantissant que les valeurs réelles seront à l'intérieur de cet intervalle [16]. Par ailleurs, la monotonie de la fonction  $f$  permet de garantir la monotonie de l'inclusion [26].

### 3.3.1.3 Facteurs de DCC flous

Généralement la connaissance des valeurs des facteurs  $\beta$  des DCC, est imparfaite. Ces facteurs peuvent être modélisés par des nombres flous  $\tilde{\beta}$  de type triangulaire (cf.figure 3.3) [87].

Chaque facteur de DCC flou  $\tilde{\beta}_i$  peut être décrit par l'ensemble de ses  $\alpha$ -coupes comme l'indique l'équation (3.10). L'intervalle  $[\beta^{(\alpha)}]$  est l'ensemble disjoint des valeurs que peut prendre  $\beta$  avec un niveau de confiance  $(1 - \alpha)$ .  $[\beta^{(\alpha)}]$  est un intervalle borné par les deux valeurs  $[\beta_L^{(\alpha)}, \beta_R^{(\alpha)}]$ .

D'après les équations 3.3, 3.11 et 3.12, les différents taux de défaillance s'écrivent :

$$\tilde{\lambda}_i^{(i)} = (1 - \tilde{\beta}) \cdot \lambda_i \rightarrow [\lambda_{i_L}^{(i),(\alpha)}, \lambda_{i_R}^{(i),(\alpha)}] = [(1 - \beta_R^{(\alpha)}) \cdot \lambda_i, (1 - \beta_L^{(\alpha)}) \cdot \lambda_i] \quad (3.13)$$

$$\tilde{\lambda}_i^{(ccf)} = \tilde{\beta} \cdot \lambda_i \rightarrow [\lambda_{i_L}^{(ccf),(\alpha)}, \lambda_{i_R}^{(ccf),(\alpha)}] = [\beta_L^{(\alpha)} \cdot \lambda_i, \beta_R^{(\alpha)} \cdot \lambda_i] \quad (3.14)$$

$\tilde{\lambda}_i$  : Le taux de défaillance du  $i^{me}$  composant, représenté par un nombre flou singulier, une valeur précise généralement fournie par le constructeur mais qui pourrait être étendue à des nombres flous non singuliers.

### 3.3.2 Proposition d'évaluation par arbres de défaillances flous

L'analyse des arbres de défaillances conventionnelles est basée sur l'approche probabiliste. La probabilité d'occurrence de l'événement indésirable (probabilité de défaillance du système complet) est calculée à partir des probabilités d'occurrence des événements de base (probabilités de défaillance des composants du système). Les probabilités de défaillance des composants sont calculées à partir de leurs paramètres de défaillance.

Nous proposons, pour les probabilités d'occurrences des événements de base incertaines, l'utilisation des probabilités de défaillances floues au lieu d'utiliser des valeurs de probabilités singulières. Ainsi, à chaque probabilité de défaillance d'un événement de base de l'arbre, nous attribuons un degré d'incertitude. La distribution de la probabilité de défaillance du système  $P_S$  est calculée à partir des distributions des probabilités de défaillances  $P_i$  de ses composants.

La probabilité d'occurrence floue de l'événement sommet d'une association des portes "ET" est donnée par :

$$\tilde{P}_S(t) = \prod_{i=1}^n \tilde{P}_i(t) \quad (3.15)$$

$\tilde{P}_i(t)$  la probabilité d'occurrence floue du  $i^{me}$  composant et  $\tilde{P}_S(t)$  la probabilité d'occurrence floue de l'événement sommet.

L'approche floue proposée et la méthode des  $\alpha$ -coupes sont utilisées pour calculer les bornes inférieure et supérieure de la probabilité de l'événement indésirable. Chaque

probabilité floue  $\tilde{P}_i(t)$  d'un évènement de base  $i$  est décrite par l'ensemble d'intervalles pour tout  $\alpha \in [0, 1]$  (cf. équations (3.10)).

Sachant que  $\partial P_S / \partial P_i > 0$ , en appliquant les équations (3.11) et (3.12), la probabilité d'occurrence floue  $\tilde{P}_S(t)$  de l'évènement sommet peut être déterminée comme suit :

$$\tilde{P}_S(t) \Rightarrow [P_{S_L}^{(\alpha)}(t), P_{S_R}^{(\alpha)}(t)] = \left[ \prod_{i=1}^n P_i(t)_L^{(\alpha)}, \prod_{i=1}^n P_i(t)_R^{(\alpha)} \right] \quad (3.16)$$

De la même façon nous déterminons la probabilité d'occurrence floue de l'évènement sommet d'une association des portes " OU " :

$$\tilde{P}_S(t) = 1 - \prod_{i=1}^n (1 - \tilde{P}_i(t)) \quad (3.17)$$

Sachant que  $\partial P_S / \partial P_i > 0$

$$\tilde{P}_S(t) \Rightarrow [P_{S_L}^{(\alpha)}(t), P_{S_R}^{(\alpha)}(t)] = \left[ 1 - \prod_{i=1}^n (1 - P_i(t)_L^{(\alpha)}), 1 - \prod_{i=1}^n (1 - P_i(t)_R^{(\alpha)}) \right] \quad (3.18)$$

Dans l'arbre représenté à la figure 3.2, l'approche proposée est utilisée pour calculer la valeur de la probabilité d'occurrence floue de l'évènement indésirable, en utilisant les expressions de  $\tilde{P}^{(ccf)}$  et de  $\tilde{P}^{(i)}$ .

Soit  $\tilde{y} = \tilde{P}_T = f(\tilde{P}_i^{(i)}, \tilde{P}_i^{(ccf)})$ , l'approche proposée est utilisée pour déterminer les bornes inférieure et supérieure de  $\tilde{y}$ , en utilisant les équations (3.11) et (3.12) appliquées à (3.6).

Sachant  $\partial y / \partial P_i^{(i)} > 0$  et  $\partial y / \partial P_i^{(ccf)} > 0$ , les intervalles de la probabilité floue d'occurrence résultante de l'évènement sommet du système, peuvent être déterminés comme suit [87] :

$$\tilde{y} \Rightarrow [y_L^{(\alpha)}, y_R^{(\alpha)}]$$

$$\text{avec } \begin{cases} P_{T_L}^{(\alpha)}(t) = 1 - (1 - P_L^{(\alpha),(i)}(t)) \cdot (1 - P_L^{(\alpha),(ccf)}(t)) \\ P_{T_R}^{(\alpha)}(t) = 1 - (1 - P_R^{(\alpha),(i)}(t)) \cdot (1 - P_R^{(\alpha),(ccf)}(t)) \end{cases} \quad (3.19)$$

En utilisant le nombre flou de la figure 3.3 sur l'arbre de défaillances de la figure 3.2, les bornes inférieure et supérieure des  $\tilde{P}^{(i)}$  et  $\tilde{P}^{(ccf)}$  sont données en réécrivant les

équations (3.5) et (3.6) à partir des équations (3.11) et (3.12). Sachant que  $\partial P^{(i)}/\partial\beta < 0$  et  $\partial P^{(ccf)}/\partial\beta > 0$  :

$$\tilde{P}^{(ccf)}(t) \Rightarrow [P_L^{(\alpha),(ccf)}(t), P_R^{(\alpha),(ccf)}(t)] = [1 - e^{-\beta_L^{(\alpha)} \cdot \lambda \cdot t}, 1 - e^{-\beta_R^{(\alpha)} \cdot \lambda \cdot t}] \quad (3.20)$$

$$\tilde{P}^{(i)}(t) \Rightarrow [P_L^{(\alpha),(i)}(t), P_R^{(\alpha),(i)}(t)] = [(1 - e^{-(1-\beta_R^{(\alpha)}) \cdot \lambda \cdot t})^2, (1 - e^{-(1-\beta_L^{(\alpha)}) \cdot \lambda \cdot t})^2] \quad (3.21)$$

La démarche d'analyse menée sur une seule couche d'un SIS et conduisant aux équations (3.19) - (3.21) peut être étendue à l'ensemble des couches du SIS à l'arbre de défaillances complet des SIS.

### 3.3.3 Application : Etude d'un HIPS

Le système présenté à la figure 3.4 a été proposé, [110], pour évaluer son  $PF D_{avg}$  dans le cas où les paramètres caractéristiques sont précis. Ce système est utilisé ici comme exemple d'application pour illustrer l'approche proposée.

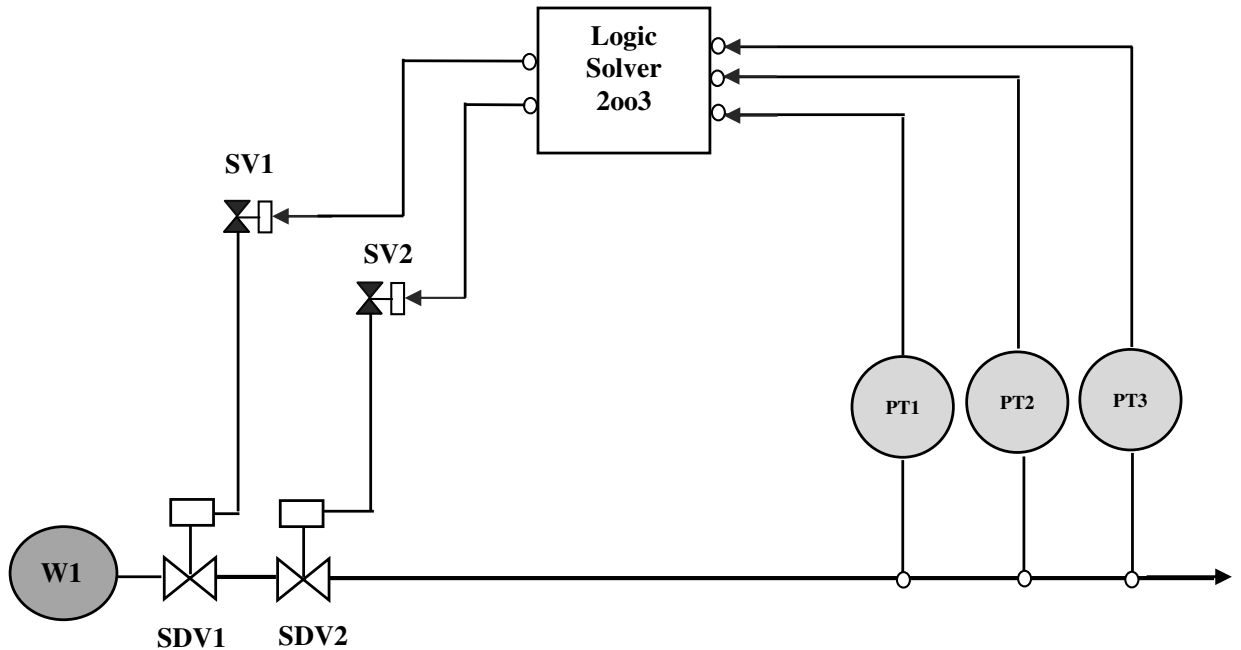


FIGURE 3.4 – Schéma fonctionnel du HIPS

Le SIS étudié est destiné à protéger le circuit aval d'une surpression émanant d'un puits W1. Son fonctionnement est le suivant : quand la valeur de la pression dans la

canalisation dépasse un certain seuil, elle est détectée par les trois capteurs de pression,  $PT_i$ , qui envoient l'information à l'unité logique qui contrôle son caractère majoritaire 2/3 (2oo3). Si au moins deux des trois signaux reçus des capteurs confirment la présence d'une surpression dans la canalisation, l'unité logique commande l'ouverture des électrovannes  $SV1$  et  $SV2$ , ce qui à pour conséquence de couper l'alimentation hydraulique qui maintenait ouvertes les vannes  $SDV1$  et  $SDV2$ . Ces dernières se ferment alors et suppriment ainsi le risque de surpression dans le circuit aval.

L'événement redouté auquel nous nous intéressons est justement l'inhibition du SIS, qui se traduit par la non fermeture des deux vannes de secours [58].

La représentation sous forme de bloc-diagramme de fiabilité du HIPS est donnée dans la figure 3.5.

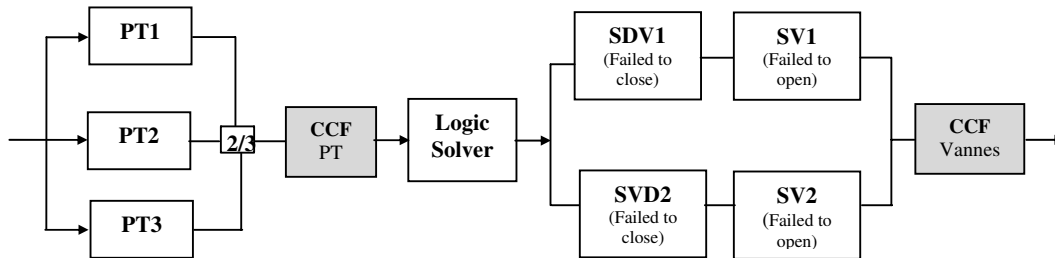


FIGURE 3.5 – Bloc-Diagramme de fiabilité du HIPS

Le solveur logique ne fait pas apparaître de cause commune de défaillance car il n'y a qu'un seul élément. En revanche, la partie actionneur se divise en deux préactionneurs qui commandent les actionneurs de puissance. Il y a donc une cause commune de défaillance pour chacune de ses sous-couches. Trois défaillances de causes communes peuvent être considérées.

L'arbre des défaillances relatif au HIPS étudié est représenté à la figure 3.6. Les défaillances indépendantes et de causes communes des composants y sont aussi représentées.

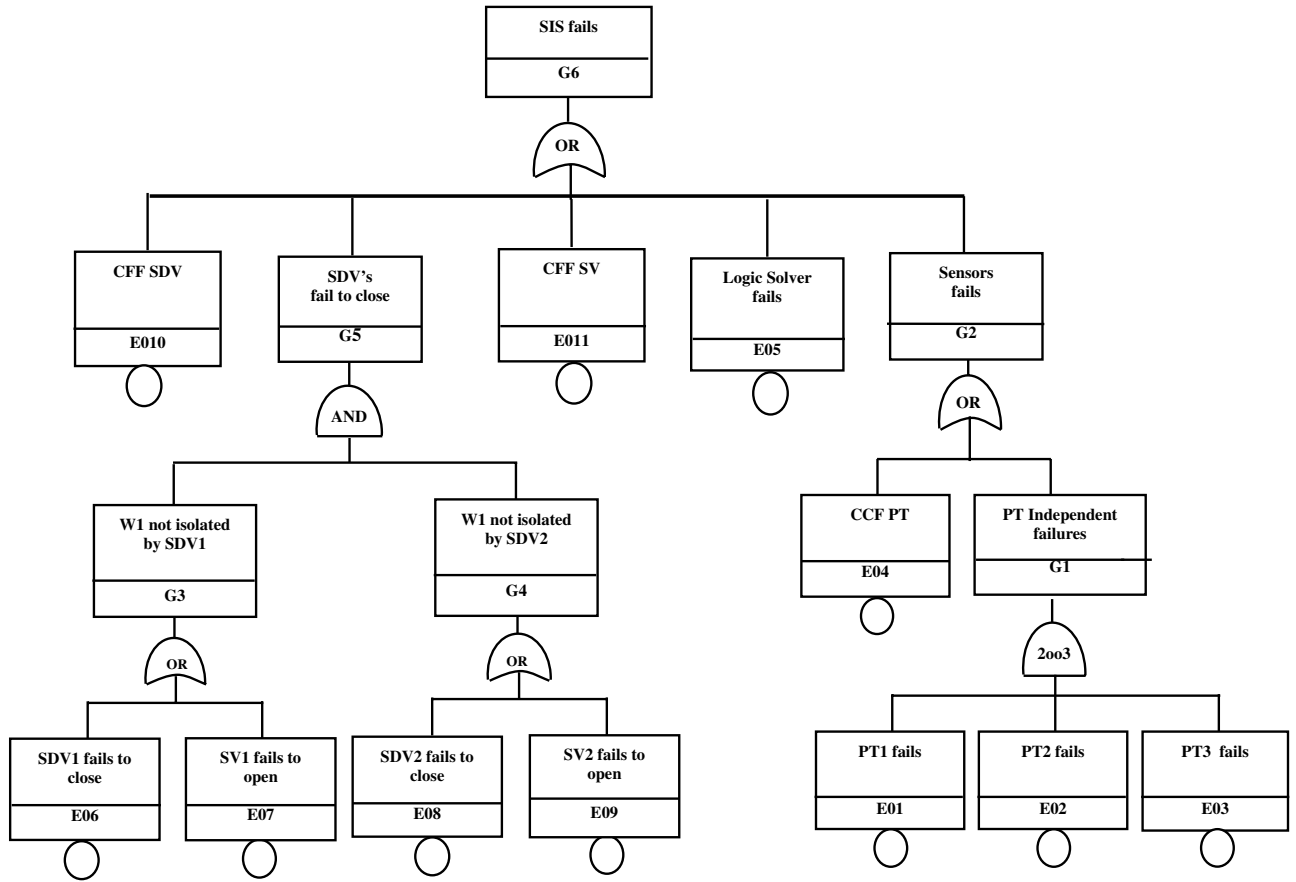


FIGURE 3.6 – Arbre de défaillances relatif au HIPS

### 3.3.3.1 Proposition de l'évaluation de la $PF D_{avg}$ par une approche probabiliste floue

Les probabilités de défaillance des composants sont déterminées à partir de leurs paramètres de défaillance imprécis. Nous supposons que les taux de défaillance des composants sont constants.

Les valeurs des paramètres de défaillance incertaines sont représentées par des nombres flous triangulaires (cf. figure 2.1). L'approche proposé permet de traiter l'incertitude du facteur de DCC dans l'évaluation de la  $PF D_{avg}$  et le niveau SIL des SIS, sans faire l'hypothèse des évènements rares.

Les paramètres caractéristiques des composants des sous systèmes du HIPS de la figure 3.4 sont des nombres flous du type triangulaire  $\langle m_i, a_i, b_i \rangle$  (fournis par les experts), avec,  $m_i$  la valeur modale, la valeur la plus probable ;  $a_i$  la limite à gauche de  $m_i$  et  $b_i$  la limite à droite de  $m_i$ . La table 3.1 donne les valeurs de ces trois paramètres pour le facteur

de DCC de chaque sous ensemble du HIPS. Les composants du système sont considérés non réparables et à taux constants.

TABLE 3.1 – Paramètres caractéristiques du HIPS

Composants	$\lambda(h^{-1})$	$\beta$ (%)	$T_i(h)$	
			Cas 1	Cas 2
$PT_i$	$7.00E^{-7}$	$< 5, 3, 8 >_{LR}$	$T_1 = 2190$	$T_1 = 730$
$SDV_i$	$3.10E^{-6}$	$< 10, 8, 13 >_{LR}$	$T_2 = 2190$	$T_2 = 1460$
$SV_i$	$2.80E^{-6}$	$< 10, 8, 13 >_{LR}$	$T_2 = 2190$	$T_2 = 1460$
Logic Sover	$2.15E^{-7}$	–	$T_3 = 2190$	$T_3 = 2190$

La  $PFD_{avg}$  est calculée par intégration dans le temps de la probabilité de défaillance instantanée  $PFD$  du SIS assurant la fonction de sécurité. En utilisant la méthode des arbres de défaillances flous proposée, celle des  $\alpha$ -coupes et les opérations arithmétiques définies précédemment, on détermine la probabilité de défaillance du SIS à partir des distributions des paramètres caractéristiques de ses composants représentés par des nombres flous de type  $L - R$ .

Pour le calcul de la  $PFD_{avg}$  et la classification du SIL du HIPS, on utilise un intervalle de test  $T_i$  qui correspond à la fréquence à laquelle on teste le SIS étudié (cf. Chapitre 1). Deux cas sont traités. selon que les tests des composants sont réalisés simultanément ou non. L'ensemble des données numériques pour les deux cas est fourni dans le tableau 3.1.

**1<sup>er</sup> Cas : tous les composants du système sont testés simultanément.**

Lorsque tous les composants du système sont testés simultanément [81]. Pour chaque  $\alpha$ -coupe nous déterminons les bornes supérieure et inférieure de la  $PFD_{avg}$  du HIPS.

La figure 3.7 montre la variation en fonction du temps de l'indisponibilité instantanée  $PFD$  du HIPS étudié pour  $\alpha = 0$  et  $\alpha = 1$ , ainsi que sa valeur moyenne  $PFD_{avg}$ . Pour  $\alpha = 1$ , le HIPS passe plus de 58% de son temps dans le domaine de SIL 3, ce qui explique l'obtention d'une valeur moyenne,  $PFD_{avg}^{(\alpha=1)}$ , égale à  $0.941 \times 10^{-3}$  et classe ce HIPS au niveau SIL 3. Pour  $\alpha = 0$ , la  $PFD$  résultante varie entre deux bornes. Dans le cas où la  $PFD$  est maximale, le HIPS passe plus de 60% de son temps dans le domaine de SIL 2, ce qui conduit à une valeur moyenne,  $PFD_{avgR}^{(\alpha=0)}$ , égale à  $1.153 \times 10^{-3}$ . Alors que la variation de la  $PFD$  minimale permet de classer le HIPS au niveau SIL 3.

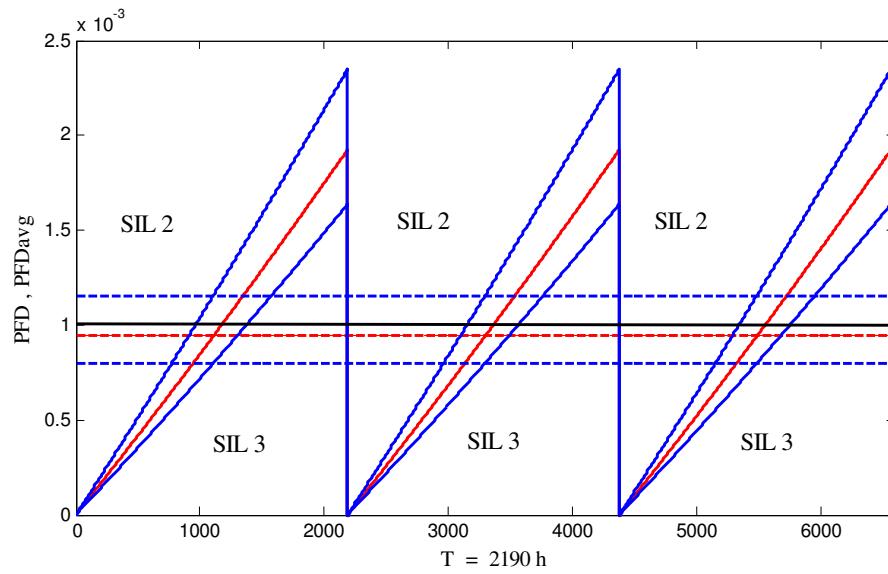


FIGURE 3.7 – La  $P\tilde{F}D$  et  $P\tilde{F}D_{avg}$  du HIPS dans le cas 1, pour  $\alpha = 0$  and  $\alpha = 1$

La figure 3.8 montre le nombre flou de type triangulaire représentant l'imprécision résultante sur la  $P\tilde{F}D_{avg}$  du HIPS étudié [81]. La  $P\tilde{F}D_{avg}$  varie de  $0.798 \times 10^{-3}$  jusqu'à  $1.153 \times 10^{-3}$ , ce qui conduit à la variation du niveau de sécurité du HIPS, d'un niveau de SIL3 ( $P\tilde{F}D_{avg} \in [10^{-4}, 10^{-3}]$ ) à un niveau SIL2 ( $P\tilde{F}D_{avg} \in [10^{-3}, 10^{-2}]$ ).

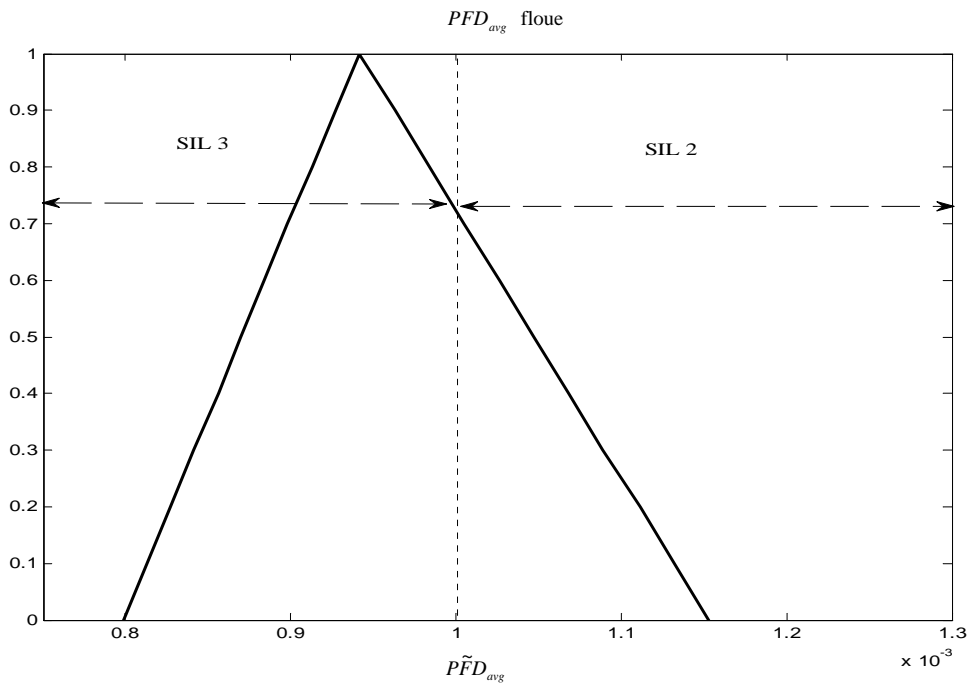


FIGURE 3.8 –  $P\tilde{F}D_{avg}$  floue du HIPS pour le cas 1

Les résultats obtenus montrent que l'imprécision sur le facteur de DCC amène à une variation du niveau de SIL du SIS alors qu'une valeur précise mais incertaine aurait fourni un niveau unique de SIL 3 correspondant à la  $PFD_{avg}^{(\alpha=1)}$ . L'imprécision sur la  $P\tilde{F}D_{avg}$  induit donc une incertitude sur la qualification de performance du HIPS [87].

Pour une classification de performance sans incertitude, il est nécessaire de changer soit le jeux de composants, soit la structure du SIS (niveau de redondance) soit augmenter notre connaissance du facteur de défaillance de cause commune [81]. Le décideur a la responsabilité d'accepter ou non le risque potentiel lié à l'incertitude que le facteur de cause commune induit sur la qualification du SIS.

**2<sup>me</sup> cas : les composants du système sont testés à des intervalles de temps différents**

Comme dans le cas précédent, la  $PFD$  du système est encadrée par des bornes supérieure et inférieure liées à l'intervalle défini par l' $\alpha$ -coupe grâce à la monotonie inclusive de la fonction indisponibilité associée à ce système.

L'évolution de la  $PFD$  du SIS ainsi que sa valeur moyenne  $PFD_{avg}$ , représentée en pointillés, pour ( $\alpha = 0$  et  $\alpha = 1$ ) sont fournies dans la figure 3.9.

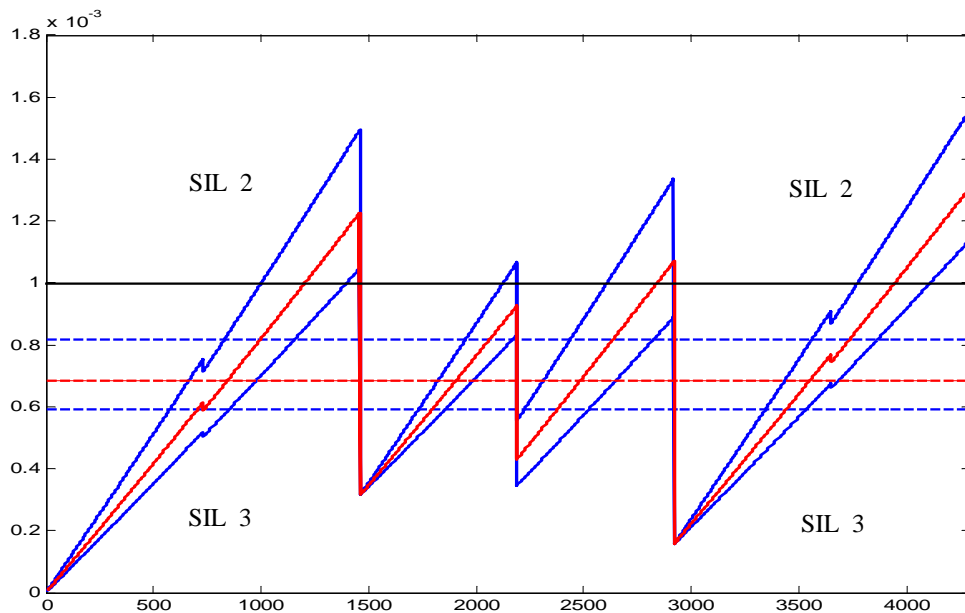


FIGURE 3.9 – Variation de la  $PFD$  et la  $P\tilde{F}D_{avg}$  du HIPS pour le cas 2

Les résultats de cette simulation (cf. figure 3.9), montre que l'encadrement de la  $PFD$  est conservé. Le HIPS passe la plus part de son temps dans la zone de SIL 3, quelque soit

$\alpha \in [0, 1]$ .

Pour chaque  $\alpha$ -coupe, on détermine les bornes supérieure et inférieure de la  $PFD$  du SIS ainsi que sa  $PFD_{avg}$ .

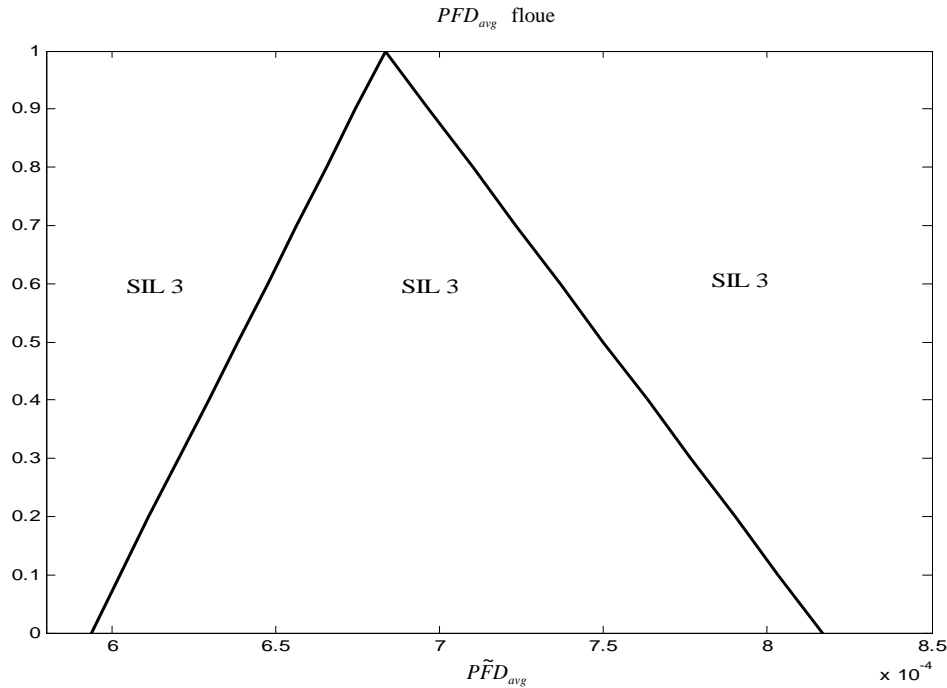


FIGURE 3.10 –  $P\tilde{F}D_{avg}$  floue du HIPS pour le cas 2

La  $P\tilde{F}D_{avg}$  est un nombre flou de type triangulaire représenté dans la figure 3.10. Cette probabilité de défaillance varie de  $0.593 \times 10^{-3}$  jusqu'à  $0.816 \times 10^{-3}$ , ce qui correspond à un niveau de SIL3 ( $PFD_{avg} \in [10^{-4}, 10^{-3}]$ ) pour le HIPS en question. Il n'y a pas d'ambiguïté sur le niveau de SIL de ce SIS.

Cette imprécision de la  $P\tilde{F}D_{avg}$  est, comme précédemment, due à l'imprécision des valeurs des facteurs de DCC,  $\beta$ , mais la modification de la périodicité des tests a permis de réduire l'incertitude sur la qualification du SIS. Le décideur est placé dans une situation claire concernant la qualification du HIPS.

### 3.3.3.2 Validation de l'approche proposée par simulation de Monte Carlo

Pour la validation des résultats précédents on utilise des probabilités de second ordre, la valeur de  $\beta$  varie dans une plage correspondant au support  $([a_i, b_i])$  du nombre flou  $\tilde{\beta}_i$  (cf. tableau 3.1).

Le principe insuffisant de Laplace [64] (tout ce qui est équiprobable est équiprobable)

conduit à la modélisation du paramètre imprécis par une distribution de probabilité sur l'ensemble de valeurs des paramètres imprécis. Les lois des distributions utilisées pour la simulation sont ; la loi uniforme et la loi triangulaire [87].

**a) Loi uniforme**

La loi uniforme (cf. figure 3.11) est utilisée quand on n'a aucune information exceptée la connaissance de l'intervalle  $([a_i, b_i])$ . Il n'y a alors aucune raison de penser, a priori, qu'un évènement soit plus probable qu'un autre.

Une variable aléatoire  $\beta$  est distribuée uniformément sur l'intervalle  $[a_i, b_i]$  si sa densité de probabilité est constante sur cet intervalle :

$$\beta_i \rightarrow U(a_i, b_i) \tag{3.22}$$

$$f(\beta_i) = \begin{cases} \frac{1}{b_i - a_i} & \text{si } a_i \leq \beta_i \leq b_i \\ 0 & \text{sinon} \end{cases} \tag{3.23}$$

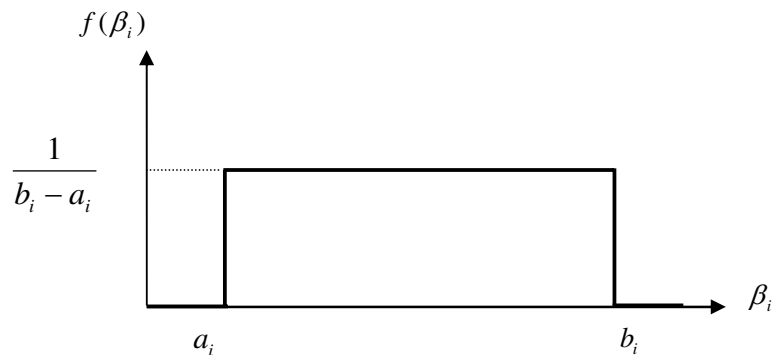


FIGURE 3.11 – Densité de probabilité de la loi uniforme

**b) Loi Triangulaire**

Les distributions de probabilité triangulaires peuvent être utilisées pour représenter notre ignorance au sujet des facteurs de DCC (cf. équation (3.24)) [81]. La loi triangulaire (cf. figure 3.12) est utilisée si on dispose d'une estimation ; du minimum  $a_i$ , du maximum  $b_i$  et de la valeur la plus probable  $m_i$  (même paramètres  $\langle m_i, a_i, b_i \rangle$  que ceux du nombre flou  $\tilde{\beta}_i$ ). Les valeurs utilisées pour construire les distributions de probabilité sont celles du tableau 3.1.

$$\beta_i \rightarrow \Delta(a_i, m_i, b_i) \quad (3.24)$$

La loi triangulaire continue sur le support  $[a_i, b_i]$  et de mode  $m_i$  est définie par la densité suivante sur  $[a_i, b_i]$  :

$$f(\beta_i) = \begin{cases} \frac{2(\beta_i - a_i)}{(m_i - a_i) \cdot (b_i - a_i)} & \text{si } a_i \leq \beta_i \leq m_i \\ \frac{2(b_i - \beta_i)}{(b_i - m_i) \cdot (b_i - a_i)} & \text{si } m_i \leq \beta_i \leq b_i \\ 0 & \text{sinon} \end{cases} \quad (3.25)$$

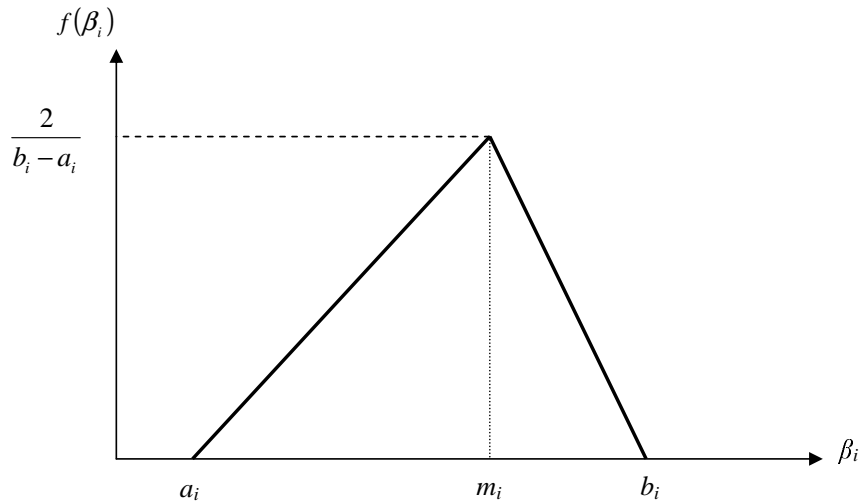


FIGURE 3.12 – Densité de probabilité de la loi triangulaire

### c) Résultats de la simulation

Un tirage de type Monte-Carlo permet alors de combiner l'ensemble des valeurs des paramètres imprécis au travers du modèle choisi, ici un arbre de défaillances où les probabilités des événements de base sont imprécises. Le problème d'imprécision sur la valeur de  $\beta$  pourrait être abordé selon la théorie des probabilités [87].

Le tirage de Monte Carlo consiste à un simple tirage aléatoire de 2000 triplets valeurs de chaque facteur  $\beta$  les équations (3.22) et (3.24). Le tirage de Monte Carlo réalisé permet de déterminer les variations de la  $PF D_{avg}$  du HIPS modélisé par l'arbre de défaillances

de la figure 3.6 dans le cas où tous les composants du SIS sont testés simultanément (cf. Tableau 3.1). La distribution de la  $PFD_{avg}$  du HIPS est représentée par la figure 3.13.

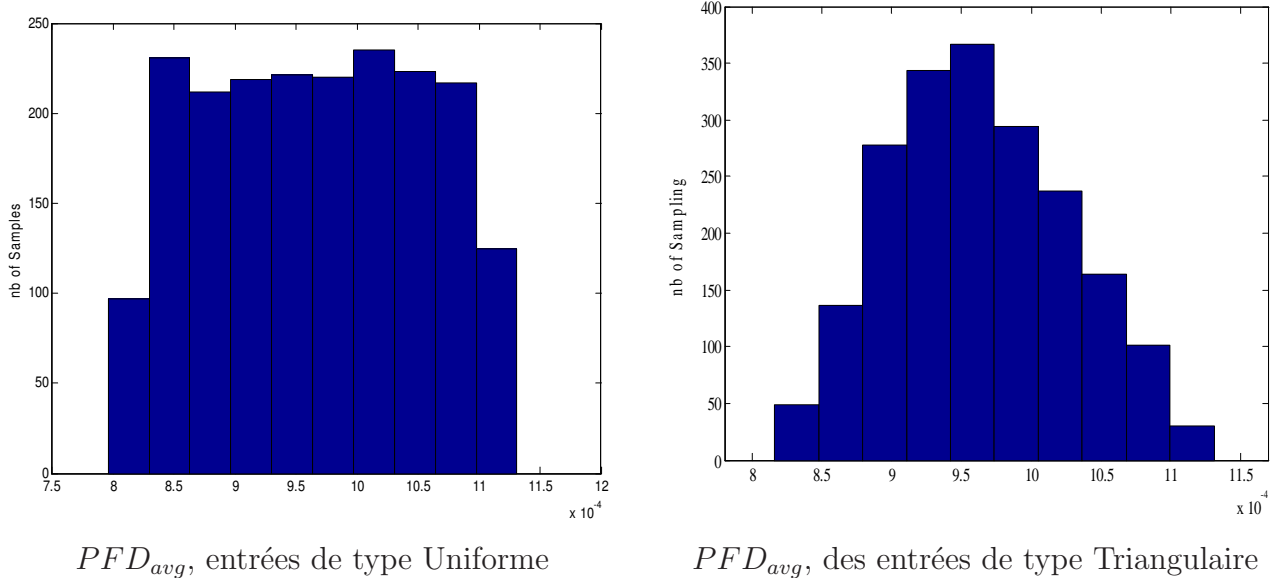


FIGURE 3.13 – Histogrammes des résultats de la simulation de Monte Carlo

De l'histogramme de la figure 3.13, la valeur des bornes inférieure et supérieure de la  $PFD_{avg}$  du HIPS sont :  $[0.807 \times 10^{-3}, 1.146 \times 10^{-3}]$ . Des résultats obtenus à partir de la simulation de Monte Carlo et de l'approche floue proposée, plusieurs éléments sont particulièrement intéressants. Le support de la  $\tilde{PFD}_{avg}$   $[0.798 \times 10^{-3}, 1.153 \times 10^{-3}]$  contient les bornes supérieure et inférieure des probabilités obtenues par tirage de Monte Carlo.

### 3.3.3.3 Importance des sources d'informations

Dans l'approche proposée, nous avons implicitement considéré une seule et unique source d'information fournissant les valeurs floues des paramètres  $\beta_i$  puisque on a combiné les intervalles liés aux mêmes niveaux  $\alpha$ . En effet, le niveau  $\alpha$  est en relation directe avec le niveau de confiance de la source [40]. Aussi, prendre les coupes de même niveau  $\alpha$  suppose le même niveau de confiance, ceci n'est obtenu que de la même source. Si les sources sont différentes et en l'absence de connaissance sur les dépendances entre sources, les niveaux  $\alpha$  de chaque source sont indépendants [4].

Pour tenir compte de cette indépendance, nous procédons alors à un tirage aléatoire de  $J$  ensembles de niveaux  $\alpha$ , pour chaque nombre flou  $\tilde{\beta}_i$ , ce qui fournit les intervalles de valeurs que l'on combine dans l'arbre de défaillances selon la méthode proposée [40], [4]. Nous obtenons ainsi un ensemble d'intervalles résultant dont le niveau de confiance est inconnu [29]. Il suffit alors de considérer le même pour chaque intervalle, tel que :

$$([\underline{PFD}_{avg}, \overline{PFD}_{avg}, \frac{1}{j}]) \quad j \in J \quad (3.26)$$

L'agrégation de ces intervalles peut être menée comme le propose Ferson [39], Les bornes supérieure  $\overline{F}$  et inférieure  $\underline{F}$  de la densité des fonctions cumulatives de la  $PFD_{avg}$  sont calculées en utilisant :

$$\underline{F}(x) = \sum_{\underline{PFD}_{avg, j} \geq x} \frac{1}{j} \quad (3.27)$$

$$\overline{F}(x) = \sum_{\overline{PFD}_{avg, j} < x} \frac{1}{j} \quad (3.28)$$

Le HIPS proposé à la figure 3.4 est un système à trois couches. Un facteur  $\beta$  de DCC est établi par couche. Deux facteurs  $\beta$  différents peuvent être choisis puisque la couche unité de traitement est une architecture '1oo1'. Chaque  $\beta$  est un nombre flou décrit par ses  $\alpha$ -coupes. On note  $\alpha_1$  et  $\alpha_2$  les  $\alpha$ -coupes des nombres flous des facteurs  $\beta$  des DCC respectivement de la couche capteur et de la couche actionneur.

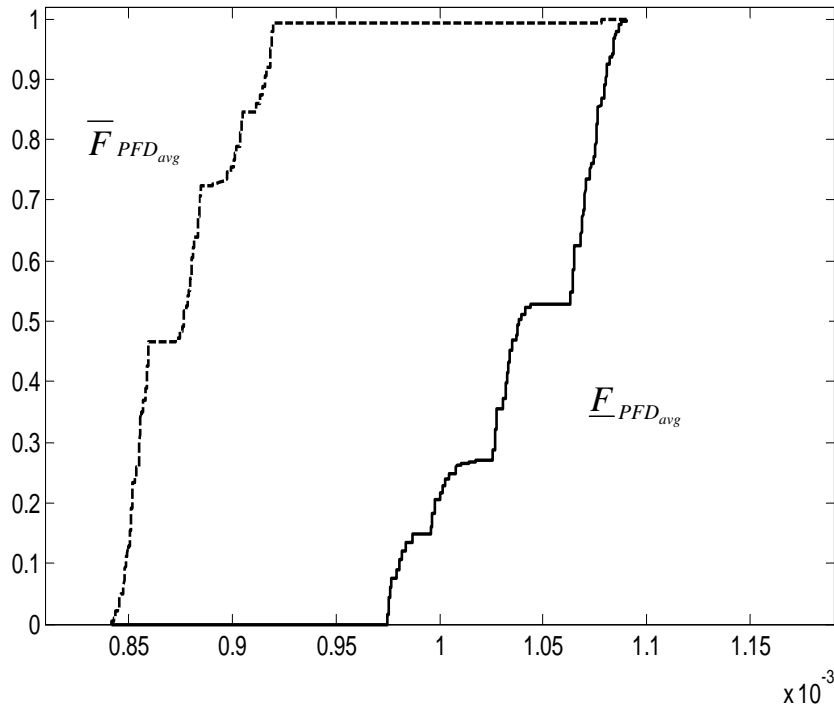


FIGURE 3.14 – Distribution cumulée supérieure et inférieure de la  $PFD_{avg}$

La figure 3.14 donne les densités de probabilités cumulées supérieure et inférieure issues de l'agrégation de 100 intervalles déterminés à partir du tirage aléatoire de 100 couples de valeurs  $\beta_1^{(\alpha_1)}$  et  $\beta_2^{(\alpha_2)}$  pour les alpha-coupes;  $\alpha_1$  et  $\alpha_2$ .

La comparaison des résultats de la figure 3.13 à ceux de la figure 3.14, montre que la  $PFD_{avg}$  du HIPS est encadrée par une p-boîte construite à partir des facteurs de DCC. La p-boîte  $[\underline{F}_{PFD_{avg}}, \overline{F}_{PFD_{avg}}]$  généralise l'idée de l'intervalle d'une paire de points à une paire de probabilités cumulées.

### 3.3.4 Conclusion partielle

L'approche floue proposée dans ce chapitre est basée sur l'utilisation des nombres flous pour représenter l'incertitude des probabilités de DCC des SIS. A partir des facteurs DCC imprécis, nous avons proposé une étude basée sur l'arithmétique floue contrainte proposée par Buckley et nous avons montré l'impact de l'imprécision d'un événement élémentaire sur la qualification de performance d'un SIS.

Contrairement aux travaux de Sallak, l'approche proposée permet une évaluation plus précise de la  $PFD_{avg}$  et du niveau SIL des SIS, en intégrant plus de paramètres notamment, le facteur  $\beta$  de DCC et sans faire l'hypothèse des événements rares. Cependant, il n'est pas toujours possible d'éliminer les répétitions d'évènements et l'hypothèse des événements rares n'est pas toujours vérifiée.

Nous avons également proposé la prise en compte de plusieurs sources d'information pour la définition des valeurs des facteurs de DCC et montré comment agréger la  $PFD_{avg}$  résultante sous la forme d'une famille de probabilités imprécises.

## 3.4 Evaluation des performances des SIS à l'aide des P-boxes

La représentation de l'imprécision par une famille de probabilité p-boxes [39] est particulièrement intéressante. Elle est utilisée quand le type de distribution de probabilités est connu mais la connaissance des valeurs des paramètres caractéristiques est imparfaite, ou bien dans le cas où nous disposons d'informations statistiques descriptives (min, max, moyenne, ...) sans connaître la distribution sous-jacente.

Dans ce dernier cas, l'imprécision sur la probabilité est prise en compte par une distribution ou par un intervalle et la distribution sous-jacente est inconnue. De fait, faire l'hypothèse d'une loi de probabilité est un apport significatif d'information dont l'impact sur l'étude menée n'est pas négligeable (loi uniforme). La modélisation par un intervalle de probabilités est une alternative séduisante menant vers les travaux de Walley [131] sur les probabilités supérieure et inférieure ou vers la théorie des p-boxes largement développée par Ferson [38]; [37].

Dans cette section, les travaux de Ferson sont utilisés [37] pour traiter du problème d'imprécision sur la connaissance de la valeur du facteur de défaillance de cause commune et sa prise en compte dans l'évaluation de la performance d'un SIS. La théorie des familles de probabilités imprécises (p-boxes) est utilisée pour représenter l'incertitude de la connaissance du facteur de DCC. Par la suite l'intégration de la modélisation des paramètres par des p-boxes dans les arbres de défaillance est traitée pour l'évaluation imprécise de la performance et la détermination des niveaux SIL des SIS [84].

### 3.4.1 Les P-boxes

Les p-boxes  $[\underline{F}, \overline{F}]$  généralisent l'idée d'intervalle [89] d'une paire de points à une paire de probabilités cumulées. Elles apparaissent comme un choix naturel pour les modèles paramétriques avec des paramètres imprécis [37] ; [10].

On peut imaginer qu'un expert puisse fournir un modèle probabiliste  $P_\Theta$  pour représenter sa connaissance sur les paramètres d'un système. Cependant, si l'expert est incapable d'estimer avec exactitude la valeur des paramètres  $\theta \in \Theta$  du modèle probabiliste  $P_\Theta$ , il fournit un encadrement de chacun des paramètres  $\theta \in [\underline{\Theta}, \overline{\Theta}]$ .

Soit  $F_\Theta$  la fonction de répartition associée au modèle probabiliste  $P_\Theta$ . Une p-boxe peut être alors définie  $[\underline{F}, \overline{F}]$  à partir de cette information en résolvant les deux problèmes suivants [4] :

$$\underline{F}(x) = \inf_{\theta \in [\underline{\Theta}, \overline{\Theta}]} F_\Theta(x) \quad \text{et} \quad \overline{F}(x) = \sup_{\theta \in [\underline{\Theta}, \overline{\Theta}]} F_\Theta(x) \quad (3.29)$$

Par exemple, un expert décide d'après son expérience, qu'une variable  $X$  suit une loi uniforme  $P_{(a,b)} = U(a, b)$  et estime la valeur des paramètres  $a$  et  $b$  telle que  $a \in [\underline{a}, \overline{a}]$  et  $b \in [\underline{b}, \overline{b}]$ . Nous notons  $U([\underline{a}, \overline{a}], [\underline{b}, \overline{b}])$  une p-boxe de type uniforme.

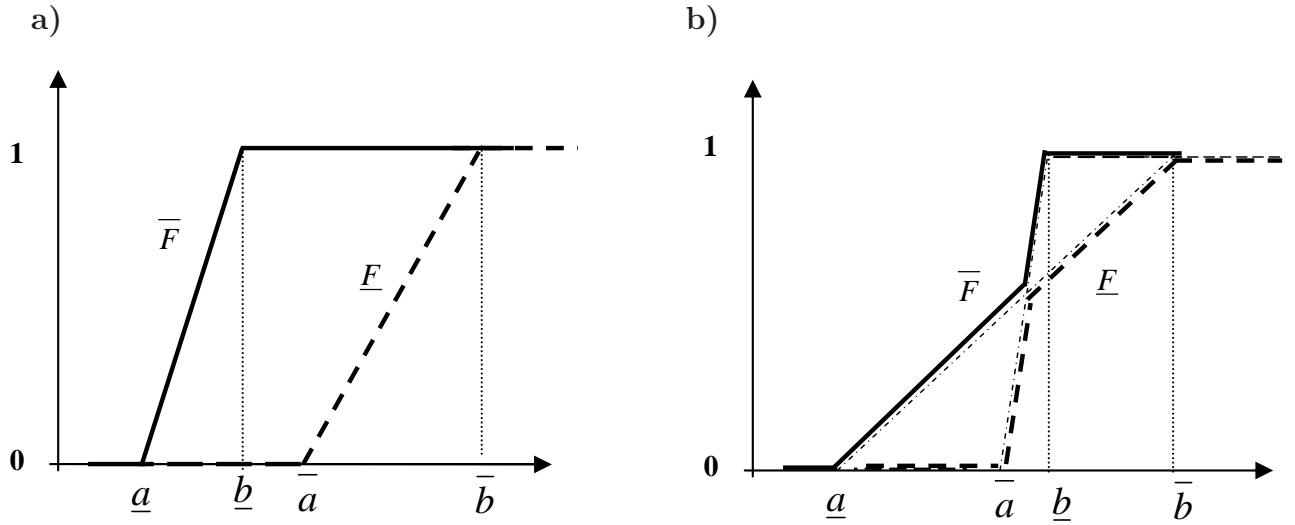


FIGURE 3.15 – Représentation d'une p-boîte de type uniforme

Soit une fonction  $Z = f(X, Y)$  des quantités incertaines  $X$  et  $Y$ . Les entrées incertaines,  $X$  et  $Y$ , sont représentées respectivement sous formes de p-boîte  $[\underline{F}_X, \bar{F}_X]$  et  $[\underline{F}_Y, \bar{F}_Y]$ . Elles sont discrétisées respectivement en  $m$  et  $n$  intervalles, chaque p-boîte est décrit par une série d'intervalles :

$$\{(x_i = [\underline{x}_i, \bar{x}_i], p_i)\} \quad , i = 1, \dots, m \text{ et } \{(y_j = [\underline{y}_j, \bar{y}_j], q_j)\} \quad , j = 1, \dots, n.$$

Il s'agit d'une discrétisation canonique. Chaque intervalle de probabilités est alors propagé par un produit cartésien à travers une fonction  $f$  [135]; [134]; [10]. Alors le  $(i, j)^{ime}$  élément du produit cartésien de la fonction  $f(X, Y)$ , est :  $(f(x_i, y_j, \frac{1}{m} \times \frac{1}{n}))$ .

$f(x_i, y_j)$  est l'extension d'intervalle des éléments  $x_i$  et  $y_j$ . La p-boîte résultante  $[\underline{F}_Z, \bar{F}_Z]$ , dans le cas d'indépendance entre les variables d'entrées, est alors ordonnée comme suit :  $(f(x_i, y_j, \frac{1}{m} \times \frac{1}{n}))$  pour  $i = 1, \dots, m$  et  $j = 1, \dots, n$ .

Le calcul d'intervalles étant sous-distributif, le résultat d'un calcul est donc bien plus imprécis qu'il ne pourrait l'être. Buckley a précisé dans [16] que si  $f$  était monotone alors le calcul de l'intervalle de sortie  $y$  peut être mené en choisissant de manière adéquate les bornes des entrées [87], [84].

Le choix des bornes des intervalles d'entrée est fait suivant le signe de la dérivée partielle de la sortie  $y$  par rapport aux variables d'entrée  $p_i$  (suivant le signe  $\partial f / \partial p_i$ ), de manière à obtenir en sortie l'intervalle le plus petit garantissant que les valeurs réelles seront à l'intérieur de cet intervalle [16].

Il s'agit d'utiliser le calcul d'intervalles développé dans la section 3.3.1.2 aboutissant aux équations (3.11) et (3.12). Nous proposons dans la suite d'adapter les équations obtenues dans l'approche d'intervalles flous afin de l'appliquer dans la manipulation des familles de probabilités imprécises. Le calcul d'intervalle est ici un élément de base qui doit être appliqué en respectant les particularités de la théorie des p-boxes.

### 3.4.2 Modélisation de l'imprécision des DCC à l'aide des P-boxes

En supposant que le facteur de DCC ne soit pas connu avec précision mais sous forme d'une famille de probabilités. L'imprécision sur les probabilités de défaillance des composants de base est prise en compte en utilisant des p-boxes de type uniforme (cf. figure 3.16) [84].

Ainsi, les facteurs de DCC  $\beta$  introduits dans l'étude précédente (cf. section 3.2.3) sont remplacés par des p-boxes d'une loi uniforme  $[\underline{F}_{\beta_i}, \overline{F}_{\beta_i}]$ . Chaque facteur de DCC  $\beta_i$  est décrit par une série de paire de probabilités cumulées. La p-boxe (figure 3.16) est canoniquement discrétisée en  $m$  éléments sous la forme d'un couple (intervalle, masse) :

$$[\underline{F}_{\beta_i}, \overline{F}_{\beta_i}] = \{([\underline{\beta}_{i_1}, \overline{\beta}_{i_1}], p_i); ([\underline{\beta}_{i_2}, \overline{\beta}_{i_2}], p_i); \dots; ([\underline{\beta}_{i_j}, \overline{\beta}_{i_j}], p_i); \dots; ([\underline{\beta}_{i_m}, \overline{\beta}_{i_m}], p_i)\} \quad (3.30)$$

avec  $p_i = \frac{1}{m}$  et  $\sum_i p_i = 1$ .

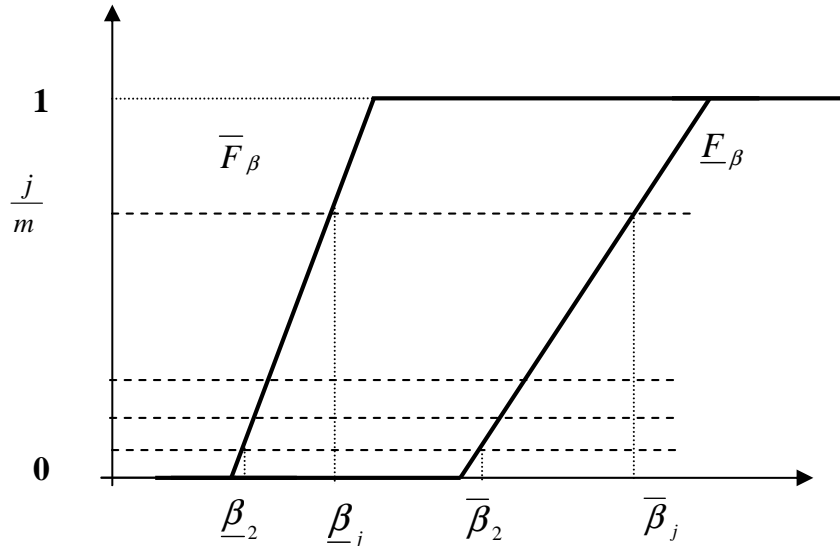


FIGURE 3.16 – Représentation du facteur de DCC par une p-boxe de type uniforme.

### 3.4.2.1 Evaluation imprécise de la $PF D_{avg}$

En utilisant l'arithmétique contrainte de Buckley et la théorie des P-boxes, on détermine la probabilité d'occurrence de l'évènement sommet de l'arbre de défaillances représenté à la figure 3.2 [84].

L'approche proposée est ainsi utilisée pour calculer les bornes supérieure et inférieure de la probabilité d'occurrence de l'évènement sommet, en utilisant les expressions des intervalles  $[P(t)^{ccf}]$  et  $[P(t)^{(i)}]$ .

Soit  $[y] = [P_T(t)] = f([P(t)_i^{(i)}], [P(t)_i^{ccf}])$ , les bornes inférieure et supérieure de  $[y]$  sont déterminés, en utilisant les équations (3.11) et (3.12).

Sachant que  $\partial y / \partial P^{(i)} > 0$  et  $\partial y / \partial P^{ccf} > 0$ , alors les bornes des intervalles de la p-boxe résultante de la probabilité d'occurrence de l'évènement sommet du système sont :

$$\underline{P}_T(t) = 1 - (1 - \underline{P}^{(i)}(t)) \cdot (1 - \underline{P}^{ccf}(t)) \quad (3.31)$$

$$\overline{P}_T(t) = 1 - (1 - \overline{P}^{(i)}(t)) \cdot (1 - \overline{P}^{ccf}(t)) \quad (3.32)$$

En appliquant la p-boxe de la figure 3.16, sur l'arbre de défaillances de la figure 3.2 selon la méthode proposée, les bornes inférieure et supérieure des p-boxes  $[F_{P^{ccf}}]$  et  $[F_{P^{(i)}}]$  sont données en réécrivant les équations (3.5) et (3.6) à partir des équations (3.11) et (3.12).

Sachant que  $\partial P^{ccf} / \partial \beta > 0$  et  $\partial P^{(i)} / \partial \beta < 0$ , les  $[P^{ccf}(t)]$  et  $[P^{(i)}(t)]$  sont déterminées comme suit :

$$[P^{ccf}(t)] = [1 - e^{-\underline{\beta} \cdot \lambda \cdot t}, 1 - e^{-\overline{\beta} \cdot \lambda \cdot t}] \quad (3.33)$$

$$[P^{(i)}(t)] = [(1 - e^{-(1-\overline{\beta}) \cdot \lambda \cdot t}), (1 - e^{-(1-\underline{\beta}) \cdot \lambda \cdot t})^2] \quad (3.34)$$

La démarche d'analyse menée sur une seule couche d'un SIS et conduisant aux équations (3.33) et (3.34) peut être étendue à l'ensemble des couches à l'arbre de défaillances complet pour les HIPS (cf. figure 3.6).

En utilisant la méthode des arbres de défaillances proposée, celle des p-boxes et l'arithmétique d'intervalles contrainte de Buckley [16], la  $PF D$  du HIPS est déterminée à partir

des valeurs des paramètres caractéristiques des composants du HIPS [84].

TABLE 3.2 – Paramètres caractéristiques du HIPS sous forme de p-boxes

Composants	$\lambda(h^{-1})$	$\beta(\%)$	$T_i(h)$
$PT_i$	$7.00E^{-7}$	$U([5, 3]; [5, 8])$	$T_1 = 2190$
$SDV_i$	$3.10E^{-6}$	$U([8, 10]; [10, 13])$	$T_2 = 2190$
$SV_i$	$2.80E^{-6}$	$U([8, 10]; [10, 13])$	$T_2 = 2190$
Logic Solver	$2.15E^{-7}$	–	$T_3 = 2190$

Les facteurs  $\beta_i$  sont modélisés par des p-boxes de type uniforme (cf. Tableau 3.2), décomposées en une liste de paires de la forme (intervalle, masse), à chaque intervalle est associé une masse de probabilité [39]. En ne considérant que l'imprécision sur les  $\beta_i$ , nous pouvons en mesurer l'influence sur la  $PF_{D_{avg}}$  du HIPS. Les composants du système sont indépendants, c'est-à-dire que toutes les variables aléatoires décrivant l'indisponibilité des composants sont indépendantes.

Dans la table 3.2, les  $T_i$  représentent les intervalles de temps entre tests. Nous traitons le cas où les tests des composants sont réalisés simultanément et ne provoquent pas l'indisponibilité de la SIF.

A partir des facteurs de DCC imprécis modélisés par des p-boxes de type uniforme, les bornes inférieure et supérieure de la probabilité moyenne de défaillance à la sollicitation du HIPS sont calculées en utilisant les équations (3.11) et (3.12). Pour déterminer les distributions de la p-boxe résultante de la  $[F_{PF_{D_{avg}}}]$ , les équations (3.30), (3.33) et (3.34) sont utilisées. Le résultat est fourni à la figure 3.17.

Nous constatons donc que l'imprécision sur le facteur de DCC amène à une variation du niveau de SIL du SIS. La p-box résultante  $[F_{PF_{D_{avg}}}]$  varie entre deux bornes qui couvrent deux niveaux de SIL. En outre, la variation de la  $\underline{F}_{PF_{D_{avg}}}$  amène à une variation du niveau de sécurité du SIS puisqu'elle couvre un niveau SIL 3 et un niveau SIL 2. En revanche, la variation de la  $\overline{F}_{PF_{D_{avg}}}$  couvre un seul niveau de SIL et permet de classer avec certitude

le SIS dans le domaine SIL 3 [84].

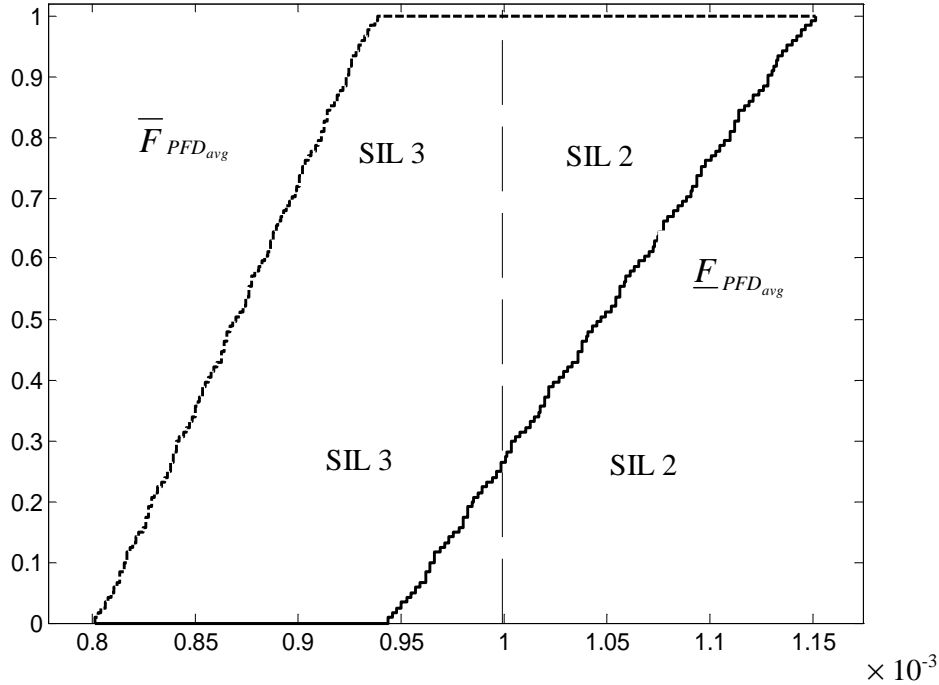


FIGURE 3.17 – P-boxe résultante de la  $PFD_{avg}$  du HIPS

Le résultat, figure 3.17, montre que la probabilité moyenne de défaillance à la demande,  $PFD_{avg}$ , varie de  $0.798 \times 10^{-3}$  jusqu'à  $1.153 \times 10^{-3}$ , ce qui donne pour le HIPS étudié un niveau de SIL3 ( $PFD_{avg} \in [10^{-4}, 10^{-3}]$ ) ou un niveau SIL2 ( $PFD_{avg} \in [10^{-3}, 10^{-2}]$ ). Nous constatons donc que l'imprécision sur le facteur  $\beta$  de DCC entraîne une variation du niveau de SIL du SIS. L'imprécision sur la  $PFD_{avg}$  induit donc une incertitude sur la qualification de performance du SIS [84].

L'utilisation de la théorie des familles de probabilités imprécises p-boxes dans les arbres de défaillance a permis de traiter l'impact de l'imprécision du facteur  $\beta$  des DCC sur la performance d'un HIPS. A partir des facteurs de DCC imprécis modélisés par des p-boxes de type uniforme, nous avons proposé une étude basée sur l'arithmétique d'intervalles et nous avons montré l'impact de l'imprécision des données élémentaires sur la quantification de la performance d'un SIS. Ainsi, nous avons obtenu une p-boxe de type quasi uniforme de la  $PFD_{avg}$  du SIS qui a mis en évidence l'existence d'incertitudes concernant le niveau de SIL de ce SIS [84].

L'imprécision sur la  $[F_{PFD_{avg}}]$  induit donc une incertitude sur la qualification de performance du SIS. Il faut noter que l'approche proposée et les résultats obtenus à partir des facteurs DCC peuvent être étendus à d'autres paramètres caractéristiques du SIS étudié

comme les taux de défaillance des composants ou le taux de couverture de diagnostic.

## 3.5 Conclusion

L'évaluation des SIS peut se faire par l'utilisation d'une approche probabiliste floue. La probabilité floue est caractérisée par une fonction d'appartenance triangulaire et l'intervalle est défini par ses bornes. En utilisant la méthode des  $\alpha$ -coupes la combinaison des probabilités floues et intervalles permet de donner plusieurs intervalles emboîtés .

L'approche proposée se base sur l'arbre de défaillances et sur la méthode des  $\alpha$ -coupes. Chaque probabilité floue d'un événement de base est décrite par un ensemble d'intervalles. Cette méthode est appliquée à un HIPS dans les cas ; les systèmes sont testés simultanément et à des intervalles de temps différents. Les résultats obtenus par cette méthode ont été validé par une approche de simulation de Monte Carlo.

La deuxième proposition concerne l'extension des travaux de Ferson (la théorie des p-boxes) à l'évaluation de la  $PFD_{avg}$  d'un SIS en se basant sur son arbre de défaillances. Cette méthode a été appliquée et a montré que les imprécisions sur les valeurs des facteurs de DCC conduisent à la variation du niveau SIL du SIS.

# 4

## Contribution à l'évaluation des performances des SIS à paramètres imprécis par chaînes de Markov

### Sommaire

---

<b>4.1</b>	<b>Introduction</b>	<b>94</b>
<b>4.2</b>	<b>Evaluation quantitative des SIS</b>	<b>94</b>
4.2.1	Les paramètres caractéristiques des SIS	95
4.2.1.1	Taux de couverture de diagnostic DC	95
4.2.1.2	Défaillances de mode commun	95
4.2.2	Evaluation de la $PFD_{avg}$ à l'aide des Chaînes de Markov	96
<b>4.3</b>	<b>Proposition d'évaluation de la <math>PFD_{avg}</math> par l'approche intervalles</b>	<b>98</b>
4.3.1	Chaînes de Markov à intervalles	98
4.3.2	Modélisation des paramètres caractéristiques des SIS par intervalles	99
4.3.3	Application à un HIPS	101
4.3.3.1	Présentation du système	101
4.3.3.2	Utilisation des chaînes de Markov multiphases à intervalles	102
4.3.3.3	Validation par une approche aléatoire	110
4.3.3.4	Conclusion partielle	111
<b>4.4</b>	<b>Chaînes de Markov multiphases floues pour l'évaluation de la <math>PFD_{avg}</math></b>	<b>111</b>
4.4.1	Présentation des chaînes de Markov floues	112

---

4.4.2	Modélisation des paramètres caractéristiques des SIS par des nombres flous . . . . .	114
4.4.3	Application au HIPS . . . . .	115
4.4.3.1	Approche des chaînes de Markov multiphase floue . . . . .	115
4.4.3.2	Validation de l'approche floue par une approche aléatoire	118
4.4.3.3	Comparaison entre l'approche proposée et l'approche aléatoire . . . . .	120
<b>4.5</b>	<b>Conclusion . . . . .</b>	<b>121</b>

---

---

## 4.1 Introduction

Ce chapitre concerne la proposition de deux approches pour l'évaluation imprécise des performances des SIS réparables, faiblement sollicités et périodiquement testés en modélisant l'incertitude sur la connaissance des taux de défaillance des composants.

La première approche traite l'imprécision sous forme d'intervalles. Dans la seconde approche les paramètres de défaillance sont décrits par des nombres flous. Ces deux approches sont basées sur l'utilisation des chaînes de Markov pour la détermination de la  $PFD_{avg}$  des SIS réparables. Une application support est proposée afin de montrer l'intérêt de nos approches pour l'évaluation des SIL en présence d'informations imparfaites.

Les probabilités élémentaires des chaînes de Markov sont remplacées en premier lieu par des intervalles permettant aux experts fiabilistes d'exprimer leurs incertitudes dans l'énoncé des valeurs de probabilités de défaillances et autres paramètres des systèmes. En second lieu l'imprécision de la connaissance des paramètres imprécis des SIS est considérée sous forme de nombres flous.

Les approches proposées doivent garantir les bornes des probabilités obtenues et la pertinence des résultats est affirmée par comparaison avec une approche par tirage de Monte Carlo. Nous montrons ainsi l'intérêt pour le décideur de connaître l'imprécision sur le paramètre de performance et nous proposons des éléments d'analyse pour appuyer la décision de qualification de performance d'un SIS.

## 4.2 Evaluation quantitative des SIS

L'évaluation quantitative d'un SIS, s'apparente à un calcul d'indisponibilité de sa fonction de sécurité à la sollicitation [30]. Dans ce cadre, les chaînes de Markov apportent une bonne formalisation des SIS faiblement sollicité [65]. Cette approche est souvent utilisée en sûreté de fonctionnement lorsque l'on souhaite modéliser un système réparable (pour la prise en compte des taux de réparation) avec des composants à taux de défaillance constants.

Le calcul de la performance des SIS, se base sur les hypothèses suivantes :

- Toutes les informations sur le comportement du SIS et de ses composants sont disponibles.
- L'évaluation probabiliste des boucles de sécurité s'applique à des composants ayant des défaillances aléatoires et modélisées par une distribution exponentielle [72].
- Les pannes sont classées en quatre catégories. Les défaillances sûres sont distinguées des défaillances dangereuses, chacune de ces catégories étant divisée en défaillances détectées et non détectées.

## 4.2.1 Les paramètres caractéristiques des SIS

### 4.2.1.1 Taux de couverture de diagnostic DC

La norme IEC 61508 [54] définit le taux de couverture pour les tests de diagnostic comme étant le rapport du taux de défaillance des pannes dangereuses détectées  $\lambda_{DD}$  (par un test de diagnostic) et du taux de défaillance total des pannes dangereuses  $\lambda_D$  (détectées et non détectées) [54].

$$DC = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \quad (4.1)$$

L'évaluation ou l'estimation de  $DC$  se fait par une Analyse des Modes de Défaillances et de leurs Effets (AMDE) au niveau des différents composants d'un système [42], éventuellement par retour d'expérience [123]. On cherche ainsi à déterminer les défaillances possibles et à savoir si elles peuvent être détectées. On calcule alors le rapport du taux de défaillance des pannes dangereuses détectées et du taux total des pannes dangereuses [65].

Le taux de couverture intervient dans la détermination des taux de défaillances dangereuses détectées  $\lambda_{DD}$  et dangereuses non détectées  $\lambda_{DU}$ .

$$\lambda_{DD} = DC.\lambda_D \quad \text{et} \quad \lambda_{DU} = (1 - DC).\lambda_D \quad (4.2)$$

$\lambda_D$  est le taux de défaillances dangereuses totales détectées et non détectées des modules des composants des architectures étudiées.

### 4.2.1.2 Défaillances de mode commun

La norme IEC 61508 [54] rappelle la présence des DCC pour les architectures redondantes qui peuvent apparaître dans les canaux suite à une même cause. Des études sur la mise en place et l'évaluation des modes communs ont été réalisées par différents auteurs [47], [41], [91], [78].

Dans ce travail, nous avons privilégié le modèle du facteur  $\beta$  en raison de la complexité raisonnable de sa mise en oeuvre, ce qui en fait d'ailleurs l'un des modèles les plus répandus. L'introduction de ce modèle dans les analyses de fiabilité permet ainsi de calculer la part des DCC sur la probabilité de défaillance d'un système.

Le facteur  $\beta$  quantifie la cause commune de défaillance. Il est défini comme la probabilité d'une défaillance de cause commune, sachant la présence d'une défaillance.

Le choix du facteur  $\beta$  induit les valeurs des taux des défaillances indépendantes,  $\lambda_i^{(i)}$  (respectivement taux des défaillances du mode commun,  $\lambda_i^{(cff)}$ ) (cf. section 3.1.3). Ainsi, les expressions de  $\lambda_i^{(i)}$  et  $\lambda_i^{(cff)}$  sont données par les équations :

$$\begin{cases} \lambda_i^{(i)} = (1 - \beta) \cdot \lambda_i \\ \lambda^{(ccf)} = \beta \cdot \lambda_i \end{cases} \quad (4.3)$$

La norme IEC 61508 [54], définit le facteur  $\beta$  comme une fraction du taux des défaillances matérielles aléatoires dangereuses d'un des canaux de l'architecture analysée [54], alors que les théories exposées précédemment appliquaient ce facteur à toutes les défaillances matérielles aléatoires des composants d'un groupe de cause commune qu'elles soient sûres ou dangereuses [77].

Si  $\beta$  modélise les défaillances de mode commun en l'absence de tests de diagnostic, il vient :

$$\lambda_i^{(ccf)} = \beta \cdot \lambda_D \quad (4.4)$$

La prise en compte des capacités de détections des tests de diagnostic se traduit par :

$$\lambda_i^{(ccf)} = \beta_U \cdot \lambda_{DU} + \beta_D \cdot \lambda_{DD} \quad (4.5)$$

$\beta_U$  représente le facteur des DCC pour les fautes dangereuses non détectées. Il est égal au facteur applicable en l'absence de tests de diagnostic.  $\beta_D$  modélise les DCC pour les fautes dangereuses détectées par les tests de diagnostic.

De ce fait et d'après les équations (4.1) - (4.5), les différents taux des défaillances dangereuses détectées et non détectées deviennent :

$$\begin{cases} \lambda_{DD}^{(i)} = (1 - \beta_D) \cdot \lambda_{DD} = (1 - \beta_D) \cdot DC \cdot \lambda_D \\ \lambda_{DD}^{(ccf)} = \beta_D \cdot \lambda_{DD} = \beta_D \cdot DC \cdot \lambda_D \\ \lambda_{DU}^{(i)} = (1 - \beta_U) \cdot \lambda_{DU} = (1 - \beta_U) \cdot (1 - DC) \cdot \lambda_D \\ \lambda_{DU}^{(ccf)} = \beta_U \cdot \lambda_{DU} = \beta_U \cdot (1 - DC) \cdot \lambda_D \end{cases} \quad (4.6)$$

### 4.2.2 Evaluation de la $PF D_{avg}$ à l'aide des Chaînes de Markov

La méthode des chaînes de Markov [45], [83], [65] apporte une bonne formalisation des états que peuvent prendre les SIS en fonction des événements rencontrés et des paramètres étudiés (taux de défaillance, facteur de DCC, ...).

La loi de transition d'une chaîne de Markov est définie par l'équation suivante :

$$p^{(n)}(S_j) = \sum_i p^{(n-1)}(S_i) \cdot a_{ij} \quad (4.7)$$

$p^{(n)}(S_j)$  est la mesure de la probabilité d'être dans l'état  $S_j$  à l'instant  $n$  et les  $a_{ij}$  représentent les taux de transition de l'état  $S_i$  vers l'état  $S_j$ .

L'équation (4.7) représente la probabilité que le système étudié soit dans l'état  $S_j$  à l'instant  $n$  à partir de n'importe quel autre état  $S_i$  à l'instant  $(n-1)$  selon une probabilité de transition  $a_{ij}$  de  $S_i$  à  $S_j$  définie dans la matrice de transition  $A = (a_{ij})$ .

Les SIS faiblement sollicités ont la particularité d'être périodiquement testés. Ces tests appelés tests de vérification permettent de détecter les défauts latents qui empêcheraient le SIS de remplir sa fonction de sécurité à la sollicitation [123]. Ils permettent d'améliorer le niveau SIL du système sans faire de modification à la conception des systèmes de sécurité.

Généralement, un seul intervalle de test est considéré, pour vérifier la fonction de sécurité de l'ensemble du système mais certaines applications exigent l'utilisation des intervalles de test différents propres à chaque sous système du SIS. Nous supposons que l'on teste fonctionnellement chaque sous-système indépendamment les uns des autres.

L'état du SIS est donc connu à ces instants et les probabilités des différents états sont également connues. Les chaînes de Markov multiphases [110]; [58]; [30] sont des modèles appropriés (cf. section 1.4.2.5). En ne considérant qu'un seul intervalle de test, il n'y a qu'une matrice de passage  $M$  permettant l'affectation de la distribution de probabilités d'être dans les différents états  $S_j$  aux instants d'inspection  $(k.t_i)$  vers la distribution de probabilités aux instants,  $(k.t_i + \Delta t)$ .

$$p^{(k.t_i + \Delta t)} = p^{(k.t_i)} \cdot M \quad (4.8)$$

avec  $k \in \mathbb{N}^+$

Les SIS étant composés de plusieurs sous-systèmes et composants, il est possible que plusieurs matrices de passages  $M_i$  soient utilisées au cours du temps même si les inspections sont normalement répétées à intervalles de temps constants. Grâce aux équations (4.7) - (4.8), nous pouvons déterminer la probabilité de défaillance à la demande du SIS. La probabilité moyenne de défaillance à la demande est ensuite calculée comme suit :

$$PFD_{avg} = \frac{1}{k \cdot \Delta t} \cdot \sum_{n=0}^k \sum_{S_j} p^{(n)}(S_j) \cdot \Delta t \quad (4.9)$$

où  $k \cdot \Delta t \in [0, T_M]$

$T_M$  est le temps de mission,  $S_j$  sont les états de défaillances dangereuses et  $P^{(n)}(S_j)$  est la probabilité d'être dans un de ces états à l'instant  $n$ . La quantification du niveau

SIL du SIS est alors obtenue par référence aux données du tableau 1.1.

Les conditions d'exploitation (environnement) des SIS, sont souvent différentes des conditions des données fournies par es experts du domaine, permettant la définition des valeurs des paramètres caractéristiques des SIS. C'est le cas du facteur de DCC ou le taux de couverture de diagnostic. Ces paramètres résultent dans la plupart des cas d'un travail d'expertise pouvant être guidé par l'expérience ou par estimation. Dans ce cas, les experts ou les concepteurs fournissent des estimations imprécises des paramètres caractéristiques des composants. Les bases de données fournissent des statistiques descriptives (min, max, moyenne) et la distribution réelle reste inaccessible [4], [10].

A partir des données fournies par les experts, l'imprécision des paramètres peut être modélisée par plusieurs manières. Une vision purement probabiliste basée sur l'utilisation de la simulation de Monte Carlo conduit à la modélisation d'un paramètre imprécis par une distribution de probabilité sur l'ensemble des valeurs qu'il peut prendre. L'imprécision peut être représentée tout aussi simplement en ne faisant pas d'hypothèse sur la distribution mais en utilisant des intervalles [90].

### 4.3 Proposition d'évaluation de la $PF D_{avg}$ par l'approche intervalles

L'approche par intervalles proposée permet de traiter le problème d'imprécision dans l'évaluation de la performance des SIS à l'aide des chaînes de Markov multiphases. Les probabilités de transition des chaînes de Markov sont remplacées par des intervalles [86] permettant aux experts fiabilistes d'exprimer leurs incertitudes dans l'énoncé des valeurs de probabilités de défaillances et autres paramètres des systèmes.

#### 4.3.1 Chaînes de Markov à intervalles

La loi de transition d'une chaîne de Markov classique est définie par les équations (1.13) et (4.7). Dans le cas où les  $a_{ij}$  ne sont pas connus avec précision mais appartiennent avec certitude à des intervalles [69] :  $[p^{(n)}(S_j)]$  et  $[a_{ij}]$  pour  $i, j = 1, \dots, r$ , on peut écrire.

$$[p^{(n)}(S_j)] = [p_L^{(n)}(S_j), p_R^{(n)}(S_j)] \Rightarrow p_L^{(n)}(S_j) \leq p^{(n)}(S_j) \leq p_R^{(n)}(S_j) \quad (4.10)$$

$$[a_{ij}] = [a_{ij,L}, a_{ij,R}] \Rightarrow a_{ij,L} \leq a_{ij} \leq a_{ij,R} \quad (4.11)$$

La loi de transition de la chaîne de Markov à intervalles est donnée par la relation suivante :

$$[p^{(n)}] = [p^{(n-1)}].[A] \quad (4.12)$$

$[A]$  est la matrice de transition décrite par l'équation 4.13, elle est constituée des différentes valeurs  $a_{ij}$  représentées sous formes d'intervalles.

$$[A] = \begin{bmatrix} [a_{1,1}] & [a_{1,2}] & \dots\dots\dots & [a_{1,r}] \\ [a_{2,1}] & [a_{2,2}] & \dots\dots\dots & [a_{2,r}] \\ \cdot & \cdot & \dots\dots\dots & \cdot \\ [a_{r,1}] & [a_{r,2}] & \dots\dots\dots & [a_{r,r}] \end{bmatrix} \quad (4.13)$$

A partir des équations (4.7), (4.10) - (4.12) les probabilités supérieure et inférieure des différents états sont obtenues en résolvant le problème suivant [69] :

$$\begin{cases} p_L^{(n)}(S_j) = \inf \sum_{S_i, a_{ij}} p^{(n-1)}(S_i) \cdot a_{ij} & , \quad j = 1, \dots, r \\ p_R^{(n)}(S_j) = \sup \sum_{S_i, a_{ij}} p^{(n-1)}(S_i) \cdot a_{ij} & , \quad j = 1, \dots, r \end{cases} \quad (4.14)$$

A partir des équations (4.14) et (1.14) les bornes supérieure et inférieure de la probabilité  $p^n(S_j)$  d'être dans les différents états  $S_j$  à l'instant  $n$  sont :

$$\begin{cases} p_L^{(n)}(S_j) = \inf \sum_i p^{(0)}(S_i) \cdot a_{ij}^n \\ p_R^{(n)}(S_j) = \sup \sum_i p^{(0)}(S_i) \cdot a_{ij}^n \end{cases} \quad (4.15)$$

### 4.3.2 Modélisation des paramètres caractéristiques des SIS par intervalles

La valeur du taux de couverture  $DC$  peut être modélisée par un intervalle  $[DC]$  borné par deux valeurs  $[DC_L, DC_R]$ . De même, la valeur du facteur de DCC,  $\beta$ , peut aussi être représentée par un intervalle borné par deux valeurs  $[\beta_L, \beta_R]$ .

En utilisant l'arithmétique des intervalles développée dans le chapitre 2 (section 2.3) et le jeu d'équations (4.6), les différents taux de défaillances dangereuses deviennent :

$$[\lambda_{DD}^{(i)}] = [DC] \cdot (1 - [\beta_D]) \cdot \lambda_D = [DC_L \cdot (1 - \beta_{D,R}), DC_R \cdot (1 - \beta_{D,L})] \cdot \lambda_D \quad (4.16)$$

$$[\lambda_{DD}^{(ccf)}] = [DC] \cdot [\beta_D] \cdot \lambda_D = [DC_L \cdot \beta_{D,L}, DC_R \cdot \beta_{D,R}] \cdot \lambda_D \quad (4.17)$$

$$[\lambda_{DU}^{(i)}] = (1 - [DC]) \cdot (1 - [\beta]) \cdot \lambda_D = [(1 - DC_R) \cdot (1 - \beta_R), (1 - DC_L) \cdot (1 - \beta_L)] \cdot \lambda_D \quad (4.18)$$

$$[\lambda_{DU}^{(ccf)}] = (1 - [DC]).(1 - [\beta]).\lambda_D = [(1 - DC_R).\beta_L.\lambda_D, (1 - DC_L).\beta_R.\lambda_D] \quad (4.19)$$

Les paramètres  $[\lambda_{DD}]$  et  $[\lambda_{DU}]$  intègrent directement la matrice de transition caractéristique du système étudié.

Pour la prise en compte des paramètres définis ci-dessus, le système peut être modélisé par les chaînes de Markov multiphases à intervalles. Cette opération nécessite l'utilisation des équations (4.8) et (4.15) et l'adaptation de leur traitement. Les probabilités supérieure et inférieure aux différents instants d'inspection sont obtenues en utilisant les équations suivantes :

$$\begin{cases} p_L^{(k.t_i+\Delta t)} = M.p_L^{(k.t_i)} \\ p_R^{(k.t_i+\Delta t)} = M.p_R^{(k.t_i)} \end{cases} \quad (4.20)$$

avec  $k \in \mathbb{N}^+$ .

La  $PFD_{avg}$  est calculée lorsque la fonction de sécurité est faiblement sollicitée. Elle est égale à l'indisponibilité moyenne calculée sur la durée de mission ou éventuellement sur l'intervalle de test si tous les composants sont testés simultanément.

$$[PFD_{avg}] \Rightarrow \begin{cases} PFD_{avg,L} = \frac{1}{k.\Delta t} \cdot \sum_{n=0}^k \sum_{S_j} p_L^{(n)}(S_j) \cdot \Delta t \\ PFD_{avg,R} = \frac{1}{k.\Delta t} \cdot \sum_{n=0}^k \sum_{S_j} p_R^{(n)}(S_j) \cdot \Delta t \end{cases}, k.\Delta t \in [0, T_M] \quad (4.21)$$

### 4.3.3 Application à un HIPS

#### 4.3.3.1 Présentation du système

Le HIPS étudié [110], est destiné à protéger le circuit aval d'une surpression émanant du puits  $W_1$ .

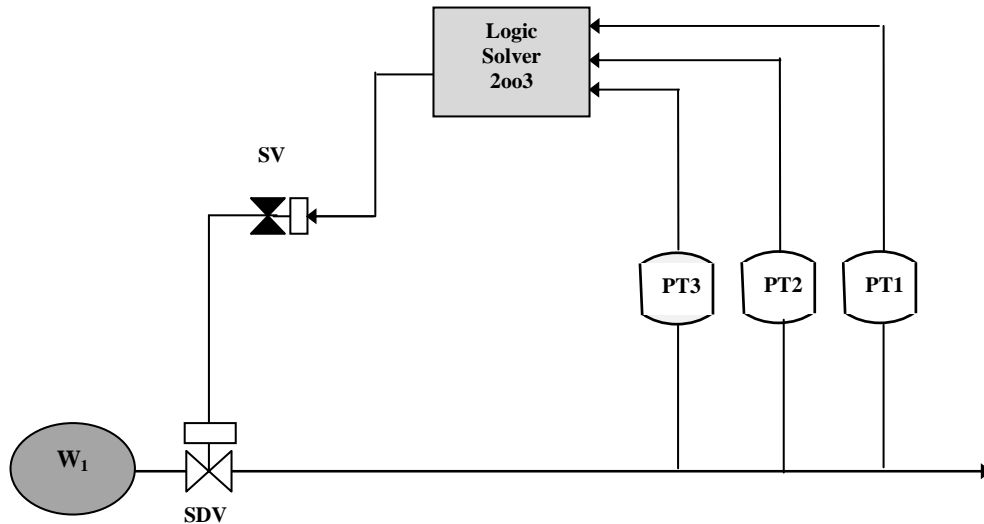


FIGURE 4.1 – Schéma fonctionnel d'un HIPS

Son fonctionnement est le suivant : quand la valeur de la pression dans la canalisation dépasse un certain seuil, elle est détectée par les trois capteurs de pression  $PT_i$  qui envoient l'information à l'unité logique qui contrôle son caractère majoritaire  $2oo3$ . Si au moins deux des trois signaux reçus des capteurs confirment la présence d'une surpression dans la canalisation, l'unité logique commande l'ouverture de la vanne solénoïde  $SV$ . Cela a pour conséquence de couper l'alimentation hydraulique qui maintenait ouverte la vanne  $SDV$ . Celle-ci se ferme alors et supprime ainsi le risque de surpression dans le circuit aval. L'événement redouté auquel on s'intéresse est l'inhibition du SIS qui se traduit par la non fermeture de la vanne de secours  $SDV$ .

Le HIPS en question est composé de :

- la partie capteur en architecture  $2oo3$ , constituée de trois capteurs de pression  $PT_i$ .
- la partie unité logique (Logic Solver) en architecture  $1oo1$ .
- la partie actionneur en architecture  $1oo2$ , composés par les vannes  $SV$  et  $SDV$

Le bloc-diagramme de fiabilité du HIPS est représenté à la figure 4.2.

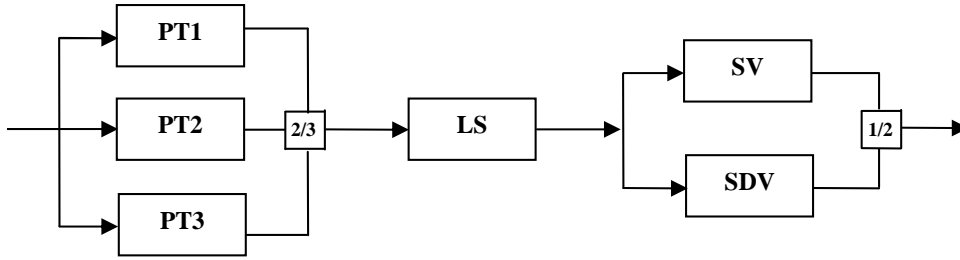


FIGURE 4.2 – Bloc-diagramme de fiabilité du HIPS

Les chaînes de Markov multiphases à intervalles proposées sont utilisées pour évaluer la  $PFD_{avg}$  du HIPS de la figure 4.1, à partir de ces paramètres caractéristiques imprécis représentés sous forme d'intervalles selon l'approche proposée dans les sections précédentes.

Les paramètres caractéristiques des composants du SIS sont donnés dans le tableau 4.1. Le facteur de DCC,  $\beta$ , ainsi que le taux de couverture  $DC$  de chaque sous ensemble sont décrits sous forme d'intervalles fournis par des experts. En ne considérant que l'imprécision sur  $\beta$  et  $DC$ , il s'agit de déterminer l'influence de l'imprécision sur la performance du HIPS.

#### 4.3.3.2 Utilisation des chaînes de Markov multiphases à intervalles

Le HIPS étudié est formé de six composants, chacun pouvant avoir deux états : opérant ou en défaillance dangereuse détectée et non détectée. La construction de la chaîne de Markov par l'espace d'état consiste en l'analyse de  $3^6$  états possibles.

Afin de simplifier les calculs, nous proposons d'évaluer la  $PFD_{avg}$  de chacun des sous-systèmes en série qui constituent le SIS et à les sommer pour obtenir la  $PFD_{avg}$  globale.

La  $PFD_{avg}$  du SIS de la figure 4.1 est calculée par la combinaison de la probabilité de défaillance de tous les sous systèmes assurant ensemble la fonction de sécurité. Elle est exprimée par les formules suivantes sous l'hypothèse d'évènements rares [54] :

$$[P_{HIPS}] = [P_{Cap}] + [P_{UL}] + [P_{Act}] \quad (4.22)$$

$$[P_{HIPS}] = [P_{2oo3}] + [P_{1oo1}] + [P_{1oo2}] \quad (4.23)$$

$P_{HIPS}$ ,  $P_{Cap}$ ,  $P_{UL}$ ,  $P_{Act}$  ; représentent respectivement la probabilité de défaillance à la sollicitation du HIPS, de la partie capteur, la partie unité logique et la partie actionneur.

En utilisant la méthode proposée, chaînes de Markov multiphases à intervalles, la probabilité de défaillance du SIS lors de sa sollicitation est déterminée à partir des paramètres caractéristiques imprécises de ses composants modélisés sous formes d'intervalles.

Les valeurs numériques des paramètres caractéristiques des composants du SIS sont donnés dans le tableau 4.1. Le facteur  $\beta$  de DCC ainsi que le taux de couverture  $DC$  de chaque sous ensemble sont décrits par un intervalle de valeurs fournis par des experts du domaine.

TABLE 4.1 – Paramètres caractéristiques sous forme d'intervalles

Composants du SIS	$\lambda_D(h^{-1})$	DC	$\beta(\%)$	$MTTR(h)$	$T_i(h)$
$PT_i$	$7.00E - 7$	[0.3, 0.7]	[4, 7]	10	$T_1 = 730$
$SDV$	$3.10E - 6$	[0.1, 0.4]	[9, 12]	8	$T_2 = 1460$
$SV$	$3.10E - 6$	[0.1, 0.4]	[9, 12]	8	$T_2 = 1460$
<i>Logic Sover</i>	$1.45E - 7$	[0.7, 0.9]	–	10	$T_3 = 2190$

Pour calculer la  $PF D_{avg}$ , un intervalle de temps  $T_i$  lié à la fréquence de test du SIS est défini.

Dans cette étude, nous proposons d'utiliser des intervalles de test différents propres à chaque sous système du SIS. Nous supposons ainsi que l'on teste fonctionnellement chaque sous-système indépendamment les uns des autres.

Les figures 4.3 à 4.6 représentent les modèles de Markov multiphases relatifs aux différents sous systèmes du SIS étudié.

Le sous-système capteur est en architecture 2oo3. Ce système étant périodiquement testé (intervalle entre tests égal à  $T_1$ ), son comportement au cours d'une mission de durée donnée est correctement décrit par un modèle markovien multiphases, comme schématisé à la figure 4.3.

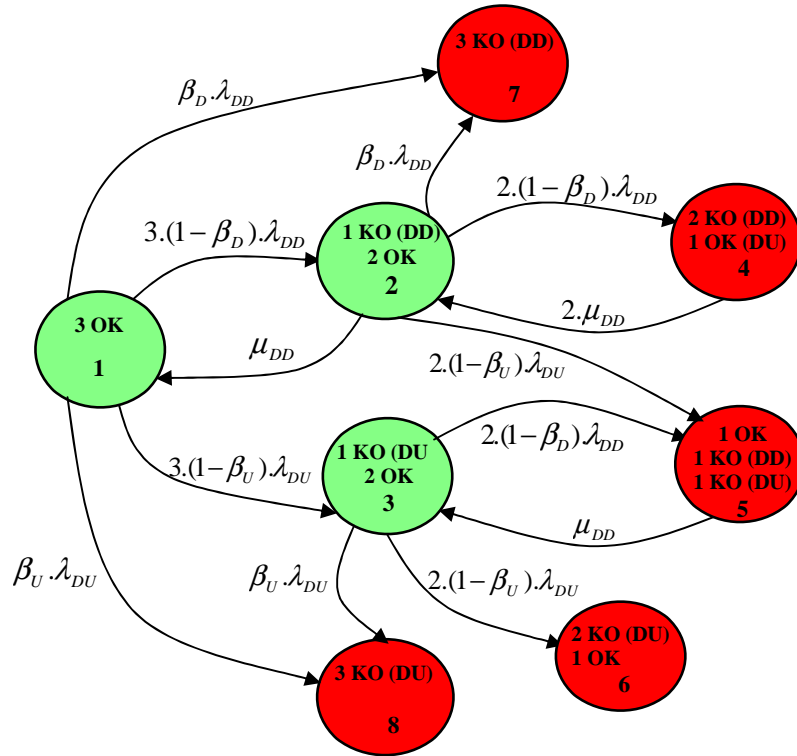


FIGURE 4.3 – Modèle de Markov multiphases relatif au sous système capteurs en architecture 2oo3

$\mu_{DD}$  représente le taux de réparation spécifique aux défaillances dangereuses détectées par le test de diagnostic.

Dans le graphe de Markov représenté à la figure 4.3, l'approche par intervalle proposée pour calculer les bornes supérieure et inférieure de la  $PF D_{avg}$  de l'architecture 2oo3 est appliquée en utilisant les équations (4.20), (4.21) et (4.24).

Les valeurs des probabilités d'occupation des états au début  $d_i$  de la phase  $i$  sont

déduites de celles obtenues aux termes  $f_{i-1}$  de la période  $(i-1)$ , de la manière suivante :

$$p_l(d_i) = M_1 \times p_l(f_{i-1}), l = 1, \dots, 8$$

$$\begin{bmatrix} p_1(d_i) \\ p_2(d_i) \\ p_3(d_i) \\ p_4(d_i) \\ p_5(d_i) \\ p_6(d_i) \\ p_7(d_i) \\ p_8(d_i) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} p_1(f_{i-1}) \\ p_2(f_{i-1}) \\ p_3(f_{i-1}) \\ p_4(f_{i-1}) \\ p_5(f_{i-1}) \\ p_6(f_{i-1}) \\ p_7(f_{i-1}) \\ p_8(f_{i-1}) \end{bmatrix} \quad (4.24)$$

$M_1$  permet de caractériser la détection des défaillances latentes en réaffectant (cf. figure 4.4) :

- $p_2(f_{i-1})$  et  $p_3(f_{i-1})$  à  $p_2(d_i)$
- $p_4(f_{i-1})$ ,  $p_5(f_{i-1})$  et  $p_6(f_{i-1})$  à  $p_4(d_i)$
- $p_7(f_{i-1})$  et  $p_8(f_{i-1})$  à  $p_7(d_i)$ .

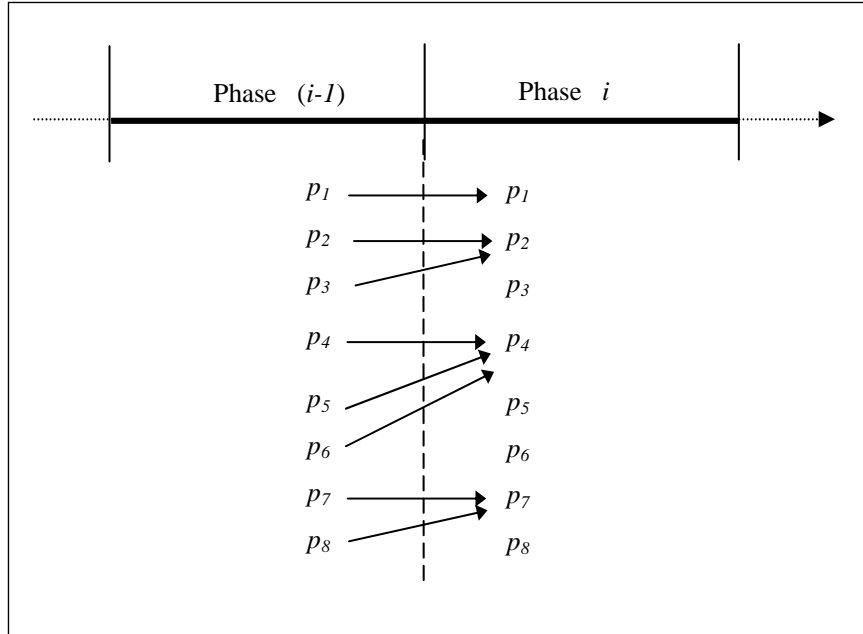


FIGURE 4.4 – Enchaînement des phases de l' architecture 2oo3

L'unité logique est une architecture *1oo1*. Le comportement de ce sous système périodiquement testé (intervalle entre tests égal à  $T_2$ ) peut être modélisé par un modèle markovien multiphases [58] schématisé par la figure 4.5.

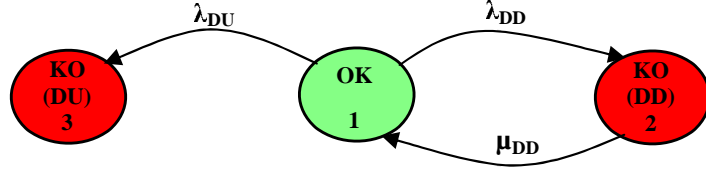


FIGURE 4.5 – Modèle de Markov multiphases relatif au sous système unité logique de traitement

La figure 4.5 modélise le sous système unité logique de traitement. Les trois états décrits par le modèle markovien [59] et les phases s'enchaînent au moment du test de la manière suivante :

- Si le système est dans l'état 1, le système est en marche, il y reste.
- Si le système est dans l'état 2, le système est en panne et les défaillances sont immédiatement détectées (DD), puis réparées.
- le système est dans l'état 3, le système est en panne et les pannes demeurent cachées et ne sont détectées (DU) qu'à l'occasion du prochain test périodique puis réparées.

De l'architecture étudiée (cf. figure 4.5), on détermine la matrice de passage d'interphases  $M_2$ .

$$p_k(d_i) = M_2 \times p_k(f_{i-1}), k = 1, \dots, 3$$

$$\text{avec } M_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad (4.25)$$

La partie actionneur est une architecture *1oo2*. Son modèle multiphases [59] tenant compte à la fois du comportement propre sans et avec DCC de l'architecture *1oo2* est

représenté à la figure 4.6.

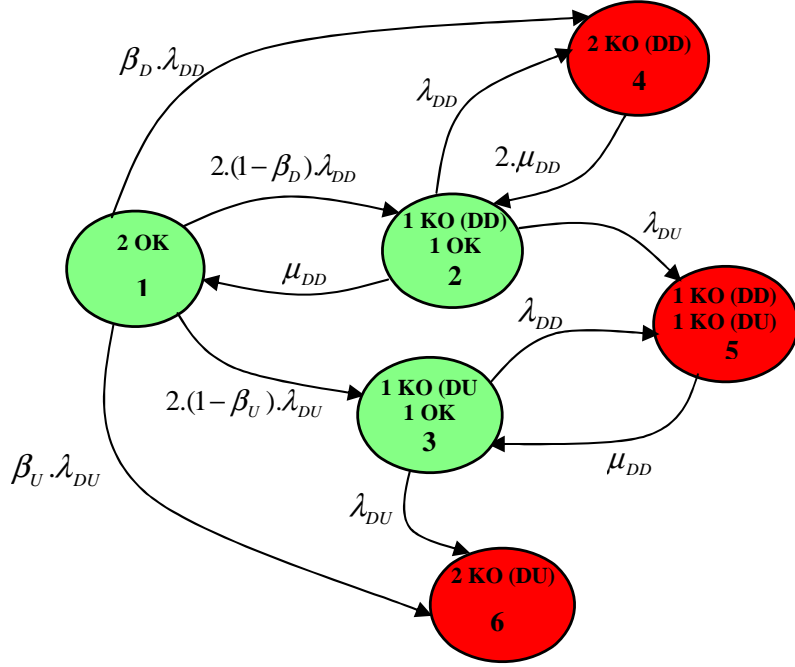


FIGURE 4.6 – Modèle de Markov multiphases relatif au sous système actionneurs

La matrice de passage interphases  $M_3$  est donnée par l'équation 4.26. Les valeurs des probabilités d'occupation des états sont comme suit (cf. figure 4.7) :

$$\begin{bmatrix} p_1(d_i) \\ p_2(d_i) \\ p_3(d_i) \\ p_4(d_i) \\ p_5(d_i) \\ p_6(d_i) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} p_1(f_{i-1}) \\ p_2(f_{i-1}) \\ p_3(f_{i-1}) \\ p_4(f_{i-1}) \\ p_5(f_{i-1}) \\ p_6(f_{i-1}) \end{bmatrix} \quad (4.26)$$

$$\Rightarrow p_j(d_i) = M_3 \times p_j(f_{i-1}), j = 1, \dots, 6$$

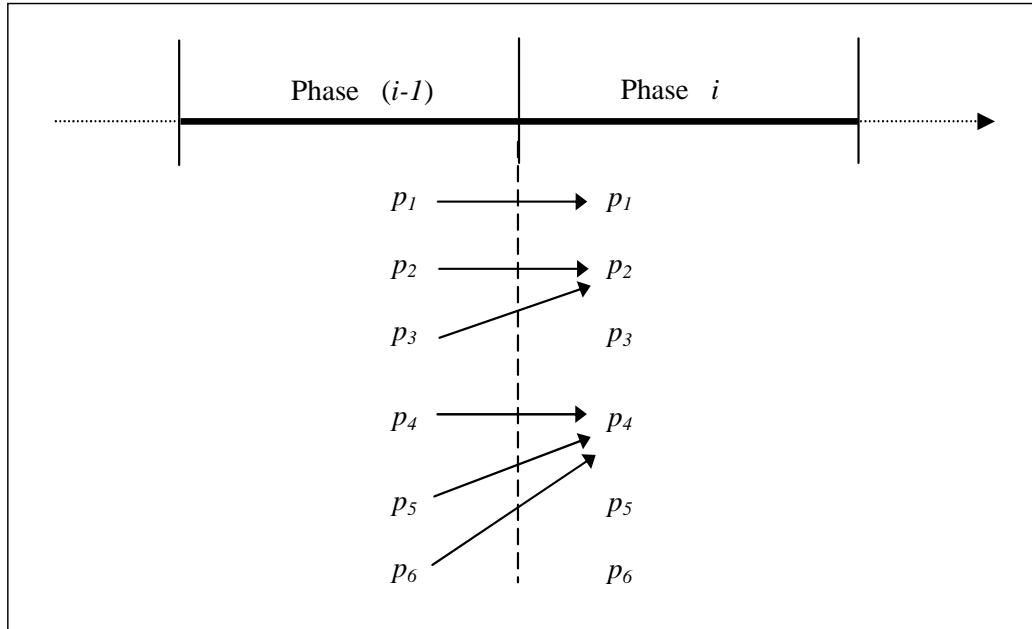


FIGURE 4.7 – Enchaînement des phases dans l'architecture 1oo2

La  $PFD_{avg}$  de l'architecture 1oo2, pour un taux de couverture  $DC$  et un facteur de DCC imprécis, est calculée en utilisant les équations (4.20), (4.21) et (4.26).

La  $PFD_{avg}$  du HIPS de la figure 4.1, est calculée par la combinaison de la probabilité de défaillance de tous les sous systèmes assurants ensemble la fonction de sécurité (cf. équations 4.22, 4.23).

La figure 4.8 montre l'évolution de la probabilité de défaillance à la sollicitation au cours du temps [ $PFD$ ] du HIPS étudié, ainsi que sa valeur moyenne [ $PFD_{avg}$ ], les compo-

sants du système sont testés aux intervalles de temps précisés dans le tableau 4.1.

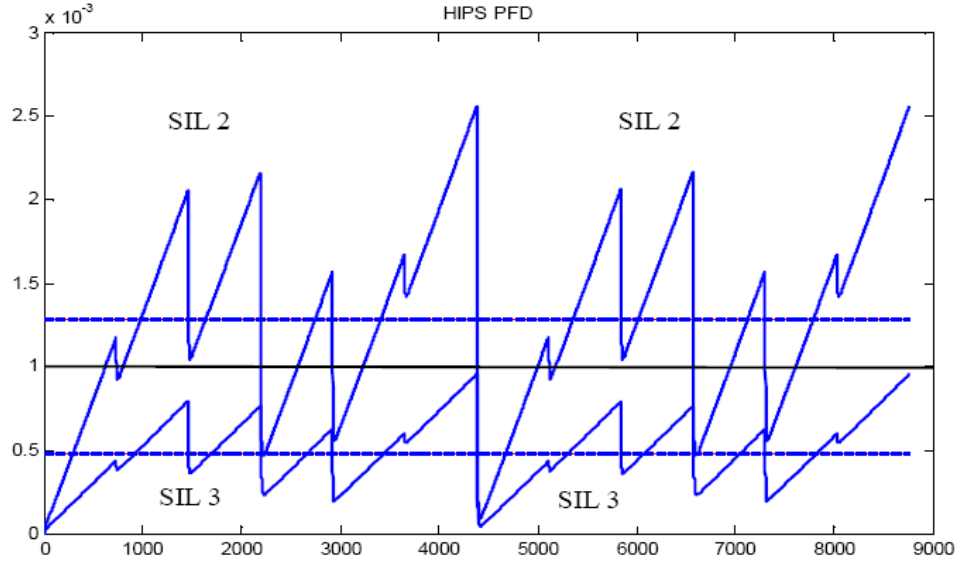


FIGURE 4.8 – Variation de la  $[PFD]$  et  $[PFD_{avg}]$  du HIPS

La  $PFD$  du système est encadrée par les bornes supérieure et inférieure de la  $[PFD]$ , liées à l'intervalle défini pour les paramètres caractéristiques grâce à la propriété de monotonie dans l'inclusion de la fonction disponibilité associée à ce système.

La  $[PFD_{avg}]$  résultante est un intervalle. Cette probabilité de défaillance varie de  $0.484 \times 10^{-3}$  jusqu'à  $1.283 \times 10^{-3}$ , ce qui entraîne une variation du niveau de sécurité pour le HIPS étudié, d'un niveau de SIL3 ( $PFD_{avg} \in [10^{-4}, 10^{-3}]$ ) à un niveau SIL2 ( $PFD_{avg} \in [10^{-3}, 10^{-2}]$ ).

On constate que l'imprécision sur le facteur de DCC  $\beta$  et le taux de couverture de diagnostic  $DC$  amène à une variation du niveau de SIL du HIPS alors qu'une valeur précise mais incertaine nous aurait fourni un niveau unique de SIL. L'imprécision de la  $[PFD_{avg}]$  induit donc une incertitude sur la qualification de performance du SIS.

Si nous recherchons une classification de performance sans incertitude, il est alors nécessaire de changer soit le jeu de composants, soit la structure du SIS (niveau de redondance) soit augmenter notre connaissance des paramètres caractéristiques tel que le taux de couverture de diagnostic ou le facteur de défaillance de cause commune. Le décideur a la responsabilité d'accepter ou non le risque potentiel lié à l'incertitude que le facteur de cause commune  $\beta$  et le taux de couverture de diagnostic  $DC$  induisent sur la qualification du HIPS. Il y a là un compromis coût/risque que le décideur doit arbitrer.

### 4.3.3.3 Validation par une approche aléatoire

Pour la validité des résultats de la  $PF D_{ag}$  obtenus à partir de la méthode des chaînes de Markov à intervalle proposée, on utilise une approche purement probabiliste. Cela revient à supposer que la connaissance sur le facteur,  $\beta$  de DCC et sur le taux de couverture de diagnostic  $DC$  est de nature aléatoire. Cette approche consiste à représenter le paramètre incertain par une distribution de probabilité et à tenir compte de l'incertitude relative à ces paramètres dans le calcul de la  $PF D_{ag}$  du HIPS. La technique de propagation de l'incertitude la plus usuelle est la méthode par tirage aléatoire de Monte Carlo. Puisqu'on ne dispose pas d'informations sur la nature de la distribution des paramètres caractéristiques du HIPS, la distribution uniforme (cf. equation 3.23) est choisie.

$$\begin{aligned}\beta_i &\rightarrow U([\beta_{i,L}, \beta_{i,R}]) \\ DC_i &\rightarrow U([DC_{i,L}, DC_{i,R}])\end{aligned}\tag{4.27}$$

Ce choix est le plus usuel dans le cadre de probabilités, malgré qu'il n'exprime pas correctement notre ignorance au sujet de la vraie distribution de probabilités des paramètres  $\beta$  et  $DC$ . Grâce au tirage de Monte Carlo, les variations  $PF D_{avg}$  du HIPS, modélisé par les chaînes de Markov multiphases, peuvent être déterminées.

La simulation de Monte Carlo consiste en un tirage aléatoire de 2000 valeurs de chaque paramètre représenté par une distribution uniforme selon l'équation 4.27. La distribution de la  $PF D_{avg}$  du HIPS est représentée à la figure 4.9.

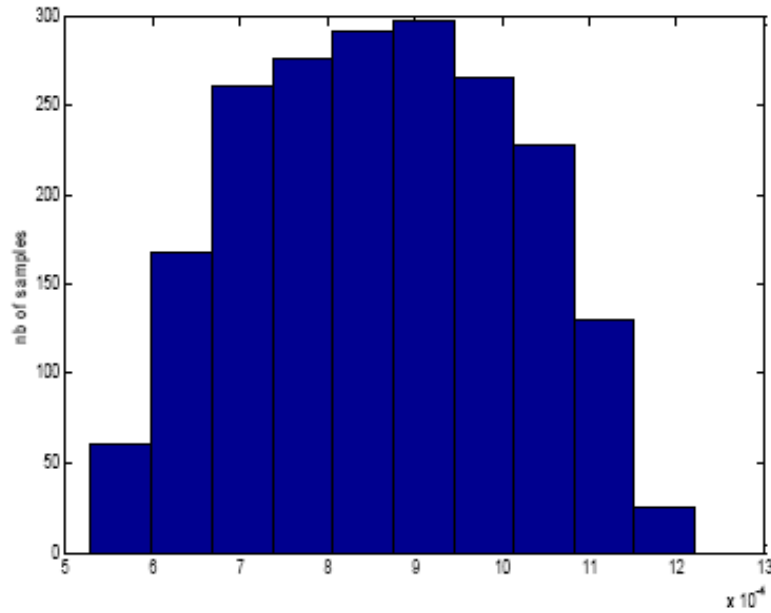


FIGURE 4.9 – Distribution de la  $PF D_{avg}$

A partir des résultats représentés à la figure 4.9, les valeurs des bornes inférieure et supérieure de la  $PF D_{avg}$  du HIPS sont déterminés :  $0.515 \times 10^{-3}$  et  $1.261 \times 10^{-3}$ . La  $PF D_{avg}$  appartient donc à l'intervalle limité par ces deux bornes.

Nous constatons que la  $PF D_{avg}$  déterminée par l'approche des chaînes de Markov à intervalles contient les bornes supérieure et inférieure des probabilités obtenues par tirage de Monte Carlo.

#### 4.3.3.4 Conclusion partielle

A partir des valeurs imprécis de taux de couverture de diagnostic et du facteur de DDC, on a proposé une approche basée sur l'utilisation de la théorie des intervalles au sein des chaînes de Markov multiphases pour l'évaluation de la  $PF D_{avg}$  des HIPS. Ainsi, nous avons obtenu un intervalle de la  $PF D_{avg}$  du HIPS en question qui a mis en évidence l'existence d'incertitudes concernant le niveau de SIL de ce SIS. La simulation de Monte Carlo pour la propagation des valeurs des paramètres caractéristiques du SIS a montré comment l'approche proposée permet de faire le calcul de manière efficace en garantissant le plus petit intervalle final de la  $PF D_{avg}$ .

Le calcul d'intervalles est fréquemment utilisé pour modéliser l'imprécision sur les paramètres des systèmes. Les incertitudes sont alors représentées sous la forme d'intervalles de valeurs et le calcul des performances revient à faire un calcul de pire cas et de meilleur cas. L'inconvénient majeur de ce type de calcul d'intervalles est son caractère peu informatif en termes de quantification de l'incertitude.

Dans certains cas, nous disposons des informations imprécises sous une forme légèrement plus riche qu'un intervalle, par exemple, le mode et les bornes minimale et maximale d'un paramètre imprécis. Dans ce cas on peut utiliser des nombres flous. Les probabilités floues sont un des moyens les plus adaptés pour modéliser l'imprécision et l'incertitude, il reflète naturellement le format linguistique des informations données par un expert. Dans ce qui suit nous nous intéressons à étendre les calculs d'intervalles développés au paragraphe précédant aux nombres flous et nous discutons leurs intégrations dans les chaînes de Markov multiphases.

## 4.4 Chaînes de Markov multiphases floues pour l'évaluation de la $PF D_{avg}$

L'objectif ici est de calculer la  $PF D_{avg}$  du HIPS à partir de ses paramètres caractéristiques imprécis tel que le taux  $DC$  et le facteur de DCC,  $\beta$ , en utilisant les chaînes de Markov multiphases floues. On propose de traiter l'imprécision des paramètres caractéristiques des HIPS, par des nombres flous [83].

L'approche proposée utilise les chaînes de Markov à états non flous et probabilités de

transition floues. Les chaînes de Markov floues sont traitées par la méthode proposée par Buckley [17], [83]. Les probabilités élémentaires des chaînes de Markov sont remplacées par des nombres flous (cf. section 2.3.3) et découpées en  $\alpha$ -coupes [82]. Chaque  $\alpha$ -coupe d'une probabilité floue est utilisée pour calculer l' $\alpha$ -coupe correspondante à la matrice de transition de la chaîne de Markov. Elle permet de déterminer la probabilité floue de défaillance du SIS lors de sa sollicitation [83], [87], [85].

#### 4.4.1 Présentation des chaînes de Markov floues

Dans cette section, nous traitons du problème d'imprécision dans l'évaluation de la  $PFD_{avg}$  des HIPS à l'aide des chaînes de Markov multiphases floues [83]. Les probabilités élémentaires des chaînes de Markov sont remplacées par des nombres flous triangulaires. Cependant, l'approche proposée permet de traiter l'incertitude épistémique des paramètres caractéristiques tels que, le facteur de DCC et le taux de couverture  $DC$  [80], [85].

Si on considère une matrice de transition  $A$  comme définie dans l'équation 1.12, à chaque  $a_{ij}$  est maintenant associée une valeur floue  $\tilde{a}_{ij}$ .

La loi de transition de la chaîne de Markov floue est donnée par la relation suivante :

$$\tilde{p}^{(n)} = \tilde{p}^{(n-1)} \cdot \tilde{A} \quad (4.28)$$

$\tilde{A}$  est la matrice de transition floue décrite par l'équation 4.13, elle est constituée des différentes valeurs  $\tilde{a}_{ij}$  représentées sous formes des nombres flous.

$$\tilde{A} = \begin{bmatrix} \tilde{a}_{11} & \tilde{a}_{12} & \dots & \tilde{a}_{1r} \\ \tilde{a}_{21} & \tilde{a}_{11} & \dots & \tilde{a}_{2r} \\ \cdot & \cdot & \dots & \cdot \\ \tilde{a}_{r1} & \tilde{a}_{r2} & \dots & \tilde{a}_{rr} \end{bmatrix} \quad (4.29)$$

Comme nous l'avons précisé, en utilisant la méthode des  $\alpha$ -coupes, les nombres flous sont des intervalles emboîtés [83], [82]. Chaque coefficient  $\tilde{a}_{ij}$  peut alors être décrit par l'ensemble de ses  $\alpha$ -coupes :  $\tilde{a}_{ij} \rightarrow [a_{ij,L}^{(\alpha)}, a_{ij,R}^{(\alpha)}]$  (cf. équation 2.29).

Toutefois, la restriction suivante sur les  $\tilde{a}_{ij}$  est considérée : il existe une valeur  $\tilde{a}_{ij}^{(\alpha=1)}$  de telle sorte que  $A = (a_{ij})$  soit la matrice de transition de la chaîne de Markov [82]. Cette matrice est caractérisée par le fait que la somme de chacune de ses lignes est égale à un.

Pour calculer  $\tilde{A}^{(n)} = (\tilde{a}_{ij}^{(n)})$ , on utilise la multiplication restreinte des matrices floues proposée par Buckley [17]. Il rappelle la contrainte sur la matrice de transition décrite par

l'équation suivante :

$$C = \{a = (a_1, a_2, \dots, a_r) | a_i \geq 0, \sum_{i=1}^r a_i = 1\} \quad (4.30)$$

avec  $a_i$  est la  $i^{me}$  entité du vecteur  $a$ .

Ainsi, le domaine des  $\alpha$ -coupes est défini comme suit :

$$Dom_i[\alpha] = \left( \prod_{i=1}^r \tilde{a}_{ij}^{(\alpha)} \right) \cap C, \quad (4.31)$$

avec  $\tilde{a}_{ij}^{(\alpha)}$  est une  $\alpha$ -coupe de la probabilité de transition floue  $\tilde{a}_{ij}$ .

$Dom[\alpha]$  est le produit cartésien des  $r$  intervalles  $[a_{ij,L}^{(\alpha)}, a_{ij,R}^{(\alpha)}]$  liés aux coupes de niveau  $\alpha$  produisant un "hyper-rectangle" dans l'espace de dimension  $r$  qui est alors intersecté avec l'ensemble  $C$  [16], [82].

$$Dom[\alpha] = \prod_{i=1}^r Dom_i[\alpha], \quad 0 \leq \alpha \leq 1; \quad 1 \leq i \leq r \quad (4.32)$$

Pour calculer  $a_{ij}^{(n)}$ , il existe une certaine fonction  $f_{ij}^{(n)}$  des  $a_{ij}$  tel que :

$$a_{ij}^{(n)} = f_{ij}^{(n)}(a_{11}, \dots, a_{rr}) \quad (4.33)$$

L'équation (4.33) indique que les coefficients de la matrice de transition  $A^{(n)}$  à l'instant  $n$  peuvent être dérivés par une fonction spécifique des élément de la matrice  $A = (a_{ij})$ .

On considère  $f_{ij}^{(n)}$  une fonction de  $(a_{11}, \dots, a_{rr}) \in Dom[\alpha]$ . Les lignes de  $f_{ij}^{(n)}$  sur  $Dom[\alpha]$  peuvent être formulées comme suit :

$$\tilde{a}_{ij}^{(n)(\alpha)} = f_{ij}^{(n)}(Dom[\alpha]) \quad (4.34)$$

Pour calculer tous les  $[a_{ij}^{(n)(\alpha)}]$ , les bornes de ces intervalles doivent être déterminées. La résolution du système d'équations (4.35) est nécessaire [16] :

$$\begin{cases} a_{ijL}^{(n)(\alpha)} = \min_{a_{ij}} \{f_{ij}^{(n)}(Dom[\alpha])\} \\ a_{ijR}^{(n)(\alpha)} = \max_{a_{ij}} \{f_{ij}^{(n)}(Dom[\alpha])\} \end{cases} \quad (4.35)$$

avec  $\tilde{a}_{ij}^{(n)} \rightarrow [a_{ijL}^{(n)(\alpha)}, a_{ijR}^{(n)(\alpha)}]$ , pour tous les  $\alpha$ .

Les solutions du jeu d'équations (4.35) peuvent être déterminées par un algorithme d'optimisation. Il s'agit donc d'utiliser la formulation optimale de la chaîne de Markov dans l'équation (4.35). Des propriétés de monotonie de la fonction permettent toutefois de simplifier notablement le processus d'optimisation qui se réduit alors à un calcul d'intervalles particulier [83], [80].

La probabilité floue  $\tilde{p}^{(n)}(S_j)$  d'être dans les différents états  $S_j$  à l'instant  $n$  est calculée en utilisant le système d'équations (4.36) suivant :

$$\begin{cases} p_L^{(n),(\alpha)}(S_j) = \sum_i p^{(0)}(S_i) \cdot a_{ijL}^{(n)(\alpha)} \\ p_R^{(n),(\alpha)}(S_j) = \sum_i p^{(0)}(S_i) \cdot a_{ijR}^{(n)(\alpha)} \end{cases} \quad (4.36)$$

#### 4.4.2 Modélisation des paramètres caractéristiques des SIS par des nombres flous

Les paramètres caractéristiques introduits dans la section 4.1 sont remplacés par des nombres flous triangulaires. Chaque paramètre flou peut être décrit par l'ensemble de ses  $\alpha$ -coupes [80].

Le taux de couverture de diagnostic flou  $\tilde{DC}$  est décrit par l'ensemble de ses  $\alpha$ -coupes  $DC^{(\alpha)}$  tel que  $DC^{(\alpha_2)} \subseteq DC^{(\alpha_1)}$  si  $\alpha_1 \leq \alpha_2$ .  $DC^{(\alpha)}$  représente l'intervalle des valeurs pouvant être prises par  $DC$  avec un niveau de confiance  $(1 - \alpha)$ . Ainsi,  $DC$  est borné par deux valeurs  $[DC_L^{(\alpha)}, DC_R^{(\alpha)}]$  (cf. équation 2.29) [85].

De la même manière, l'imprécision du facteur  $\beta$  de DCC est modélisée par un nombre flou triangulaire. Le facteur de DCC flou  $\tilde{\beta}$  est décrit par l'ensemble de ses  $\alpha$ -coupes.  $[\beta_L^{(\alpha)}, \beta_R^{(\alpha)}]$  est l'intervalle borné par deux valeurs.

Les différents taux de défaillance dangereuse flous sont déterminés à partir d'une forme étendue de l'arithmétique d'intervalles, selon l'approche développée (cf. eq (4.16)-(4.19)) [85].

Nous introduisons les paramètres  $\tilde{DC}$  et  $\tilde{\beta}$  dans la matrice de transition du modèle de Markov multiphases. Ainsi, on utilise l'équation (4.8) pour calculer les probabilités supérieure et inférieure à des différents instants d'inspection, décrites par le système d'équa-

tions (4.37) suivant :

$$\begin{cases} p_L^{(k.t_i+\Delta t),(\alpha)} = M.p_L^{(k.t_i),(\alpha)} \\ p_R^{(k.t_i+\Delta t),(\alpha)} = M.p_R^{(k.t_i),(\alpha)} \end{cases} \quad (4.37)$$

avec  $k \in \mathbb{N}^+$

La  $PFD_{avg}$  est calculée lorsque la fonction de sécurité est faiblement sollicitée. Elle est égale à l'indisponibilité moyenne calculée sur l'intervalle de test  $[0, T_i]$  dans le cas où les composants sont testés simultanément.

$T_M$  représente la durée de mission.

$$P\tilde{F}D_{avg}^{(\alpha)} = [PFD_{avg,L}^{(\alpha)}, PFD_{avg,R}^{(\alpha)}] \rightarrow \begin{cases} PFD_{avg,L}^{(\alpha)} = \frac{1}{k.\Delta t} \cdot \sum_{n=0}^k \sum_{S_j} p_L^{(n),(\alpha)}(S_j) \cdot \Delta t \\ PFD_{avg,R}^{(\alpha)} = \frac{1}{k.\Delta t} \cdot \sum_{n=0}^k \sum_{S_j} p_R^{(n),(\alpha)}(S_j) \cdot \Delta t \end{cases} \quad (4.38)$$

où  $k.\Delta t \in [0, T_M]$ ;  $T_M$  est le temps de mission.

### 4.4.3 Application au HIPS

L'objectif est de calculer la  $PFD_{avg}$  du HIPS présenté à la section 4.3.3.1, à partir des paramètres caractéristiques imprécis tel que le taux de couverture de diagnostic et le facteur de DCC, en utilisant les chaînes de Markov floues multiphases [83], [85].

Comme nous l'avons déjà mentionné à la section 4.3.2.1 et afin de simplifier le modèle de Markov multiphases du HIPS, nous proposons de calculer la  $PFD_{avg}$  de chacun des sous-systèmes en série qui constituent le SIS et à les additionner pour obtenir la  $PFD_{avg}$  globale. En ne considérant que l'imprécision sur  $\beta$  et  $DC$ , nous allons évaluer leur influence sur la performance du HIPS.

#### 4.4.3.1 Approche des chaînes de Markov multiphase floue

La  $PFD_{avg}$  du SIS de la figure 4.1, est calculée par la combinaison de la probabilité de défaillance de tous les sous systèmes assurants ensemble la fonction de sécurité. La  $PFD$  est déterminée à partir des équations (4.39) et (4.40) [54], sous l'hypothèse d'occurrence des événements rares :

$$\tilde{P}_{HIPS}^{(\alpha)} = \tilde{P}_{Sens}^{(\alpha)} + \tilde{P}_{LS}^{(\alpha)} + \tilde{P}_{Act}^{(\alpha)} \quad (4.39)$$

$$\tilde{P}_{HIPS}^{(\alpha)} = \tilde{P}_{2oo3}^{(\alpha)} + \tilde{P}_{1oo1}^{(\alpha)} + \tilde{P}_{1oo2}^{(\alpha)} \quad (4.40)$$

En utilisant la méthode des chaînes de Markov multiphases floues proposée et celle des  $\alpha$ -coupes, la probabilité de défaillance du SIS à la sollicitation est déterminée à partir des distributions floues des paramètres caractéristiques de ses composants. Les paramètres caractéristiques des composants du HIPS sont donnés dans le tableau 4.2. Le facteur  $\beta$  de DCC ainsi que le taux de couverture  $DC$  de chaque sous ensemble est décrit par un triplet de paramètres  $\langle m_i, a_i, b_i \rangle$  fournis par des experts.

TABLE 4.2 – Paramètres caractéristiques des composants du HIPS

SIS Composants	$\lambda_D(h^{-1})$	DC	$\beta(\%)$	MTTR(h)	$T_i(h)$
$PT_i$	$7.00E - 6$	$\langle 0.5, 0.3, 0.7 \rangle$	$\langle 5, 3, 7 \rangle$	10	$T_1 = 730$
$SDV$	$4.66E - 6$	$\langle 0.2, 0.1, 0.4 \rangle$	$\langle 10, 9, 12 \rangle$	8	$T_2 = 1460$
$SV$	$4.66E - 6$	$\langle 0.2, 0.1, 0.4 \rangle$	$\langle 10, 9, 12 \rangle$	8	$T_2 = 1460$
<i>LogicSover</i>	$2.25E - 6$	$\langle 0.8, 0.7, 0.9 \rangle$	–	10	$T_3 = 2190$

Dans cette application, les intervalles de test sont différents à chaque sous système du SIS. Nous supposons ainsi que l'on teste fonctionnellement chaque sous-système indépendamment les uns des autres. La  $PF\tilde{D}_{avg}$  est calculée sur un intervalle de temps  $T_i$  lié à la fréquence de test du SIS.

La variation de la  $PF\tilde{D}_{avg}$  du HIPS, figure 4.1, est déterminée à partir de la combinaison de la probabilité de défaillance de tous les sous systèmes en utilisant les équations (4.39) et (4.40)).

La figure 4.10 montre l'évolution de la probabilité de défaillance à la sollicitation au cours du temps,  $P\tilde{F}D$  du HIPS étudié ainsi que sa valeur moyenne  $P\tilde{F}D_{avg}$  pour ( $\alpha = 0$  et  $\alpha = 1$ ). Les composants du système sont testés aux intervalles de temps précisés dans

le tableau 4.2.

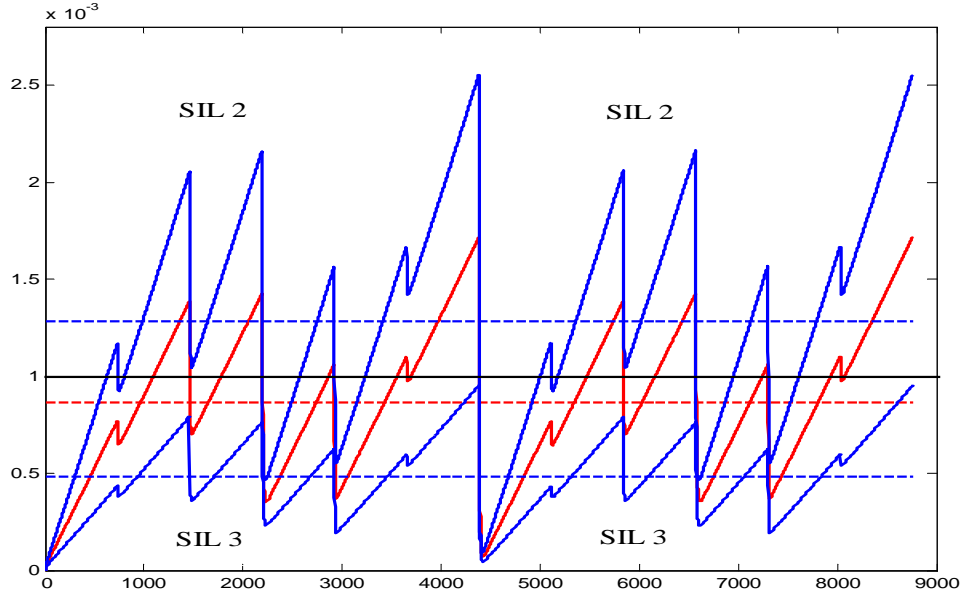


FIGURE 4.10 – Variation de la  $P\tilde{F}D$  du HIPS ainsi que sa  $P\tilde{F}D_{avg}$  pour ( $\alpha = 0$  et  $\alpha = 1$ )

La  $P\tilde{F}D$  du système est encadrée par des bornes supérieure et inférieure liées à l'intervalle défini par l' $\alpha$ -coupe de niveau 0. La propriété de monotonie dans l'inclusion de la fonction indisponibilité associée au SIS étudié, permet de garantir que les intervalles des  $\alpha$ -coupes de niveau supérieur à 0 sont égaux aux valeurs du support de la donnée à la figure 4.10.

Pour  $\alpha = 1$ , le HIPS passe plus de 60% de son temps dans le domaine de SIL 3, ce qui conduit à une valeur moyenne,  $PFD_{avg}^{(\alpha=1)}$ , égale à  $0.874 \times 10^{-3}$  et classe ce HIPS au niveau SIL 3. Pour  $\alpha = 0$ , la  $PFD$  résultante varie entre deux bornes. Dans le cas où la  $PFD$  est minimale, le HIPS passe tout son son temps dans le domaine de SIL 3, ce qui conduit à une valeur moyenne,  $PFD_{avg_L}^{(\alpha=0)}$ , égale à  $0.484 \times 10^{-3}$ . Alors que la variation de la  $PFD$  maximale permet de classer le HIPS au niveau SIL 2.

La  $P\tilde{F}D_{avg}$  du HIPS, est calculée pour chaque  $\alpha$ -coupe en utilisant l'équation (4.38). La figure 4.11 montre le nombre flou de type triangulaire représentant l'imprécision sur la  $PFD_{avg}$  du HIPS induite par l'imprécision des taux de couverture  $DC$  et des facteurs

$\beta$  de DCC.

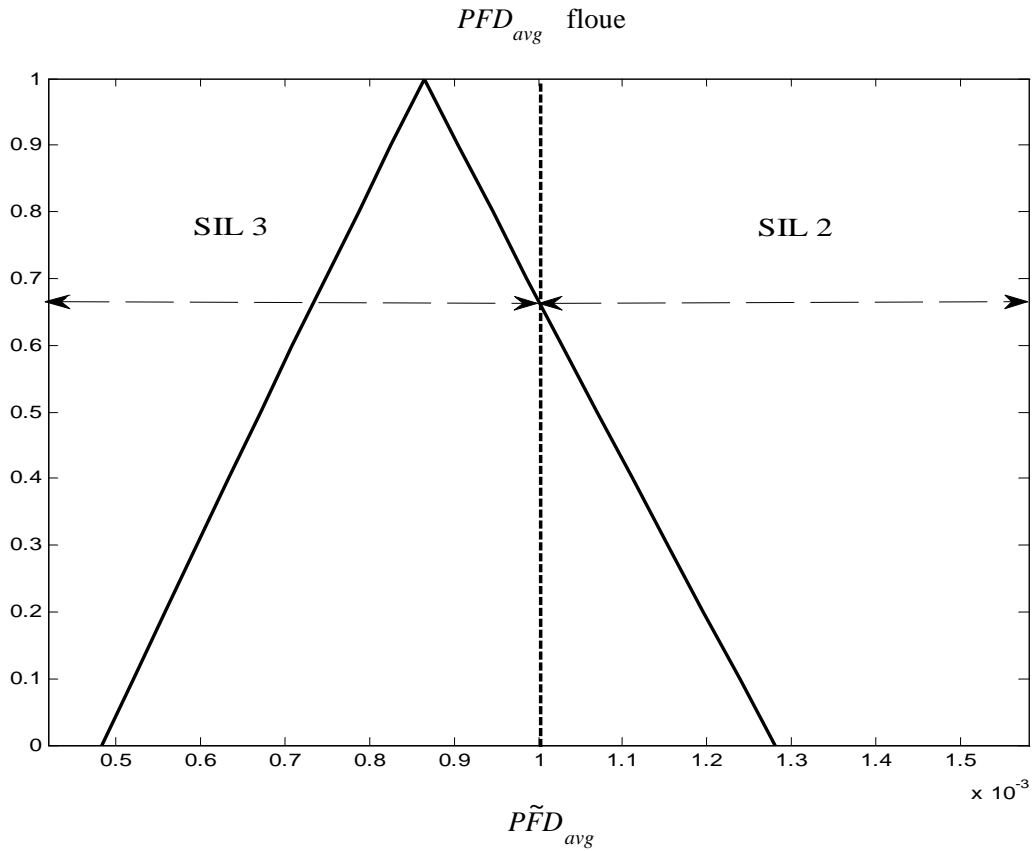


FIGURE 4.11 – La  $P\tilde{F}D_{avg}$  floue du HIPS étudié

La  $PF\tilde{D}_{avg}$  varie de  $0.484 \times 10^{-3}$  jusqu'à  $1.283 \times 10^{-3}$  pour ( $\alpha = 0$ ) ce qui correspond à niveau de confiance de 100%. Dans ce cas le niveau de sécurité du HIPS étudié varie d'un niveau de SIL3 à un niveau SIL2 (cf. tableau 1.1).

Le HIPS a un SIL 3 avec un niveau de confiance de 33% puisque pour ( $\alpha = 0.67$ ) , la  $PF\tilde{D}_{avg}^{(0.67)}$  varie de  $0.737 \times 10^{-3}$  jusqu'à  $0.998 \times 10^{-3}$ .

L'imprécision sur le facteur  $\beta$  de DCC et le taux de couverture  $DC$  amène à une variation du niveau SIL du HIPS. L'importance de l'imprécision sur la qualification des systèmes de sécurité mérite une attention toute particulière.

#### 4.4.3.2 Validation de l'approche floue par une approche aléatoire

Le problème d'imprécision sur les valeurs de  $DC$  et  $\beta$  pourrait être envisagé uniquement sous l'angle des probabilités avec des distributions de probabilités de second ordre.

En considérant les valeurs de  $\beta$  et DC dans une plage de valeurs correspondant au support des nombres flous (cf. Tableau 4.2). Le principe d'insuffisance de Laplace est appliqué et conduit à considérer des lois uniformes pour représenter l'imprécision des valeurs des taux DC et les facteurs  $\beta$  de DCC.

$$DC_i \rightarrow U(DC_{i,L}^{(\alpha)}, DC_{i,R}^{(\alpha)}) \quad (4.41)$$

$$\beta_i \rightarrow U(\beta_{i,L}^{(\alpha)}, \beta_{i,R}^{(\alpha)}) \quad (4.42)$$

Le tirage de Monte Carlo, permet aussi de déterminer les variations de la  $PFD_{avg}$  du SIS modélisée par les chaînes de Markov multiphases (cf. équations (4.7) - (4.21)) en utilisant l'approche par tirage de Monte Carlo.

A partir d'un tirage aléatoire de 2000 valeurs des paramètres DC et  $\beta$  représentés par des distributions uniformes (cf. équation ((4.41) et (4.42)). La distribution de la  $PFD_{avg}$  du HIPS pour ( $\alpha = 0$ ) est représentée à la figure 4.12.

La plage de variation de la  $PFD_{avg}$  obtenue par l'approche aléatoire est utilisée comme objet de comparaison avec les résultats déterminés par l'approche des chaînes de Markov floues.

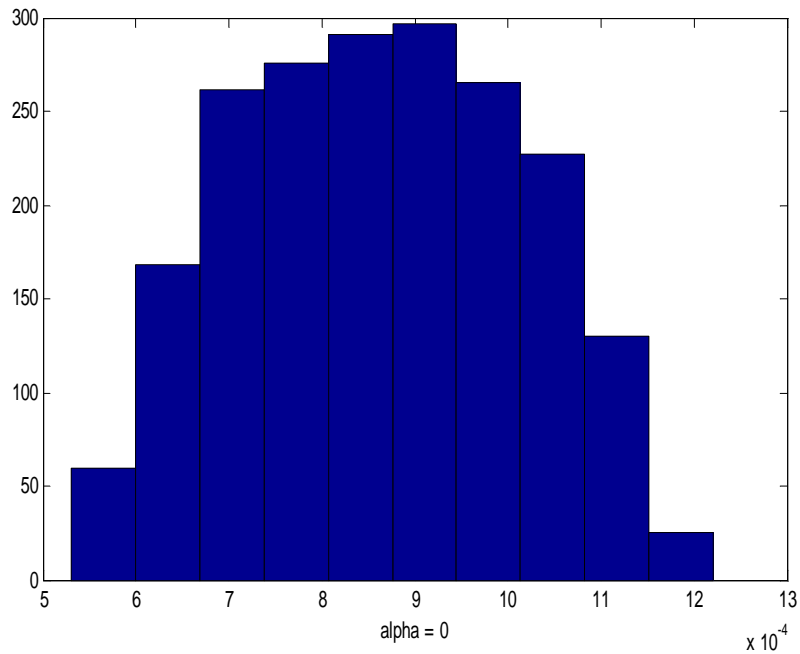


FIGURE 4.12 – Histogramme de la  $PFD_{avg}$  du tirage de Monte Carlo

La valeur des bornes inférieure et supérieure de la  $PFD_{avg}$  du HIPS appartient à l'intervalle  $[0.515 \times 10^{-3}, 1.261 \times 10^{-3}]$ . Le support de la  $P\tilde{F}D_{avg}$  floue (cf. figure 4.11) contient les bornes supérieure et inférieure des probabilités obtenues par tirage de Monte Carlo. Pour obtenir des valeurs exactes des bornes du support de la  $P\tilde{F}D_{avg}$ , il est nécessaire d'augmenter considérablement le nombre de tirages.

#### 4.4.3.3 Comparaison entre l'approche proposée et l'approche aléatoire

En effet, comme le montre la figure 4.13, plus le nombre de tirage Monte Carlo augmente plus les bornes de la  $PFD_{avg}$  résultante convergent vers les valeurs exactes des bornes calculées par l'approche floue proposée [10].

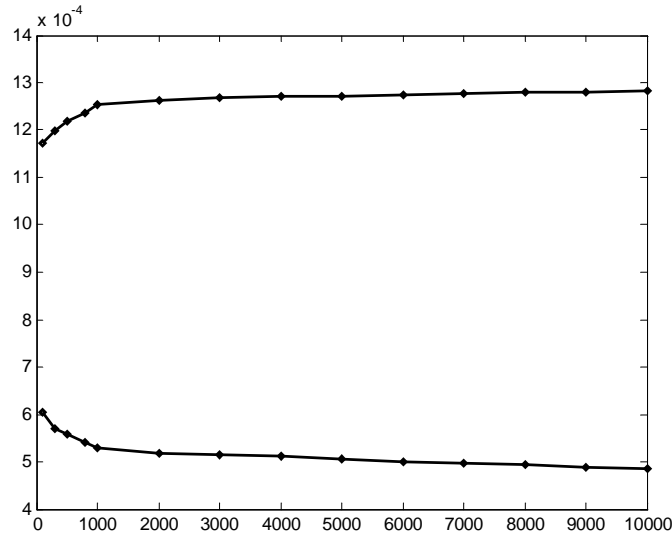


FIGURE 4.13 – Convergence des bornes estimées de la  $PFD_{avg}$  en fonction du nombre de tirage

On réalise un tirage de Monte Carlo de 2000 valeurs pour différentes valeurs de  $\alpha$ . Pour chaque  $\alpha$ -coupe on détermine les bornes supérieure et inférieure de la  $PFD_{avg}$  du HIPS à partir du tirage aléatoire de ces paramètres caractéristiques imprécis modélisés par des distributions de probabilités uniformes.

Pour les différentes valeurs de  $\alpha$ , nous comparons la  $PFD_{avg}$  du HIPS par la méthode des chaînes de Markov floues et par la simulation de Monte Carlo, comme le montre la figure 4.14.

Les bornes de la  $PFD_{avg}$  déterminées par la simulation de Monte Carlo convergent vers les valeurs obtenues par la méthode des chaînes de Markov multiphases floue proposée. Ce point montre la pertinence de l'approche floue en termes d'exactitude des résultats

et d'efficacité.

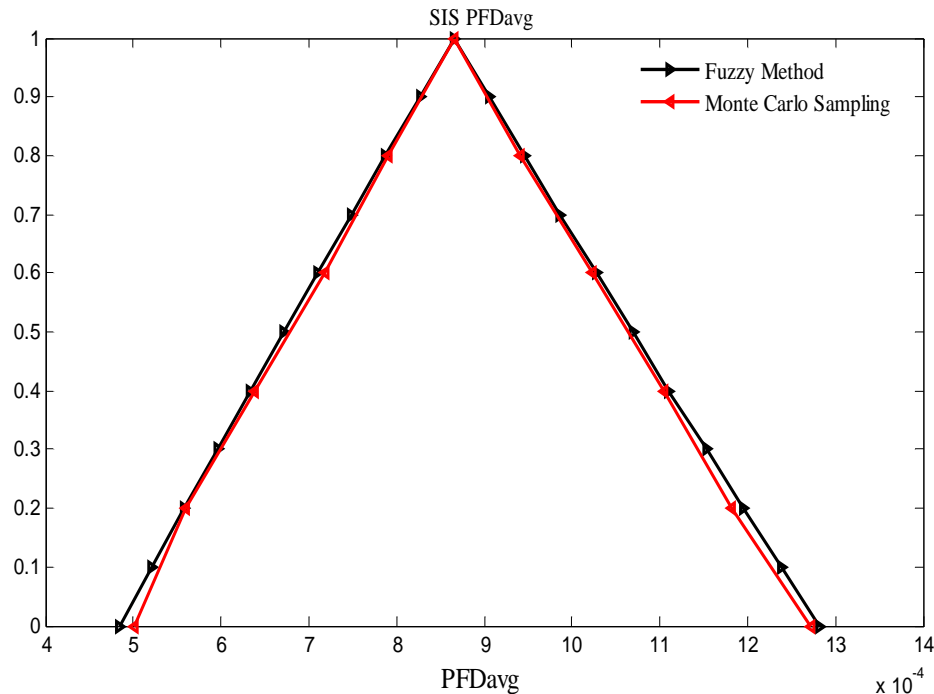


FIGURE 4.14 – Comparaison entre l'approche floue et aléatoire

L'approche proposée est basée sur l'utilisation des nombres flous au sein des chaînes de Markov multiphases a permis d'évaluer la performance la  $PFD_{avg}$  des HIPS à paramètres imprécis. Le choix de nombres flous triangulaires correspond à la formulation linguistique de l'imprécision par les experts mais peut être largement étendu à toute autre forme (trapézoïdales, gaussiennes ...). L'approche a aussi montré l'impact de l'imprécision des paramètres de défaillances sur l'imprécision de la performance du HIPS.

## 4.5 Conclusion

Les chaînes de Markov constituent un outil de quantification pour la modélisation des SIS réparables et faiblement sollicités. L'évaluation d'un SIS s'apparente au calcul de l'indisponibilité de sa fonction de sécurité à la sollicitation.

La première proposition consiste à remplacer les probabilités de transition dans les chaînes de Markov par des intervalles. En se basant sur l'arithmétique d'intervalles, les performances peuvent être déterminées sous formes d'intervalles. Cette méthode a été appliquée pour l'évaluation de la  $PFD_{avg}$  d'un HIPS. Les résultats obtenus ont été validé

par une simulation de Monte Carlo.

Dans la deuxième approche les probabilités de transition des chaînes de Markov sont des nombres flous découpés en  $\alpha$ -coupes. Le calcul des probabilités de transition se ramène au calcul d'intervalles. La résolution des équations ainsi déterminées conduit à l'évaluation du SIS. Cette méthode a été appliquée pour l'évaluation de la  $PFD_{avg}$  d'un HIPS. Les résultats obtenus ont été validés par la simulation de Monte Carlo. L'intervalle donné par Monte Carlo est contenu dans celui de l'approche floue proposée.

# Conclusion générale

La norme IEC 61508 est la norme de référence pour la spécification et la conception des SIS. Sa déclinaison sectorielle dans le domaine du process industriel est destinée aux concepteurs et utilisateurs de ce domaine. Ces normes de sécurité fonctionnelle introduisent une approche probabiliste pour l'évaluation quantitative de la performance du SIS et la qualification de cette performance par des niveaux de sécurité référencés.

L'introduction de probabilité dans la mesure de niveau d'intégrité a entraîné la mise en place de nouveaux concepts tels que les notions de calculs de probabilité moyenne de défaillance à la sollicitation  $PF D_{avg}$  ou de défaillance par unité de temps. Différentes techniques sont néanmoins préconisées dans les annexes de la norme sans toutefois exclure toute méthode pertinente de calcul probabiliste. Parmi les méthodes citées, on trouve les arbres de défaillances, les blocs diagramme fiabilité ainsi que les chaînes de Markov. La performance ainsi calculée permet alors de qualifier le niveau SIL du SIS selon les niveaux définis par la norme qui en sont l'un des points clés. Cette évaluation s'apparente à un calcul d'indisponibilité de la fonction de sécurité.

Pour La représentation des informations imparfaites les méthodes qu'on a étudiées se basent sur l'une des théories suivantes ; probabilités, intervalles, ensembles flous, familles des probabilités cumulées (p-boxes), . . . Les méthodes d'évaluation développées pour la modélisation des SIS se basent particulièrement sur l'arbre de défaillances et sur les chaînes de Markov.

L'utilisation des arbres de défaillances pour l'évaluation des performances des systèmes à paramètres imprécis peut se faire soit par la méthode de Singer ou par la méthode des  $\alpha$ -coupes. L'évaluation des performances des systèmes réparables représentés par les chaînes de Markov à paramètres flous, peut être obtenue par :

- Les chaînes de Markov à états non flous et probabilités de transitions floues.
- La méthode des  $\alpha$ -coupes.
- Le modèle de Markov avec système d'inférence flou.

L'évaluation des SIS peut se faire par l'utilisation d'une approche probabiliste floue. La probabilité floue est caractérisée par une fonction d'appartenance triangulaire et l'intervalle est défini par ses bornes. La combinaison des probabilités floues et intervalles donne plusieurs intervalles emboîtés (méthode des  $\alpha$ -coupes). Dans ce contexte deux approches

---

ont été proposé :

- La première se base sur l'arbre de défaillances et sur la méthode des  $\alpha$ -coupes. Chaque probabilité floue d'un évènement de base est décrite par un ensemble d'intervalles. Cette méthode est appliquée à un HIPS dans les cas ; les systèmes sont testés simultanément et à des intervalles de temps différents. Les résultats obtenus par cette méthode ont été validés par une approche de simulation de Monte Carlo.
- La deuxième proposition concerne l'extension des travaux de Ferson (la théorie des p-boxes) à l'évaluation de la  $PFD_{avg}$  d'un SIS en se basant sur son arbre de défaillances. Cette méthode a été appliquée et a montré que les imprécisions sur les valeurs des facteurs de DCC conduisent à la variation du niveau SIL du SIS.

Dans la dernière partie de ce travail on s'est intéressé à l'évaluation des SIS modélisés par les chaînes de Markov. Elles constituent un outil de quantification de la performance des SIS réparables et faiblement sollicités. L'évaluation d'un SIS s'apparente au calcul de l'indisponibilité de sa fonction de sécurité à la sollicitation. Dans ce cadre deux approches d'évaluation ont été proposées.

- La première proposition consiste à remplacer les probabilités de transition dans les chaînes de Markov par des intervalles. En se basant sur l'arithmétique d'intervalles, les performances peuvent être déterminées sous formes d'intervalles. Cette méthode a été appliquée pour l'évaluation de la  $PFD_{avg}$  d'un HIPS. Les résultats obtenus ont été validé par une simulation de Monte Carlo.
- Dans la deuxième approche les probabilités de transition des chaînes de Markov sont des nombres flous découpés en  $\alpha$ -coupes. Le calcul des probabilités de transition se ramène au calcul d'intervalles. La résolution des équations ainsi déterminées conduit à l'évaluation du SIS. Cette méthode a été appliquée pour l'évaluation de la  $PFD_{avg}$  d'un HIPS. Les résultats obtenus ont été validés par la simulation de Monte Carlo. L'intervalle donné par Monte Carlo est contenu dans celui de l'approche floue proposée.

Il serait important d'étendre les calculs à la théorie de Dempster-Shafer et de discuter son intégration surtout dans l'approche Markovienne. Cette théorie peut être utilisée pour l'évaluation des performances des SIS à paramètres incertains.

Une autre perspective intéressante, il s'agit d'utiliser d'autres méthodes de sûreté de fonctionnement pour l'évaluation des performances des SIS en présence d'informations imparfaites comme les réseaux de Petri ou les réseaux bayésiens.

# Bibliographie

## A

---

- [1] Augustin, T., Miranda, E., and Vejnarová, J. (2009). Imprecise probability models and their applications. *International Journal of Approximate Reasoning*, 50(4) :581 – 582. Imprecise Probability Models and their Applications (Issues in Imprecise Probability).
- [2] Avrachenkov, K. E. and Sanchez, E. (2002). Fuzzy markov chains and decision-making. *Fuzzy Optimization and Decision Making*, 1(2) :143–159.

## B

---

- [3] Barros, A., Grall, A., and Vasseur, D. (2009). Estimation of common cause failure parameters with periodic tests. *Nuclear engineering and Design*, 239(4) :761–768.
- [4] Baudrit, C. (2007). *Représentation et propagation de connaissances imprécises et incertaines : application à l'évaluation des risques liés aux sites et aux sols pollués*. PhD thesis, Université de Toulouse III Paul Sabatier, France.
- [5] Baudrit, C., Guyonnet, D., and Dubois, D. (2007). Joint propagation of variability and imprecision in assessing the risk of groundwater contamination. *Journal of Contaminant Hydrology*, 93(1-4) :72–84.
- [6] Berleant, D. (1993). Automatically verified reasoning with both intervals and probability density. *Interval Computations*, 2 :48–70.
- [7] Berleant, D. and Goodman-Strauss, C. (1998). Bounding the results of arithmetic operations on random variables of unknown dependency using intervals. *Reliable Computing*, 4(2) :147–65.
- [8] Berleant, D., Xie, L., and Zhang, J. (2003). Statool : A tool for distribution envelope determination (denv), an interval-based algorithm for arithmetic on random variables. *Reliable Computing*, 9(2) :91–108.
- [9] Berleant, D. and Zhang, J. (2004a). Bounding the times to failure of 2-component systems. *IEEE Transactions on Reliability*, 53(4) :542–550.
- [10] Berleant, D. and Zhang, J. (2004b). Representation and problem solving with distribution envelope determination (denv). *Reliability Engineering & System Safety*, 85(3) :153–168.
- [11] Beugin, J. (2006). *Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé*. PhD thesis, Université de Valenciennes et du Hainaut-Cambrésis, France.

- 
- [12] Beugin, J., Renaux, D., and Cauffriez, L. (2007). A sil quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems. *Reliability Engineering and System Safety*, 92 :16861700.
  - [13] Bhattacharyya, M. (1999). Fuzzy markovian decision process. *Fuzzy Sets and Systems*, 99(3) :273 – 282.
  - [14] Bouchon-Meunier, B. (1995). *La logique floue et ses applications. Vie artificielle*.
  - [15] Brissaud, F. and Lanternier, B. (2009). Les probabilités de défaillances comme indicateurs de performances des barrières techniques de sécurité approche analytique. In *8ème édition du congrès international QUALITA 2009 Besançon (France)*.
  - [16] Buckley, J. (2005). *Fuzzy Probabilities : New Approach and Applications (Studies in Fuzziness and Soft Computing)*. Springer-Verlag New York, Inc.
  - [17] Buckley, J. and Eslami, E. (2002). Fuzzy markov chains : Uncertain probabilities. *MathWare and Soft Computing*, 9(4) :33–41.
  - [18] Bukowski, J. (2001). Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems. *IEEE Trans Reliab*, 50(3) :321329.

## C

---

- [19] Cepin, M. (1995). Sequentiel versus staggered testing towards dynamic psa. In *Proceedings of the second regional meeting on nuclear energy in Central Europe*, pages 184–9.
- [20] Charpentier, P. (2002). *Architecture d’automatisme en sécurité des machines : Etude des conditions de conception liées aux défaillances de mode commun*. PhD thesis, Nancy Université, Institut National Polytechnique de Lorraine, France.
- [21] Coolen, F. and Utkin, L. (2007). *Imprecise reliability : A concise overview*, chapter 10, pages 1959–1966.
- [22] Crossman Richard J., Coolen-Schrijner Pauline, S. D. C. F. P. (2009). Imprecise markov chains with an absorbing state. In *6th International Symposium on Imprecise Probability : Theories and Applications*. Durham, United Kingdom.

## D

---

- [23] Dempster., A. P. (1967). Upper and lower probabilities induced by a multivalued mapping. *annals of mathematical statistics. Reliability Engineering and System Safety*, 38(12) :325339.
- [24] Desroches, A., Leroy, A., and Vallée, F. (2003). *La gestion des risques : principes et pratiques*, volume 1. Lavoisier, France.
- [25] Dixon, W. (2007). Uncertainty propagation in population level salinity risk models. Technical Report 164, Arthur Rylah. Institute for Environmental Research, Melbourne, Australia.
- [26] Dubois, D., Foulloy, L., Mauris, G., and Prade, H. (2004). Probability-possibility transformations, triangular fuzzy sets, and probabilistic inequalities. *Reliable computing*, 10 :273–297.

- 
- [27] Dubois, D. and Prade, H. (1988). *Possibility theory. an approach to computerized processing of uncertainty*. Plenum Press.
- [28] Dubois, D. and Prade., H. (1994). *Traitement du Signal*, chapter La fusion d'informations imprécises, page 447458.
- [29] Dubois, D. and Prade, H. (2006). *Concepts et Méthodes pour laide à la décision*, volume 1, chapter Représentation formelle de lincertain et de limprécis.
- [30] Dutuit, Y., Innal, F., Rauzy, A., and Signoret, J.-P. (2008). Probabilistic assessments in relationship with safety integrity levels by using fault trees. *Reliability Engineering and System Safety*, 93(12) :1867–1876.

## E

---

- [31] EN50126 (1999). *Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS)*.
- [32] EN50128 (2001). *Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems*.
- [33] EN50129 (1998). *Safety related electronic systems for signalling*.
- [34] Exida. *Safety Equipment Reliability Handbook*. 2nd Edition.

## F

---

- [35] Farmer., F. R. (1967). *Siting criteria : a new approach*. *Atom*, chapter 128, page 152166.
- [36] Ferdous, R., Khan, F., Veitch, B., and Amyotte, P. R. (2009). Methodology for computer aided fuzzy fault tree analysis. *Process Safety and Environmental Protection*, 87(4) :217–226.
- [37] Ferson, S. and Hajagos, J. (2004). Arithmetic with uncertain numbers : rigorous and (often) best-possible answers. *Reliability Engineering and System Safety*, 85(5) :135–152.
- [38] Ferson, S., Kreinovich, V., Ginzburg, L., Myers, D., and Sentz, K. (2002). Constructing probability boxes and dempster-shafer structures. Technical report, Sandia National Laboratory, Tech. Rep.
- [39] Ferson, S., Kreinovich, V., Hajagos, J., Oberkamp, W., and Ginzburg, L. (2007). Experimental uncertainty estimation and statistics for data having interval uncertainty. Technical Report 5, SAND2007-0939, Sandia National Laboratories, Albuquerque, NM.
- [40] Fetz, T. and Oberguggenberger, M. (2004). Propagation of uncertainty through multivariate functions in the framework of sets of probability measures. *Reliability Engineering and System Safety*, 85 :73–87.
- [41] Fleming, K. (1974). A reliability model for common mode failures in redundant systems. Technical report.

---

## G

---

- [42] Goble, W. M. and Brombacher, A. C. (1999). Using a failure modes, effects and diagnostic analysis (fmeda) to measure diagnostic coverage in programmable electronic systems. *Reliability Engineering and System Safety*, 66(2) :145 – 148.
- [43] Goble, W. M. and Cheddie., H. (2006). Safety instrumented systems verification-practical probabilistic calculations. Technical report, ISA.
- [44] Guo, H. and Yang, X. (2006). A simple reliability block diagram method for safety integrity verification. *Reliability Engineering and System Safety*, 92 :12671273.
- [45] Guo, H. and Yang, X. (2008). Automatic creation of markov models for reliability assessment of safety instrumented systems. *Reliability Engineering and System Safety*, 93 :807815.
- [46] Guth, M. A. (1991.). A probability foundation for vagueness and imprecision in fault tree analysis. *IEEE Transactions on Reliability*, 40 :563570.

---

## H

---

- [47] Hauge, S., Hokstad, P., Langseth, H., and Oien, K. (2006). Reliability prediction method for safety instrumented systems. Technical report.
- [48] Helton, J. C. and Oberkampf, W. L. (2004). Alternative representations of epistemic uncertainty. *Reliability Engineering and System Safety*, 85 :110.
- [49] Hoepfer, V., Saleh, J., and Marais, K. (2009). On the value of redundancy subject to common-cause failures : Toward the resolution of an on-going debate. *Reliability Engineering & System Safety*, 94(12) :1904 – 1916.
- [50] Hokstad, P. and Rausand, M. (2008). Common cause failure modeling : status and trends. In Misra, K. B., editor, *Handbook of Performability Engineering*, chapter 39, pages 621–640. Springer London.
- [51] Houtermans, M. and Rouvroye, J. (2005). The influence of design parameters on the probability of failure on demand (pfd) performance of safety instrumented systems (sis). Technical report, Electronic.
- [52] Humphreys, R. A. (1987). Assigning a numerical value to the beta factor common cause evaluation. In *Proceedings of the National Reliability Conference*.

---

## I

---

- [53] Ibanez-Llano, C., Rauzy, A., Meléndez, E., and Nieto, F. (2009). Minimal cut sets-based reduction approach for the use of binary decision diagrams on probabilistic safety assessment fault tree models. *Journal of Risk and Reliability*, 223(4) :301311.
- [54] IEC61508 (1998). *Functional safety of electrical/electronic/programmable electronic (e/e/pe) safety related systems*. International Electrotechnical Commission (IEC).
- [55] IEC61511 (2000). *Functional safety : Safety instrumented systems for the process industry sector*.

- 
- [56] IEC61513 (2001). *Centrales nucléaires : Instrumentation et contrôle commande des systèmes importants pour la sûreté, Prescriptions générales pour les systèmes*. International Electrotechnical Commission (IEC).
- [57] IEC62061 (2005). *Sécurité des machines : Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*. International Electrotechnical Commission (IEC).
- [58] Innal, F. (2008). *Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances Analyse critique de la norme CEI 61508*. PhD thesis, Université Bordeaux I, France.
- [59] Innal, F., Dutuit, Y., and Rauzy, A. (2006). Quelques interrogations et commentaires relatifs à la norme cei 61508. In *In Proceedings of the Lambda Mu 2006 Conference, Lille, France*.
- [60] Innal, F., Dutuit, Y., Rauzy, A., and Signoret, J.-P. (2010). New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, 224.
- [61] ISA-TR84 (2002). *ISA-TR84.00.02. Safety Instrumented Functions (SIF) - Safety Integrity Levels (SIL) Evaluation Techniques*. The Instrumentation, Systems, and Automation Society, 67 Alexander Drive P.O. Box 12277 Research Triangle Park, North Carolina 27709.

## J

---

- [62] Jaulin., L. (2000). Le calcul ensembliste par analyse par intervalles et ses applications. In *Habilitation à diriger des recherches, Université d'Angers*.
- [63] Jaulin, L., Kieffer, M., Didrit, O., and Walter, E. (2001). *Applied interval analysis*. Springer Verlag.
- [64] Jaynes, E. (2003). *Probability Theory : The Logic of Science*, volume 16. Cambridge University Press.
- [65] Jin, H., Lundteigen, M., and M.Rausand (2011). Reliability performance of safety instrumented systems : A common approach for both low-and high-demand mode of operation. *Reliability Engineering and System Safety*, 96 :365–373.
- [66] Jones, B., Jenkinson, I., and Wang, J. (2010). The use of fuzzy set modelling for maintenance planning in a manufacturing industry. *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, 224(1) :35–48.

## K

---

- [67] Kaucher, E. (1980). *Interval Analysis in the Extended Interval Space IR*, volume 2. Computing Suupl.
- [68] Kaufman, A. and Gupta, M. M. (1991.). *Introduction to Fuzzy Arithmetic Theory and Application*. Van Nostrand Reinhold Company, New York.

- 
- [69] Kozine, I. and Utkin, L. (2002). Interval valued finite markov chains. *Reliable computing*, 8 :97113.
- [70] Kruse, R., Buck-Emden, R., and Cordes, R. (1987). Processor power considerations – an application of fuzzy markov chains. *Fuzzy Sets and Systems*, 21(3) :289 – 299.

## L

---

- [71] Lamy, P. (2002). Probabilité de défaillance dangereuse d’un système : explications et exemple de calcul. Note Scientifique et Technique 225, Institut national de recherche et sécurité (INRS).
- [72] Lanternier, B. and Dranguet, J.-M. (2007.). Maintenance optimization of sensors for certification in compliance with the iec 61511 standard. In Aven, T. and Druijm, editors, *Safety En.*
- [73] Lilleheier, T. (2008). Analysis of common cause failures in complex safety instrumented systems. Master’s thesis, Norwegian University of Science and Technology.
- [74] Lilleheier, T. and Brissaud, F. (2009). Modélisation des causes communes de défaillances d’un système instrumenté de sécurité particulier. In *8ème édition du congrès international QUALITA 2009 Besançon (France)*.
- [75] Limbourg, P., Savic, R., Petersen, J., and Kochs, H.-D. (2008). Modelling uncertainty in fault tree analyses using evidence theory. *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, 222(3) :291–302.
- [76] Liu, Y. and Rausand, M. (2011). Reliability assessment of safety instrumented systems subject to different demand modes. *Journal of Loss Prevention in the Process Industries*, 24 :49–56.
- [77] Lundteigen, M. A. and Rausand, M. (2007). Common cause failures in safety instrumented systems on oil and gas installations : Implementing defense measures through function testing. *Journal of Loss Prevention in the Process Industries*, 20(3) :218 – 229.

## M

---

- [78] Marshall, F., Rasmuson, D., and Mosleh, A. (1998). Common-cause failure parameter estimations. Technical report, Washington DC : US Nuclear Regulatory Commission, NUREG/CR-5497.
- [79] Mazouni, M.-H. (2008). *Pour une Meilleure Approche du Management des Risques : De la modélisation Ontologique du Processus Accidentel au Système Interactif d’Aide à la Décision*. PhD thesis, Nancy Université, Institut National Polytechnique de Lorraine, France.
- [80] Mechri, W. and BenOthman, K. (2010). Probabilistic fuzzy approach for the imprecise evaluation of safety instrumented systems. *International Review of Modeling and Simulation*, 3(3) :388–400.
- [81] Mechri, W., Simon, C., and BenOthman, K. Uncertainty analysis of common cause failure in safety instrumented systems. *Journal of Risk and Reliability. Professional Engineering Publishing*.

- 
- [82] Mechri, W., Simon, C., BenOthman, K., Aubry, J.-F., and Benrejeb, M. (2009a). Evaluation imprécise de l'indisponibilité des systèmes par chaînes de markov floues. In *Congrès Performances et Nouvelles Technologies en Maintenance, Autrans Grenoble*.
- [83] Mechri, W., Simon, C., BenOthman, K., and Benrejeb, M. (2010a). Chaînes de markov floues multi-phases pour l'évaluation de la performance imprécise des systèmes instrumentés de sécurité. In *la Sixième Conférence Internationale Francophone d'Automatique Nancy, CIFA 2010, Nancy, France*.
- [84] Mechri, W., Simon, C., BenOthman, K., and Benrejeb, M. (2011a). Evaluation des performances imprécises des sis par des familles de densités de probabilités. In *Proceedings of the QUALITA 2011 Conference, Angés, France*.
- [85] Mechri, W., Simon, C., BenOthman, K., and Benrejeb, M. (2011b). Uncertainty evaluation of safety instrumented systems by using markov chains. In *IFAC World Congress, Milano, Italy*.
- [86] Mechri, W., Simon, C., Othman, K. B., Aubry, J.-F., and Benrejeb, M. (2009b). Chaîne de markov mutiphases à intervalle pour l'évaluation de performance des sis. In *Proceedings of the QUALITA 2009 Conference, Besançon, France*.
- [87] Mechri, W., Simon, C., Othman, K. B., and Benrejeb, M. (2010b). Analyse de l'imprécision de taux de défaillance de cause commune pour l'évaluation des performances des sis. In *8ème Conférence Internationale de Modélisation et Simulation Modélisation, Hammamet, Tunisie*.
- [88] Mkhida, A. (2008). *Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'Intelligence*. PhD thesis, Nancy Université, Institut National Polytechnique de Lorraine, France.
- [89] Moore, R. (1966). *Interval Analysis*. Prentice-Hall, New York.
- [90] Moore, R. (1979). *Studies in Applied Mathematics. SIAM*, chapter Methods and applications of interval analysis.
- [91] Mosleh, A. and Siu, N. (1987). A multiparameter event based common cause failure model. *Proceedings of the 9th international conference on structural mechanics in reactor technology*, (2) :147152.

## N

---

- [92] Neumaier, A. (1990). *Interval methods for systems of equations*. Number 2. Cambridge University Press.
- [93] Neumaier, A. (2004). Clouds, fuzzy sets and probability intervals. *Reliable Computing*, 10(4) :249272.

## O

---

- [94] OHSAS18001 (1999). *Système de management de la santé et de la sécurité au travail - Spécification - BSI, Afnor*.
- [95] OREDA (2009). *Offshore reliability data handbook, 5th Edition*.

---

## R

---

- [96] Rausand, M. and Hoyland, A. (2004). *System Reliability Theory; Models, Statistical Methods and Applications*. New York, Wiley, 2nd edition.
- [97] Rauzy, A. (1993). New algorithms for fault trees analysis. *Reliability Engineering & System Safety*, 59(5) :203–211.
- [98] Rauzy, A., Dutuit, Y., and Signoret, J.-P. (2006). Assessment of safety integrity levels with fault trees. In *ESREL Estoril, Portugal*.
- [99] Rauzy, A., Gauthier, J., and Leduc, X. (2007.). Assessment of large automatically generated fault trees by means of binary decision diagrams. *Journal of Risk and Reliability. Professional Engineering Publishing.*, 221(2) :95105.
- [100] Regan, H., Ferson, S., and Berleant, D. (2004). Equivalence of methods for uncertainty propagation of real-valued random variables. *International Journal of Approximate Reasoning*, 36(1) :1–30.

## S

---

- [101] Sallak, M. (2007). *Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité*. PhD thesis, Nancy Université, Institut National Polytechnique de Lorraine, France.
- [102] Sallak, M., Simon, C., and Aubry, J.-F. (2006a). Aide à la décision dans la réduction de l'incertitude des sil : une approche floue/possibiliste. *e-STA, Revue des Sciences et Technologies de l'Automatique*.
- [103] Sallak, M., Simon, C., and Aubry, J.-F. (2006.b). Evaluating safety integrity level in presence of uncertainty. In *In KONBiN 2006, The 4th International Conference on Safety and Reliability, Krakow, Poland*.
- [104] Sallak, M., Simon, C., and Aubry, J.-F. (2008). A fuzzy probabilistic approach for determining safety integrity level. *IEEE Transactions on Fuzzy Systems*, 16(1) :239–248.
- [105] Sandri, S. (1991). *La combinaison de l'information incertaine et ses aspects algorithmiques*. PhD thesis, Université Paul Sabatier, Toulouse, France.
- [106] Schonbeck, M., Rausand, M., and Rouvroye, J. (2010). Human and organisational factors in the operational phase of safety instrumented systems : A new approach. *Safety Science*, 48 :310–318.
- [107] Signoret, J.-P. Analyse des risques des systèmes dynamiques : approche markovienne. Technical report, Techniques de l'Ingénieur.
- [108] Signoret, J.-P. (1986). Etude probabiliste des systèmes périodiquement testés. Technical report, rapport DGEP/SES/ARF/JPS/co no. 86, 009 ELF Aquitaine Production.
- [109] Signoret, J.-P. (2004). High integrity protection system (hips)overcoming sil calculation difficulties. Technical report, TOTAL document, Pau.
- [110] Signoret, J. P. (2005). Methodology sil evaluations related to hips. Technical report, Total, Draft Memo.

- 
- [111] Signoret, J.-P. (2006). Managing risks in hips by making sil calculations effective. In *IQPC2006, Aberdeen, Great Britain*.
- [112] Signoret, J.-P., Dutuit, Y., and Rauzy, A. (2007). High integrity protection systems (hips) : Methods and tools for efficient safety integrity levels (sil) analysis and calculations. In *Risk, Reliability and Societal Safety Aven and Vinnem (eds)*.
- [113] Simon, C., Sallak, M., and Aubry., J.-F. (2007). Sil allocation of sis by aggregation of experts opinions. In *ESREL, Safety and Reliability Conference, Stavanger, Norvège*.
- [114] Simon, C. and Weber, P. (2009). Imprecise reliability by evidential networks. *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, 223(2) :119–131.
- [115] Singer, D. (1990). A fuzzy set approach to fault tree and reliability analysis. *Fuzzy Sets and Systems*, 34(2) :145–155.
- [116] Skulj, D. (2009). Discrete time markov chains with interval probabilities. *International Journal of Approximate Reasoning*, 50(8) :1314 – 1329. Special Section on Interval/Probabilistic Uncertainty.
- [117] Soman, K. P. and Misra, K. B. (1993). Fuzzy fault tree analysis using resolution identity. *The Journal of Fuzzy Mathematics*, pages 193–212.
- [118] Stojakovic, M. (2010). Imprecise set and fuzzy valued probability. *Journal of Computational and Applied Mathematics*, In Press, Corrected Proof :–.
- [119] Summers, A., Ford, K., and Raney, G. (1999). Estimation and evaluation of common cause failures. Houston, Texas. Loss Prevention Symposium, American Institute of Chemical Engineers Spring Meeting.
- [120] Symeonaki, M. A. and Stamou, G. B. (2004). Theory of markov systems with fuzzy states. *Fuzzy Sets and Systems*, 143(3) :427 – 445.

## T

---

- [121] Tanaka, H., Fan, L. T., Lai, F. S., and Toguchi, K. (1983). Fault tree analysis by fuzzy probability. *IEEE Transactions on Reliability*, 32 :453457.
- [122] Tanrioven, M., Wu, Q., Turner, D., Kocatepe, C., and Wang, J. (2004). A new approach to real-time reliability analysis of transmission system using fuzzy markov model. *International Journal of Electrical Power & Energy Systems*, 26(10) :821 – 832.
- [123] Torres-Echeverr, A., Martorell, S., and Thompson, H. (2009). Modelling and optimization of proof testing policies for safety instrumented systems. *Reliability Engineering and System Safety*, 94(4) :838 – 854.
- [124] Torres-Echeverria, A. and Thompson, H. (2007). Multi-objective genetic algorithm for optimization of system safety and reliability based on iec 61508 requirements : a practical approach. *Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability*, 221(3) :193–205.
- [125] Tucker, W. and Ferson, S. (2003). Probability bounds analysis in environmental risk assessment. In *Applied Biomathematics, Setauket, New York*.

---

## U

---

- [126] Utkin, L. and Coolen, F. (2007). *New metaheuristics, neural and fuzzy techniques in reliability*, volume 2, chapter Imprecise reliability : An introductory overview, pages 261–306. Computational intelligence in reliability engineering.

## V

---

- [127] Vaurio, J. (2007). Consistent mapping of common cause failure rates and alpha factors. *Reliability Engineering and System Safety*, 92(5) :628 – 645.
- [128] Velten-Philipp, W. and Houtermans, M. (2005). The effect of diagnostic and periodic testing on the reliability of safety systems. Technical report, Electronic.
- [129] Villemeur, A. (1987). *Evaluation de la fiabilité, disponibilité et maintenabilité des systèmes réparables : la méthode de l'Espace des Etats*. Number 2. Eyrolles.
- [130] Villemeur, A. (1998). *Sûreté de fonctionnement des systèmes industriels*. Number 2. Eyrolles.

## W

---

- [131] Walley, P. (1991). *Statistical Reasoning with Imprecise Probabilities*, volume In Press, Corrected Proof. Chapman and Hall, London.
- [132] Wang, J. and Qiu, Z. (2010). The reliability analysis of probabilistic and interval hybrid structural system. *Applied Mathematical Modelling*, In Press, Corrected Proof :—.
- [133] Wang, Y., West, H. H., and Mannan., M. S. (2004). The impact of data uncertainty in determining safety integrity level. *Process Safety and Environmental Protection*, 82 :393397.
- [134] Williamson, R. and Downs, T. (1990). Probabilistic arithmetic i : Numerical methods for calculating convolutions and dependency bounds. *International Journal of Approximate Reasoning*, 4 :89–158.

## Y

---

- [135] Yager, R. R. (1986). Arithmetic and other operations on dempster-shafer structures. *International Journal of Man-Machine Studies*, 25(5) :357–366.

## Z

---

- [136] Zadeh, L. (1965). *Fuzzy sets*. Information and control.
- [137] Zadeh, L. (1968). Probability measures of fuzzy events. *J. Math. Anal. Appl*, 23 :421427.
- [138] Zadeh, L. (1998). Maximizing sets and fuzzy markov algorithmsmaximizing sets and fuzzy markov algorithms. *IEEE Trans. on Systems*, 28 :915.
- [139] Zhang, T., Long, W., and Sato, Y. (2003). Availability of systems with self-diagnostic components-applying markov model to iec 61508-6. *Reliability Engineering Systems Safety*, 80 :133141.