Université de Batna 2-Mostefa Ben Boulaid

Institut d'Hygiène & Sécurité Industrielle

Laboratoire de Recherche en Prévention Industrielle

THÈSE

Présentée pour obtenir le grade de

DOCTEUR EN SCIENCES

EN

Hygiène & Sécurité Industrielle

Option : Gestion des Risques

PAR

Mr SAL Rachid

Apport des Techniques Floues et Possibilistes au Diagnostic des Défaillances des Systèmes de Sécurité

Soutenue le 15 Juillet 2018 devant le Jury composé de :

Mme. Zidani Fatiha, Professeure à l'Université de Batna2	Présidente
Mr. Nait-Said Rachid, Professeur à l'Université de Batna2	Rapporteur
Mr. Djebabra Mébarek, Professeur à l'Université de Batna2	Co-Rapporteur
Mr. Korichi Mourad, Professeur à l'Université de Ouargla	Examinateur
Mr. Innal Fares, Maître de Conférences «A» à l'Université de Skikda	Examinateur
Mr. Benafia Ali, Maître de Conférences «A» à l'Université de Batna1	Examinateur

2017-2018

Table des matières

Remerciements 1
Résumé 2
Abstract 3
Liste de acronymes 4
Liste des figures 5
Liste des tableaux 6

Introduction générale 7

Chapitre I Intérêt des tests dans le diagnostic des défaillances des systèmes de sécurité..... 12
I.1 Introduction 12
I.2 Systèmes Instrumentés de sécurité et terminologies relatives 13
I.2.1 Définition d'un SIS 13
I.2.2 Composition d'un SIS 15
I.2.3 Fonction instrumentée de sécurité 16
I.2.4 Niveau d'intégrité de sécurité 16
I.2.5 Mesures de performance des SIS 17
I.2.5.1 Probabilité moyenne de défaillance à la demande (PFD_{avg}) 18
I.2.5.2 Probabilité de défaillance dangereuse par heure (PFH) 18
I.2.6 Classification des défaillances dans la norme IEC 61508 18
I.3 Système de diagnostic 21
I.3.1 De la maintenance préventive au diagnostic 21
I.3.2 Quelques définitions fondamentales 22
I.3.3 Les différentes étapes de diagnostic d'un système 23
I.3.4 Méthodes de diagnostic 24
I.4 Intérêt des tests des SIS dans le diagnostic 26
I.4.1 Tests de diagnostic 27
I.4.2 Proof tests 28
I.4.3 Proof tests complets et tests partiels 31
I.5 Conclusion 33

Chapitre II Evaluation des systèmes par le modèle de Markov flou 35
II.1 Introduction 35
II.2 Incertitude dans le processus d'évaluation des risques 37
II.2.1 Sources d'incertitude 37
II.2.2 Incertitudes des paramètres caractéristiques du SIS 39
II.2.2.1 Taux de couverture de diagnostic DC 41
II.2.2.2 Facteur β des défaillances de cause commune 41
II.3 Modélisation floue 43
II.3.1 Théorie des ensembles flous 43
II.3.1.1 Définitions 43
II.3.1.2 Caractéristiques d'un sous-ensemble flou 44
II.3.1.3 Nombres flous 46
II.3.1.4 Notion d'α coupe 47
II.3.1.5 Opérations arithmétiques sur les nombres flous 48
II.3.2 Evaluation flou de la performance 48
II.3.2.1 Model de Markov flou 48
II.3.2.2 PFD floue 52
II.4 Conclusion 53

Chapitre III Diagnostic de la performance des SIS dans un environnement flou : Effets des stratégies de test 54
III.1 Introduction 54
III.2 Code informatique 55
III.3 Description du système HIPPS 56
III.4 Modèles de Markov Flous des sous-systèmes de l'HIPPS 59
III.4.1 Sous-système solveur logique (unité logique) 59
III.4.2 Sous-système capteur 59
III.4.3 Sous-système actionneur 60
III.5 Données des paramètres des composants de l'HIPPS 61
III.6 Résultats et discussion 62
III.6.1 Comparaison des PFD floues selon la première stratégie 62
III.6.2 Comparaison des PFD floues selon la seconde stratégie 65
III.6.3 Effet des stratégies sur la $P\tilde{F}D_{avg}$ 67
III.7 Conclusion 70

Chapitre IV Analyse de l'effet des variations des données imparfaites sur la performance des SIS 71
IV.1 Introduction 71
IV.2 Principe de l'analyse de sensibilité 72
IV.3 Formalisme mathématique 74
IV.4 Résultats 75
IV.4.1 Effet de la variation de β sur la $P\tilde{F}D_{avg}$ 75
IV.4.2 Effet de la variation du DC sur la $P\tilde{F}D_{avg}$ 76
IV.4.3 Comparaison de la $P\tilde{F}D_{avg}$ avec les SILs conventionnels 78
IV.4.4 Analyse de similarité entre les PFD floues 79
IV.5 Conclusion 81

Conclusion générale 82

Références bibliographiques 84
Annexe 90

Remerciements

Le travail présenté dans ce mémoire a été effectué au sein de l'équipe « Sureté de Fonctionnement » du Laboratoire de Recherche en Prévention Industrielle, Institut d'Hygiène et Sécurité, Université de Batna 2. J'exprime mes profonds remerciements à mon encadreur le professeur NAIT-SAID Rachid pour son aide, ses encouragements et ses pertinentes orientations tout au long de ce travail.

Je tiens à remercier également le professeur DJEBABRA Mébarek d'avoir accepter d'être le Co-encadreur de cette thèse et pour ses encouragements et l'intérêt qu'il a accordé à ce travail.

J'exprime mes plus vifs remerciements à Madame ZIDANI Fatiha, Professeure à l'Université de Batna 2, qui a bien voulue me faire l'honneur de présider ce jury.

J'exprime toute ma gratitude à Monsieur KOURICHI Mourad , professeur à l'Université de Ouargla ; Monsieur INNAL Fares, Maître de Conférences «A» à l'Université de Skikda; Monsieur BENAFIA Ali, Maître de Conférences «A» à l'Université de Batna1, pour avoir bien voulu me faire l'honneur de juger ce travail et de participer à ce jury.

Mes remerciements s'adressent également au groupe flou: Mme OUAZRAOUI Nouara, Maître de Conférences «B», Mme CHERGUI Loubna, Maîtres assistant «A», Melle ACHOURI Nouhed, Maîtres assistant «A», Mr. BOURARECHE Mouloud, Maîtres assistant «A», Mr. SELLEMI Ilyes Maîtres assistant «A», Mr. TOUAHAR Hafed et Mr. SEKIOU Samir.

Que ma femme trouve ici mes vifs et profonds remerciements pour ses aides précieuses, sa patience et ses encouragements permanents pour l'aboutissement de ce travail.

Enfin, je n'oublie pas d'exprimer mes remerciements à tous mes collègues enseignants et personnel de l'institut d'Hygiène et Sécurité Industrielle de Batna.

Résumé

Les systèmes instrumentés de sécurité sont actuellement largement utilisés dans l'industrie des procédés afin de protéger les installations contre toute situation dangereuse qui peut se produire. Pour cela, le diagnostic des défaillances dangereuses qui entravent le SIS d'exécuter ses fonctions de sécurité s'avère nécessaire et important. Dans ce contexte et afin d'atteindre cet objectif, les différents tests (tests de diagnostic, proof tests et les tests partiels) appliqués aux SIS et qui sont spécifiés par les deux normes IEC 61508 et IEC 61511 qui traitent de la sécurité fonctionnelles des systèmes relatifs à la sécurité, peuvent être utilisés avantageusement pour détecter et localiser les défaillances possibles qui peuvent surgir dans ces systèmes. Ce présent travail consiste alors à exploiter ces tests pour des fins de diagnostic. De plus et vu l'importance de ces test, nous avons examiné deux stratégies de test, à savoir le test simultané et le test échelonné pour montrer l'impact de ces stratégies de test sur la performance des SIS faiblement sollicités et périodiquement testés dans un environnement incertain. En tant que paramètres pertinents du SIS, le facteur de défaillance de cause commune β et le taux de couverture diagnostique DC sont modélisés par des nombres flous triangulaires et sont injectés dans le modèle de Markov flou pour calculer la PFD_{avg} floue qui caractérise la performance du SIS. Une analyse de sensibilité est effectuée pour montrer l'effet de la variation du facteur β et du taux DC floues sur le PFD_{avg} floue du SIS. Un cas d'application axé sur un système de protection contre la pression à haute intégrité (HIPPS) est réalisé.

Mots clès : Défaillances de cause commune, Couverture de diagnostic, Incertitude, Chaîne de Markov floues, PFD floue, Stratégies de test.

Abstract

Instrumented safety systems are currently widely used in the process industry to protect facilities against any dangerous situation that may occur. For this, the diagnosis of dangerous failures that hinder the SIS from performing its safety functions is necessary and important.
In this context and in order to achieve this objective, the various tests (diagnostic tests, proof tests and partial tests) applied to SIS and which are specified by the two standards IEC 61508 and IEC 61511 which deal with the functional safety of the safety-related systems, can be used to detect and locate possible failures that may arise in these systems. This work consists in exploiting these tests for diagnostic purposes. In addition, and given the importance of these tests, we examined two test strategies, namely the simultaneous test and the staggered test, to show the impact of these test strategies on the performance of SIS in low demand mode and periodically tested in an uncertainty environment. As a relevant parameters of SIS, common cause failure factor β and diagnostic coverage rate DC are modeled by triangular fuzzy numbers and are injected into the fuzzy Markov model to calculate the fuzzy PFD_{avg} that characterizes the SIS performance. A sensitivity analysis is carried out to show the effect of fuzzy beta and DC variation on fuzzy PFD_{avg} of the SIS. An application case focused on a high integrity pressure protection system (HIPPS) is carried out.

Keywords: Common cause failures, Diagnostic coverage, Uncertainty, Fuzzy Markov chains, Fuzzy PFD, Test strategies.

ملخص

تستخدم حالياً أنظمة السلامة الآلية (السيس) على نطاق واسع في مصانع العمليات لحماية المنشآت من أي وضع خطير قد يحدث. لهذا ، فإن تشخيص حالات الأعطاب الخطيرة التي تعيق نظام السلامة الآلي (السيس) عن أداء وظائفه الأمنية أمر ضروري ومهم. في هذا السياق ومن أجل تحقيق هذا الهدف، فان الاختبارات المختلفة (الاختبارات التشخيصية واختبارات الإثبات والاختبارات الجزئية) المطبقة على نظام السلامة الآلي والمحددة من خلال المعيارين 61508 و 61511ذات الصلة بالأمان , يمكن استخدامها لاكتشاف و تحديد الأعطاب المحتملة التي قد تنشأ في هذه الأنظمة. في هذا العمل الذي أجريناه, قمنا باستغلال هذه الاختبارات من أجل التشخيص. بالاضافة الى هذا, و بالنظر الى أهمية هذه الاختبارات, قمنا بفحص استراتجيتن من الأختبار لأظهار أثر هاتين الأسراتجيتين على حسن أداء السيس في بيئة غير مؤكدة. كوسائط مهمة للسيس,قمنا بنمذجة العامل بيتا و المعدل دي سي بأرقام غامضة (فلو) مثلثية و تم ادخالها في نموذج ماركوف الغامض لحساب البدفي الغامض. كما قمنا كذالك باجراء تحليل الحساسية لأظهار تأثير تغيير العامل بيتا و المعدل دي سي الغامضين على البدفي الغامض لهذا السيس. كتطبيق لهذا العمل اخترنا نظام HIPPS.

الكلمات المفتاحية : الأعطاب ذات السبب المشترك, التغطية التشخيصية, الريبة, سلاسل ماركوف الغامضة, البدفي الغامض, استراتجيات الأختبار.

Liste des acronymes

SIS : Safety Instrumented System (Système Instrumenté de sécurité).

EUC : Equipment Under Control (Equipement Commandé ou Equipement à protéger).

PES : Programmable Electronic system.

IEC : International Electrotechnical Commission (Commission Electrotechnique Internationale).

E/E/EP : Electrique/Electronique/Electronique programmable.

LS : Logic Solver (unité logique).

FE : Final Element (élément final).

SIF : Safety Instrumented Function (fonction instrumentée de sécurité).

SIL : Safety Integrity Level (niveau d'intégrité de sécurité).

PFD_{avg} : Average Probability of Failure on Demand (probabilité moyenne de défaillance à la demande).

PFH : average frequency of dangerous failure or Probability of a dangerous Failure per Hour (Probabilité de défaillance dangereuse par heure).

DC : Diagnostic Coverage (couverture de diagnostic).

DU : Undetected Dangerous failures (défaillances dangereuses non détectées).

DD : Detected Dangerous failures (défaillances dangereuses détectées).

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

PST : Partial Stroke Testing (test partiel de la course de la vanne).

AdD : Arbre des défaillances.

DBF : Diagrammes Blocs de Fiabilité.

CCF : Common Cause Failure (défaillances de cause commune).

FMC : Fuzzy Markov Chain (Chaînes de Markov floues).

RFMM : Restricted Fuzzy Matrix Multiplication (multiplication restreinte des matrices floues).

$P\tilde{F}D_{avg}$: fuzzy Average Probability of Failure on Demand (probabilité moyenne de défaillance à la demande floue).

Liste des figures

Chapitre I

Figure I.1 : Classification des barrières de sécurité 8

Figure I.2 : Un exemple de SIS 9

Figure I.3 : Classification des défaillances 14

Figure I.4 : Tests et diagnostic des SIS 21

Figure I.5 : Impact des tests périodiques sur la fiabilité 24

Chapitre II

Figure II.1 : Caractéristique d'un sous-ensemble flou 39

Figure II.2 : Nombre flou triangulaire 40

Figure II.3 : α-coupe d'un nombre flou 41

Chapitre III

Figure III.1 : Schéma du système HIPPS étudié 51

Figure III.2 : Diagramme bloc de fiabilité de l'HIPPS 51

Figure III.3 : Modèle de Markov multiphase flou du solveur logique en 1oo1 53

Figure III.4 : Modèle de Markov multiphase flou du capteur en 2oo3 54

Figure III.5 : Modèle de Markov multiphase flou de l'actionneur en 1oo2 55

Figure III.6 $P\tilde{F}D(t)$ de la SIF liée à la première stratégie 58

Figure III.7 : $P\tilde{F}D_{avg}$ de la SIF liée à la première stratégie 58

Figure III.8 : $P\tilde{F}D(t)$ de la SIF liée à la seconde stratégie 60

Figure III.9 : $P\tilde{F}D_{avg}$ de la SIF liée à la seconde stratégie 61

Figure III.10 Effet des stratégies sur la $P\tilde{F}D_{avg}$ de la SIF 63

Chapitre IV

Figure IV.1 : Principe de l'analyse de sensibilité 66

Figure IV.2 : Effet de la variation de β sur la $P\tilde{F}D_{avg}$ 70

Figure IV.3 Effet de la variation du DC sur la $P\tilde{F}D_{avg}$ 71

Figure IV.4 Mesures de possibilité et nécessité de la $P\tilde{F}D_{avg} \leq L$ 72

Figure IV.5 Distance de Hamming 74

Liste des tableaux

Chapitre I

Table I.1 : SILs définis par la norme IEC 61508 11

Table I.2 : Proportion de défaillances relatives aux constituants d'un SIS 25

Chapitre III

Table III.1 : Données numériques des composants de l'HIPPS 56

Chapitre IV

Table IV.1 : Mesures de possibilité et de nécessité liées à la seconde stratégie 73

Introduction générale

Les établissements industriels ne se préoccupent plus uniquement des performances des systèmes en terme de qualité, de productivité et de rentabilité mais aussi en terme de sécurité. Les moyens à mettre en œuvre pour réduire les risques sont nombreux et variés. La conception du procédé et le choix des équipements participent en premier lieu 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 de conditions anormales de fonctionnement. Néanmoins, ces actions restent parfois insuffisantes et il faut introduire d'autres systèmes de sécurité pour réduire encore le risque à un niveau acceptable. Des systèmes spécifiques appelés systèmes instrumentés de sécurité (SIS) sont introduits pour pallier à ce besoin et ayant pour objectif de réduire les risques d'occurrence d'événements dangereux tout en garantissant la protection des équipements, des opérateurs humains et de l'environnement [Sallak 2007], [Mkhida 2008].

Les SIS sont utilisés pour exécuter des fonctions de sécurité, ils sont aussi appelés boucles de sécurité [Mkhida 2008]. Ils comprennent tous les matériels et logiciels nécessaires pour obtenir la fonction de sécurité désirée. Ces systèmes 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, les biens et l'environnement [Mkhida 2008].

La disponibilité des SIS est donc d'une grande importance pour ces procédés industriels afin de les protéger contre toute situation dangereuse qui peut se produire. Pour cela, le diagnostic des défaillances des éléments qui constituent le SIS s'avère nécessaire et important. En effet, le besoin est bien exprimé pour assurer surtout le diagnostic des défaillances dangereuses qui entravent le SIS d'exécuter sa (ou ses) fonction(s) de sécurité.

Dans ce contexte et afin d'atteindre cet objectif, les différents tests (tests de diagnostic, proof tests et les tests partiels) appliqués aux SIS et qui sont spécifiés par les deux normes IEC 61508 et IEC 61511 qui traitent de la sécurité fonctionnelles des systèmes relatifs à la

sécurité, peuvent être utilisés avantageusement pour détecter et localiser les défaillances possibles qui peuvent surgir dans ces systèmes. L'intérêt de cette idée est l'exploitation de ces tests pour des fins de diagnostic afin d'améliorer la performance des SIS. Effectivement, l'application de ces tests permet de diagnostiquer très tôt les défaillances et d'en éliminer le maximum. Ceci a un effet direct sur la réduction de la PFD_{avg} et par conséquent l'amélioration de la fiabilité et la disponibilité des SIS. Rausand dans [Rausand 2014] montre par exemple que l'ajout des tests partiels aux proof tests permet de prolonger l'intervalle entre les proof tests puisque une fractions de défaillances-DU est révélée et réparée dans un intervalle de temps plus court après leur apparition.

Etant donné l'importance de ces tests, la littérature présente plusieurs types de stratégies de test [Torres-Echeverria et al. 2009]. Dans le cadre de notre travail nous avons examiné deux stratégies de test, à savoir le test simultané et le test échelonné. Pour cela, nous avons tenté de montrer l'effet de ces stratégies de test sur la performance des SIS faiblement sollicités et périodiquement testés dans un environnement incertain.

Les normes IEC 61508 et IEC 61511 introduisent une approche probabiliste pour l'évaluation quantitative de la performance des systèmes instrumentés de sécurité et la qualification de cette performance par des niveaux de sécurité référencés. En effet pour les SIS faiblement sollicité, ces deux normes prévoient la probabilité moyenne de défaillance (dangereuse) à la demande (PFD_{avg} pour Average Probability of Failure on Demand) comme un critère quantitatif qui permet de juger la performance d'un SIS.

Cette performance doit être évaluée par des méthodes référencées comme les équations simplifiées, les arbres de défaillances (AdD), les diagrammes blocs de fiabilité (DBF), les chaînes de Markov ainsi que les réseaux de Pétri [Innal 2008], [Rausand 2014].

La performance ainsi calculée permet d'affecter au SIS un niveau d'intégrité de sécurité selon les niveaux définis dans la norme IEC 61508. Parmi plusieurs méthodes explorées, il a été conclu que le modèle de Markov est le plus approprié pour l'évaluation de la PFD_{avg} car il permet de modéliser facilement différentes situations [Goble and Cheddie 2005], [Innal et al. 2006].

Dans les études de fiabilité, on suppose que les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation, ...) sont souvent disponibles, précises et validés par le retour d'expérience [Sallak 2007]. Dans certains cas, le retour d'expérience est

malheureusement insuffisant pour valider avec précision ces données de fiabilité. En outre, l'évolution constante de la complexité des installations industrielles, de l'environnement et des conditions d'exploitations 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 aves précision leurs paramètres de défaillance.

Les SIS sont des dispositifs sur lesquels nous n'avons pas forcément de retour d'expérience en quantité. Ceci est d'autant plus vrai lorsque ces SIS sont faiblement sollicités. Ceci va poser donc un problème de manque de données pour l'évaluation de la performance des SIS. Pour pallier à ce problème, les analystes font recours généralement soit aux bases de données génériques, soit aux jugements d'experts pour estimer les données de fiabilité des composants des SIS. Cependant, le recours à ces sources ne peut engendrer que de l'imprécision sur ces données. La grande question qui se pose est la suivante : "où doit-on trouver des données de fiabilité de qualité, qui peuvent être utilisées pour évaluer la performance de tels systèmes hautement fiables pour lesquels l'on dispose d'un grand manque de connaissance et le retour d'expérience est malheureusement faible et insuffisant ?" [Innal et al. 2016].

Dans le but de surmonter cette difficulté, des méthodes autres que les approches probabilistes classiques (les ensembles flous par exemples) peuvent utiliser avantageusement ces données pour prendre en compte l'imprécision (qu'on appelle aussi incertitude de type épistémique) liée à aux paramètres de défaillance et calculer la PFD_{avg} qui caractérise la performance du SIS.

La théorie des ensembles flous est un outil puissant pour traiter l'incertitude des paramètres dans les modèles de fiabilité [Markowski et al. 2011], [Bowles et pelaez 1995]. Les modèles flous reflètent bien la formulation approximative des données fournies par un expert ou issus de la littérature, comme est « autour de m » ou est « entre a et b ». On peut utiliser avantageusement ces représentations de l'incertitude des paramètres pour évaluer la performance du SIS dans un environnement flou [Zadeh 1965].

Le présent document est organisé en quatre chapitres :

- Le premier chapitre présente les différents concepts liés aux systèmes instrumentés de sécurité tels que la composition d'un SIS, le niveaux d'intégrité de sécurité, la fonction instrumentée de sécurité, les mesures de performances des SIS et la classification des défaillances établie par la norme IEC 61508. Nous présentons aussi le principe du système de diagnostic et les approches utilisées, à savoir l'approche de diagnostic qualitative qui repose sur les techniques de l'intelligence artificielle et l'approche de diagnostic quantitative basée sur un modèle mathématique décrivant le comportement dynamique du système à surveiller. Et enfin, nous nous intéressons aux différents tests appliqués aux SIS tels que les tests de diagnostic, les proof tests et les tests partiels et comment ils peuvent être exploités pour des fins de diagnostic.

- Le second chapitre examine brièvement la notion d'incertitude liée au processus d'évaluation des risques et ces différentes sources en insistant surtout sur l'incertitude relatives aux paramètres caractéristiques des SIS tels que le facteur de défaillance de cause communes β et le taux de couverture DC. Nous présentons aussi les concepts de base de la théorie des ensembles flous. Le dernier point évoqué dans ce chapitre est le modèle de Markov flou pour l'évaluation de la performance des SIS en utilisant l'approche développée par Buckley et Eslami dite "multiplication restreinte des matrices floue (RFMM pour Restricted Fuzzy Matrix Multiplication).

- Le troisième chapitre consiste à évaluer la PFD_{avg} floue d'un HIPPS par les chaînes de Markov floues en considérant deux stratégies de test, à savoir le test simultané et le test échelonné. Le long de ce chapitre nous tentons de montrer l'effet de ces deux stratégies de test sur la performance du SIS faiblement sollicités et périodiquement testés dans un environnement incertain. Les probabilités élémentaires des chaînes de Markov sont remplacées par des nombres flous triangulaires et découpées en α-coupes. Les paramètres caractéristiques imprécis de l'HIPPS, en l'occurrence le facteur β et le taux DC, sont modélisés par des nombres flous triangulaires.

- Le quatrième chapitre présente, dans un premier temps, le principe théorique de l'analyse de sensibilité. Il consiste à montrer que la variation des paramètres d'entrée d'un modèle peut influencer sa variable de sortie. L'analyse de sensibilité vise à identifier les variables

les plus importantes dans un modèle, c'est-à-dire les variables qui ont le plus d'impact sur la sortie du modèle. Dans un second temps, nous appliquons ce principe pour voir l'effet de variation du facteur β et du taux DC flous sur la PFD_{avg} floue.

Evidemment, ces quatre chapitres sont cadrés par une introduction et une conclusion générales. La conclusion générale permet de dresser un bilan du travail réalisé ainsi que les perspectives envisageables.

Chapitre I

Intérêt des tests dans le diagnostic des défaillances des systèmes de sécurité

I.1 Introduction

De nos jours, la plupart des processus industriels s'équipent de plus en plus avec des systèmes automatiques complexes afin d'améliorer la productivité et la qualité de leurs produits. En raison de cette complexité, ces processus industriels, en particulier les paramètres caractéristiques de leur comportement, sont surveillés en permanence par des dispositifs qualifiés de systèmes instrumentés de sécurités (SIS).

Un SIS est conventionnellement Composé de trois sous-systèmes principaux : les éléments de détection, les solveurs logiques et les éléments finaux. L'objectif principal assigné à de tels systèmes est de détecter l'apparition d'une situation dangereuse, lorsque des conditions prédéterminées sont violées telles que les points de consigne pour la pression, la température, le niveau, etc., qui pourrait conduire à un accident et ensuite implémenter un ensemble de mesures nécessaires pour mettre l'équipement commandé (EUC pour Equipment Under Control) dans un état sûr [Innal et al. 2016].

Donc, la disponibilité des SIS est d'une grande importance pour ces processus industriels afin de les protéger contre toute situation dangereuse qui peut se produire. Pour cela, le diagnostic des défaillances des éléments qui constituent le SIS s'avère nécessaire et important. En effet, le besoin est bien exprimé pour assurer surtout le diagnostic des défaillances dangereuses qui entravent le SIS d'exécuter sa fonction de sécurité. Les tests prévus par les normes IEC 61508 et IEC 61511 sont des moyens importants pour améliorer la disponibilité des SIS. Ils sont établis pour détecter les défaillances des éléments du SIS. Dans

ce travail, nous allons montrer comment ces tests peuvent être utile dans le diagnostic des défaillances et essayons de profiter de leur intérêt afin d'améliorer la performance des SIS.

Dans ce chapitre, nous introduisons, dans un premier temps, les différents concepts liés aux systèmes instrumentés de sécurité tels que le niveau d'intégrité de sécurité, la fonction instrumentée de sécurité, les mesures de performance des SIS. Puis, dans un second temps, nous évoquons le principe du système de diagnostic et les approches utilisées, à savoir l'approche quantitative basée sur un modèle mathématique qui représente le comportement dynamique du système à surveiller et l'approche qualitative basée sur les techniques de l'intelligence artificiels. En dernier, nous nous intéressons aux différents types de tests utilisés, tels que les tests de diagnostic, les proofs tests et les tests partiels, pour détecter les défaillances dangereuses qui empêchent un SIS à exécuter sa fonction de sécurité et voir leur impact sur sa performance.

I.2 Systèmes Instrumentés de sécurité et terminologies relatives

I.2.1 Définition d'un SIS

La normes IEC 61508 est une norme internationale qui porte plus particulièrement sur les systèmes E/E/EP (électriques/électroniques/électroniques programmables) de sécurité. Cette norme définit les systèmes relatifs aux applications de sécurité comme : ***un système E/E/EP (électriques/électroniques/électroniques programmables), relatif aux applications de sécurité, comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.*** **Q**uant à la norme IEC 61511 qui découle de la norme mère IEC 61508 et qui est spécifique à l'industrie des procédés, elle définit un système instrumenté de sécurité de la façon suivante : ***système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unité(s) logique(s) et d'élément(s) terminal (aux).***

Les SIS sont donc des systèmes utilisés comme moyens de prévention et comportent une proportion grandissante de systèmes électriques, électroniques ou encore électroniques programmables (E/E/EP). Ces systèmes sont devenus plus complexes et disposent d'un nombre important de traitement ce qui rend alors difficile la connaissance de chaque modes de défaillance par l'examen des comportements possibles [Mkhida 2008], [Rausand 2014].

Les SIS sont utilisés pour exécuter des fonctions instrumentées de sécurité dans les industries de production par processus. Ce sont des moyens de sécurité chargés de surveiller que le procédé ne franchit pas certaines limites (au-delà desquelles il pourrait devenir dangereux) et d'actionner les organes de sécurité lorsqu'un tel danger se présente. Ils visent donc à mettre le procédé en un état stable ne présentant pas de risque pour les personnes et l'environnement lorsque le procédé s'engage dans une voie comportant un risque réel (feu, explosion, ...). Etant donnée que les SIS sont considérés comme des barrières de sécurité, la figure I.1 montre la classification des SIS parmi les autres barrières de sécurité [Sklet 2006].

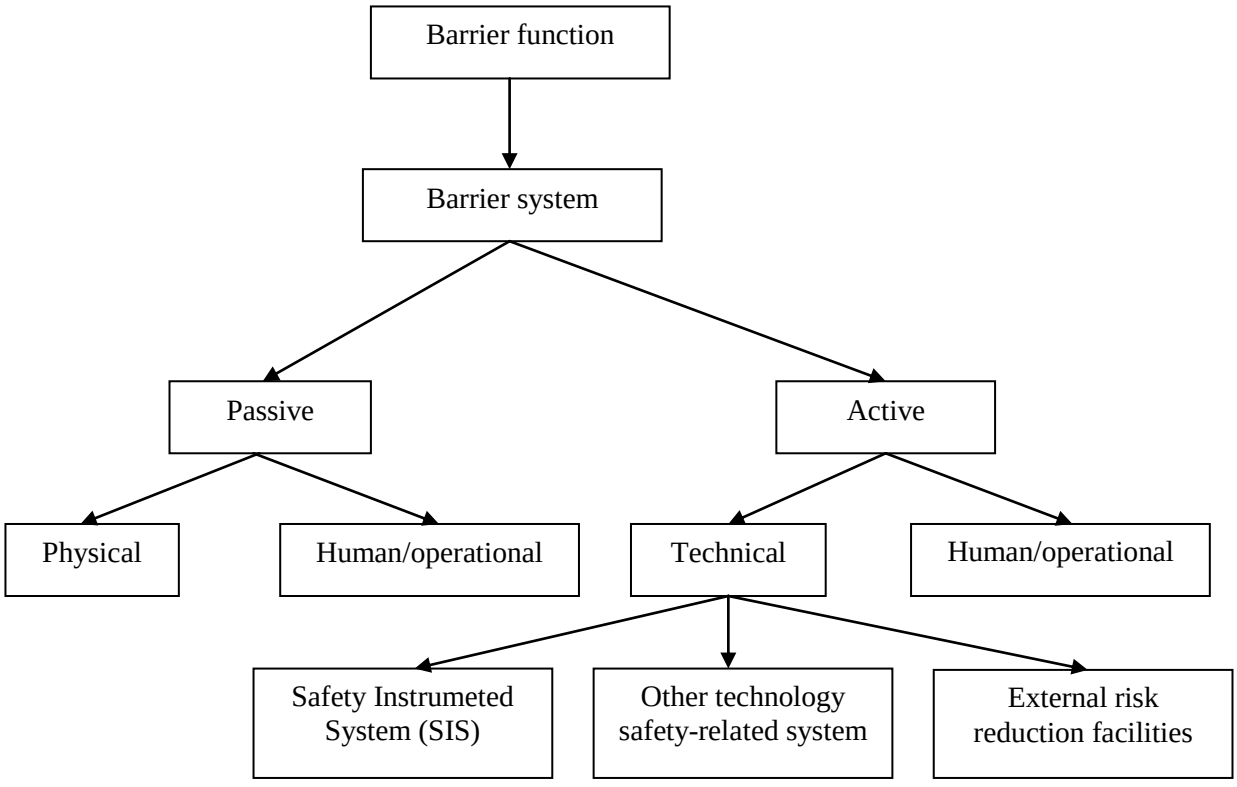


Fig.I.1 Classification des barrières de sécurité

I.2.2 Composition d'un SIS

D'une façons générale, un SIS se compose de trois sous-systèmes comme le montre la figure I.2 :

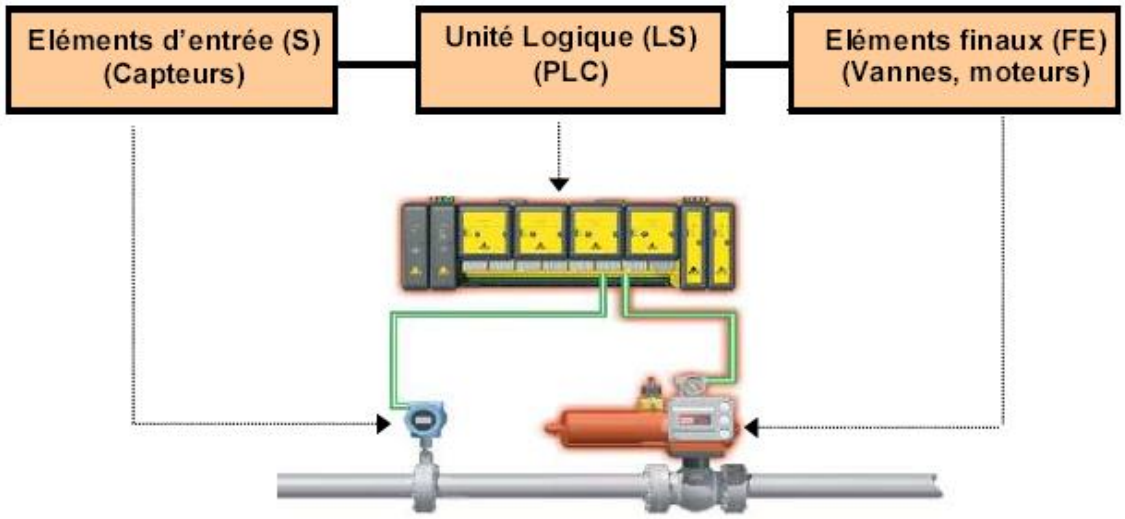


Fig. I.2 Un exemple de SIS

- Sous-système Capteur (Sensor) : il est constitué d'un ensemble d'éléments d'entrée (capteurs, détecteurs) qui surveillent l'évolution des paramètres physico-chimiques représentatifs du comportement du procédé (température, pression, niveau, ...). Si au moins un de ces paramètres dévie au-delà d'une valeur de consigne et s'y maintient , ce fait constitue, donc, ce qu'on appelle une demande ou une sollicitation émanant du procédé, de l'EUC. Cette déviation est détectée par les capteurs concernés qui envoient un signal au sous-système logic solver.

- Sous-système 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 qui est l'actionneur. Le sous-système logic solver peut être un automate programmable ou un micro-ordinateur doté de logiciels spécifiques [Mkhida 2008].

- Sous-système actionneur FE (Final Element) : il agit directement (vanne d'arrêt d'urgence) ou indirectement (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 [Mechri 2011], [Innal 2008].

I.2.3 Fonction instrumentée de sécurité

Une fonction de sécurité exécutée par un SIS est une fonction instrumentée de sécurité (SIF : Safety Instrumented Function). L'objectif d'une SIF est de mettre ou de maintenir l'EUC dans un état sûr lorsqu'une demande survient afin de protéger les personnes, les biens et l'environnement. Donc, la SIF n'est déclenchée que si le SIS est sollicité suite à la détection d'une dérive potentiellement dangereuse d'un paramètre physico-chimique du procédé au-delà d'une valeur de consigne. En général, un SIS peut réaliser plusieurs SIF [Mechri 2011], [Innal 2008]. Une fonction instrumentée de sécurité est spécifiée pour s'assurer que les risques sont maintenus à un niveau acceptable par rapport à un événement dangereux spécifique [Mkhida 2008].

I.2.4 Niveau d'intégrité de sécurité

Les normes de sécurité fonctionnelle IEC 61508 et IEC 61511 définissent le niveau d'intégrité de sécurité (Safety Integrity Level : SIL) pour définir le niveau de réduction du risque, c'est-à-dire le niveau d'intégrité de sécurité que doit avoir un système de protection. Elle permettent donc de définir le niveau SIL qui doit être atteint par un SIS qui réalise la fonction de sécurité suite à une analyse de risque [Sallak et al. 2006], [Wang et al. 2004], [Schonbeck et al. 2010]. Plus le SIL a une valeur élevée plus la réduction est importante.

Les SILs se caractérisent par des indicateurs discrets positionnés sur une échelle à quatre niveaux. Le SIL 4 désigne le degré de sécurité le plus élevé et le SIL 1 désigne l'exigence la plus faible. Il est important de noter qu'un SIL est toujours lié à une SIF spécifique et non à un SIS, et qu'une fonction de sécurité n'est pas une SIF sauf si un SIL est attribué à la fonction de sécurité [Rausand 2014].

Le tableau I.1 regroupe les différents niveaux de SIL définis par la norme IEC 61508.

Table I.1 SILs définis par la norme IEC 61508.

SIL	PFDavg	PFH
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	$PFD_{avg} \in [10^{-5}, 10^{-4}]$	$PFH \in [10^{-9}, 10^{-8}]$

I.2.5 Mesures de performance des SIS

La norme IEC 61508 spécifie deux indicateurs de sécurité relatifs aux systèmes E/E/EP dédiés à la sécurité. Ces deux indicateurs sont utilisés pour l'évaluation des performances des SIS suivant les modes de fonctionnement d'une SIF cités par cette norme. Il s'agit de la probabilité moyenne de défaillance à la demande (PFD_{avg}) et la probabilité de défaillance dangereuse par heure (PFH) [Mechri 2011], [Rausand 2014], [IEC 61508, 2010].

La norme IEC 61508 s'applique aussi bien aux systèmes de sécurité qui fonctionnent sur sollicitation (mode faible demande) que ceux qui fonctionnent en permanence (mode demande élevée ou continue).

Un SIS est en mode de fonctionnement à faible demande lorsque la fréquence de demande n'est pas plus grande que une fois par an et au plus égale à deux fois la fréquence des tests périodiques. A partir de l'architecture du SIS réalisant la fonction instrumentée de sécurité (SIF) faiblement sollicitée, la PFD_{avg} (*Average Probability of* Failure *on Demand*) est évaluée sur un intervalle de temps [0, t]. De même, un SIS en mode de fonctionnement continu ou à demande élevée implique une forte sollicitation du SIS. Il est considéré ainsi lorsque la fréquence de demande est plus grande que une fois par an ou supérieure à deux fois la fréquence des tests périodiques [IEC 61508, 2010], [Mkhida 2008], [Innal 2008], [Liu and Rausand 2011].

I.2.5.1 Probabilité moyenne de défaillance à la demande (PFD_{avg})

La probabilité moyenne de défaillance (dangereuse) à la demande, est la mesure de la performance d'une SIF fonctionnant en mode faible demande. La PFD_{avg}, 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 sollicité par un EUC [Rausand 2014], [Innal 2008]. La PFD_{avg} est un critère quantitatif qui permet donc de juger la performance d'une SIF d'un SIS.

Pour un système testé périodiquement sur un intervalle de test égale à τ, on peut alors écrire :

$$PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} PFD(t)dt \qquad \text{(I.1)}$$

Où $PFD(t)$ est la probabilité de défaillance dangereuse instantanée.

I.2.5.2 Probabilité de défaillance dangereuse par heure (PFH)

Pour les SIF fonctionnant en mode demande élevée ou en mode continu, la norme IEC61508 exige que la mesure de la performance soit spécifiée par la fréquence moyenne des défaillances dangereuses (PFH pour *average frequency of dangerous failure*). L'abréviation PFH est retenue de la première édition de la norme IEC 61508 (version 1997) où la mesure était appelée " Probability of a dangerous Failure per Hour". L'abréviation est toujours utilisée même si le nom a changé [Rausand 2014].

I.2.6 Classification des défaillances dans la norme IEC 61508

Généralement un système peut se trouver dans l'un des quatre états suivants [Lamy 2002] :

- ***Etat normal*** : la fonction de sécurité du système est valide et il n'existe pas de défaillance.
- ***Etat normal dégradé*** : la fonction de sécurité est valide, des composants du système peuvent être défaillants. Le système peut réagir dès l'apparition d'un événement dangereux.

- ***Etat de sécurité*** : il s'agit d'un état du système pour lequel la sécurité est réalisée. Le système peut entrer dans cet état dés qu'une défaillance d'un ou plusieurs composants se produit. Dans ce cas, la défaillance peut être : soit détectée ou non détectée, mais elle n'a pas d'action néfaste vis-à-vis la sécurité.
- ***Etat de défaillance dangereuse*** : c'est un état du système ou la fonction de sécurité n'est plus réalisée, un ou plusieurs composants sont défaillants. Le système entre dans cet état dés qu'un risque d'accident apparait et le système ne répond pas à une demande d'activation de la fonction de sécurité.

La norme IEC 61508 distingue deux types de défaillances : les défaillances dangereuses et les défaillances sûres (voir figure I.3). Une défaillance est dite dangereuse si la SIF n'est plus en mesure de répondre à une demande, sinon elle est dite sûre.

Toutes les défaillances détectées en ligne par les tests de diagnostic sont qualifiées de défaillances détectées. Celles qui ne sont pas détectées sont qualifiées de défaillances non détectées. Les défaillances peuvent être divisées comme suit [Jin et al. 2011], [Lamy 2002], [Liu and Rausand 2011] :

- ***Les défaillances sûres et détectées*** : ces défaillances font passer le système de l'état normal à l'état de sécurité, leur taux de défaillance est noté λ_{SD}.
- ***Les défaillances sûres et non détectées*** : ces défaillances font passer le système de l'état normal à l'état dégradé, leur taux de défaillance est noté λ_{SU}.
- ***Les défaillances dangereuses et détectées*** : ces défaillances 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 λ_{DD}.
- ***Les défaillances dangereuses et non détectées*** : ces défaillances font passer le système de l'état normal à l'état de défaillance dangereux, leur taux de défaillance est noté λ_{DU}.

La somme des taux de défaillances sûres détectées et non détectées donne le taux de défaillances sûres, noté λ_S :

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \qquad \text{(I.2)}$$

La somme des taux de défaillances dangereuses détectées et non détectées donnent le taux de défaillances dangereuses, noté λ_D :

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{I.3}$$

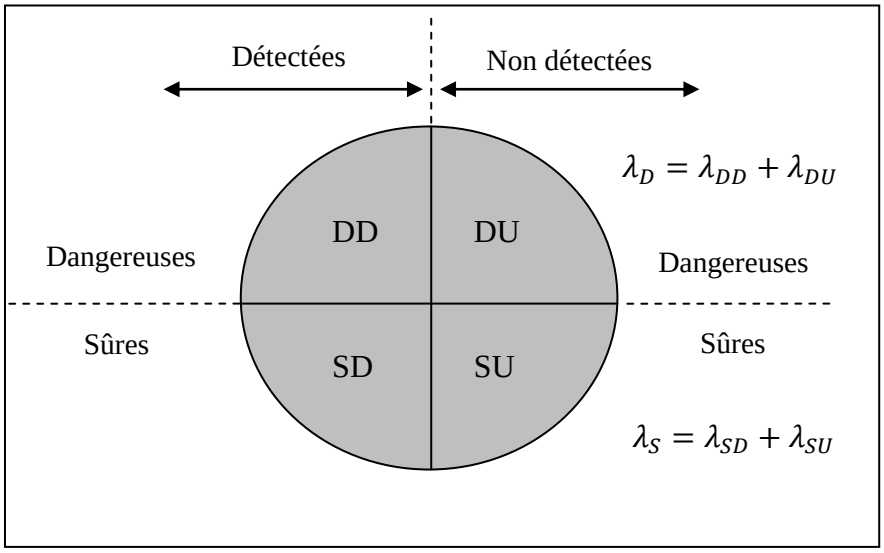


Fig. I.3 Classification des défaillances.

Les défaillances sûres sont supposées avoir un effet négligeable sur la PFD_{avg}, puisque la PFD_{avg} se calcul en se basant sur les défaillances dangereuses et la réparation des défaillances sûres est généralement terminée en un peu de temps [Jin and Rausand 2014]. Donc, seules les défaillances dangereuses seront prises en compte dans la suite de ce document.

Les défaillances dangereuses détectées, notée défaillances-DD, sont des défaillances détectées par les tests de diagnostic. Les défaillances dangereuses non détectées, notées défaillances-DU, sont des défaillances détectées uniquement par les proof tests et une partie par les tests partiels comme il sera montré ultérieurement [Jin and Rausand 2014], [Liu and Rausand 2013].

I.3 Système de diagnostic

La complexité sans cesse croissante des systèmes automatisés s'est accompagnée d'une demande toujours plus forte de la disponibilité et de la sécurité des installations industrielles. L'accroissement de la disponibilité peut être obtenu par une amélioration de la fiabilité des éléments mais aussi par la mise en œuvre d'une stratégie de maintenance adaptée à l'installation étudiée [Lyonnet et al. 2012]. On distingue essentiellement deux types de maintenance : la maintenance corrective dans laquelle les actions sont menées après apparition de la défaillance et la maintenance préventive dans laquelle les actions sont menées avant l'apparition de la défaillance.

Bien que le second type semble le plus séduisante, ce type de maintenance n'est pas systématiquement appliquée à l'ensemble d'un procédé industriel. Dans la pratique, les deux types coexistent toujours. Une bonne maintenance consiste alors à mettre en œuvre, pour chaque équipement, sous-ensemble, voire chaque élément, la technique la mieux adaptée. le choix d'une stratégie de maintenance s'opère en fonction des connaissances disponibles sur l'installation et des objectifs à atteindre [Lyonnet et al. 2012], [Bigret 1997].

I.3.1 De la maintenance préventive au diagnostic

L'objectif de la maintenance préventive est de déterminer l'ensemble des actions à exercer sur le procédé afin de ne pas subir l'effet d'une défaillance. La maintenance préventive, basée sur la surveillance en continu de l'évolution du système considéré, nécessite la conception d'un système de diagnostic permettant la détection précoce de déviations faibles par rapport à une caractérisation du système en fonctionnement nominale, afin de prévenir l'occurrence d'un dysfonctionnement [Lyonnet 2012], [Mobley 1992].

Les grandeurs surveillées peuvent être très diverses : un courant électrique, une température, une pression, un débit, un niveau de vibration et bien d'autres encore. Le suivi d'une grandeur donnée s'effectue en mesurant sa valeur régulièrement dans le temps. La grandeur surveillée peut subir, au cours du fonctionnement de l'installation deux types de variation : des fluctuations autour de sa valeur nominale qui sont dues aux diverses perturbations agissant sur le système considéré ou une dérive qui peut être due à un phénomène d'usure, un phénomène de dégradation progressive, à des conditions d'environnement anormales. Le suivi de cette grandeur permet alors de vérifier qu'elle ne

s'écarte pas, de façon significative, de sa valeur nominale. Dans le cas d'une déviation jugée anormale (étape de détection d'un défaut), il s'agit de localiser l'origine de cette anomalie (étape de diagnostic du défaut), puis de prendre les mesures qui s'imposent pour un retour au fonctionnement normal du système (étape de prise de décision). Ces différentes étapes sont réalisées à l'aide de ce que nous appelons un système de diagnostic [Lyonnet 2012], [ISO18436, 2004].

Un système de diagnostic doit donc être en mesure de réaliser les trois étapes essentielles suivantes : la détection d'un défaut, le diagnostic du défaut et la prise de décision pour un retour à la normale. Le diagnostic a pour objectif de rechercher l'origine d'un défaut constaté. Un défaut correspond à une déviation jugée anormale d'une grandeur caractéristique du système [Lyonnet 2012], [Dubuisson 1990].

I.3.2 Quelques définitions fondamentales

Pour bien saisir les choses, il convient de définir certains concepts liés à la notion de diagnostic [Zwingelstein 1995], [Iserman 2011] :

- *fonctionnement normal d'un système* : un système est dit dans un état de fonctionnement normal lorsque les variables le caractérisant (variables d'entrée, variable de sortie, paramètres du système) demeurent au voisinage de leurs valeurs nominales. Le système est dit défaillant dans le cas contraire.
- *défaut* : on appelle défaut tout écart entre la caractéristique observée (ou mesurée) sur le dispositif et la caractéristique théorique. Cet écart est idéalement nul en l'absence de défaut. Les défauts peuvent apparaître au niveau des capteurs, des actionneurs ou au niveau du processus lui-même.
- *Défaillance* : une défaillance est l'altération ou la cessation de l'aptitude d'un système à accomplir sa ou ses fonctions requises avec les performances définies dans les spécifications techniques. Une défaillance est un dysfonctionnement du système, le processus présente alors un fonctionnement inacceptable du point de vue performance. Il est clair qu'une défaillance implique l'apparition d'un défaut puisqu'il existe un écart entre la caractéristique mesurée et théorique. En revanche, un défaut n'implique pas nécessairement une défaillance puisque le dispositif peut très bien continuer à assurer sa fonction principale.

- *Panne* : Une panne est l'inaptitude d'un système à accomplir une fonction requise. Une panne résulte toujours d'une défaillance et donc d'un défaut.

Défaut ⟶ Défaillance ⟶ Panne

I.3.3 Les différentes étapes de diagnostic d'un système

Le diagnostic d'un système donné nécessite un certain nombre d'étapes résumées comme suit [Lyonnet 2012], [Zwingelstein 1995], [Iserman 2011], [Adrot 2000], [Braun 1989].

a) Acquisition de données : La procédure de diagnostic nécessite de disposer d'informations sur le fonctionnement du système à surveiller. Ces informations sont recueillies lors d'une phase d'acquisition de données suivie d'une validation. Cette étape implique donc l'utilisation de capteurs permettant de mesurer les différentes variables du processus.

b) Etape d'élaboration d'indicateurs de défauts : A partir des mesures réalisées et des observations issues des opérateurs chargés de l'installation, il s'agit de construire des indicateurs permettant de mettre en évidence les éventuels défauts pouvant apparaître au sein du système. Dans le domaine du diagnostic, les indicateurs de défauts sont couramment dénommés les résidus ou symptômes. Un résidu représente un écart entre les grandeurs estimées et mesurées. Donc, l'étape d'élaboration d'indicateurs de défauts consiste à comparer le comportement réel du système à un comportement de référence. Cet écart de comportement doit être idéalement nul en l'absence de défaut et différent de zéro dans le cas contraire.

c) Etape de détection de défauts : Cette étape permet de décider si le système se trouve ou non dans un état de fonctionnement normal. On pourrait penser qu'il suffit de tester la non-nullité des résidus pour décider de l'apparition d'un défaut. En pratique, le problème n'est pas si simple, car les grandeurs mesurées sont toujours entachées de bruits. De plus, le système surveillé est toujours soumis à des perturbations et le modèle utilisé, qu'il soit quantitatif ou qualitatif, n'est qu'une représentation toujours imparfaite de la réalité, de sorte que les résidus peuvent être non nuls en l'absence de défauts.

d) Etape de localisation de défauts : Dans cette étape de localisation de défauts, il s'agit de déterminer, à partir des résidus détectés non nuls, le ou les éléments défaillants. On appelle signature d'un défaut l'effet de celui-ci sur un ou plusieurs résidus. Si l'on dispose de la signature des défauts, il est possible, à partir de celle-ci, de remonter des effets (résidus non nuls) aux causes (les éléments défaillants). En résumé, une procédure de diagnostic comprend deux étapes, une étape de génération de résidus et une étape d'évaluation des résidus.

e) Etape de prise de décisions : Le fonctionnement incorrect du système étant constaté, il s'agit de décider de la marche à suivre afin de conserver les performances souhaitées du système sous surveillance. Cette prise de décision doit permettre de générer les actions correctrices nécessaires à un retour à la normale de fonctionnement de l'installation.

I.3.4 Méthodes de diagnostic

Les premières méthodes de diagnostic furent basées sur la redondance des matériels jugés critiques pour le fonctionnement du système. La redondance matérielle est très répandue dans les domaines où la sûreté de fonctionnement est cruciale pour la sécurité des personnes et de l'environnement, comme dans l'aéronautique et le nucléaire. Les principaux inconvénients de la redondance matérielle sont liés aux coûts dus à la multiplication des éléments ainsi qu'à l'encombrement et poids supplémentaire qu'elle génère [Lyonnet 2012].

Les spectaculaires progrès réalisés dans le domaine des calculateurs numériques permettent aujourd'hui la mise en œuvre, dans le milieu industriel, des méthodes modernes de l'automatique et de l'intelligence artificielles. Cette nouvelle approche permet d'éliminer en partie, voire même en totalité, la redondance matérielle pour le diagnostic des systèmes industriels . On peut globalement distinguer deux grandes familles de méthodes de diagnostic [Lyonnet 2012], [Iserman 2011] :

- les méthodes basées sur une modélisation des systèmes qui sont aussi dénommées par diagnostic quantitatif.
- les méthodes basées sur l'intelligence artificielle appelées diagnostic qualitatif.

Le fait de distinguer ce qui est de l'ordre du quantitatif et du qualitatif, ne doit pas laisser penser que ces deux aspects sont disjoints. En réalité, ces deux types d'approches coexistent souvent au sein du système de diagnostic. L'utilisation conjointe des méthodes

quantitatives et qualitatives permet l'exploitation de l'ensemble des connaissances disponibles concernant le fonctionnement du système. Le choix d'une méthode par rapport à une autre, pour l'accomplissement de telle ou telle étape de diagnostic, est imposé par le type de connaissance dont on dispose sur le système [Lyonnet 2012] :

a) Méthode de diagnostic quantitatif

L'approche quantitative consiste à utiliser un modèle mathématique du système à surveiller pour réaliser la détection et la localisation des défauts. Cette approche repose sur l'idée que les grandeurs mise en jeu sont mesurables et que le modèle mathématique, censé représenter objectivement le système, est exploité pour être mis au profit du diagnostic. Si le modèle mathématique reflète convenablement le comportement dynamique du système à surveiller, tout écart entre les grandeurs estimées par le modèle mathématique et les grandeurs mesurées traduit l'apparition d'un ou plusieurs défauts. Les défauts sont alors détectés par comparaison des résidus à des seuils convenablement choisis. Ces résidus représentent des changements ou divergences entre le comportement réel du processus et celui prévu par le modèle. L'objectif du résidu est d'être sensible aux défauts. Ainsi, en l'absence de défauts, c'est- à-dire en fonctionnement normal, le résidu doit avoir une valeur nulle. En présence d'un défaut, le résidu aura une valeur non nulle.

Les approches les plus utilisées pour la génération des résidus sont [Kempowsky 2004], [Lyonnet 2012], [Iserman 2011] : l'approche par espace de parité, l'approche à base d'observateurs et l'approche par estimation paramétrique.

Une fois les résidus générés, ils doivent être évalués pour déterminer la présence ou non d'un défaut. Cette évaluation des résidus est établie en utilisant des seuils convenables.

Le principal inconvénient de l'approche quantitative est la nécessité d'avoir des modèles mathématiques assez précis et complets, ce qui n'est pas toujours facile, voire impossible, pour des processus complexes tels que les processus chimiques. Un autre inconvénient de cette approche est la difficulté de modéliser les perturbations pouvant engendrer des erreurs dans le modèle[[Lyonnet 2012] [Iserman 2011].

b) Méthode de diagnostic qualitative

L'approche qualitative permet de représenter le comportement du procédé par des modèles non plus mathématiques mais des modèles de type symbolique. Dans cette approche, les connaissances utilisables reposent sur le savoir d'experts et sur un ensemble de données issues du procédé. Dans le diagnostic qualitatif, on trouve l'ensemble des méthodes basées sur l'intelligence artificielle telles que la reconnaissance des formes, les systèmes experts et les réseaux neurones . L'objectif de l'intelligence artificielle est de tenter d'imiter les processus cognitifs humains [Lyonnet 2012].

L'inconvénient majeur de ces méthodes de diagnostic est la nécessité de disposer d'une quantité importante d'information sur le comportement du système à surveiller et ses pannes possibles, ce qui rend donc les calculs complexes pour le diagnostic en ligne. Par fois, il est vraiment difficile de regrouper toute cette information, et surtout lorsqu'il s'agit de systèmes de nouvelle technologie. De plus, ces méthodes sont également très sensibles aux erreurs de modélisation [Lyonnet 2012], [Pernestal 2009].

I.4 Intérêt des tests des SIS dans le diagnostic

Les tests sont des moyens d'une grande importance pour améliorer la disponibilité des SIS. Ils sont établis pour détecter les défaillances des éléments du SIS, vérifier et contrôler le bon fonctionnement des SIF. Comme il a été mentionné ci-dessus, les systèmes de diagnostic visent à détecter, à localiser et à réparer les défaillances qui peuvent apparaître dans les systèmes à surveiller. En se référant à l'objectif des tests des SIS, nous pouvons dire que ces tests (tests de diagnostic, proofs tests, tests partiels, ...) peuvent réaliser les étapes de détection et de localisation des défauts d'un système de diagnostic. Dans le cadre notre travail, nous allons partir de cette idée pour exploiter ces tests à des fins de diagnostic ce qui permet ainsi d'améliorer la performance des SIS. Le schéma de la figure I.4 illustre cette idée :

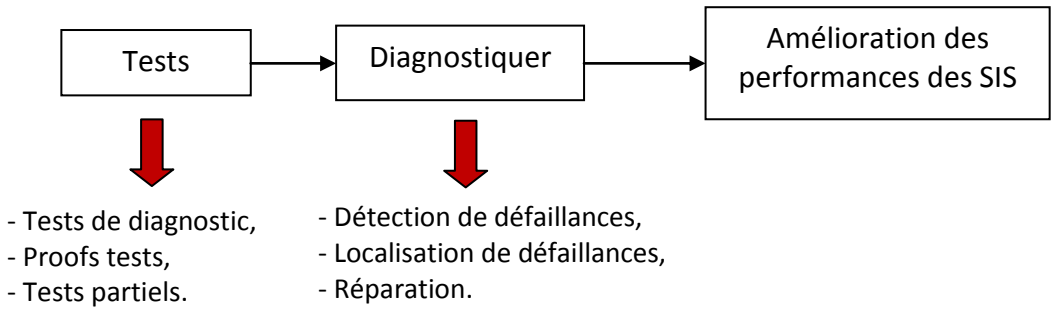


Fig. I.4 Tests et diagnostic des SIS.

Généralement, nous distinguons trois principaux types de tests : les tests de diagnostic (diagnostic testing), les proof tests (proof testing) et les tests partiels (partial tets). Ces trois types de tests sont détaillés ci-après.

I.4.1 Tests de diagnostic

Les tests de diagnostic sont des tests en ligne (online tests) qui détectent les défaillances aléatoires des composants d'un SIS. Ils détectent les défaillances automatiquement et ne nécessite pas l'arrêt du processus. Ils utilisent des fonctionnalités de tests autonomes intégrés (par exemple les chiens de garde) pour détecter les défaillances qui empêchent les SIS de répondre à une demande. Les défaillances identifiées sont annoncées par des alarmes localement au niveau de l'équipement et dans la salle de contrôle. [Rausand 2014].

Les défaillances détectées par les tests de diagnostic sont appelées les défaillances dangereuses détectées que l'on peut noter ici par défaillance-DD. Lorsqu'une défaillance-DD est identifiée, une action immédiate de l'opérateur, chargé de la maintenance, est nécessaire pour réparer le défaut et mettre l'EUC (processus) dans un état sécurisé. Cette réaction rapide aux défaillances-DD doit être conçue pour éviter les déclenchements intempestives (spurious trip) des SIS et limiter au maximum leurs temps en mode dégradé [Rausand 2014].

Les défaillances typiques qui peuvent être détectées par les tests de diagnostic sont : la perte de signal, signal hors portée, élément final en mauvaise position... Un test de diagnostic nécessite du matériels additionnels et/ou des instruction programmées et ajoute une

complexité aux canaux. Il est important de vérifier que la fonction de diagnostic elle-même n'est pas susceptible de nuire à la fonction de sécurité.

On ne peut pas parler des tests de diagnostic sans évoquer un paramètre très important lié à ce type de tests qui est le taux de couverture de diagnostic. La normes IEC 61508 définit le taux de couverture de diagnostic DC (Diagnostic Coverage) pour les tests de diagnostic comme le rapport de taux des défaillances dangereuses détectées λ_{DD} (par un test de diagnostic) et le taux total des défaillances dangereuses λ_D (détectées et non détectées).

Ce taux de couverture de diagnostic reflète la qualité et l'étendue des tests automatiques en ligne. Plus ce taux est important, plus grande est la confiance dans le SIS du fait que les situations sûres prédominent par rapport aux situations dangereuses lors de l'occurrence de défaillances [Mkhida 2008].

L'évaluation du taux DC peut se faire par une analyse des modes de défaillance et de diagnostic au niveau des différents composants d'un système [Goble and Brombacher 1999]. On cherche ainsi à déterminer les défaillances possibles et à savoir si elles peuvent être détectées [Jin et al. 2011]. Donc, la détermination du taux de couverture de diagnostic DC résulte le plus souvent d'un travail d'expertise. La norme IEC 61508 classe généralement le taux DC en 3 catégories : faible (inférieur à 60%), moyen (compris entre 60 et 90%) et élevé (supérieur à 99%) [IEC 61508, 2010]. Cette manière de classer le taux DC d'une part, et le fait de dire que ce taux DC résulte généralement d'un travail d'expertise d'autre part, nous permet de dire que le choix d'une valeur de ce taux pour un calcul donné ne peut être dissociée de la notion de subjectivité. C'est aux experts d'estimer la valeur du taux DC qu'il faut prendre pour évaluer la PFDavg, par exemple. Ceci nous conduit à poser la question suivante : Comment faut-il estimer la valeur du taux DC lorsque on se place par exemple dans le cas "inférieur à 60%"? Est-ce qu'on prend la valeur 20%, 30%,... Donc, cette manière d'estimation ne peut engendrer que de l'imprécision sur les valeurs du taux DC utilisées dans les différents calculs. Ceci nous laisse penser comment il faut tenir compte de ces imprécisions afin de ne pas surestimé ou sous-estimé les valeurs calculées.

I.4.2 Proof tests

Les proof tests sont des tests périodiques soigneusement planifiés, qui sont conçus pour détecter toutes les défaillances latentes d'un SIS qui n'ont pas été révélées par les tests de

diagnostic. Contrairement aux tests de diagnostic, les proof tests nécessitent l'arrêt du processus. Les défaillances révélées par ce type de tests sont appelées défaillances dangereuses non détectées (undetected dangerous failures) que l'on peut noter par défaillances-DU [Rausand 2014].

Les proof tests sont exécutés hors ligne, à des intervalles réguliers, au niveau du système pour vérifier les SIF d'un SIS, alors que le test de diagnostic est plutôt une détection interne en fonctionnement (en ligne) qui agit au niveau composant. [LAMY 2002]. Après le proof test et la réparation associée, le SIS est supposé être "aussi bon que neuf" ou "aussi proche que possible de cette condition". Pour préciser que le proof test est conçu pour déceler toutes les défaillances-DU possibles, ce test est parfois appelé un proof test complet (Full proof test en anglais) ou un proof test parfait (perfect proof test) [Rausand 2014].

Le proof test peut aussi être effectué au niveau des sous-systèmes mais cela s'applique plus à l'industrie du process. [LAMY 2002]. Dans la pratique, un proof test est souvent divisé en sous-tests de sorte que le sous-système capteur, le sous-système unité logique et le sous-système actionneur (élément final) sont testés à différents moments. Dans plusieurs cas, les proof tests sont exécutés manuellement, cependant avec les nouvelle technologies ils peuvent également être automatique ou semi-automatique [Rausand 2014], [Mkhida 2008].

Parmi les bénéfices des proof test est leur contribution dans l'amélioration de la fiabilité des systèmes de sécurité et la réduction de la PFD. L'impact des proof tests sur la fiabilité est montré dans la figure I.5.

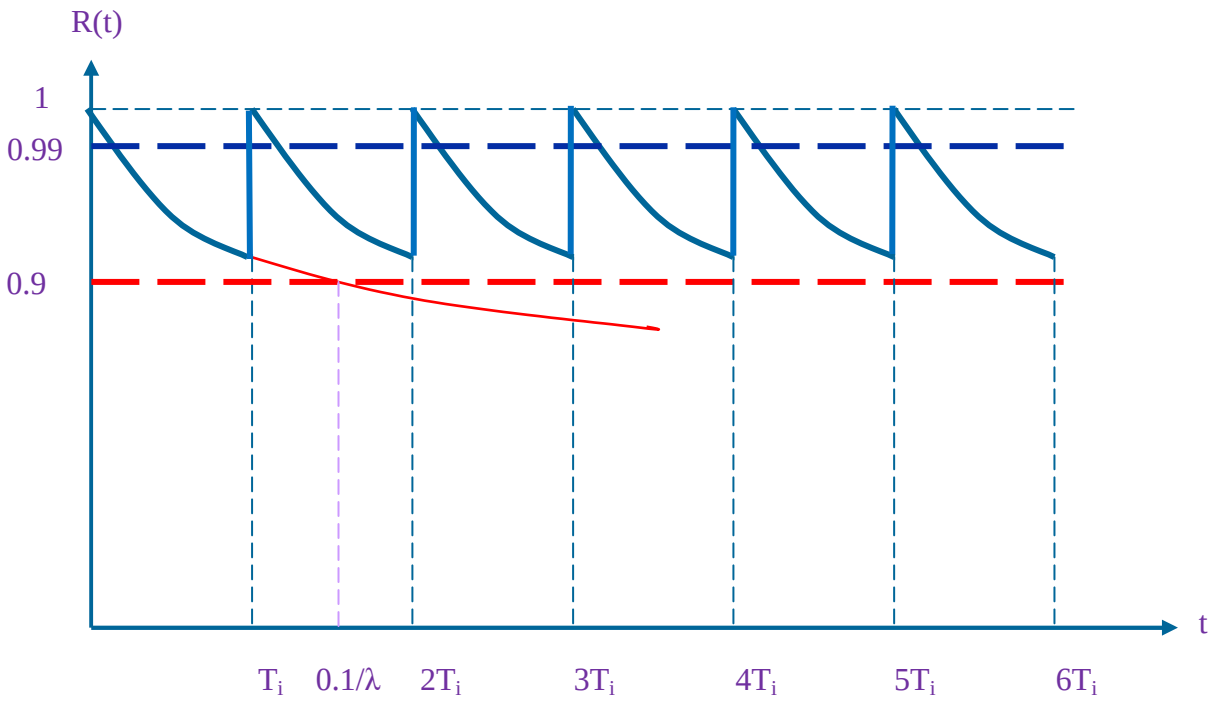


Fig. I.5 Impact des tests périodiques sur la fiabilité.

La figure I.5 montre bien le rétablissement de la fiabilité du système après chaque proof test et ainsi le niveau SIL désiré peut être maintenu. La mesure de la fiabilité R(t) exprime tout simplement l'inverse de la PFD et l'on constate bien sur le graphe qu'en absence des tests périodiques, la valeur R(t) se dégrade nettement et sort de la bande [0.9 , 0.99], par conséquent le SIL n'est plus maintenu à sa valeur [Mkhida 2008]. Comme nous l'avons montré à travers cette description, le proof test peut constituer une démarche qui aide à diagnostiquer les défaillances-DU et donc à améliorer la performance des SIS.

Les proof tests peuvent être effectués en utilisant plusieurs stratégies. Torres-Echeveria et al. [Torres-Echeverria et al. 2009] énumèrent trois stratégies de test principales :

- Test simultané (simultaneous test) où tous les composants sont testés en même temps. Cette stratégie ne convient pas à certains systèmes, car le système n'est pas protégé par le SIS pendant l'exécution du test.

- Test séquentiel (sequential test) où tous les composants sont testés consécutivement l'un après l'autre. Juste après qu'un composant a été testé et mis en service, le

composant suivant est testé et ainsi de suite jusqu'à la fin avec tous les composants du sous-système.

- Test échelonné (staggered test) où tous les composants sont testés avec leur propre période de temps ou dans le même intervalle de test, mais à des moments différents. C'est la stratégie la plus répandue car elle augmente la disponibilité de sécurité du SIS.

I.4.3 Proof tests complets et tests partiels

Les tests partiels sont des tests planifiés, qui sont conçus pour révéler, sans perturber significativement l'EUC, une partie des défaillances-DU traditionnellement détectées uniquement par des proof tests. Ils sont introduit récemment comme complément aux proof tests pour améliorer la fiabilité des SIS opérant en mode de fonctionnement faible demande. [Rausand 2014], [Jin and Rausand 2014].

Une application commune de ces tests partiels est le PST (Partial Stroke Testing pour PST) des vannes ou test partiel de la course de la vanne. Le PST est utilisé comme un moyen semi-automatique pour tester les vannes d'arrêt des processus (Process shutdown valves). [Lundteigen and Rausand 2008].

Les vannes, qui représentent un cas particulier des éléments finaux, sont considérées comme les composants les plus fragiles du fait qu'elles restent sans bouger pendant de longues périodes. Ceci est d'autant plus vrai lorsqu'il s'agit des SIS qui fonctionnent en mode faible demande [Raju 2005]. Le tableau I.2 donne les proportions de défaillance des constituants d'un SIS [Mkhida 2008].

Table I.2 Proportion de défaillances relatives aux constituants d'un SIS

Capteurs	Unités logiques	Eléments finaux
35%	15%	50%

Ce tableau montre bien que la proportion des défaillances des éléments finaux est plus grande que celle des capteurs et des unités logiques.

Le problème rencontré souvent dans les vannes est le blocage en position de fermeture ou d'ouverture du fait qu'il s'agit de dispositifs statiques qualifiés de dormants. Ces éléments ne sont appelés à réagir qu'au moment où il y a une demande suite à un danger qui se présente. Malheureusement, du fait de la durée importante de la non réaction (leur mise en repos) de ces vannes, un certain nombre d'entre elles ne répond pas au moment opportun et elles restent coincer dans leur position de repos [Raju 2005]. C'est pourquoi le PST consiste à tester régulièrement les vannes sur un pourcentage de leur course (10 à 20%) afin de s'assurer que celles-ci ne resteront pas bloquées lorsque l'on en aura besoin. La vanne est actionnée sur une partie de sa course pour tester sa fonctionnalité sans interruption de la production. La proportion de 20% de la course est choisie en se référant au principe de Pareto (règle des 80/20), ce test à 20% permet de déceler 80% des défaillances [MKHIDA 2008].

Donc, un PST signifie une fermeture ou une ouverture partielle d'une vanne puis la remettre à sa position initiale. Ce mouvement de la vanne est si petit que l'impact sur le débit ou la pression du processus est négligeable, mais le mouvement de la vanne peut être suffisant pour révéler plusieurs types de défaillances dangereuses. Le PST peut alors convenir à des processus où un mouvement de petite valeur ne provoque pas de perturbations qui peuvent conduire à des arrêts du processus, ce qui se répercute directement sur la production. Pour de tels processus, il est peut être économiquement viable d'exécuter des PST plus fréquemment que des proof tests [Lundteigen and Rausand 2008].

Cependant, le PST a des limites. Le test de course partielle ne garantit pas que la vanne fonctionnera lorsqu'elle sera sollicitée pour une fermeture complète par exemple. En effet, il se peut qu'il y ait un nouveau blocage et donc la vanne ne se ferme pas complètement mais uniquement à 20% de la course.

D'autres solutions alternatives au PST consistent à utiliser une vanne de dérivation (by-pass) autour de la vanne d'arrêt ou prévoir une redondance. Ces solutions sont qu'elles soient coûteuses ou potentiellement dangereuses [Gruhn et al. 1998]. En effet le doublement du nombre de vannes augmente le coût de l'équipement de base, mais aussi les coûts de mains d'œuvre liés aux essais de maintenance puisque les tests périodiques portent sur un nombre plus élevé de vannes. En plus, les coûts de la tuyauterie supplémentaire pour les vannes de dérivation sont importants. Le danger peut provenir d'une vanne de dérivation qui ne peut remplacer la vanne d'arrêt au moment du test de celle-ci hors ligne.

Un proof test qui révèle toutes les défaillances-DU, où le SIS après ce test est restauré dans une condition "aussi bonne que neuve", s'appelle un proof test parfait (perfect proof test en anglais) ou un proof test complet (Full proof test en anglais). Dans les calculs de fiabilité, on suppose généralement que les proof tests sont des proof tests parfaits. Dans la pratique, il se peut que certains proof tests ne soient pas parfaits en raison [Lundteigen and Rausand 2008], [Rausand 2014] : (i) que le proof test est inadéquat et n'est pas capable de révéler toutes les défaillances-DU, (ii) que le proof test est effectué dans des conditions qui diffèrent d'une situation de demande réelle, (iii) d'une mauvaise exécution du proof test.

Les tests partiels sont évidemment considérés comme des proof tests imparfait car ils ne permettent quant à eux que de détecter une fraction de défaillance-DU laissant les autres non détectées jusqu'au lancement du proof test [Lundteigen and Rausand 2008]. Les inspections visuelles, les contrôles incomplets et les essais imparfaits sont des exemples de test partiels. Les tests partiels sont moins efficaces que les proof tests mais ils peuvent être préférés aux proof tests pour les raisons suivantes [Brissaud et al.] : (i) Les proof tests exigent souvent des arrêts de production qui sont parfois inacceptables du point de vue coût, (ii) Les proof tests perturbent les processus et (iii) certains systèmes de sécurité ne peuvent pas être pleinement testés sans dégradation ou destruction (mures coupe feux, disques de ruptures).

Les tests partiels sont réalisés pour consolider les proof tests afin d'éliminer le maximum de défaillance-DU. En effet, la PFD_{avg} est réduite lorsque des tests partiels sont introduits car une fractions de défaillances-DU est révélée et réparée dans un intervalle de temps plus court, après leur apparition, que par des proof tests. Ainsi, l'ajout des tests partiels aux proof tests améliore la fiabilité des SIFs et permet de prolonger l'intervalle entre les proof tests. En conséquence, les coûts d'exploitation et d'entretien peuvent être réduits car on aura moins d'arrêts de production programmés et moins d'heures de mains d'œuvre pour la réparation des défaillances-DU [Lundteigen and Rausand 2008], [Rausand 2014].

I.5 Conclusion

Les SIS sont devenus actuellement très répandus dans les différentes industries en raison de leur importance et du rôle que jouent ce type de systèmes dans la prévention des accidents potentiels qui peuvent se produire. Pour ces industries, la disponibilité des SIS est primordiale. Toute défaillance qui peut entraver un SIS d'exécuter sa (ou ses) fonction(s)

instrumentée(s) de sécurité doit être révélée et réparée. Pour cela, nous nous sommes concentrés, le long de ce chapitre, sur les différents tests que nous venons de présenter et nous avons montré clairement que ces tests peuvent contribuer dans le diagnostic des défaillances et ainsi améliorer la performance des SIS.

Dans le chapitre suivant nous nous focalisons sur l'incertitude qui peut affecter certains paramètres dans le processus d'évaluation des risques et comment cette incertitude peut poser réellement un grand problème dans l'évaluation de la performance des SIS.

Chapitre II

Evaluation des systèmes par le modèle de Markov flou

II.1 Introduction

Face aux enjeux importants pour la santé, les biens et l'environnement, la sécurité fonctionnelle des SIS doit être évaluée en accord avec les normes IEC 61508 et IEC 61511 [IEC 61508, 2010], [IEC 61511, 2003]. Dans ce contexte, un élément majeur développé dans ces normes est l'évaluation quantitative de la performance du SIS mis en œuvre. En effet pour une SIF faiblement sollicitée, ces normes prévoient la PFD_{avg} comme un critère quantitatif qui permet de juger la performance d'un SIS [Innal 2008], [Rausand 2014]. Dans ce mémoire, nous nous plaçons uniquement dans le contexte des SIS faiblement sollicités.

Cette performance doit être évaluée par des méthodes référencées comme les équations simplifiées, les arbres de défaillances (AdD), les diagrammes blocs de fiabilité (DBF), les chaînes de Markov ainsi que les réseaux de Pétri [Innal 2008], [Rausand 2014]. Dans ce cadre, les chaînes de Markov comme modèle de fiabilité sont largement utilisées pour l'évaluation des PFD des SIS. En effet, parmi plusieurs méthodes explorées, il a été conclu que le modèle de Markov est le plus approprié car ; il permet de modéliser facilement différentes situations [Goble and Cheddie 2005], [Innal et al. 2006].

Dans les études de fiabilité et d'indisponibilité par le modèle de Markov, on suppose que les probabilités de transitions, basées sur les données de fiabilité des composants (taux de défaillance, taux de réparation), sont souvent disponibles (banques ou bases de données de fiabilité), précises et validées par le retour d'expérience [sallak 2007]. Suite à ces considérations, on peut dire que l'évaluation quantitative, dans ces études traditionnelles, ne

pose aucun problème. Cependant, nous pouvons s'interroger sur leur adaptation à des systèmes hautement fiables pour lesquels les défaillances sont très rares et le retour d'expérience est insuffisant pour valider avec précision ces données. C'est le cas des SIS qui opèrent en mode faible demande [Sallak 2007], [Wang et al. 2004], [Villmeur 1988].

Pour faire face à ce problème de manque de données et dans le but d'évaluer la performance des SIS, les analystes font recours généralement soit aux bases de données de fiabilité génériques, soit aux jugements d'experts pour estimer les taux de défaillance des composants des SIS. Cependant, l'utilisation de ces données, issues de ces sources, introduit des incertitudes. Ce manque de données concernant les composants du SIS peut conduire à des résultats incertain, et ainsi produire une valeur sous-estimée ou surestimée de la performance du SIS [Markowski et al. 2011].

La grande question qui se pose est : "Où doit-on trouver des données de fiabilité de qualité, qui peuvent être utilisées pour évaluer la performance de tels systèmes hautement fiables pour lesquels l'on dispose d'un grand manque de connaissance et le retour d'expérience est malheureusement faible et insuffisant ?".

Dans le but de surmonter cette difficulté, des méthodes autres que les approches probabilistes classiques (les ensembles flous par exemples) peuvent utiliser avantageusement ces données pour prendre en compte l'imprécision liée aux paramètres de défaillance et calculer la PFD_{avg} qui caractérise la performance du SIS [Markowski et al. 2011], [Bowles and Pelaez 1995].

Les paramètres des composants d'un SIS tels que les taux de défaillance, la couverture de diagnostic DC (diagnostic coverage), les défaillances de causes communes CCF (Common Cause Failure) sont des sources d'incertitude qui affectent la performance du SIS. Par conséquent, les modèles flous basés sur des nombres flous sont largement utilisés pour traiter l'incertitude de ces paramètres.

Dans ce chapitre, nous examinons brièvement la notion d'incertitude liée au processus d'évaluation des risques et ces différentes sources en insistant surtout sur l'incertitude relatives aux paramètres caractéristiques du SIS tels que le facteur β et le taux DC. Puis, nous introduisons des concepts de base concernant la théorie des ensembles flou. Et enfin, nous présentons le modèle de Markov flou qui consiste à traiter les chaînes de Markov floues pour l'évaluation de la performance des SIS en utilisant l'approche développée par Buckley et

Eslami [Buckley and Eslami 2002] dite multiplication restreinte des matrices floues (RFMM pour Restricted Fuzzy Matrix Multiplication).

II.2 Incertitude dans le processus d'évaluation des risques

II.2.1 Sources d'incertitude

L'incertitude est un mot courant dans notre langage quotidien, mais il est utilisé avec des significations différentes dans différents contextes. En ce qui concerne les évaluations de la fiabilité et des risques l'interprétation de l'incertitude est encore débattue [Jin et al. 2012]. Selon [Jin et al. 2012] les probabilités dans les évaluations du risque et de fiabilité doivent être interprétées comme des probabilités subjectives. Cela s'applique également pour la PFD_{avg}. Effectivement lors du calcul de la PFD_{avg}, nous utilisons la connaissance disponible pour sélectionner les modèles et les paramètres appropriés, nous calculons une valeur pour la PFD_{avg} et nous appelons enfin de compte cette valeur notre PDF_{avg} estimée. Dans ce processus, nous sommes conscients que nous faisons beaucoup de simplifications et d'approximations qui influenceront la PFD_{avg} estimée et rendront notre estimation incertaine [Jin et al. 2012].

L'incertitude peut provenir de deux causes principales, la variation naturelle et le manque de connaissance sur le système ou le processus. Ces deux catégories d'incertitudes sont appelées respectivement incertitude aléatoire et incertitude épistémique. L'incertitude aléatoire est due à la variabilité naturelle du phénomène alors que l'incertitude épistémique résulte du manque de connaissances.

L'incertitude épistémique peut être réduite si de nouvelles connaissances et informations sur le système peuvent être acquises, alors que l'incertitude aléatoire ne peut pas être réduite et elle est parfois appelées incertitude irréductible [Rausand 2014], [Jin et al. 2012], [Cooke and Bedford 2001]. Cependant plusieurs types d'incertitudes qui étaient auparavant classés comme aléatoire sont maintenant considérés comme épistémiques, ce qui indique que la classification d'incertitude n'est pas fixe, mais peut varier à mesure que la compréhension fondamentales des phénomènes naturels augmente. Certains auteurs considèrent donc que toute incertitude est épistémique[Jin et al. 2012]. Dans le cadre de ce

présent document, seules les sources d'incertitudes épistémiques seront brièvement examinées. Nous distinguons donc trois types d'incertitudes épistémiques :

- **Incertitude de complétude (completeness uncertainty)**

Ce type d'incertitude dépend essentiellement de facteurs qui ne sont pas inclus dans les modèles d'évaluation des risques. Deux catégories relatives à ce type d'incertitude sont décrites dans la littérature, à savoir l'incertitude de complétude connue et l'incertitude de complétude inconnue. L'incertitude connue est souvent due à des facteurs manquants dans le processus d'analyse. En effet, différentes raisons peuvent être considérées comme les origines de cette incertitude, à savoir le manque de compréhension des modèles de traitement, le manque de données utilisées par ces modèles ou l'incompétence des analystes. La deuxième catégorie, parfois appelée «ignorance», est due à des facteurs inconnus liés aux systèmes tels que la complexité du processus «interactions internes / externes», le caractère invisible des mécanismes de défaillance des composants, la mauvaise compréhension de certaines propriétés du système et des facteurs opérationnels et environnementaux.

- **Incertitude de modèle (modeling uncertainty)**

Cette incertitude est rencontrée dans les évaluations de fiabilité et des risques. Elle est associée aux modèles de fiabilité utilisés dans la modélisation des caractéristiques du système. Cette incertitude survient du fait que n'importe quel modèle, que ce soit de nature conceptuelle ou mathématique, n'est qu'une représentation simplifiée de la réalité du phénomène ou du système étudié. De nombreux facteurs peuvent contribuer à cette incertitude, notamment [CCP 2000], [Abrahamsson 2002], [Markowski et al. 2010] , [Leduy 2011] : la bonne connaissance du phénomène étudié, l'inadéquation des modèles utilisés dans le processus d'évaluation des risques, le niveau de détail requis dans une évaluation, l'inadaptation des modèles aux spécificités du système, le degré de simplification adopté, les hypothèses formulées par les experts pour modéliser le phénomène et les formules approximatives utilisées dans l'évaluation.

- **Incertitude paramétrique (parameter uncertainty)**

Ce sont les incertitudes qui se rapportent essentiellement aux données utilisées dans les modèles d'évaluation de la fiabilité. Cette source d'incertitude est souvent due au manque de données et de pertinence causé par une mauvaise statistique utilisée dans les paramètres

estimés. En outre, elle peut être inhérente aux bases de données génériques en tant que sources d'information pour les évaluations de fiabilité. De plus, d'autres facteurs tels que les conditions spécifiques, l'environnement opérationnel et les procédures de maintenance peuvent être considérés comme les origines de cette incertitude. Ce type d'incertitudes est fréquent car les données disponibles et utilisées dans le secteur industriel sont souvent incomplètes, incorrectes et entachées d'incertitudes. On a souvent tendance à utiliser des valeurs moyennes uniques ou des intervalles de confiance issus du retour d'expérience, de la littérature ou des jugements d'experts. Notons enfin que ce type d'incertitudes est facile à quantifier car il existe des méthodes mathématiques qui permettent leur traitement quantitatif [CCP 2000], [Markowski et al. 2010]. Le présent document traite de type d'incertitude que l'on peut rencontrer dans l'évaluation des performances du SIS.

II.2.2 Incertitudes des paramètres caractéristiques du SIS

Les SIS sont des systèmes qui ont pour objectif de mettre le procédé qu'ils surveillent en position de repli de sécurité (c'est à dire un état stable ne présentant pas de risque pour les personnes, les équipements et l'environnement) lorsque celui-ci évolue vers une voie comportant un risque réel. Un SIS en mode faible demande, qui est le mode le plus courant dans l'industrie des procédés, est normalement passif et ne sera activé qu'en cas de demande. En effet, dans les installation industrielles, les SIS sont des systèmes rarement sollicités et qui ne sont activés que suite à une demande émanant d'un EUC pour le protéger contre les événements dangereux qui peuvent se produire et durant les opérations normales du processus, ces systèmes demeurent statiques et dormants. Selon Goble [Goble et Cheddie 2005] la période moyenne entre l'occurrence d'événements dangereux est souvent estimée à plus d'une dizaine d'années. De plus, les SIS sont conçus pour être très fiables et l'on s'attend donc à ce que peu de défaillances se produisent même pendant une longue période d'exploitation. De ce fait, on peut dire que les composants des SIS n'ont pas fonctionné assez longtemps pour fournir des données statistiques suffisantes sur les défaillances [Sallak 2007] [Wang et al. 2004], [Jin et al. 2012]. Pour ce mode de fonctionnement, les SIS sont alors des dispositifs sur lesquels nous n'avons pas de données en quantité suffisante et le retour d'expérience est naturellement faible. Ainsi, les probabilités manipulées pour l'évaluation de la performance des SIS peuvent sembler peu crédibles ce qui induit une grande incertitude sur leurs valeurs.

Le même problème se pose également lorsque l'on traite de nouveaux composants, en empruntant des données de laboratoire et génériques ou en manipulant des jugements d'experts [Markowski et al. 2010], [Sallak et al. 2008]. En outre, les taux de défaillance que nous trouvons, par exemple dans la base OREDA, sont basés sur des données de composants qui ont été installés plusieurs années (souvent 10 à 15 ans) avant la fin de la collection des données. En raison du développement technologique rapide, par exemples les capteurs intelligents, ces estimations des taux de défaillances peuvent ne pas représenter du tout la technologie qui sera utilisée dans les nouveaux SIS. De plus, les conditions opérationnelles et environnementales des éléments utilisés dans un nouveau SIS sont parfois très différentes des conditions dans lesquelles les données ont été collectées [Jin et al. 2012]. Tout ceci ne fait que réduit notre connaissance et par conséquent augmenter l'incertitude. Selon Kletz [Kletz 1999], les données de fiabilité recueillies pour un composant peuvent changer d'un facteur de 3 ou 4, et un facteur de 10 n'est pas à exclure.

D'autres paramètres des composants du SIS sont également concernés par le manque de données, tels que les taux DC et les facteurs CCF. Le choix du taux DC et du facteur CCF est bien justifié par le fait que, dans de nombreuses situations, il existe peu de directives sur la façon d'estimer ces paramètres en termes de modèles de support de données. Ainsi, par rapport aux taux de défaillance dangereux qui sont généralement disponibles dans les sources de données telles que OREDA, le taux DC et le facteur CCF sont plutôt estimés par des jugements d'experts [Jin et al. 2012], [Mechri et al. 2013]. De plus, pour ces paramètres, la norme IEC 61508 ne définit que quelques ordres de grandeur. Donc, cette manière d'estimation de ces paramètres ne peut engendrer que de l'imprécision sur leurs valeurs utilisées dans les différents calculs.

Pour pallier à ce problème, la théorie des ensembles flous est un outil puissant pour traiter l'incertitude des paramètres dans les modèles de fiabilité [Markowski et al. 2011], [Bowles and Pelaez 1995]. Les modèles flous reflètent bien la formulation approximative des données fournies par un expert ou issus de la littérature, comme est « autour de m » ou est « entre a et b ». On peut utiliser avantageusement ces représentations de l'incertitude des paramètres pour évaluer la performance du SIS dans un environnement flou [Zadeh 1965].

II.2.2.1 Taux de couverture de diagnostic DC

Les défaillances des SIS peuvent être classées selon deux types de défaillances : les défaillances dangereuses (D) et les défaillances sûres (S). Une défaillance est dite dangereuse si la SIF est inhibé par cette défaillance, sinon elle est dite sûre. Dans ce document, seules les défaillances-D sont prises en compte pour déterminer la PFD_{avg}. Les défaillances-D peuvent être subdivisées en défaillances dangereuses détectées (DD) et dangereuses non détectées(DU). Les défaillances-DD sont révélées par des tests de diagnostic, tandis que les défaillances-DU ne sont révélées que par des proof tests [Rausand 2014].

La norme IEC 61508 définit le taux de couverture de diagnostic DC (Equation II.1) comme le rapport entre le taux de défaillance des pannes dangereuses détectées λ_{DD} (par un test de diagnostic) et le taux de défaillance total des pannes dangereuses λ_D (détectée et non détectée) [IEC 61508, 2010].

$$DC = \frac{\lambda_{DD}}{\lambda_D} \qquad \text{avec} \qquad \lambda_D = \lambda_{DD} + \lambda_{DU} \tag{II.1}$$

En pratique, L'évaluation du taux de couverture de diagnostic DC résulte le plus souvent d'un travail d'expertise. La norme IEC 61508 classe généralement ce taux DC en trois catégories et ne définit que quelques ordres de grandeur. Donc, cette manière d'estimer le taux DC ne fait qu'engendrer de l'imprécision sur les valeurs utilisées dans les différents calculs.

Alors, compte tenu de l'incertitude sur le taux DC, les taux flous des défaillances-DD, $\tilde{\lambda}_{DD}$, et des défaillances-DU, $\tilde{\lambda}_{DU}$, sont alors déterminés par :

$$\tilde{\lambda}_{DD} = \widetilde{DC}\lambda_D \qquad \text{et} \qquad \tilde{\lambda}_{DU} = (1 - \widetilde{DC})\lambda_D \tag{II.2}$$

II.2.2.2 Facteur β des défaillances de cause commune

Les défaillances de cause commune (CCF pour *Common Cause Failures*) constituent une menace sérieuse pour la fiabilité du SIS et peuvent entraîner des défaillances simultanées des canaux redondants. Dans de nombreux cas, il peut être nécessaire de considérer l'impact des CCF sur la performance du SIS [Lundteigen and Rausand 2007], [Hokstad and Rausand 2008]. La norme IEC 61508 a souligné la présence des CCF pour les architectures

redondantes qui peuvent apparaître dans les canaux suite à la même cause. En outre, elle met l'accent sur la nécessité de contrôler les CCF afin de maintenir le SIL de la fonction de sécurité.

L'évaluation des CCF peut être déterminée à partir des données du retour d'expérience. Mais, très peu de sources de données sont disponibles pour les CCF. La seule exception concerne l'industrie de l'énergie nucléaire qui a établi la base de données internationale sur les causes communes. Les CCF dépendent fortement des conditions physiques et des conditions opérationnelles et environnementales. Il est donc difficile d'affirmer qu'un taux CCF dans une installation sera similaire au taux CCF dans une autre installation [Jin et al. 2012]. Ce manque de données relatives aux CCF ne fait qu'engendrer de l'imprécision sur ce paramètre important dans l'évaluation de la performance des SIS. Cependant, étant donné la difficulté d'obtenir de telles données, des modèles paramétriques de CCF ont été développés. Parmi ces modèles, nous trouvons le modèle du facteur β, la méthode PDS, le modèle des lettres grecques multiples (MGL), le modèle du facteur α et le modèle du taux de défaillance binomial [Rausand 2014], [Lundteigen et Rausand 2007], [Hoyland et Rausand 2004].

Dans ce travail, nous utilisons le modèle du facteur β, qui a été introduit par Fleming en 1975, en raison de sa simplicité. De plus, il est suggéré comme un modèle de CCF approprié dans la norme IEC 61508 [Rausand 2014]. L'idée du modèle du facteur β est de diviser le taux de défaillance total λ d'un composant en deux parties : $\lambda^{(i)}$ qui est le taux de défaillance indépendant du composant et $\lambda^{(c)}$ qui est le taux de défaillance de cause commune. Selon le modèle du facteur β, le taux de défaillance total d'un composant est :

$$\lambda = \lambda^{(i)} + \lambda^{(c)} \tag{II.3}$$

Le modèle du facteur β indique la proportion relative des défaillances de cause commune parmi toutes les défaillances du composant. Le paramètre β est défini comme la probabilité de défaillance due à une cause commune étant donné l'occurrence d'une défaillance. L'expression de β est donnée par :

$$\beta = \frac{\lambda^{(c)}}{\lambda^{(i)}+\lambda^{(c)}} = \frac{\lambda^{(c)}}{\lambda} \tag{II.4}$$

Où : $\lambda^{(c)} = \beta\lambda$ et $\lambda^{(i)} = (1-\beta)\lambda$ (II.5)

Notons β le facteur des CCF pour les défaillances-DU et β_D pour les défaillances-DD. Selon les équations (II.2) et (II.5), et compte tenu de l'incertitude sur le facteur β et le taux DC, les différents taux flous des défaillances dangereuses détectées et non détectées deviennent :

$$\begin{cases} \tilde{\lambda}_{DD}^{(i)} = (1-\tilde{\beta}_D)\tilde{\lambda}_{DD} = (1-\tilde{\beta}_D)\tilde{D}C\ \lambda_D \\ \tilde{\lambda}_{DD}^{(c)} = \tilde{\beta}_D\tilde{\lambda}_{DD} = \tilde{B}_D\ \tilde{D}C\ \lambda_D \\ \tilde{\lambda}_{DU}^{(i)} = (1-\tilde{\beta})\tilde{\lambda}_{DU} = (1-\tilde{\beta})(1-\tilde{D}C)\lambda_D \\ \tilde{\lambda}_{DU}^{(c)} = \tilde{\beta}\tilde{\lambda}_{DU} = \tilde{\beta}(1-\tilde{D}C)\lambda_D \end{cases} \quad (II.6)$$

II.3 Modélisation floue

II.3.1 Théorie des ensembles flous

La théorie des ensembles flous a été introduite par le professeur Lotfi Zadeh [Zadeh 1965] avec l'idée de pouvoir manipuler des informations exprimées en langage naturel. Cet objectif a nécessité d'étendre la théorie des ensembles classique. Dans la théorie des ensembles classique une proposition peut être vraie ou fausse, tandis qu'en théorie des ensembles flous une proposition peut être partiellement vraie et fausse.

II.3.1.1 Définitions

Définition 1

Un sous-ensemble usuel (classique) A d'un ensemble de référence Ω peut être défini par sa fonction caractéristique :

$$\mu_A : \Omega \longrightarrow \{0,1\} \quad \text{II.7)}$$

Un élément x de l'ensemble de référence Ω est un élément du sous-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 de la fonction caractéristique $\mu_A(x)$ est donnée comme suit :

$$\mu_A(x) = \begin{cases} 1 & si \quad x \in A \\ 0 & si \quad x \notin A \end{cases} \tag{II.8}$$

Définition 2

Un sous-ensemble flou $\tilde{A}$ est caractérisé par sa fonction d'appartenance $\mu_{\tilde{A}}(x)$; Zadeh [Zadeh 1965] en donne la définition suivante : "Un sous-ensemble flou $\tilde{A}$ sur un référentiel Ω est caractérisé par une fonction d'appartenance $\mu_{\tilde{A}}$ qui associe à chaque élément x de Ω un nombre réel dans l'intervalle [0,1]" :

$$\mu_{\tilde{A}} : \Omega \longrightarrow [0,1] \tag{II.9}$$

La valeur de $\mu_{\tilde{A}}(x)$ représente le degré d'appartenance de x à A. Le degré d'appartenance d'un élément x de Ω à A n'appartient plus à la paire $\{0,1\}$ comme pour un ensemble classique, mais à l'intervalle réel [0,1]. Si $\mu_{\tilde{A}}(x) = 1, x$ appartient totalement à A. Si $\mu_{\tilde{A}}(x) = 0, x$ n'appartient pas du tout à A. Si $0 < \mu_{\tilde{A}}(x) < 1, x$ appartient partiellement à A.

La fonction d'appartenance peut être aussi défini par :

$$\mu_{\tilde{A}}(x) = \begin{cases} 1 & si \quad x \in A \\ 0 & si \quad x \notin A \\ \alpha & si \quad 0 < \alpha < 1 \end{cases} \tag{II.10}$$

II.3.1.2 Caractéristiques d'un sous-ensemble flou

Un sous-ensemble flou $\tilde{A}$ présente les caractéristiques suivantes :

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

$$Supp\left(\tilde{A}\right) = \{x \in \Omega, \mu_{\tilde{A}}(x) > 0\} \quad \text{(II.11)}$$

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

$$h\left(\tilde{A}\right) = Sup_{x\in\Omega}\mu_{\tilde{A}}(x) \quad \text{(II.12)}$$

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

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

$$Noy(\tilde{A}) = \{x \in \Omega\,, \mu_{\tilde{A}}(x) = 1\} \quad \text{(II.13)}$$

La figure II.1 illustre les trois caractéristiques décrites ci-dessus.

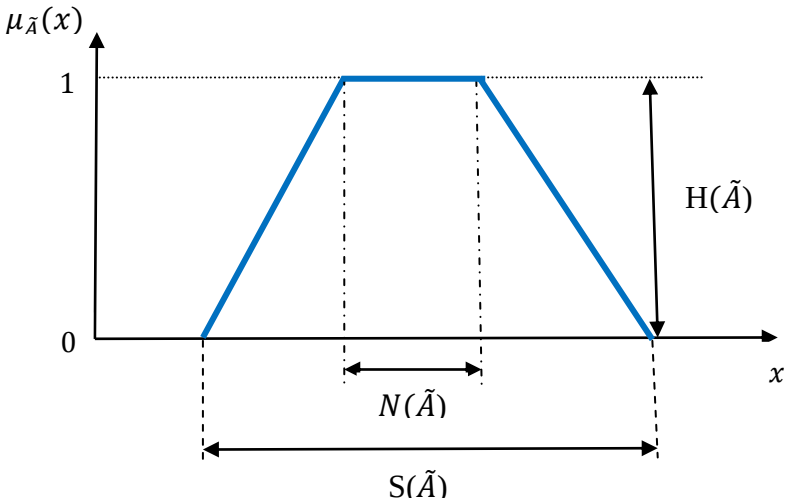


Fig. II.1 Caractéristique d'un sous-ensemble flou.

II.3.1.3 Nombres flous

On appelle «nombre flou» tout sous-ensemble flou Ã du référentiel Ω, qui satisfait aux propriétés suivantes :

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

Comme dans le cadre de notre travail, on ne s'est intéressé qu'aux fonctions triangulaires en raison de leur simplicité, seule cette représentation est décrite ici. Le nombre flou triangulaire peut être noté par le triplet (m , a , b), comme le montre la Figure II.2.

Mathématiquement, la fonction d'appartenance correspondante s'écrit donc :

$$\mu_{\tilde{A}}(x) = \begin{cases} \frac{x-a}{m-a} & , \quad a \leq x \leq m \\ 1 & , \quad x = m \\ \frac{b-x}{b-m} & , \quad m \leq x \leq b \\ 0 & , \quad ailleurs \end{cases} \qquad \text{(II.14)}$$

Nous notons $\tilde{A} = (m, a, b)$ un nombre flou triangulaire. m sa valeur modale avec $\mu_{\tilde{A}}(m) = 1$, a est la largeur de son support à gauche de m, encore appelé étalement gauche, b celle de son support à droite de m, encore appelé étalement droit.

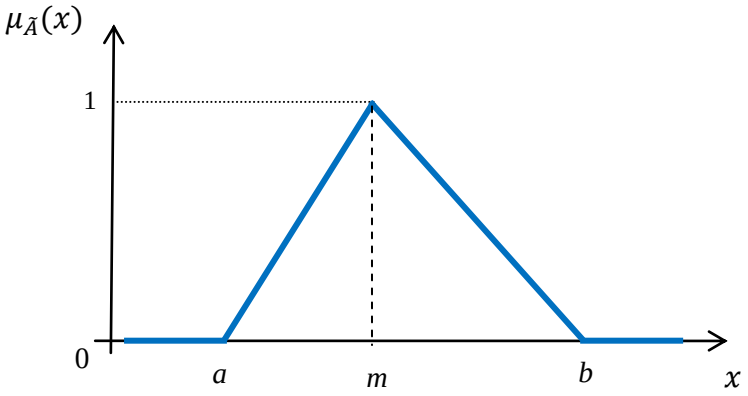


Fig. II.2 Nombre flou triangulaire.

II.3.1.4 Notion d'α coupe

Un nombre flou Ã peut être représenté généralement, soit par sa fonction d'appartenance, soit par ses coupes de niveau α. Une α-coupe est définie comme suit :

$$\tilde{A}_\alpha = \{x \in \Omega \, , \mu_{\tilde{A}}(x) \geq \alpha\} \ , \ \alpha \in [0,1] \qquad \text{(II.15)}$$

Les opérations arithmétiques utilisées pour manipuler les nombres flous requièrent beaucoup de ressources. Kaufman et Gupta [Kaufman and Gupta 1991] ont montré que ces efforts de calculs peuvent être largement simplifiés par la décomposition des fonctions d'appartenance des nombres flous en α-coupes. En effet, si nous considérons un nombre flou Ã de fonction d'appartenance $\mu_{\tilde{A}}(x)$ (voir figure II.3), nous pouvons obtenir plusieurs intervalles emboîtés en utilisant la méthode des α-coupes. $A_L^{(\alpha)}$ et $A_R^{(\alpha)}$ représentent respectivement les limites droites et gauches de la fonction d'appartenance $\mu_{\tilde{A}}(x)$ à chaque coupe de niveau α.

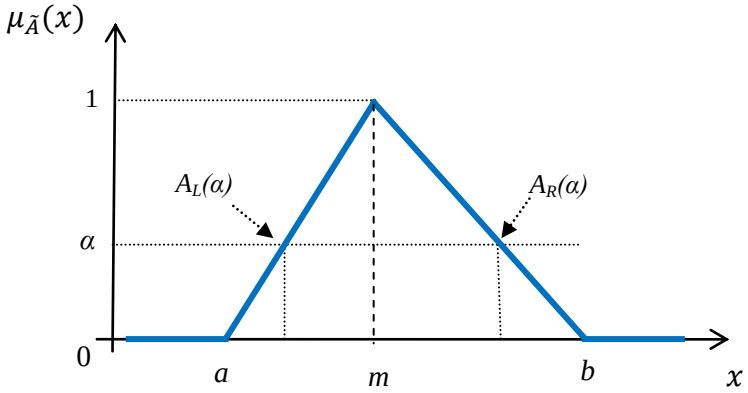


Fig. II.3 α-coupe d'un nombre flou.

En utilisant la méthode des α-coupes, un nombre flou peut être représenté par l'expression suivante :

$$\tilde{A} \longrightarrow \left[A^{(\alpha)}\right] = \left[A_L^{(\alpha)} \, , A_R^{(\alpha)}\right] \ , \ 0 \leq \alpha \leq 1 \qquad \text{(II.16)}$$

II.3.1.5 Opérations arithmétiques sur les nombres flous

La décomposition des fonctions d'appartenance des nombres flous en α-coupes a largement facilitée les différentes opérations arithmétiques sur ces nombres. Soient $\tilde{A}$ et $\tilde{B}$ deux nombres flous représentés respectivement par les intervalles $\left[A_L^{(\alpha)}, A_R^{(\alpha)}\right]$ et $\left[B_L^{(\alpha)}, B_R^{(\alpha)}\right]$ pour chaque α-coupe. Les opérations arithmétiques appliquées à ces deux nombres flous donnent les expressions suivantes :

1. Addition : $\tilde{C} = \tilde{A} + \tilde{B} \rightarrow \left[C_L^{(\alpha)}, C_R^{(\alpha)}\right] = \left[A_L^{(\alpha)} + B_L^{(\alpha)}, A_R^{(\alpha)} + B_R^{(\alpha)}\right]$ (II.17)
2. Soustraction : $\tilde{C} = \tilde{A} - \tilde{B} \rightarrow \left[C_L^{(\alpha)}, C_R^{(\alpha)}\right] = \left[A_L^{(\alpha)} - B_R^{(\alpha)}, A_R^{(\alpha)} - B_L^{(\alpha)}\right]$ (II.18)
3. Produit : $\tilde{C} = \tilde{A} \,.\, \tilde{B} \rightarrow \left[C_L^{(\alpha)}, C_R^{(\alpha)}\right]$

avec : $\begin{cases} C_L^{(\alpha)} = \min(A_L^{(\alpha)}.B_L^{(\alpha)},\ A_L^{(\alpha)}.B_R^{(\alpha)},\ A_R^{(\alpha)}.B_L^{(\alpha)}, A_R^{(\alpha)}.B_R^{(\alpha)}) \\ C_R^{(\alpha)} = \max(A_L^{(\alpha)}.B_L^{(\alpha)},\ A_L^{(\alpha)}.B_R^{(\alpha)},\ A_R^{(\alpha)}.B_L^{(\alpha)}, A_R^{(\alpha)}.B_R^{(\alpha)}) \end{cases}$ (II.19)

4. Division : $\tilde{C} = \tilde{A}/\tilde{B} \rightarrow \left[C_L^{(\alpha)}, C_R^{(\alpha)}\right]$

avec : $\begin{cases} C_L^{(\alpha)} = \min(A_L^{(\alpha)}/B_L^{(\alpha)},\ A_L^{(\alpha)}/B_R^{(\alpha)},\ A_R^{(\alpha)}/B_L^{(\alpha)}, A_R^{(\alpha)}/B_R^{(\alpha)}) \\ C_R^{(\alpha)} = \max(A_L^{(\alpha)}/B_L^{(\alpha)},\ A_L^{(\alpha)}/B_R^{(\alpha)},\ A_R^{(\alpha)}/B_L^{(\alpha)}, A_R^{(\alpha)}/B_R^{(\alpha)}) \end{cases}$ (II.20)

II.3.2 Evaluation flou de la performance

II.3.2.1 Model de Markov flou

Plusieurs recherches ont montré l'intérêt des Chaînes de Markov floues (en anglais Fuzzy Markov Chain : FMC) lorsqu'il s'agit de données de transition imprécises. Voir par exemple [Avrachenkov and Sanchez 2002], [Buckley and Eslami 2002], [Li and Xiu 2014], [Kozine and Utkin 2002]. Buckley et Eslami [Buckley and Eslami 2002] ont traité des chaînes de Markov floues régulières et absorbantes en utilisant une méthode appelée multiplication restreinte des matrices floues (en anglais Restricted Fuzzy Matrix Multiplication : RFMM).

Comme le calcul de la FPD floue d'une SIF est principalement basé sur cette approche, plus de détails seront examinés dans cette section. Mais avant, certains des résultats de base des chaînes de Markov classiques finies sont présentés afin de voir les similitudes et les différences avec les chaînes de Markov floues (voir par exemple: [Buckley 2005], [Cassandras and Lafortune 2008]).

Une chaîne de Markov finie a un nombre fini d'états possibles; le processus de Markov est considéré seulement aux moments où l'état du système change. Ainsi, l'ensemble des états est $S = \{S_1, S_2, \dots, S_r\}$. Lorsque le processus est dans l'état S_i à l'instant (étape) n, la probabilité qu'il passe à l'état S_j à l'instant suivant (n+1) est fournie par :

$$p_{ij} = Prob\left(S_j^{(n+1)} \middle| S_i^{(n)}\right) \tag{II.21}$$

où $1 \leq i, j \leq r$ et $t = 1, 2, \dots$. Les p_{ij} sont des probabilités de transition qui ne dépendent pas des états dans lesquels se trouvait le processus avant l'état actuel. La matrice de transition $M = (p_{ij})$ est une matrice $r \times r$ des probabilités de transition. Une propriété importante de M est que les sommes des lignes sont égales à l'unité, c'est-à-dire $\sum_{j \neq i} p_{ij} = 1$, et chaque $p_{ij} \geq 0$.

Soit la matrice M^n le produit de M n-fois. Ainsi, le *ijème* élément $p_{ij}^{(n)}$ de M^n donne la probabilité que la chaîne de Markov, commençant dans l'état S_i , soit dans l'état S_j après n étapes. Selon l'équation de Chapman-Kolmogorov, la probabilité $P_j^{(n)}$, $1 \leq j \leq r$, est le $j^{ième}$ élément dans le vecteur de probabilité $P^{(n)}$ de dimension $1 \times r$ donné par :

$$P^{(n)} = P^{(n-1)}M \tag{II.22}$$

Si $P^{(0)} = \left(P_1^{(0)}, P_2^{(0)}, \dots, P_r^{(0)}\right)$ représente la distribution initiale, alors l'équation de récurrence (II.22) s'écrit :

$$P^{(n)} = P^{(0)}M^n \tag{II.23}$$

Il a été avancé que l'équation (II.23) peut être utilisée pour résoudre de nombreux modèles markoviens, soit ergodiques ou absorbants [Goble and Cheddie 2005]. Dans une chaîne de Markov ergodique, chaque état peut être atteint directement ou indirectement à partir de n'importe quel autre état. Dans une chaîne absorbante, lorsque la chaîne atteint un état absorbant, elle reste dans cet état, c'est-à-dire que S_i est un état absorbant si $p_{ii} = 1$ et $p_{ij} = 0$ pour $i \neq j$. Dans notre cas, les sous-systèmes de SIS sont modélisés par des graphes de Markov absorbant, et l'équation de récurrence (II.23) est utilisée pour calculer les probabilités des états de défaillance dangereux à différents instants de l'intervalle de proof test $[0, \tau]$.

Si les probabilités de transition sont estimées ou fournies par des experts, nous obtenons une matrice de transition floue $\widetilde{M} = (\tilde{p}_{ij})$, où les $\tilde{p}_{ij}$ sont des probabilités de transition floues, c'est-à-dire des possibilités de transition, modélisées par des nombres flous. Comme un cas particulier, certaines valeurs de p_{ij} peuvent être données comme un nombre exact. Selon le théorème de décomposition [Zadeh 1965], $\widetilde{M}$ peut s'écrire :

$$\widetilde{M}=\cup_\alpha \alpha M_\alpha = \left(\cup_\alpha \alpha p_{ij}[\alpha]\right) \ , \ 0 \leq \alpha \leq 1 \qquad \text{(II.24)}$$

Si $0 < p_{ij} < 1$ alors on supposera que $0 < \tilde{p}_{ij} < 1$, avec la restriction qu'il y a $p_{ij} \in p_{ij}[\alpha]$ pour $0 \leq \alpha \leq 1$, de sorte que la matrice de transition exacte $M = (p_{ij})$ représente une chaîne de Markov finie (les sommes des lignes égales à l'unité).

L'équation (II.23) peut être fuzzifiée comme suit :

$$\tilde{P}^{(n)} = \tilde{P}^{(0)}\widetilde{M}^n \qquad \text{(II.25)}$$

Compte tenu de l'équation (II.24) et pour $0 \leq \alpha \leq 1$, nous écrivons :

$$P^{(n)}[\alpha] = P^{(0)}[\alpha]\left(p_{ij}^{(n)}[\alpha]\right) \qquad \text{(II.26)}$$

où $\widetilde{M}^n = \left(\tilde{p}_{ij}^{(n)}\right)$ and $\tilde{P}^{(0)} = \left(\tilde{P}_1^{(0)}, \tilde{P}_2^{(0)}, \ldots, \tilde{P}_r^{(0)}\right)$. Comme prouvé par Buckley [Buckley 2005], l'α-coup $p_{ij}^{(n)}[\alpha]$, associée au nombre flou $\tilde{p}_{ij}^{(n)}$, est un intervalle fermé et borné pour

tout α, i, j et n. Plus précisément, $p_{ij}^{(n)}[\alpha]$ est une fonction du vecteur ligne $v = (p_{11}, \dots, p_{rr})$ du domaine $Dom[\alpha]$ qui est défini comme :

$$Dom[\alpha] = \prod_{i=1}^{r} Dom_i[\alpha] \tag{II.27}$$

Où $Dom_i[\alpha]$ est le produit cartésien des α-coupes $p_{ij}[\alpha]$ de $\tilde{p}_{ij} (0 \leq \alpha \leq 1$ et $1 \leq i, j \leq r)$ intersectées avec la condition C liée à la matrice de transition exacte $M = (p_{ij})$, c'est-à-dire :

$$Dom_i[\alpha] = (\prod_{j=1}^{r} p_{ij}[\alpha]) \cap C \tag{II.28}$$

Avec

$$C = \{p = (p_1, \dots, p_r) | p_i \geq 0, \sum_{i=1}^{r} p_i = 1\} \tag{II.29}$$

En limitant $p_{ij} \in p_{ij}[\alpha]$ à être dans $Dom[\alpha]$, la matrice exacte $M = (p_{ij})$ forme un FMC. Alors une α-coupe $p_{ij}^{(n)}[\alpha]$ de $\widetilde{M}^n$ est l'ensemble de tout M^n pour $v \in Dom[\alpha]$. C'est la base du RFMM qui sera utilisé pour résoudre l'équation (II.25).

Pour les grandes matrices et pour des valeurs de n dépassant un certain ordre, le calcul de $\tilde{P}^{(n)} = \left(\tilde{P}_1^{(n)}, \tilde{P}_2^{(n)}, \dots, \tilde{P}_r^{(n)}\right)$ par l'arithmétique de l'α-coupe est fastidieux et les résultats ne sont pas satisfaisants [Buckley 2005]. Ainsi, les intervalles $P_j^{(n)}[\alpha]$, associés au $j^{ième}$ nombre flou $\tilde{P}_j^{(n)}$ de $\tilde{P}^{(n)}$, peuvent être obtenus en résolvant le problème d'optimisation suivant [Li and Xiu 2014], [Kozine and Utkin 2002], [Buckley 2005] :

$$P_{jL}^{(n)}(\alpha) = inf_{A,B} \sum_{i=1}^{r} P_{i,\alpha}^{(0)} p_{ij,\alpha}^{(n)}, \quad \text{for } 0 \leq \alpha \leq 1 \text{ and } j = 1, \dots, r \tag{II.30}$$

et

$$P_{jR}^{(n)}(\alpha) = sup_{A,B} \sum_{i=1}^{r} P_{i,\alpha}^{(0)} p_{ij,\alpha}^{(n)}, \quad \text{for } 0 \leq \alpha \leq 1 \text{ and } j = 1, \dots, r \tag{II.31}$$

pour que

$$A = \left\{ P_{i,\alpha}^{(0)} \middle| P_{iL}^{(0)}(\alpha) \leq P_{i,\alpha}^{(0)} \leq P_{iR}^{(0)}(\alpha) \right\} \tag{II.32}$$

$$B = \left\{ p_{ij,\alpha}^{(1)} \middle| p_{ij,L}^{(1)}(\alpha) \leq p_{ij,\alpha}^{(1)} \leq p_{ij,R}^{(1)}(\alpha) \; and \; \sum_{j=1}^{r} p_{ij,\alpha}^{(1)} = 1 \right\} \tag{II.33}$$

pour tout α, i and j. L et R représentent les limites gauche et droite de l'intervalle $P_j^{(n)}[\alpha]$, et $p_{ij,\alpha}^{(1)}$ est simplement le $ij^{ème}$ élément de la matrice exacte M extraite de la matrice α-coupe $M_\alpha = \left(p_{ij}[\alpha]\right)$, c'est-à-dire, $p_{ij,\alpha}^{(1)} = p_{ij,\alpha}$.

II.3.2.2 PFD floue

La disponibilité d'un système redondant (un sous-système d'un SIS) est liée à sa fonction essentielle. Soit $S = \{S_1, S_2, \dots, S_r\}$ l'ensemble de tous les états possibles de ce système. Pour certains de ces états, le système fonctionne, alors que pour d'autres états, il ne fonctionne pas. Soit U le sous-ensemble de S pour lequel le système redondant fonctionne. Le sous-ensemble pour lequel ce système ne fonctionne pas est alors D = S-U. Supposons que S est ordonné de sorte que les m premiers états représentent les états de fonctionnement. Par conséquent, $U = \{S_1, S_2, \dots, S_m\}$ et $D = \{S_{m+1}, S_{m+2}, \dots, S_r\}$.

Le système redondant n'est pas disponible tant qu'il se trouve dans l'un des états défaillants (c'est-à-dire en D). Son PFD, c'est-à-dire, indisponibilité, à un moment n est alors :

$$PFD^{(n)} = \sum_{j=m+1}^{r} P_j^{(n)} \tag{II.34}$$

Avec des probabilités floues, l'équation (II.34) devient :

$$P\tilde{F}D^{(n)} = \sum_{j=m+1}^{r} \tilde{P}_j^{(n)} \tag{II.35}$$

Où le signe "∑" dans l'équation (II.35) représente l'addition floue qui peut être effectuée en utilisant la méthode α-coupe (théorème de décomposition), nous obtenons :

$$P\tilde{F}D^{(n)}[\alpha] = \sum_{j=m+1}^{r} P_j^{(n)}[\alpha], \text{ pour tout } \alpha \text{ dans } [0, 1]. \tag{II.36}$$

Comme il a été mentionné à l'introduction de ce chapitre, la PFD_{avg}, d'un SIS faiblement sollicité, est l'indicateur le plus utilisé pour caractériser sa performance probabiliste. Donc, si

l'intervalle de test $[0, \tau]$ est subdivisé en N segments égaux $[t_i, t_{i+1}]$ $(i = 0, 1, .., N)$, de sorte que N.Δt = τ avec $\Delta t = t_{i+1} - t_i$, alors la PFD_{avg} flou ($P\tilde{F}D_{avg}$) sur [0, τ] s'écrit comme suit :

$$P\tilde{F}D_{avg} = \frac{1}{N.\Delta t}\sum_{n=1}^{N} P\tilde{F}D^{(n)}.\Delta t \quad \text{(II.37)}$$

Ou simplement :

$$P\tilde{F}D_{avg} = \frac{1}{N}\sum_{n=1}^{N} P\tilde{F}D^{(n)} \quad \text{(II.38)}$$

Ainsi, pour chaque α-coupe de la $P\tilde{F}D_{avg}$, les limites inférieure et supérieure s'écrivent :

$$PFD_{avg,L}(\alpha) = \frac{1}{N}\sum_{n=1}^{N} PFD_{L}^{(n)}(\alpha) \quad \text{(II.39)}$$

$$PFD_{avg,R}(\alpha) = \frac{1}{N}\sum_{n=1}^{N} PFD_{R}^{(n)}(\alpha) \quad \text{(II.40)}$$

II.4 Conclusion

La théorie des ensembles flous est un outil puissant qui permet de traiter l'incertitude qui affecte les différents paramètres. Dans ce chapitre, les paramètres imprécis qui caractérisent les SIS tels que le facteur β et le taux DC sont représentés par des nombres flous triangulaires.

La méthode d'évaluation de la performance des SIS, développée dans ce chapitre, se base particulièrement sur le modèle de Markov flou pour traiter les chaines de Markov floues lorsqu'il s'agit de données de transition imprécises. Cette méthode d'évaluation utilise l'approche développée par Buckley et Eslami appelée multiplication restreinte des matrices floues (RFMM).

Chapitre III

Diagnostic de la performance des SIS dans un environnement flou : Effet des stratégies de test

III.1 Introduction

Dans ce chapitre, nous avons tenté de montrer l'effet des stratégies de test sur la performance des SIS faiblement sollicités et périodiquement testés dans un environnement incertain. Pour cela, deux types de stratégies de test sont considérés : les tests simultanés et les tests échelonnés. 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. Ils permettent d'améliorer le niveau SIL sans faire de modification sur le système.

En tant que paramètres pertinents du SIS et vu qu'ils sont entachés d'incertitude, le facteur β, qui caractérise les défaillances de cause communes (CCF), et le taux de couverture de diagnostic DC sont modélisés par des nombres flous triangulaires et sont alors injectés dans le modèle de Markov flou pour l'évaluation de la $P\tilde{F}Davg$ de la SIF du SIS. L'incertitude ou le manque de connaissance à propos des données relatives à ces paramètres est exprimé par des nombres flous.

Les chaînes de Markov floues sont traitées par la méthode proposée par Buckley [Buckley and Eslami 2002]. Les probabilités élémentaires des chaînes de Markov sont remplacées par des nombres flous triangulaires et découpées en α-coupes. Bien qu'un nombre flou puisse avoir des formes très variées (trapézoïdales, rectangulaires, triangulaires, ...), dans ce travail, on ne manipule que les nombres flous triangulaires. L'intérêt de cette représentation

triangulaire 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 loi normale [Dubois et al. 2004], [Innal et al. 2016]. Un autre avantage des nombres flous triangulaires est la facilité d'utilisation grâce à la simplification des opérations arithmétiques flous [Kaufman and Gupta 1991].

Pour illustrer l'approche proposée, un système de protection contre la pression à haute intégrité (HIPPS pour High Integrity Pressure Protection System) est utilisé ici comme un cas d'application pour calculer sa PFD_{avg} floue à partir de ses paramètres caractéristiques imprécis en l'occurrence le facteur β et le taux DC. L'objectif principal de ce travail est d'analyser l'effet des stratégies de test et de montrer comment ces stratégies peuvent affecter la performance du SIS dans un environnement incertain [Sal et al. 2017].

III.2 Code informatique

Comme mentionné au chapitre II, pour certains α fixés dans [0,1], nous calculons la matrice d'intervalle $M_\alpha = \left(p_{ij}[\alpha]\right)$. Ensuite, par une sélection aléatoire (RS), les valeurs $p_{ij,\alpha}$ sont extraites de M_α et normalisées par ligne afin de satisfaire la contrainte (II.33). Le résultat est une matrice exacte $M = (p_{ij,\alpha})$ à partir de laquelle on calcule, pour différentes valeurs de n (pas), à la fois les matrices de puissance M^n et les probabilités d'état correspondant $P_{j,\alpha}^{(n)}$, $1 \leq j \leq r$. Dans notre cas, une heure est choisie comme un incrément car elle peut être considérée comme négligeable par rapport à l'intervalle de test [0, τ] [Goble and Cheddie 2005]. La RS est raisonnablement répétées de telle sorte que l'ensemble des solutions possibles soit déterminé, à savoir $P_{RS}^{(n)} = \left\{P_{j,k}^{(n)}(\alpha) |\, k = 1, 2, \ldots, 100, ..\right\}$. C'est une recherche purement aléatoire mais peut être très acceptable pour un grand nombre de sélections [Buckley et al. 2004]. Les points extrêmes de l'intervalle $P_j^{(n)}[\alpha]$ sont dérivés des équations (II.30) et (II.31), la PFD_{avg} floue est fournie par les équations (II.39) et (II.40).

Dans le but de réaliser et faciliter tout nos calculs, nous avons développé pour cela un programme informatique sous l'environnement Matlab. L'algorithme global de calcul est le suivant [Sal et al. 2017] :

1. Lire le vecteur de probabilité initial $P^{(0)} = \left(P_1^{(0)}, P_2^{(0)}, \dots, P_r^{(0)}\right)$ comme une estimation exacte,
2. Répéter la boucle α, $\alpha = 0, 0.1, \dots, 0.9, 1$,
3. Calculer $M_\alpha = \left(p_{ij}[\alpha]\right)$,
4. Répétez la boucle de temps, $n = 0, 1, 2, \dots, \tau - 1, \tau$,
5. Répétez la boucle RS, $k = 1, 2, \dots, 100, ..$,
6. Sélectionner aléatoirement $p_{ij,\alpha} \in p_{ij}[\alpha]$ de sorte que $\sum_{j=1}^{r} p_{ij,\alpha} = 1$ pour tout i et construire M,
7. Calculer M^n,
8. Calculer $P^{(n)} = P^{(0)} M^n$,
9. Enregistrer $P^{(n)}$,
10. Fin de la boucle RS,
11. Calculer $P_{jL}^{(n)}(\alpha)$ et $P_{jR}^{(n)}(\alpha)$,
12. Calculer $PFD_L^{(n)}(\alpha)$ et $PFD_R^{(n)}(\alpha)$,
13. Fin de la boucle de temps,
14. Calculer $PFD_{avg,L}(\alpha)$ et $PFD_{avg,R}(\alpha)$
15. Fin de la boucle α.

III.3 Description du système HIPPS

Le système présenté dans la figure III.1 a été étudié dans la référence [Signoret 2005]. C'est un système de protection contre la pression à haute intégrité (High Integrity Pressure Protection System : HIPPS) qui est un SIS typique. Ce système est utilisé ici comme exemple d'application pour illustrer l'approche proposée. Cet HIPPS est destiné à protéger le circuit aval d'un système de production offshore contre une surpression due à son circuit amont (puits pétrolier W1).

Ce SIS est composé de trois sous-systèmes en série. Le premier est constitué de trois capteurs de pression (PT_i), structurés en architecture 2oo3. Le second sous-système est constitué d'un solveur logique (LS) ayant une architecture 1oo1. Le troisième sous-système est l'actionneur (élément final) avec une architecture 1oo2. Chaque canal est composé d'une électrovanne SV_i et d'une vanne d'arrêt SDV_i.

Le fonctionnement de ce système est le suivant : quand la valeur de la pression dans la canalisation dépasse un certain seuil spécifié, elle est détectée par les trois capteurs PT_i. Ces trois capteurs envoient l'information à l'unité logique (solveur logique) LS qui contrôle et traite son caractère majoritaire 2003. Si au moins deux des trois signaux reçus des capteurs confirment la présence d'une surpression dans la canalisation, le solveur logique commande l'ouverture des électrovannes SV_1 et SV_2, ce qui à pour conséquence de couper l'alimentation hydraulique qui maintenait ouvertes les vannes d'arrêt SDV_1 et SDV_2. Ces dernières se ferment alors et suppriment ainsi le risque de surpression dans le circuit avale.

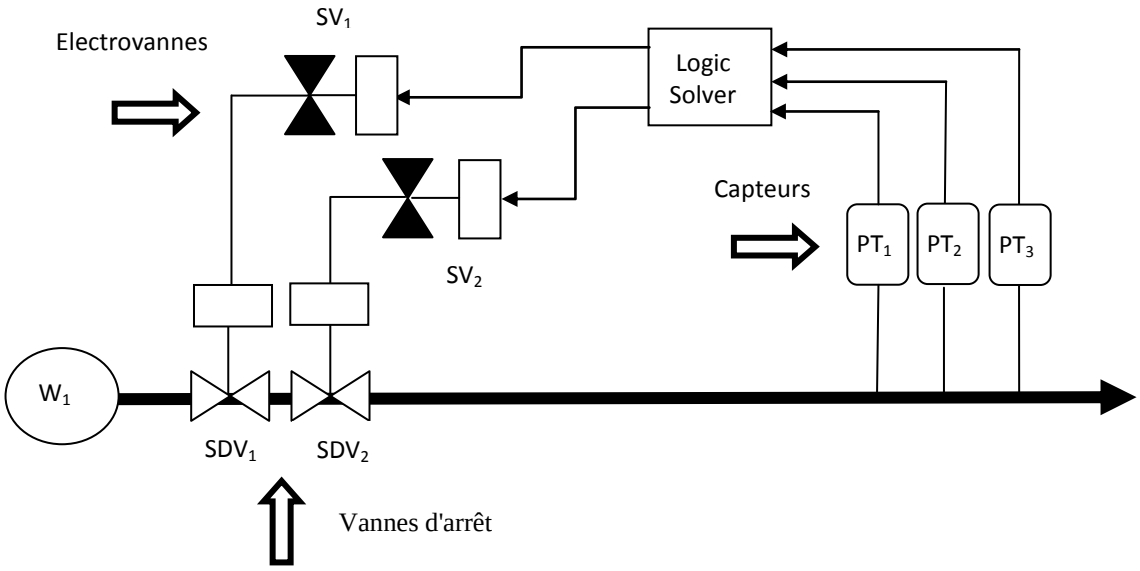


Fig. III.1 Schéma du système HIPPS étudié.

Le diagramme bloc de fiabilité de l'HIPPS est donné par la figure III.2.

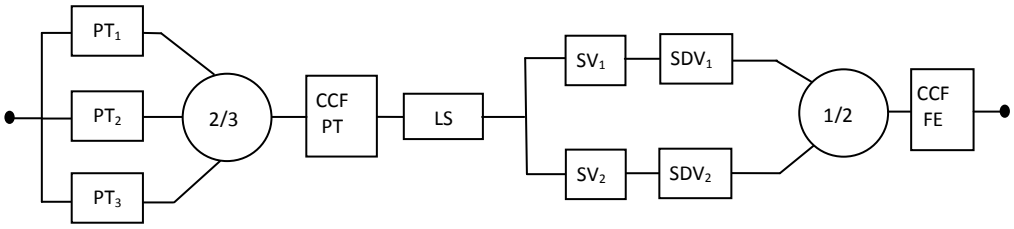


Fig. III.2 Diagramme bloc de fiabilité de l'HIPPS.

Dans ce travail, nous calculons la PFD floue de l'HIPPS en considérant l'incertitude sur le taux DC et le facteur β en utilisant les chaînes de Markov floues. L'incertitude sur ces paramètres est modélisée par des nombres flous triangulaires. La $P\tilde{F}D_{avg}$ de l'HIPPS est calculée en utilisant la méthode α-coupe :

$$FDavgHIPPS(\alpha) = PFDavgCap(\alpha) + PFDavgLS(\alpha) + PFDavgAct(\alpha) \\ = PFDavg2oo3(\alpha) + PFDavg1oo1(\alpha) + PFDavg1oo2(\alpha) \qquad \text{(III.1)}$$

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

Pour calculer la PFD(t) floue instantanée ($P\tilde{F}D(t)$) et la $P\tilde{F}Davg$ de la SIF du SIS, nous avons considéré deux stratégies de test [Sal et al. 2017] :

- La première est la stratégie de test simultanée. Tous les sous-systèmes du SIS sont testés simultanément pour vérifier la fonction de sécurité du SIS. Pour cette stratégie, nous choisissons un intervalle de test égal à un an ($T_i = 8760$ heures).

- La deuxième stratégie est la stratégie de test échelonné. En référence à la norme IEC 61508 et sur la base des pratiques industrielles actuelles [Honey Well 2012], [Rausand 2014], l'intervalle de test pour cette stratégie est subdivisé en trois intervalles. Le premier intervalle de test est égal à 3 mois ($T_1 = 2190$ heures) et ne concerne que le sous-système capteur. Le second intervalle , consacré au sous-système actionneur, est de six mois (T_2 =4380 heures). Il faut noter que dans cet intervalle le sous-système capteur est testé implicitement car ce dernier doit être testé chaque 3 mois. Le dernier intervalle de test est égale à un année (T_3 = 8760 heures), il concerne le sous-système solveur logique. Comme pour le second intervalle, en plus du test du sous-système solveur logique, on test aussi les deux autres sous-systèmes chacun durant son propre intervalle de test.

Dans le cadre de ce travail, nous supposons que les deux stratégies de test considérées sont parfaites, et par conséquent après chaque test toutes les défaillances-DU sont révélées et réparées. Ainsi, le SIS est supposé être dans un état "aussi bon que neuf ou aussi proche que possible de cette condition".

Le but principal de ce chapitre est d'analyser l'impact de ces deux stratégies de test sur la PFD floue en présence d'incertitude sur le taux DC et le facteur β.

III.4 Modèles de Markov Flous des sous-systèmes de l'HIPPS

III.4.1 Sous-système solveur logique (unité logique)

Le sous-système solveur logique représenté par l'architecture 1oo1 est modélisé par la chaîne de Markov multiphase floue représentée par la figure III.3 [Mechri et al. 2013]. Dans ce graphique, nous avons trois états. L'état 1 représente l'état de fonctionnement et les deux autres états sont des états de défaillance.

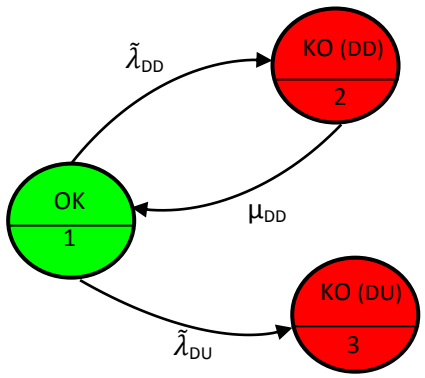


Fig. III.3 Modèle de Markov multiphase flou du solveur logique en 1oo1.

III.4.2 Sous-système capteur

La figure III.4 décrit la chaîne de Markov multiphase floue du sous-système capteur ou du sous-système transmetteur de pression [Mechri et al. 2013]. Ce modèle comporte trois types d'états: (i) état de fonctionnement (état 1), (ii) états de fonctionnement en mode dégradé (états 2 et 3), (iii) états de défaillance (de l'état 4 à 10).

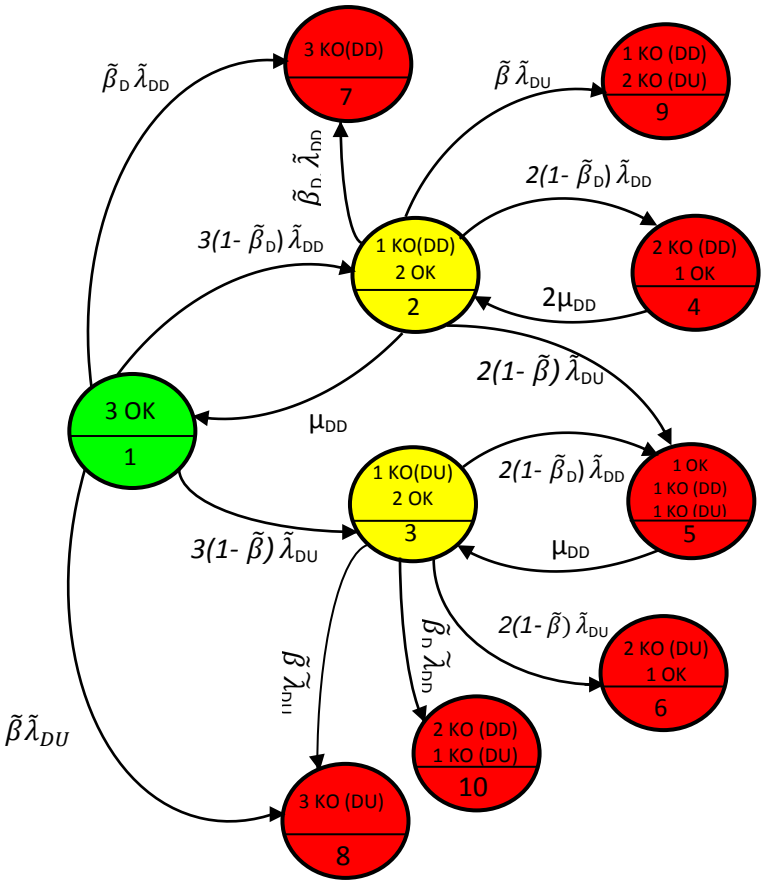


Fig. III.4 Modèle de Markov multiphase flou du capteur en 2oo3.

III.4.3 Sous-système actionneur

Le sous-système actionneur est configuré dans une architecture 1oo2. Son comportement est décrit par le modèle de Markov multiphase flou représenté par la figure III.5 [Mechri et al. 2013]. L'état 1 est un état de fonctionnement. Les états 2 et 3 sont des états de fonctionnement en mode dégradé. Le reste des états (états 4, 5 et 6) sont des états de défaillances.

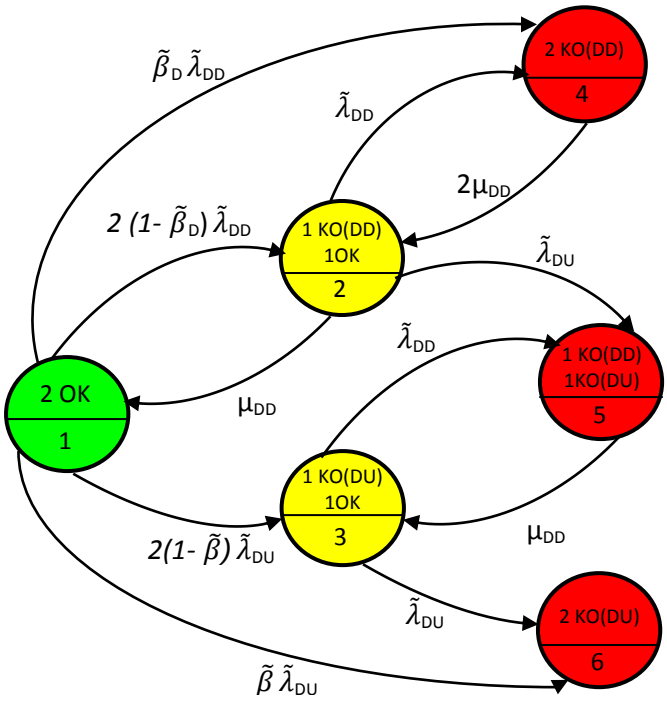


Fig. III.5 Modèle de Markov multiphase flou de l'actionneur en 1oo2.

III.5 Données des paramètres des composants de l'HIPPS

Les données relatives aux paramètres des composants de l'HIPPS sont prises à partir de la référence [Hauge et al. 2010]. Les valeurs des paramètres sont données dans la table III.1. Pour examiner l'effet des stratégies de test sur la performance de l'HIPPS en présence d'incertitude sur le facteur β et le taux DC, ces deux paramètres sont décrits, pour chaque sous-système, par des nombres flous triangulaire. Il convient de noter que l'incertitude sur le facteur β et le taux DC n'est pas restrictive, mais apparaît évidemment sur λ_{DD} et λ_{DU} bien que le taux de défaillance dangereux λ_D et le taux de restauration μ_{DD} des composants de l'HIPPS restent exactes (valeurs uniques) [Sal et al. 2017].

Table III.1 Données numériques des composants de l'HIPPS.

Composants du SIS	$\lambda_D(h^{-1})$	$\widetilde{DC}$ (%)	$\tilde{\beta}$ (%)	MTTR (h)	Ti (h) Pour la première stratégie	Ti (h) Pour la Seconde stratégie
PT_i	2.4E-6	(60 , 50 , 70)	(4 , 3 , 5)	2	T_1=8760	T_1=2190
SDV_i	4.4E-6	(20 , 10 , 30)	(3 , 2, 4)	4	T_2=8760	T_2=4380
SV_i	4.4E-6	(20 , 10 , 30)	(3 , 2 , 4)	4	T_2=8760	T_2=4380
LS	1.00E-6	(90 , 80 , 100)	/	6	T_3=8760	T_3=8760

III.6 Résultats et discussion

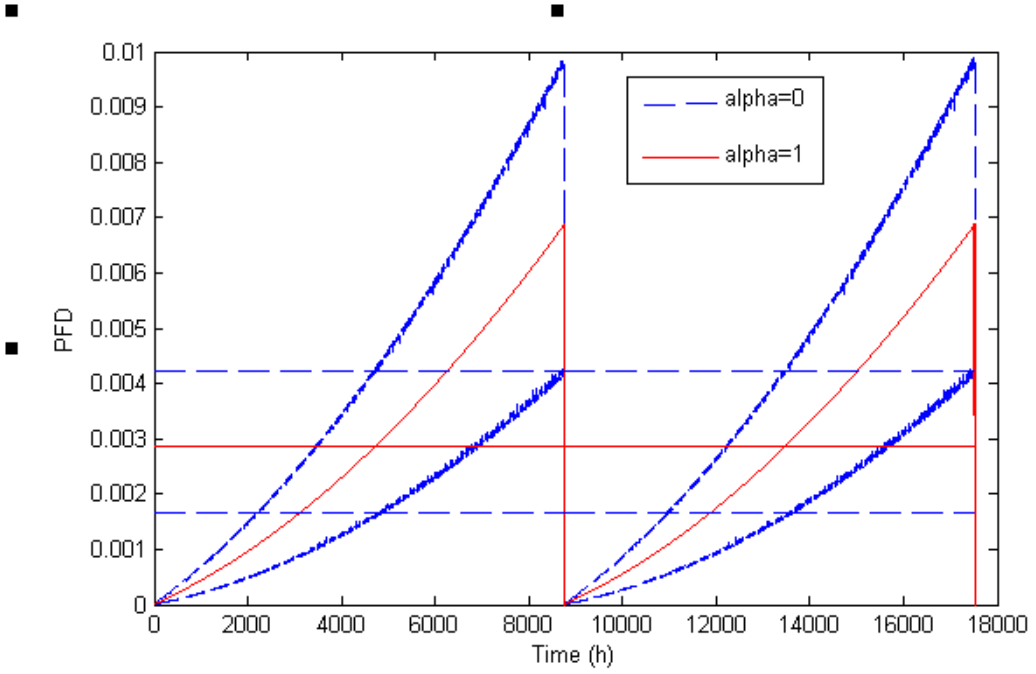
III.6.1 Comparaison des PFD floues selon la première stratégie

Les PFD floues sont calculées en considérant l'incertitude sur les valeurs des deux paramètres β et DC. Les résultats sont fournis par la résolution de chaînes de Markov floues via un programme informatique développé pour élaborer tout les calculs comme il a été décrit dans le paragraphe III.2. Trois cas sont considérés séparément : dans le premier cas nous supposons que l'incertitude affecte uniquement le taux DC, pour le deuxième cas l'incertitude affecte le facteur β seul et pour le troisième cas l'incertitude affecte les deux paramètres à la fois (cas réel) [Sal et al. 2017].

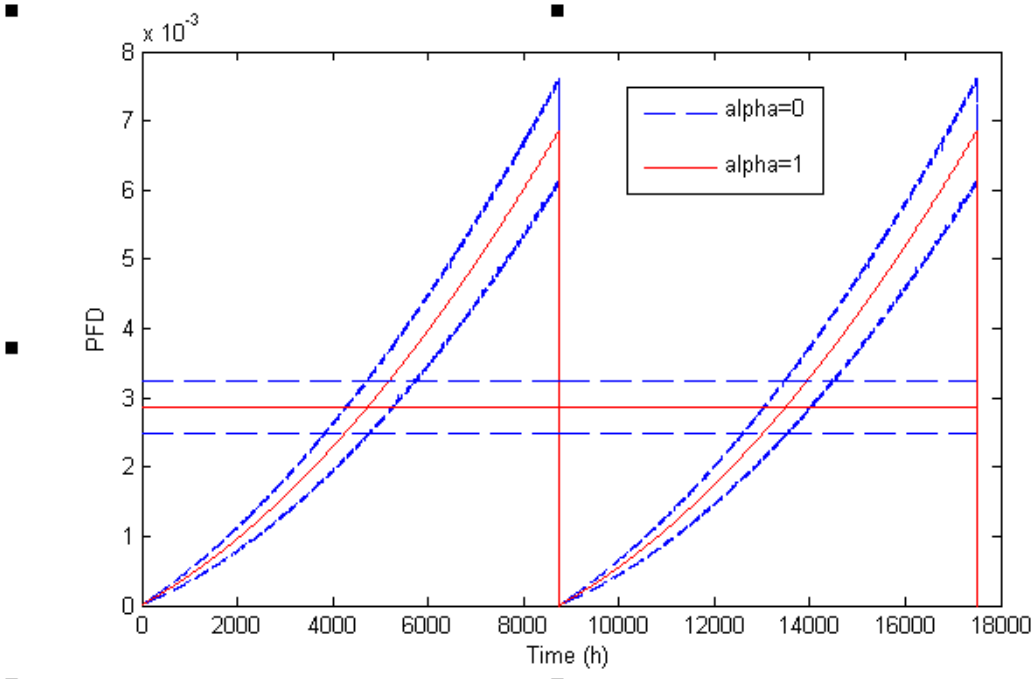
Les figures III.6 (a)-(c) montrent la représentation graphique de la PFD(t) floue instantanée alors que la figure III.7 montre celles de la $P\tilde{F}D_{avg}$. Les graphes de la figure III.7 sont exclusivement représentés par des nombres flous. En référence à la valeur modale ($PFD_{avg} = 2.8664$ E-3) qui est commune aux trois nombres flous, nous pouvons remarquer qu'ils ont des supports différents. En effet, l'incertitude sur DC semble avoir plus d'effet sur la $P\tilde{F}D_{avg}$ par rapport à l'incertitude sur β : le support de la $P\tilde{F}D_{avg}$ lié au DC flou est plus large que celui du β flou, c'est à dire :

$$PFD_{\beta}^{(\alpha=0)} = [2.49157 \text{ E-3} \;,\; 3.24076 \text{ E-3}] \subset PFD_{DC}^{(\alpha=0)} = [1.97657 \text{ E-3} \;,\; 3.7944 \text{ E-3}]$$

(a)


alpha=0
alpha=1
PFD
Time (h)
0.01
0.009
0.008
0.007
0.006
0.005
0.004
0.003
0.002
0.001
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000

(b)


x 10^-3
alpha=0
alpha=1
PFD
Time (h)
8
7
6
5
4
3
2
1
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000

(c)

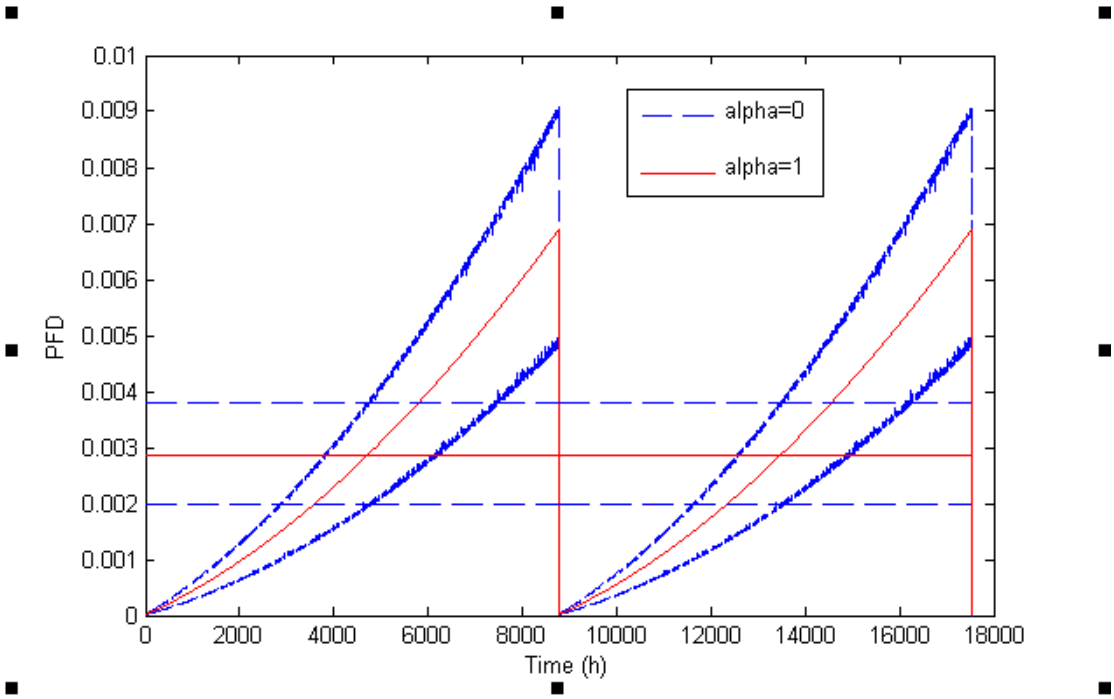


Fig. III.6 $P\tilde{F}D(t)$ de la SIF liée à la première stratégie.

(a) $\tilde{\beta}$ et $\widetilde{DC}$, (b) $\tilde{\beta}$ et DC exact, (c) β exact et $\widetilde{DC}$.

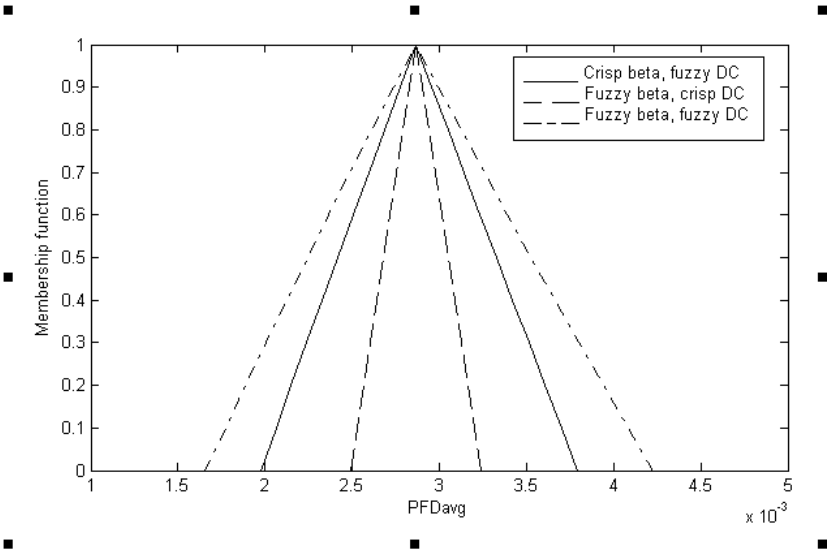


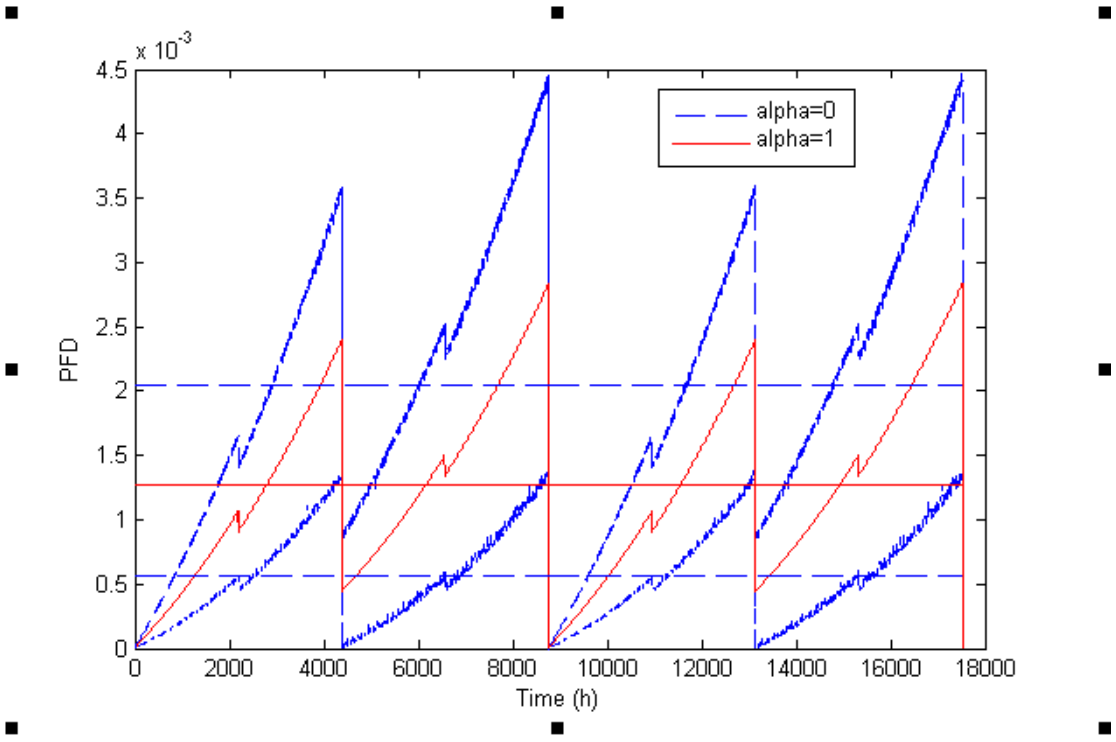
Fig. III.7 $P\tilde{F}D_{avg}$ de la SIF liée à la première stratégie.

L'incertitude sur les deux paramètres ($\tilde{\beta}$ and $\widetilde{DC}$) donne le support le plus large, il est compris entre 1,6563 E-3 à 4,2233 E-3 pour α = 0 avec une valeur modale égale à 2,8866 E-3. Le système a un SIL 2.

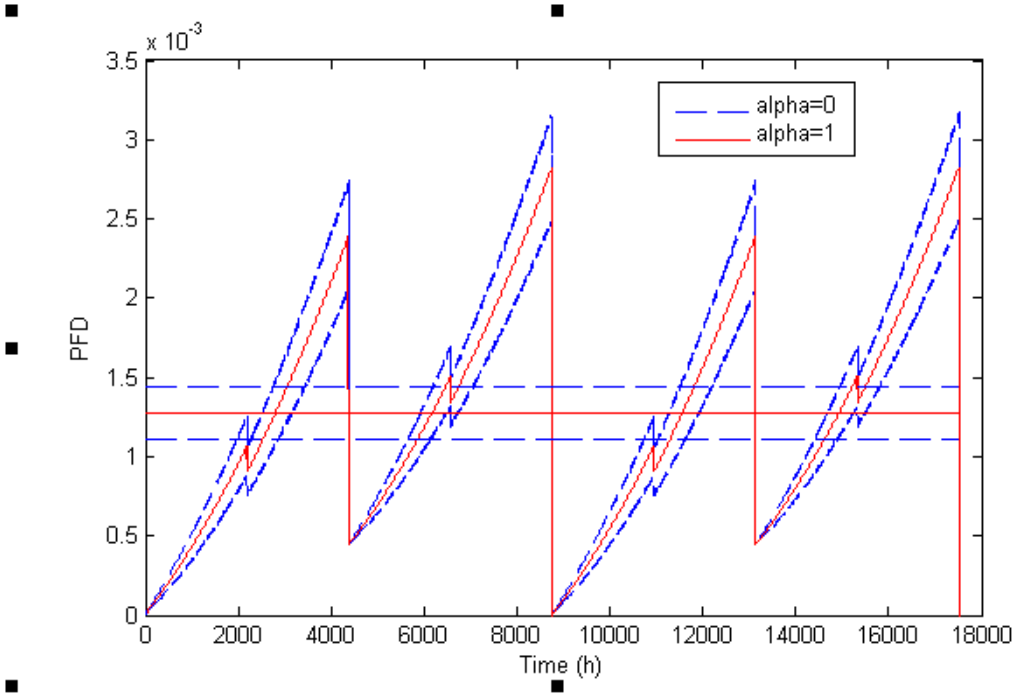
III.6.2 Comparaison des PFD floues selon la seconde stratégie

Les graphes des $P\tilde{F}D(t)$ de la SIF liée à cette stratégie sont représentés par les figures III.8 (a)-(c) et ceux des $P\tilde{F}D_{avg}$ sont donnés par la figure III.9 sous forme d'un nombre flou.

(a)



(b)



(c)

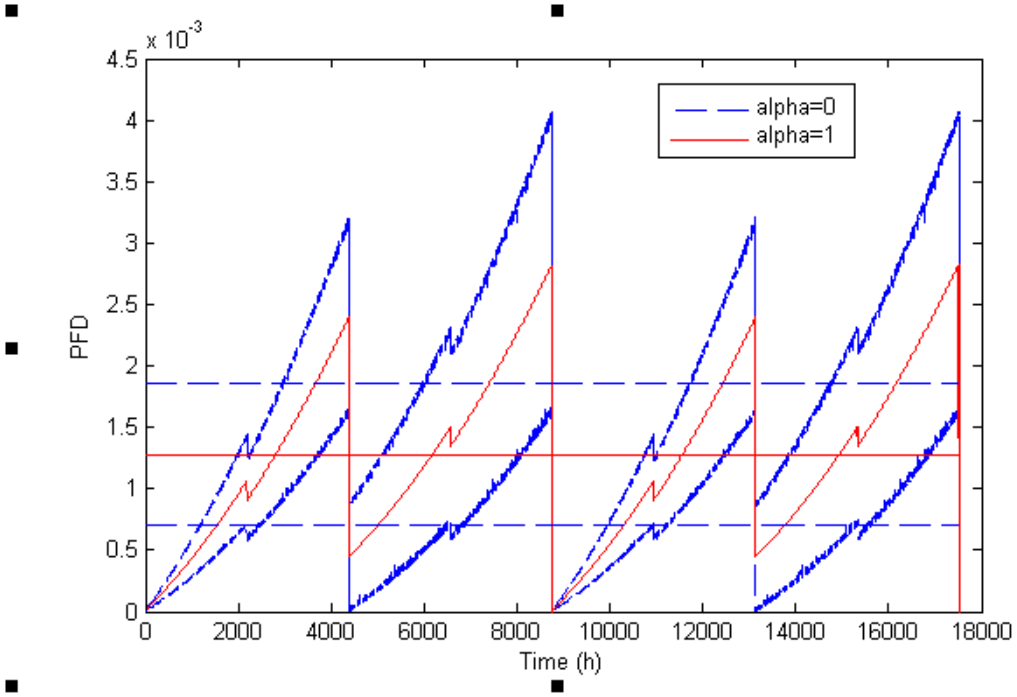


Fig. III.8 $P\tilde{F}D(t)$ de la SIF liée à la seconde stratégie.

(a) $\tilde{\beta}$ et $\widetilde{DC}$, (b) $\tilde{\beta}$ et DC exact , (c) β exact et $\widetilde{DC}$.

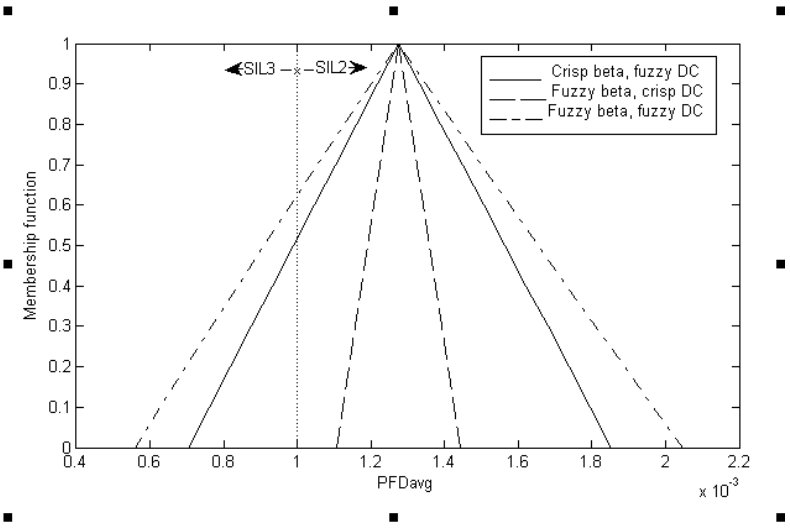


Fig. III.9 $P\tilde{F}D_{avg}$de la SIF liée à la seconde stratégie.

Pour la seconde stratégie, les remarques précédentes restent les même sauf que la $P\tilde{F}D_{avg}$ liée à l'incertitude sur DC dépasse le SIL 2 et atteint le SIL 3. Les mêmes résultats sont évidemment obtenus lorsque l'incertitude affecte les deux paramètres β et DC. Numériquement, nous avons :

$$PFD_{avg,DC}^{(\alpha=0)} = [1\mathrm{E}-4 \ , \ 1\mathrm{E}-3] \overset{\subset}{_{\Phi}} [7.0490\mathrm{E}-4 \ , \ 1.8538\mathrm{E}-3]$$

Où $\overset{\subset}{_{\Phi}}$ signifie l'inclusion par intervalles. Ce résultat peut s'expliquer par l'effet de la stratégie de maintenance, comme on peut le voir également dans le paragraphe qui suit.

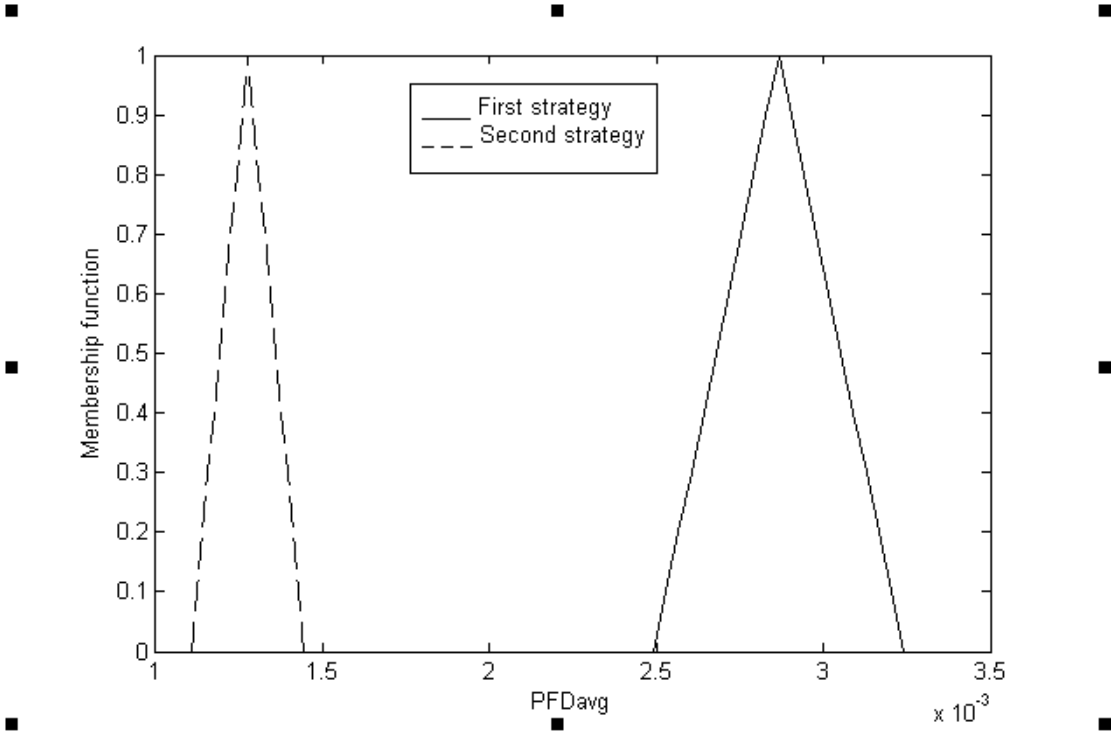
III.6.3 Effet des stratégies sur la $P\tilde{F}D_{avg}$

La figure III.10-(a) montre la variation de la $P\tilde{F}D_{avg}$ dans le cas de ($\tilde{\beta}$ et DC exact) en considérant les deux stratégies. Nous pouvons voir que la $P\tilde{F}D_{avg,\tilde{\beta}}$ issue de la seconde stratégie est inférieure à la $P\tilde{F}D_{avg,\tilde{\beta}}$ liée à la première. Cependant, les deux nombres flous appartiennent toujours au SIL 2, ce qui peut s'expliquer par l'effet faible de l'incertitude sur β.

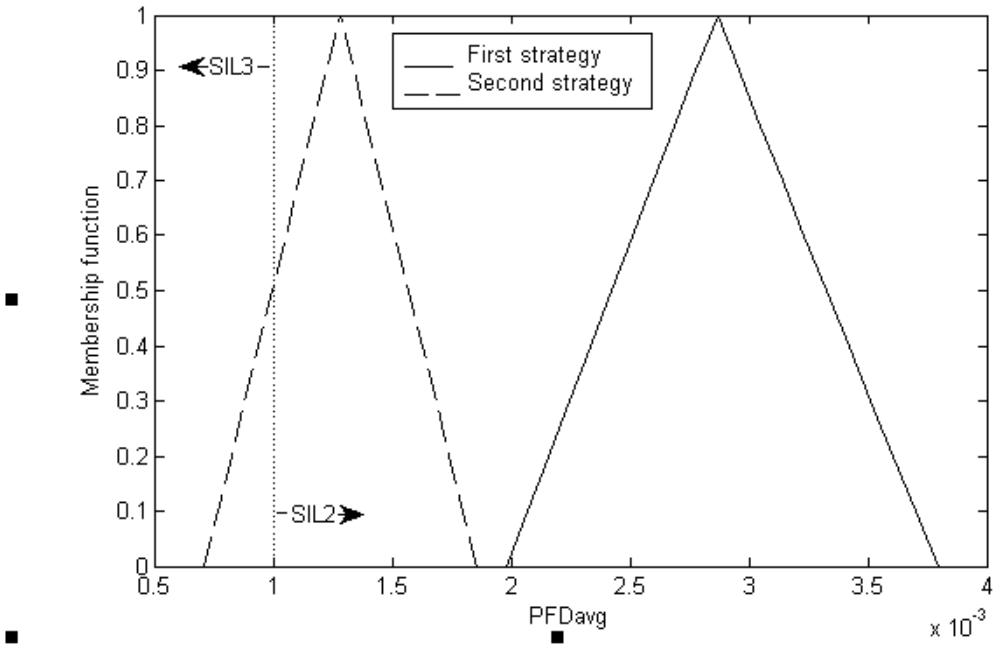
Les cas de (β exact et $\widetilde{DC}$) et ($\tilde{\beta}$ et $\widetilde{DC}$) sont représentés par les figures III.10 (b)-(c) respectivement. La $P\tilde{F}D_{avg}$ diminue quand on considère la seconde stratégie. Évidemment, la diminution est relativement importante lorsque l'incertitude affecte les deux paramètres. La

$P\tilde{F}D_{avg}$ dépasse le SIL 2 et atteint l'intervalle SIL 3 lorsque l'on considère la seconde stratégie.

(a)



(b)



(c)

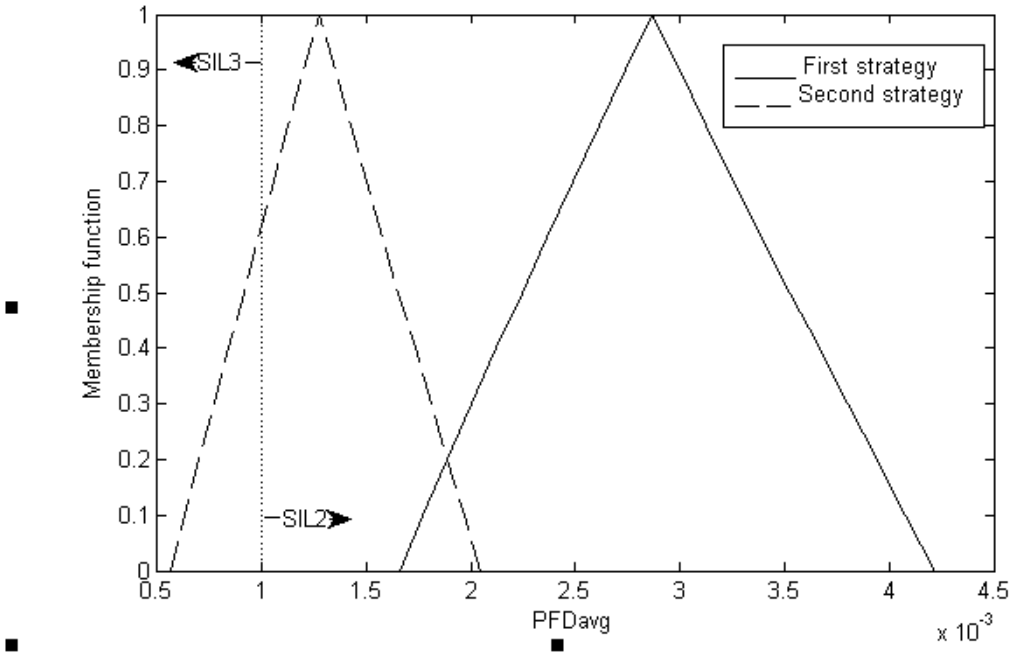


Fig. III.10 Effet des stratégies sur la $P\tilde{F}D_{avg}$ de la SIF.

(a) $\tilde{\beta}$ et DC exact , (b) β exact et $\widetilde{DC}$, (c) $\tilde{\beta}$ et $\widetilde{DC}$.

III.7 Conclusion

Ce chapitre a traité principalement de l'impact des stratégies de test sur la performance du SIS dans un environnement flou. L'incertitude des paramètres caractéristiques du SIS est modélisée par des nombres flous triangulaires. Les PFD floues du SIS sont calculées en considérant l'incertitude sur les valeurs du facteur β et du taux DC. Deux types de stratégies sont considérés : les tests simultanés et les tests échelonnés. Un cas d'application axé sur un système de protection contre la pression à haute intégrité (HIPPS) est réalisé. Les calculs sont effectués en résolvant les chaînes de Markov floues via un code informatique développé sous l'environnement Matlab.

Premièrement, nous avons montré lequel des deux paramètres étudiés, c'est-à-dire le facteur $\tilde{\beta}$ et le taux $\widetilde{DC}$, a plus d'effet sur la $P\tilde{F}D_{avg}$ du SIS. Il a été montré que, pour la même stratégie de test, l'incertitude sur DC semble avoir plus d'effet sur la $P\tilde{F}D_{avg}$ par rapport à l'incertitude sur β. En effet, le support de la $P\tilde{F}D_{avg}$ lié au taux $\widetilde{DC}$ est plus large que celui du facteur $\tilde{\beta}$.

Dans un deuxième temps, nous avons effectué une comparaison entre les deux stratégies de test. Il semble que la $P\tilde{F}D_{avg}$ sous le test échelonné est inférieure à celle avec le test simultané. Pour la première stratégie (test simultané), la $P\tilde{F}D_{avg}$ est toujours comprise dans l'intervalle SIL 2 pour les trois cas considérés, mais pour la seconde stratégie, elle dépasse l'intervalle SIL 2 et atteint l'intervalle SIL 3 pour les cas (b) et (c). Ce résultat montre clairement l'effet de la deuxième stratégie sur la $P\tilde{F}D_{avg}$ de l'HIPPS.

Chapitre IV

Analyse de l'effet des variations des données imparfaites sur la performance des SIS

IV.1 Introduction

L'analyse de sensibilité est un outil utilisé dans un large éventail de domaines. Elle est appliquée dans la biologie, l'économie, la géographie, ... et en particulier l'engineering.

L'analyse de sensibilité aide l'analyste d'avoir une bonne idée sur la solution choisie par lui lorsqu'il essaye de voir l'impact de toute modification des valeurs d'entrée d'un ou de plusieurs paramètres.

Dans ce chapitre, nous examinons en premier lieu le principe général de l'analyse de sensibilité qui consiste à étudier les effets des variations des paramètres d'entrée sur la sortie du modèle. Dans un second lieu, nous exposons notre idée qui se base principalement sur la variation de deux paramètres pertinents, qui sont le facteur $\tilde{\beta}$ et le taux $\widetilde{DC}$, et voir leur impact sur la $P\tilde{F}D_{avg}$ qui constitue notre variable de sortie pour les deux stratégies [Sal et al. 2017]. En dernier lieu, des mesures de possibilité et de nécessité sont réalisés afin de montrer lequel des deux paramètres qui a le plus d'impact sur la $P\tilde{F}D_{avg}$. La distance de Hamming montre clairement la stratégie qui influence la $P\tilde{F}D_{avg}$.

IV.2 Principe de l'analyse de sensibilité

L'analyse de sensibilité dans le contexte de l'analyse des risques peut être définie comme : une analyse qui examine comment les résultats d'un calcul ou d'un modèle varient lorsque les variables d'entrée sont modifiées [Rausand 2011].

Une analyse de sensibilité est un examen quantitatif de la façon dont les résultats de l'analyse varient avec le changement :

- des paramètres d'entrée (par exemple, taux de défaillance, probabilités, temps de réparation),
- des hypothèses de l'analyse (par exemple, liées à l'exploitation, la maintenance, l'indépendance),
- de La structure du modèle (par exemple, la structure d'un arbre de défaillance).

L'analyse de sensibilité est effectuée en changeant une entrée incertaine à la fois et en montrant comment les résultats d'un modèle changent sur la gamme de valeurs possibles de cette entrée. Le schéma de la figure IV.1 illustre le principe de l'analyse de sensibilité.

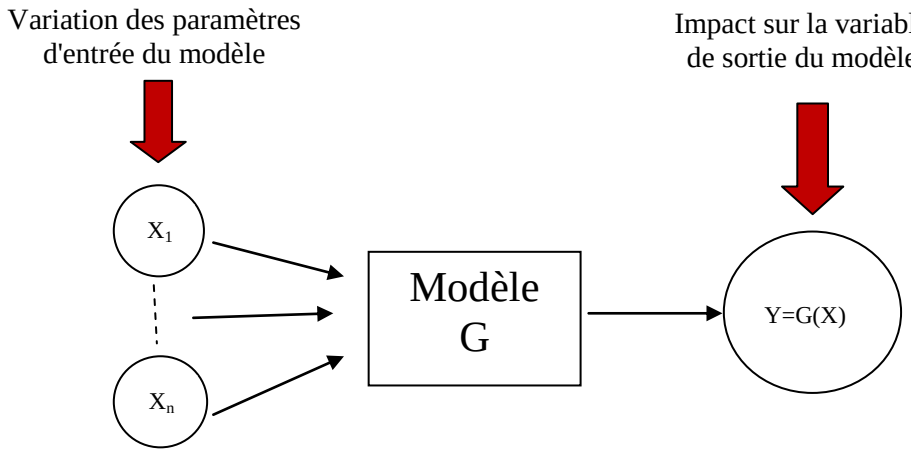


Fig. IV.1 Principe de l'analyse de sensibilité.

L'analyse de sensibilité est le plus souvent utilisée pour étudier les effets des variations des paramètres d'entrée. Supposons que nous utilisons le modèle mathématique $g(x) = g(x_1, x_2, ..., x_n)$ où $x_1, x_2, ..., x_n$ sont les n variables ou paramètres d'entrée indépendants. La sensibilité de ce modèle par rapport à la variable X_i est définie par [Rausand 2011] :

$$I(i) = \frac{\partial g(x_i)}{\partial (x_i)} \quad \text{(IV.1)}$$

L'analyse de sensibilité vise à identifier les variables les plus importantes dans un modèle, c'est-à-dire les variables qui ont le plus d'impact sur la sortie du modèle. L'analyse de sensibilité permettra également d'identifier les composants pour lesquels les données sont ou ne sont pas sensibles à l'analyse.

Lorsqu'il est possible d'établir une expression mathématique d'une valeur de sortie en fonction des valeurs d'entrée, on peut déterminer la sensibilité des paramètres d'entrée en prenant les dérivées partielles de cette fonction. C'est une pratique courante dans l'analyse des arbres de défaillances où nous déterminons la sensibilité selon la mesure d'importance de Birnbaum [Rausand 2011] :

$$I^B(i/t) = \frac{\partial Q_0(t)}{\partial q_i(t)} \quad \text{(IV.2)}$$

Une mesure d'importance est utilisée pour calculer la contribution relative de l'incertitude dans chaque paramètre d'entrée à l'incertitude dans la sortie du modèle. Plusieurs mesures d'importance ont été proposées, et les plus importantes d'entre elles sont discutées dans les références [Villmeurs 1988], [Pagès and Gondran 1980], [Hoyland and Rausand 2004]. L'analyse de sensibilité est souvent effectuée en changeant la valeur d'un certain paramètre à la fois tout en maintenant les autres paramètres à leurs valeurs nominales. Ainsi, nous pouvons étudier l'impact relatif de chaque changement sur la sortie du modèle.

Une analyse de sensibilité peut être utilisée pour révéler les faiblesses du modèle, pour étudier les effets d'hypothèses et de simplifications spécifiques, et dans certains cas, pour étudier l'effet des actions de réduction des risques proposées.

Dans une analyse par arbre de défaillance, nous pouvons, par exemple, étudier le changement de la probabilité de l'événement sommet en configurant quatre détecteurs de gaz comme un système 2oo4 au lieu d'un système 3oo4.

L'analyse de sensibilité peut aider l'analyste à comprendre la dynamique du système. En manipulant un large éventail de valeurs, elle peut lui donner un aperçu sur le

comportement du système dans des situations extrêmes. En effet, en étudiant comment le système réagit aux variations de ses variables d'entrée, l'analyse de sensibilité permet de répondre à un certain nombre de questions. L'analyse de sensibilité peut être également utilisée pour attirer l'attention de l'analyste sur les sous-systèmes et les éléments qui ont le plus d'impact sur le risque d'un système [Rausand 2011].

IV.3 Formalisme mathématique

L'analyse de sensibilité est effectuée pour montrer l'effet de la variation de $\tilde{\beta}$ et $\widetilde{DC}$ sur la $P\tilde{F}D_{avg}$ du SIS. La $P\tilde{F}D_{avg}$ calculée avec $\tilde{\beta}$ et $\widetilde{DC}$ est prise comme référence. En augmentant β ou en diminuant DC la PFD_{avg} augmente.

Comme tous les sous-systèmes du SIS sont concernés par la variation DC, seuls les sous-systèmes redondants du SIS sont concernés par la variation β. Les équations suivantes sont utilisées pour caractériser les variations de $\tilde{\beta}$ et $\widetilde{DC}$:

$$\tilde{\beta} = \tilde{\beta}_{ref} + \Delta\beta \qquad \text{et} \qquad \widetilde{DC} = \widetilde{DC}_{ref} - \Delta DC \tag{IV.3}$$

avec

$\tilde{\beta}_{ref}$: $\tilde{\beta}$ de référence. , $\Delta\beta$: variation de β.

$\widetilde{DC}_{ref}$: $\widetilde{DC}$ de référence. , ΔDC : variation de DC.

Le choix des valeurs $\Delta\beta$ et ΔDC devrait assurer une certaine proportionnalité et une variation cohérente. Dans notre cas, la proportion 2/5 pour $\Delta\beta/\Delta DC$ est utilisée pour caractériser cette proportionnalité. A noter que seules deux valeurs ΔDC sont prises en compte car la limite inférieure du DC atteint des valeurs négatives à partir de ΔDC = 15% pour le sous-système actionneur (architecture 1oo2) [Sal et al. 2017].

Les variations $\Delta\beta$ et ΔDC sont prises séparément et la propagation de ces variations peut s'écrire comme :

$$P\tilde{F}D_{avg,sens} = P\tilde{F}D_{avg,ref} + \Delta P\tilde{F}D_{avg,sens} \tag{IV.4}$$

avec $P\tilde{F}D_{avg,sens}$: $P\tilde{F}D_{avg}$ issue de l'analyse de sensibilité.

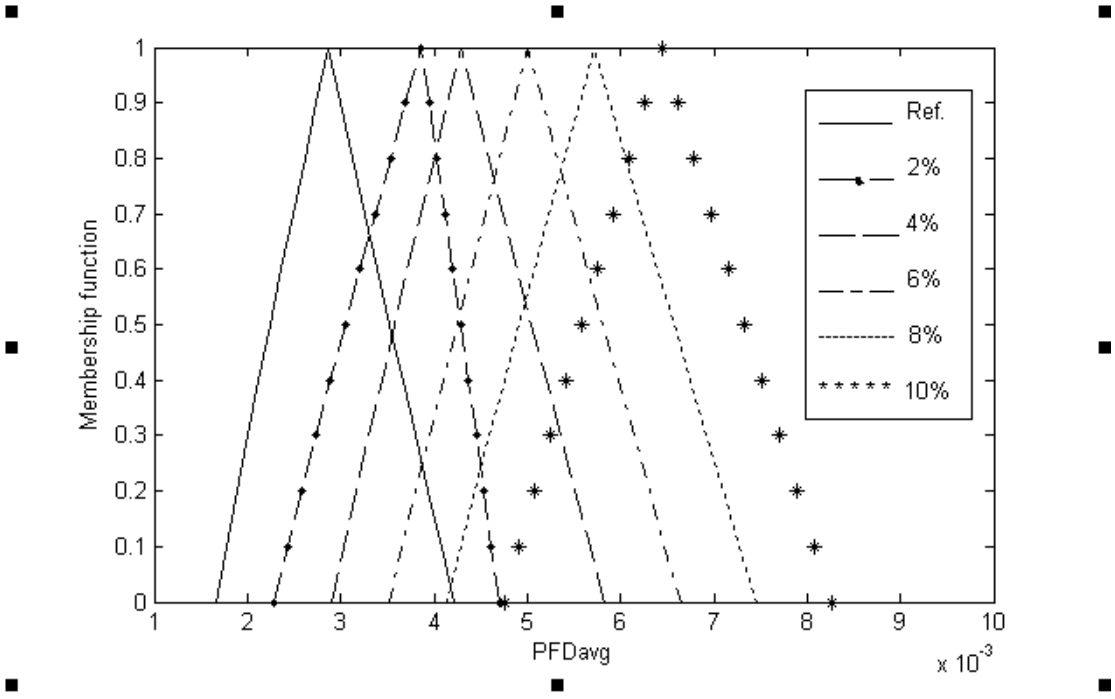
$P\tilde{F}D_{avg,ref}$: $P\tilde{F}D_{avg}$ de référence.

IV.4 Résultats

IV.4.1 Effet de la variation de β sur la $P\tilde{F}D_{avg}$

Les figures IV.2 (a)-(b) montrent l'effet de la variation de β sur la $P\tilde{F}D_{avg}$ pour les deux stratégies. Nous pouvons voir que la $P\tilde{F}D_{avg}$ dépasse le SIL 2 et atteint le SIL 3 pour la deuxième stratégie.

(a)



(b)

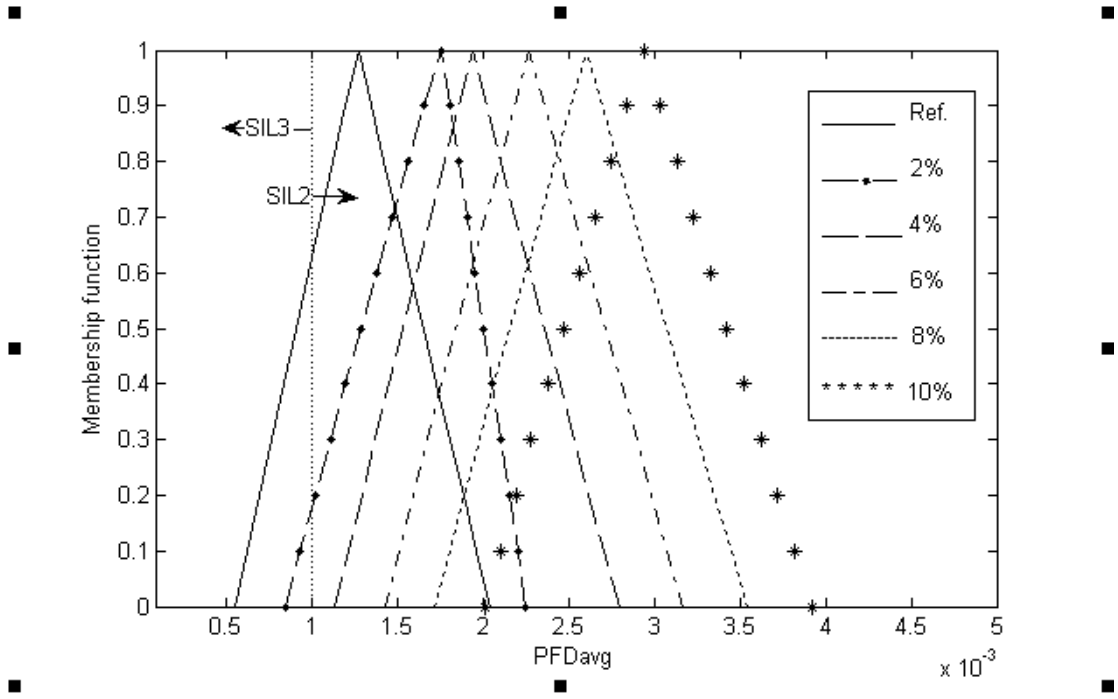
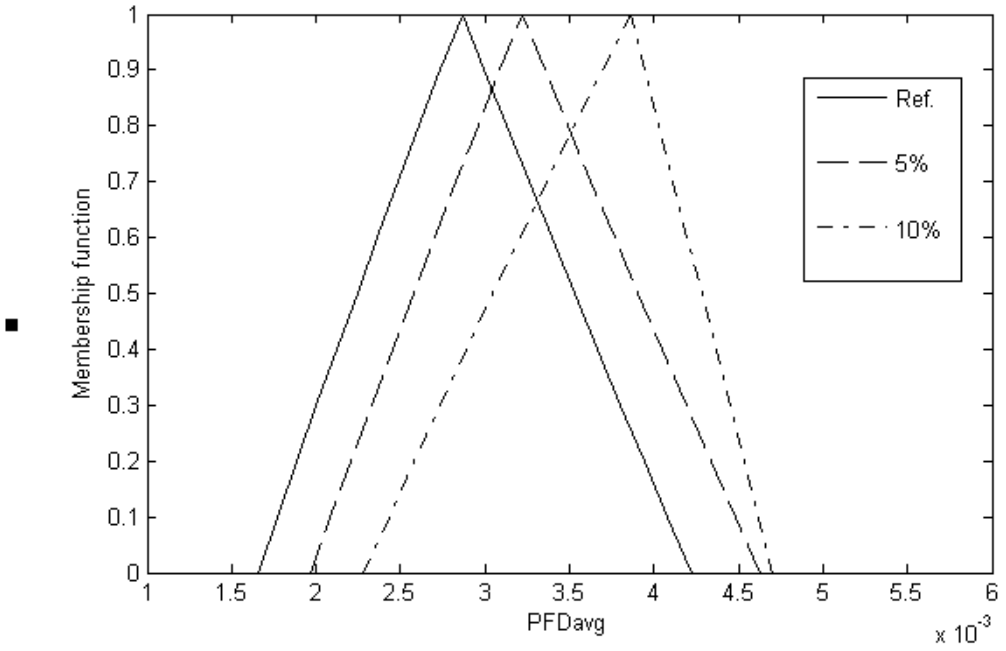


Fig. IV.2 Effet de la variation de β sur la $P\tilde{F}D_{avg}$.
(a) Première stratégie et (b) Seconde stratégie

IV.4.2 Effet de la variation du DC sur la $P\tilde{F}D_{avg}$

Les figures IV.3 (a)-(b) montrent l'effet de la variation du DC sur la $P\tilde{F}D_{avg}$ pour les deux stratégies. Comme pour la variation de β, la seconde stratégie est plus efficace. Nous remarquons bien que la $P\tilde{F}D_{avg}$ dépasse toujours le SIL 2 et atteint le SIL 3 pour la deuxième stratégie.

(a)



(b)

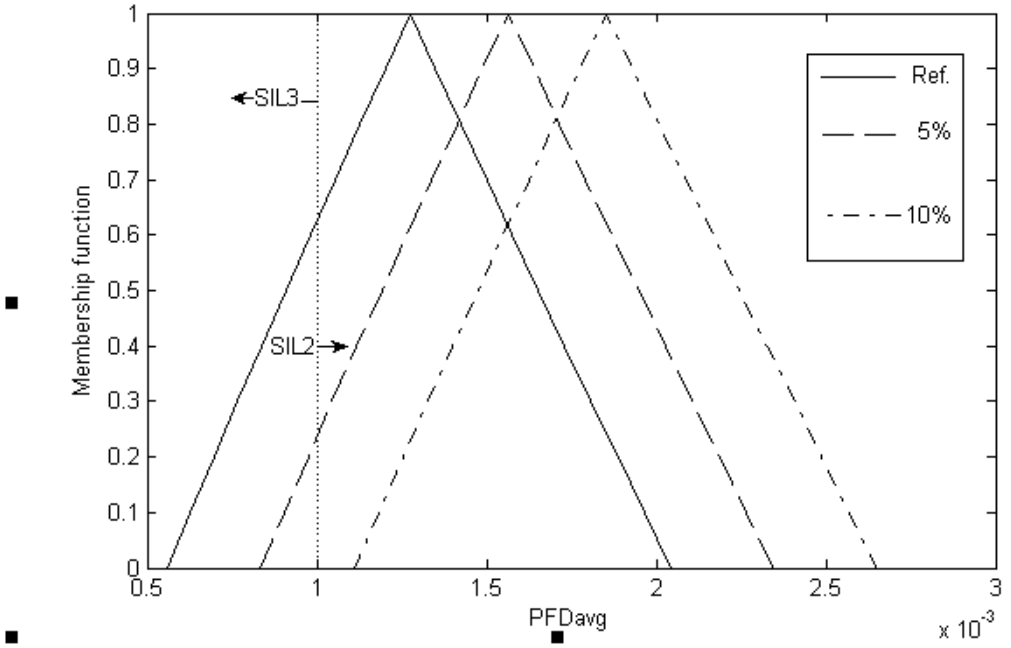


Fig. IV.3 Effet de la variation du DC sur la $P\tilde{F}D_{avg}$.
(a) Première stratégie et (b) Seconde stratégie

Pour une meilleure explication de l'effet de $\Delta\beta$ et ΔDC sur la $P\tilde{F}D_{avg}$ dans les deux stratégies, nous calculons d'une part les mesures de possibilité et de nécessité comme indices de classement de la $P\tilde{F}D_{avg}$ et la valeur seuil d'un intervalle SIL [Dubois et Prade 1983]. D'autre part, la distance de Hamming en tant que mesure de similarité des nombres flous sera calculée pour montrer la différence entre les $P\tilde{F}D_{avg,ref}$ et $P\tilde{F}D_{avg}$ provenant de différentes variations de β et DC [Kaufmann 1977].

IV.4.3 Comparaison de la $P\tilde{F}D_{avg}$ avec les SILs conventionnels

Comme il existe une relation de classement entre la $P\tilde{F}D_{avg}$ et les valeurs limites des intervalles SIL, nous pouvons considérer le problème de la comparaison d'une quantité floue et d'un nombre exact (crisp) en utilisant des mesures de possibilité et de nécessité. Soit l'inégalité $p \le L$, où p est une variable possibiliste dans une $P\tilde{F}D_{avg}$ et L est une valeur limite d'intervalle. Considérant l'inégalité floue $\boldsymbol{P\tilde{F}D_{avg} \le L}$, les mesures de possibilité et de nécessité comme indices de classement peuvent s'écrire [Dubois et Prade 1983] :

$$Pos\left(P\tilde{F}D_{avg} \le L\right) = sup\left\{\mu_{P\tilde{F}D_{avg}}(p) \middle| p \le L\right\} \quad \text{(IV.5)}$$

$$Nes\left(P\tilde{F}D_{avg} \le L\right) = 1 - sup\left\{\mu_{P\tilde{F}D_{avg}}(p) \middle| p > L\right\} \quad \text{(IV.6)}$$

Ces mesures de possibilité et de nécessité sont représentés par la figure IV.4 :

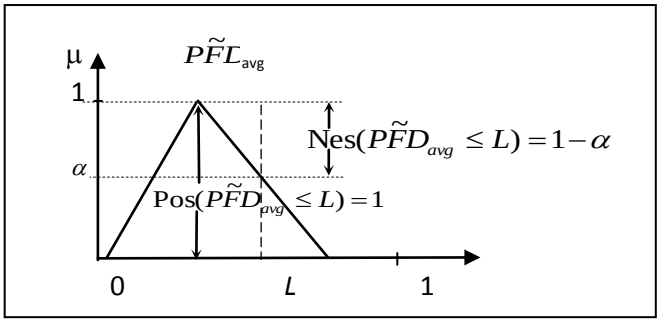


Fig. IV.4 Mesures de possibilité et nécessité de la $P\tilde{F}D_{avg} \le L$.

Les tables IV.1-a et IV.1-b montrent les mesures de possibilité et de nécessité dans le cas de la seconde stratégie. Pour la première stratégie, ces mesures sont nulles puisqu'il n'y a pas de chevauchement entre SIL 2 et SIL 3.

Table IV.1 Mesures de possibilité et de nécessité liées à la seconde stratégie. (a) $\Delta\beta$ et (b) ΔDC

(a)

	Ref.	2%	≥4%
Pos($\boldsymbol{P\tilde{F}D_{avg} \leq 10^{-3}}$)	0.63	0.18	0
Nes($\boldsymbol{P\tilde{F}D_{avg} \leq 10^{-3}}$)	0	0	0

(b)

	Ref.	5%	10%
Pos($\boldsymbol{P\tilde{F}D_{avg} \leq 10^{-3}}$)	0.63	0.25	0
Nes($\boldsymbol{P\tilde{F}D_{avg} \leq 10^{-3}}$)	0	0	0

Nous pouvons voir que Pos($P\tilde{F}D_{avg} \leq 10^{-3}$) relatif à ΔDC est légèrement supérieur à celui relatif à $\Delta\beta$. Ce résultat est en accord avec celui montré, au chapitre III, sur les figures III.10-b et III.10-c.

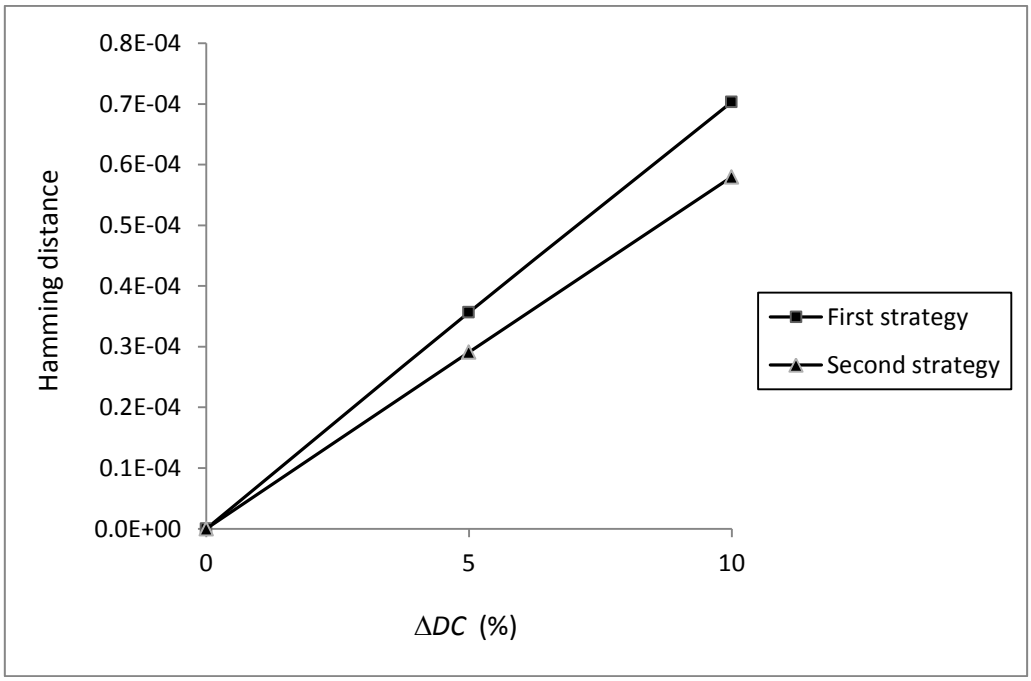
IV.4.4 Analyse de similarité entre les PFD floues

Comme toutes les $P\tilde{F}D_{avg}$ issues de l'analyse de sensibilité pour la variation de β et du DC sont clairement séparés (pas de chevauchement entre les nombres flous) seules les valeurs limites du support et modale sont considérées dans le calcul de la distance de Hamming. Considérant la représentation paramétrique de $P\tilde{F}D_{avg,ref}$ et $P\tilde{F}D_{avg,sens}$, la distance de Hamming (HD) peut être calculée comme [Kaufmann 1977] :

$$HD = \frac{1}{3}(|a_2 - a_1| + |m_2 - m_1| + |b_2 - b_1|) \quad \text{(IV.7)}$$

Pour montrer l'effet des deux stratégies sur les valeurs de la $P\tilde{F}D_{avg}$, nous avons calculé la distance de Hamming entre la $P\tilde{F}D_{avg,ref}$ et la $P\tilde{F}D_{avg,sens}$ pour les différentes valeurs de $\Delta\beta$ et ΔDC. Les résultats sont illustrés par les figures IV.5 (a)-(b).

(a)



(b)

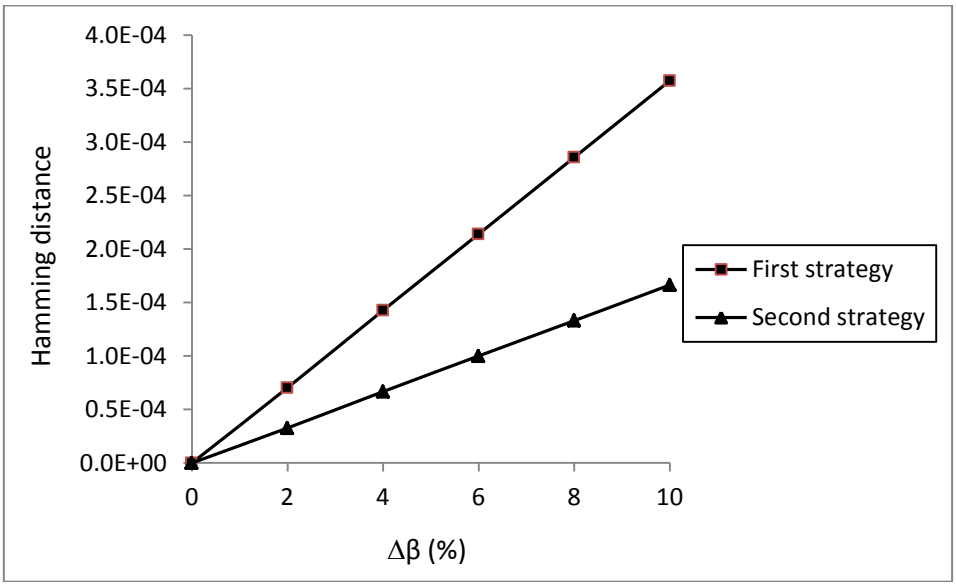


Fig. IV.5 Distance de Hamming.
(a) ΔDC et (b) $\Delta\beta$.

Comme on peut le voir, pour $\Delta\beta$ et ΔDC, les valeurs de la distance de Hamming obtenues pour la seconde stratégie sont inférieures à celles de la première. Ce résultat consolide les résultats de la section III.6.3 où nous avons montré clairement l'effet de la deuxième stratégie sur la $P\tilde{F}D_{avg}$ par rapport à la première. En effet, en référence aux figures IV.5 (a)-(b), la droite liée à la seconde stratégie exprime un effet de minimisation de la PFD_{avg} floue par cette stratégie, c'est-à-dire que la variation PFD_{avg} floue est moins rapide qu'avec la première stratégie.

Par conséquent, un accent particulier doit être mis sur le SIL requis lorsqu'il s'agit de réduire les risques dans un environnement incertain. L'intégrité de sécurité possibiliste basée sur des nombres flous permet le chevauchement sur l'échelle de SIL conventionnelle en tant qu'intervalles exactes adjacents. En considérant la seconde stratégie (test échelonné), la probabilité floue $P\tilde{F}D_{avg,ref}$ implique plutôt un SIL2, mais un SIL3 est aussi plus ou moins atteinte (Pos($P\tilde{F}D_{avg} \leq 10^{-3}$)=0.63) avec plus d'exigence probabiliste. La même remarque peut être étendue à de petites variations de $\tilde{\beta}$ et $\widetilde{DC}$. Cependant, de grandes variations de ces deux paramètres impliquent complètement un SIL2 (Nes($P\tilde{F}D_{avg} \leq 10^{-3}$)=0).

En pratique, on peut utiliser la mesure de nécessité Nes($P\tilde{F}D_{avg} \leq L$) $= \lambda$ (voir Figure IV.3), où L et λ sont la limite supérieure du SIL requis et un niveau de confiance imposé, respectivement, pour surmonter le problème d'interprétation des valeurs SIL et assurer la réduction de risque nécessaire telle que définie par la norme IEC 61508.

IV.5 Conclusion

L'analyse de sensibilité consiste à montrer l'effet de la variation de $\tilde{\beta}$ et $\widetilde{DC}$ sur la $P\tilde{F}D_{avg}$. Les mesures de possibilité et de nécessité montrent que l'effet de la variation de $\widetilde{DC}$ est légèrement supérieur à l'effet de la variation de $\tilde{\beta}$. En utilisant la distance de Hamming, il a été montré que la $P\tilde{F}D_{avg}$ est significativement influencée par la seconde stratégie (test échelonné).

Conclusion générale
et perspectives

1. Travail réalisé

Les normes IEC 61508 et 61511 sont les normes de référence pour la conception, le fonctionnement et le test des SIS. 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 de sécurité a entraînée la mise en place de nouveaux concepts tels que la PFD_{avg} pour les SIS faiblement sollicité et la PFH pour les SIS fortement sollicité. Comme dans ce mémoire, nous nous sommes intéressé uniquement aux SIS faiblement sollicité et périodiquement testés, alors, la PFD_{avg} est le critère qui permet de juger de la performance des SIS. Cette performance doit être évaluée par des méthodes référencées comme les diagrammes blocs de fiabilité (DBF), les arbres de défaillances (AdD), les chaînes de Markov ainsi que les réseaux de Pétri. Parmi plusieurs méthodes explorées, il a été conclu que le modèle de Markov est le plus approprié car il permet de modéliser facilement différentes situations.

Le grand problème que rencontre toute méthode quantitative est le manque de données de fiabilité pour pouvoir évaluer les performances des SIS. Ce manque de données ne peut engendrer que de l'imprécision sur les valeurs des paramètres utilisés dans les calculs. Pour surmonter cette difficulté, nous avons fait appel à une approche probabiliste floue qui est la théorie des ensembles floue pour modéliser l'imprécision liée à ces paramètres. Dans notre étude, les deux paramètres pertinents du SIS et qui sont entachés d'incertitude sont le facteur β et le taux DC. Ces deux paramètres sont modélisés par des nombres flous triangulaires. La $P\tilde{F}Davg$ de la fonction instrumentée de sécurité du SIS est évaluée par les chaînes de Markov floues utilisant la méthode des α-coupe.

Les tests périodiques constituent une tâche très importante pour les systèmes instrumenté de sécurité faiblement sollicités. C'est pourquoi notre travail s'est accentué sur ces tests pour les exploiter à des fins de diagnostic et montrer leurs impact sur la performance des SIS dans un environnement flou. Pour cela, deux types de stratégies de tests sont considérés : les tests simultanés et les tests échelonnés. Il a été montré que, pour la même stratégie de test, l'incertitude sur le taux DC semble avoir plus d'effet sur la $P\tilde{F}D_{avg}$ par rapport à l'incertitude sur le facteur β. Et lorsque nous avons effectué une comparaison entre les deux stratégies de test, les résultats montrent clairement l'effet de la deuxième stratégie (tests échelonnés) sur la $P\tilde{F}D_{avg}$ de l'HIPPS par rapport à la première (tests simultanés).

Une analyse de sensibilité est effectuée pour montrer l'effet de la variation de $\tilde{\beta}$ et $\widetilde{DC}$ sur la $P\tilde{F}D_{avg}$. Les mesures de possibilité et de nécessité montrent que l'effet de la variation de $\widetilde{DC}$ est légèrement supérieur à l'effet de la variation de $\tilde{\beta}$. En utilisant la distance de Hamming, il a été montré que la $P\tilde{F}D_{avg}$ est significativement influencée par la seconde stratégie (test échelonné).

2. Perspectives

Les perspectives de ce travail peuvent être résumées dans les points suivants :

- Il sera très intéressant de penser à modéliser les données imprécises par d'autres formalismes tels que les systèmes d'inférence flous.
- Etendre l'évaluation de la performance des SIS en présence de paramètres imprécis à d'autres méthodes de sûreté de fonctionnement tels que les réseaux de Pétri flous

Références bibliographiques

A

- ABRAHAMSSON M (2002). "Uncertainty in Quantitative Risk Analysis-Characterisation and Methods of Treatment". Department of Fire Safety Eng., Lund University, Report no 1024.

- ADROT O (2000). "Diagnostic à base de modèles incertains utilisant l'analyse par intervalle : l'approche bornante". Thèse de doctorat, Université de Nancy, France.

- AVRACHENKOV KE and Sanchez E (2002). "Fuzzy Markov Chains and Decision-Making". Fuzzy Optimization and Decision Making 1: 143-159.

B

- BIGRET R and Féron JL (1997). "Diagnostic, maintenance, disponibilité des machines tournantes. Modèle, mesurage, analyse des vibration", Masson.

- BOUGUELID MS (2007), "Contribution à l'application de la reconnaissance des formes et la théorie des possibilités au diagnostic adaptatif et prédictif des systèmes dynamiques". Thèse de doctorat soutenue le 12 décembre 2007 à l'Université de Reims Champagne-Ardenne, France.

- BOWLES JB and Pelaez CE (1995). "Application of fuzzy logic to reliability engineering". Proceedings of the IEEE 83(3).

- BRAUN SG (1989). "An overview. Mechanical signature analysis and diagnostic applications. IMMDC.

- BRISSAUT F, Barros A and Bérenguer C. "Evaluation et optimisation des probabilités de défaillance à la demande (PFD) soumis à des tests de révision partiels". Politiques de tests partiels et système de sécurité.

- BUCKLEY JJ (2005). "Fuzzy Probabilities: A New Approach and Applications". Springer, Berlin.

- BUCKLEY JJ and Eslami E (2002). "Fuzzy Markov Chains: Uncertain Probabilities". Mathware and Soft Computing 9(1).

- BUCKLEY JJ, Reilly K and Zheng X (2004). "Fuzzy probabilities for web planning". Soft Computing 8:464-476.

C

- CASSANDRAS CG and Lafortune S (2008). "Introduction to discrete event systems". 2nd edition, Springer, Berlin.

- CCP (2000). "Guidelines for Chemical Process Safety Quantitative Risk". Second edition, American Institute of Chemical Engineers, New York. USA.

- COOKE R, Bedford T (2001). "Probabilistic Risk Analysis: Foundations and Methods". Combridge University Press.

D

- DUBOIS D and Prade H (1983). "Ranking Fuzzy Numbers in the Setting of Possibility Theory". Information Sciences, 30: 183-224.

- DUBOIS D, Foulloy L, Mauris G and Prade H (2004). "Probability-possibility transformations, triangular fuzzy sets, and probabilistic inequalities". Reliable computing, 10:273-297.

- DUBUISSON B (1990). "Diagnostic par reconnaissance de formes". Editions Hermès, Paris.

G

- GOBLE WM and Brombacher AC (1999). "Using a failure mode, effects and diagnostic analyses (FMEDA) to measure diagnostic coverage in programmable electronic systems". Reliability Engineering and System Safety, 66(2) : 145-148.

- GOBLE WM and Cheddie H (2005). "Safety Instrumented Systems Verification: Practical Probabilistic Calculations". Raleigh, NC, ISA-The Instrumentation, Systems, and Automation Society, USA.

- GRUHN P, Pittmann J, Wiley S and Leblanc T (1998). "Quantifying the impact of partial strock valve testing of safety instrumented system. ISA Transaction 37, pp. 87-94.

H

- HAUGE S, Langseth H and Onshus T (2010). "Reliability data for safety instrumented system : PDS handbook". SINTEF report A 13502.

- HOKSTAD P and Rausand M (2008). "Common cause failure modeling: status and trends". In: Misra KB, editor Handbook of performability engineering, 621-640, Springer, London.

- HONEY WELL (2012). "Reliability & Availability Calculations". Project In Amenas, Algeria. Document No: 4500116867-G11-011.

- HOYLAND A and Rausand M (2004). "System Reliability Theory: Models, Statistical Methods and Applications". Second edition, Hoboken, NJ: Wiley.

- HOYLAND A and Rausand M (2004). "System Reliability Theory: Models, Statistical Methods and Applications". Second edition, Hoboken, NJ: Wiley.

I

- IEC 61508 (2010). "Functional safety of electrical /electronic/programmable electronic safety related systems. Part 1-7". International Electrotechnical Commission, Geneva.

- IEC 61511 (2003). "Functional safety: Safety instrumented systems for the process in industry sector. Part 1-3". International Electrotechnical Commission, Geneva.

- INNAL F (2008), "Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances. Anayse critique de la norme CEI 61508". Thèse de doctorat soutenue le 03 juillet 2008 à l'Université Bordeaux 1, France.

- INNAL F, Chebila M and Dutuit Y (2016), "Uncertainty handling in safety instrumented systems according to IEC 61508 and new proposal based on coupling Monte Carlo analysis and fuzzy sets". Journal of Loss Prevention in the Process Industries.

- INNAL F, Dutuit Y and Rauzy A (2006). "Quelques interrogations et commentaires relatifs à la norme CEI 61508". In Proceeding of the Lambda Mu 2006 Conference, Lille, France.

- ISERMANN R (2011). "Fault-Diagnosis Applications.Model-Based Condition Monitoring : Actuators, Drives, Machinery, Plants, Sensors, and Fault-tolerant Systems". Springer.

- ISO 18436 (2004). "Surveillance et diagnostic d'état des machines - Exigences relatives à la formation et à la certification du personnel".

J

- JIN H and Rausand M (2014). "Reliability of safety instrumented systems subject to partial testing and common cause failures". Reliability Engineering and System Safety, 121 : 146-151.

- JIN H, Lundteigen MA and Rausand M (2011). "Reliability performance of safety instrumented systems : A common approach for bothlow-andhigh-demand mode of operation. Reliability Engineering and System Safety, 96 : 365-373.

- JIN H, Lundteigen MA and Rausand M (2012). "Uncertainty assessment of reliability estimates for safety instrumented system". Journal of Risk and Reliability 226: 646-655.

K

- KAUFMANN A (1977). "Introduction à la théorie des sous-ensembles flous à l'usage des ingénieurs (fuzzy sets theory), éléments théoriques de base", Tome 1, deuxième édition, Masson.

- KAUFMANN A and Gupta MM (1991). "Introduction to Fuzzy Arithmetic Theory and Application". Van Nostrand Reinhold Company, New York, USA.

- KEMPOWSKY T (2004). "Surveillance de procédés à base de méthodes de classification : conception d'un outil d'aide pour la détection et le diagnostic des défaillances". Thèse de doctorat soutenue le 14 décembre 2004 à l'Institut National des Sciences Appliquées, Toulouse, France.

- KLETZ TA (1999). "HAZOP and HAZAN : identifying and assessing process industry hazards". 4th edition, Institution of chemical engineers.

- KOZINE IO and Utkin LV (2002). "Interval-Valued Finite Markov Chains". Reliable Computing 8: 97-113.

L

- LAMY P (2002). "Probabilité de défaillance dangereuse d'un système : explication et exemple de calcul". Note Scientifique et Technique 225, Institut National de Recherche et Sécurité (INRS), France.

- LE Duy TD (2011). "Traitement des incertitudes dans les applications des Études Probabilistes de Sûreté Nucléaire". Université de Technologie, Troyes.

- LI G and Xiu B (2014). "Fuzzy Markov chains based on the fuzzy transition probability". Proceeding of the 26th Chinese Control and Decision Conference (IEEE) 4351-4356.

- 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.

- LIU Y and Rausand M (2013). "Reliability effects of test strategies on safety instrumented systems in different demand modes". Reliability Engineering and System Safety 119: 235-243.

- LUNDTEIGEN MA and Rausand M (2007). "Common cause failures in safety instrumented systems on oil and gas installation: Implementing defense measures through function testing". Journal of Loss Prevention in the Process Industries 20(3): 218-229.

- LUNDTEIGEN MN and Rausand M (2008). "Partial stroke testing of process shutdown valves: How ti determine the test coverage". Journal of Loss Prevention in the Process Industries, 21 : 579-588.

- LYONNET P, Thomas M and Toscano R (2012). "Fiabilité, diagnostic et maintenance prédictive des systèmes". Editions TEC&DOC, Lavoisier, Paris.

M

- MARKOWSKI AS, Mannan MS, Kotynia A (Bigoszewska) and Siuta D (2010). "Uncertainty aspects in process safety analysis". Journal of Loss Prevention in the Process Industries 23: 446-454.

- MARKOWSKI AS, Mannan MS, Kotynia A and Pawlak H (2011). "Application of fuzzy logic to explosion risk assessment". Journal of Loss Prevention in the Process Industries 24: 780-790.

- MECHRI W (2011), "Evaluation de la performance des systèmes instrumentés de sécurité à paramètres imprécis". Thèse de doctorat soutenue le 11 avril 2011 à l'Ecole Nationale d'Ingénieurs de Tunis, Université El-Manar de Tunis, Tunis.

- MECHRI W, Simon C, Bicking F and Ben Othmane K (2013). "Fuzzy multiphase Markov chain to handle uncertainties in safety systems performance assessment". Journal of Loss Prevention in the Process Industries 26(4): 594-604.

- MKHIDA A (2008), "Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence". Thèse de doctorat soutenue le 14 novembre 2008 à l'Institut National Polytechnique de Lorraine, Université de Nancy, France.

- MOBLEY RK (1992). "La maintenance prédictive", Masson.

P

- PAGES A and Gondran M (1980). "Fiabilité des systèmes". Edition Eyrolles.

- PERNESTAL A (2009). "Probabilistic fault diagnosis with automative applications". PhD thesis, Linköping University, Sweden.

R

- RAJU CR (2005). "Strengthening the weak link : the shutdown valve". Sicon/05. Sensors for Industry Conference, Houtson, Texas, USA, February 2005.

- RAUSAND M (2011). "Risk assessment. Theory, Methods, and Applications". Wiley publication.

- RAUSAND M (2014) Reliability of safety-critical Systems: Theory and Applications. Wiley, Hoboken, NJ.

S

- SAL R, Nait-Said R and Bourareche M (2017). "Dealing with uncertainty in effect analysis of test strategies on safety instrumented system performance". International Journal of System Assurance Engineering and Management (Springer) 8(2): 1945-1958.

- 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". Thèse de doctorat soutenue le 19 octobre 2007 à l'Institut National Polytechnique de Lorraine, Université de Nancy, France.

- SALLAK M, Simon C and Aubry JF (2006). "Aide à la décision dans la réduction de l'incertitude des SIL : une approche floue/possibiliste". Revue des Sciences et Technologies de l'Automatique.

- SALLAK M, Simon C and Aubry JF (2008). "Conception Optimale des Systèmes Instrumentés de Sécurité en présence d'Incertitudes". Communication 6B-2. 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Avignon, 6-10 octobre.

- 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.

- SIGNORET JP (2005). "Methodology SIL evaluations related to HIPS". Technical report, Total, Draft Memo.

- SKLET S (2006). "Safety barriers: Definition, classification, and performance". Journal of Loss Prevention in the Process Industries 19(5): 494-506.

V

- VILLEMEUR A (1988). "Sûreté de fonctionnement des systèmes industriels. Fiabilité-Facteurs humains-Informatisation". Editions Eyrolles, Paris.

W

- WANG Y, West HH and Mannan MS (2004). "The impact of data uncertainty in determining safety integrity level". Process Safety and Environmental Protection, 82:393-397.

Z

- ZADEH L (1965) Fuzzy Sets. Journal of Information and Control 8(3):338-353.

- ZWINGELSTEIN G (1995). "Diagnostic des défaillances". Editions Hermès, Paris.

Annexe

Exemple de Listing du programme développé sous Matlab pour le calcul des PFD.

1)

```
%*** PROGRAMME PRINCIPAL : Détermination de la PFD(t) et PFD
avg du
%LS-1oo1 du SIS
global tm nt pha pas; % Valeurs uniques pour tous les élts du
SIS
clc
tic
tm=8760; % Durée de l'intervalle de test en h "proof test"
nt=10; % Nombre de tirages aléatoires
pas=1;%Pas d'intégration dans la chaine de Markov
pha=11; % Nombre des alpha-coupes : 0,0.1,0.2,..,1

%*** Données d'entrée du LS-SIS_1oo1
% Taux de Couverture de diagnostic flous Inf et Sup
Ci1= 0.9;
Cs1= 0.9;
Cm1= 0.9;
% Taux de défaillance constant : valeur modale
Lambdam1=1e-6;

% Temps de réparation
RT1=6;

%***Appel des fonctions des architectures
% PFD LS-1oo1 du SIS : SIS1oo1(.)
[pfdinf1,pfdsup1]=SIS1oo1p(Ci1,Cs1,Cm1,RT1,Lambdam1);

% Sauvgarde des pfdinf1 et pfdsup1 dans des fichiers ascii
save mat11i pfdinf1 -ascii -double;
save mat11s pfdsup1 -ascii -double;
```

2)

```
%*** PROGRAMME PRINCIPAL : Détermination de la PFD(t) et PFD
avg du
%ESV (1oo2) du SIS
global tm nt pha pas; % Valeurs uniques pour tous les élts du
SIS
clc
tic
tm=8760; % Durée de l'intervalle de test en h "proof test"
nt=10; % Nombre de tirages aléatoires
pas=1;%Pas d'intégration dans la chaine de Markov
pha=11; % Nombre des alpha-coupes : 0,0.1,0.2,..,1

%*** Données d'entrée du ESV-SIS_1oo2
   % Taux de Couverture de diagnostic flous Inf et Sup
Ci2=0.2;
Cs2=0.2;
Cm2=0.2;
   % Facteur des causes communes Beta
Bi2=0;
Bs2=0;
Bm2=0;

   %Taux de défaillance constant : valeur modale
Lambdam2=8.8e-6;
   %Temps de réparation
RT2=4;

% PFD ESV-1oo2 du SIS : SIS1oo2(.)
[pfdinf2,pfdsup2]=SIS1oo2p(Ci2,Cs2,Cm2,Bi2,Bs2,Bm2,RT2,Lambdam
2);

% Sauvegarde des pfdinf2 et pfdsup2 dans des fichiers ascii
save mat12i pfdinf2 -ascii -double;
save mat12s pfdsup2 -ascii -double;
```

3)

```
%*** PROGRAMME PRINCIPAL : Détermination de la PFD(t) et PFD
avg du
%PT 2oo3)-SIS
global tm nt pha pas; % Valeurs uniques pour tous les élts du
SIS
clc
tic
tm=8760; % Durée de l'intervalle de test en h "proof test"
nt=10; % Nombre de tirages aléatoires
```

```
pas=1;%Pas d'intégration dans la chaine de Markov
pha=11; % Nombre des alpha-coupes : 0,0.1,0.2,..,1

%*** Données d'entrée du PT-SIS_2oo3
% Taux de Couverture de diagnostic flous Inf et Sup
Ci3=0.6;
Cs3=0.6;
Cm3=0.6;
    % Facteur Beta flous Inf et Sup
Bi3=0;
Bs3=0;
Bm3=0;
    %Temps de réparation
RT3=2;
    %Taux de défaillance constant : valeur modale
Lambdam3=2.4e-6;

% PFD PT-2oo3 du SIS : SIS2oo3(.)
[pfdinf3,pfdsup3]=SIS2oo3p(Ci3,Cs3,Cm3,Bi3,Bs3,Bm3,RT3,Lambdam
3);

% Sauvegarde des pfdinf3 et pfdsup3 dans des fichiers ascii
save mat23i pfdinf3 -ascii -double;
save mat23s pfdsup3 -ascii -double;
```

4)

```
function
[pfdinf,pfdsup]=SIS1oo2p(DCi,DCs,DCm,Bi,Bs,Bm,MTTR,Lambdam)
% Prog : Calcul de la PFD floue d'un ESV-SIS de type 1oo2
% Méthode : Resolution of Regular Fuzzy Markov Chain par
%           Restricted Fuzzy Matrix Multiplication (RFMM)
%           James J. Buckley
%clc
tic
global nt tm pha pas
% Données d'entrée
ne=6; % Nombre d'états
% Initialisations
lb=zeros(ne,ne);
ub=zeros(ne,ne);
y0=zeros(ne,ne);
pt=zeros(1,ne);
y=zeros(ne,ne);
matsol=zeros(nt,ne);

matinf=zeros(tm,ne);
matsup=zeros(tm,ne);
```

```
pbinf=zeros(1,ne);
pbsup=zeros(1,ne);

pfdinf=zeros(tm,pha);
pfdsup=zeros(tm,pha);

va=zeros(pha,1);

pfdavginf=zeros(1,pha);
pfdavgsup=zeros(1,pha);
pfdavginfmat=zeros(tm,pha);
pfdavgsupmat=zeros(tm,pha);

pfdinfvect1=zeros(tm,1);
pfdsupvect1=zeros(tm,1);
pfdsupvect11=zeros(tm,1);
pfdavginfvect1=zeros(tm,1);
pfdavgsupvect1=zeros(tm,1);
pfdavgsupvect11=zeros(tm,1);

% vecteur de probabilités initial
p0=[1 0 0 0 0 0];

% Taux de Couverture de diagnostic flous Inf et Sup
%DCi=0.1;
%DCs=0.4;
%DCm=0.2;
% DCx=DCi*DCs;
% DCm=sqrt(DCx);
% Facteur des causes communes Beta
%Bi=0.09;
%Bs=0.12;
%Bm=0.10;
%Temps de réparation
%MTTR=8;
%Taux de défaillance constant : valeur unique
%Lambdam=4.66e-6;
%Lambdas=1e-5
%X=Lambdai*Lambdas
%m=sqrt(Lambdai,Lambdas)
%m=sqrt(X)
%pause
pha=1; % indice pour stocker les différentes alpha-coupes
alpha=0; % Cas du support
while alpha<=1
% Taux de Couverture de Diagnostic alpha-coupes (parties
ascendante et descendante)
DCia=alpha*(DCm-DCi)+DCi;
DCsa=-alpha*(DCs-DCm)+DCs;
% Taux de défaillance alpha-coupes
```

```
LDDs=Lambdam*DCsa;
LDUs=Lambdam*(1-DCia);% Soustraction floue 1-DCalpha

LDDi=Lambdam*DCia;
LDUi=Lambdam*(1-DCsa); %Soustraction floue 1-DCalpha
%LDi=Lambdaia/2.;

% Taux des DCC Beta alpha-coupes (ascendantes et descendantes)
Bia=alpha*(Bm-Bi)+Bi;
Bsa=-alpha*(Bs-Bm)+Bs;
% Expression des BD et BU flous
BUi=Bia;
BUs=Bsa;
% Supposition : BU=2xBD (Thèse Innal)
BDi=Bia/2;
BDs=Bsa/2;

%Taux de réparation constant : valeur unique
MDD=1/MTTR;
format long
%Matrice de transition à intervalles: bornes inf(lb)et bornes
sup(ub)
lb=[1-(BDs*LDDs+2*(1-BDi)*LDDs+2*(1-BUi)*LDUs+BUs*LDUs) 2*(1-
BDs)*LDDi 2*(1-BUs)*LDUi BDi*LDDi 0 BUi*LDUi;
   MDD 1-(LDDs+MDD+LDUs) 0 LDDi LDUi 0;
   0 0 1-(LDDs+LDUs) 0 LDDi LDUi;
   0 2*MDD 0 1-2*MDD 0 0;
   0 0 MDD 0 1-MDD 0;
   0 0 0 0 0 1];

ub=[1-(BDi*LDDi+2*(1-BDs)*LDDi+2*(1-BUs)*LDUi+BUi*LDUi) 2*(1-
BDi)*LDDs 2*(1-BUi)*LDUs BDs*LDDs 0 BUs*LDUs;
   MDD 1-(LDDi+MDD+LDUi) 0 LDDs LDUs 0;
   0 0 1-(LDDi+LDUi) 0 LDDs LDUs;
   0 2*MDD 0 1-2*MDD 0 0;
   0 0 MDD 0 1-MDD 0;
   0 0 0 0 0 1];

  % Cas des valeurs modales : un seul tirage
  if alpha==1
      nt=1;
  end
  t=1;
  while t<=tm % boucle de temps
  ti=t;

  for k=1:nt% boucle de tirages

   %Génération aléatoire de la matrice de trans précise
y0=lb+(ub-lb)*rand;
```

```
   %Détermination de la matrice de trans dont la somme des lig
=1
soml0=sum(y0,2);% "2" : Somme de chaque ligne de y0
for i=1:ne %Nbre de lignes de y0
    y(i,:)=y0(i,:)/soml0(i);
end
  %ps=eye(ne);
 %Détermination du vecteur solution pt à l'instant t
 pt=p0;
 com=1;
  while com<=ti
    pt=pt*y;
    %ps=ps*y
    com=com+pas;
  end

  %ps

  %Stockage des solutions possibles dans une matrice pour
chaque tirage k
  matsol(k,:)=pt;
  y0=zeros(ne,ne);

end % de tirages

%Recherche des valeurs inf et sup des probabilités-solutions à
t
 for j=1:ne %Nbre d'éléments de pt stockée
   pbinf(j)=min(matsol(:,j));
   pbsup(j)=max(matsol(:,j));
 end

 %Stockage des pb inf et sup pour chaque instant t
 matinf(t,:)=pbinf;
 matsup(t,:)=pbsup;
 pfdinf(t,pha)=pbinf(4)+pbinf(5)+pbinf(6);
 pfdsup(t,pha)=pbsup(4)+pbsup(5)+pbsup(6);
 matsol=zeros(k,ne);
 pbinf=zeros(1,ne);
 pbsup=zeros(1,ne);

 t=t+pas; % incrémentation imposée par pas
end % de temps
ki2=k;
ti2=t
alphaS2=alpha

pha=pha+1; % Compteur variant selon alpha
alpha=alpha+0.1; % Incrémentation des alpha-coupes
end % de alpha
pha=pha-1;
```

```
% Conservation de la variable alpha : va(pha)=alpha
 va=0:0.1:1; % Incrément=0.1

% Calcul des alpha-coupes de la PFD avg
% Somme des colones des pfdinf et pfdsup y compris les zéros
pfdinfsom=sum(pfdinf);
pfdsupsom=sum(pfdsup);
% Moyenne des lignes pour les valeurs différentes de zéros
(par pas)
pfdavginf=pfdinfsom*pas/tm
pfdavgsup=pfdsupsom*pas/tm

%Sauvegarde des pfd avg
save avg1oo2i pfdavginf -ascii -double;
save avg1oo2s pfdavgsup -ascii -double;

% Stockage de tm=dim(vt) pfdavginf et pfdavgsup
% en vu d'une représentation graphique
tt=1;
while tt<=tm
        pfdavginfmat(tt,:)=pfdavginf;
        pfdavgsupmat(tt,:)=pfdavgsup;
        tt=tt+pas;
   end

% Affectation des colonnes de pfdinf, pfdsup, pfdavginf et
pfdavgsup dans
% des vecteurs et localisation des valeurs <>0 par la fonction
find
% Le vecteur indtemps correspond aux valeurs <>0

pfdinfvect1=pfdinf(:,1);% instantannée pour alpha=0
indtemps=find(pfdinfvect1);

%lgindtemps=length(indtemps);

pfdsupvect1=pfdsup(:,1);% instantannée pour alpha=0

pfdsupvect11=pfdsup(:,11);%alpha=1, identique à pfdinf(:,11)

pfdavginfvect1=pfdavginfmat(:,1);% avg inf pour alpha=0

pfdavgsupvect1=pfdavgsupmat(:,1);% avg sup pour alpha=0

pfdavgsupvect11=pfdavgsupmat(:,11);%avg sup pour alpha=1
identique à avg inf

% Représentation graphique de la PFD(t)PFDavg du SDV-SIS_1oo2
figure(3);% pha=1 -> alpha=0, pha=11 -> alpha=1, pour laquelle
on trace une seule courbe pfdsup(:,11) et pfdavgsupmat(:,11)
```

```
plot(indtemps,pfdinfvect1(indtemps),'-
.',indtemps,pfdsupvect1(indtemps),'+',indtemps,pfdsupvect11(in
dtemps),'*',indtemps,pfdavginfvect1(indtemps),'-
.',indtemps,pfdavgsupvect1(indtemps),'+',indtemps,pfdavgsupvec
t11(indtemps),'*')
title('PFD of ESV subsystem');
xlabel('Time (h)');
ylabel('PFD');

% Représentation graphique des alpha-coupes de la PFDavg
figure(4);
plot(pfdavginf,va,'-.',pfdavgsup,va,'-.')
title('Fuzzy average PFD of ESV subsystem');
xlabel('PFD');
ylabel('Membership function');

toc
```

5)

```
%*** PROGRAMME PRINCIPAL : Détermination et Représentation de
la PFD(t) et PFD avg du SIS
%global tm nt pha vt va ; % Valeurs uniques pour tous les élts
du SIS
clc
tic % Début Chronomètre
% Valeurs d'entrée uniques pour tous les élts du SIS
tm=8760; % Durée de l'intervalle de test en h "proof test"
%nt=100; % Nombre de tirages aléatoires
pha=11; % Nombre des alpha-coupes : 0,0.1,0.2,..,1
npt=1;% Nombre d'intervalles de test
pas=1;%Pas d'intégration dans la chaine de Markov
% Initialisation
pfdinf3t3=zeros(tm,pha);
pfdsup3t3=zeros(tm,pha);
pfdinf2t2=zeros(tm,pha);
pfdsup2t2=zeros(tm,pha);
%pfdsisinf1=zeros(tm,pha);
%pfdsissup1=zeros(tm,pha);
%pfdsisinf2=zeros(tm,pha);
%pfdsissup2=zeros(tm,pha);
pfdavginfm1=zeros(tm,pha);
pfdavgsupm1=zeros(tm,pha);
pfdavginfm2=zeros(tm,pha);
pfdavgsupm2=zeros(tm,pha);
indtm=zeros((tm/pas)+1,1);% vecteur de temps integrant, en
plus de indtemps, la valeur tm
%format long
```

```
%Lecture des pfd inf et sup des architectures 1oo1, 1oo2 et
2oo3 à partir de fichiers
pfdinf1=load('mat11i');
pfdsup1=load('mat11s');
%pause;
pfdinf2=load('mat12i');
pfdsup2=load('mat12s');
%pause;
pfdinf3=load('mat23i');
pfdsup3=load('mat23s');

%Lecture des vecteurs temps et alpha à partir de fichiers
%indtemps=load('vectemps');
%va=load('vectalpha');


%***DÉTERMINATION DE LA PFD(T) DU SIS SELON LES STRATÉGIES DE
TEST
%% STRATÉGIE DE RÉFÉRENCE "FIRST STRATEGY" : CAS OÙ LES
ÉLÉMENTS DU SIS SONT TESTÉS SIMULTANÉMENT

 format long;
 pfdsisinf1=pfdinf1+pfdinf2+pfdinf3;
 pfdsissup1=pfdsup1+pfdsup2+pfdsup3;

 % PFDavg calculée avec prise en compte des valeurs de PFD(tm)
 %%pfdsisavginf1=mean(pfdsisinf1)
 %%pfdsisavgsup1=mean(pfdsissup1)

 % Calcul des alpha-coupes de la PFD avg
% Somme des colones des pfdinf et pfdsup y compris les zéros
pfdsisinf1som=sum(pfdsisinf1);
pfdsissup1som=sum(pfdsissup1);
% Moyenne des lignes pour les valeurs différentes de zéros
(par pas)
pfdsisavginf1=pfdsisinf1som*pas/tm
pfdsisavgsup1=pfdsissup1som*pas/tm
%size(pfdsisavginf1)
%size(pfdsisavgsup1)
%pause;
%Sauvegarde des pfd avg inf et sup de la première stratégie
save avgsis1i pfdsisavginf1 -ascii -double;
save avgsis1s pfdsisavgsup1 -ascii -double;

 % Stockage de tm=dim(vt) pfdsisavginf et pfdsisavgsup
% en vu d'une représentation graphique
  tt=1;
while tt<=tm
    pfdavginfm1(tt,:)=pfdsisavginf1;%V alpha
    pfdavgsupm1(tt,:)=pfdsisavgsup1;%V alpha
    tt=tt+pas;
```

```
end

% Affectation des colonnes de pfdinf, pfdsup, pfdavginf et
pfdavgsup à
% des vecteurs pour alpha=0 et alpha=1

% pfd instantannées
pfdsisinfvec1=pfdsisinf1(:,1);%alpha=0
pfdsissupvec1=pfdsissup1(:,1);%alpha=0
pfdsissupvec11=pfdsissup1(:,11);%alpha=1

%pfd moyennes
pfdsisavginfvec1=pfdavginfm1(:,1);
pfdsisavgsupvec1=pfdavgsupm1(:,1);
%avgsuptm=pfdsisavgsupvec1(tm)
pfdsisavgsupvec11=pfdavgsupm1(:,11);

% Localisation des valeurs des pfd <>0 par la fonction find
% Le vecteur indtemps correspond aux valeurs de temps<>0
indtemps=find(pfdsisinfvec1);% indtemps est le même V alpha
%Affectation de indtemps à indtm pour la prise en compte de la
valeur tm
% pour les pfd instantannées seulement :
length(indtm)=length(indtemps)+1
indtm=indtemps;
indtm(tm/pas+1)=tm;

% Test et réparation "as good as new" du SIS à l'instant tm;
RT négligeable
pfdsisinfvec1(tm)=0; % equivalente à la pfd à t=0 pour alpha=0
pfdsissupvec1(tm)=0; % idem
pfdsissupvec11(tm)=0;% équivalente à la pfd à t=0 pour alpha=1

% Représentation graphique des PFD(t)et PFDavg du SIS

    % Ecriture de la variable va contenant les alpha :
va(pha)=alpha
   va=0:0.1:1; % Incrément=0.1
%pause
figure(7);% pha=1 -> alpha=0, pha=11 -> alpha=1 :une seule
courbe pfdsissup1(:,11) et pfdsisavgsupm1(:,11)
k=0;
while k<=npt % nbre de proof test
  plot(indtm+k*tm,pfdsisinfvec1(indtm),'-
.',indtm+k*tm,pfdsissupvec1(indtm),'--
.',indtm+k*tm,pfdsissupvec11(indtm),'-
',indtemps+k*tm,pfdsisavginfvec1(indtemps),'-
.',indtemps+k*tm,pfdsisavgsupvec1(indtemps),'--
.',indtemps+k*tm,pfdsisavgsupvec11(indtemps),'-')
  k=k+1;
  hold on
```

```
end
title('PFD of the SIF related to the first strategy');
xlabel('Time (h)');
ylabel('PFD');

% Représentation graphique des alpha-coupes de la PFDavg du
SIS
figure(8);
plot(pfdsisavginf1,va,'-.',pfdsisavgsup1,va,'-.')
title('Fuzzy PFDavg of the SIF related to the first
strategy');
xlabel('PFDavg');
ylabel('Membership function');

%% SECOND STRATEGY : CAS OÙ LES ÉLÉMENTS DU SIS ONT DES
INTERVALLES DE TEST DIFFÉRENTS
% PT : tm/4 ; SDV : tm/2 ; LS : tm
% Attention ! tm doit être divisible par 2 et par 4

%% Réecriture de la PFD de PT et SDV sur [0, tm]
%% en tenant compte des intervalles de tests

% Cas de PT
tt3=1;
while tt3<=tm
t3=1;
  while t3<=tm/4
    pfdinf3t3(tt3,:)=pfdinf3(t3,:);
    pfdsup3t3(tt3,:)=pfdsup3(t3,:);
       t3=t3+pas; % Incrémentation par pas relative au proof
test de PT
       tt3=tt3+pas; % Incrémentation par pas relative au proof
test du SIS
  end

end

% Cas de SDV
tt2=1;
while tt2<=tm
t2=1;
  while t2<=tm/2
    pfdinf2t2(tt2,:)=pfdinf2(t2,:);
    pfdsup2t2(tt2,:)=pfdsup2(t2,:);
       t2=t2+pas; % Incrémentation par pas relative au proof
test de SDV
       tt2=tt2+pas; % Incrémentation par pas relative au proof
test du SIS
  end

end
```

```
% Cas de LS
% PFD LS = pfdinf1 et pfdsup1 car elles restent inchangées sur
[0, tm]


% PFD(t) du SIS
 pfdsisinf2=pfdinf1+pfdinf2t2+pfdinf3t3;
 pfdsissup2=pfdsup1+pfdsup2t2+pfdsup3t3;

 % Calcul des alpha-coupes de la PFD avg
% Somme des colones des pfdinf et pfdsup y compris les zéros
pfdsisinf2som=sum(pfdsisinf2);
pfdsissup2som=sum(pfdsissup2);
% Moyenne des lignes pour les valeurs différentes de zéros
(par pas)
pfdsisavginf2=pfdsisinf2som*pas/tm
pfdsisavgsup2=pfdsissup2som*pas/tm
%size(pfdsisavginf2)
%size(pfdsisavgsup2)
%pause;

 %Sauvegarde des pfd avg inf et sup de la deuxième stratégie
save avgsis2i pfdsisavginf2 -ascii -double;
save avgsis2s pfdsisavgsup2 -ascii -double;

% Stockage de tm=dim(vt) pfdsisavginf2 et pfdsisavgsup2
% en vu d'une représentation graphique
tt=1;
while tt<=tm
 pfdavginfm2(tt,:)=pfdsisavginf2;
 pfdavgsupm2(tt,:)=pfdsisavgsup2;
 tt=tt+pas;
end

% Affectation des colonnes de pfdinf, pfdsup, pfdavginf et
pfdavgsup à
% des vecteurs pour alpha=0 et alpha=1

% pfd instantannées
pfdsisinfvec2=pfdsisinf2(:,1);%alpha=0
pfdsissupvec2=pfdsissup2(:,1);%alpha=0
pfdsissupvec22=pfdsissup2(:,11);%alpha=1

%pfd moyennes
pfdsisavginfvec2=pfdavginfm2(:,1);
pfdsisavgsupvec2=pfdavgsupm2(:,1);
%avgsuptm=pfdsisavgsupvec1(tm)
pfdsisavgsupvec22=pfdavgsupm2(:,11);

% Localisation des valeurs des pfd <>0 par la fonction find
```

```
% Le vecteur indtemps correspond aux valeurs de temps<>0
%indtemps=find(pfdsisinfvec1/2): indtemps est le même pour les
deux stratégies
%Affectation de indtemps à indtm pour la prise en compte de la
valeur tm
% pour les pfd instantannées seulement : identique à la
première stratégie
%indtm=indtemps
%indtm(tm/pas+1)=tm;

% Test et réparation "as good as new" du SIS à l'instant tm;
RT négligeable
pfdsisinfvec2(tm)=0; % equivalente à la pfd à t=0 pour alpha=0
pfdsissupvec2(tm)=0; % idem
pfdsissupvec22(tm)=0;% équivalente à la pfd à t=0 pour alpha=1

% Représentation graphique des PFD(t)et PFDavg du SIS
figure(9);% pha=1 -> alpha=0, pha=11 -> alpha=1 :une seule
courbe pfdsissup1(:,11) et pfdsisavgsupm1(:,11)
k=0;
while k<=npt % nbre de proof test
  plot(indtm+k*tm,pfdsisinfvec2(indtm),'-
.',indtm+k*tm,pfdsissupvec2(indtm),'--
.',indtm+k*tm,pfdsissupvec22(indtm),'-
',indtemps+k*tm,pfdsisavginfvec2(indtemps),'-
.',indtemps+k*tm,pfdsisavgsupvec2(indtemps),'--
.',indtemps+k*tm,pfdsisavgsupvec22(indtemps),'-')
  k=k+1;
  hold on
end
title('PFD of the SIF related to the second strategy');
xlabel('Time (h)');
ylabel('PFD');

% Représentation graphique des alpha-coupes de la PFDavg du
SIS
figure(10);
plot(pfdsisavginf2,va,'-.',pfdsisavgsup2,va,'-.')
title('Fuzzy PFDavg of the SIF related to the second
strategy');
xlabel('PFDavg');
ylabel('Membership function');

toc
```