République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université El-Hadj Lakhdar - Batna
Institut d'Hygiène et Sécurité Industrielle
Laboratoire de Recherche en Prévention Industrielle (LRPI)

MEMOIRE

Présenté pour l'obtention du diplôme de

MAGISTERE

EN HYGIENE ET SECURITE INDUSTRIELLE

Option : Gestion du Risque

Par

Loubna CHERGUI

Ingénieur en Hygiène et Sécurité Industrielle

Thème

Diagnostic des Défaillances et Optimisation des Architectures des Systèmes Instrumentés de Sécurité : Apport de la Logique Floue

Soutenu le 15 février2010 devant le jury composé de :

M.	Mébarek DJEBABRA, Professeur à l'Université de Batna	Président
M.	Rachid NAIT-SAID, Maître de Conférences à l'Université de Batna	Rapporteur
M.	Abdellah TAMRABAT, Maître de Conférences à l'Université de Batna	Examinateur
M.	Kheireddine CHAFAA, Maître de Conférences à l'Université de Batna	Examinateur
M.	Rachid SAL, Maître Assistant Classe A à l'Université de Batna	Membre Invité

2010

Remerciements

Le travail présenté dans ce mémoire a été mené au sein de Laboratoire de Recherche en Prévention Industrielle (LRPI) de l'INSTITUT d'Hygiène et Sécurité Industrielle de l'Université de Batna, dans le cadre d'un Mémoire de Magister en Hygiène et Sécurité Industrielle. Option Gestion du Risque.

J'adresse toute ma gratitude à mon promoteur Monsieur Rachid NAIT-SAID, Maître de Conférences à l'Université de Batna de m'avoir proposé ce sujet de mémoire et de m'avoir encadré. Pour sa collaboration inestimable, sa disponibilité et pour tous les conseils judicieux, pour ces critiques pertinentes, pour ça souplesse de travail. Je voudrais le remercier aussi pour sa patience et son soutien.

J'exprime mes profonds remerciements à Monsieur Rachid SAL, Maître Assistant à l'Université de Batna, et à Madame Nouara OUAZRAOUI, Maître Assistante à l'Université de Batna pour leur aide et leurs encouragements tout au long de ce travail.

Je remercie vivement également tous ceux qui ont contribué à développer une ambiance de travail agréable. En particulier, un grand merci à mes collègues du Magister :M^{lle}Achouri Nouhed,et Monsieur Bourareche Mouloud, ainsi que les étudiants du Magister Rabah Bilal , Sekoui Samir et Sallami Ilyas qui ont contribué à la mise au point de ce travail.

Mes remerciements iront naturellement vers tous ceux qui ont accepté avec bienveillance de participer au jury de mémoire :
Je remercie Monsieur Mébarek DJEBABRA, Professeur à l'Université de Batna pour avoir présidé le jury. Je salue également monsieur Kheireddine CHAFAA, Maître de Conférences à l'Université de Batna et Monsieur Abdellah TAMRABAT, Maître de Conférences à l'Université de Batna, d'avoir accepté d'examiner ce mémoire.

Enfin un grand merci à tous mes amis qui m'ont encouragé de près ou de loin pendant la fin de mon mémoire.

Dédicace

Je dédie ce travail à mes parents et toute la famille…

Table des matières

Table des figures vi

Liste des tableaux iii

Acronymes 1

Glossaire 2

Introduction générale 5

Chapitre 1: Systèmes Instrumentés de Sécurité

Introduction…….....9
1.1 Notions de sécurité…….....10
1.1.1 Principes généraux de protection……..…….....10
1.1.1.1 Sécurités passives……...…….....10
1.1.1.2 Sécurités actives……..…….....10
1.1.2 Sécurité fonctionnelle……..……..…….... ..11
1.1.2.1 Définitions……..……..... 11
1.1.2.2 Systèmes relatifs aux applications de sécurité ……...….. .11
1.2 Cadre normatif……..…….....12
1.2.1 Norme CEI 61508 ……..…….....12
1.2.2 Norme CEI 61511 ……..…….....15
1.2.3 Norme CEI 62061 ……..…….....17
1.2.4 Norme ISA-84……..…….....17
1.3 Cycle de vie de sécurité……..…….....18
1.4 Systèmes instrumentés de sécurité et terminologies relatives……..20
1.4.1 Définition d'un SIS……...…….20
1.4.2 Fonction instrumentée de sécurité……...…….....21
1.4.3 Propriétés d'un SIS……...……..21
1.4.4 Composition d'un SIS……...…….....22
1.4.4.1 Composition minimale d'un SIS……...……..22
1.4.4.2 Composition d'un SIS en fonction des tâches à accomplir ……....24
1.4.5 Redondance au sein d'un S.I.S……....25
1.4.6 Tests de système instrumenté de sécurité……...26
1.4.6.1 Test de diagnostic ……..26
1.4.6.2 Proof Test ……..26
1.4.7 Niveau d'intégrité de sécurité (SIL) …….....27
1.4.7.1 Paramètres Influant dans le calcul de SIL…….29
1.4.7.2 Méthode pour la détermination de SIL……..30
Conclusion……...31

Chapitre 2: Évaluation de l'Indisponibilité des Systèmes Instrumentés de Sécurité par le modèle Markovien

Introduction……...33
2.1 Évaluation de sûreté de fonctionnement des systèmes par chaîne de Markov ……....34
2.1.1 Processus de Markov, espace des états……...34

2.1.2 Système à deux dispositifs parallèles…….....35
2.1.3 Systèmes à deux dispositifs série……...…….....38
2.1.4 Système à redondance majoritaire ……...…….....39
2.1.5 Système à redondance passive ……...39
2.2 Détermination du PFD de l'architecture 1oo1 par le modèle Markovien conventionnel ……..40
2.2.1 Détermination du taux de réparation μ_{DU} ……....40
2.2.2 Modèle markovien 1oo1…….....41
2.2.3 Détermination de la disponibilité de l'architecture 1oo1……..…41
2.2.4 Détermination de l'indisponibilité moyenne PFD_{avg} du canal ……....42
2.3 Détermination du PFD de l'architecture 1oo2 par le modèle Markovien conventionnel ……42
2.3.1 Détermination du taux de réparation μ'_{DU} ……...43
2.3.2 Modèle markovien 1oo2 ……...43
2.3.3 Détermination de la disponibilité de l'architecture 1oo2……..44
2.3.4 Détermination de l'indisponibilité moyenne PFD_{avg} du 1oo2 ……...45
2.4 Détermination du PFD de l'architecture 2003 par le modèle Markovien conventionnel ……..45
2.4.1 Modèle markovien 2oo3 …….....46
2.4.2 Détermination de la disponibilité de l'architecture 2oo3 ……....46
2.4.3 Détermination de la t_{GE} d'indisponibilité pour 2oo3…….....46
2.4.4 Détermination de l'indisponibilité moyenne PFD_{avg} du 2oo3 ……..……..47
2.5 Exemple numérique…….... .47
Conclusion ……..…49

Chapitre 3 : Approche Markovienne Floue pour l'Evaluation de l'Indisponibilité des systèmes instrumentés de sécurité
Introduction……..50
3.1 Représentation des connaissances imparfaites……...51
3.1.1 Théorie des ensembles flous……...51
3.1.1.1 Définitions……...51
3.1.1.2 Principe d'extension de Zadeh……....53
3.1.1.3 Opérations simples sur les ensembles flous…….……...53
3.1.1.4 Notion d'alpha-coupe…..……...……..55
3.1.1.5 Compositions de relations floues ……..…….....56
3.1.1.6 Fermeture transitive d'une relation floue……...56
3.2 Détermination de la PFD des SIS par le modèle Markovien flou……..…….....58
3.2.1 Architecture 1oo1……...58
3.2.2 Architecture 1002 ……....63
Conclusion……....66

Chapitre 4: Evaluation des SIL d'un système opérationnel
Introduction ……..67
4.1 Description du système ……..68
4.1.1Rôle du four H401 …….....68
4.1.2 Décomposition structurelle et fonctionnelle du système four H401 …….....69
4.1.2.1 Sous système d'alimentation…….....69
4.1.2.2 Sous système de contrôle…….....69
4.1.2.3 Sous-système d'alarme…….....71
4.1.2.4 Sous-système d'arrêt d'urgence (système instrumenté de sécurité).....72
4.2 Diagnostic des défaillances des systèmes instrumentés de sécurité……...74
4.2.1 Application de l'approche Markovienne classique…….....75
4.2.2Application de l'approche Markovienne floue…….....78
4.2.3 Comparaison des deux modèles flou et conventionnel…….....82

Conclusion …….....82

Conclusion générale.....…….....83

Bibliographie.....…….....84

Table des figures

1.1-Structure générale de la norme IEC 61508[IEC61508, 2002]…..…….……... 13
1.2-Norme CEI 61508 et normes dérivées[Smith et Simpson, 2004] …….……..14
1.3-Structure générale de la norme IEC 61511[IEC61511, 2003]…….16
1.4-Exemple de fonction instrumenté de sécurité[Fal et Ldurka, 2000**]**……21
1.5-Shéma d'un SIS simple……...22
1.6-Schéma d'un SIS effectuant plusieurs taches ……24
1.7-Schéma d'un SIS recevant plusieurs informations ……25
1.8-Méthode de calcul de SIL……....29
2.1 -Processus markovien……...34
2.2 -Deux dispositifs et un seul réparateur…….....35
2.3-Fiabilité…….....36
2.4 -Deux dispositifs et deux réparateurs……. 37
2.5 -Détection de la panne totale…….…...37
2.6- Détection imparfaite de la panne…….……38
2.7- Fiabilité série…….....38
2.8-Diagrammes blocs physique et de fiabilité 1oo1…….…...40
2.9-Processus d'occurrence d'une défaillance non détectée sur [0, T_1] ……40
2.10-Graphe de Markov 1oo1 [Zhang et al, 2003]…….. ……..41
2.11-Diagrammes blocs physique et de fiabilité 1oo2 ……....43
2.12-Graphe de Markov 1oo2 ……...43
2.13-Diagrammes blocs physique et de fiabilité 2oo3……...45
2.14-Graphe de Markov 2oo3……....46
2.15-Evolution de l'indisponibilité de l'architecture 1oo1 en fonction du temps …….……...47
2.16-Effet des tests périodiques sur l'indisponibilité de l'architecture 1oo1 ……..…47
2.17-Evolution de l'indisponibilité de l'architecture 1oo2 en fonction du temps ……....48
2.18 Effet des tests périodiques sur l'indisponibilité de l'architecture 1oo2…….48
2.19- Evolution de l'indisponibilité de l'architecture 2oo3 en fonction du temps…….... 48
2.20-Effet des tests périodiques sur l'indisponibilité de l'architecture2003……....49
3.1-Ensemble flou trapézoïdal …….....52
3.2-Nombres flous triangulaires…….53
3.3-Exemple d'inclusion……... 53
3.4-Alpha-coupes d'un nombre flou…..……...…….... .55
3.5-Modèle Markovien contenu relatif à l'architecture 1oo1 …….……..59
3.6- Modélisation du taux de défaillance imprécis λ_{DD} par un nombre flou triangulaire……..…60

3.7- Modélisation du λ_{DD}, $\widetilde{\mu}_{DU}$ et $\widetilde{\mu}_{DD}$ par des nombres flous triangulaires ……...…60

3.8- Premier éliment le la matrice $\widetilde{M}$ ……..61

3.9- Modélisation du $1-(\lambda_{DD}+\lambda_{DU})\Delta t$ ……...61

3.10- *PFD* floue à l'instant *t* avec les *α*-coupes ……....62

3.11- courbes de la *PFD* 1001 floue pour α=0, α=0.5, et α=1 ……..62

3.12- courbe de la *PFD* 1001 après la défuzzification ……...…...63

3.13-Modèle Markovien contenu relatif à l'architecture 1oo2 ……....64

3.14- Courbes de la *PFD* 1002 floue pour α=0, α=0.5, et α=1 ……..……...65

3.15- courbe de la *PFD*1002 après defuzzification….....……..……...65

4.1- Rôle du four H401…….....68

4.2-Système de contrôle dans le four H401…….....70

4.3-Automate programmable PLC[JGC,2005] …….....73

4.4-Architecture 2oo3 de PLC[JGC,2005] …….....73

4.5- Architecture 1oo2 des vannes…….....74

4.6- Schéma simple du SIS…….....75

4.7- Evolution de l'indisponibilité du système en fonction du temps pour DC=60%……..... 76

4.8-Effet des tests périodiques sur l'indisponibilité du système pour DC=60% ……..... ……76

4.9- Evolution de l'indisponibilité du système en fonction du temps pour DC=90%……..... 77

4.10- Effet des tests périodiques sur l'indisponibilité du système pour DC=90%……..... …..77

4.11- Modélisation du taux de défaillance imprécis λ_D par un nombre flou triangulaire.....79

4.12-Variations des *PFD* du système pour α=0, α=0.5, et α=1 et DC=60%……..... ……...…79

4.13-Variation de la *PFD* du système après la defuzzification pour DC=60%……..…….... ……...80

4.14-Variations des *PFD* du système pour α=0, α=0.5, et α=1 et DC=90%…….....81

4.15-Variation de la *PFD* du système après la défuzzification pour DC=90%…….....82

Liste des tableaux

1.1 - Vue d'ensemble du cycle de vie de sécurité d'un SIS [IEC61511, 2003]……..18
1.2-Niveaux d'intégrité de sécurité selon la norme CEI 61508 [IEC61508, 2002]……...28
4.1- Sous-système d'alimentation ……69
4.2- Sous-système de contrôle ……..70
4.3- Sous-système d'alarme……...71
4.4- Les valeurs des taux de défaillance, et de la MTTF pour DC=60%..... .75
4.5- Les valeurs des taux de défaillance, et de la MTTF pour DC=90% .....……....77
4.6- Données numériques des taux de défaillance, et de la MTTF pour DC=60% …….....78
4.7- Données numériques des taux de défaillance, et de la MTTF pour DC=90% …….....81

Acronymes

A	Disponibilité
DCS	Distributed Controller System
E/E/PE	Electriques/Electroniques/Electroniques Programmables de sécurité.
ESD	Emergency Shut Down
FAL	Flow Alarm Low
FALL	Flow Alarm Low Low
FF	Failure Frequency
FV	Flow Valve
FT	Flow Transmitter
IEC	International Electrotechnical Comission
ISA	Instrument Society of America
ISO	International Organization for Standardization
MDT	Mean Down Time
MMF	Modèle de Markov Flou
MTTR	Mean Time To Restoration
PAHH/LL	Pressure Alarm High High/Low Low
PAH	Pressure Alarm High
PAL	Pressure Alarm Low
P_{CC}	Probabilité de défaillance de cause commune
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PFD_{avg}	Average Probability of Failure on Demand
PLC	Programmable Logic Controller
PSH/L	Pressure Switch High/Low
SIS	Safety Instrumented System
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SRECS	Systèmes de Commande Électriques Relatifs à la Sécurité de machines
TAH	Temperature Alarm High
TAHH	Temperature Alarm High High
T_1	Proof-test interval
t_{C1}	durée moyenne d'indisponibilité due à une défaillance non détectée d'un canal.
t_{CE}	durée moyenne globale d'indisponibilité pour les architectures 1oo2 et 2oo3
TI	Temperature Indicator
TV	Temperature Valve
H!! !	Taux de défaillance d'un canal
µ	Taux de réparation d'un canal
H_D	Taux de défaillance dangereuse du canal
H_{DD}	Taux de défaillance dangereuse détectée du canal
H_{DU}	Taux de défaillance dangereuse non détectée du canal
$µ_{DU}$	Taux de réparation dangereuse non détectée du canal
ß	Proportion de défaillance de cause commune non détectées (exprimées par une fraction dans les équations et par un pourcentage dans les autres cas)
$ß_D$	Défaillances détectées par les tests de diagnostics et ayant une cause commune (exprimées par une fraction dans les équations et par un pourcentage dans les autres cas)

Glossaire

Selon la norme CEI 61508 [IEC61508, 2002] :

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

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

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

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

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

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

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

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

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

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

Défaillance de cause commune

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

Détecté

Révélé ; Déclaré

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

Non détecté

Non révélé ; Non déclaré

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

Couverture de diagnostic

Fraction exprimant la décroissance de la probabilité de défaillance dangereuse du matériel résultant du fonctionnement des tests de diagnostic automatique.

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

Disponibilité A (t)

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

Taux de défaillance λ(t)

C'est la probabilité pour que le système soit défaillant Cette définition s'applique pour tout type d'éléments (système, sous-système, module, Composant).

Taux de défaillance dangereuse λD(t)

C'est la probabilité que le système soit défaillant de telle sorte qu'il soit incapable d'exécuter la fonction de sécurité attendue.

Probabilité de défaillance sur demande PFD (t) (Probability Failure on Demand)

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

Probabilité moyenne de défaillance sur demande PFDavg (Average of the probability failure on demand)

C'est la valeur moyenne par rapport à l'intervalle de temps entre proof test (test fonctionnel) de la probabilité de défaillance sur demande. Selon l'existence de proof test ou non, la valeur moyenne se calculera par rapport à l'intervalle de temps Ti entre ces proof tests.

$$PFD_{avg} = \frac{1}{Ti}\int_{0}^{Ti} PFD\ (t)\,dt$$

Cette grandeur s'utilise dans le cas des systèmes à faible sollicitation et c'est un nombre sans dimension.

MTTR (Mean Time To Repair)

C'est le taux moyen mis pour réparer le système.

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

Introduction générale

❖ Problématique

La principale vocation de la sécurité est d'éliminer les risques inacceptables qui pourraient affecter la santé des personnes, dégrader les biens et/ ou l'environnement. Pour assurer cette sécurité, il faut d'abord avoir une bonne organisation. Un effort de standardisation avait été fait avec la norme ISO 18000 mais celle-ci n'a jamais réellement vu le jour car les différents organismes internationaux participant à l'élaboration de cette norme internationale n'ont pu se mettre d'accord. Ceci a permis à d'autres référentiels de s'imposer tel que l'OSHAS 18000.

La sécurité, ce n'est évidemment pas que de l'organisation. C'est aussi des méthodologies à suivre, des moyens techniques à déployer. Et pour cela, une norme s'est imposée à l'échelle internationale : l'IEC 61508. Il s'agit d'une norme orientée "performances", c'est-à-dire qu'elle laisse à l'utilisateur le soin de réaliser son analyse du risque et elle lui propose des moyens pour réduire ce risque. Elle porte plus particulièrement sur les systèmes E/E/PE (électrique/électronique/électronique programmable de sécurité). En principe, elle ne concerne pas les systèmes simples, pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance.

L'application de la norme IEC61508 et des normes filles, notamment la 61511 pour l'industrie de process, a radicalement changé la position des entreprises par rapport au problème de la sécurité. En effet, ces normes imposent une obligation de résultats plutôt qu'une obligation de moyens. Dans ce contexte, un élément majeur développé dans ces normes est l'évaluation quantitative de la performance du système de sécurité mis en œuvre et la qualification de cette performance par des niveaux référencés. Ainsi, lorsque les installations présentent un risque non tolérable, qui ne peut être réduit par des solutions passives ou des conceptions plus fiables, les systèmes instrumentés de sécurité (SIS) sont mis en œuvre pour ramener le risque à un niveau acceptable. Cette performance doit alors être prouvée par des évaluations selon des méthodes référencés comme les arbres de défaillances, les chaînes de Markov, les réseaux de Pétri... pour s'indicer aux niveaux d'intégrité de sécurité (SIL) définis dans la norme[IEC61511, 2003]. Cette évaluation s'apparente à un calcul d'indisponibilité de la fonction de sécurité lors de sa sollicitation. Dans ce cadre, les chaînes de Markov ont été largement utilisées avec les avantages et inconvénients qu'on leur connaît.

Les systèmes instrumentés de sécurité sont des dispositifs sur lesquels nous n'avons pas forcément de retour de données en quantité. Ceci est d'autant plus vrai lorsque ces dispositifs sont faiblement sollicités, et pour lesquels le retour d'expérience est naturellement faible. De ce fait, le constat est que si dans les études d'indisponibilité des systèmes, les probabilités manipulées sont souvent considérés précises et parfaitement déterminables, dans les systèmes instrumentés de sécurité, leur précision est soumise à questionnement. Pour les systèmes instrumentés de sécurité fortement sollicités, le retour d'expérience est plus important, mais les données sont souvent synthétisées par des descripteurs tels que max, min et moyenne. Dans ce cas, la probabilité sous-jacente n'est pas connue avec précision. L'imprécision est donc liée à un manque de données (statistiques) sur les paramètres des composants et systèmes: valeurs des taux de défaillance et de réparation des composants. Ce problème de précision est connu et appréhendé de diverses manières. La théorie des ensembles flous semble offrir un cadre très adéquat pour la prise en compte des données imprécises et imparfaites. En effet la modélisation des taux de défaillance et de réparation par un nombre flou est une forme simple de l'imprécision, et les opérations floues permettent une estimation des probabilités de défaillance des composants ainsi que l'indisponibilité des SIS .

❖ Objectif

Le travail présenté dans ce mémoire a pour objectif de traiter l'évaluation de l'indisponibilité des SIS en présence de données imprécises et/ou incertaines.

Le formalisme des chaînes de Markov floues est choisi pour servir de support pour cette évaluation. Les transitions sont caractérisées par des probabilités floues permettant le calcul des PFD floues et les SIL correspondants.

❖ Organisation du mémoire

Le premier chapitre est dédié aux systèmes instrumentés de sécurité (SIS). Un tour d'horizon est effectué décrivant les normes de sécurité relatives aux SIS. La norme CEI 61508 est la norme générique et dispose d'autres déclinaisons selon le secteur industriel. Cette norme formalise une démarche pour l'estimation du risque que présente le procédé et permet d'évaluer la diminution du risque que doit apporter le système instrumenté de sécurité. Cette norme est basée sur l'analyse du risque et son évaluation permettant d'obtenir une intégrité de sécurité qui se matérialise par des niveaux d'intégrité de sécurité (*Safety Integrity Level* : SIL).

Dans le second chapitre, on s'intéresse à l'utilisation des chaînes de Markov pour l'évaluation performante de l'indisponibilité des systèmes instrumentés de sécurité où les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation, etc.) sont des valeurs ponctuelles et peuvent être connues avec précision et validées par le retour d'expérience.

Le troisième chapitre est consacré à la présentation de l'approche Markovienne floue. Nous examinerons les chaînes de Markov à transitions floues, que nous avons choisies pour évaluer les SIL des Fonctions Instrumentées de Sécurité (*SIF : Safety Instrumented Functions*). Cette approche permet de prendre en compte les incertitudes relatives aux paramètres de fiabilité (taux de défaillance et de réparation).

Dans le dernier chapitre, afin de mettre en valeur l'approche floue développé dans le chapitre précédent, nous présenterons une application à un système réel, qui mettra en évidence l'intérêt des résultats obtenus avec cette approche.

Ce travail de mémoire sera clôturé par une conclusion générale résumant le travail accompli.

Chapitre 1

Systèmes Instrumentés de Sécurité

Introduction

Les moyens à mettre en œuvre pour réduire les risques sont nombreux et variés. La conception du procédé, 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 dysfonctionnement.

Ces approches ne sont pas toujours suffisantes. Pour réduire encore les risques, il faut prévoir des systèmes de sécurité. Celles -ci participent soit à la prévention (en minimisant la probabilité d'apparition d'un risque), soit à la protection (pour limiter les conséquences d'un dysfonctionnement)**.** Les systèmes instrumentés de sécurité (SIS) sont souvent utilisés comme moyens de prévention et entrent en action lorsque le process se trouve dans des conditions anormales (et hors contrôle) et qu'une situation anormale risque de se développer et porter atteinte aux hommes, à l'environnement et aux biens.

Notre objectif, dans ce premier chapitre, est de faire un tour d'horizon des différentes caractéristiques des systèmes instrumentés de sécurité.

1.1 Notions de sécurité

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

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

1.1.1 Principes généraux de protection

Nous pouvons distinguer les mesures de sécurité par leur mode d'action : les sécurités passives et les sécurités actives.

1.1.1.2 Sécurités passives

La sécurité passive désigne tous les éléments mis en jeu afin de réduire les conséquences d'un accident lorsque celui-ci n'a pu être évité. Elle agit par sa seule présence, sans intervention humaine ni besoin en énergie (exemple : bâtiment de confinement, cuvette de rétention, etc.).

Cependant, il ne faut pas réduire la sécurité passive à la limitation des conséquences des accidents (l'isolation électrique est une mesure passive et préventive).

1.1.1.3 Sécurités actives

La sécurité active désigne tous les éléments mis en jeu afin d'éviter les accidents. Elle nécessite une action, une énergie et un entretien (exemple : détecteur, vannes, etc.).

La sécurité d'une installation repose sur l'utilisation de ces deux modes d'action. Une préférence est donnée au mode passif quand il est techniquement possible. Des critères de qualité sont exigés pour le mode actif, notamment la tolérance à la première défaillance : doublement de l'organe de sécurité (redondance). La sécurité fonctionnelle reste l'un des moyens les plus importants pour la prise en compte des risques. D'autres moyens de réduction ou d'élimination des risques, tels que la sécurité intégrée dans la conception, sont également d'une importance essentielle…)[Sellak,2007].

1.1.2 Sécurité fonctionnelle

1.1.2.1 Définitions

Selon la norme IEC 61061 [IEC61061, 1998], la sécurité fonctionnelle est le sous ensemble de la sécurité globale se rapportant à la machine et au système de commande de la machine qui dépend du fonctionnement correct des systèmes électriques de commande relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque.

Suivant la norme IEC 61508 [IEC61508, 2002], la sécurité fonctionnelle est le sous-ensemble de la sécurité globale qui dépend du bon fonctionnement d'un système ou d'un équipement en réponse à ses entrées.

La sécurité fonctionnelle couvre les produits ou systèmes mettant en œuvre des solutions de protection fondées sur diverses technologies :

- Mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable, optique, etc.
- Ou toute combinaison de ces technologies.

1.1.2.2 Systèmes relatifs aux applications de sécurité

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

Les systèmes de sécurité sont définis en termes d'absence de risque inacceptable de blessure ou de préjudice à la santé des personnes. Les dommages aux personnes peuvent être directs ou indirects, comme des dommages aux biens ou à l'environnement par exemple. Certains systèmes peuvent être principalement conçus pour se prémunir contre des pannes ayant des implications économiques majeures. Ceci signifie que dans l'esprit, à objectifs techniques comparables ou identiques, il n'y a pas de différence entre un système de sécurité et un système de contrôle commande. L'IEC 61508 [IEC61508, 2002] et l'IEC 61511 [IEC61511, 2003] peuvent

donc être utilisées pour développer n'importe quel système E/E/PE comportant des fonctions critiques, telles que la protection des équipements, des biens ou de la productivité.

1.2 Cadre normatif

1.2.1 Norme CEI 61508

En 1984, le comité technique 65 de la CEI a commencé une tâche de définition d'une nouvelle norme internationale relative à la sécurité. Cette norme CEI 61508 [IEC61508, 2002] est la seule norme multisectorielle traitant de l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP ; relies à la sécurité elle traite à la fois le matériel et le logiciel. C'est également la seule norme très technique qui apporte des clés, auxquelles il suffit de se conformer pour atteindre un objectif. Cette norme est orientée performances en laissant à l'utilisateur le soin de réaliser son analyse de risque et elle lui propose des moyens pour réduire ce risque. Elle ne concerne pas les systèmes simples, pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Par exemple, un système comportant des fins de course et des relais électromécaniques reliés à un disjoncteur peut être étudié sans avoir recours à la CEI 61508. La norme CEI 61508 repose sur deux concepts qui sont fondamentaux vis-à-vis de son application : le cycle de vie en sécurité et les niveaux d'intégrité de sécurité.

Cette norme s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs électriques/électroniques/électroniques programmables. Elle comprend 7 parties (figure 1.1), afin de couvrir les multiples aspects des systèmes E/E/PE :

– 61508-1 : Prescriptions générales.
– 61508-2 : Prescriptions propres aux systèmes E/E/PE.
– 61508-3 : Prescriptions relatives au logiciel.
– 61508-4 : Définitions et abréviations.
– 61508-5 : Exemples de méthodes pour déterminer le niveau d'intégrité de la sécurité.
– 61508-6 : Guides pour l'application des parties 2 et 3 de la norme.
– 61508-7 : Tour d'horizon des techniques et des mesures.

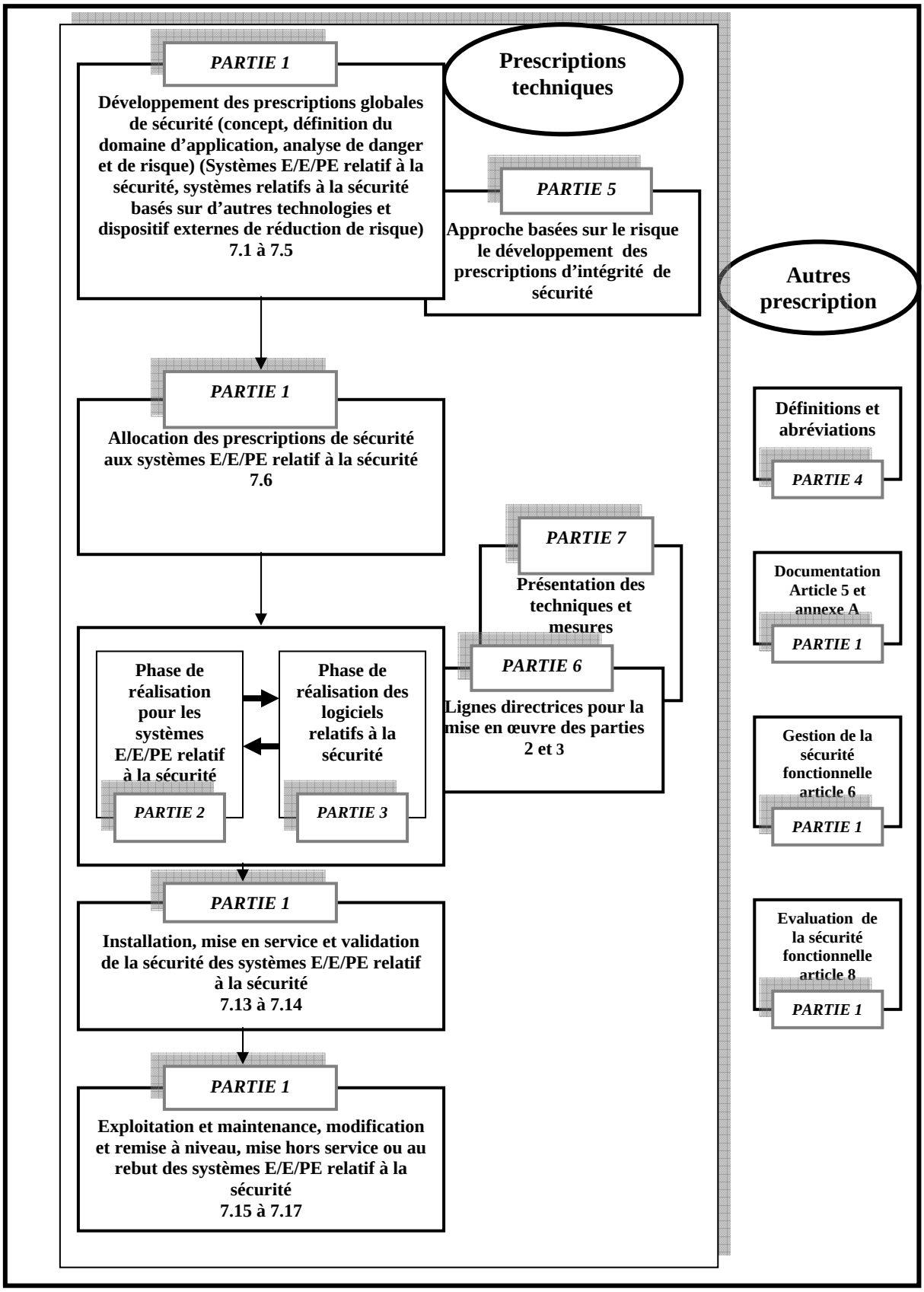

Figure 1.1- Structure générale de la norme IEC 61508 [IEC61508, 2002]

La norme CEI 61508 est la base d'autres normes sectorielles (ex : machines, procédés continus, ferroviaire, nucléaire) ou de produits (ex : variateurs de vitesse). Elle influence donc le développement des systèmes E/E/PE et des produits concernés par la sécurité à travers tous les secteurs. La figure (figure 1.2) [Smith et Simpson, 2004] montre la norme CEI 61508 générique et ses normes filles par secteur d'activité

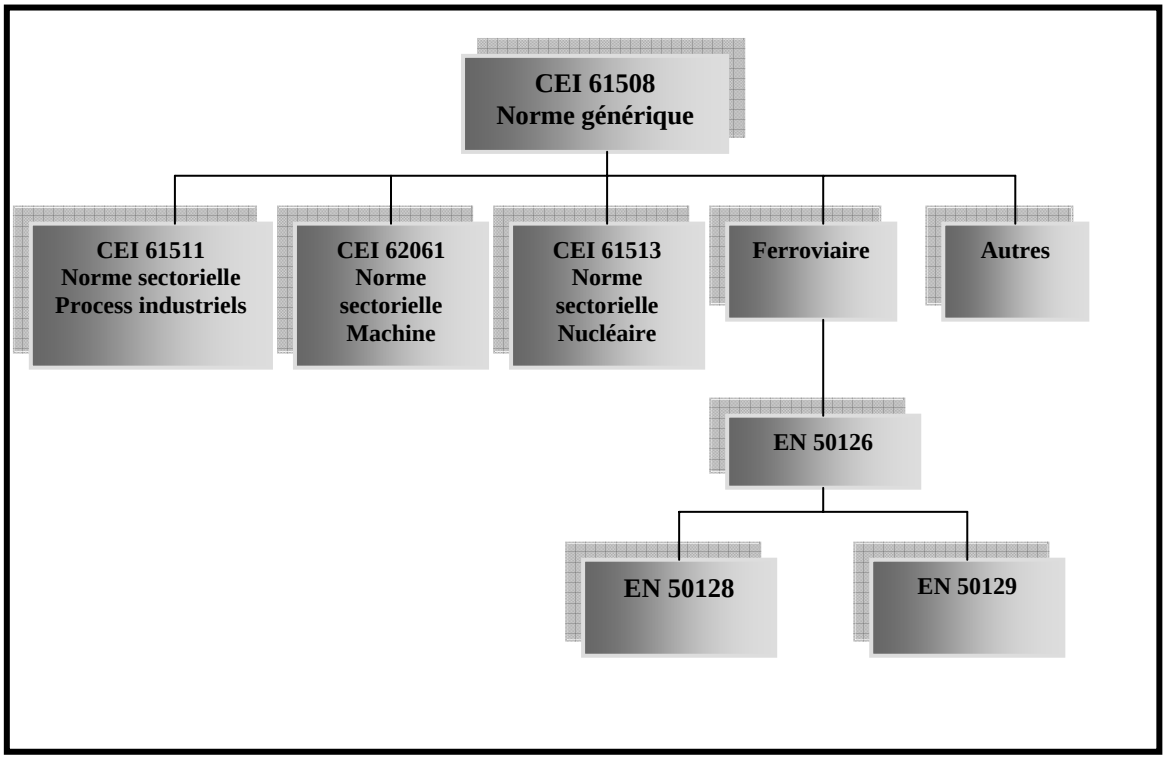

Figure 1.2- Norme CEI 61508 et normes dérivées [Smith et Simpson, 2004]

L'IEC 61508 [IEC61508, 2002] a pour but de :

- Fournir le potentiel des technologies E/E/PE pour améliorer à la fois les performances économiques et de sécurité.
- Elle fournit une méthode de développement pour réaliser la sécurité fonctionnelle des systèmes relatifs à la sécurité.
- Elle définit des niveaux d'intégrité de sécurité (SIL) des systèmes E/E/PE relatifs à la sécurité.
- Elle décrit une approche basée sur l'analyse de risque pour déterminer les niveaux d'intégrité de sécurité (SIL) à atteindre pour un risque donné.
- Elle fixe des objectifs quantitatifs de défaillances dangereuses des systèmes de sécurité en fonction des niveaux d'intégrité de sécurité.
- Elle décrit les principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité.

- Elle concerne toutes les phases du cycle de vie des matériels et du logiciel (depuis la conceptualisation, en passant par la conception, l'installation, l'exploitation, la maintenance, jusqu'à la mise hors service).
- Permettre des développements technologiques dans un cadre global de sécurité,
- Fournir une approche système, techniquement saine, suffisamment flexible pour le futur,
- Fournir une approche basée sur le risque pour déterminer les performances des systèmes concernés par la sécurité,
- Fournir une norme générique pouvant être utilisée par l'industrie, mais qui peut également servir à développer des normes sectorielles (par exemple : machines, usines chimiques, ferroviaires ou médicales) ou des normes produit (par exemple : variateurs de vitesse),
- Fournir les moyens aux utilisateurs et aux autorités de réglementation d'acquérir la confiance dans les technologies basées sur l'électronique programmable,
- Fournir des exigences basées sur des principes communs pour faciliter :

    - une compétence améliorée de la chaîne d'approvisionnement des fournisseurs de sous systèmes et de composants à des secteurs variés,
    - des améliorations de la communication et des exigences (c'est-à-dire de clarifier ce qui doit être spécifié),
    - le développement de techniques et de mesures pouvant être utilisées par tous les secteurs, augmentant de ce fait la disponibilité des ressources,
    - le développement des services d'évaluation de la conformité si nécessaire.

1.2.2 Norme CEI 61511

La norme sectorielle CEI 61511 concerne les systèmes instrumentés de sécurité pour le secteur les processus industriels. Cette norme présente une approche relative aux activités liées au cycle de vie de sécurité, pour satisfaire à ces normes minimales. Cette approche a été adoptée afin de développer une politique technique rationnelle et cohérente. Dans la plupart des cas, la meilleure sécurité est obtenue par une conception de processus de sécurité intrinsèques, chaque fois que cela est possible, combinée, au besoin, avec d'autres systèmes de protection, fondés sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable) et qui couvrent tous les risques résiduels identifiés. Elle comprend trois parties :

1. Cadre, définitions, exigences pour le système, le matériel et le logiciel,
2. Lignes directrices pour l'application de la CEI 61511-1,
3. Conseils pour la détermination des niveaux exigés d'intégrité de sécurité.

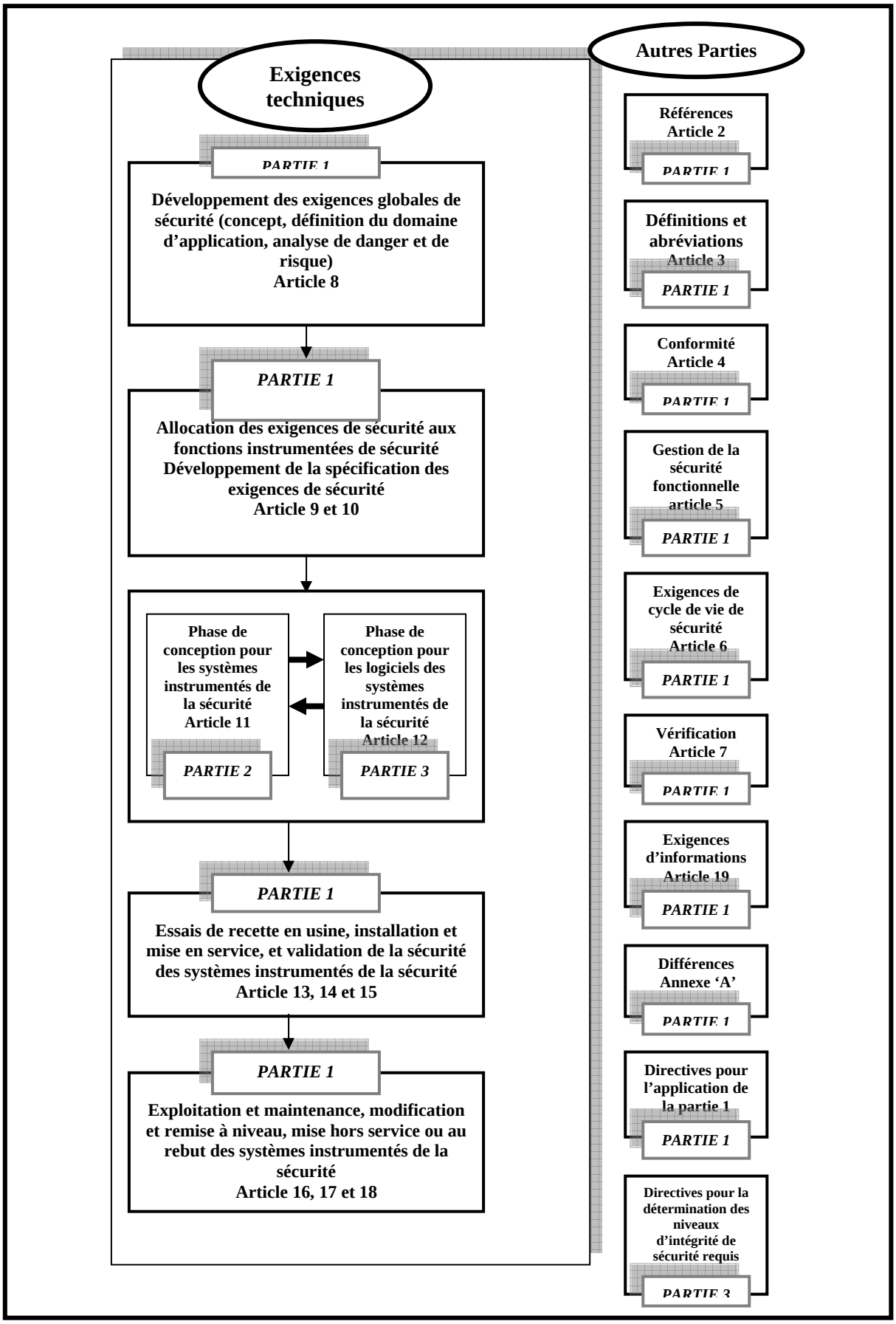

Figure 1.3-Structure générale de la norme IEC 61511 [IEC61511, 2003]

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

La norme CEI 61511 restreint le périmètre aux systèmes pour des applications SIL 1 à 3 (les applications SIL 4 ne pouvant être traitées par un SIS seul). Les applications qui nécessitent l'utilisation d'une fonction instrumentée de sécurité de niveau d'intégrité de sécurité SIL 4 sont rares dans l'industrie de processus. Ces applications doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité [IEC61511, 2003].

1.2.3 Norme CEI 62061

La norme CEI 62061 [IEC62061, 2005] est spécifique au secteur des machines dans le cadre de la CEI 61508. Elle est destinée à faciliter la spécification du fonctionnement des systèmes de commande électriques relatifs à la sécurité par rapport aux dangers significatifs des machines.

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

L'IEC 62061 a été rédigée dans l'objectif de devenir une norme internationale harmonisée pour la directive Machine. Ceci a été rendu possible en réduisant le périmètre de la CEI 61508 pour n'inclure que des exigences concernant des produits. La commission européenne reconnaît implicitement que l'EN 954-1 [EN 954-1,1996] est notoirement insuffisante dès que les chaînes de sécurité des machines contiennent des automatismes programmés. Elle recommande (sans encore l'imposer) d'appliquer la CEI 62061 [Rique.2005].

1.2.4 Norme ISA-84

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

La norme ISA-84 dispose uniquement de trois niveaux d'intégrité de sécurité, SIL1 à SIL3. C'est une norme nationale et incomplète par rapport à la norme CEI 61511 qui est une harmonisation de normes de plusieurs pays.

En 2004, le comité d'ISA SP84 a voté pour adopter le CEI 61511 comme nouvelle version d'ISA-84 (ANSI/ISA S84.00.01- 2004) [ISA 84.00.01, 2004]. Il y a, cependant, une différence significative entre la norme ISA-84 et la norme CEI 61511. ISA-84 a ajouté une clause première génération dans la nouvelle version (2004) qui permet l'utilisation continue des systèmes instrumentés de sécurité qui suivent la version originale de la norme [ISA-S84, 1996]. ISA est en cours de développement de directives et exemples d'implémentation basés sur le standard. Ceux-ci seront édités en tant que rapports techniques [Rique.2005].

1.3 Cycle de vie de sécurité

Dans toute fonction de processus, la sécurité fonctionnelle obtenue dépend d'un certain nombre d'activités exécutées de manière satisfaisante l'adoption d'une approche systématique du cycle de vie de sécurité vis-à-vis d'un système instrumenté de sécurité vise à s'assurer que toutes les activités nécessaires pour obtenir la sécurité fonctionnelle sont conduites et qu'il peut être démontré pour les autres qu'elles ont été exécutées dans un ordre approprié. La CEI 61511-1 présente un cycle de vie typique au Tableau1.1.

Tableau 1.1 - Vue d'ensemble du cycle de vie de sécurité d'un SIS [IEC61511, 2003]

Phase ou activité du cycle de vie en sécurité	**Objectifs**	**Données**	**Résultats**
Analyse des risques et conception des couches de protection	Identification des dangers et des événements dangereux liés au procédé et aux équipements associés, de la séquence d'événements conduisant à un événement dangereux, des risques du procédé associés à l'événement dangereux, des exigences de réduction des risques et des fonctions instrumentées de sécurité requises pour assurer la réduction des risques nécessaire	Conception du procédé, architecture et organisation humaine	Description des fonctions instrumentées de sécurité requises et des exigences d'intégrité de sécurité associées
Affectation des fonctions de sécurité aux couches de protection	Allocation des fonctions de sécurité aux couches de protection et pour chaque fonction instrumentée de sécurité, spécification du niveau d'intégrité de sécurité associé	Description des fonctions instrumentées de sécurité et des exigences d'intégrité de sécurité associées	Description de l'affectation des exigences de sécurité.
Spécification des exigences de sécurité du	Spécification des exigences pour chaque SIS, en termes de fonctions instrumentées de sécurité	Description de l'affectation des exigences	Exigences de sécurité du SIS ;

SIS	requises et de leur intégrité de sécurité associée, en vue d'assurer une sécurité fonctionnelle appropriée	de sécurité.	Exigences de sécurité du logiciel.
Conception et réalisation du SIS	Conception du SIS de façon à satisfaire aux exigences concernant les fonctions instrumentées de sécurité et l'intégrité de sécurité.	Exigences de sécurité du SIS. Exigences de sécurité du logiciel.	Conception du SIS en conformité avec ses exigences de sécurité; Planification des essais d'intégration du SIS.
Installation, mise en service et validation du SIS	Intégration et test du SIS. Validation du fait que le SIS satisfait en tous points les exigences de sécurité en termes de fonctions instrumentées de sécurité et d'intégrité de sécurité.	Conception du SIS ; Plan des tests d'intégration du SIS. Exigences de sécurité du SIS. Plan de validation de sécurité du SIS.	SIS en complet état de marche en conformité avec les modifications de conception résultant des tests d'intégration. Validation de la sécurité du SIS. Plan de validation du SIS.
Exploitation et maintenance du SIS	Vérification du fait que la sécurité fonctionnelle du SIS est maintenue pendant l'exploitation et la maintenance	Exigences concernant le SIS. Conception du SIS. Exploitation et maintenance du SIS	Exploitation et maintenance du SIS.
Modification du SIS	Réalisation des corrections, améliorations ou adaptations du SIS qui assurent l'obtention et le maintien du niveau d'intégrité de sécurité requis.	Exigences de sécurité du SIS révisées	Résultats de la modification du SIS.
Retrait de service	Mise en place d'une procédure de revue, d'une organisation adéquate, et garantie que les SIF restent adéquates.	Exigences de sécurité du système « à la construction » et documentation du procédé	SIF démantelé.
Vérification du SIS	Test et évaluation des résultats d'une phase pour s'assurer de leur exactitude et de leur cohérence par rapport aux produits et normes fournis comme données pour cette phase.	Plan de vérification du SIS pour chaque phase.	Résultats de la vérification du SIS pour chaque phase.
Evaluation de la sécurité fonctionnelle du SIS	Analyse et appréciation de la sécurité fonctionnelle réalisée par le SIS.	Plan d'évaluation de la sécurité fonctionnelle du SIS. Exigences de sécurité du SIS	Résultats de l'évaluation de la sécurité fonctionnelle du SIS

Pour toutes les phases du cycle de vie en sécurité, une planification pour la sécurité doit définir les critères, les techniques, les mesures et les procédures à employer pour :

- Garantir que les objectifs de sécurité fonctionnelle et de niveau d'intégrité de sécurité pour tous les modes pertinents du procédé seront atteints ;
- Assurer une installation et une mise en service correct du système instrumenté de sécurité ;
- Garantir l'intégrité de sécurité des fonctions instrumentées de sécurité après l'installation du SIS;
- Maintenir l'intégrité de sécurité durant l'exploitation (essais périodiques, etc.) ;
- Gérer les phénomènes dangereux liés au procédé pendant la phase de maintenance du système instrumenté de sécurité.

1.4 Systèmes instrumentés de sécurité et terminologies relatives

1.4.1 Définition d'un SIS

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

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

Les systèmes instrumentés de sécurité sont donc utilisés comme moyens de prévention et comportent une proportion grandissante de systèmes électriques, électroniques ou encore électroniques programmables (E/E/EP). Ces systèmes sont complexes ce qui rend difficile dans la pratique la connaissance de chaque mode de défaillance par l'examen des comportements possibles et la prévision des performances en terme de sécurité.

Un système instrumenté de sécurité est un système visant à mettre le procédé en état stable ne présentant pas de risque pour l'environnement et les personnes lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu…) [Sellak, 2007].

1.4.2 Fonction instrumentée de sécurité

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

La fonction de sécurité est définie comme la fonction qui doit être réalisée par un SIS, d'autres équipements de sécurité, cette fonction de sécurité a pour but de maintenir un état sécurisé du process.

Pour illustrer et rendre plus claire cette définition, nous proposons l'exemple d'un équipement utilisé dans la fonction instrumentée de sécurité (Figure 1.4).

Cette dernière est conçue pour protéger un réservoir sous pression contenant un liquide inflammable lorsque une haute pression a lieu à l'intérieur du réservoir, cette fonction de sécurité agira selon deux procédures :

- Fermeture de la vanne pour arrêter l'alimentation du liquide.
- Arrêt de la pompe qui injecte le liquide dans le réservoir.

Il est indispensable de lister tous les composants intervenant à la réalisation de cette fonction instrumentée de sécurité, ces composants sont :Transmitteur de pression, solver, vanne, pompe.

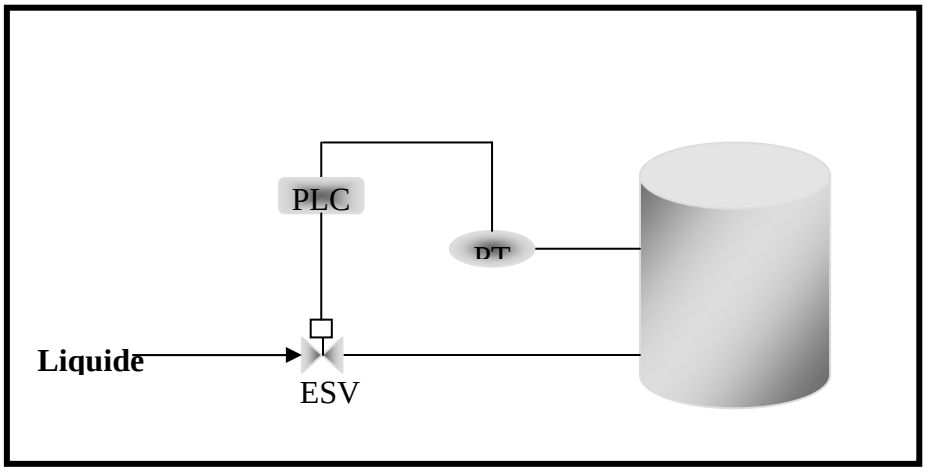

Figure 1.4-Exemple de fonction instrumenté de sécurité [Fal et Ldurka, 2000]

1.4.3 Propriétés d'un SIS

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

- Les systèmes instrumentés de sécurité nécessitent une source d'énergie extérieure pour remplir leur fonction de sécurité.
- On retrouve tout ou partie de ces différents éléments pour constituer des chaînes de sécurité.
- Plusieurs capteurs ou actionneurs peuvent être reliés à une même unité de traitement.
- Toutes les combinaisons de capteurs, d'unité de traitement et d'actionneurs qui sont exigées pour accomplir des fonctions de sécurité sont considérées comme une partie de systèmes instrumentés de sécurité.
- Les capteurs, l'unité de traitement, les éléments finaux sont des équipements de sécurité et réalisent des sous-fonctions de sécurité. L'ensemble des sous-fonctions réalise la fonction de sécurité.

1.4.4 Composition d'un SIS

1.4.4.1 Composition minimale d'un SIS

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

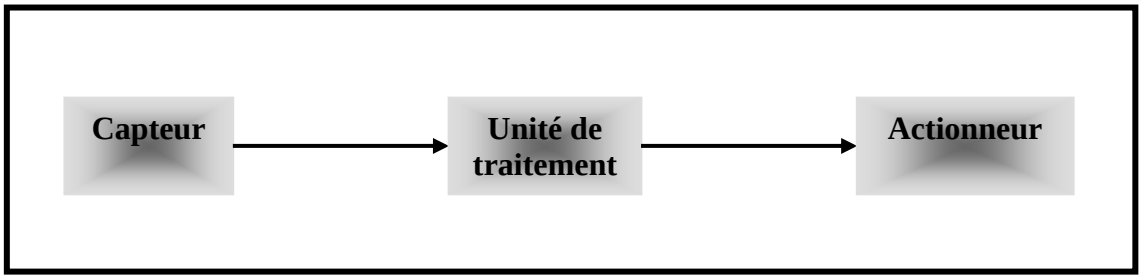

Figure 1.5-Shéma d'un SIS simple

A. Capteur

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

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

B. Unité de traitement

La fonction "traitement" peut être plus ou moins complexe [Ayault ,2005]. Elle peut se résumer à acquérir une grandeur mesurée par un capteur et à l'indiquer. Elle peut également consister à activer la commande d'un ou plusieurs actionneurs à partir d'une fonction combinatoire des informations délivrées par différents capteurs. Les unités de traitement peuvent être classées en deux catégories selon leur technologie :

- Les technologies câblées, à base de composants logiques élémentaires (relais), liés entre eux électriquement (ou de manière pneumatique).

- Les technologies programmées, à base de centrales d'acquisition ou d'alarmes, d'automates programmables (API), de systèmes numériques de contrôle commande (SNCC), de calculateurs industriels ou de cartes électroniques à microprocesseurs.

C. Actionneurs

Un actionneur peut être (vanne, moteur, servo-moteur…) transforment un signal (électrique ou pneumatique) en phénomène physique qui permet de commander le démarrage d'une pompe, la fermeture ou l'ouverture d'une vanne… Selon l'énergie motrice, on parle d'actionneur pneumatique, hydraulique ou électrique [Ayault ,2005].

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

Les capteurs, l'automate et les actionneurs sont des équipements de sécurité. Un équipement de sécurité est un élément d'un SIS qui remplit une sous-fonction de sécurité.

Exemples :

- un capteur remplit la sous-fonction "détecter du gaz",
- une vanne motorisée la sous-fonction "juguler une fuite".

Associées au traitement, l'ensemble de ces sous-fonctions permet la réalisation de la fonction instrumentée de sécurité "maîtriser une fuite".

1.4.4.2 Composition d'un SIS en fonction des tâches à accomplir

Un système instrumenté de sécurité a pour finalité, en cas de sollicitation, d'accomplir un certain nombre de fonctions (isoler une capacité, arrêter les flux de produits,….) qui elles-mêmes peuvent se décomposer en tâches (fermeture de plusieurs vannes, arrêt de plusieurs machines,…). C'est dans l'optique d'accomplir toutes les tâches que l'on trouve fréquemment au sein des SIS le montage en parallèle de plusieurs actionneurs.

A noter qu'un unique actionneur peut commander plusieurs actionneurs. Par exemple, une électrovanne trois voies située sur un réseau d'air instrumenté peut, par mise à l'atmosphère de ce réseau, commander la fermeture de toutes les vannes pneumatiques alimentées par le réseau.

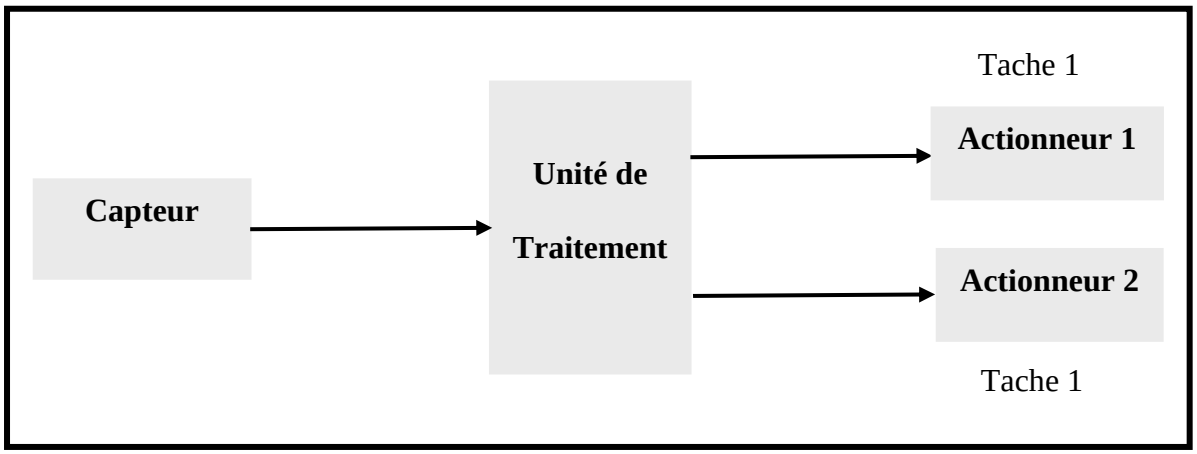

Figure 1.6-Schéma d'un SIS effectuant plusieurs taches

Beaucoup moins fréquemment, on trouve le montage en parallèle de plusieurs capteurs afin de répondre à un besoin de réception d'informations différentes (Pression et température d'un fluide par exemple) par l'unité de traitement pour décider le déclenchement des actions de sécurité (Figure1.6).

L'unité de traitement gère alors l'arrivée de différentes informations soit par un opérateur logique (par exemple, le déclenchement des actions de sécurité est réalisé si la température est supérieure à 100°C ou si la pression est supérieure à 10 bars), soit par calcul (par exemple, correction de l'information principale reçue par la deuxième information reçue).

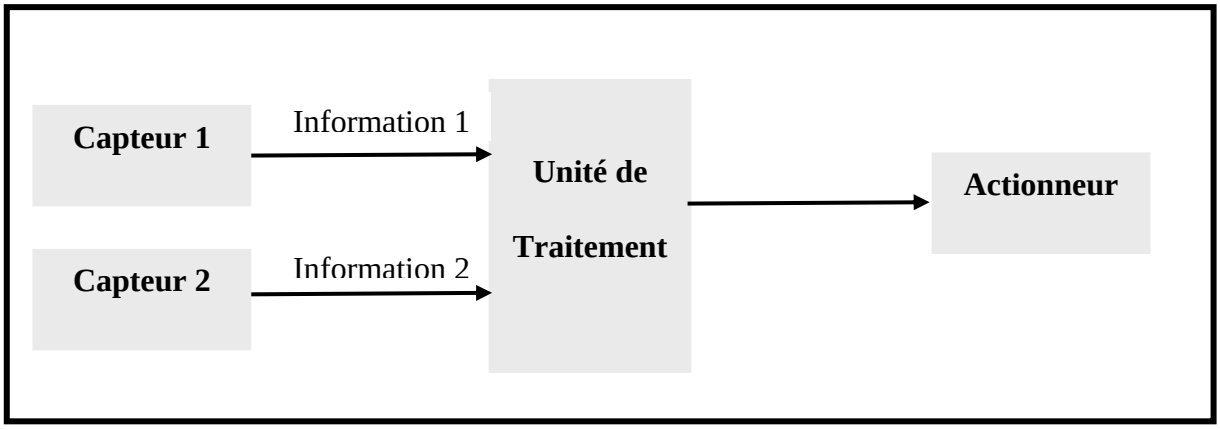

Figure 1.7-Schéma d'un SIS recevant plusieurs informations

1.4.5 Redondance au sein d'un S.I.S

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

Tous les éléments constituant un système instrumenté de sécurité peuvent être redondés : capteurs, unité de traitement, actionneurs et même les moyens de transmission.

A noter que l'on peut distinguer plusieurs types de redondance :

- **la redondance active** qui est une redondance telle que tous les moyens d'accomplir une fonction requise fonctionnent simultanément.

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

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

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

- **1oo1** (m=n=1) : Cette architecture comprend un seul élément, et toute défaillance dangereuse de cet élément empêche le traitement correct de tout signal d'alarme valide.

- **1oo2** (m = 1 et n = 2) : Cette architecture comprend deux éléments connectés en parallèle de façon que chacun puisse traiter la fonction de sécurité. Ainsi, il faudrait la défaillance dangereuse des deux éléments pour qu'un signal d'alarme valide ne soit pas traité correctement.

- **2oo2** (m = 2 et n = 2) : Cette architecture comprend deux éléments connectés en parallèle de sorte qu'il est nécessaire que les deux éléments demandent la fonction de sécurité avant que celle-ci ne survienne. La défaillance dangereuse d'un seul élément empêche le traitement correct de tout signal d'alarme valide.

- **2oo3** (m = 2 et n = 3) : Cette architecture comprend trois éléments connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie de telle sorte que l'état de sortie n'est pas modifié lorsqu'un seul élément donne un résultat différent des deux autres éléments. Il faudrait la défaillance dangereuse des deux éléments pour qu'un signal d'alarme valide ne soit pas traité correctement.

1.4.6 Tests de système instrumenté de sécurité

Généralement ces tests sont établis pour vérifier et contrôler le bon fonctionnement de *SIS*. Deux types de tests qui sont faits au niveau de *SIS* :

1.4.6.1 Test de diagnostic

Test en ligne (en fonctionnement) pour détecter des défauts, les tests de diagnostic sont effectués périodiquement et automatiquement pour détecter les défauts latents cachés qui empêchent le *SIS* (Safety Integrated System) de répondre à une demande [Lamy, 2002]**.**

Les tests de diagnostic agissent au niveau composant/interne (et non pas au niveau de la fonction de sécurité) et permettent de détecter les erreurs aléatoires (dues au matériel).

1.4.6.2 Proof Test

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

cas où le diagnostic coverage serait minimum ou insuffisant (si on ne peut pas ou ne sait pas réaliser un test de diagnostic satisfaisant), on pourra augmenter la fréquence du proof test. En augmentant la fréquence du proof test, on vérifiera plus souvent que la fonction de sécurité est bien disponible.

Le proof test est exécuté au niveau du système. C'est un test fonctionnel de la fonction de sécurité hors fonctionnement automatique sans perturbation de process (activité périodique devant être conduite selon une procédure afin de détecter les défauts latents qui empêchent le système de sécurité de remplir sa fonction de sécurité ; le système de sécurité entier doit être testé) [Lamy, 2002].

En règle générale, un proof test a une périodicité beaucoup plut important (intervalle entre test plus grand) qu'un test de diagnostic.

Alors que le test de diagnostic est plutôt une détection interne en fonctionnement. Le proof test permet de détecter les pannes latentes qui n'ont pas été vues par les tests de diagnostic.

1.4.7 Niveau d'intégrité de sécurité (SIL)

Les normes IEC 61508 [IEC 61508, 2002] et IEC 61511 [IEC61511, 2003] 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 le système de protection. Plus le SIL à une valeur élevé, plus la réduction du risque est importante. Par exemple un système de SIL 4 apporte une réduction de risque entre 10000 à 100000 alors qu'un système de SIL 1 comporte un facteur de réduction de risque compris entre 10 à 100 seulement.

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

L'utilisation des niveaux SILs permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel menant aux évènements dangereux identifiés pendant l'analyse de risque [Beugin, 2006]. Les SILs sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances dangereuses uniquement sans tenir compte des défaillances en sécurité ou défaillances sûres.

La qualité requise du SIS s'exprime par le SIL (safety integrity level) et mesure la réduction du risque obtenue par les moyens de prévention fournis par le SIS.

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

Il est important de souligner que le concept de SIL s'applique uniquement à un système instrumenté de sécurité (SIS) dans son intégralité et pas à un composant pris individuellement.

Le SIL est défini, selon l'IEC61508 [IEC61508, 2002], en 04 niveaux (plus le SIL est élevé, plus la disponibilité du système de sécurité est élevée)(Tableau 1.2).

Tableau 1.2-Niveaux d'intégrité de sécurité selon la norme CEI 61508 [IEC61508, 2002]

SIL	Probabilité moyenne de défaillance à la sollicitation (PFDavg)	Réduction de risque RR
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$10 \leq RR < 100$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$100 \leq RR < 1000$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$1000 \leq RR < 10000$
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$10000 \leq RR < 10000$

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

$$PFD_{SYS} = PFD_C + PFD_U + PFD_A \quad (1.1)$$

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

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

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

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

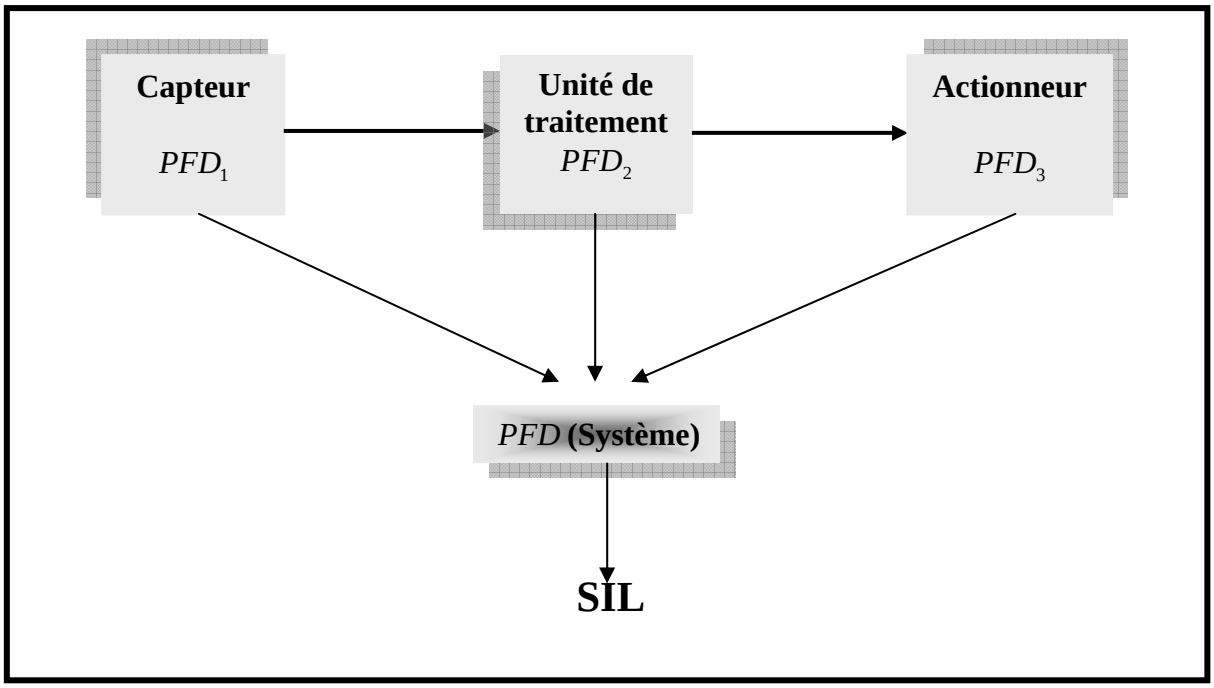

Figure 1.8-Méthode de calcul de SIL

1.4.7.1 Paramètres Influant sur le calcul de SIL

Après avoir déterminé les exigences du SIS à travers la classe SIL, il faut passer aux choses concrètes, c'est-à-dire définir le SIS, et plus précisément les solutions technologiques aptes à satisfaire au besoin.

La chaîne de sécurité doit remplir sa mission lors de la sollicitation (aspect sécurité), tout en évitant de provoquer des déclenchements intempestifs (aspect disponibilité de la production).
La qualité de la chaîne de sécurité dépend de plusieurs critères :

- Taux de défaillance (qualité des composants, redondances).

- Facteur de mode commun ou facteur ß (précautions d'installation, hétérogénéité et indépendance).

- Taux de Couverture (qualité et étendue des tests automatiques) et mode de traitement des défaillances détectées. Ce dernier aspect n'est pas évoqué dans les normes alors qu'il revêt une grande importance dans la bonne prise en compte des modes de fonctionnement des éléments du SIS.

- Temps moyen de réparation (remise en service après défaillance non déclenchante), avec ses corollaires que sont l'organisation de la maintenance et la gestion des pièces de rechange.

- Périodicité des tests manuels (organisation des tests, portée des tests).

1.4.7.2 Méthodes de détermination de SIL

La détermination du SIL d'un SIS peut s'obtenir par différentes méthodes :

- **Méthodes qualitatives** : Il s'agit de méthodes qui permettent de déterminer le niveau de SIL à partir de la connaissance des risques associés au procédé, la méthode graphe de risque par exemple.

- **Méthodes semi quantitatives** : La méthode la plus répandue est la matrice de risque. Cette matrice donne le niveau de SIL en fonction de la gravité de risque et de sa fréquence d'occurrence.

- **Méthodes quantitatives** : Il s'agit des méthodes qui permettent de calculer le PFD des SIS à partir des probabilités de défaillances de leurs composants. Les méthodes les plus répandues sont :

  - Les équations simplifiées [ISA-S84.01, 1996 ; Summers, 2000].
  - Les arbres de défaillances [Beckman, 2001; Goble et Cheddie, 1998].
  - Les chaînes de Markov [Goble et Cheddie, 1998; Bukowski et Goble ,1995; Zhang et al, 2003; Bukowski, 2005] : Cette technique est souvent utilisée en sûreté de fonctionnement lorsque l'on souhaite modéliser un système avec des composants à taux de défaillance constant et réparable. Il permet ainsi de faire une analyse dynamique du système.

Conclusion

Les systèmes instrumentés de sécurité sont utilisés pour détecter des situations dangereuses et diminuer leurs conséquences pour atteindre des niveaux de risques tolérables. La norme générique CEI 61508 et sa norme fille CEI 61511 pour le secteur des procédés continus deviennent les normes de référence pour la spécification et la conception de ce type de systèmes (SIS).

Les niveaux d'intégrité de sécurité issus de la norme sont des objectifs de sécurité utiles à l'évaluation des risques. Ils donnent une mesure de la réduction du risque obtenue par les moyens de protection fournis par le SIS. La détermination du niveau d'intégrité de sécurité dépend du calcul de la probabilité de défaillance sur demande.

Les méthodes usuelles de calcul du *PFDavg* des SIS sont des méthodes probabilistes. Ces méthodes issues des études traditionnelles de sûreté de fonctionnement où les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation, etc.) peuvent être connues avec précision et validées par le retour d'expérience.

Parmi ces méthodes, la méthode des graphes de Markov conventionnels qui est utilisée pour analyser et évaluer la sûreté de fonctionnement des systèmes réparables. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et à chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une réparation. L'objectif du chapitre suivant est la détermination du PFDavg des SIS par l'approche Markovienne classique.

Chapitre 2

Évaluation de l'Indisponibilité des Systèmes Instrumentés de Sécurité par le modèle Markovien

Introduction

Pour l'évaluation du niveau d'intégrité de sécurité (SIL) en par référence à la norme CEI61508, il est nécessaire de calculer la probabilité de défaillance à la demande de la fonction de sécurité (SIF : Safety Instrumented Function) liée au système instrumenté de sécurité (SIS).

Le deuxième chapitre est consacré à la détermination des PFD_{avg} des différentes architectures en utilisant la méthode de graphe de Markov conventionnel.

Dans la norme CEI61508, les différentes architectures de SIS étudiées sont composées de canaux. Chacun d'eux peut avoir aussi bien des défaillances détectables par test de diagnostic de taux λ_{DD}, que des défaillances non détectables de taux λ_{DU}. Ces deux taux sont considérés comme constants. Tout composant ayant subi une défaillance détectable mis en réparation après une durée égale au $MTTR$ et les défaillances de second type ne sont détectées que lors du prochain test périodique avec un temps de couverture donné et mis en réparation.

Rappelons que le composant après la réparation est considéré comme neuf et le nombre de réparateurs est suffisant.

– Nous nous plaçons dans le cas où le SIS est faiblement sollicité (moins d'une fois / an), d'où le besoin d'évaluer le *PFD* et non pas le *PFH* (probabilité de défaillance par heure). Dans ce cas, le *PFD* instantané est assimilé à une indisponibilité instantanée.

– Nous nous intéressons à l'évaluation du *PFDavg* du *SIS*. C'est pourquoi nous utilisons les taux de défaillance λ_{D} des composants qui désignent les taux de défaillance dangereuse non détectés λ_{DU} et les taux de défaillance détectés λ_{DD}.

Ces défaillances dangereuses font passer le système de l'état normal à l'état de défaillance dangereux.

–Les tests de diagnostic des composants soient réalisés simultanément.

2.1 Évaluation de sûreté de fonctionnement des systèmes par chaîne de Markov

L'étude de la fiabilité des systèmes est une composante majeure de la maîtrise des processus en entreprise. De nombreuses méthodes d'analyse quantitative existent et sont parfaitement référencées [Bajenesco ,1978 ; Bajenesco ,1980 ; Pages et Gondran, 1980 ; Villemeur, 1980]. Chaque outil présente des intérêts en termes de pouvoir, de modélisation, et de capacité de formalisation des processus dysfonctionnels avec plus ou moins de simplicité et d'ergonomie.

La théorie des processus de Markov fournit un outil efficace pour le calcul des paramètres de sûreté de fonctionnement des systèmes en fonction des paramètres de sûreté de fonctionnement des composants élémentaires utilisés. Cette théorie est particulièrement adaptée à l'étude des systèmes redondants réparables modélisables par des processus Markoviens et les systèmes dont les taux de défaillance varient au cours du temps.

2.1.1 Processus de Markov, espace des états

Un processus stochastique est composé de défaillances aléatoires d'un composant, du point de vue des phénomènes physiques.

Un processus stochastique est appelé processus de Markov si la distribution de probabilité est exclusivement déterminée par la valeur présente, et non par l'enchaînement des valeurs passées.

Sur un processus markovien, la probabilité pour qu'à l'instant $t + dt$, le système soit dans l'état i ne dépend que de l'état à l'instant t et vaut :

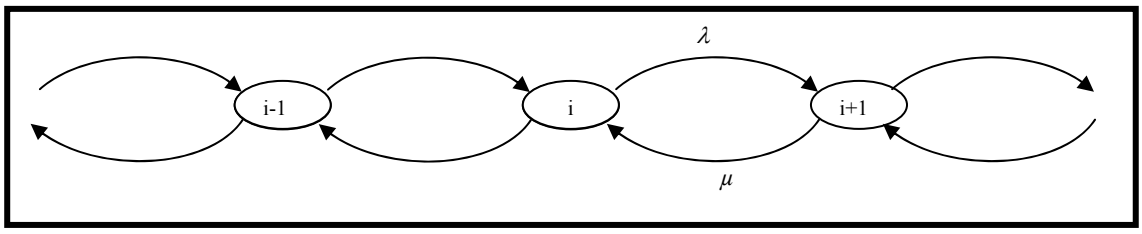

Figure 2.1 - Processus markovien

$$P_i(t+dt) = P_{i+1}(t)\,\lambda_{i+1,i}(t)dt + P_i(t)[1 - \lambda_{i,i-1}(t)dt]\,[1 - \mu_{i,i+1}(t)dt] + P_{i-1}(t)\mu_{i-1,i}\,dt \quad (2.1)$$

Soit :

$$P'_i(t) = \lambda_{i+1,i}(t)\,P_{i+1}(t) - [\,\lambda_{i,i-1}(t) + \mu_{i,i+1}(t)]\,P_i(t) + \mu_{i-1,i}(t)\,P_{i-1}(t) \quad (2.2)$$

Avec les équations aux limites :

$$P'_n(t) = -\lambda_{n,n-1}(t)\, P_n(t) + \mu_{n-1,n}(t)\, P_{n-1}(t) \quad (2.3)$$

$$P'o(t) = \lambda_{1,o}(t)\, P_1(t) - \mu_{o,1}(t)\, P_o(t) \quad (2.4)$$

Et sous forme matricielle :

$$[P'(t)] = [\lambda(t),=\mu(t)]\ [P(t)] \quad avec \quad [P(t)] = \begin{pmatrix} P_n(t) \\ .... \\ P_o(t) \end{pmatrix} \quad (2.5)$$

Sachant que :

$$\Sigma_i P_i(t) = 1 \text{ et } Pn(o) = 1 \quad (2.6)$$

Pour une redondance parallèle.

Pour *n* dispositifs identiques en redondance active, avec un seul réparateur :

$$\lambda_{i,i-1} = i\,\lambda \text{ et } \mu_{i,i+1} = \mu \quad (2.7)$$

Et avec *r* réparateurs :

$$\mu_{i,\,i+1} = (n-i)\mu \ \ pour \ \ (n-i) < r \text{ ou } r\mu \text{ pour } n-i \geq r \quad (2.8)$$

La résolution de l'équation peut être numérique (Runge Kutta), par transformée de Laplace, par exponentiation de matrice :

$$[P(t)] = [P(o)]\, e^{-[\lambda,\mu]t} \quad (2.9)$$

2.1.2- Système à deux dispositifs parallèles

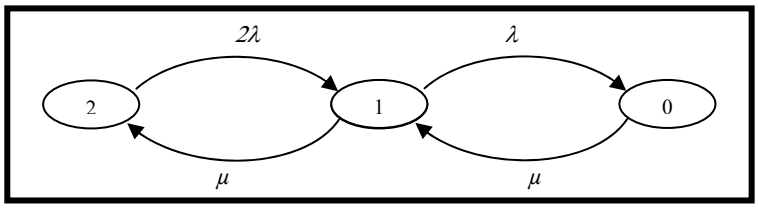

Figure 2.2 - Deux dispositifs et un seul réparateur

Avec un seul réparateur et des taux constants, la chaîne conduit à :

$$[P'] = \begin{pmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & \mu \\ 0 & \lambda & -\mu \end{pmatrix} [P(t)] \quad (2.10)$$

En régime permanent $[P'] = 0$ et compte tenu du fait que :

$$P_{2\infty} + P_{1\infty} + P_{o\infty} = 1$$

(2.11)

Il vient :

$$P_o = 2\lambda^2 / (2\lambda^2 + 2\lambda\mu + \mu^2) \quad (2.12)$$

Cette probabilité représente l'indisponibilité moyenne du système.

La disponibilité vaut :

$$A = 1 - P_o = (2\lambda\mu + \mu^2)/(2\lambda^2 + 2\lambda\mu + \mu^2) \quad (2.13)$$

Et si $\lambda << \mu$:

$$A \approx 1 - 2\lambda^2/\mu^2 \quad (2.14)$$

L'indisponibilité $1 - A$ vaut :

$$A' \approx 2\lambda^2/\mu^2 \quad (2.15)$$

Pour calculer la fiabilité, on exclut la possibilité de réparation lorsque les deux dispositifs sont en panne (présence d'un état absorbant).

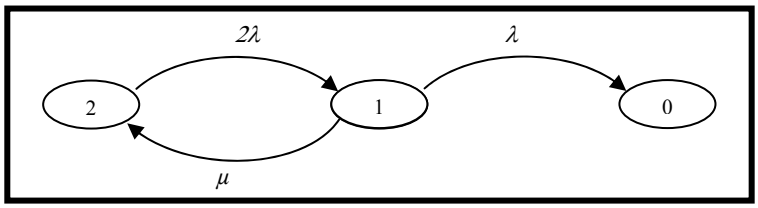

Figure 2.3 – Fiabilité

$$[P'] = \begin{pmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{pmatrix} [P(t)] \quad (2.16)$$

Et par transformation de Laplace :

$$s\,P_2(s) - 1 = -2\lambda\,P_2(s) + \mu$$

$$s\,P_1(s) = 2\lambda P_2(s) - (\lambda+\mu)$$

$$s\,P_o(s) = \lambda P_1(s)$$

D'où :

$$P_o(s) = 2\lambda^2/s[s^2 + (3\lambda + \mu)s + 2\lambda^2]$$

Soient λ_1 et λ_2 les racines du dénominateur :

$$R(t) = 1 - P_o(t) = [\ \lambda_1 e^{\lambda_2 t} - \lambda 2\ e^{\lambda_1 t}\ ] / (\lambda_1 - \lambda_2) \quad (2.17)$$

$$MTTF = (-\lambda_1/\lambda_2 + \lambda_2/\lambda_1)/(\lambda_1 - \lambda_2) = -(\lambda_1 + \lambda_2)/\lambda_1\lambda_2$$

$$MTTF = +(3\lambda + \mu)/2\lambda^2 \quad (2.18)$$

En général $\lambda << \mu$ et $MTTR \approx \mu/ 2\lambda^2$ (2.19)

Avec deux réparateurs ou plus, il vient :

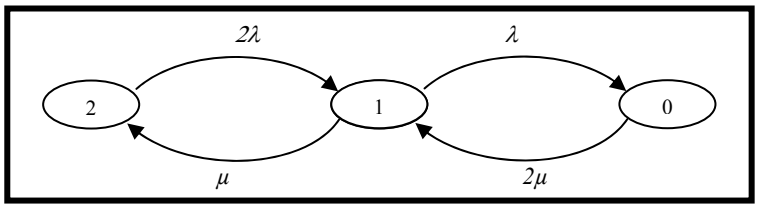

Figure 2.4 - Deux dispositifs et deux réparateurs

$$A = (\mu^2 + 2\mu\lambda)/(\lambda + \mu)^2 = 1 - (1-\mu/(\lambda+\mu))^2 \quad (2.20)$$

$$A \approx 1 - \lambda^2/\mu^2 \quad (2.21)$$

Lorsque la panne n'est détectée que si tout le système est défaillant, il vient :

$$A = 3\mu/ (2\lambda + 3\mu) = 1 - 2\lambda/ (2\lambda + 3\mu) \approx 1 - 2\lambda / (3\mu) \quad (2.22)$$

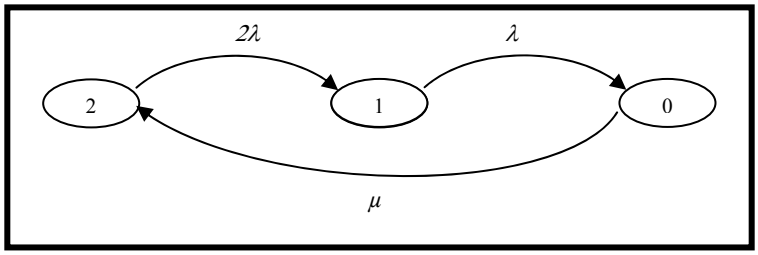

Figure 2.5 - Détection de la panne totale

Lorsque la détection des pannes n'est pas parfaite, avec un taux de non-détection ϖ *(= 1-α)* on obtient pour un ensemble à deux sous-systèmes un nouveau diagramme. L'état supplémentaire 1' correspond à une défaillance existante mais non détectée. L'indisponibilité vaut alors :

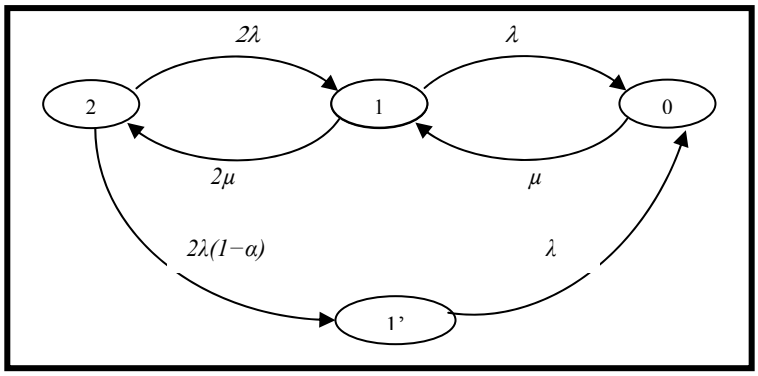

Figure 2.6- Détection imparfaite de la panne

$$A' = 2\lambda\,[\lambda + \mu\varpi\,]\,/\mu^2(1 + 2\varpi\,) \tag{2.23}$$

Si $\lambda << \mu$ et si, de plus, $\varpi << 1$

$$A' \approx 2\lambda\,(\lambda + \mu\varpi\,)/\mu^2 \tag{2.24}$$

Au lieu de $2\lambda^2/\mu^2$ si $\varpi << \lambda/\mu$

2.1.3 Systèmes à deux dispositifs série

Avec deux dispositifs identiques et deux réparateurs la chaîne conduit à :

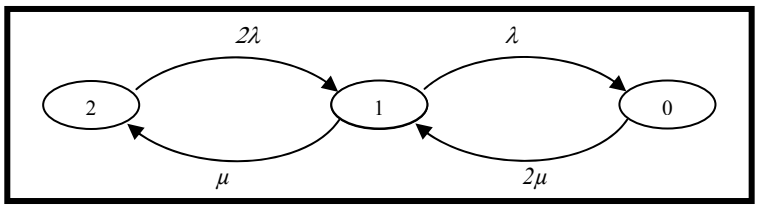

Figure 2.7- Disponibilité série

$$[P'(t)] = \begin{pmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 2\,\mu \\ 0 & \lambda & -2\,\mu \end{pmatrix} [P(t)] \tag{2.25}$$

En régime stationnaire :

$P_o = \lambda^2/(\lambda + \mu)^2$

$P_1 = 2\lambda\mu/(\lambda + \mu)^2$

Et la disponibilité moyenne vaut :

$$P_2 = A = 1 - P_o - P_1 = \mu^2/(\lambda+\mu)^2 \approx 1 - 2\lambda/\mu \quad (2.26)$$

Ce qui se généralise à des composants en série :

$$A = \Sigma A_i \quad (2.27)$$

A_i est la disponibilité d'un seul ensemble réparable

La disponibilité diminue quand le nombre de composants augmente.

2.1.4 Système à redondance majoritaire

Il ne présente d'intérêt que si la panne d'un sous-système est aussitôt détectée puis réparée. Pour un système 2/3, il vient :

$$A = A_1^2 (3 - 2A_1) \quad (2.28)$$

2.1.5 Système à redondance passive

Là encore tout dépend du nombre de réparateurs mais surtout de la fiabilité du commutateur qui doit être grande. En la supposant parfaite, pour un système à deux dispositifs :

$$A' = \lambda^2 / (\lambda^2 + \mu\lambda + \mu^2) \approx \lambda^2/\mu^2 \text{ si } \lambda_o = 0 \quad (2.29)$$

Avec un seul réparateur et :

$$A' \approx \lambda^2 /2\ \mu^2 \quad (2.30)$$

Avec deux réparateurs.

La modélisation des systèmes dynamiques par des chaînes de Markov présente bien des avantages dont notamment la possibilité d'effectuer des traitements plus précis et plus rapides que par simulation de Monte-Carlo en se ramenant à la résolution d'un système d'équations différentielles linéaires du premier ordre. Elle présente cependant deux inconvénients :

– L'emploi exclusif des taux de transition constants (loi exponentielle).

– L'explosion combinatoire des états (2^n états pour un système de n éléments à 2 états).

Il s'agit donc d'utiliser les chaînes de Markov pour évaluer les performances des SIS étudiés. Rappelons simplement que dans la norme CEI 61508 [IEC61508, 2002], différentes configurations des systèmes instrumentés de sécurité étudiés sont composées de canaux. Chaque canal peut avoir plusieurs types de configuration architecturale (architecture 1oo1 : un parmi un, 1oo2 : au moins un

parmi deux, …). Un canal peut avoir, des défaillances détectables par les tests de diagnostic, avec taux λ_{DD} et des défaillances non détectées avec un taux λ_{DU} .

2.2 Détermination du PFD de l'architecture 1oo1 par le modèle Markovien conventionnel

Cette architecture se compose d'un seul canal, il faut une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande [IEC61061, 1998].

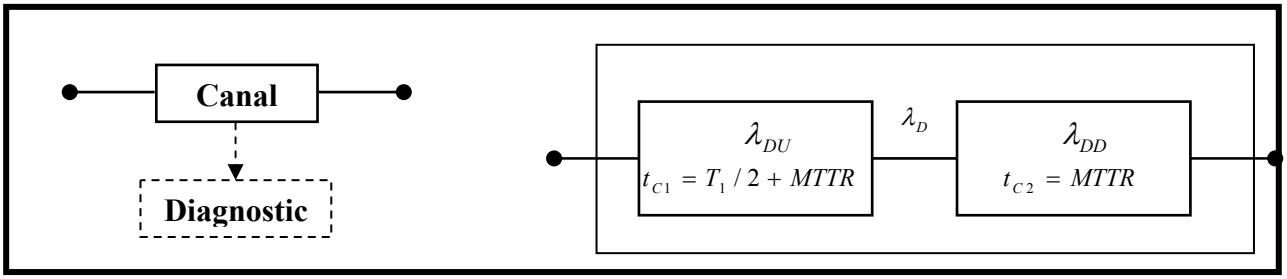

Figure 2.8-Diagrammes blocs physique et de fiabilité 1oo1

La figure(Figure 2.8) montre que la norme considère que le canal se compose de deux composants en série, au sens fiabiliste du terme, ayant respectivement pour taux de défaillance dangereuse non détecté λ_{DU} et le taux de défaillance détecté λ_{DD}.

2.2.1 Détermination du taux de réparation μ_{DU}

Si le taux de réparation lors une défaillance détectée $\mu_{DD} = 1/MTTR$ est connu, le second pour une défaillance dangereuse non détectée μ_{DU} doit être déterminé. On suppose t_{DU} la valeur moyenne de l'instant d'occurrence de défaillance dangereuse non détectée dans l'intervalle [0, T_1]

t_{C1} : La durée moyenne d'indisponibilité due à une défaillance non détectée d'un canal [Zhang et al, 2003].

Donc :

$$t_{C1} = T_1 - t_{DU} + MTTR \tag{2.31}$$

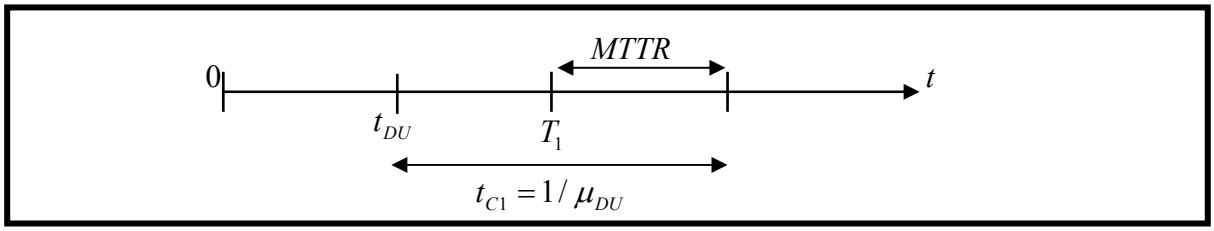

Figure 2.9-Processus d'occurrence d'une défaillance non détectée sur [0, T_1]

On obtient :

$$\mu_{DU} = \frac{1}{\frac{T_1}{2} + MTTR} \tag{2.32}$$

2.2.2 Modèle markovien 1oo1

Le comportement du système au cours d'une mission de durée donnée est décrit par un modèle Markovien comme l'indique la figure (figure 2.10)

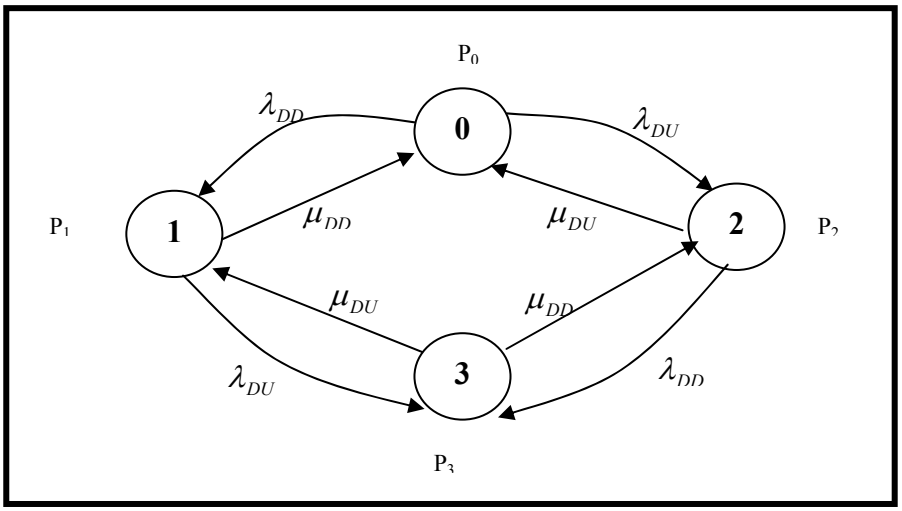

Figure 2.10-Graphe de Markov 1oo1 [Zhang et al, 2003]

Etat de système	Composant 1	Composant 2
0	0	0
1	0	1
2	1	0
3	1	1

0 : état de fonctionnement 1 : état de panne

2.2.3 Détermination de la disponibilité de l'architecture 1oo1

Les équations différentielles du système

$$\begin{cases} P_0'(t) = -(\lambda_{DD} + \lambda_{DU})P_0(t) + \mu_{DD}P_1(t) + \mu_{DU}P_2(t) \\ P_1'(t) = \lambda_{DD}P_0(t) - (\lambda_{DU} + \mu_{DD})P_1(t) + \mu_{DU}P_3(t) \\ P_2'(t) = \lambda_{DU}P_0(t) - (\lambda_{DD} + \mu_{DU})P_2(t) + \mu_{DD}P_3(t) \\ P_3'(t) = \lambda_{DU}P_1(t) + \lambda_{DD}P_2(t) - (\mu_{DD} + \mu_{DU})P_3(t) \end{cases} \tag{2.33}$$

Avec $P' = M.P$ est l'équation d'état

On construit facilement la matrice *M* par interprétation de ce graphe de Markov :

$$M = \begin{bmatrix} -(\lambda_{DD} + \lambda_{DU}) & \mu_{DD} & \mu_{DU} & 0 \\ \lambda_{DD} & -(\lambda_{DU} + \mu_{DD}) & 0 & \mu_{DU} \\ \lambda_{DU} & 0 & -(\lambda_{DD} + \mu_{DU}) & \mu_{DD} \\ 0 & \lambda_{DU} & \lambda_{DD} & -(\mu_{DD} + \mu_{DU}) \end{bmatrix} \quad (2.34)$$

La résolution du système 2.33, connaissant la distribution initiale $P(0) = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}$ peut être effectuée par la transformation de LAPLACE et la disponibilité de système :

$$A(t) = \frac{1}{(\lambda_D + \mu_D)(\lambda_U + \mu_U)} \begin{bmatrix} \mu_D \mu_U + \lambda_D \mu_U \exp -(\lambda_D + \mu_D)t + \lambda_U \mu_D \exp -(\lambda_U + \mu_U)t \\ + \lambda_D \lambda_U \exp -(\lambda_D + \lambda_U + \mu_D + \mu_U)t \end{bmatrix} \quad (2.35)$$

2.2.4 Détermination de l'indisponibilité moyenne PFD_{avg} du canal

Pour un seul canal la probabilité moyenne de défaillance à la demande est:

$$PFD_{avg} = \frac{\lambda_{DU}(\frac{T_1}{2} + MTTR) + \lambda_{DD} MTTR}{\lambda_{DU}(\frac{T_1}{2} + MTTR) + \lambda_{DD} MTTR + 1} \quad (2.36)$$

$$\lambda_{DU}(\frac{T_1}{2} + \text{MTTR}) + \lambda_{DD}\text{MTTR} << 1 \quad (2.37)$$

$$PFD_{avg} = \lambda_D \left[\frac{\lambda_{DU}}{\lambda_D}(T_1/2 + MTTR) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right] \quad (2.38)$$

Pour l'architecture 1oo1:

$$PFD_{avg} = \lambda_D t_{CE} \quad (2.39)$$

2.3 Architecture 1oo2

Cette architecture se compose de deux canaux identiques fonctionnant en redondance active, il faut donc que ces deux canaux subissent chacun une défaillance dangereuse pour que le système n'assure pas se fonction de sécurité en cas de demande [IEC61061, 1998].

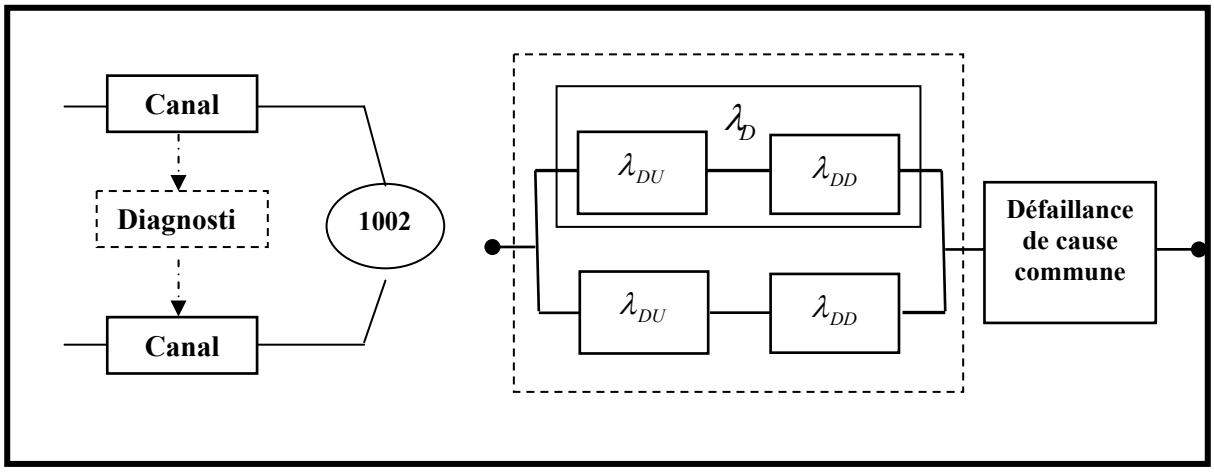

Figure 2.11-Diagrammes blocs physique et de fiabilité 1oo2

2.3.1 Détermination du taux de réparation $\mu_{DU}^{'}$

Appelons t_{C1} la durée moyenne d'indisponibilité due à une défaillance non détectée d'un canal, et t'_{DU} la valeur moyenne de l'instant d'occurrence de défaillance dangereuse non détectée dans l'intervalle *[0, T_1]* dans le système.

On utilise le même principe pour déterminer t'_{DU} :

$$t'_{DU} = \frac{\int_0^{T_1} t.f(t).dt}{\int_0^{T_1} f(t).dt} \tag{2.40}$$

On trouve $\mu'_{DU} = \frac{1}{t_{c1}} = \frac{1}{\frac{T_1}{3} + MTTR}$ (2.41)

2.3.2 Modèle markovien du 1oo2

Le graphe de Markov est :

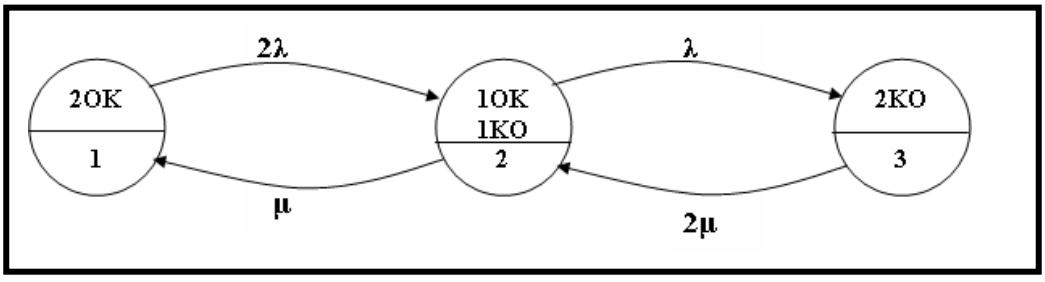

Figure 2.12-Graphe de Markov 1oo2

2.3.3 Détermination de la disponibilité de l'architecture 1oo2

Les équations différentielles du système :

$$\begin{cases} P_1'(t) = -2\lambda P_1(t) + \mu P_2(t) \\ P_2'(t) = 2\lambda P_1(t) - (\lambda + \mu) P_2(t) + 2\mu P_3(t) \\ P_3'(t) = \lambda P_2(t) - 2\mu P_3(t) \end{cases} \tag{2.42}$$

Le système (2.42) permet d'écrire :

$$\begin{bmatrix} P_1'(t) & P_2'(t) & P_3'(t) \end{bmatrix} = \begin{bmatrix} P_1(t) & P_2(t) & P_3(t) \end{bmatrix} \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 2\mu & -2\mu \end{bmatrix} \tag{2.43}$$

La relation (2.43) permet de calculer la disponibilité *A(t)* de l'architecture 1002 avec :

$$A(t) = P_1(t) + P_2(t) \tag{2.44}$$

Par la transformée de Laplace

$$A(t) = \frac{\mu(2\lambda+\mu)}{(\lambda+\mu)^2} + \frac{2\lambda^2}{(\lambda+\mu)^2} e^{-(\lambda+\mu)t} + \frac{\lambda^2}{(\lambda+\mu)^2} e^{-2(\lambda+\mu)t} \tag{2.45}$$

Alors:

$$A(\infty) = \frac{2\lambda\mu + \mu^2}{(\lambda+\mu)^2} \tag{2.46}$$

La durée moyenne d'indisponibilité du système t_{GE} est donnée par :

$$t_{GE} = MDT = \frac{1}{2\mu} = \frac{1}{2}\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right] \tag{2.47}$$

$$t_{GE} = \frac{1}{2} t_{CE} \tag{2.48}$$

2.3.4 Détermination de l'indisponibilité moyenne PFD_{avg} du 1oo2

Pour déterminer la PFD_{avg} de cette architecture nous avons :

$$PFD_{avg} = P_3 + P_{CC} \tag{2.49}$$

Avec P_{CC} est La probabilité de défaillance de cause commune, alors :

$$PFD_{avg} = \frac{\lambda^2}{(\lambda^2 + \mu^2)} + P_{CC} \approx \frac{\lambda^2}{\mu^2} + P_{CC} = \lambda^2 t_{CE}{}^2 + P_{CC} \tag{2.50}$$

$\beta_D \lambda_{DD} MTTR$ est Probabilité de défaillance de cause commune détectée.

$\beta\lambda_{DU}(\frac{T_1}{2} + MTTR)$:la Probabilité de défaillance de cause commune non détectée.

$$PFD_{avg} = 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 . t_{CE} . t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}(\frac{T_1}{2} + MTTR) \tag{2.51}$$

2.4 Architecture 2oo3

Cette architecture comprend trois canaux connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie, de telle sorte que l'état de sortie n'est pas modifié lorsqu'un seul canal donne un résultat différent de deux autres canaux [IEC61061, 1998].

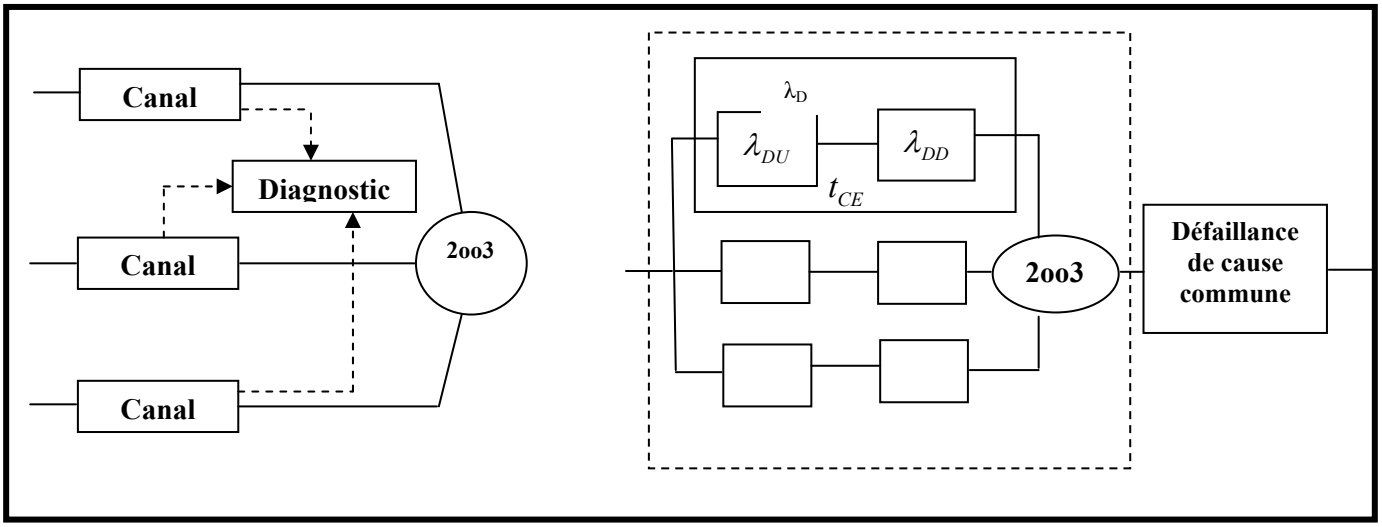

Figure 2.13-Diagrammes blocs physique et de fiabilité 2oo3

2.4.1 Modèle markovien 2oo3

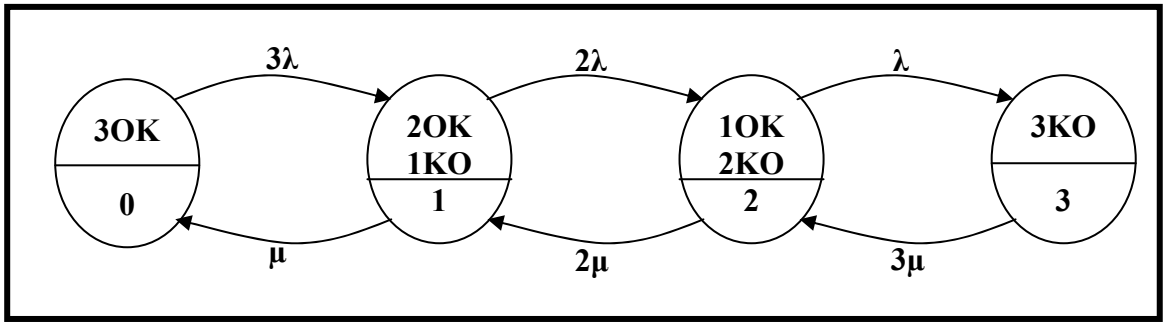

Figure 2.14-Graphe de Markov 2oo3

2.4.2 Détermination de la disponibilité de l'architecture 2oo3

Les équations différentielles du système :

$$\begin{cases} P_0'(t) = -3\lambda P_0(t) + \mu P_1(t) \\ P_1'(t) = 3\lambda P_0(t) - (2\lambda + \mu) P_1(t) + 2\mu P_2(t) \\ P_2'(t) = 2\lambda P_1(t) - (\lambda + 2\mu) P_2(t) + 3\mu P_3(t) \\ P_3'(t) = \lambda P_2(t) - 3\mu P_3(t) \end{cases} \tag{2.52}$$

Avec une méthode analogue à celle employée avec l'architecture 1002 on obtient alors :

$$A(\infty) = \frac{\mu^3 + 3\lambda\mu^2}{(\lambda + \mu)^3} \tag{2.53}$$

2.4.3 Détermination de la durée moyenne globale t_{GE} d'indisponibilité pour 2oo3

L'indisponibilité $\overline{A}(\infty)$ s'écrit:

$$\overline{A}(\infty) = 1 - A(\infty) = \frac{\lambda^2(\lambda + 3\mu)}{(\lambda + \mu)^3} \tag{2.54}$$

Et nous avons :

$$MDT = \frac{1 - A(\infty)}{FF} = \frac{\lambda + 3\mu}{6\mu^2} \approx \frac{1}{2\mu} \tag{2.55}$$

Avec : $\mu = \frac{1}{t_{CE}}$ / $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$ (2.56)

Et $\lambda << \mu$ Alors :

$$MDT = t_{GE} = \frac{1}{2\mu} = \frac{1}{2}\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right] \quad (2.57)$$

2.4.4 Détermination de l'indisponibilité moyenne PFD_{avg} du 2oo3

Donc on obtient la PFD_{avg} relative à l'architecture 2oo3 :

$$PFD_{avg} = \overline{A}(\infty) + P_{CC} = \frac{\lambda^2(\lambda + 3\mu)}{(\lambda + \mu)^3} + P_{CC} \approx \frac{3\lambda^2}{\mu^2} + P_{CC} \quad (2.58)$$

$$PFD_{avg} = 6\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 . t_{CE} . t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \quad (2.59)$$

2.5 Exemple numérique

Les données numériques utilisées sont : $\lambda_{DD}(1/h)=10^{-5}$, $\lambda_{DU}(1/h)=10^{-6}$, $T_1\ (h)= 4380$ $MTTR(h)=8$, $\beta_D=0.01$, $\beta=0.02$

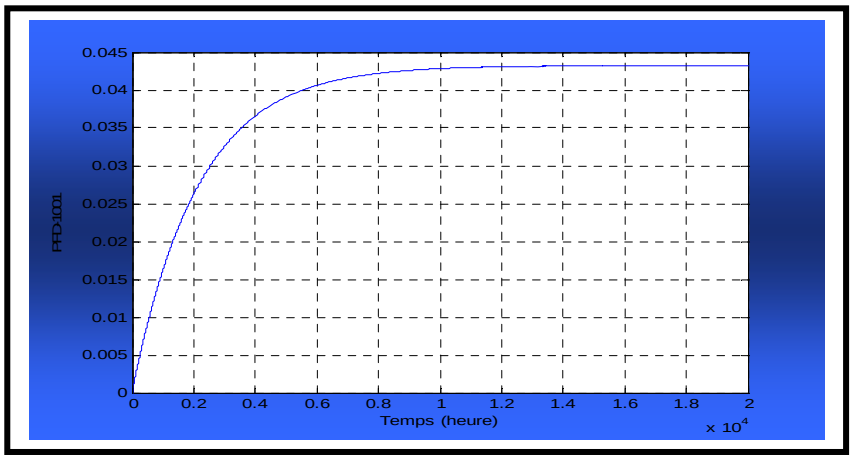

Figure 2.15- Evolution de l'indisponibilité de l'architecture 1oo2 en fonction du temps

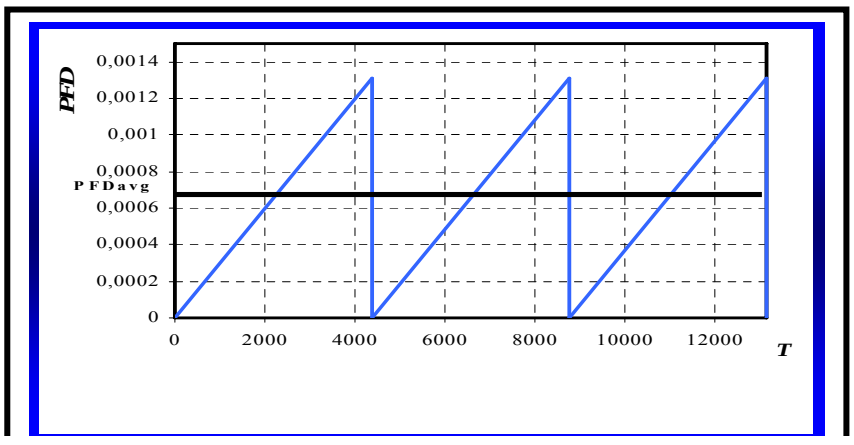

Figure 2.16- Effet des tests périodiques sur l'indisponibilité de l'architecture 1oo1

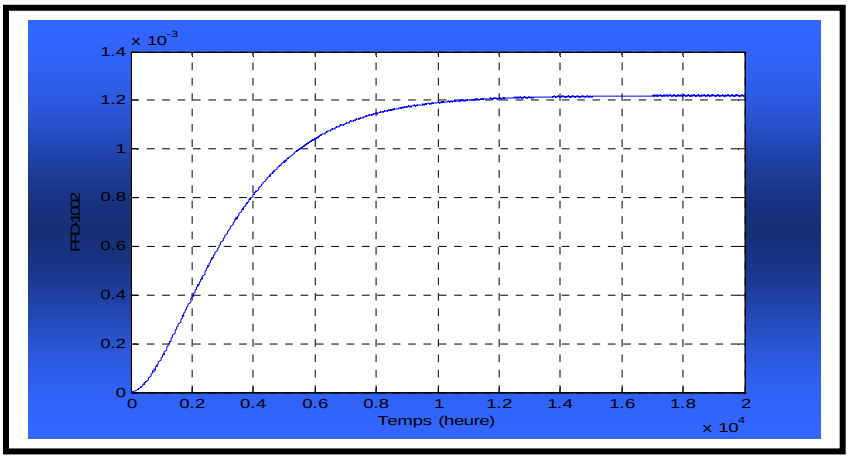

Figure 2.17- Evolution de l'indisponibilité de l'architecture 1oo1en fonction du temps

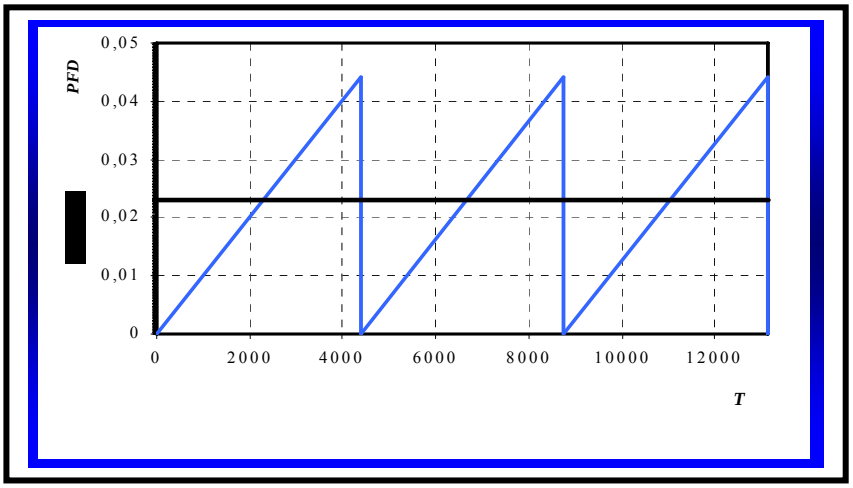

Figure 2.18 Effet des tests périodiques sur l'indisponibilité de l'architecture 1oo2

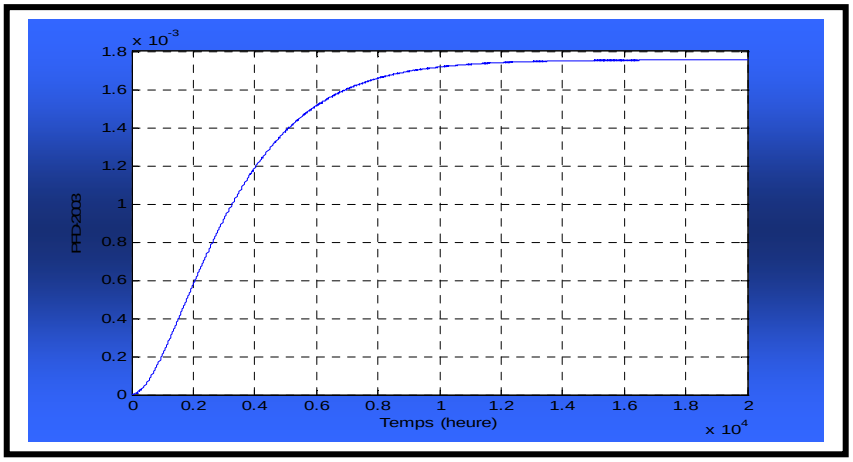

Figure 2.19- Evolution de l'indisponibilité de l'architecture 2oo3 en fonction du temps

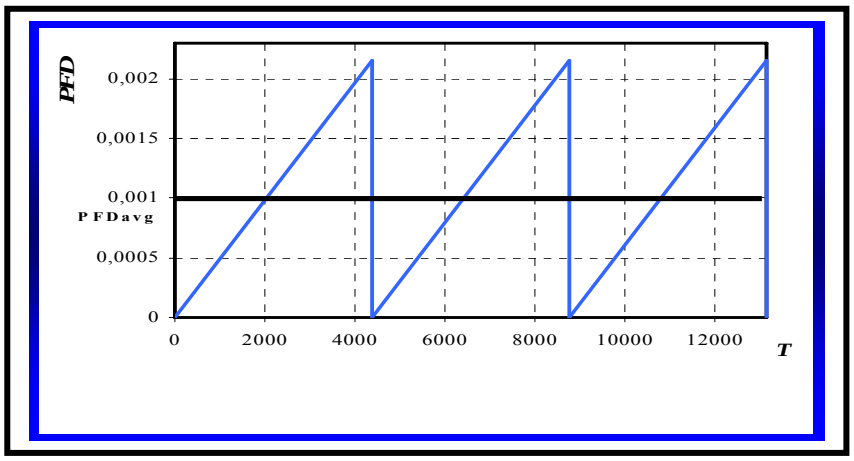

Figure 2.20 Effet des tests périodiques sur l'indisponibilité de l'architecture 2003

Nous avons remarqué dans ces courbes, que les tests périodiques assurent la détection des pannes cachées afin de maintenir la sécurité fonctionnelle prescrite. Les figures 2.16 ; 2.18 et 2.20 montre bien le rétablissement de la disponibilité du système après chaque test périodique et ainsi le niveau de SIL peut être maintenu comme le préconise la norme. La probabilité de défaillance dangereuse PFD(t) est un paramètre qui évolue dans le temps et sa valeur moyenne est donnée par PFDavg qui est représentée par la ligne horizontale dans les figures précédentes.

Si on compare les valeurs des PFDavg de l'architecture 1oo2 et 2oo3, nous remarquons aussi que Les valeurs de PFDavg de 2oo3 sont élevées par rapport à celles des architectures 1oo2. A travers cette comparaison, On conclure que l'architecture 1oo2 est plus fiable que 2oo3 et 1oo1.

Conclusion

Dans ce chapitre nous avons utilisé la méthode de graphes de Markov pour montrer comment et sous quelles hypothèses on pouvait obtenir les formules analytiques proposées dans la norme.

Les systèmes instrumentés de sécurité sont des dispositifs sur lesquels nous n'avons pas forcément de retour de données en quantité. Ceci est d'autant plus vrai lorsque ces dispositifs sont faiblement sollicités, et pour lesquels le retour d'expérience est naturellement faible. De ce fait, la précision des paramètres caractéristiques des ces systèmes est soumise à questionnement.

Dans le troisième chapitre, on s'intéresse à l'utilisation de chaînes de Markov floues, car c'est probablement le modèle le plus fin pour l'étude des paramètres de sureté de fonctionnement.

Chapitre 3

Approche Markovienne Floue pour l'Evaluation de l'Indisponibilité des systèmes instrumentés de sécurité

Introduction

Pour étudier la sûreté de fonctionnement des SIS, nous disposons d'informations qui sont généralement imparfaites. Plusieurs théories ont été développées pour permettre la modélisation et la manipulation de ces imperfections (incertitudes et imprécisions).

Nous présentons dans ce chapitre, le concept de base de sous-ensemble flou. L'utilisation de ce concept permet l'étude des systèmes Markoviens dont les états ne sont pas définis d'une manière précise. Dans la littérature, nous trouvons deux types de chaînes de Markov floues, le premier type est les chaînes de Markov à états flous et non-flous et probabilités de transitions singulières, le deuxième est les chaînes de Markov à états non-flous et probabilités de transition floues. Cette dernière approche est celle que nous avons utilisée pour l'évaluation de l'indisponibilité des systèmes instrumentés de la sécurité à taux de défaillance et de réparation imprécis.

3.1 Représentation des connaissances imparfaites

Dans les études de fiabilité des systèmes, les probabilités sont souvent considérées comme précises et parfaitement déterminables. Il est également supposé que toute l'information sur le comportement de la fiabilité du système et de ses composants est disponible. Cette complétude suppose deux conditions essentielles [Utkin et Coolen ,2007] :

-Toutes les probabilités ou les distributions de probabilités sont parfaitement connues.

-Les composants du système sont indépendants, c'est-à-dire que toutes les variables aléatoires décrivant la fiabilité des composants sont indépendantes ou, à défaut, leur dépendance est connue avec précision.

Utkin [Utkin et Coolen ,2007] précise que la première condition est rarement remplie et préconise de traiter ce problème par les intervalles de probabilités [Kozine et Utkin, 2002]. Toutefois, il faut considérer que l'utilisation des probabilités imprécises sous forme d'intervalles n'est qu'une des multiples façons de traiter le problème d'imprécision dans la connaissance des probabilités. En effet, d'autres auteurs ont considéré le problème de précision à l'aide de densités de probabilités [Coit et al, 2004], d'enveloppes de probabilités [Berleant et Zhang, 2004], de probabilités imprécises [Coolen et Utkin, 2007], de nombres flous [Cai, 1996 ; Tanaka et al, 1983; Singer, 1990; Sallak et al, 2008], de densité de possibilités [Brini et al, 2006] ou de fonctions de croyance [Guo, 2004].

3.1.1 Théorie des ensembles flous

Les ensembles flous (ou parties floues) ont été introduits afin de modéliser la représentation humaine des connaissances, et ainsi améliorer les performances des systèmes de décision qui utilisent cette modélisation.

Les ensembles flous sont utilisés soit pour modéliser l'incertitude et l'imprécision, soit pour représenter des informations précises sous forme lexicale assimilable par un système expert.

3.1.1.1 Définitions

Dans un ensemble de référence E, un ensemble flou de ce référentiel E est caractérisé par une fonction d'appartenance μ de E dans l'intervalle des nombres réels $[0, 1]$ (degré d'appartenance qui est l'extension de la fonction caractéristique d'un ensemble classique) [Zadeh, 1965] et [Kaufmann, 1972].

En fait un ensemble flou est formellement défini par l'application μ, mais pour se ramener au langage des mathématiques classiques, nous parlerons d'un ensemble flou A, et noterons μ_A sa fonction d'appartenance.

Pour un ensemble flou A d'un référentiel E on donne les définitions suivantes :

Noyau $N(A) = \{x / \mu A(x) = 1\}$ Les éléments «vraiment» dans A.

Support $S(A) = \{x / \mu A(x) \neq 0\}$ Ceux qui y sont à des degrés divers.

Pour un ensemble classique A, noyau et support sont confondus avec A, et sa fonction caractéristique μ n'admet que 0 ou 1 pour valeurs.

a- Ensemble flou trapézoïdal

L'intervalle flou couramment utilisé dans R est décrit par sa fonction d'appartenance. Le plus simple type pour ce qu'il est convenu d'appeler un «intervalle flou» est une représentation trapézoïdale:

On pose $\mu_A(x) =$

$$\begin{cases} 0 \text{ si } x < a - \alpha \text{ ou } b + \beta < x, \text{ (x hors du support de A)} \\ 1 \text{ si } a < x < b, \text{ (x dans le noyau de A)} \\ 1 + (x - a) / \alpha \text{ si } a - \alpha < x < a, \\ 1 - (b - x) / \beta \text{ si } b < x < b + \beta \end{cases} \qquad (3.1)$$

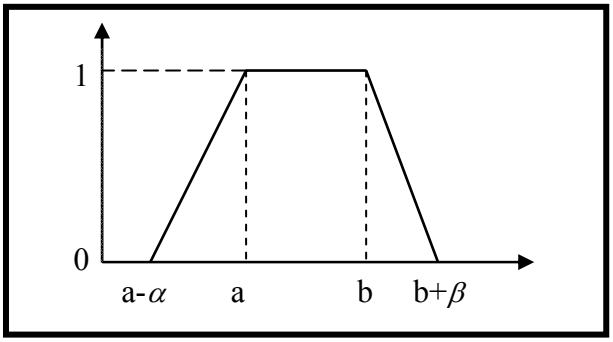

Figure 3.1- Ensemble flou trapézoïdal

b- Nombres flous triangulaires

Ils sont définis par $\mu(x) = 1$ pour $x = m$ (le mode), par 0 si $|x - m| > \sigma$, et enfin par le fait que μ est continue et affine par morceaux. On pourra voir plus loin qu'en définissant les opérations arithmétiques sur des ensembles flous réels, la somme de nombres triangulaires reste un nombre triangulaire.

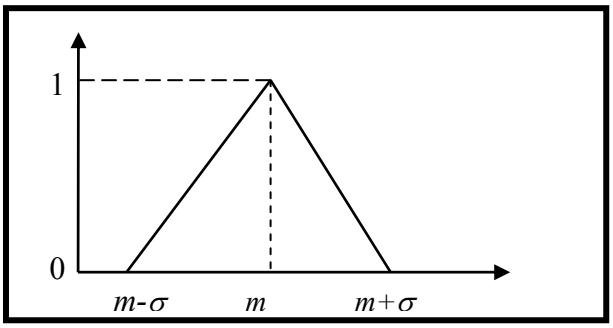

Figure 3.2- Nombres flous triangulaires

3.1.1.2 Principe d'extension de Zadeh

Ce principe énoncé pour toute relation exacte ϕ entre deux ensembles E et F, permet la généralisation au flou d'un certain nombre d'opérations:

Si A est un sous ensemble flou de E, son image B par ϕ Sera définie par :

$$\mu_B(y) = sup\{min\ (\mu_\phi(x, y),\ \mu_A(x) / x \in E\} \quad (3.2)$$

En particulier, si ϕ est une application de E dans F, on peut définir un sous-ensemble flou B de F qui sera l'image par ϕ d'un sous-ensemble flou A de E par $\mu_B(\phi(x)) = \mu_A(x)$ dans le cas où ϕ est injective, et si plusieurs éléments de E admettent la même image alors $\mu_B(y) = sup\{\mu_A(x) / \phi(x) = y\}$, ce qui signifie que chaque fois que y est obtenu, son degré d'appartenance au résultat est le meilleur degré de toutes les façons de l'obtenir et égal à 0 sinon.

3.1.1.3 Opérations simples sur les ensembles flous

a- Inclusion

Par définition, l'inclusion est étendue grâce à : $A < B \Leftrightarrow \mu A \leq \mu B$

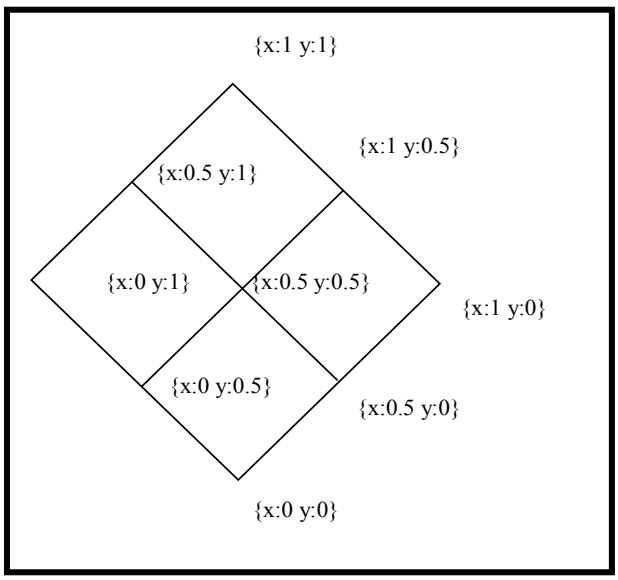

Figure 3.3- Exemple d'inclusion

Exemple des parties floues d'un ensemble fini $E = \{x, y\}$ en se limitant aux seuls degrés d'appartenances 0, 0.5 et 1. Le treillis de tous les ensembles flous avec ces seules valeurs, est formé des 9 parties ci-dessous dont 4 sont exactes (sans la valeur 0.5) et les 5 autres floues.

Cette définition d'inclusion est une simple relation de domination entre les fonctions d'appartenance, on peut facilement vérifier qu'elle généralise l'inclusion des ensembles classiques. Par exemple, on pourrait définir A= «trentaine» et B = «adulte» par des ensemble flous avec A inclus dans B.

b- Complément d'un ensemble flou

Le complémentaire d'un ensemble flou A dans un ensemble de référence E est naturellement défini par la relation (nous utiliserons le symbole de négation ¬) :

$$\mu_{\neg A} = 1 - \mu_A \tag{3.3}$$

Cette opération est involutive, c'est à dire $\neg\neg A = A$, on a d'autre part les propriétés

$$\neg\emptyset = E \text{ et } \neg E = \emptyset. \tag{3.4}$$

Ce n'est cependant pas un complément au sens des treillis car en général :

$$A \cap \neg A \neq \emptyset \text{ et } A \cup \neg A \neq E \tag{3.5}$$

c- Union et intersection

On définit l'union et l'intersection de deux ensembles flous A et B, comme respectivement le plus petit ensemble flou contenant A et B, et le plus grand ensemble flou contenu dans A et dans B d'autre part. En d'autres termes :

$$\mu_{A\cup B} = max(\mu_A, \mu_B) \qquad \mu_{A\cap B} = min(\mu_A, \mu_B) \tag{3.6}$$

Toutes les propriétés de treillis distributif et les relations de Morgan demeurent,

Ainsi l'idempotence : $A \cap A = A$ $\qquad$ $A \cup A = A$ (3.7)

La commutativité : $A \cap B = B \cap A$ $\qquad$ $A \cup B = B \cup A$ (3.8)

L'associativité :

$$A \cap (B \cap C) = (A \cap B) \cap C \qquad A \cup (B \cup C) = (A \cup B) \cup C \tag{3.9}$$

Les distributivités mutuelles

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{3.10}$$

Les relations de Morgan

$$\neg(A \cap B) = (\neg A) \cup (\neg B) \qquad \neg(A \cup B) = (\neg A) \cap (\neg B) \tag{3.11}$$

Et les lois d'absorption

$$A \cup (A \cap B) = A \cap (A \cup B) = A \tag{3.12}$$

3.1.1.4 Notion d'alpha-coupe

Les opérations arithmétiques utilisées pour manipuler les nombres flous requièrent beaucoup de ressources. Kaufman et Gupta [Kaufman et Gupta, 1991] ont montré que ces efforts de calculs sont largement simplifiés par la décomposition des fonctions d'appartenance des nombres flous en α−coupes ($0 \leq \alpha \leq 1$). En effet, si nous considérons un nombre flou A de fonction d'appartenance $\mu_{A(x)}$ (Figure. 3.4), nous pouvons obtenir plusieurs intervalles emboîtés en utilisant la méthode des α−coupes. $A^{(\alpha)}{}_L$ et $A^{(\alpha)}{}_R$ représentent respectivement les limites droites et gauches de la fonction d'appartenance $\mu_{A(x)}$ à chaque coupe de niveau α.

Les opérations arithmétiques appliquées à deux nombres flous A et B donnent les expressions suivantes :

$$C = A + B \rightarrow [C^{(\alpha)}{}_L, C^{(\alpha)}{}_R] = [A^{(\alpha)}{}_L + B^{(\alpha)}{}_L, A^{(\alpha)}{}_R + B^{(\alpha)}{}_R] \tag{3.13}$$

$$C = A - B \rightarrow [C^{(\alpha)}{}_L, C^{(\alpha)}{}_R] = [A^{(\alpha)}{}_L - B^{(\alpha)}{}_L, A^{(\alpha)}{}_R - B^{(\alpha)}{}_R] \tag{3.14}$$

$$C = A.\ B \rightarrow [C^{(\alpha)}{}_L, C^{(\alpha)}{}_R] = [\min(A^{(\alpha)}{}_L . B^{(\alpha)}{}_L . A^{(\alpha)}{}_R . B^{(\alpha)}{}_L . A^{(\alpha)}{}_L . B^{(\alpha)}{}_R . A^{(\alpha)}{}_R . B^{(\alpha)}{}_R).$$
$$\max(A^{(\alpha)}{}_L . B^{(\alpha)}{}_L . A^{(\alpha)}{}_R . B^{(\alpha)}{}_L . A^{(\alpha)}{}_L . B^{(\alpha)}{}_R . A^{(\alpha)}{}_R . B^{(\alpha)}{}_R)] \tag{3.15}$$

$$C = A / B \rightarrow [C^{(\alpha)}{}_L, C^{(\alpha)}{}_R] = [A^{(\alpha)}{}_L . A^{(\alpha)}{}_R] * [1/B^{(\alpha)}{}_L . 1/B^{(\alpha)}{}_R] \tag{3.16}$$

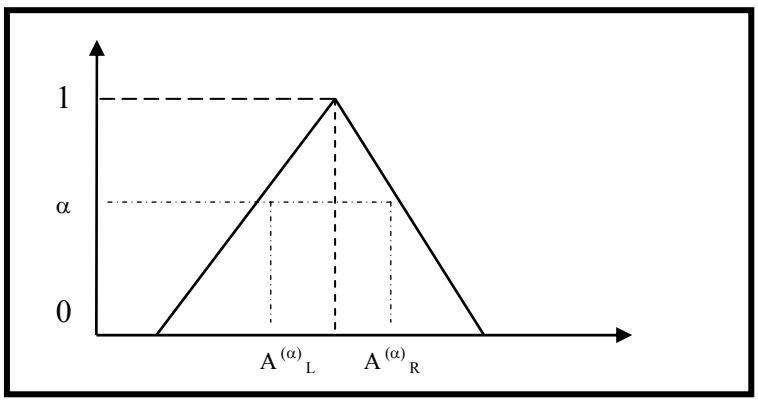

Figure 3.4-α-coupes d'un nombre flou

3.1.1.5 Compositions de relations floues

Il existe plusieurs façons de définir la composition de deux relations floues, la plus employée est la définition «max-min» conforme au principe d'extension :

$$\mu_{S \circ R}(x, z) = supy\ (min\ (\mu_R(x, y), \mu_S(y, z)) \quad (3.17)$$

En particulier si A est une relation unaire et R est binaire on peut définir de la même façon :

$$\mu_{R \circ A}(v) = max\ u\ (min\ (\mu_A(u), \mu_R(u, v))) \quad (3.18)$$

Les définitions relatives aux relations binaires exactes peuvent se généraliser aisément au flou:

Symétrie : $\forall x \forall y\ \mu_R(x, y) = \mu_R(y, x)$ (3.19)

Antisymétrie : $\forall x \forall y\ \mu_R(x, y) > 0 \Rightarrow \mu_R(y, x) = 0$ (3.20)

Réflexivité : $\forall x\ \mu_R(x, x) = 1$ (3.21)

Antiréflexivité : $\forall x\ \mu_R(x, x) = 0$ (3.22)

Transitivité : $\forall x \forall y \forall z\ \mu_R(x, z) \geq maxy\ (min\ (\mu_R(x, y)\ ,\ \mu_R(y, z)))$ (3.23)

Soit : $\mu_R \geq \mu_{R \circ R}$ ce qui permet parfois de vérifier plus rapidement la transitivité.

On peut montrer les propriétés suivantes :

R symétrique $\Leftrightarrow \forall \alpha \in [0, 1]$ La α-coupe de R est symétrique

R transitive $\Leftrightarrow \forall \alpha \in [0, 1]$ La α-coupe de R est transitive

3.1.1.6 Fermeture transitive d'une relation floue

Soit R une relation floue dans $E \times E$, on définira alors :

$$R^2 = R \circ R \quad (3.24)$$

Par

$$\mu_{R^2}(x,z) = max[min(\ \mu_{R^2}(x,y)\ ,\ \mu_{R^2}(y,z))] \quad (3.25)$$

Où $x, y, z \in E$

Soit

$$R^2 = R \circ R \subset R \quad (3.26)$$

Et de la

$$R^{K+1} \subset R^K \quad , \quad K = 1, 2, 3..... \quad (3.27)$$

Et aussi, évidemment :

$$R^K \subset R \quad , \quad K = 1, 2, 3..... \quad (3.28)$$

On appelle « fermeture transitive » d'une relation floue R, la relation :

$$\check{R} = R \cup R^2 \cup R^3 \cup .... \tag{3.29}$$

Exemple

On donne une relation R quelconque. On calcule R^2, puisR^3. On voit que $R^2 = R^3$; on peut donc s'arrêter là et $\check{R} = R \cup R^2$.

$$R = \begin{pmatrix} 0.8 & 1 & 0.1 \\ 0 & 0.4 & 0 \\ 0.3 & 0 & 0.2 \end{pmatrix} \tag{3.30}$$

$$R^2 = \begin{pmatrix} 0.8 & 0.8 & 0.1 \\ 0 & 0.4 & 0 \\ 0.3 & 0.3 & 0.2 \end{pmatrix} \tag{3.31}$$

$$R^3 = \begin{pmatrix} 0.8 & 0.8 & 0.1 \\ 0 & 0.4 & 0 \\ 0.3 & 0.3 & 0.2 \end{pmatrix} \tag{3.32}$$

$$\check{R} = R \cup R^2 = \begin{pmatrix} 0.8 & 1 & 0.1 \\ 0 & 0.4 & 0 \\ 0.3 & 0 & 0.2 \end{pmatrix} \cup \begin{pmatrix} 0.8 & 0.8 & 0.1 \\ 0 & 0.4 & 0 \\ 0.3 & 0.3 & 0.2 \end{pmatrix}$$

$$= \begin{pmatrix} 0.8 & 1 & 0.1 \\ 0 & 0.4 & 0 \\ 0.3 & 0.3 & 0.2 \end{pmatrix} \tag{2.33}$$

Après avoir introduit les concepts de base des principales théories utilisées pour la représentation des connaissances imparfaites, nous allons présenter, dans la suite, un état de l'art sur les chaînes de Markov flous, qui permettent de prendre en compte les paramètres de fiabilité imparfaits des composants dans l'évaluation de la sûreté de fonctionnement des systèmes.

3.2 Détermination de la PFD des systèmes instrumentés de sécurité par le modèle Markovien flou

Lorsque les systèmes instrumentés de sécurité sont faiblement sollicités, le retour d'expérience est faible et les probabilités en jeu sont souvent imprécises. Le problème de précision sur les taux de défaillance ou de réparation existe également lorsque l'on travaille avec de nouveaux composants. Certaines bases de données de fiabilité [OREDA, 2002; CCPS, 2002 ;IEEE,1984] fournissent les bornes inférieures et supérieures, et des valeurs moyennes des taux de défaillance, et de l'MTTF des composants. Il est alors nécessaire de définir des chaînes de Markov qui utilisent le formalisme flou, qui peuvent utiliser avantageusement ces valeurs pour prendre en compte l'imprécision (qu'on appelle aussi incertitude, liée à ces taux de défaillance et de réparation et estimer les probabilités de défaillance des composants ainsi que les *PFD* des *SIS*.

De ce fait, les différents taux de défaillance, et de réparation deviennent :

$\lambda_{DD} \in [\lambda_{DD\,\inf}, \lambda_{DD\,\sup}]$ et $\lambda_{DU} \in [\lambda_{DU\,\inf}, \lambda_{DU\,\sup}]$

$\mu_{DD} \in [\mu_{DD\,\inf}, \mu_{DD\,\sup}]$ et $\mu_{DU} \in [\mu_{DU\,\inf}, \mu_{DU\,\sup}]$

L'objectif étant de déterminer les probabilités de défaillance à la demande du *SIS*, pour déterminer son niveau d'intégrité, nous considérons que les défaillances des causes communes sont négligeables.

3.2.1 Architecture 1oo1

a- Détermination du PFD

Pour évaluer la PFDavg du SIS, nous commençons par évaluer la probabilité de défaillance sur demande à un instant t (qui représente l'indisponibilité instantanée du SIS). Ensuite, pour obtenir la PDFavg, nous déterminons la valeur moyenne des indisponibilités, que nous avons déterminé sur une période donnée.

Si nous considérons la première architecture 1001 représentée par figure 3.5 nous avons :

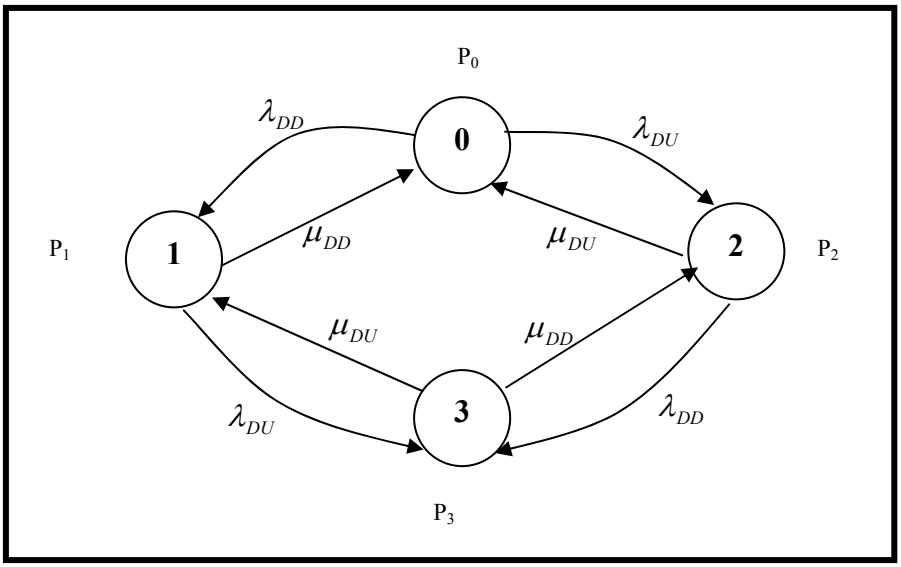

Figure 3.5-Modèle Markovien contenu relatif à l'architecture 1oo1

La matrice de transition floue de cette architecture est $\widetilde{M}$. Alors *P (n.* Δ *t)* est le vecteur flou donné par [Binh et al, 2006]:

$$\widetilde{p}(n.\Delta t) = \widetilde{M}^{\,n} op(0) \tag{3.34}$$

Avec $\widetilde{M}^{\,n}$ est la matrice puissance, et $p(0)=[1\ 0\ 0\ 0]^T$ la distribution initiale .

$$\widetilde{M} = \begin{bmatrix} 1-(\widetilde{\lambda}_{DD}+\widetilde{\lambda}_{DU})\Delta t & \widetilde{\mu}_{DD}\Delta t & \widetilde{\mu}_{DU}\Delta t & 0 \\ \widetilde{\lambda}_{DD}\Delta t & 1-(\widetilde{\lambda}_{DU}+\widetilde{\mu}_{DD})\Delta t & 0 & \widetilde{\mu}_{DU}\Delta t \\ \widetilde{\lambda}_{DU}\Delta t & 0 & 1-(\widetilde{\lambda}_{DD}+\widetilde{\mu}_{DU})\Delta t & \widetilde{\mu}_{DD}\Delta t \\ 0 & \widetilde{\lambda}_{DU}\Delta t & \widetilde{\lambda}_{DD}\Delta t & 1-(\widetilde{\mu}_{DD}+\widetilde{\mu}_{DU})\Delta t \end{bmatrix} \tag{3.35}$$

Nous proposons donc de modéliser les taux de défaillance, et de réparation imprécis par des nombres flous triangulaires. Dans sa forme la plus générale, la fonction d'appartenance d'un nombre flou triangulaire λ_{DD} par exemple (figure 3.6) est donnée par :

$$\mu(\lambda_{DD}) = 0, \qquad \lambda_{DD} < \lambda_{DD} I \tag{3.36}$$

$$\mu(\lambda_{DD}) = \frac{\lambda_{DD} - \lambda_{DD} i}{\lambda_{DD} m - \lambda_{DD} i}, \qquad \lambda_{DD} i \le \lambda_{DD} \le \lambda_{DD} m \tag{3.37}$$

$$\mu(\lambda_{DD}) = \frac{\lambda_{DD}s - \lambda_{DD}}{\lambda_{DD}s - \lambda_{DD}m} \qquad \lambda_{DD}\,i < \lambda_{DD}\,m < \lambda_{DD}\,s \tag{3.38}$$

$$\mu(\lambda_{DD}) = 0, \qquad \lambda_{DD} > \lambda_{DD}\,s \tag{3.39}$$

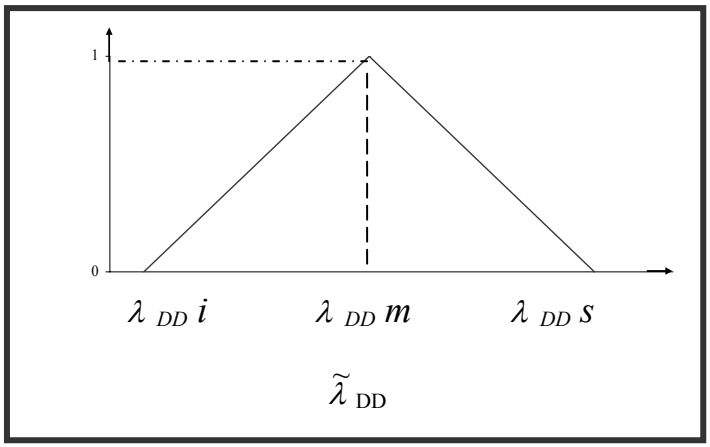

Figure 3.6- Modélisation du taux de défaillance imprécis λ_{DD} par un nombre flou triangulaire

Considérons maintenant le même problème avec le taux de défaillance imprécis $\tilde{\lambda}_{DU}$, et les taux de réparation imprécis $\tilde{\mu}_{DU}$, et $\tilde{\mu}_{DD}$ exprimés sous la forme d'intervalles (figure 3.7) :

$[\lambda_{DU}i,\ \lambda_{DU}m,\ \lambda_{DU}s]$ pour λ_{DU}.

$[\mu_{DD}i,\ \mu_{DD}m,\ \mu_{DD}s]$ et $[\mu_{DU}i,\ \mu_{DU}m,\ \mu_{DU}s]$ pour μ_{DD} et μ_{DU}.

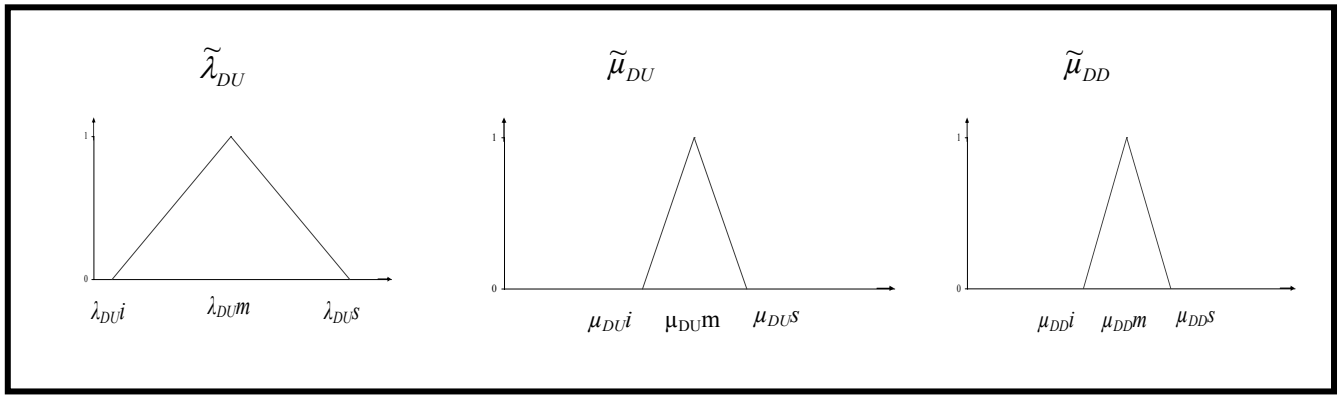

Figure 3.7- Modélisation du λ_{DD}, $\tilde{\mu}_{DU}$ et $\tilde{\mu}_{DD}$ par des nombres flous triangulaires

Ces nombres flous triangulaires sont caractérisés par les 3 paramètres, la valeur modale de la fonction d'appartenance. Elle représente la valeur la plus probable des taux de défaillance et de réparation. La limite à gauche, qu'on appelle aussi valeur basse, et la limite à droite, qu'on appelle aussi valeur haute.

Par ailleurs, l'avantage d'utiliser une forme triangulaire pour modéliser les taux de défaillance, et les taux de réparation réside dans le fait qu'elle peut être biaisée vers la droite ou vers la gauche par rapport à sa valeur la plus probable. Un autre avantage inhérent aux nombres flous triangulaires est la facilité d'utilisation grâce à la simplification des opérations arithmétiques floues [Kaufman et Gupta, 1991].

La matrice de transition floue $\widetilde{M}$ est composée d'opérations sur les nombres flous dans l'approche proposée. Le premier éliment de la matrice $\widetilde{M}$ ($\widetilde{M}(1.1)(1.1)$ par exemple, est présenté dans la figure 3.8. Pour déterminer la fonction d'appartenance du $\widetilde{M}$ (1.1), (figure 3.9) on utilisant des opérations arithmétiques simples (addition, soustraction et multiplication).

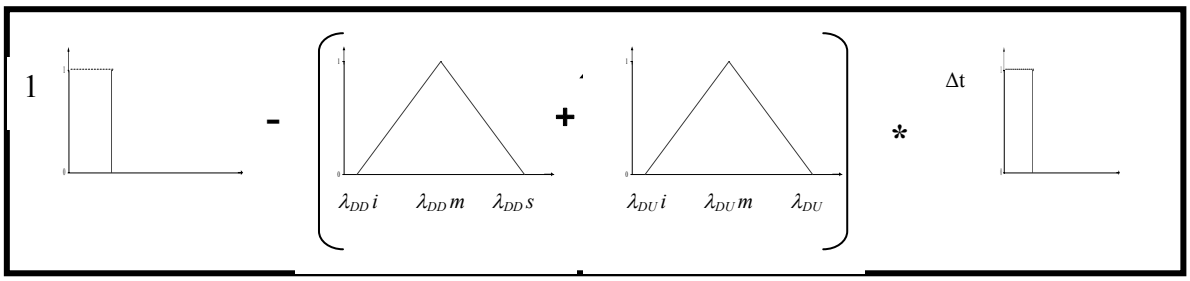

Figure 3.8- Premier éliment le la matrice $\widetilde{M}$

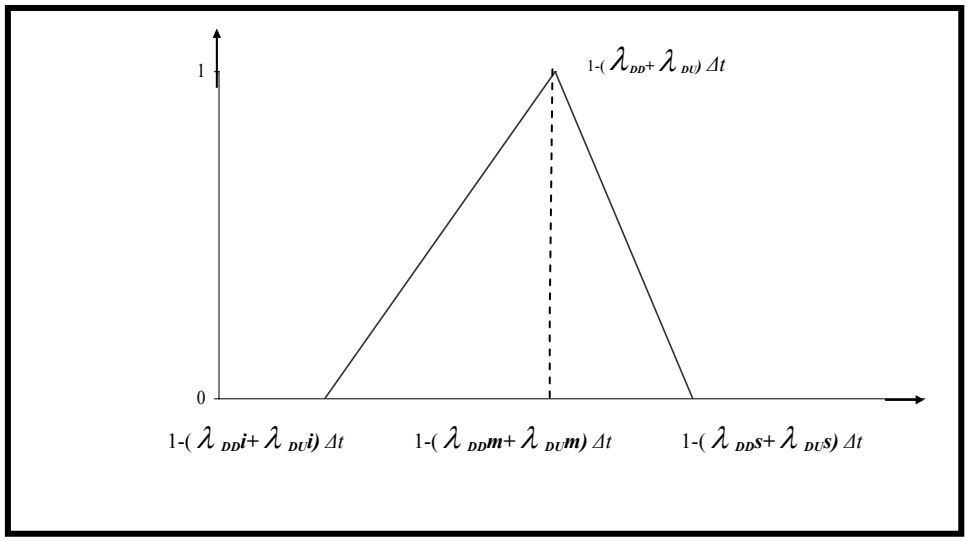

Figure 3.9- Modélisation du *1-(λ_{DD}+ λ_{DU}) Δt*

La probabilité floue de défaillance dangereuse sur demande à l'instant $t=n.\Delta t$, est donnée par :

$$P\widetilde{F}D(n\Delta t) = \widetilde{P}_1(n.\Delta t) + \widetilde{P}_2(n.\Delta t) + P_3(n.\Delta t) \tag{3.40}$$

Avec

$$[\ \widetilde{P}_0(n\Delta t) \quad \widetilde{P}_1(n.\Delta t) \quad \widetilde{P}_2(n.\Delta t) \quad P_3(n.\Delta t)\ ]^T = \widetilde{M}^n o P(0) \tag{3.41}$$

Et $p(0)=[1\ 0\ 0\ 0]^T$

À un instant $i.\Delta t$, tel que $i>1$ la $P\widetilde{F}D$ floue est présentée dans la figure 3.10.

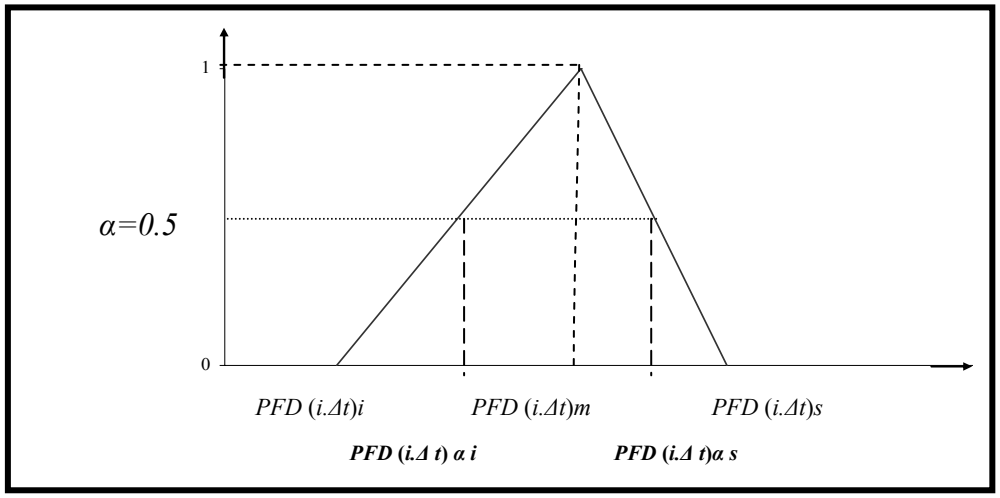

Figure 3.10- *PFD* floue à l'instant *t* avec les *α*-coupes

Nous pouvons obtenir plusieurs intervalles emboîtés en utilisant la méthode des α−coupes. $PFD\ (i.\Delta t)\alpha i$ et $PFD\ (i.\Delta t)\alpha s$ représenteront respectivement les limites gauche et droite de la fonction d'appartenance $\mu_{P\widetilde{F}D\ (i.\Delta t)}$ à chaque α −coupe. Cependant, si on considère $\alpha=0,\ \alpha=0.5,\ et\ \ \alpha=1$; on peut obtenir 5 courbes floues pour les déférentes α−coupes (figure 3.11).

b- Exemple numérique

Si nous considérons les données numériques suivantes :

- T_1=4380h ; $\lambda_D \in [3.10^{-6}, 7.10^{-6}]$; DC=0.4; et Δt=50h.

Les probabilités de défaillances dangereuses sur demande en fonction du temps, correspondant respectivement aux α−coupes, $\alpha=0,\ \alpha=0.5,\ et\ \ \alpha=1$ sont fournies à la figure (figure 3.11).

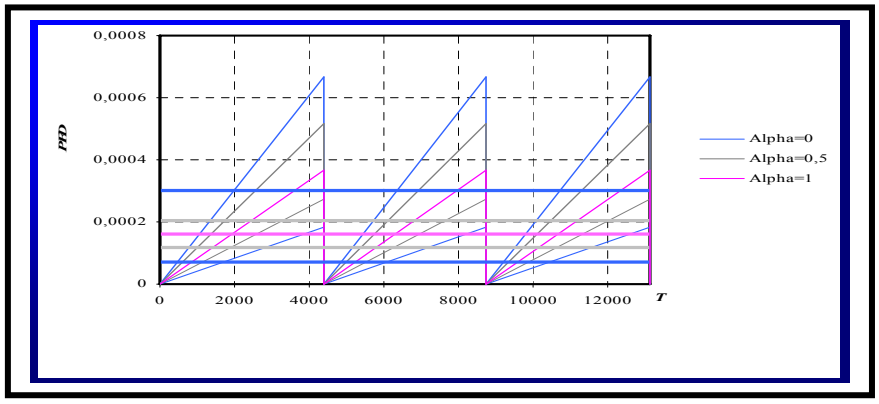

Figure 3.11- courbes de la *PFD* 1001 floue pour α=0, α=0.5, et α=1.

La probabilité de défaillance sur demande en fonction du temps, après la défuzzification, est fournie à la figure (figure 3.12) à partir de la relation de la défuzzification donnée par :

$$PFD(i\Delta t) = \frac{\sum \mu(PFD(i\Delta t)).PFD(i\Delta t)}{\sum \mu(PFD(i\Delta t))} \tag{3.42}$$

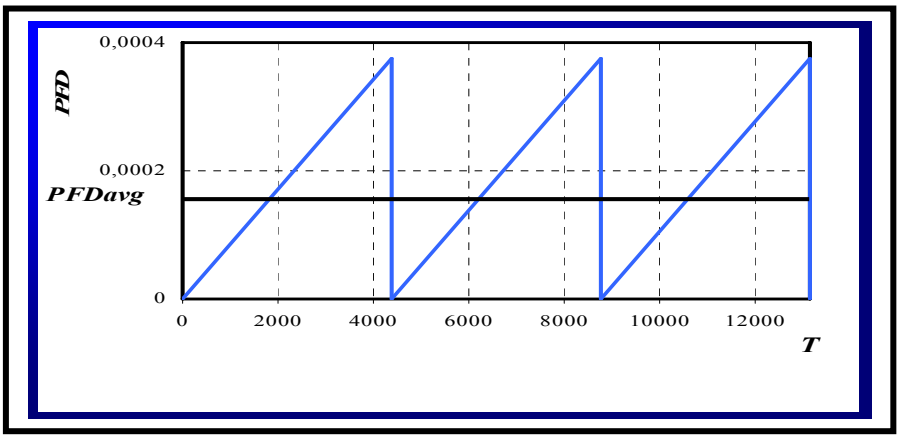

Figure 3.12- courbe de la *PFD* 1001 après défuzzification

Les figures 3.11, et 3.12 montrent que la probabilité de défaillance dangereuse de l'architecture 1oo1 reste encadrée par les probabilités supérieures et inférieures de défaillance sur demande correspondant aux α-coupes.

3.2.2 Architecture 1002

a- Détermination du PFD

Rappelons que cette architecture ce compose de deux canaux identiques en redondance chaude. Il faut donc que ces deux canaux subissent chacun une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande.

Le modèle markovien [Innal et al. 2005] de l'architecture 1002 est représenté à la figure 3.13.

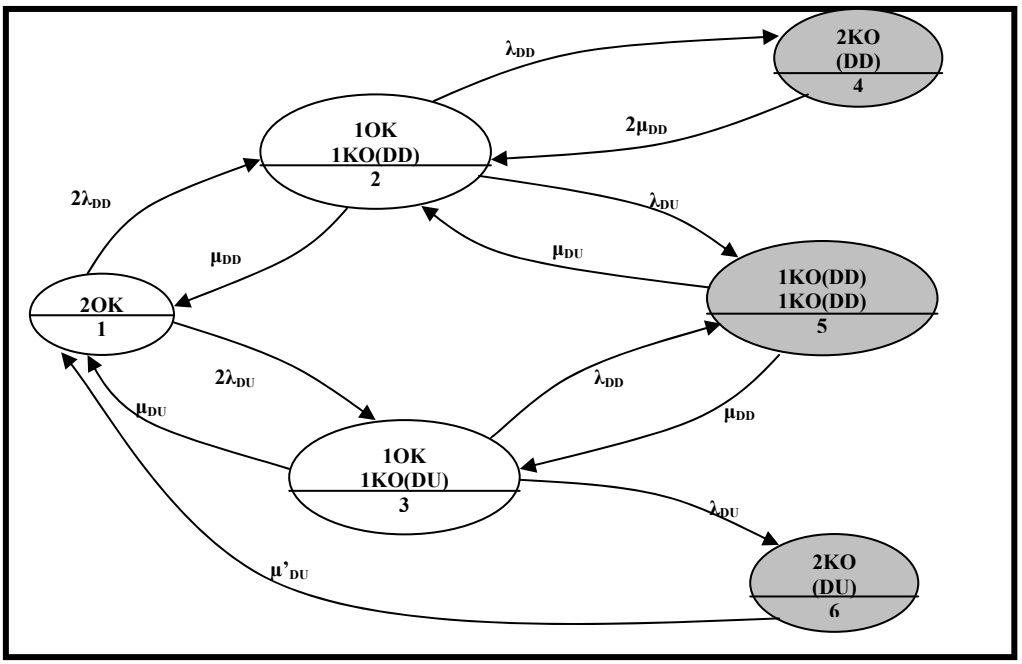

Figure 3.13-Modèle Markovien contenu relatif à l'architecture 1oo2

Nous suivant la même démarche que précédemment. La matrice floue de transition entre états est déterminée. Les probabilités de cette matrice de transition seront représentées par des nombres flous :

$$\widetilde{M}=\begin{bmatrix} 1-2(\widetilde{\lambda}_{DD}+\widetilde{\lambda}_{DU})\Delta t & 2\widetilde{\lambda}_{DD}\Delta t & 2\widetilde{\lambda}_{DU}\Delta t & 0 & 0 & 0 \\ \widetilde{\mu}_{DD}\Delta t & 1-(\widetilde{\mu}_{DD}+\widetilde{\lambda}_{DD}+\widetilde{\lambda}_{DU})\Delta t & 0 & \widetilde{\lambda}_{DD}\Delta t & \widetilde{\lambda}_{DU}\Delta t & 0 \\ \widetilde{\mu}_{DU}\Delta t & 0 & 1-(\widetilde{\mu}_{DU}+\widetilde{\lambda}_{DD}+\widetilde{\lambda}_{DU})\Delta t & 0 & \widetilde{\lambda}_{DD}\Delta t & \widetilde{\lambda}_{DU}\Delta t \\ 0 & 2\widetilde{\mu}_{DD}\Delta t & 0 & 1-2\widetilde{\mu}_{DD}\Delta t & 0 & 0 \\ 0 & \widetilde{\mu}_{DU}\Delta t & \widetilde{\mu}_{DD}\Delta t & 0 & 1-(\widetilde{\mu}_{DU}+\widetilde{\mu}_{DD})\Delta t & 0 \\ \widetilde{\mu}'_{DU}\Delta t & 0 & 0 & 0 & 0 & 1-\widetilde{\mu}'_{DU}\Delta t \end{bmatrix} \quad (3.43)$$

L'équation d'état de cette architecture est définie comme suit :

$$\left[\ \widetilde{P}_1(n.\Delta t) \quad \widetilde{P}_2(n.\Delta t) \quad \widetilde{P}_3(n.\Delta t) \quad \widetilde{P}_4(n.\Delta t) \quad \widetilde{P}_5(n.\Delta t) \quad \widetilde{P}_6(n.\Delta t)\ \right]=\widetilde{M}^{n}oP(0) \quad (3.44)$$

La probabilité floue de défaillance dangereuse sur demande à l'instant $t=n.\Delta t$, est donnée par :

$$P\widetilde{F}D(n\Delta t)=\widetilde{P}_4(n.\Delta t)+\widetilde{P}_5(n.\Delta t)+P_6(n.\Delta t) \quad (3.45)$$

Avec *p(0)=[1 0 0 0 0 0]*

b- Exemple numérique

Si nous considérons les douées numériques suivantes :

- T_1=4380h ; $\lambda_D \in [3.10^{-6}, 7.10^{-6}]$; DC=0. 9 ;et Δt=50h.

L'évolution des indisponibilités au cours du temps pour les valeurs des α−coupes 0, 0.5, et 1 est fournie par la figure (figure 3.14):

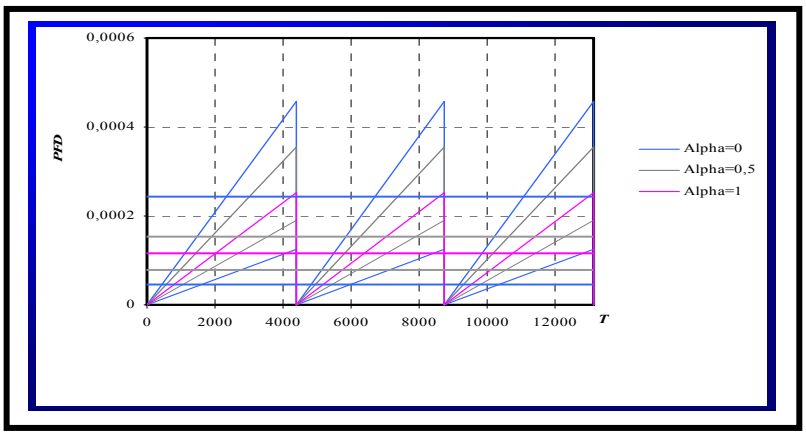

Figure 3.14- courbes de la *PFD* 1002 floue pour α=0, α=0.5, et α=1.

Et après la défuzzification, comme dans le cas précédent la $\widetilde{PFD}(n.\Delta t)$ est donnée en figure (figure 3.15)

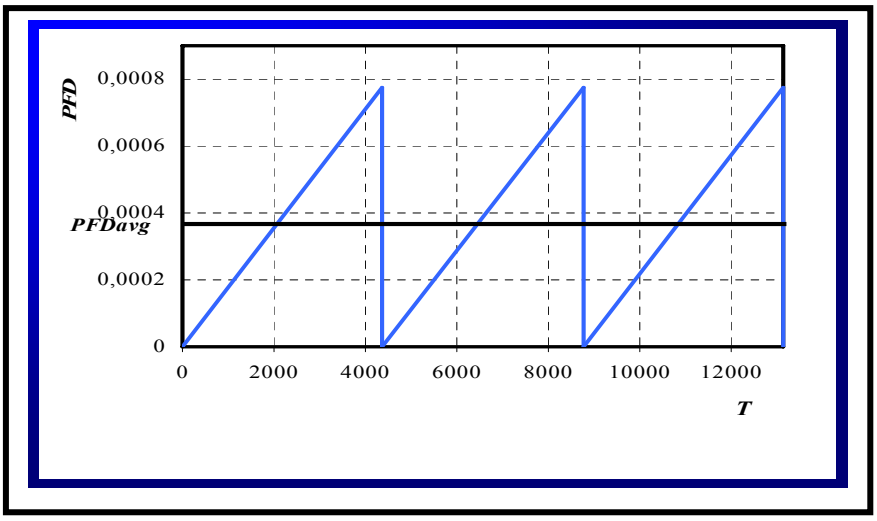

Figure 3.15- courbe de la *PFD*1002 après defuzzification

Comme dans le cas précédent, l'indisponibilité instantanée du système est encadrée par des bornes supérieure et inférieure liées aux valeurs d'α-coupes.

Conclusion

L'imprécision dans les études de fiabilité et disponibilité des systèmes est un problème significatif souvent minoré. Nous avons proposé dans ce chapitre l'étude des effets de l'imprécision sur les paramètres caractéristiques d'un système instrumenté de sécurité. Et nous avons montré que cela pouvait entraîner des variations dans sa probabilité de défaillance sur demande. Les chaînes de Markov floues sont des modèles pertinents dans ce contexte.

L'application de l'approche proposée à un système opérationnel fera l'objectif du quatrième chapitre.

Chapitre 4

Evaluation des SIL d'un système opérationnel : Four Rebouilleur

Introduction

La démarche d'évaluation du niveau d'intégrité des systèmes instrumentés de sécurité en présence de données incertaines , est appliquée à un procédé constitué d'un module « MPP0 » ,dans une installation pétrolière à Hassi R'Mel. Son rôle est le traitement du gaz naturel en le séparant pour obtenir le gaz de vente (C_1, C_2), GPL (C_3, C_4) et le condensât.

Le module est constitué de différents systèmes (ballons de séparation, colonnes de distillation, échangeurs, fours…). Ces dernières sont conçues pour assurer un bon traitement de gaz.

Dans ce module, le four H401 est considéré comme étant la partie la plus sensible qui joue un rôle important dans le fonctionnement du module.

Notre étude à porté sur le système four H401 qui est composé des éléments suivants : four H401, circuit d'alimentation gaz et liquide et le système de contrôle.

4.1 Description du système

4.1.1 Rôle du four H401

Le rôle du four dans une unité pétrolière est d'apporter la chaleur nécessaire pour réchauffer un fluide en le portant à des niveaux de température élevés [ENSPM, 2005].

Dans le MPP0 les hydrocarbures liquides[1] du fond de la colonne T401 passe dans le rebouilleur H401 pour être chauffée de 145°C jusqu'à 180°C avant de retourner vers la colonne comme reflux chaud pour séparer les gaz légers (C_1,C_2) voir(Figure 4.1) .

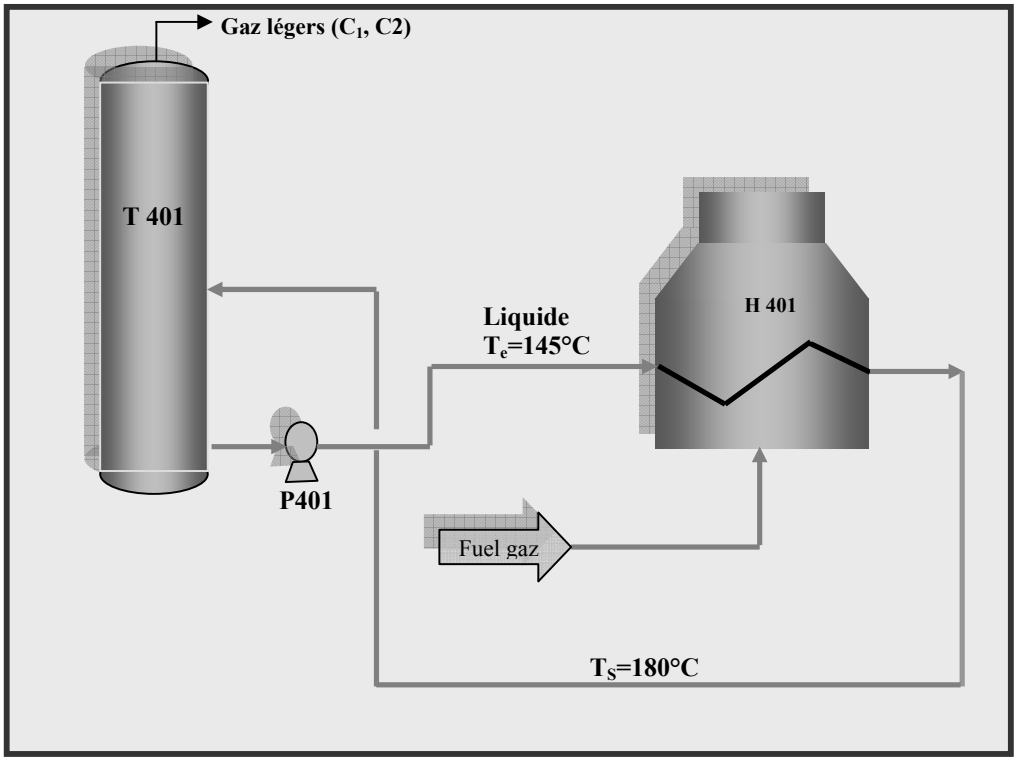

Figure 4.1- Rôle du four H401

[1] Liquide qui contient gaz sec (C_1, C_2), GPL (C_3, C_4) et condensât (C_5+)

4.1.2 Décomposition structurelle et fonctionnelle du système four H401

4.1.2.1 Sous système d'alimentation

Le système circuit d'alimentation constitué d'un circuit comburant, et un circuit Liquide (Tableau 4.1).

Tableau 4.1- Sous-système d'alimentation

Sous-systèmes	Équipements	Composants
SS1 : circuit d'alimentation [Alimentation du four rebouilleur]	**E11 :** circuit comburant (Fuel Gaz) [Assure l'alimentation en combustible]	**C111 :** Vanne TV [régulation de pression de fuel gaz en fonction de la température de liquide]
		C112 : Les pilotes [Garantir une flamme continue pour l'amorçage du fuel gaz]
		C113 : Les brûleurs [Réaliser la combustion de fuel gaz]
	E12 : circuit Liquide [Assure l'alimentation en liquide du fond de la colonne]	**C121 :** Pompes P401 A/B [pomper le liquide à l'entrée du four]
		C122 : Vanne FV [régulation de débit de liquide]
		C123 : Serpentin [Assure la circulation et l'échauffement du liquide]

4.1.2.2 Sous système de contrôle

Le contrôle dans le four concerne les paramètres suivants :

- la température de sortie du fluide de procédé doit être maintenue à 180°C.
- le débit du fluide de procédé dans le four doit être maintenu à 800m^3

Tableau 4.2- Sous-système de contrôle

Sous-systèmes	Équipements	Composants
SS2 : de contrôle [contrôle des paramètres du procédé]	**E21 :** contrôle de débit [Contrôle le débit du liquide à l'entrée du four]	**C211 :** DCS (SOLVER) [Adaptation du débit de liquide à l'entrée de four par action sur la vanne FV]
		C212 : Débitmètre FT [Mesure le débit du liquide à l'entrée de four]
	E22 : contrôle de température [Contrôle la température du liquide à l'intérieur et à la sortie du four]	**C221 :** DCS (SOLVER) [Adaptation de température de liquide à la sortie de four par action sur la vanne TV]
		C222 : Thermocouple TI [Mesure la température du liquide à la sortie du four]
		C223 : Indicateurs de température TJI [Indique la température]

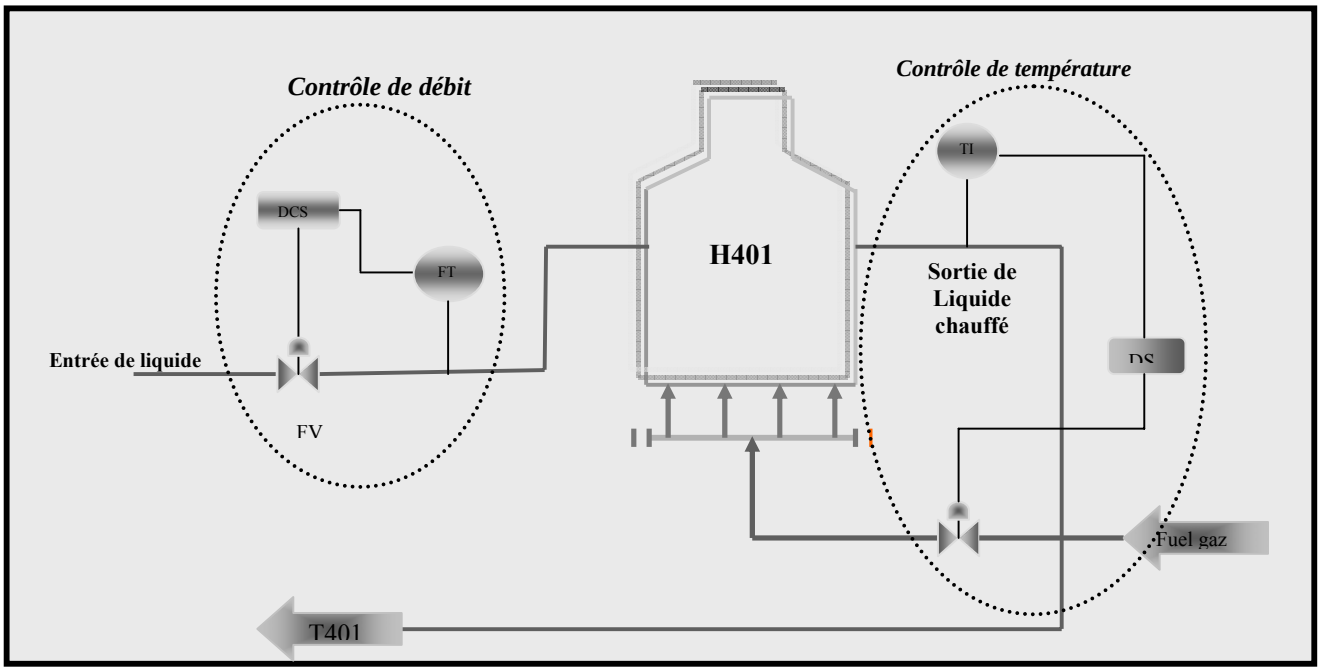

Figure4.2-Système de contrôle dans le four H401

Ce système de contrôle comprend :

-un capteur de température (TI)

-un capteur de débit (FT)

-vannes de régulation de température et débit (TV, FV)

- automate de régulation

4.1.2.3 Sous-système d'alarme

Dans le cas où le système de contrôle tombe en panne, c'est-à-dire n'exécute pas sa fonction, le système d'alarme devrait intervenir pour alerter les opérateurs afin qu'ils interviennent pour de rendre le système à l'état stable.

Tableau 4.3- Sous-système d'alarme

Sous-système	Equipement	composant
SS3 : d'alarmes [Faire alerter l'opérateur par un signal audio-visuel]	**E31 :** TAH [alarme de haute température du fluide à chauffé]	**C311 :** Thermocouple TI [Mesure la température du liquide à la sortie du four]
		C312 : DCS [Adaptation de la mesure de haute température à une alarme audio-visuel]
	E32 : FAL [alarme de bas débit du liquide 530m^3/h]	**C321 :** Débitmètre FT [Mesure le débit du liquide à l'entrée de four]
		C322 : DCS [Adaptation de la mesure de bas débit à une alarme audio-visuel]
	E33:PAL/H [alarme de basse et haute pression de fuel gaz (300 g/cm^2) / (1Kg/cm^2)]	**C331 :** Pressostat PSL [mesure la pression de fuel gaz]
		C332 : DCS [Adaptation de la mesure de basse pression à une alarme audio-visuelle]

4.1.2.4 Sous-système d'arrêt d'urgence (système instrumenté de sécurité)

Le système d'ESD (Emergency Shut Down), connu aussi sous le nom de SIS, consiste à assurer l'arrêt totale de four H401 en cas de perturbation de système de contrôle, de détection d'une anomalie ou d'autres conditions potentiellement dangereuses du procédé, afin de protéger le personnel, les équipements et l'environnement.

Le système d'ESD est un système complètement autonome qui est destiné uniquement à l'arrêt d'urgence. Le système ESD intervient dans les cas suivants:

- Température

- Très haute température du fluide à chauffé : TAHH : 320 °C.
- Très haute température de la cheminée : TAHH : 550 °C.

- Débit bas du fluide a chauffé

Le seuil bas de débit du liquide est un facteur de déclenchement du four, plus ce débit décroît, plus la température du liquide augmente :
FALL : 380 m^3/h.

- Pression du fuel gaz

Les seuils bas et haut de pression de fuel gaz sont des facteurs de déclenchement du four
PALL: 150g/Cm2.
PAHH: 1.3Kg/Cm2

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

A- Capteurs

Chaque facteur de déclenchement possède un seul capteur, ce dernier est destiné pour mesurer les paramètres du procédé dans le four (température, débit, pression) puis envoyer les signaux vers l'unité de traitement

- TSHH capteur de Très haute température du fluide a chauffé
- TI capteur de Très haute température de la cheminée
- FSLL capteur de très bas Débit du fluide a chauffé

- PSHH/LL capteur de (très basse/très haute) Pression du fuel gaz

B- Unité de traitement PLC (TRICONEX)

L'architecture adoptée sera le modulaire triplex, avec 03 processeurs séparés à structure de bus triplex, tous les système en parallèles. Chaque processeur exécutera ses programmes d'application individuellement simultanément et indépendamment, en vérifiant les données, en exécutent les instructions logiques et contrôle les signaux.

La technologie TMR (Triple Majority Redandency) de Triconex utilise trois systèmes de contrôle parallèles isolés et plusieurs possibilités de diagnostic intégrées dans un seul système. Le système utilise le principe de 2 sur 3 votes pour assurer une très grande intégrité, une absence d'erreur et un fonctionnement ininterrompu. Le voteur 2 sur 3 assure un signal à la sortie s'il y a un signal sur deux voies sur les trois voies (Figure 4.4).

Le système doit procéder automatiquement au contrôle de tous ses composants pour identifier les défaillances. Ces essais de diagnostics seront exécutés au démarrage du système et pendant son exploitation.

Lors de la détection d'une défaillance, une alarme descriptive sera générée pour signalisation visuelle.

Figure 4.3-Automate programmable PLC[JGC,2005]

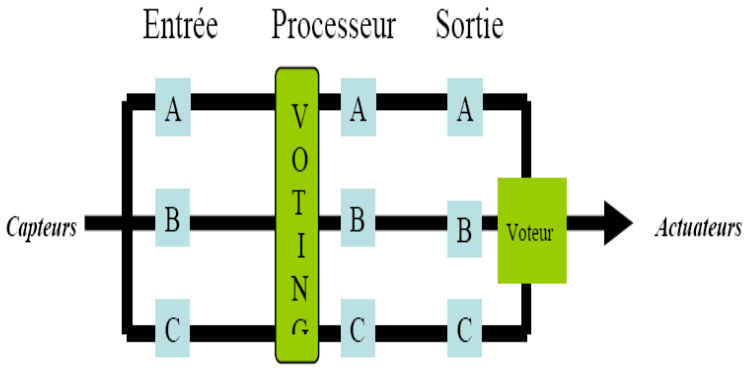

Figure 4.4-Architecture 2oo3 de PLC[JGC,2005]

C- Les actionneurs

Sont deux électrovannes en parallèles (tout ou rien) commandés par le PLC. En cas d'existence de facteur de déclenchement, on a une fermeture des vannes (UV1, UV2) pour couper l'alimentation de fuel gaz.

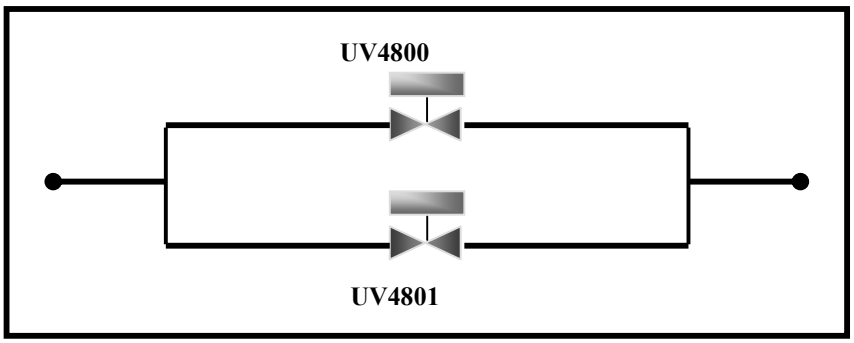

Figure 4.5- Architecture 1oo2 des vannes

4.2 Evaluation de l'Indisponibilité des systèmes instrumentés de sécurité

a-Hypothèses

– Nous nous plaçons dans le cas où le SIS est faiblement sollicité (moins d'une fois / an), d'où le besoin d'évaluer le *PFD* et non pas le *PFH* (probabilité de défaillance par heure). Dans ce cas, le *PFD* instantané est assimilé à une indisponibilité instantanée.

– Nous nous intéressons à l'évaluation du *PFDavg* du *SIS*. C'est pourquoi nous utilisons les taux de défaillance λ_D des composants qui désignent les taux de défaillance dangereuse non détectées λ_{DU} et les taux de défaillance détectés λ_{DD}:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \tag{4.1}$$

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \tag{4.2}$$

Ces défaillances dangereuses font passer le système de l'état normal à l'état de défaillance dangereux.

– Les composants sont réparables.

– Il n'existe pas de dépendance entre les défaillances des composants (le facteur de causes communes de défaillances est nul $ß_D$=ß=0).

–Les tests de diagnostic des composants soient réalisés simultanément.

Tous les calculs que nous avons effectué concerne le SIS décrire par le schéma suivant :

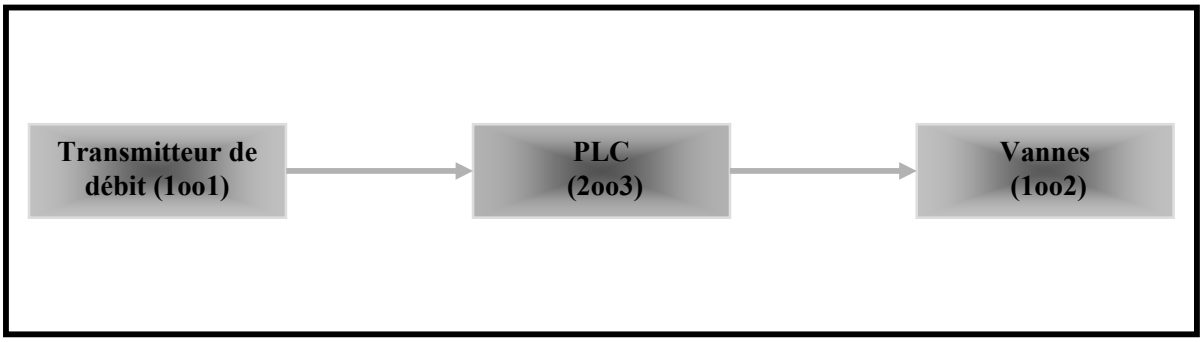

Figure 4.6- Schéma simple du SIS

La probabilité moyenne de défaillance sur demande du système instrumenté de sécurité est déterminée par le calcul et la combinaison de La probabilité moyenne de défaillance sur demande pour tous les sous-systèmes assurant ensemble la fonction de sécurité.

4.2.1 Application de l'approche Markovienne classique

Pour calculer la *PFDavg* de notre *SIS*, nous avons utilisé les expressions obtenues par le modèle de Markov (chapitre 2).

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

Tableau 4.4- Les valeurs des taux de défaillance, et de la MTTF pour DC=60%

DC=60%				
paramètre / composant	λ_D (1/h)	λ_{DD} (1/h)	λ_{DU}(1/h)	MTTR (h)
Transmitteur de débit	1.5×10^{-6}	0.9×10^{-6}	0.6×10^{-6}	9.8
Vanne	2.7×10^{-6}	1.62×10^{-6}	1.08×10^{-6}	12
PLC	10^{-8}	0.6×10^{-8}	0.4×10^{-8}	10.2

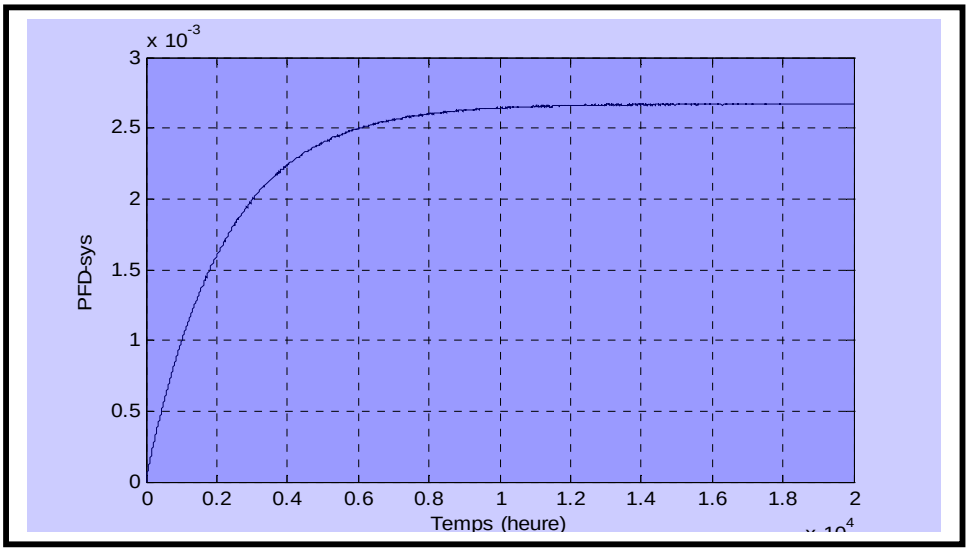

Figure 4.7- Evolution de l'indisponibilité du système en fonction du temps pour DC=60%

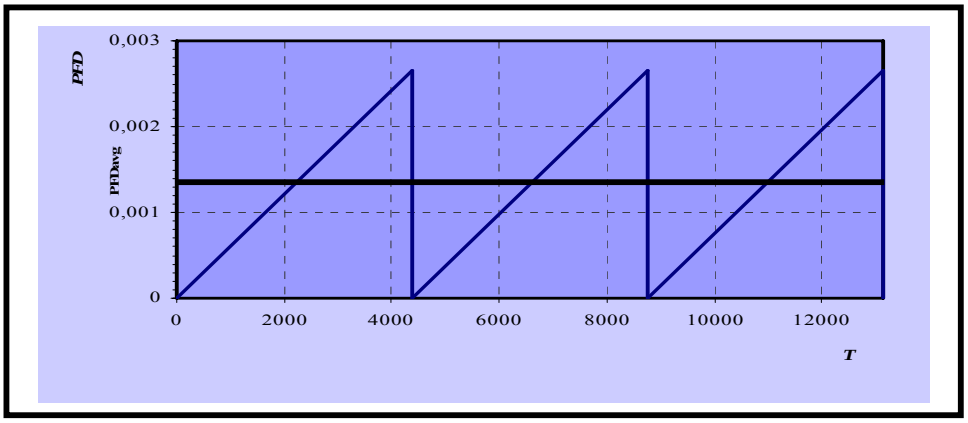

Figure 4. 8 Effet des tests périodiques sur l'indisponibilité du système pour DC=60%

Un examen de ces figures conduit aux commentaires suivants :

- La *PFDavg* qui correspond à la valeur moyenne déduite de la deuxième courbe, est égale à $1{,}33.10^{-3}$, ce qui correspond à un *SIL 2* pour le système.

On constate que la valeur maximale de la *PFD (t)*, pour un *DC=60%* reste dans le domaine *SIL 2*.

Tableau 4.5- Les valeurs des taux de défaillance, et de la MTTF pour DC=90%

DC=90%				
paramètre / composant	λ_D (1/h)	λ_{DD} (1/h)	λ_{DU}(1/h)	MTTR (h)
Transmitteur de débit	1.5×10^{-6}	1.35×10^{-6}	0.15×10^{-6}	9.8
Vanne	2.7×10^{-6}	2.43×10^{-6}	0.27×10^{-6}	12
PLC	10^{-8}	0.9×10^{-8}	0.1×10^{-8}	10.2

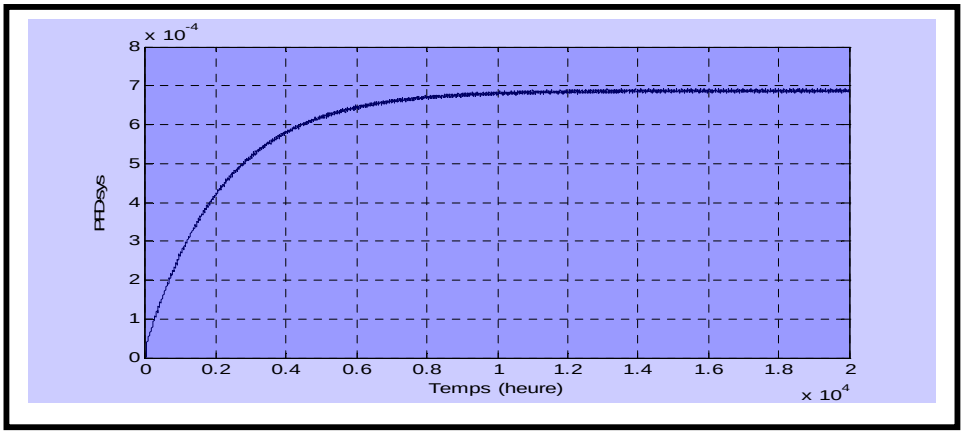

Figure 4.9- Evolution de l'indisponibilité du système en fonction du temps pour DC=90%

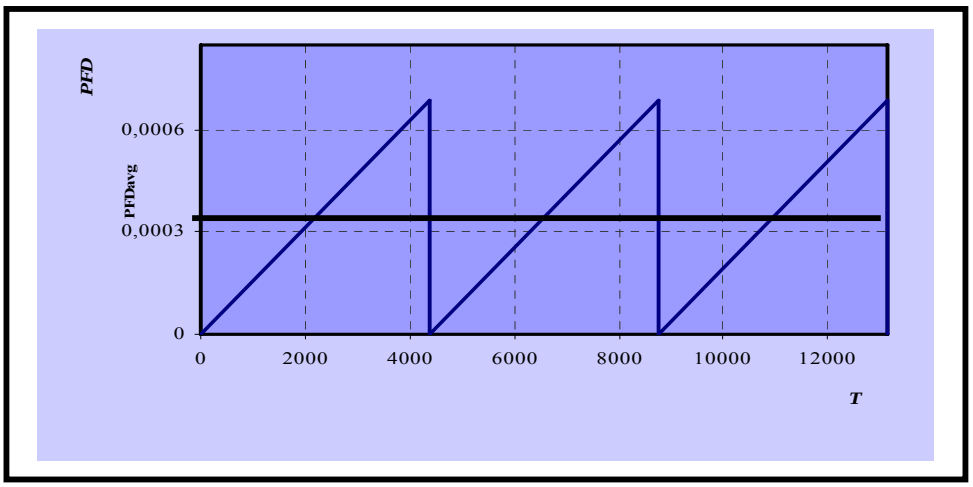

Figure 4. 10 Effet des tests périodiques sur l'indisponibilité du système pour DC=90%

La figure 4. 10 montre l'évolution de la probabilité de défaillance dangereuse instantanée en fonction du temps, pour un DC=90%. La probabilité moyenne de défaillance sur demande est PFD avg= $3{,}4310^{-4}$ qui correspond à un SIL 3. Nous constatons que la variation du taux de couverture de diagnostic implique une variation du niveau de SIL du système.

Les bases de données de fiabilité [OREDA, 2002; CCPS, 2002]. Comme nous l'avons souligné précédemment, est fournissent les bornes inférieures et supérieures, et des valeurs moyennes des taux de défaillance, et de la MTTF des composants. Nous pouvons dire que le taux de défaillance du composant est d'environ m défaillances par an. Dans ce cas, l'information sur le taux de défaillance et de l'MTTF du composant est vague ou floue. L'imperfection de cette information est considérée comme une imprécision qui sera, par exemple, modélisée par un nombre flou.

4.2.3 Application de l'approche Markovienne floue

Toutes les probabilités floues de défaillance et de réparation des composants sont du type triangulaire et caractérisées par les 3 paramètres *mi*, *ai* et *bi*, tel que *mi* est la valeur modale avec $\mu_{PFD}(mi) = 1$, *ai* est la limite à gauche de *mi* et *bi* est la limite à droite de *mi*. Dans le tableau 4.6, nous donnons les valeurs des 3 paramètres *mi*, *ai* et *bi* pour chaque composant du *SIS*.

Les valeurs données sont en conformité avec les valeurs usuelles données dans les bases de données de fiabilité [OREDA, 2002].

Les résultats sont donnés par le tableau 4.6 pour un DC =60%.

Tableau 4.6- Données numériques des taux de défaillance, et de la MTTF pour DC=60%

DC=60%												
paramètre / **composant**	**λ_D (1/h)**			**λ_{DD} (1/h)**			**λ_{DU} (1/h)**			**MTTR (h)**		
	λ_Di	**λ_Dm**	**λ_Ds**	**λ_{DD}i**	**λ_{DD}m**	**λ_{DD}s**	**λ_{DU}i**	**λ_{DU}m**	**λ_{DU}s**	**MTTRi**	**MTTRm**	**MTTRis**
Transmitteur de débit	1,627E-07	2,305E-06	1,046E-05	9,765E-08	1,383E-06	6,278E-06	6,510E-08	9,221E-07	4,185E-06	35.77	6,633	31.92
Vanne	0	5,318E-07	5,268E-05	0	3,191E-07	3,161E-05	0	2,127E-07	2,107E-05	0	2,550	20.24
PLC	1,109E-09	1,581E-08	7,188E-08	6,652E-10	9,487E-09	4,313E-08	4,434E-10	6,325E-09	2,875E-08	0	3,873	49.22

La représentation graphique de λ_D par exemple est donnée par la figure (4.11)

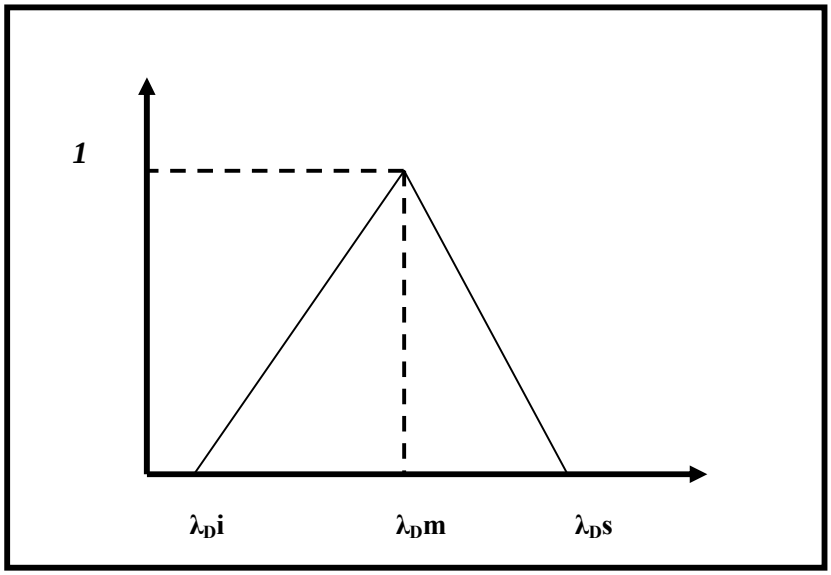

Figure 4.11- Modélisation du taux de défaillance imprécis λ_D par un nombre flou triangulaire

La figure 4.12 donne la distribution de la probabilité floue pour chaque α-coupe et pour un DC=60%.

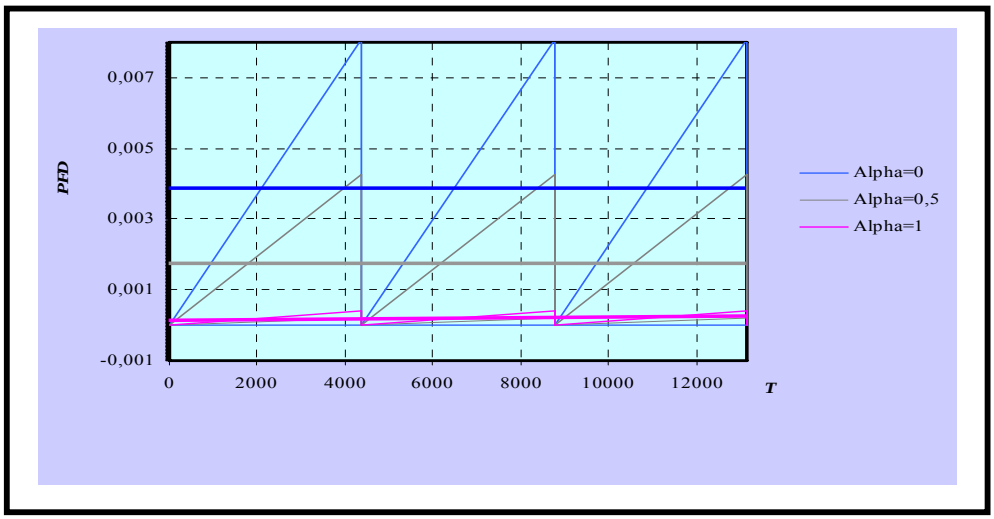

Figure 4. 12. Variations des *PFD* du système pour α=0, α=0.5, et α=1 et DC=60%

-Discussion des résultats

Si on considère $\alpha=0$, $\alpha=0.5$, *et* $\alpha=1$; on peut obtenir 5 courbes floues pour les différentes α−coupes. Pour $\alpha_i=0$, on constate que La probabilité moyenne de défaillance PFDavg=1,042.10^{-5} ce qui donne un SIL4 (PFDavg $\in [10^{-5}, 10^{-4}[$).

Et pour $\alpha_s=0$, la PFDavg=4,041.10^{-3} avec un SIL2 (PFDavg $\in [10^{-3}, 10^{-2}[$,

Pour $\alpha_s=0.5$ La probabilité moyenne de défaillance PFDavg= 2,123.10^{-3}, et lorsque $\alpha_i=0.5$ PFDavg=1,078.10^{-4}, ce qui donne un SIL3 (PFDavg $\in [10^{-4}, 10^{-3}[$) ou selon la tableau 1.1 qui définit le niveau de SIL en fonction de la valeur du PFDavg.

Et pour $\alpha_s=0$, la PFDavg=12,052.10^{-4} avec un SIL3

Nous remarquons qu'il existe une incertitude concernant le niveau de SIL du SIS, c'est pourquoi nous allons utiliser la méthode de défuzzification pour tenter de donner une valeur moyenne.

La probabilité de défaillance sur demande en fonction du temps, après la défuzzification, est fournie à la figure 4.13 à partir de la relation de la défuzzification donnée précédemment dans le chapitre 3 la PFDavg du SIS est égale à 1,526.10^{-3} qui correspond à un SIL2.

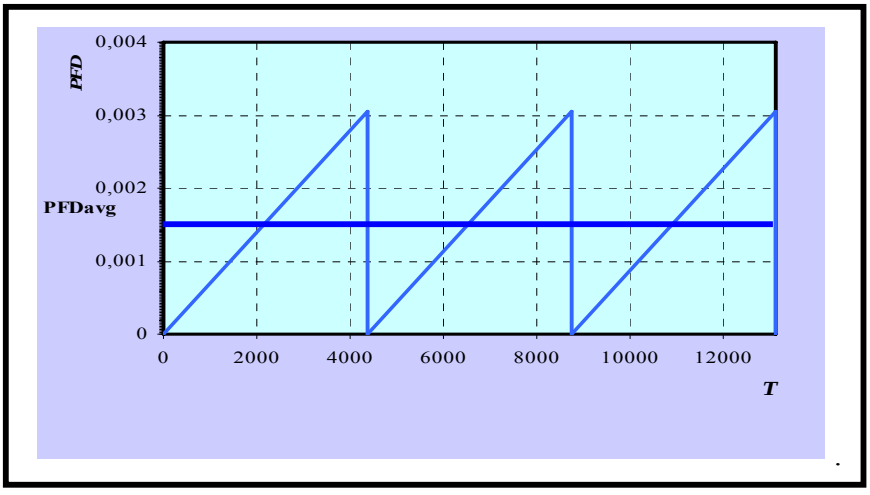

Figure 4. 13. Variation de la *PFD* du système après la defuzzification pour DC=60%

L'ensemble des données numériques pour le DC=90%, est fourni dans le tableau 4.6

Tableau 4.7- données numériques des taux de défaillance, et de la MTTF pour DC=90%

DC=90%												
paramètre	**λ_D (1/h)**			**λ_{DD} (1/h)**			**λ_{DU} (1/h)**			**MTTR (h)**		
composant	**λ_Di**	**λ_Dm**	**λ_Ds**	**λ_{DD}i**	**λ_{DD}m**	**λ_{DD}s**	**λ_{DU}i**	**λ_{DU}m**	**λ_{DU}s**	**MTTRi**	**MTTRm**	**MTTRis**
Transmitteur de débit	1,627E-07	2,305E-06	1,046E-05	1,465E-07	2,075E-06	9,417E-06	1,627E-08	2,305E-07	1,046E-06	35.77	6,633	31.92
Vanne	0	5,318E-07	5,268E-05	0	4,786E-07	4,741E-05	0	5,318E-08	5,268E-06	0	2,550	20.24
PLC	1,109E-09	1,581E-08	7,188E-08	6,652E-10	9,487E-09	4,313E-08	4,434E-10	6,325E-09	2,875E-08	0	3,873	49.22

-Discussion des résultats

La probabilité moyenne de défaillance sur demande est PFDavg= $3{,}324.10^{-3}$dans le cas où α=0s, le SIS dans le domaine de SIL 2, Lorsque α=0i, la probabilité moyenne de défaillance sur demande est égale à $1{,}237.10^{-5}$ et classe le système de SIL4. Nous constatons que l'imprécision amène très rapidement une variation du niveau de SIL du système.

Dans les résultats de la défuzzification (figure 4.15), l'encadrement de la probabilité instantanée de défaillance sur demande est donne PFDavg=$1{,}341.10^{-3}$ ce qui place ce système sur un SIL 2.

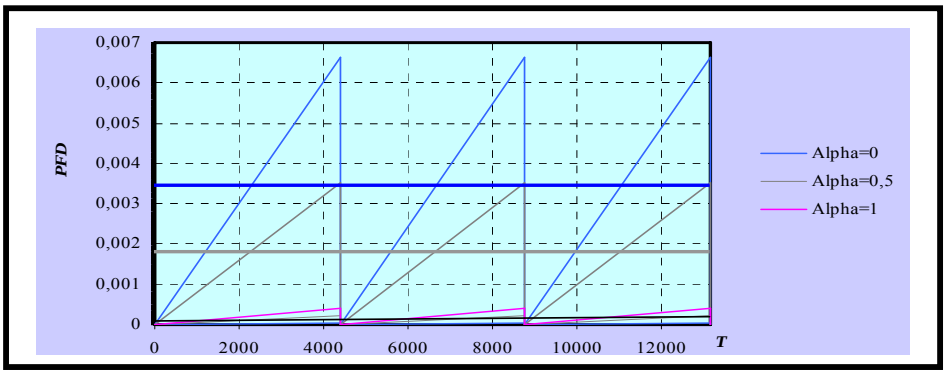

Figure 4. 14. Variations des *PFD* du système pour α=0, α=0.5, et α=1 et DC=90%

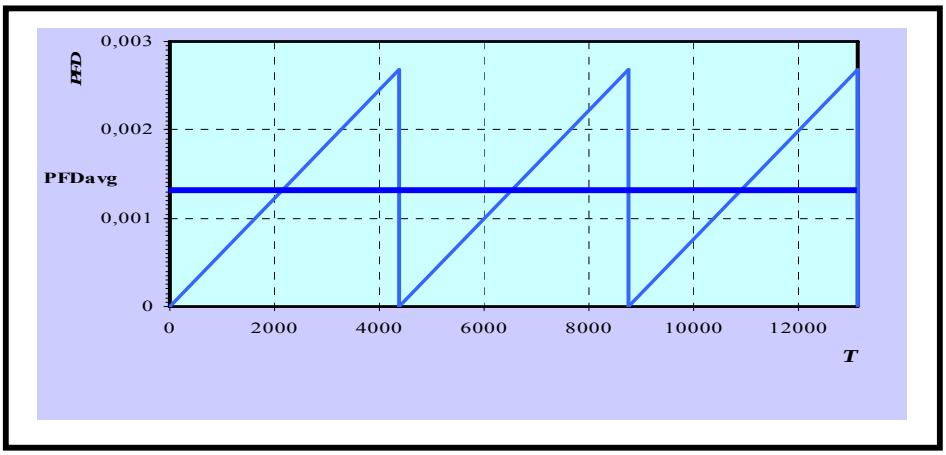

Figure 4. 15. Variation de la *PFD* du système après la défuzzification pour DC=90%

4.2.4 Comparaison des deux modèles flou et conventionnel

En comparant les résultats des deux modèles, nous constatons qui' il y a une différence remarquable. Pour un DC=60%, le modèle classique donne un SIL 2, alors qu'en présence de donnée incertaine, le modèle flou donne un niveau d'intégrité variant entre un SIL2 et un SIL 4. Lorsque le DC=90% le modèle conventionnel donne un SIL 3, et l'approche markovienne floue donne une variation entre SIL2 et SIL 4.

Conclusion

Dans ce chapitre, nous avons montré l'intérêt de l'approche floue, au travers une étude de cas réel. En présence de données imparfaites (prise en compte de l'imprécision des taux de défaillance et de réparation), plusieurs SIL sont possibles pour un même SIS, d'où la non négligence de l'importance de l'imprécision sur la qualifications des SIS et qu'une attention particulière doit êtres portée à leur dimensionnement.

Conclusion générale

Ce mémoire s'inscrit dans le cadre de la maîtrise et l'amélioration de la compréhension des normes sur la sécurité fonctionnelle, notamment en présence de données de fiabilité incertaines et /ou imprécises ainsi que leurs effets dans des problèmes de maîtrise des risques. En outre, c'est principalement la prise en compte de l'imprécision et des incertitudes relatives aux données de fiabilité des composants constituent les SIS.

La représentation par graphes d'états (Markov) a permis la modélisation de l'évolution prévisible du système et la prise en compte des dépendances temporelles et stochastiques. Nous avons examiné, dans un premier temps, l'utilisation de cette méthode pour évaluer la PFDavg des SIS dans le cas où les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation, etc.) peuvent être connues avec précision et validées par le retour d'expérience. On a mise en exergue la différence entre les résultats obtenus par le modèle Markovien et ceux figurant dans la norme IEC 61508 ; la norme est conservative, car donnant des résultats légèrement pessimistes.

Les problèmes réels sont difficilement appréhendés par une connaissance précise des probabilités, alors nous avons présenté, par la suite, la problématique de la prise en compte des incertitudes relatives aux données de fiabilité des composants des SIS. Ce problème de précision dans la connaissance des valeurs de probabilités est connu et appréhendé de diverses manières. Dans notre travail nous avons utilisé les chaînes de Markov floues pour évaluer le PFDavg des SIS et déduire le SIL des SIF exigées pour ces SIS, pour deux architectures types. Ainsi, en utilisant la méthode des $\alpha-$coupes, nous avons obtenu une PFD floue du SIS. Et nous avons montré que cela pouvait entraîner des variations de qualification de son niveau d'intégrité de sécurité.

Enfin, à travers une application à un système opérationnel qu'est un four rebouilleur, des deux modèles markovien (classique, et flou), qui a servi de support à l'illustration de la différance entre les résultats obtenus pas ces deux méthodes. Nous avons trouvé que la PFD calculé par le modèle markovien flou a mis en évidence l'existence d'incertitude concernant le SIL du SIS .La quantification de cette incertitude a souligné le fait que plusieurs SIL étaient probables pour un même SIS à cause de l'imprécision des taux de défaillance et de réparation de ses composants, ce qui imposera plus d'exigence en matière de gestion du risque.

Bibliographie

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

[Bajenesco ,1978]T.Bajenesco, Initiation à la fiabilité électronique, Masson, 1978.

[Bajenesco ,1980]T.Bajenesco, Problèmes de fiabilité des composants électroniques actuels, Masson, 1980.

[Beckman, 2001] L. Beckman, Easily assess complex safety loops. Chem Eng Progr 2001.

[Bellman et Zadeh, 1970] R. E. Bellman and L. Zadeh. Decision-making in a fuzzy environment. Management Science Series, B17:141–164, 1970.

[Berleant et Zhang, 2004] D. Berleant, J. Zhang. Bounding the times to failure of 2-component systems, IEEE Transactions on Reliability, 2004.

[Beugin, 2006]J.Beugin. Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé Thèse de doctorat de l'Université de Valenciennes et du Hainaut-Cambrésis, 2006.

[Bhattacharyya, 1999] M. Bhattacharyya. Fuzzy markovian decision process. Fuzzy Sets and Systems, pages 273–282, 1999.

[Binh et al, 2006]P.T.T. Binh, and T.Q.D.Khoa, Member. IEEEApplication of Fuzzy Markov in Calculating Reliability of Power SystemsP.T.T.Binh and T.Q.D.Khoa are with Faculty of Electrical and Electronics Engineering, Hochiminh University of Technology, Viet Nam1-4244-0288-3/06/$20.00 ©2006 IEEE

[Brini et al, 2006] A. Brini, M. Boughanem, D. Dubois. Réseaux possibilistes pour un modèle de recherche d'information, dans Conférence francophone en Recherche d'Information et Applications, Lyon, 15/03/2006-17/03/2006, 2006.

[Bukowski et Goble, 1995] J. Bukowski, W. Goble. Using Markov models for safety analysis of programmable electronic systems. ISA Trans, 1995.

[Bukowski, 2005] J. Bukowski. A comparison of techniques for computing PFD average. In: Proceedings of the annual reliability and maintainability symposium, 2005.

[Cai, 1996] K. Cai. System failure engineering and fuzzy methodology: An introductory overview, Fuzzy Sets and Systems, 83, 113 133, 1996.

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

[Coit et al, 2004] D. Coit, T. Jin, N. Wattanapongsakorn. System optimization with Component Reliability estimation uncertainty : A multicriteria Approach, IEEE Transactions on Reliability, 53(3), 2004.

[Coolen et Utkin, 2007] F. Coolen, L. Utkin. Imprecise reliability: A concise overview, in Risk, Reliability and Societal Safety, ESREL07, 2007.

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

[ENSPM, 2005] ENSPM,*Condition de fonctionnement et construction des fours tubulaires*., 2005.

[EN 954-1,1996] EN 954-1. Sécurité des machines. Partie des systèmes de commandes relatives à la sécurité. Partie 1 : Principes généraux, décembre 1996.

[Esogbue et Bellman, 1984] A. O. Esogbue and R. E. Bellman. Fuzzy dynamic programming and its extensions. TIMS/Studies in Management Sciences, 20 :147–167, 1984.

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

[Goble et Cheddie, 1998] W. Goble, H. Cheddie. Control system safety evaluation and reliability. US: ISA; 1998.

[Guo, 2004] L. Guo. Software Quality and Reliability Prediction Using Dempster-Shafer Theory, PhD in computer and information science, College of Engineering and Mineral Resources at West Virginia University, Lane Department of Computer Science and Electrical Engineering, Morgantown, West Virginia, 2004.

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

[IEC61508, 2002] IEC 61508. Sécurité fonctionnelle des systèmes électriques/électroniques /électroniques programmables relatifs à la sécurité, partie 6, mars 2002.

[IEC61511, 2003]IEC 61511. Functional safety – Safety instrumented systems for the process industry. International Electrotechnical Commission, Geneva, Switzerland, 2003.

[IEC62061, 2005] IEC62061. Sécurité des machines : Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurités. International Electrotechnical Commission (IEC), 2005.

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

[Innal et al., 2005] F. Innal, Y. Dutuit, M. Djebabra. Analyse critique des formules de base données dans la norme internationnale cei 61508-6. In Proceedings of the QUALITA 2005 Conference, Bordeaux, France, 2005

[ISA-S84, 1996] ISA-S84. Application of safety instrumented systems for process industries, 01.1996.

[ISA 84.00.01, 2004] ISA 84.00.01–2004. Functional Safety Instrumented Systems for the Process Industries, Parts 1–3, 2004.

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

[Kaufmann, 1972] A. Kaufmann. Méthodes et modèles de la recherche opérationnelle. Dunod, France, 1972.

[Kaufman et Gupta, 1991] A. Kaufman and M. M. Gupta. Introduction to Fuzzy Arithmetic Theory and Application. Van Nostrand Reinhold Company, New York, 1991.

[Kosmowski,2006] K. T. Kosmowski. Functional safety concept for hazardous systems and new challenges. Journal of Loss Prevention in the Process Industries 19, pp. 298-305, 2006.

[Kozine et Utkin, 2002] I. Kozine, L. Utkin. Interval valued Finite Markov Chains, Reliable computing, 2002.

[Kruse et al., 1991] R. Kruse, E. Schwecke, J. Heinsohn. Uncertainty and Vagueness in Knowledge-Based Systems. Springer-Verlag, 1991.

[Kurse et al., 1987] R. Kurse, R. Buck-Emden, R. Cordes. Processor power considerationsan application of fuzzy markov chains. Fuzzy Sets and Systems, 21 :289–299, 1987.

[Lamy,2002] P.Lamy. Probabilité de défaillance dangereuse d'un système explications et exemple de calcul. INRS, septembre 2002.

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

[Pages et Gondran, 1980]A.Pages, M. Gondran, Fiabilité des systèmes, Eyrolles, 1980

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

[Rique.2005] B. Rique. Guide d'interprétation et d'application de la norme CEI 61508 et de ses normes dérivées IEC 61511 (ISA-84.01) et IEC 62061. ISA (The instrumentation, Systems, and Automation Society), Section France, 2005.

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

[Sellak et al, 2008] M. Sallak, C. Simon, J-F. Aubry. A Fuzzy Probabilistic Approach for Determining Safety Integrity Level, IEEE Transactions on Fuzzy Systems, 16(1), 2008.

[Singer, 1990] D. Singer .A fuzzy set approach to fault tree and reliability analysis Fuzzy Sets and Systems, 34, 145-155, 1990.

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

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

[Symeonaki et Stamou, 2004] M. A. Symeonaki, G. B. Stamou. Theory of markov systems with fuzzy states. Fuzzy Sets and Systems, 143 :427–445, 2004.

[Tanaka et al, 1983] H. Tanaka, L. Fan, F. Lai, K. Toguchi. Fault tree analysis by fuzzy probability, IEEE Transactions on Reliability, 32, 1983.

[Tanrioven et al., 2004] M. Tanrioven, Q. H. Wub, D. R. Turner, C. Kocatepe, and J. Wang. A new approach to real time reliability analysis of transmission system using fuzzy markov model. Electrical Power and Energy Systems, 26 :821–832, 2004.

[Utkin et Coolen, 2007] L. Utkin. F. Coolen,New metaheuristics. neural & fuzzy techniques in reliability, G. Levitin (Eds), 2007.

[Villemeur, 1980]A.Villemeur, Sûreté de fonctionnement des systèmes industriels, Eyrolles, 1988.

[Zadeh, 1965] L. Zadeh. Fuzzy sets. Information and Control, 8 :338–353, 1965.

[Zadeh, 1998] L. Zadeh. Maximizing sets and fuzzy Markov algorithms. IEEE Trans. on Systems, Man, and Cybernetics, 28 :9–15, 1998.

[Zhang et al, 2003] T. Zhang, W. Long, Y. Sato. Availability of systems with selfdiagnostic components-applying Markov model to IEC 61508-6. Reliab Eng System Saf, 2003.