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

MAGISTER

EN HYGIENE ET SECURITE INDUSTRIELLE

Option : Gestion du Risque

Par

Samir SEKIOU

Ingénieur en Hygiène et Sécurité Industrielle

Diagnostic des Défaillances des Systèmes Instrumentés de Sécurité : Simulation et Etude Expérimentale

---

*Mémoire soutenu le **03/02/2013** devant le jury d'examen composé de :*

M. Djebabra Mébarek,	Professeur à l'Université de Batna	Président
M. Nait-Said Rachid,	Professeur à l'Université de Batna,	Rapporteur
M. Drid Said,	Professeur à l'Université de Batna,	Co-Rapporteur
M. Menacer Arezki,	Maître de Conférences A à l'Université de Biskra,	Examinateur
M. Innal Fares,	Maître de Conférences A à l'Université de Batna,	Examinateur
M. Sal Rachid,	Maître Assistant A à l'Université de Batna,	Membre Invité

2013

Dédicace

Je dédié ce travail A

Mes parents et toute la famille.

A tous mes amis.

A ceux qui m'aiment.

A ceux qui j'aime.

Remerciements

Le travail présenté dans ce mémoire a été mené au sein de laboratoire (LSPIE) et le 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, Professeur 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 Said DRID, Professeur à l'Université de Batna, d'avoir accepté de co-diriger ce travail avec autant d'effort, d'attention et de patience jusqu'à son achèvement. Il m'a beaucoup enseigné et aidé à enrichir mes connaissances dans le domaine de diagnostic et de la simulation en me donnant des conseils sages et significatifs.

Aussi, j'exprime mes profonds remerciements à Mme Nouara OUZRAOUI, Maître Assistante « A » à l'université de Batna, Mr Mouloud BOURARECHE, Maitre Assistant « A » à l'université de Batna et Mr Choayb DJEDDI pour leurs Soutiens physiques et moraux.

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 Module « 0 » au niveau de Hassi R'mel : Monsieur Sid Ahmed, Salim, Amar et toutes l'équipe d'intervention et salle de contrôle 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 Fares INNAL, Maître de Conférences A à l'Université de Batna, Monsieur Arezki MENACER, Maître de Conférences A à l'Université de Biskra et Monsieur Rachid SAL, Maître Assistant *A 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.

Tables des matières

Acronymes ..... **viii**

Table des figures ..... **xiii**

Liste des tableaux ..... **xvi**

Introduction générale 1

1 Problématique 1

2 Objectif 2

3 Organisation du mémoire 2

Chapitre 1 Diagnostic des défauts

1.1 Introduction 4

1.2 Terminologie et définition 5

1.2.1 Défaut 5

1.2.2 Dégradation 5

1.2.3 Défaillance 6

1.2.4 Panne 6

1.2.5 Symptôme,Observation,Mesure 6

1.2.6 Détection de défaut 7

1.2.7 Localisation de défaut 7

1.2.8 Identification de défaut 8

1.3 Diagnostic 10

1.4 l'interne du diagnostic 10

1.5 Organisation générale de la procédure de diagnostic 11

1.6 Surveillance, diagnostic et supervision 13

1.7 Place et procédure de détection 14

1.8 Critères de performance d'un système de diagnostic 16

1.9 La redondance pour le diagnostic 16

1.10 Classification des méthodes de diagnostic 18

1.10.1 Méthode externe (méthode sans modèle) 19
1.10.1.1 Reconnaissance des formes 20
1.10.1.2 Réseaux de neurones artificiels 20
1.10.1.3 Système experts 21
1.10.2 Méthodes internes (méthodes avec modèle) 21
1.10.2.1 Méthodes à base de modèle quantitatif 24
1.10.2.2 Méthodes à base de modèle qualitatif 25
1.10.2.3 Méthodes mixtes 25
1.11 Conclusion 26

Chapitre 2 Système instrumenté de sécurité

2.1 Introduction 27
2.2 Notion de sécurité 28
2.2.1 Principes généraux de protection 28
2.2.2 Sécurité fonctionnelle 29
2.3 Cadre normatif 30
2.3.1 Norme CEI 61508 30
2.3.2 Norme CEI 61511 33
2.3.3 Norme CEI 62061 35
2.3.4 Norme ISA 84 35
2.4 Systèmes instrumentée de sécurité 36
2.4.1 Définition d'un SIS 36
2.4.2 Fonction instrumentée de sécurité 37
2.4.3 Propriétés d'un SIS 38
2.4.4 Composition d'un SIS 39
2.4.5 Rodondance au sein d'un SIS 42
2.4.6 Tests de système instrumenté de sécurité 43
2.4.6.1 Test de diagnostic 43
2.4.6.2 Proof test 44
2.4.6.3 L'avantage des tests dans les SIS 46
2.4.6.4 Test partiel de la course de vanne 46

2.4.7. Niveau d'intégrité de sécurité....48
2.4.7.1 Paramêtres influant sur le calcul de SIL....50
2.4.7.2 Méthodes de détermination de SIL....51
2.5 Réduction des risques par les SIS....51
2.5.1 Les SIS comme couche de protection....51
2.5.2 Réduction des risques....53
2.6 Problèmes typiques des SIS....53
2.7 Classification des défaillances....54
2.7.1 Classifications retenue dans la norme....54
2.7.2 Classifications proposée par SINTEF....57
2.8 Contraintes architecturales....58
2.9 Conclusion....59
Chapitre 3 Evaluation de l'indisponibilité des systèmes instrumentés de sécurité par le modèle Makovien
3.1 Introduction....61
3.2 **Architecture 1001**....62
3.2.1 Détermination du taux de réparation....63
3.2.2 Détermination de la disponibilité de l'architecture 1oo1....65
3.2.3 Détermination de la durée moyenne globale d'indisponibilité....67
3.2.4 Détermination de l'indisponibilité moyenne PFD_{avg} du cannal....68
3.3 **Architecture 1002**....69
3.3.1 Détermination du taux de réparation....70
3.3.2 Modèle markovien 1oo2....71
3.3.3 Détermination de la disponibilité de l'architecture 1oo2....71
3.4 **Architecture 2oo3**....72
3.4.1 Détermination de la disponibilité de l'architecture 2oo3....74
3.5 **Evaluation des SIL d'un système opérationnel : Four rebouilleur**....75
3.5.1 Rôle du four H401....75
3.5.2 Zones de four....76

3.5.2.1 Zone de radiation (rayonnement.....76
3.5.2.2 Zone de convection.....76
3.5.3 Construction de four H401 76
3.5.3.1 Faisceaux tubulaires (Serpentin.....76
3.5.3.2 Brûleurs 76
3.5.3.3 Les pilotes.....76
3.5.3.4 Cheminée.....76
3.5.3.5 Registre.....76
3.5.4 La décomposition structurelle et fonctionnelle du système four H401.....78
3.5.4.1 Sous système d'alimentation 78
3.5.4.2 Sous système de contrôle.....79
3.5.4.3 Sous-système d'alarme.....81
3.5.4.4 Sous-système d'arrêt d'urgence (SIS) 82
3.5.4.4.1 Les capteurs.....82
3.5.4.4.2 Unité de traitement PLC (TRICONEX)…… 83
3.5.4.4.3 Les actionneurs.....84
3.5.5 Calcul de PFDavg du SIS 84
3.5.5.1 Par les équations de modèle Markovien.....84
3.5.5.2 Calcul du PFDavg par les équations simplifiées 86
3.5.5.3 Comparaison des résultats……86
3.6 Conclusion ……..87

Chapitre 4 Simulation et Etude Expérimentale

4.1 Introduction 88
4.2 Présentation détaillée du système.....89
4.2.1 Décomposition du système.....89
4.2.2 Sous système d'arrêt d'urgence (SIS) 89
4.3 Simulation et Interprétation.....90
4.3.1 Système avec un seul capteur.....90
4.3.1.1 Mode de défaillance des composants du SIS …..…….90

4.3.1.2 Modèle de simulation du système à un seul capteur 90
4.3.1.3 Résultats et Interprétation.....91
4.3.2 Simulation du système avec deux capteurs 97
4.3.2.1 Modèle de simulation du système par simulink 97
4.3.2.2 Résultats et Interprétation.....98
4.4 Etude Expérimentale.....100
4.4.1 Présentation du banc d'essais 100
4.4.2 Résultats et interprétation 102
4.5 Conclusion.....107
Conclusion Générale 109
Annexe……...111
Bibliographie.....118

Acronymes

A Disponibilité

DC Diagnostic coverage (couverture de diagnostic)

DCS Distributed Controller System

E/E/PE Electriques/Electroniques/Electroniques Programmables de sécurité.

ESD Emergency Shut Down (système d'arrêt d'urgence)

FAL Flow Alarm Low(Alarm de Bas Débit)

FALL Flow Alarm Low Low (Alarm de Trés Bas Debit)

FF Failure Frequency (Frequance de Défaillance)

FV Flow Valve (Vane de Débit)

FT Flow Transmitter (Transmiteur de Débit)

IEC International Electrotechnical Comission (Commission International d'Electronique)

ISA Instrument Society of America (

ISO International Organization for Standardization (Organisation International de Standardisation)

MDT Mean Down Time (Durée Moyenne de non Fonctionnement)

MTTR Mean Time To Restoration (Durée Moyenne de Réparation)

PAHH/LL Pressure Alarm High High/Low Low(Alarm de Trés Haute /Trés Bas Pression)

PAH Pressure Alarm High (Alarm de Haute Pression)

PAL Pressure Alarm Low (Alarm de Bas Pression)

P_{CC} Probabilité de défaillance de cause commune

PFD Probability of Failure on Demand (Probabilité de Défaillance à la Demande)

PFH Probability of Failure per Hour (Probabilité de Défaillance par Heure)

PFD_{avg} Average Probability of Failure on Demand (Probabilité de Défaillance moyenne à la Demande)

PLC Programmable Logic Controller (

PSH/L Pressure Switch High/Low (switch de Pression Haute/Bas)

SIS Safety Instrumented System (Système Instrumenté de Sécurité)

SIF Safety Instrumented Function (Fonction Instrumenté de Sécurité)

SIL Safety Integrity Level (Niveau d'Intégrité de Sécurité)

SRECS Systèmes de Commande Électriques Relatifs à la Sécurité de machines

TAH Temperature Alarm High (Alarmde Haute Temperature)

TAHH Temperature Alarm High High (Alarmde Trés Haute Temperature)

T_1	Proof-test interval (Intervalle de Proof Test)
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 (Indicateur de Pression)
TV	Temperature Valve (Vanne de Temperature)
λ	Taux de défaillance d'un canal
μ	Taux de réparation d'un canal
λ_D	Taux de défaillance dangereuse du canal
λ_{DD}	Taux de défaillance dangereuse détectée du canal
λ_{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 $\lambda_D(t)$

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.

Table des Figures

Figure 1.1. *Difficulté de localisation des défauts* 8
Figure 1.2. *Biais de capteur* 9
Figure 1.3. *Dérive capteur* 9
Figure 1.4. *Valeur aberrante* 9
Figure 1.5. *Les différentes étapes du diagnostic industriel* 12
Figure 1 .6. *Principe du diagnostic des systèmes commandés* 13
Figure 1.7. *Procédure de détection et d'isolation des défauts*....15
Figure 1.8. *Place de la détection dans le diagnostic FDI* 15
Figure 1.9. *Redondance physique*....17
Figure 1.10. *Classifications des méthodologies de diagnostic industriel*....18
Figure 1.11. *Exemple montrant les vecteurs formes dans un espace de dimension 2* 20
Figure 1.12. *Diagnostic à base de modèles* 23
Figure 1.13. *Principe de génération des résidus* 24
Figure 2.1. *Structure générale de la norme IEC 61508* 31
Figure 2.2. *Norme CEI 61508 et normes dérivées* 32
Figure 2.3. *Structure générale de la norme IEC 61511* 34
Figure 2.4. *Fonction instrumentée de sécurité*....37
Figure 2.5. *Exemple de fonction instrumenté de sécurité* 38
Figure 2.6. *Schéma d'un SIS*....39
Figure 2.7. *Schéma d'un SIS effectuant plusieurs taches* 41
Figure 2.8. *Schéma d'un SIS recevant plusieurs informations*....41
Figure 2.9. *Proportion de défaillances selon un exemple illustré dans la norme* 44
Figure 2.10. *Impact des tests périodiques sur la disponibilité*....46
Figure 2.11. *Concept de couches de protection*....52
Figure 2.12. *Réduction nécessaire du risque réalisée par un seul SIS*....53
Figure 2.13. *Causes primaires des défaillances des systèmes de commande* 53
Figure 2.14. *Classification des défaillances selon leurs causes*....55
Figure 2.15. *Typologie des défaillances selon la norme CEI 61508*....55
Figure 2.16. *Classification des défaillances selon SINTEF* 57
Figure 3.1. *Diagrammes blocs physique et de fiabilité 1oo1*....62

Figure 3.2. *Modèle markovien multi-phases de l'architecture 1001*.....62
Figure 3.3. *Modèle markovien continu de l'architecture 1001* 63
Figure 3.4. *Processus d'occurrence d'une défaillance non détectée sur [0, T_1]* 63
Figure 3.5. *Graphe de Markov 1oo1* 65
Figure 3.6. *Diagrammes blocs physique et de fiabilité 1oo2* 69
Figure 3.7. *Modèle markovien multi-phases de l'architecture 1002*.....69
Figure 3.8. *Modèle markovien continu de l'architecture 1002* 70
Figure 3.9. *Graphe de Markov approché de l'architecture 1002* 71
Figure 3.10. *Diagrammes blocs physique de fiabilité 2003* 72
Figure 3.11. *Modèle markovien continu de l'architecture 2003* 73
Figure 3.12. *Modèle markovien approché de l'architecture 2003* 73
Figure 3.13. *Echauffement de liquide par le four H401*.....75
Figure 3.14. *Le Four Rebouilleur H401* 77
Figure 3.15. *Système de contrôle dans le four H401*.....80
Figure 3.16. *Automate programmable PLC* 83
Figure 3.17. *Architecture 2003 de PLC*.....83
Figure 3.18. *Architecture 1002 des Vannes*.....84
Figure 3.19. *Schéma simple du SIS*.....84
Figure 3.20. *Calcul des PFDavg par les équations de modèle Markovien* 85
Figure 4.1. *Schéma des sous systèmes d'un four rebouilleur*.....89
Figure 4.2. *Schéma simple du SIS*.....89
Figure 4.3. *Schéma de simulink du système avec un seul capteur*.....90
Figure 4.4.*Variation de la température en fonction du temps dans le cas normal et défaillant* 91
Figure 4.5. *Défauts des modules d'I/O* 92
Figure 4.6. *Fonctionnement sans défauts* 92
Figure 4.7. *Défaillance de PLC1* 93
Figure 4.8. *Défaillance de PLC1 et PLC2*.....93
Figure 4.9. *Défaillance de PLC1, PLC2 et PLC3* 94
Figure 4.10. *Variations de température sans et avec défaillance du PLC (SIS*.....95
Figure 4.11. *Variations de température sans et avec défaillance des électrovannes*.....95
Figure 4.12. *Variations de température sans et avec défaillance du capteur* 96
Figure 4.13. *Schéma de simulation du système à deux capteurs*.....97
Figure 4.14. *Schéma du SIS à deux capteurs*…….98

Figure 4.15. *Système sans défaut*.....98
Figure 4.16. *Système défaillant*.....98
Figure 4.17. *Cas de défaillance du Capteur 2 du SIS* 98
Figure 4.18. *Cas de défaillance du Capteur 2 (SIS) et du capteur 1 (DCS)*.....99
Figure 4.19. *Cas de défaillance du capteur1 (DCS) et du capteur 2 (PLC)*.....99
Figure 4.20. *Défaillance du système puis défaillance du capteur2 du PLC*.....100
Figure 4.21. *Défaillance du capteur2 du PLC puis défaillance du système*.....100
Figure 4.22. *Synoptique du banc d'essais à deux capteurs*..... 102
Figure 4.23. *Système sans défaut*..... 103
Figure 4.24. *Système défaillant*..... 103
Figure 4.25. *Défaillance du capteur 1 après défaillance du Système* 103
Figure 4.26. *Défaillance du capteur 1 avant défaillance du Système* 104
Figure 4.27. *Défaillance de capteur 2(PLC) et Capteur 1(DCS*..... 104
Figure 4.28. *Défaillance du capteur 2 (PLC*..... 104
Figure 4.29. *Défaillance du capteur 2-PLC et du Capteur 1-DCS*..... 105
Figure 4.30. *Défaillance du capteur 2, puis du Système, puis du capteur 1*..... 105
Figure 4.31. *Défaillance du capteur 2, puis du capteur 1, puis du Système* 106
Figure 4.32. *Défaillance du PLC 1*..... 106
Figure 4.33. *Défaillance des PLC 1 et 2*..... 106
Figure 4.34. *Défaillance des PLC 1, 2 et 3*..... 107
Figure 4.35. *Défaillance des Vannes (Fermeture intempestive*..... 107

Liste des Tableaux

Tableau 2.1. *Proportion de défaillances relatives aux constituants d'un SIS* 47
Tableau 2.2. *Niveaux d'intégrité de sécurité : Probabilité de défaillances lors d'une sollicitation* 49
Tableau 2.3. *Niveaux d'intégrité de sécurité : Probabilité de défaillances dangereuses de la SIF* 49
Tableau 2.4. *Contraintes architecturales sur les SIS du type A* 58
Tableau 2.5. *Contraintes architecturales sur les SIS du type B* 59
Tableau 3.1. *Etats de système* 65
Tableau 3.2. *PFDavg de l'architecture 1001* 68
Tableau 3.3. *PFDavg de l'architecture 1002* 72
Tableau 3.4. *PFDavg de l'architecture 2003* 74
Tableau 3.5. *Sous-système d'alimentation* 78
Tableau 3.6. *Sous-système de contrôle* 79
Tableau 3.7. *Sous-système d'alarme* 81
Tableau 3.8. *Calcul des PFDavg par les équations de modèle markovien* T_1*=4380h* 86
Tableau 3.9. *Calcul des PFDavg par les équations simplifiées* T_1*=4380h* 86
Tableau 4.1. *Principaux modes de défaillance des composants* 90
Tableau 4.2. *Principaux éléments du banc d'essais*.....101

Introduction générale

1. Problématique

Les Systèmes Instrumentés de Sécurité (SIS), décrits par les normes IEC 61508 et IEC 61511, jouent un rôle primordial dans la prévention des accidents pouvant survenir dans les systèmes industriels. Ils entrent en action lorsque le process se trouve dans des conditions anormales et qu'une situation dangereuse risque de se développer. Les SIS sont des associations de capteurs, d'unité de traitement et d'actionneurs, ayant pour objectif de remplir des fonctions de sécurité.

L'indisponibilité des SIS compromet la sûreté du système global. Par suite, l'évaluation de cette indisponibilité en terme probabiliste et l'analyse des défaillances des éléments d'un SIS et leurs effets sur ses fonctions s'avère nécessaire. Ces défaillances sont classées par catégorie, selon qu'elles donnent lieu à une défaillance sûre du système de sécurité (ex. ce dernier arrête le process en l'absence de toute anomalie) ou à une défaillance dangereuse empêchant le système de sécurité de répondre en présence d'une situation dangereuse. Une autre catégorisation est celle des défaillances détectées et non détectées par le système. La détection se fait par un diagnostic automatique intégré et le niveau de diagnostic est mesuré par le facteur de couverture de diagnostic (i.e. le taux des défaillances qui peuvent être détectées automatiquement par le système) qui a un impact important sur la performance des SIS.

A nos jours, le besoin est bien exprimé pour assurer la détection des modes de défaillances dangereuses. Ce besoin est d'autant plus grand qu'il s'agit de SIS utilisant la technologie des unités de traitement programmables (Programmable Electronic System, PES).

Le diagnostic peut être actif ou passif. Le diagnostic actif contrôle continuellement la partie (hardware/software) qui devrait être diagnostiquée pour assurée une performance satisfaisante du SIS, même en l'absence d'une déviation anormale. Le diagnostic passif contrôle seulement cette partie quand un événement anormal ou un test du système se réalise. Il est recommandé que certaines formes de diagnostic actif soient appliquées quand un SIS a un niveau d'intégrité élevé et utilisant un PES. Initialement, les concepteurs des PES réalisent un diagnostic interne pour fournir un niveau de certitude que le PES est opérationnel. Les programmes de diagnostic utilisés sont connus sous le nom de « watchdog ».

La complexité des architectures des SIS faits que le diagnostic de leurs défaillances par simulation sur ordinateur devient un outil indispensable. La simulation trouve une application directe dans l'amélioration des performances des SIS. Plus spécifiquement, la simulation en temps réel se révèlera importante pour confirmer que le SIS atteignent les spécifications du niveau d'intégrité exigé en présence de danger. Une simple simulation peut être exécutée sur un ordinateur connecté à un SIS.

2. Objectif

Le but essentiel de ce mémoire est d'étudier par simulation puis par validation expérimentale le diagnostic des défaillances des SIS.

3. Organisation du mémoire

Le premier chapitre présente les principes fondamentaux sur lesquels repose le diagnostic des défauts des systèmes physiques. L'objectif de ce chapitre est de présenter les techniques les plus courantes en diagnostic d'équipements industriels. Dans la littérature associée à ce domaine, on peut trouver plusieurs définitions quelque fois divergentes. C'est pourquoi nous nous positionnons dans la première partie de ce chapitre, en donnant des définitions des mots clés qui sont utiles pour la compréhension de ce mémoire.

Le second 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 troisième chapitre, on s'intéressera à l'évaluation de la performance des systèmes instrumentés de sécurité où les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation, etc.) sont des valeurs pouvant être connues et validées par retour d'expérience.

Dans le dernier chapitre, on présentera les résultats de simulation des défauts dans un SIS, puis les résultats expérimentaux issus d'une étude sur dSPACE 1l03 DS.

Ce travail de mémoire sera clôturé par une conclusion générale qui donnera une synthèse du travail effectué et les principaux résultats obtenus ainsi que les perspectives envisagées.

1

Diagnostic des défauts :

Définition et Terminologie

1.1. Introduction :

Les progrès récents des sciences ont entraîné un changement considérable dans divers secteurs industriels. Les industriels modernes s'équipent de plus en plus avec des systèmes automatiques complexes, afin d'améliorer la productivité et la qualité de leurs produits tout en réduisant leur coût de traitement. Les équipements modernes sont sujets aux défaillances. Ces dernières peuvent réduire considérablement la production et même dans certain cas, mettre en péril la vie des personnes et l'équilibre de l'environnement. Il est alors légitime pour ces industriels d'acquérir une technicité efficace de supervision, dotée d'un outil de diagnostic adapté afin de limiter les conséquences engendrées par les défaillances et d'améliorer la sécurité des personnels assurant ainsi une fiabilité et une disponibilité accrues de leurs outils de production.

Le diagnostic, en exploitant les données recueillies sur un système et sur son environnement, permet de déterminer le mode des défaillances dans lequel se trouve ce système et de localiser les éléments responsables en explicitant les causes qu'ils ont induit [MOH 07].Toutes ces informations, apportées par le diagnostic, sont très utiles pour prendre une décision, qui est soit de maintenir le système sous le même mode de fonctionnement si celui-ci est normal, soit de corriger ce mode ou bien d'arrêter le système s'il est interdit ou dangereux.

La recherche dans le domaine du diagnostic industriel a connu une évolution accélérée durant ces deux dernières décennies, que se soit sur le plan théorique ou sur le plan pratique. L'intérêt croissant porté aux problèmes du diagnostic tient du fait que l'une des principales préoccupations du milieu industriel est l'augmentation de l'efficacité et du rendement, en

termes de coûts et de délais [BEN 05]. De plus, le diagnostic trouve des applications diverses dans tous les secteurs tels que l'industrie, la médecine, l'administration,…etc. Ainsi, avec cet intérêt accru, s'est développée une littérature abondante dédiée au diagnostic industriel. De nombreux ouvrages de référence parmi lesquels [DUB 90] [ZWI 95],… consacrés à la résolution de divers problèmes, ont été publiés.

Ce chapitre vise à rappeler la terminologie utilisée dans la littérature. Il introduit en premier lieu, le diagnostic et son intérêt dans le domaine industriel, La procédure de diagnostic de défaillances et de dégradations susceptibles d'affecter les différentes entités d'un processus industriel. Il met en place les concepts de surveillance, de diagnostic et de supervision et situe la place de la détection dans le diagnostic FDI (Fault Detection and Isolation). Une classification des méthodes de diagnostic en deux catégories est adoptée : les méthodes internes (à base de modèle) et les méthodes externes (sans modèle).

1.2. Terminologie et définitions :

La diversité des définitions trouvées dans différents travaux fait que nous avons estimé important d'établir un lexique sur les termes qui seront utiles pour la compréhension du présent mémoire. Nous présentons ici quelques définitions prise des références suivantes : [DER 09], [RIP 99], [ROD 05], [ZWI 95].

1.2.1. Défaut :

C'est une déviation du système par rapport à son comportement normal, qui ne l'empêche pas de remplir sa fonction. Un défaut est donc une anomalie qui concerne une ou plusieurs propriétés du système, pouvant aboutir à une défaillance et parfois même à une panne [DER 09].

Les défauts sont des évènements qui apparaissent à différents endroits du système. Dans la littérature, les défauts sont classés en fonction de leur localisation. Définissant alors des types de défauts susceptibles d'altérer le bon fonctionnement d'un système. Celui-ci peut être divisé en trois catégories distinctes [RIP 99] :

- les biais,
- les dérives,
- les valeurs aberrantes.

Ces catégories seront détaillées dans la suite de ce chapitre.

1.2.2. Dégradation : tout état qui se caractérise par une évolution irréversible des caractéristiques d'un système est une dégradation. La dégradation peut être liée à des facteurs directs, tels que l'usage, le temps …, ou à des facteurs indirects, tels que l'humidité, la

température …. La dégradation peut aboutir à une défaillance, quand les performances du système sont en dessous d'un seuil d'arrêt défini par les spécfications fonctionnelles [DER 09].

1.2.3. Défaillance : une défaillance est une anomalie altérant ou empêchant l'aptitude d'une unité fonctionnelle à accomplir la fonction souhaitée. Une défaillance correspond à un passage d'un état à un autre, par opposition à une panne qui est un état. Par abus de langage, cet état de panne on pourra l'appeler mode de défaillance [DER 09].

Une défaillance implique l'existence d'un défaut, puisqu'elle aboutit à un écart entre la caractéristique mesurée et la caractéristique de référence. Inversement, un défaut ne conduit pas nécessairement à une défaillance. En effet, le système peut très bien conserver son aptitude à assurer une fonction requise, si les défauts qui l'affectent n'ont pas d'impacts significatifs sur la mission. Si une défaillance peut conduire à une cessation de l'exécution de la mission principale du système, ce dernier est déclaré en état de panne. Ainsi, la panne est toujours le résultat d'une défaillance.

On peut classer les défaillances selon leur degré de sévérité par :

- **Défaillance critique** : nécessite une intervention d'urgence.
- **Défaillance significative** : nécessite un processus de traitement.
- **Défaillance absorbable** : pouvant être ignorée dans un premier temps.

1.2.4. Panne : c'est la conséquence d'une défaillance affectant le système, aboutissant à une interruption permanente de capacité à remplir une fonction requise et pouvant provoquer son arrêt complet. C'est la cause de l'apparition des symptômes.

Deux types de pannes peuvent être distingués :

- les pannes permanentes : une fois la panne est produite, elle nécessite une action de réparation.
- les pannes intermittentes : le système peut retrouver son fonctionnement nominal après l'occurrence de la panne. Une panne intermittente est généralement le résultat d'une dégradation partielle et progressive d'un composant du système, pouvant aboutir à une panne permanente.

1.2.5. Symptôme, Observation, Mesure [DER 09]**:**

Un symptôme correspond à une ou plusieurs observations qui révèlent d'un dysfonctionnement. Il s'agit d'un effet qui est la conséquence d'un comportement anormal.

Une observation est une information obtenue à partir du comportement ou du fonctionnement réel du système.

Une mesure est une observation élémentaire du fait qu'elle reflète une et une seule grandeur physique. Elle est représentée par une variable dont le contenu est l'image d'une grandeur physique. Son obtention s'effectue par l'intermédiaire de capteurs.

1.2.6. Détection de défaut :

Le module de détection permet de déterminer si le système physique fonctionne normalement et a pour objectif de signaler la présence d'un défaut en comparant le comportement courant du système avec celui donné pour référence. Malheureusement, il est impossible en pratique d'obtenir un comportement de référence scrupuleusement identique à celui du système en fonctionnement normal. À cause de cette différence, les outils de détection sont généralement de nature statistique (tests d'hypothèses).Un risque d'erreur subsiste donc. Détecter un défaut inexistant peut provoquer un arrêt inutile et générer une perte de confiance des opérateurs (probabilité de fausse détection). A l'opposé, omettre un défaut, qui peut entraîner ultérieurement une panne, est préjudiciable (probabilité de non- détection). Il subsiste donc nécessairement un compromis induisant la recherche d'un réglage permettant de minimiser ces probabilités. A ce stade, l'objectif est de déterminer si un événement affectant le système est le signe d'une anomalie et par conséquent de distinguer les évènements qualifiés de normaux (réaction de la commande pour rejeter une perturbation, action d'un opérateur) de ceux qui ne le sont pas (défaut) [ADR 00].

1.2.7. Localisation de défaut :

Il s'agit de localiser le sous-système affecté par le défaut détecté, responsable de la défaillance du système. La localisation consiste, en effet, à remonter les symptômes pour retrouver l'ensemble des éléments défaillants. Ce problème est difficile à résoudre. En effet, il est possible de déterminer une défaillance, ou une panne, résultant d'un défaut .par contre, le problème inverse, comme il est plus difficile à résoudre, puisque une panne peut résulter d'un ou plusieurs défauts, comme il est montré dans la figure (1.1).

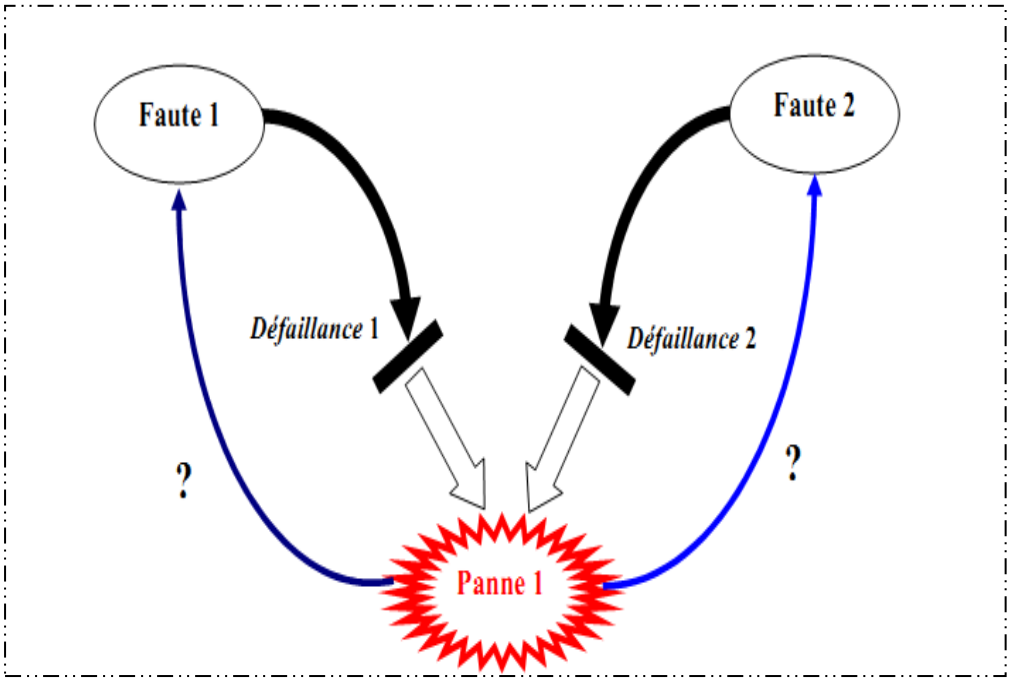


Figure 1.1. **Difficulté de localisation des défauts** [ADR 00].

1.2.8. Identification de défaut :

Le module d'identification a pour but de caractériser le défaut en durée et en amplitude afin de le classifier par types et degrés de sévérité. Ainsi, il peut servir à assurer le suivi de son évolution, ce qui est fort utile dans le cas d'un changement de comportement lent dû au vieillissement et à l'usure. De plus, ce module peut comprendre une procédure visant à déterminer la cause du défaut, c'est-à-dire son origine [ADR 00].

Cette partie d'identification du défaut est la dernière phase de la procédure de diagnostic. Lorsque l'on conçoit un système de diagnostic, la première question que l'on doit se poser, est de savoir ce que l'on veut détecter. Cela revient à déterminer le type de dysfonctionnement que l'on veut diagnostiquer et donc définir le type de défauts susceptibles d'altérer le bon fonctionnement d'un système. Celui-ci peut être divisé en trois catégories distinctes : de biais, de dérive, ou de valeur aberrante [BAR 10].

Un biais correspond à un saut brutal du signal. La figure (1.2) simule un biais d'amplitude 5 à l'instant 50 appliqué à un signal bruité. C'est le cas pour des capteurs dont un composant élémentaire est défaillant. Ce défaut affecte le système d'une manière permanente et peut occasionner de graves dégâts.

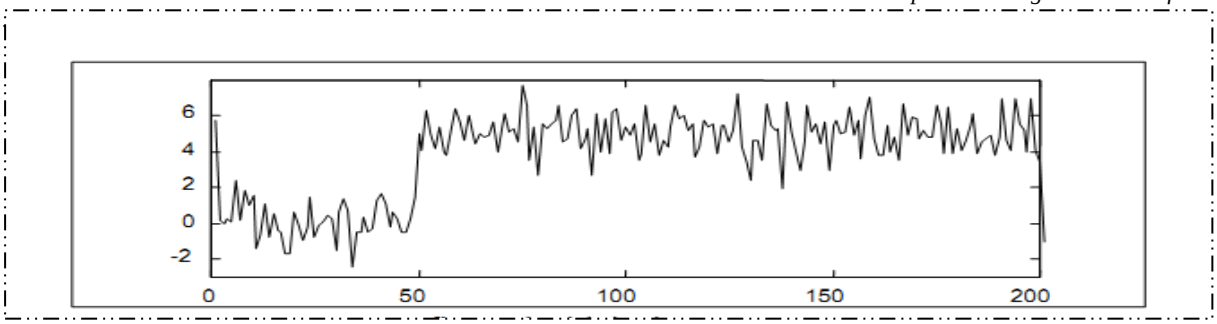


Figure 1.2. Biais de capteur [RIP 99]

Une dérive se manifeste par une croissance lente et continue du signal, et donc un éloignement progressif de sa valeur nominale. Ces défauts permanents sont plus difficiles à détecter à leur origine du fait de leur faible amplitude et de leur lente évolution. La figure (1.3) montre une dérive capteur affectant le système au temps 50 avec une dérive de 0.01 par unité de temps. Par exemple, certains capteurs peuvent présenter une dérive de plus de 10% après 1 an d'activité, à cause d'un échauffement intensif ou d'un encrassement.

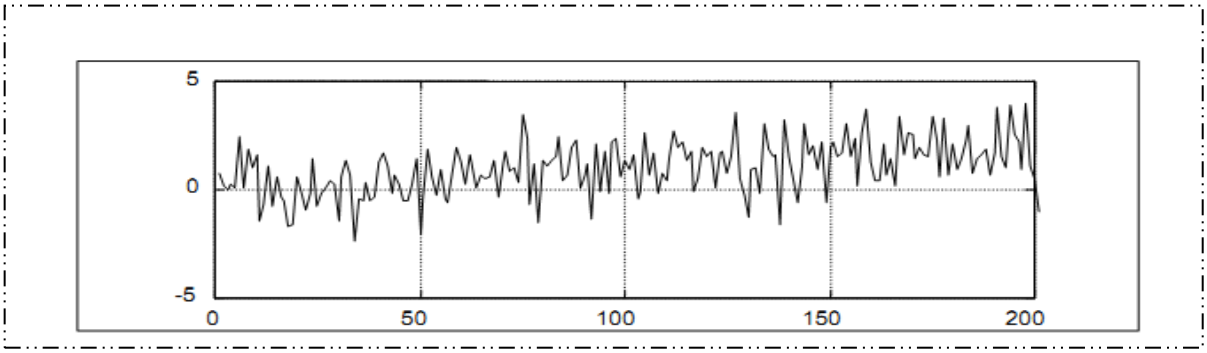


Figure 1.3. Dérive capteur [RIP 99]

Enfin, **les valeurs aberrantes** sont des défauts dits fugitifs : elles affectent le système de manière instantanée. Leur cause est souvent due à un parasite, par exemple une perturbation électromagnétique. Elles se manifestent par un écart important et sporadique par rapport à la valeur nominale du signal. La figure (1.4) représente un tel défaut au temps 50.

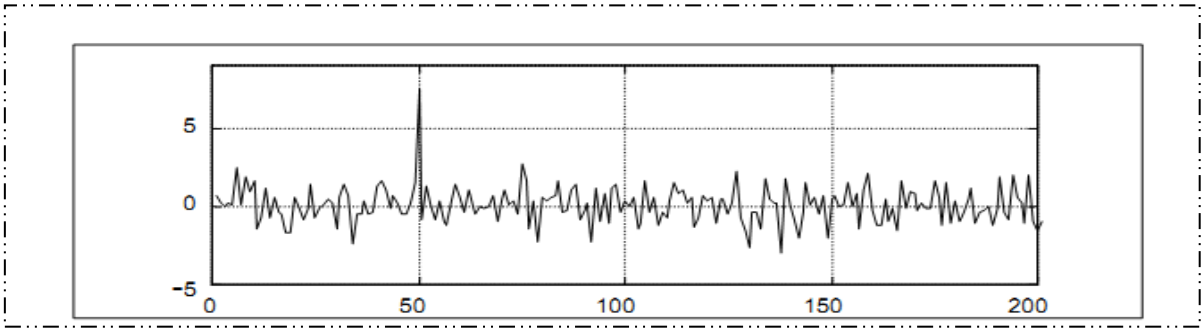


Figure 1.4. Valeur aberrante [RIP 99]

1.3. Diagnostic :

Le diagnostic des défauts des systèmes industriels est à l'origine de nombreux travaux durant ces dernières années. Il est défini comme l'opération permettant de détecter un défaut, de localiser son origine et de déterminer ses causes. Son principe général consiste à confronter les données relevées au cours du fonctionnement réel du système avec celles émanant de la connaissance dont dispose sur son fonctionnement normal ou nominal. Diagnosis signifie en grecque ; « Dia » : Par, et « Gnosis » : connaissance, i.e. **par connaissance**.il s'agit d'acquérir la connaissance et de produire une décision à travers les signes observables [LAL 08]. Il établit un lien de cause à effet entre un symptôme observé et la défaillance qui est survenue, ses causes et ses conséquences [BAR 10]. On distingue classiquement trois étapes :

- localisation, détermine le sous système fonctionnel à l'origine de l'anomalie et progressivement affine cette détermination pour désigner l'organe ou dispositif élémentaire défectueux ;
- identification, détermine les causes qui ont engendré la défaillance constatée, etc. ;
- explication, justifie les conclusions du diagnostic.

Pour ce qui suit, on peut adapter la définition suivante :

Un diagnostic est l'identification de la (ou des) cause (s) probables d'un (ou des) défaut(s) survenue(s) ou encourue(s) dans un système à l'aide d'un raisonnement logique fondé sur des observations recueillies sur ce même système par inspection, par contrôle ou par tests, [AFNOR].

1.4. L'intérêt du diagnostic :

L'intérêt pour le diagnostic des défauts s'explique par la complexité croissante des systèmes industriels qui sont de plus en plus exigeants en termes des contraintes de sécurité, de fiabilité (probabilité d'obtenir le service attendu), de disponibilité (probabilité de trouver le système en état de remplir sa mission), de sûreté (capacité du système à résister à une utilisation incorrecte) et d'intégrité (capacité du système à résister à des défaillances).En fait, la possibilité qu'un système tombe en panne croît malgré les précautions de manipulation, le développement de techniques de conception de la commande et l'expérience des opérateurs humains de supervision. Par conséquent, un module de diagnostic, voire système, adapté est nécessaire pour empêcher la propagation d'un défaut et pour limiter leurs conséquences qui peuvent être catastrophiques au niveau économique et environnemental. Pour cela ce module doit être rapide, robuste et moins coûteux, peut prémunir au mieux des défaillances.

D'une manière générale, L'objectif de la fonction diagnostic est de rechercher les causes et de localiser les organes qui ont entraîné une observation particulière [RAC 06]. A partir de l'observation d'un état de panne, la fonction diagnostic est chargée de retrouver la faute qui en est à l'origine. Ce problème est difficile à résoudre. En effet si, pour une faute donnée, il est facile de prédire la panne résultante, la démarche inverse qui consiste à identifier la faute à partir de ses effets, est beaucoup plus ardue. Une défaillance peut généralement être expliquée par plusieurs fautes. Il s'agit alors de confronter les observations pour fournir la bonne explication. Le diagnostic devient de ce fait un levier, sa maîtrise dans une entreprise contribue à l'amélioration de la compétitivité de l'outil de production.

1.5. Organisation générale de la procédure de diagnostic :

La procédure de diagnostic de défaillances et de dégradations susceptibles d'affecter les différentes entités d'un processus industriel s'articule autour des étapes suivantes [ZWI 95] :

- L'extraction des informations nécessaires à la mise en forme des caractéristiques associées aux fonctionnements normaux et anormaux, à partir de moyens de mesures appropriées ou d'observations réalisées lors des rondes par les personnels de surveillance,
- L'élaboration des caractéristiques et signatures associées à des symptômes révélateurs de défaillances et de dégradations en vue de la détection d'un dysfonctionnement,
- La détection d'un dysfonctionnement par comparaison avec des signatures associées à des états de fonctionnements normaux et la définition d'indicateurs de confiance dans la détection,
- La mise en œuvre d'une méthode de diagnostic de la défaillance ou de la dégradation à partir de l'utilisation des connaissances sur les relations de cause à effet,
- La prise de décision en fonction des conséquences futures des défaillances et des dégradations. Cette prise de décision peut de conduire à un arrêt de l'installation si les conséquences de la défaillance sont importantes pour la sécurité des personnes et des biens ou à une reconfiguration du fonctionnement du procédé pour éviter une perte de production en attendant le prochain arrêt de production le plus propice aux opérations de maintenance corrective.

La figure (1.5) représente l'ensemble des tâches à réaliser pour assurer un fonctionnement satisfaisant d'un processus industriel [BAR 10]. Dont le module de diagnostic est alimenté par toutes les informations disponibles sur le système. Ces informations incluent les mesures des variables et toute autre information pouvant être utile pour le diagnostic comme, par exemple, la structure du système. Le module de diagnostic traite les observations et produit une liste de défauts possibles pouvant affecter le système au cours du temps. Il aide donc à surveiller un procédé complexe et par conséquent à prendre une décision pour effectuer une reprise de la commande si possible.

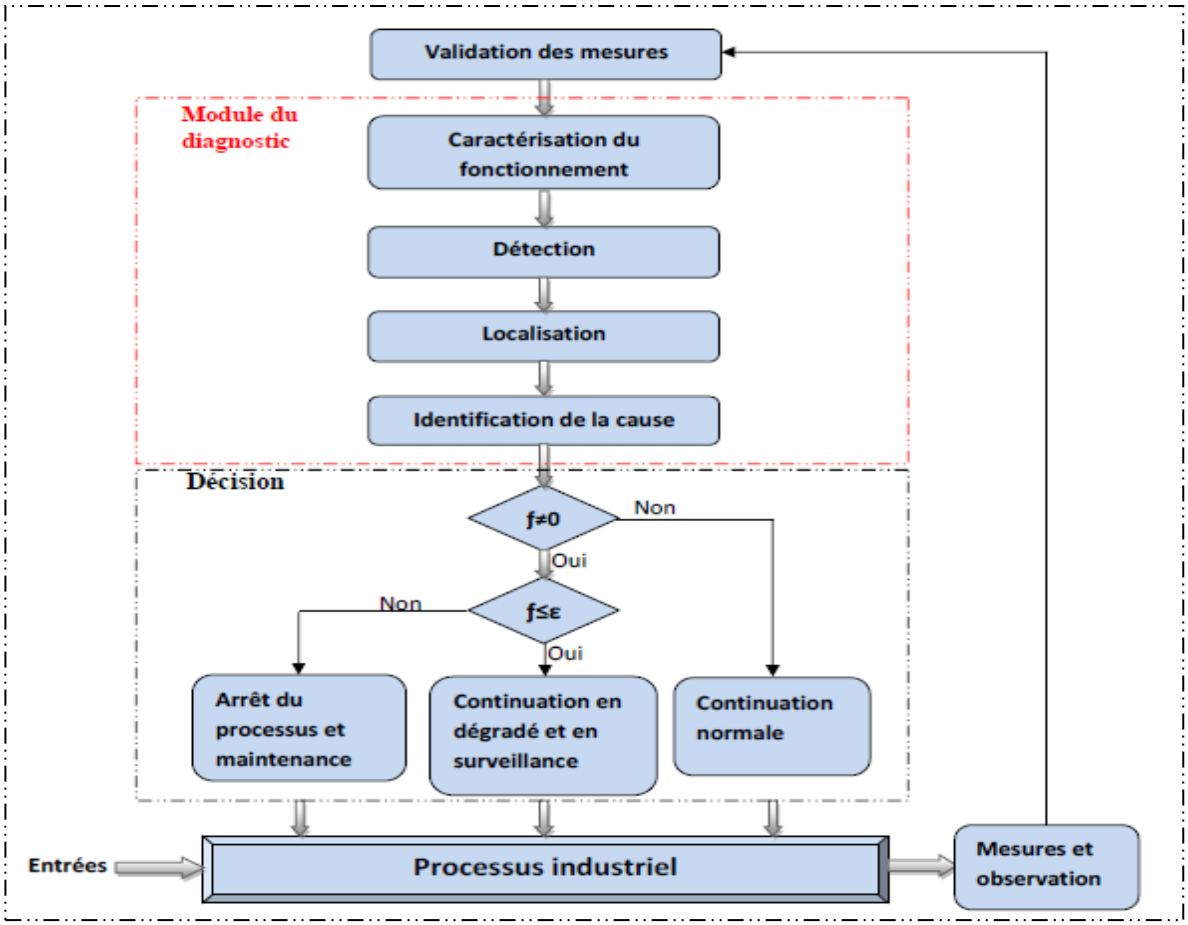


Figure 1.5. Les différentes étapes du diagnostic industriel [BAR 10].
f : défaut, ε : défaut seuil.

L'extraction des informations nécessaires à la mise en forme des caractéristiques associées aux fonctionnements normaux et anormaux, à partir des moyens de mesures appropriées ou observation réalisées hors des rondes par les personnels de surveillance [SAL 08].

L'élaboration des caractéristiques et signatures associées à des symptômes révélateurs de défaillances et de dégradations en vue de la détection d'un dysfonctionnement.

Souvent, un processus industriel est constitué d'un système réglé par un contrôleur dans le but d'améliorer ses performances. Dans ce cas, les variables connues sont les sorties du contrôleur et les mesures de sorties fournies par les capteurs.

Ce cas est illustré par la figure (1.6) qui illustre une complication fondamentale pour la synthèse du module de diagnostic due à la présence non seulement des défauts mais aussi de perturbation. Ces deux types d'entrées non contrôlées et généralement non mesurables affectent l'évolution du système et dégradent ses performances. Les perturbations appelées aussi entrées inconnues, ne sont pas considérées comme des défauts mais influencent également l'évolution du système. Le module de diagnostic doit distinguer de ce fait l'influence provoquée par ces entrées inconnues et celle causée par les défauts.

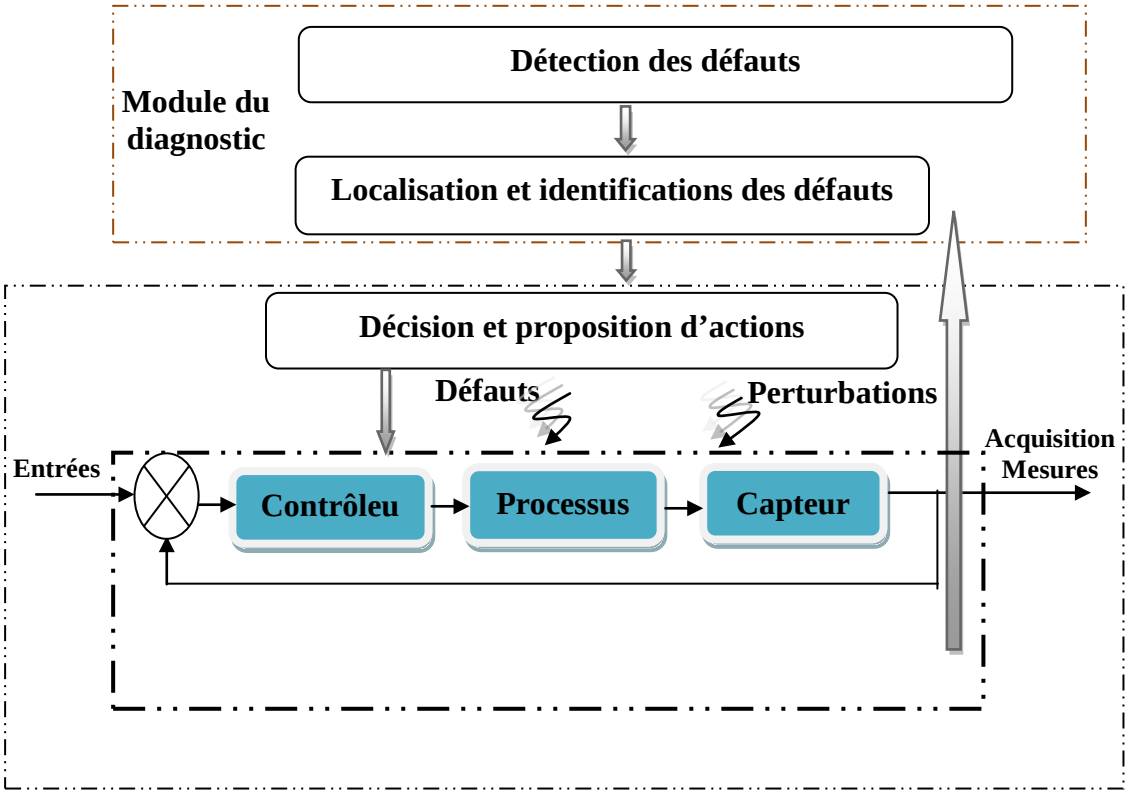


Figure 1.6. Principe du diagnostic des systèmes commandés [BAR 10]

Enfin, le diagnostic des défaillances industriels, s'il est réalisé avec efficacité permet de détecter et de localiser précocement les défauts, devient par la suite un moyen contribuant à la disponibilité de l'outil de production.

1.6. Surveillance, diagnostic et supervision :

Dans un grand nombre d'applications industrielles, une demande croissante est apparue en matière de remplacement des politiques de maintenance curative par des stratégies de maintenance préventive. Cette mutation d'une situation où on « subit les pannes » à une

situation où on « maîtrise les pannes », nécessite quelques moyens technologiques ainsi que la connaissance de techniques d'analyse appropriées. La fonction surveillance en continu de l'évolution de l'équipement à travers des données quantifiables et qualifiables permet ainsi de prévenir un dysfonctionnement avant qu'il n'arrive et d'écarter les fausses alarmes qui peuvent ralentir la production.

Dans la littérature associée au domaine de la surveillance d'équipements industriels. La surveillance est un dispositif passif, informationnel, qui analyse l'état du système et fournit des indicateurs. La surveillance consiste notamment à détecter et classer les défaillances en observant l'évolution du système, puis à les diagnostiquer en localisant les éléments défaillants et en identifiant les causes premières [RAC 06].

La surveillance des procédés industriels consiste à générer des alarmes à partir des informations délivrées par des capteurs. Elle traite les données disponibles en ligne, afin d'obtenir son état de fonctionnement [KEM 04]. Elle recueille les signaux en provenance du procédé et de la commande et reconstitue l'état réel du système commandé. Des seuils sont définis sur des variables clés par des experts du procédé selon des critères de sécurité concernant les hommes, l'installation et son environnement. Elle a un rôle passif vis-à-vis du système de commande et du procédé [COM 91]. Cependant, la complexité et la taille de l'installation augmentent rapidement la quantité d'informations à analyser, rendant la surveillance complexe. Il est donc très utile d'adjoindre à la surveillance, une aide à la décision à travers un module de diagnostic.

Le diagnostic s'intègre dans le cadre plus général de la surveillance et de la supervision. C'est un système d'aide à la décision, son objectif est de localiser les composants ou les organes défaillants d'un procédé et éventuellement de déterminer les causes. Le diagnostic établit donc un lien de cause à effet entre un symptôme observé et la défaillance qui est survenue, tout en considérant qu'un même symptôme peut apparaître pour différentes causes [BAR 10].

La supervision a pour objectif de surveiller et de contrôler l'exécution d'une opération et le fonctionnement d'une installation. Elle a donc un rôle décisionnel et opérationnel en vue de la reprise de la commande. La supervision élabore des solutions correctives en ayant la connaissance des causes, ou des organes ayant générés une défaillance.

1.7. Place et Procédure de détection :

La définition établie ici pour le diagnostic, intègre le module de détection. En fait, cette fonction représente très souvent un sujet de débat concernant sa place précise. En effet, de nombreuses approches considèrent la détection comme un élément à part du diagnostic et le

voient plutôt comme une entité de la surveillance [COM 91], [COM 00b], [DAN 97]. D'autres travaux préfèrent la considérer comme une information primordiale et indissociable du diagnostic et définissent le diagnostic comme la détection, la localisation et l'identification de défauts. Ce sont les méthodes à base de modèles appelées FDI (Fault Detection and Isolation) [BAR10].

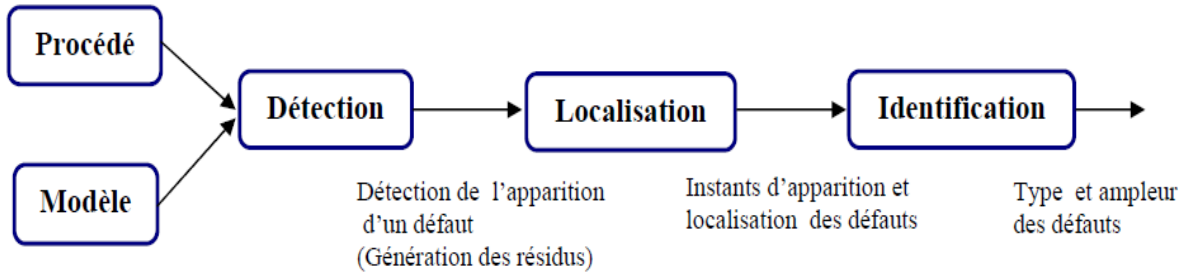


Figure1.7: Procédure de détection et d'isolation des défauts [BAR 10].

La détection permet de détecter tout écart du comportement normal du système et alerte les opérateurs humains de la présence d'un défaut. La localisation permet de remonter à l'origine de l'anomalie et de localiser le ou les composants défectueux. Cette localisation est importante puisque la propagation d'une panne provoque souvent l'apparition de nouveaux défauts. Enfin, l'identification détermine l'instant d'apparition de la panne, sa durée et son importance. Le diagnostic aide donc les opérateurs humains à surveiller un procédé complexe et par conséquent à prendre une décision pour effectuer une reprise de la commande [PHI 06]. La figure (1.8) illustre le synoptique de la détection et localisation des défauts.

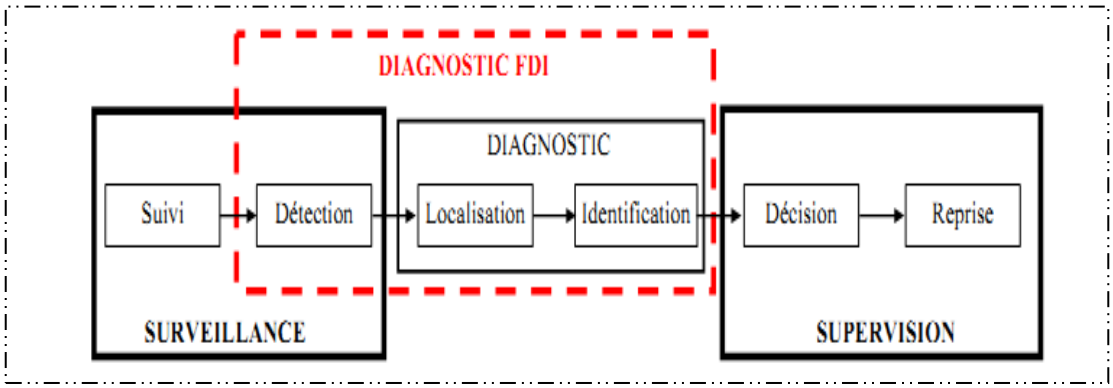


Figure 1.8. Place de la détection dans le diagnostic FDI [PHI 06].

1.8. Critères de performance d'un système de diagnostic :

Comment s'assurer que le système de diagnostic développé soit le plus performant possible ? Pour répondre à une telle question, il convient tout d'abord de définir en vertu de quels critères le système peut être évalué. D'une manière générale, nous pouvons regrouper les différents critères de performance du système de détection de la manière suivante [RIP 99] : détectabilité, isolabilité, sensibilité, robustesse, coût économique et temps de développement.

La notion de détectabilité est l'aptitude du système de diagnostic à pouvoir déceler la présence d'une défaillance sur le procédé. Elle est fortement liée à la notion d'indicateurs de défauts (résidus) : le générateur de résidu doit, d'une certaine manière, être sensible à la défaillance que l'on souhaite détecter.

L'isolabilité est la capacité du système de diagnostic à remonter directement à l'origine du défaut. Une alarme engendre bien souvent de nouvelles alarmes et il devient dès lors difficile de retrouver l'organe défaillant. La propriété d'isolabilité est liée à la structure des résidus et à la procédure de détection elle-même.

La sensibilité caractérise l'aptitude du système à détecter des défauts d'une certaine amplitude. Elle dépend non seulement de la structure des résidus mais aussi du rapport de l'amplitude du bruit de mesure avec celle du défaut.

La robustesse détermine la capacité du système à détecter des défauts indépendamment des erreurs de modélisation (sensibilité du résidu aux défauts et insensibilité vis-à-vis des perturbations). Généralement, la robustesse est définie par rapport à toutes les entrées inconnues.

En pratique, d'autres critères sont à prendre en considération. En phase d'industrialisation, les contraintes ergonomiques et économiques sont essentielles. Les aspects temps réel sont par exemple prépondérants pour un système de diagnostic embarqué sur un véhicule. La rapidité de détection peut être un facteur déterminant. De même, les coûts économiques vont conditionner la stratégie de diagnostic : le système nécessite-t-il des composants trop chers pour sa conception, le temps de développement est-il trop important ? Autant de points à vérifier afin de satisfaire le cahier des charges.

1.9. La redondance pour le diagnostic :

Le principe de redondance permet de mettre à disposition plusieurs ressources pour réaliser une même fonction ou une même tâche. Certaines redondances permettent d'agir sur le procédé et d'en modifier le comportement alors que d'autres permettent à une ressource donnée de disposer de plusieurs moyens d'acquisition d'une même information.

On distingue ici trois types principaux de redondance : La redondance d'information, la redondance physique et la redondance analytique.

- Redondance d'information : Le concept de base des systèmes de diagnostic est la redondance d'informations. Cette redondance de connaissances sur le système fournit plusieurs informations différentes sur une même variable du système. Il est ainsi possible de vérifier la cohérence de cette information par des tests de cohérence que nous allons exposer [RIP 99]. Celle-ci se divise en deux : la redondance physique et la redondance analytique.

- Redondance physique (matérielle) : Le moyen le plus direct pour obtenir une information fiable sur une même variable est de disposer de plusieurs capteurs la mesurant simultanément. Une redondance à trois permettra notamment d'isoler un capteur défaillant.

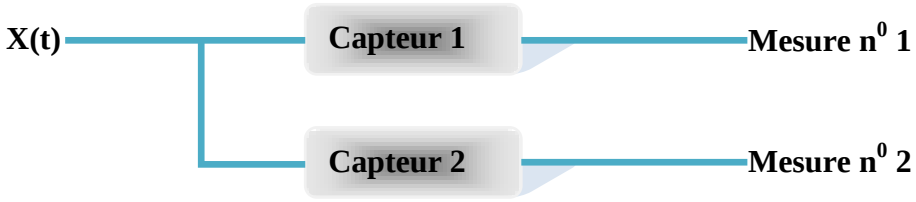


Figure 1.9. Redondance physique.

La redondance physique souffre d'un désavantage majeur : doubler ou tripler le nombre de capteurs revient à augmenter considérablement son coût et à affronter des problèmes d'encombrement liées à l'installation et à la maintenance de ces capteurs. L'ajout de capteurs supplémentaires permettra aussi d'avoir des informations additionnelles à mettre à profit dans le cadre de la redondance analytique.

- Redondance analytique : la redondance analytique consiste à utiliser des informations supplémentaires issues, non plus de capteurs, mais de modèles permettant l'élaboration de grandeurs de même nature que celles issues des capteurs auxquelles elles vont être comparées dans les mêmes conditions que dans la méthode de redondance simple, c'est-à-dire par une évaluation de leur cohérence ; ces modèles ne sont autres que des relations mathématiques reliant certaines données mesurées à des grandeurs de sortie [ZWI 95].

L'utilisation de la redondance analytique, en créant des informations nouvelles, augmente l'ordre de la redondance directe préalablement fixée par le nombre de capteurs. On pourra ainsi traiter des informations issues de capteurs uniques ou de dispositifs dont la redondance n'était que de deux. En effet, la comparaison de deux informations ne permet que la détection d'une éventuelle défaillance sans pour autant permettre la détermination de la voie défaillante par contre, un vote logique à trois permet cette identification.

L'utilisation de la redondance analytique s'impose donc si l'on désire réaliser la validation de mesure dont la redondance matérielle est insuffisante. Par ailleurs, elle présente un autre intérêt vis-à-vis de la redondance simple : elle permet sous certaines conditions, de détecter des pannes dites de mode commun. Ces dernières sont des défaillances identiques et simultanées, affectant deux ou plusieurs capteurs. L'utilisation d'un modèle excité par des grandeurs indépendantes, normalement à l'abri de pannes de mode commun, permet une détection de ce genre de défaillance.

1.10. Classifications des méthodes de diagnostic :

Les méthodes de diagnostic sont nombreuses et variées, elles correspondent à la diversité des problèmes rencontrés. Il est possible de les classer selon le schéma de la figure (1.10).

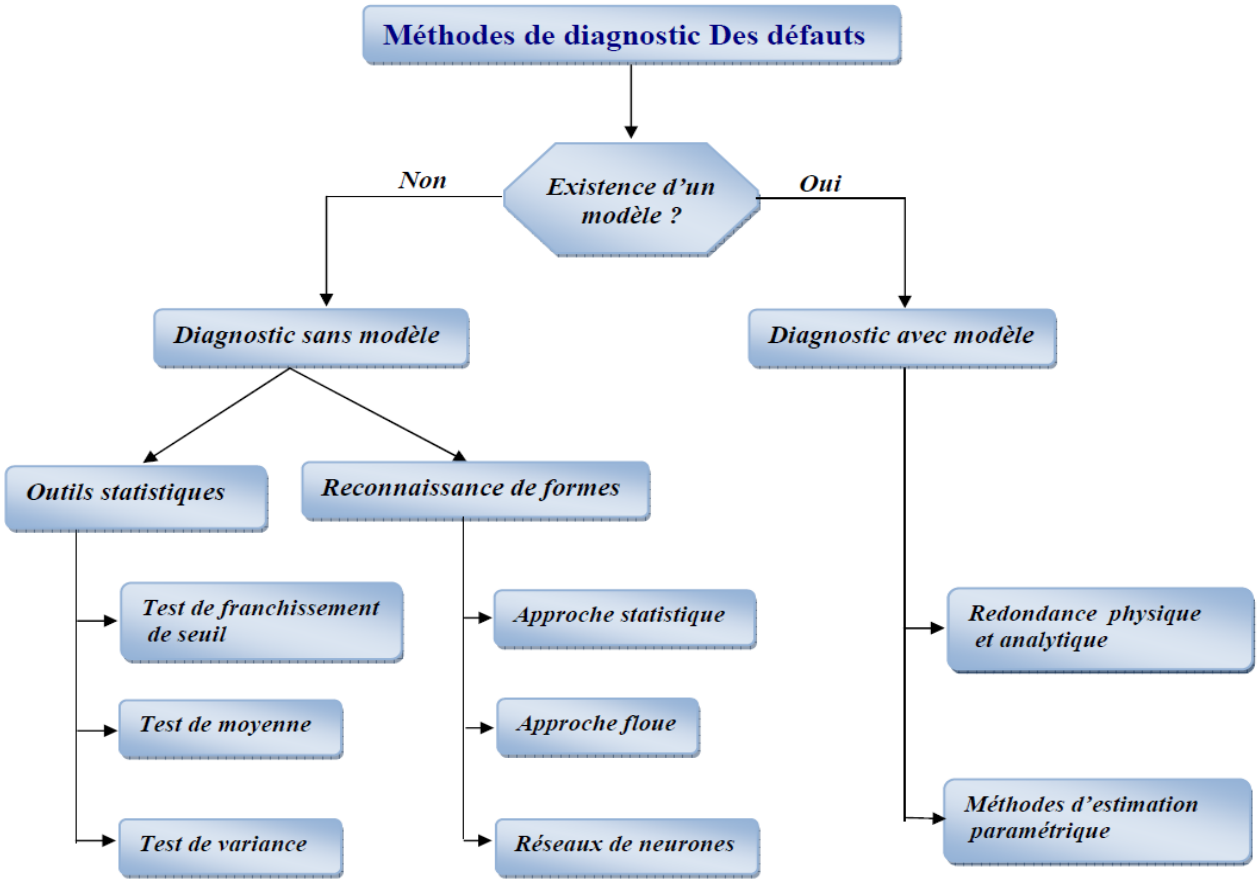


Figure 1.10 : Classifications des méthodologies de diagnostic industriel [OUA 09].

Les méthodes de diagnostic industriel tel qu'elles sont présentées dans ce paragraphe sont illustrées sur la figure (1.10). L'existence d'un modèle formel ou mathématique de l'équipement détermine la méthode de diagnostic utilisée. Le diagnostic avec modèle se compose essentiellement de deux techniques : méthodes de redondance

physique et analytique et méthodes d'estimation paramétrique. D'un autre côté, les méthodes qui ne se basent pas sur l'existence du modèle se divisent en deux catégories : méthodes utilisant des outils statistiques et méthodes de reconnaissance des formes.

Les outils statistiques établissent des tests sur les signaux d'acquisition. Ces tests ne sont capables d'assurer que la fonction détection de défaillances. Par contre, les techniques de diagnostic par reconnaissance des formes sont plus élaborées par rapport aux simples tests statistiques et sont capables de détecter et de diagnostiquer les défaillances.
Les méthodes les plus familières aux automaticiens sont les méthodes basées sur l'utilisation de modèles mathématiques. Celles-ci utilisent la redondance existant entre les différentes variables mesurées en termes de relations statiques ou dynamiques.
Aussi dans la littérature, on retrouve deux catégories de méthodes dédiées au diagnostic [ZWI 95], internes et externes. Ces méthodes diffèrent selon la nature et l'étendue de la connaissance accessible du système. Les critères du choix d'une méthode de diagnostic peuvent se résumer comme suit :

- la dynamique du système (discrète, continue ou hybride),
- la structure d'implémentation (comparateur, filtre, référence, ...),
- la nature de l'information (quantitative et/ou qualitative),
- la complexité du système (large ou simple),
- la profondeur de l'information disponible sur le système (structurelle, analytique et/ou heuristique).

1.10.1. Méthode externe (méthode sans modèle) :

Ces méthodes ont été développées pour pouvoir étudier efficacement la dynamique d'un système pour lequel le modèle mathématique est difficile à établir voir même inexistant. Le système est considéré comme étant une boite noire où seules les entrées et les sorties observables peuvent être mesurées. Ces mesures sont appelées signatures externes. La connaissance qualitative et/ou quantitative de ces signatures est précieuse pour l'étude de ces systèmes. Ces méthodes sont basées sur un retour d'expérience et ont donc l'avantage d'être performantes avec un minimum de connaissance a priori. Dans la littérature, de nombreux travaux ont permis leur mise au point et leur utilisation comme par exemple la reconnaissance des formes, les systèmes experts [ZWI 95] et les réseaux de neurones artificiels.

1.10.1.1. Reconnaissance des formes (RDF) :

La Reconnaissance des Formes (RdF) est une science qui regroupe l'ensemble des algorithmes ou méthodes permettant la classification d'objets ou de formes en les comparants à des formes-types [BOU 97]. On suppose que chaque observation, appelée aussi forme, réalisée sur un système est caractérisée par un certain nombre de paramètres ou d'attributs. Chaque forme peut donc être représentée à l'aide d'un vecteur appelé "vecteur forme" dans un espace appelé "espace de représentation". On suppose aussi que dans cet espace on peut observer des formes de types différents, appelées aussi "prototypes" ou "formes-types". Dans un cas idéal, où la notion de bruit n'est pas prise en compte, chaque nouvelle forme serait exactement confondue avec l'une des formes-types. Par contre, dans un cas réel, afin de traduire l'influence des perturbations sur le système étudié (bruit de mesure, précision des capteurs,…), une nouvelle observation sera rarement confondue avec l'une des formes-types. Il est alors difficile d'isoler un point unique de l'espace comme représentant de la forme-type. Une zone restreinte, appelée "classe" et notée C_i, est définie autour de chaque forme-type de l'espace de représentation en englobant les formes semblables comme le montre la figure ci-dessous [MOH 07].

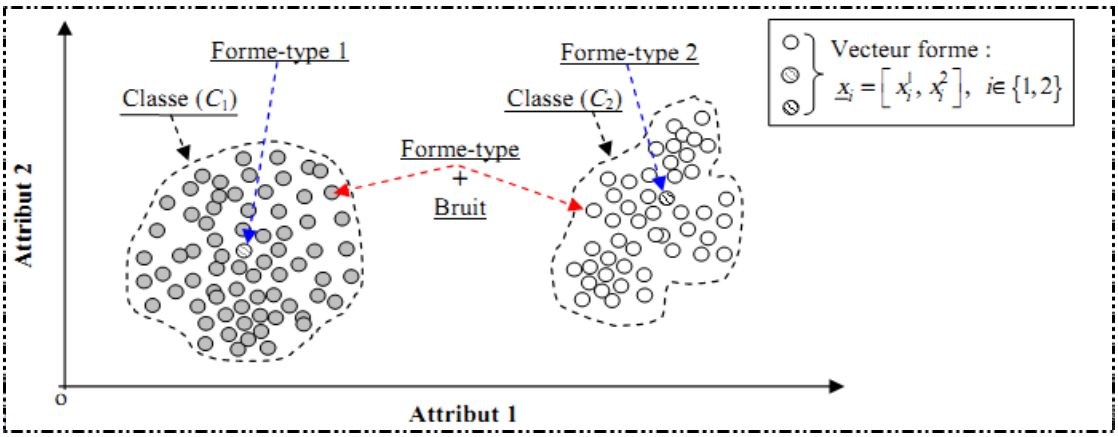


Figure 1.11. Les vecteurs formes dans un espace de deux dimensions [MOH 07]

1.10.1.2. Réseaux de neurones artificiels :

Un RNA est un système informatique constitué d'un nombre de processeurs élémentaires (ou nœuds) interconnectés entre eux qui traite de façon dynamique l'information qui lui arrive à partir des signaux extérieurs. De manière générale, l'utilisation des RNA se fait en deux phases. Tout d'abord, la synthèse du réseau est réalisée et comprend plusieurs étapes : le choix du type de réseau, du type de neurones, du nombre de couches, des méthodes d'apprentissage. L'apprentissage permet alors, sur la base de l'optimisation d'un critère, de reproduire le comportement du système à modéliser. Il consiste dans la recherche d'un jeu de paramètres (poids) et peut s'effectuer de deux manières : supervisé (le réseau utilise les

données d'entrée et de sortie du système à modéliser) et non supervisé (seules les données d'entrée du système sont fournies et l'apprentissage s'effectue par comparaison entre exemples). Quand les résultats d'apprentissage obtenus par le RNA sont satisfaisants, il peut être utilisé pour la généralisation. Il s'agit ici de la deuxième phase où de nouveaux exemples qui n'ont pas été utilisés pendant l'apprentissage sont présentés au RNA pour juger de sa capacité à prédire les comportements du système ainsi modélisé. Leur faible sensibilité aux bruits de mesure, leur capacité à résoudre des problèmes non linéaires et multi-variables, à stocker les connaissances de manière compacte, à « apprendre » en ligne et en temps réel, sont des propriétés qui rendent l'utilisation des RNA attrayante [ORA 05]. Leur emploi peut alors se faire à trois niveaux :

- comme modèle du système à surveiller en état normal et générer un résidu d'erreur entre les observations et les prédictions,
- comme système d'évaluation de résidus pour le diagnostic,
- ou comme système de détection en une seule étape (en tant que classificateur), ou en deux étapes (pour la génération de résidus et le diagnostic).

1.10.1.3. Systèmes experts :

Par opposition aux techniques de reconnaissance des formes et aux réseaux de neurone artificiels, réservés principalement au diagnostic externe, les systèmes experts, par leur capacité à reproduire le raisonnement d'un expert humain dans un domaine donné, offrent des perspectives plus larges car ils permettent de résoudre aussi bien les problèmes de diagnostic externe que les problèmes de diagnostic interne. Un système expert est un système informatique destiné à résoudre un problème précis à partir d'une analyse et d'une représentation des connaissances et du raisonnement d'un (ou plusieurs) spécialiste(s) de ce problème [ZWI 95]. Les systèmes experts, capables de raisonner avec des connaissances de « surface » (analyse des signatures externes) ou avec des connaissances « profondes » (connaissance de modèles directs) ont fait une percée industrielle très remarquée pour le diagnostic de petits systèmes. Par contre pour des systèmes industriels complexes, la diffusion est plus lente principalement en raison des coûts très élevés de développement, d'exploitation et de maintenance.

1.10.2. Méthodes internes (méthode avec modèle) :

Les méthodes internes nécessitent une connaissance approfondie du système étudié, afin de le représenter analytiquement [ZWI 95] sous forme d'un modèle quantitatif et/ou qualitatif.

L'estimation des variations des paramètres du modèle, dans le cas continu, permet de détecter un éventuel défaut ou de déceler un résidu par rapport au système réel.

Dans la littérature relative aux techniques d'identification les modèles peuvent être rangés en deux classes : les modèles paramétriques et non paramétriques.

Les modèles paramétriques sont des outils permettant de prédire les réponses dynamiques et statiques du processus quelle que soit la nature des signaux d'excitation. Ils sont caractérisés par un nombre fini de paramètres qui interviennent dans la structure mathématique retenue pour représenter le modèle. Par structure du modèle, on sous entend des relations fonctionnelles nécessaires pour décrire le processus. Détermination de la structure et estimation des paramètres sont des problèmes liés. Si la valeur estimée d'un paramètre est exemple nulle, l'élément qui lui correspond dans la structure peut être supprimé. Si de nombreuses techniques permettant de détecter une structure mal adaptée, très peu de méthodes existent pour déterminer les nouveaux éléments qui doivent compléter la structure pour augmenter la qualité du modèle.ces modèles se classent en différentes catégories déduites soit d'une compréhension physique des phénomènes à l'intérieur du processus, soit sur des fondements empiriques ou sur une approche mixte.

- Les modèles de représentation « les modèles de comportement » sont construits uniquement à partir d'un jeu de données expérimentales, sans se préoccuper des lois de physiques. Une telle approche est la seule possible si la compréhension du fonctionnement est restreinte ou trop complexe et coûteuse à modéliser. Dans ce cas l'utilisation de tels modèles permet d'obtenir des modèles satisfaisants mais dont les paramètres n'auront aucun sens physique ce qui sera pénalisant pour le diagnostic.
- Les modèles de connaissances reposent sur les lois qui réagissent le processus. En raison de son principe, il est conseillé à des fins de diagnostic d'identifier les paramètres d'un tel modèle. En effet, les modifications des relations de cause à effet sont immédiatement interprétables par les spécialistes du processus. Ces modèles possèdent l'avantage considérable de permettre de simuler le comportement réel du processus pour des signaux d'excitation très variés. Par contre, ils nécessitent un investissement très important dans la compréhension de la physique des phénomènes avec des spécialistes. Les résultats seront décevants si le modèle est trop simplifié ou si trop de paramètres doivent être déterminés. En effet, le modèle fournira une bonne représentation mais l'interprétation physique peut être remise en question. On observera que les temps de calcul demandés par leurs simulations seront loin d'être négligeables ce qui entraînera des problèmes pour réaliser le diagnostic en temps réel.

- Modèle mixte : Ce modèle résulte d'un compromis entre le modèle physique et le modèle empirique. Un modèle mixte peut résulter de la simplification d'un modèle physique trop complexe, par exemple, en linéarisant les équations ou bien en utilisant des paramètres physique globaux. On peut faire appel également à ce type de modèle pour un processus complexe décomposable en une structure hiérarchisée de systèmes, sous systèmes et composants. Ainsi tout ou partie des systèmes et sous systèmes seront modélisés par des modèles empiriques. Cependant il est nécessaire de prendre des précautions lorsque trop de phénomènes sont considérés : l'intégration de tous ces phénomènes pouvant conduire à des difficultés de simulation et à une validité réduite du modèle.

Les modèles non paramétriques sont réservés exclusivement à la modélisation des caractéristiques dynamiques des processus. Ils ne dépendent pas d'une structure d'un modèle mathématique dont la structure est connue. Ces modèles correspondent aux réponses fréquentielles et temporelles des processus.

Le diagnostic à base de modèles génère des indicateurs de défauts, résidus, contenant des informations sur les anomalies ou les dysfonctionnements du procédé à diagnostiquer. Un écart entre l'état réel du système et celui estimé par le modèle, représentant le fonctionnement nominal, est mesuré. Les résidus doivent alors être assez sensibles aux défauts pour leur détection, localisation et identification (figure 1.12).

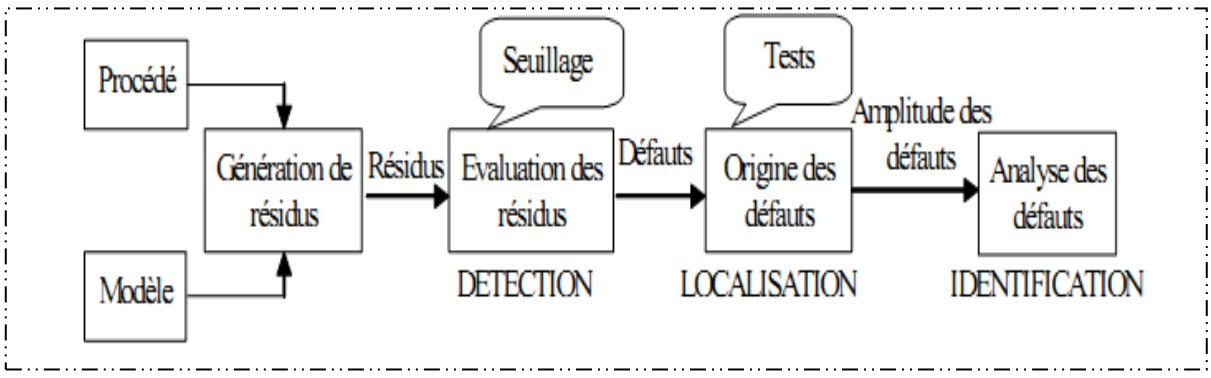


Figure 1.12. Diagnostic à base de modèles [ZWI 95**]**

Parmi les méthodes internes à base de modèles, on peut distinguer les méthodes basées sur des modèles quantitatifs, les méthodes basées sur des modèles qualitatifs et les méthodes basées sur les deux modèles.

1.10.2.1. Méthodes à base de modèle quantitatif :

Ces modèles sont construits à partir des lois fondamentales (physique, chimie,…) et décrit par des relations mathématiques sur les entrées-sorties du système. Diverses approches pour la détection de défaillances à partir des modèles mathématiques ont été développées depuis les années 70 [ISE 97].

Ces méthodes dites « méthodes des résidus » comportent deux étapes : d'une part, la génération des résidus et, d'autre part, le choix d'une règle de décision pour le diagnostic. Les résidus représentent des changements ou divergences entre le comportement réel du processus et celui prévu par le modèle. La figure (1.13) illustre le principe le plus général pour la génération des résidus.

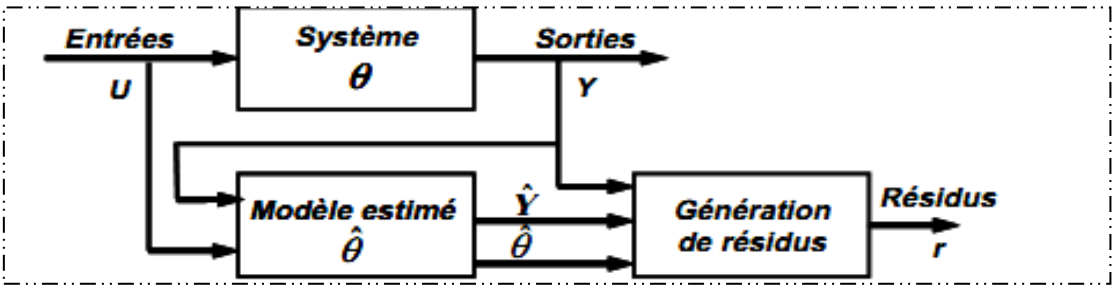


Figure 1.13. Principe de génération des résidus

L'objectif du résidu est d'être sensible aux défauts. Ainsi, normalement, en l'absence de défaillances, c'est-à-dire en fonctionnement normal, le résidu doit avoir une valeur nulle. Au contraire, en présence d'un défaut, le résidu aura une valeur non nulle.

Les techniques les plus utilisées pour la génération des résidus, à partir de modèles analytiques, sont listées ci-dessous [KEM 04] :

- Equations de parité
- Estimation d'état à partir d'observateurs ou filtres de kalman
- Estimation paramétrique
- Analyse structurelle

Une fois les résidus générés, ils doivent être évalués pour déterminer la présence ou non d'une défaillance. Cette évaluation des résidus est établie principalement par l'utilisation de seuils fixes ou adaptatifs pour éviter les fausses alarmes. Néanmoins, la plupart du temps, les résidus sont corrélés entre eux. Pour gérer cette corrélation, le maximum de vraisemblance généralisée peut être utilisé. Il s'agit d'une technique qui, sous l'hypothèse que les variables ont une distribution connue, usuellement la distribution normale, permet d'estimer les paramètres d'un modèle (d'une équation ou d'un système, linéaire ou non linéaire) avec des

restrictions sur les paramètres (coefficients, matrice de variances et covariances) ou non. Plus spécifiquement, la technique consiste à construire une fonction appelée fonction de vraisemblance (construite à partir de la fonction de densité) et à maximiser son logarithme par rapport aux paramètres inconnus.

Le principal inconvénient des méthodes analytiques de détection de défaillances et diagnostic est la nécessité d'avoir des modèles mathématiques assez précis et complets, ce qui n'est pas toujours facile, voire impossible, pour des processus complexes tels que les processus chimiques. Ces modèles sont limités aux représentations linéaires ou des modèles non linéaires très spécifiques. Un autre inconvénient est la modélisation des perturbations qui peuvent engendrer des erreurs dans le modèle. En plus, si un type de faute n'a pas été modélisé de manière spécifique, il n'y a pas de garanties que les résidus soient capables de le détecter. Finalement, l'adaptabilité de ces approches aux changements du processus n'est pas considérée.

1.10.2.2. Méthodes à base de modèle qualitatif :

Les méthodes à base de modèles qualitatifs permettent de représenter le comportement du procédé avec un certain degré d'abstraction à travers des modèles non plus mathématiques mais des modèles de type symbolique [ZWI 95]. Les modèles qualitatifs doivent représenter de manière qualitative des systèmes continus, discrets et/ou hybrides pour que le diagnostic soit capable de détecter les déviations du fonctionnement normal, localiser la défaillance et en déterminer la ou les causes. Pour les systèmes continus, les modèles qualitatifs sont fréquemment basés sur des graphes causaux ou des graphes causaux temporels. Une abstraction qualitative des comportements continus peut être représentée par des modèles à base d'événements discrets (SED), ou par la théorie de supervision. Pour les SED, de nombreuses approches sont proposées utilisant des outils tels que les automates, les équations logiques ou les Réseaux de Pétri (RdP) avec observation partielle ou totale du fonctionnement du procédé.

1.10.2.3. Méthodes mixtes :

Une intégration des modèles discrets et des modèles continus peut être retrouvée également dans les systèmes dynamiques hybrides. Les méthodes à base de modèles quantitatifs et qualitatifs reposent d'une part sur une évaluation quantitative pour la détection d'un défaut et d'autre part sur une analyse qualitative des transitoires pour la localisation et l'identification. Ces méthodes ont l'avantage de combiner les points forts des méthodes à base de modèles quantitatifs et ceux à base de modèles qualitatifs. Cependant, elles sont lourdes à implémenter [MOH 07].

1.11. Conclusion :

Dans ce chapitre nous avons essayé de présenter une étude assez exhaustive des différentes techniques de détection et de localisation des défaillances. Nous avons commencé par rappeler un certain nombre de notions fondamentales ainsi que l'intérêt du diagnostic dans le domaine industriel. En effet en considérant le diagnostic comme une composition de trois modules : la détection, la localisation et l'identification, une terminologie appropriée au diagnostic a été présentée. Les notions de diagnostic ainsi que des défauts, de défaillance, de panne, de détection, de la localisation et d'identification ont été proposées.

Ensuite, nous avons présenté un état de l'art des différentes méthodes de diagnostic de défaillances pour des applications industrielles. Deux grandes catégories ont été dégagées ; méthodes externe et interne. Les méthodes externes sont essentiellement basées sur les connaissances de l'expert. Les méthodes internes sont, quand à elles, représentées par des modèles quantitatifs et/ou qualitatifs. Le choix d'une de ces méthodes dépend essentiellement des connaissances disponibles sur le procédé, sans oublier les considérations techniques et économiques. Néanmoins, nous avons constaté que ces méthodes ont des limitations et qu'un cadre de travail pour la résolution des problèmes de façon collective, utilisant des raisonnements différents et parallèles, s'avère être une alternative attractive pour relever les défis du diagnostic d'unités industrielles complexes.

2

Système Instrumenté de Sécurité

2.1. 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. Ceux-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.

2.2. Notions de sécurité :

Selon [DES et al 03], 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 02] 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.

2.2.1. Principes généraux de protection :

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

2.2.1.1. 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).

2.2.1.2. 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…) [SEL 07].

2.2.2. Sécurité fonctionnelle :

2.2.2.1. Définitions :

Selon la norme IEC 61061 [IEC61061 98], 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 02], 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.

2.2.2.2. 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 02] et l'IEC 61511 [IEC61511 03] 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.

2.3. Cadre normatif :

2.3.1. 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 02] 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 2.1), 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.

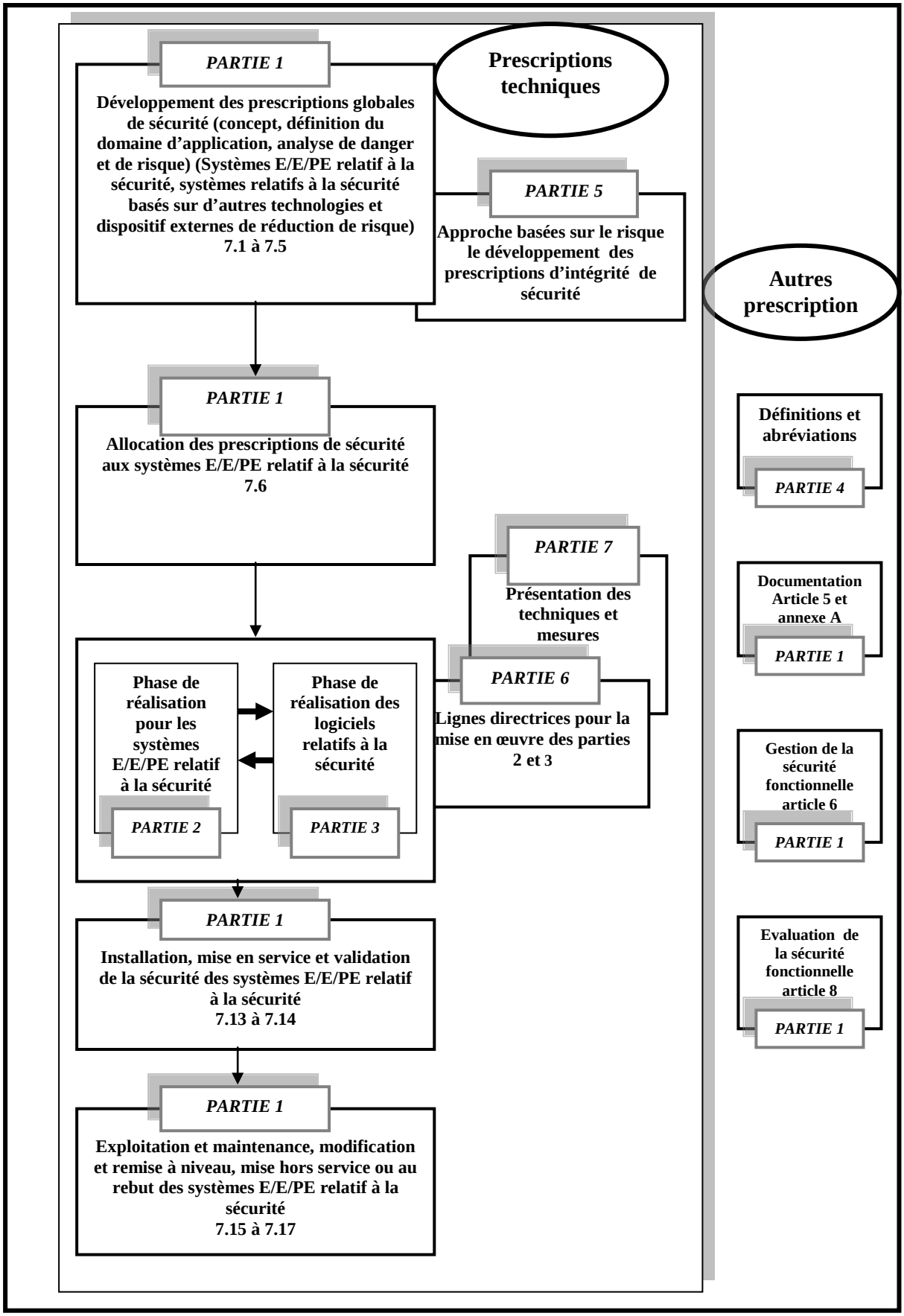


Figure 2.1. Structure générale de la norme IEC 61508 [IEC61508 02]

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 2.2) [SMI 04] montre la norme CEI 61508 générique et ses normes filles par secteur d'activité

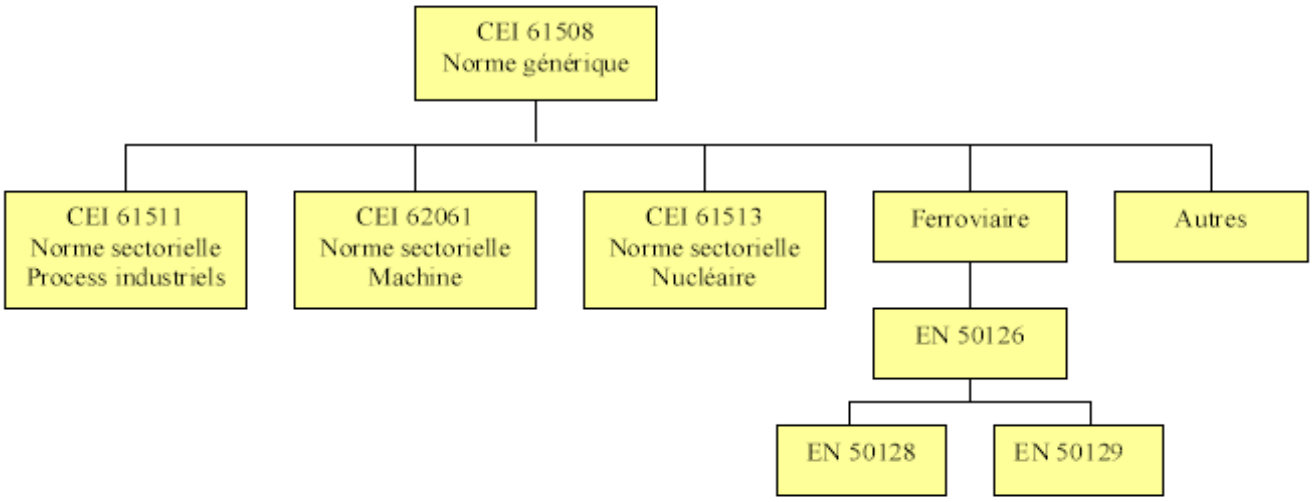


Figure 2.2. Norme CEI 61508 et normes dérivées [SMI 04]

L'IEC 61508 [IEC61508 02] 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.

2.3.2. 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.

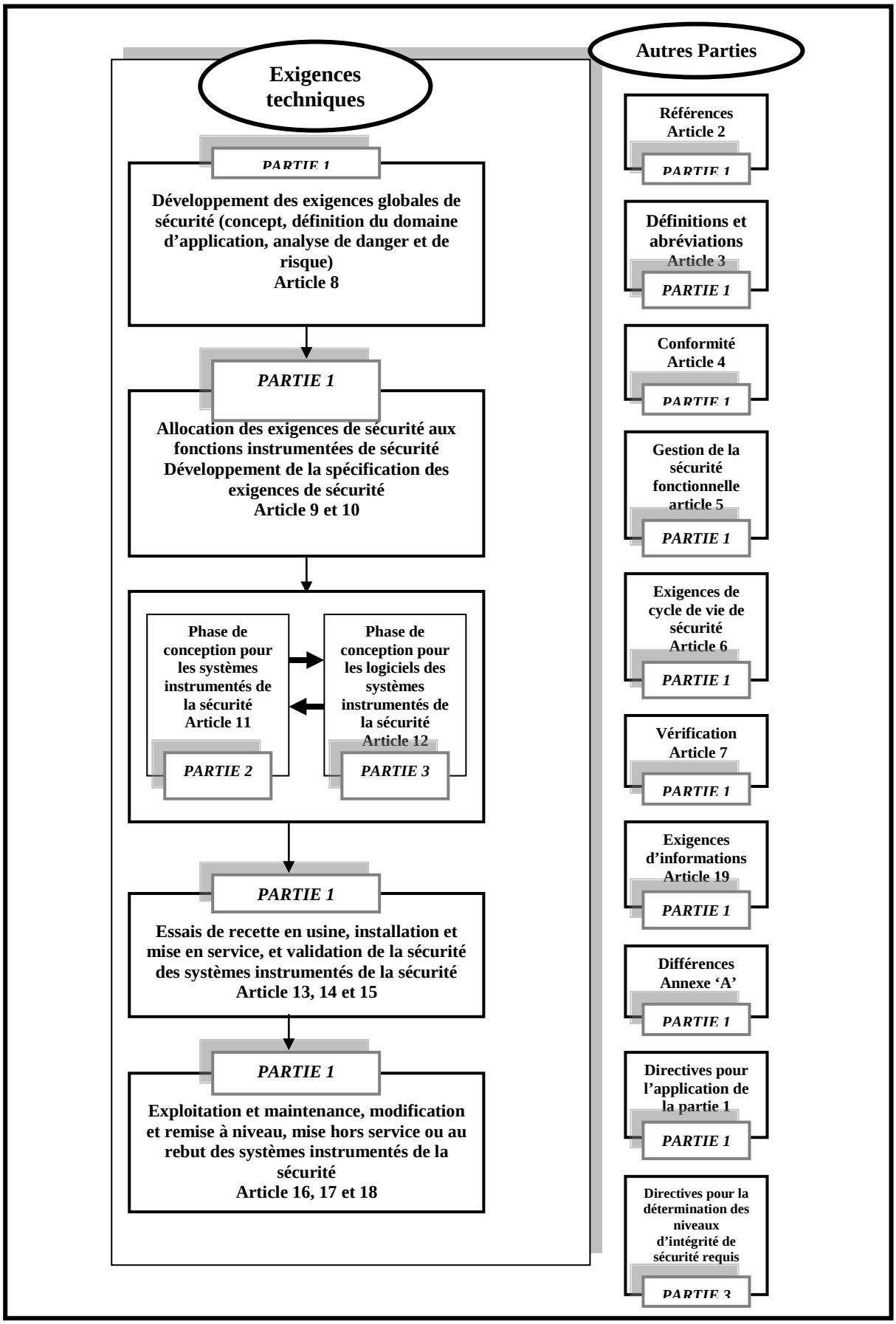


Figure 2.3. Structure générale de la norme IEC 61511 [IEC61511 03]

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 03].

2.3.3 Norme CEI 62061

La norme CEI 62061 [IEC62061 05] 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 96] 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 [RIQ 05].

2.3.4. 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 [SUM 00].

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 04]. 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 96]. 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 [RIQ 05].

2.4. Systèmes instrumentés de sécurité :

2.4.1. Définition d'un SIS :

La norme CEI 61511 [IEC61511 03] 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 02] 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…) [SEL 07].

2.4.2. 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 00].

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.

Une fonction instrumentée de sécurité est spécifiée pour s'assurer que les risques sont maintenus à un niveau acceptable par rapport à un événement dangereux spécifique.

Une fonction instrumentée de sécurité est à réaliser par un système instrumenté de sécurité (ou par une combinaison des composantes de ce système), par un système relatif à la sécurité basé sur une autre technologie ou par un dispositif externe de réduction de risque. [MKH 08]

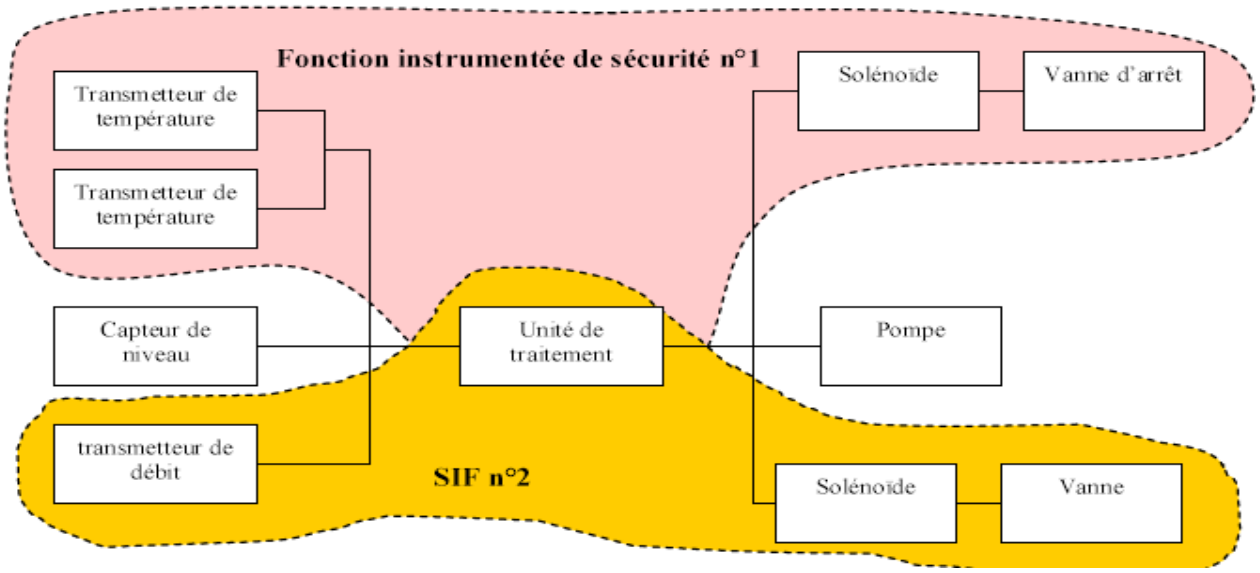


Figure 2.4. Fonction instrumenté de sécurité [MKH 08]

Pour illustrer et rendre plus claire cette définition, nous proposons l'exemple d'un équipement utilisé dans la fonction instrumentée de sécurité (Figure 2.5).

Cette dernière est conçue pour protéger un réservoir sous pression contenant un liquide inflammable lorsqu'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.

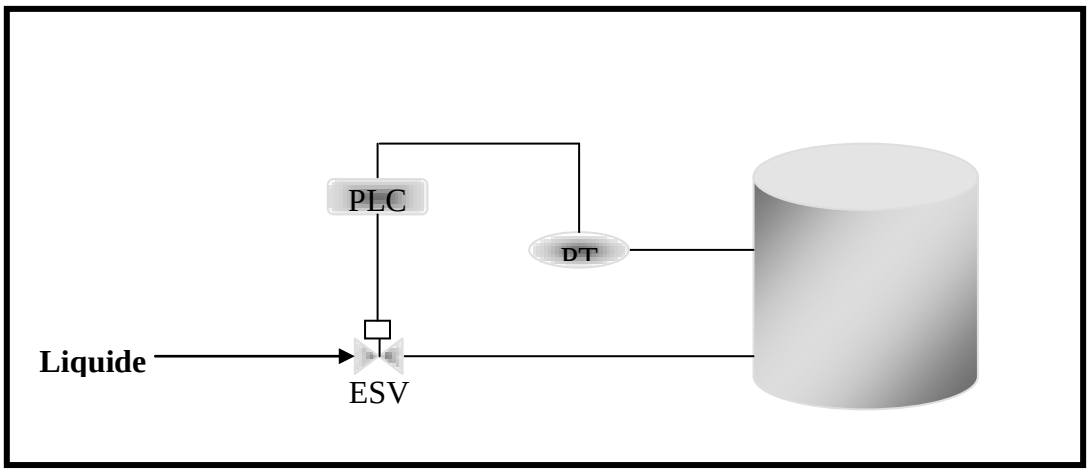


Figure 2.5. Exemple de fonction instrumenté de sécurité [FAL 00]

2.4.3. 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.

2.4.4. Composition d'un SIS :

2.4.4.1. 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 [AYA 05].

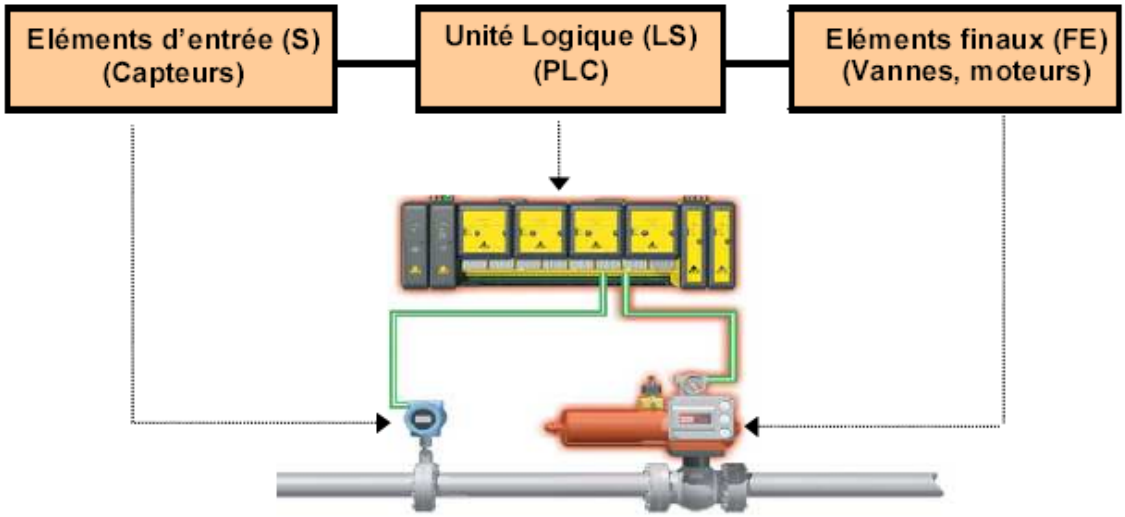


Figure 2.6. Schéma d'un SIS [INN 08].

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 [AYA 05].

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 [AYA 05]. 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 [AYA 05].

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".

2.4.4.2. 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.

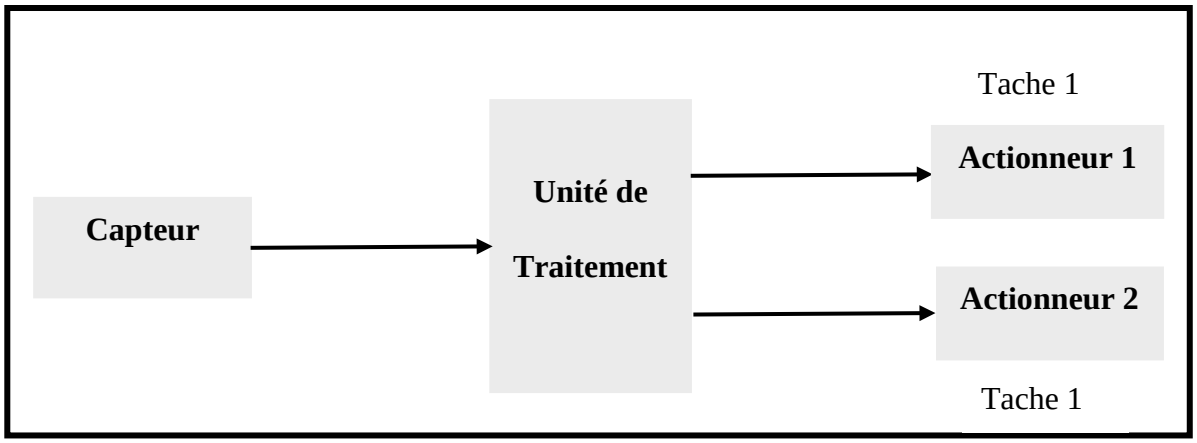


Figure 2.7. Schéma d'un SIS effectuant plusieurs taches

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 (Figure 2.7).

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).

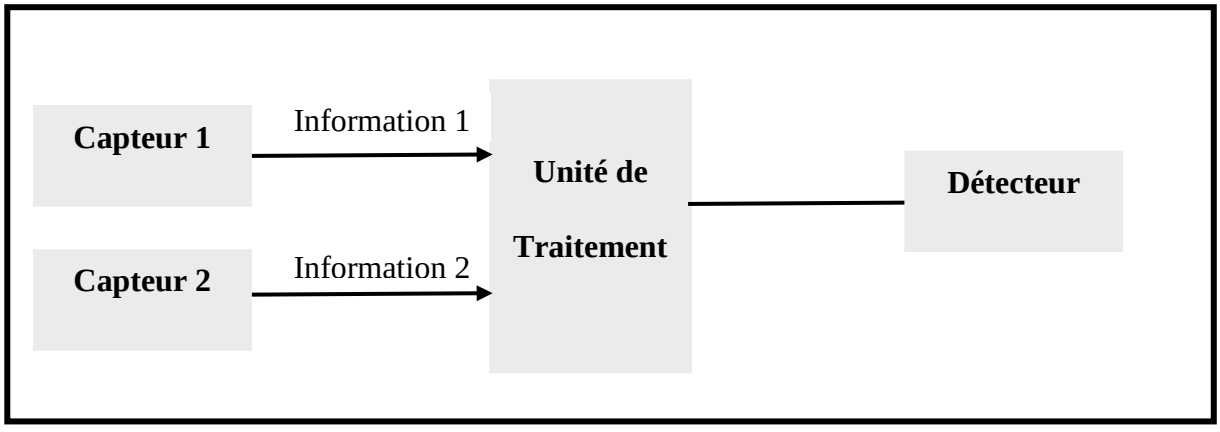


Figure 2.8. Schéma d'un SIS recevant plusieurs informations

2.4.5. 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 majoritaire 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.

- **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.

2.4.6. Tests de système instrumenté de sécurité :

Les normes et directives en matière de sécurité imposent de vérifier régulièrement l'état de fonctionnement des éléments constituant la chaîne de sécurité. Le niveau de SIL attribué à un SIS est calculé en prévoyant des tests périodiques sur les différents éléments qui composent le système.

Les normes mentionnent clairement les tests en ligne et hors ligne comme une condition pour maintenir le niveau de SIL pour les systèmes de sécurité.

Si toutes les défaillances étaient détectées, il ne serait pas nécessaire de vérifier périodiquement les éléments entrant dans la composition d'un SIS.

Le problème posé parfois est celui de la périodicité de ces tests et la planification des arrêts des procédés pour maintenance qui deviennent de moins en moins fréquents. En effet, il paraît déraisonnable d'interrompre délibérément la production dans un procédé pour tester une vanne qui ne sera peut-être jamais sollicitée. Du coup, dans certains cas, il faut parfois attendre six ans pour avoir l'occasion de tester une vanne d'arrêt hors ligne [GRU 98].

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 :

2.4.6.1. 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 [LAM 02]**.**
Le diagnostic (test en ligne) et les inspections visuelles sont des moyens très importants pour vérifier si un SIS est capable d'atteindre ses fonctions de sécurité et de révéler les défaillances qui entravent la mise en sécurité du procédé au moment où il y a une demande [LUN 07].
Le diagnostic est un moyen de détection en ligne des déviations, des dégradations et des divergences et il est souvent réalisé par du matériel et du logiciel dédiés et implémentés dans les dispositifs (par exemple, les chiens de garde).

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).
Les défaillances détectées par les tests de diagnostic sont appelées défaillances dangereuses détectées [CEI 00]. D'autres métriques sont aussi spécifiées par la norme. La figure suivante illustre la répartition des défaillances selon la norme.

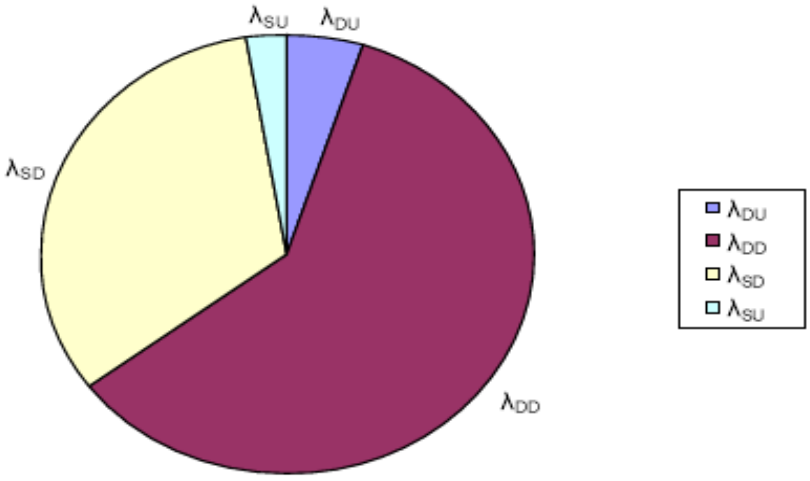


Figure 2. 9. Proportion de défaillances selon un exemple illustré dans la norme [CEI 00]

- λ_{DD} : Taux de défaillances dangereuses détectées,
- λ_{DU} : Taux de défaillances dangereuses non détectées,
- λ_{SD} : Taux de défaillances en sécurité détectées,
- λ_{SU} : Taux de défaillances en sécurité non détectées.

2.4.6.2. Proof Test :

La norme définit le test périodique comme un essai effectué pour révéler des défauts non détectés dans un système instrumenté de sécurité, de telle sorte que, au besoin, le système puisse être restauré dans sa fonctionnalité de conception.

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) [LAM 02]**.** 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.
Il existe deux types de tests de diagnostics [LAM 02] :

- Les diagnostics de référence : comparaison par rapport à une valeur prédéterminée comme la mesure de la période (watch dog), le rebouclage de toutes les sorties sur une entrée,
- Les diagnostics par rapport à une opérationnelle

La norme CEI 61508 définit un taux de couverture de diagnostic pour les tests automatiques de diagnostic comme le rapport de taux de défaillances dangereuses détectées (par un test de diagnostic) sur le taux total des défaillances dangereuses (détectées et non détectées).

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{dangereuses}} \qquad (2.1)$$

Ce taux de couverture de diagnostic reflète la qualité et l'étendue des tests automatiques en ligne. Sa grande valeur désigne la pertinence de traitement des défaillances détectées par leur détection. Plus ce taux est important, plus grande est la confiance dans le système instrumenté de sécurité du fait que les situations sûres prédominent par rapport aux situations dangereuses lors de l'occurrence de défaillances.
Les tests périodiques et les inspections visuelles sont réalisés alors qu'il y a arrêt de production. Ils sont destinés à révéler les défaillances non détectées par les tests en ligne. Ils sont réalisés à des intervalles réguliers. La durée de ces intervalles a une conséquence directe sur la probabilité de défaillance sur demande relative à la fonction de sécurité exécutée. Les défaillances révélées par ce type de tests sont appelées par la norme défaillances dangereuses détectées.
Dans plusieurs cas, les tests et les inspections visuelles sont exécutés manuellement. Cependant, les tests sont devenus automatiques avec les nouvelles technologies comme par exemple le test partiel de course de vanne [SUM 00b].

2.4.6.3. L'avantage des tests dans les SIS :

La tendance vers l'utilisation des instruments intelligents dans les applications de sécurité est motivée par la capacité qu'offre ce type d'instruments à être diagnostiqués en ligne mais aussi au pouvoir de validation en regard des conditions environnantes [NOB 04] [MAC 04].

Les tests périodiques assurent la détection des pannes cachées afin de maintenir la sécurité fonctionnelle prescrite. L'impact des tests périodiques sur la disponibilité est montré dans la figure suivante :

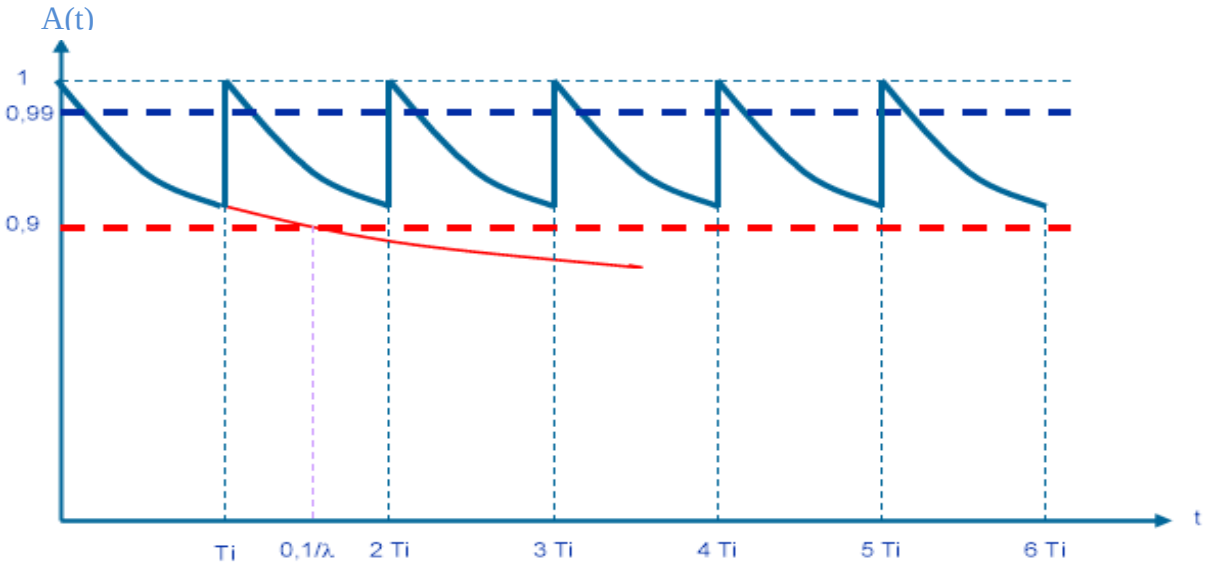


Figure 2.10. Impact des tests périodiques sur la disponibilité

La figure (2.10) 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 métrique R(t) exprime tout simplement l'inverse de la probabilité de défaillance sur demande PFD et l'on voit bien qu'en absence de tests périodiques, la valeur de R(t) se dégrade nettement et sort de la bande [0,9 0,99], par conséquent le SIL ne peut plus être maintenu à sa valeur.

Les tests dans les éléments finaux typiquement les vannes d'arrêt se concrétisent partiellement sur une partie de la course. Ces tests partiels peuvent être pratiqués à des périodes très rapprochées afin de permettre le maintien du niveau SIL au niveau initial.

2.4.6.4. Test partiel de la course de vanne (PVST) :

Les actionneurs constituent le maillon le plus faible de la boucle de sécurité [RAJ 05]. C'est pourquoi bon nombre de fabricants et chercheurs se sont penché sur la question afin de proposer des solutions. Un cas particulier des actionneurs est celui des vannes utilisées dans

les systèmes instrumentés de sécurité. Ces vannes sont considérées comme les composants les plus fragiles du fait qu'elles restent sans bouger pendant de longues périodes, et les obturateurs auront tendance à se coller.

Capteurs	Unités de traitement	Actionneurs
35 %	**15 %**	**50 %**

Tableau 2.1. Proportion de défaillances relatives aux constituants d'un SIS [AUB 04]

Une solution proposée tant par les fabricants que les chercheurs consiste à réaliser des tests périodiques sur une partie de course de l'obturateur de la vanne ce qui est communément appelé PVST (Partial Valve Stroke Testing : Test Partiel de la Course de Vanne).

Le problème rencontré souvent dans les vannes est le blocage en fermeture ou en ouverture du fait qu'il s'agit de dispositifs statiques qualifiés de dormants. Ces éléments ne sont appelés à réagir qu'au moment où il y a une demande suite à un danger qui se présente. Malheureusement, du fait de la durée importante du non réaction (leur mise en repos) de ces vannes, un certain nombre d'entre elles ne répond pas au moment opportun et elles restent coincées dans leur position de repos.

C'est pourquoi le PVST consiste à tester régulièrement les vannes sur un pourcentage de leur course (10 à 20%) afin de s'assurer que celles-ci ne resteront pas bloquées lorsqu'on en aura besoin. La vanne se trouve actionnée sur une partie de sa course pour tester sa fonctionnalité sans interruption de la production. La proportion de 20 % de la course est choisie en se référant au principe de Pareto (règle des 80/20) [PAR 01], ce test à 20% permet de déceler 80% des défauts.

Le PVST a cependant des limites. Le test de course partielle ne garantit pas que la vanne fonctionne lorsqu'elle sera sollicitée pour une fermeture complète. En effet, il se peut qu'il y ait un blocage au niveau de la nouvelle butée et donc que la vanne ne se ferme pas complètement mais uniquement à 20% de sa course.

L'élément qui détermine la position de la vanne est le positionneur de vanne. Il est doté d'intelligence. Il est monté sur des organes de réglage et détermine une position bien précise de la vanne par rapport au signal de commande (grandeur directrice élaborée par un microprocesseur). Il compare le signal de commande provenant d'un dispositif de réglage avec la course de l'organe de réglage et émet une pression d'air.

D'autres solutions alternatives au PVST consistent à utiliser une vanne de dérivation (bypass) autour des vannes d'arrêt ou prévoir une redondance. Ces solutions sont ou coûteuses ou potentiellement dangereuses [GRU 98]. En effet, le doublement du nombre de vannes augmente le coût de l'équipement de base, mais aussi les coûts de mains d'œuvre liés aux essais de maintenance puisque les tests périodiques portent sur un nombre plus élevé de vannes. En plus, les coûts de la tuyauterie supplémentaire pour les vannes de dérivation sont importants. Le danger peut provenir d'une vanne de dérivation qui ne peut remplacer la vanne d'arrêt au moment de test de celle-ci hors ligne.

2.4.7. Niveau d'intégrité de sécurité (SIL) :

Les normes IEC 61508 [IEC 61508 02] et IEC 61511 [IEC61511 03] 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 [IEC61508 02] ou des fonctions instrumentés de sécurité selon la norme IEC 61511 [IEC61511 03].

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 [BEU 06]. 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 02] 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 02], en 04 niveaux (plus le SIL est élevé, plus la disponibilité du système de sécurité est élevée) (tableaux 2.2 et 2.3).

FONCTIONNEMENT A LA SOLLICITATION		
Niveau d'intégrité de sécurité (SIL)	**Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})**	**Réduction de risque cible (RR)**
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$100\,000 \leq RR < 10\,000$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10\,000 \leq RR < 1\,000$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$1\,000 \leq RR < 100$
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$100 \leq RR < 10$

Tableau 2.2. Niveaux d'intégrité de sécurité : Probabilité de défaillances lors d'une sollicitation

FONCTIONNEMENT A MODE CONTINU	
Niveau d'intégrité de sécurité (SIL)	**Probabilité de défaillance dangereuse par heure**
4	$10^{-9} \leq PFD_{avg} < 10^{-8}$
3	$10^{-8} \leq PFD_{avg} < 10^{-7}$
2	$10^{-7} \leq PFD_{avg} < 10^{-6}$
1	$10^{-6} \leq PFD_{avg} < 10^{-5}$

Tableau 2.3. Niveaux d'intégrité de sécurité : Probabilité de défaillances dangereuses de la SIF

Dans ces deux tableaux, les fonctions instrumentées de sécurités ainsi que les systèmes instrumentés de sécurité sont différenciés selon le mode de fonctionnement par l'utilisation des

paramètres PFDavg et PFH. Chaque SIL est délimité par une borne maximale et une borne minimale [MKH 08].

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 02] :

$$PFD_{SYS} = PFD_C + PFD_U + PFD_A \quad (2.2)$$

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.

2.4.7.1. 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).

2.4.7.2. 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 96], [SUM 00].
  - Les arbres de défaillances [BEC 01], [GOB 98].
  - Les chaînes de Markov [GOB 98], [BUK 95], [ZHA et al 03], [BUK 05] : 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.

2.5. Réduction des risques par le SIS :

2.5.1. Les SIS comme couche de protection :

La figure (2.11) montre le concept des couches de protection et la composition des différents types de systèmes relatifs à la sécurité (SRS) comme définis dans la norme CEI 68511-3. Il est à noter qu'il existe une distinction claire entre les BPCS et les SIS comme composantes des couches de protection. L'objectif primaire d'un BPCS est d'optimiser les conditions de conduite de procédé afin de maximiser la qualité et la production. Les systèmes instrumentés

de sécurité s'appliquent pour prévenir des situations dangereuses (prévention) et réduire les conséquences d'événements dangereux (protection). La distinction est motivée par le fait que le BPCS n'est nécessairement pas utilisé pour contribuer à la réduction de risque et parfois il est lui-même source de risques potentiels. [MKH 08]

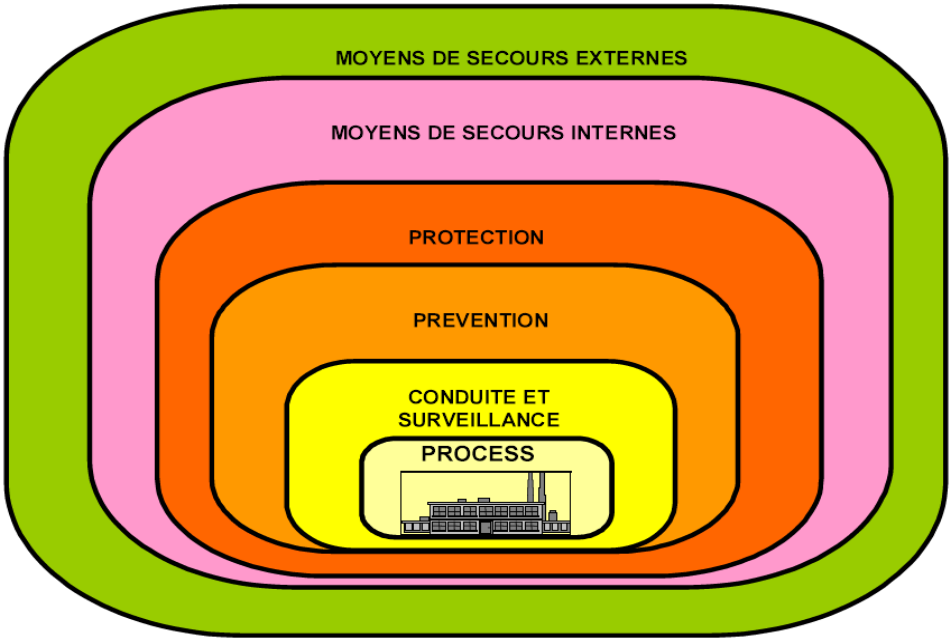


Figure 2.11. Concept de couches de protection

Les méthodes de réduction sont de différents types et concernent tout d'abord le procédé dont la conception doit être plus au moins sûre. La conduite et la surveillance sont assurées par les systèmes de commande de procédés de base (BPCS), les systèmes de surveillance (alarmes du procédé) et par la surveillance des opérateurs.

La partie prévention des couches de protection est assurée par les dispositifs de sécurité mécaniques, par les alarmes suivies d'action et par les systèmes instrumentés de sécurité de prévention. La protection est assurée par des dispositifs de sécurité mécaniques, la supervision par l'opérateur et par les systèmes instrumentés de sécurité d'atténuation [KNE 02]. Les moyens de secours internes et externes concernent respectivement les procédures d'évacuation lors de l'occurrence d'une situation critique ainsi que la réaction du public après une radiodiffusion d'urgence

Il faut noter qu'il existe un amalgame à propos de l'emplacement des systèmes instrumentés de sécurité comme couche de protection. Certains auteurs qualifient la couche allouée à ce type de systèmes comme une couche de prévention [KNE 02] (la norme aussi d'ailleurs) [CEI 03] alors que ce type de systèmes est voué uniquement à la protection par la réduction du risque nécessaire de telle sorte que ce risque devienne tolérable [MKH 08].

2.5.2. Réduction des risques :

Le schéma suivant, issu de l'annexe C de la norme 61508-5, rend compte le concept de réduction du risque.

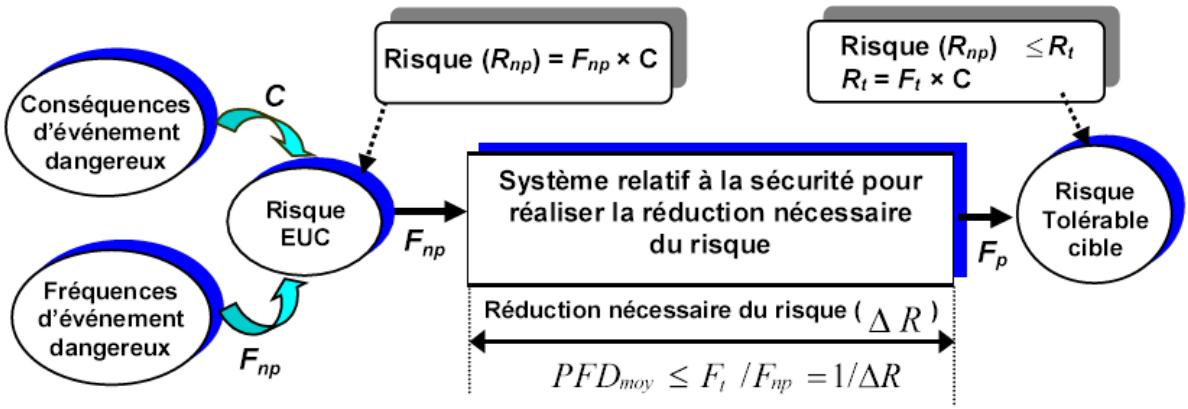


Figure 2.12. Réduction nécessaire du risque réalisée par un seul SIS [INN 08]

2.6. Problèmes typiques des systèmes instrumentés de sécurité :

Une étude réalisée par [HSE 95] a illustré l'origine d'un nombre de défaillances de systèmes conduisant à des événements dangereux très sérieux.

Les défaillances des systèmes ne sont pas tout simplement dues à des opérations incorrectes. En effet, les défaillances concernent les différentes étapes de la durée de vie d'un système (figure 2.13).

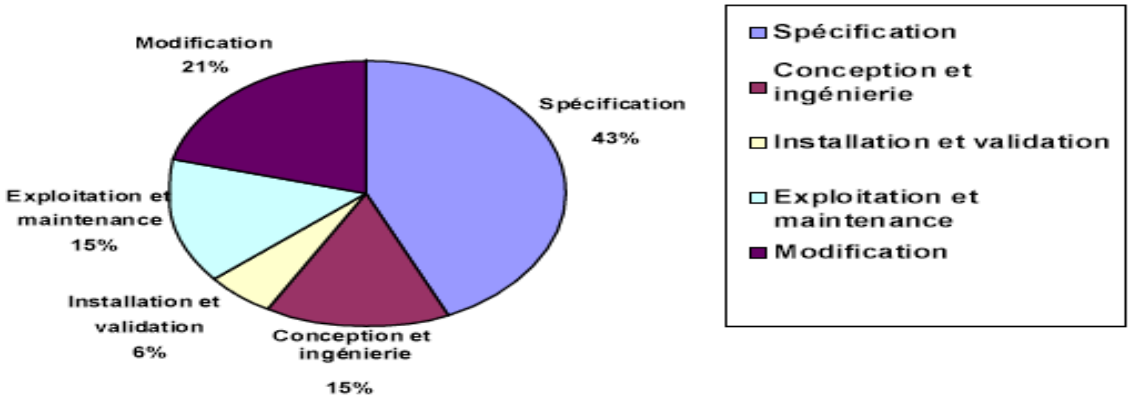


Figure 2.13. Causes primaires des défaillances des systèmes de commande [HSE 95].

Shell [SHE 98] a réalisé une autre étude illustrative à l'usine nationale de GNL en Oman au Moyen-Orient. Le procédé de production complet a été composé des systèmes de

rétablissement de champ, d'une installation de transformation centrale, et d'un complexe de liquéfaction. Pendant une étude de sécurité basée sur l'intégrité de sécurité SIL, la conclusion est que :

- 67% des fonctions instrumentées de sécurité (SIF) semblent sur-calibrées en terme de SIL,
- 27% n'exigent aucun changement. Elles sont correctement calibrées,
- 6% des SIF semblent sous-calibrées.

Shell a réalisé un certain nombre de ces études sur différents sites qui ont présenté des résultats comparables.

Les fautes pourraient avoir été produites pendant l'évaluation des risques et la spécification des conditions de sécurité ; des défaillances pourraient également avoir été faites pendant la conception et l'exécution du SIS, ou pendant la validation. Généralement après avoir passé en revue les deux études précédentes, la conclusion tirée est que les défaillances pourraient se produire à différentes étapes du cycle de vie [MKH 08].

2.7. Classification des défaillances :

2.7.1. Classification retenue dans la norme :

La norme distingue les défaillances aléatoires du matériel et les défaillances systématiques.

Défaillances aléatoires du matériél : « défaillances survenant de manière aléatoires et résultant de divers mécanismes de dégradations au sein du matériel »

Défaillances systématiques : « défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropries ».

Les défaillances aléatoires du matériel sont relativement bien comprises. Les données relatives à cette catégorie de défaillances sont, dans la plupart du temps, disponibles.

Les défaillances systématiques sont difficiles à modéliser et de ce fait moins compréhensibles.

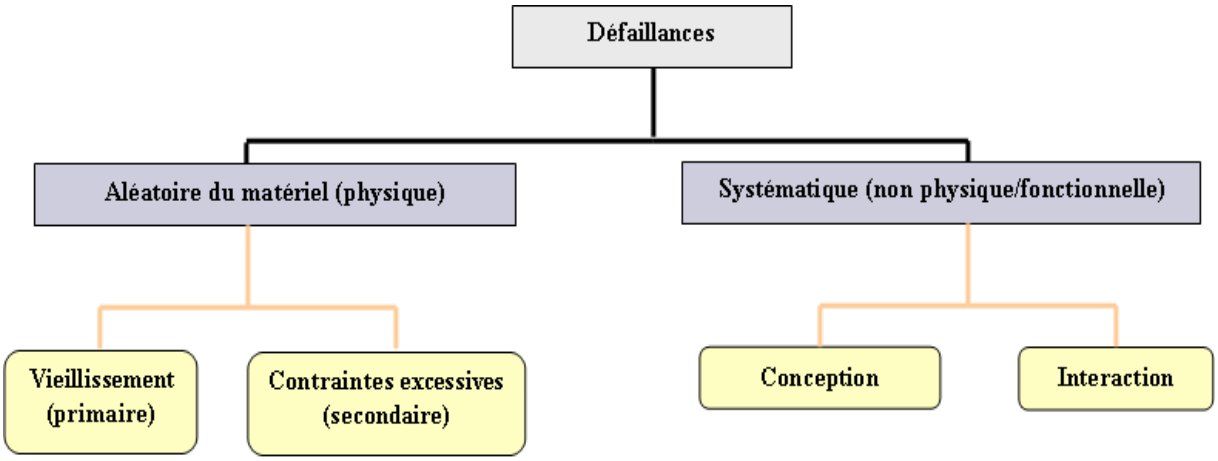


Figure 2.14 Classification des défaillances selon leurs causes

Dans ces conditions, la norme distingue, à la page 40 de son volume 4, les défaillances dangereuses, des défaillances sûres :

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

Une autre partition résulte du fait que ces défaillances peuvent être ou non détectées par des tests en ligne. Les premières sont dénommées défaillances détectées (detected failures) et les secondes, qui ne peuvent être révélées que lors de tests périodiques hors ligne ou lors de la sollicitation du SIS par l'EUC, sont dénommées défaillances non détectées (undetected failures). Le schéma suivant est classiquement présenté pour résumer cette double partition.

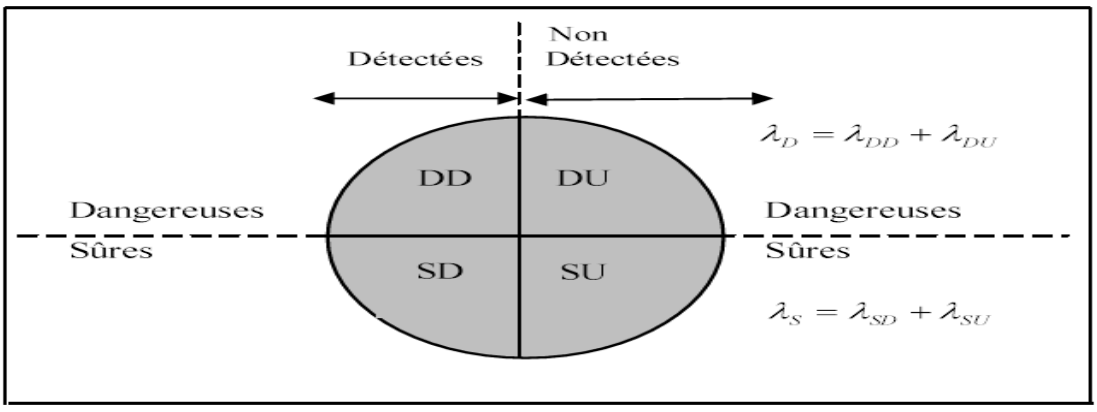


Figure 2.15. Typologie des défaillances selon la norme CEI 61508

La simplicité de cette classification appelle trois commentaires :

- La première définition n'est pas auto-suffisante car elle est « à tiroirs » (défaillance dangereuse → état dangereux). Il conviendrait donc de définir auparavant ce qu'est un état dangereux. Ce qui n'est pas fait explicitement dans la norme qui renvoie aux notions de situation dangereuse et d'événement dangereux. La notion d'événement redouté serait plus appropriée, car ce type d'événement est plus facile à identifier comme résultant de la présence d'un état dangereux (le SIS est indisponible et donc dans l'impossibilité de remplir sa fonction) et de la survenue d'une demande émanant de l'EUC qui doit être protégé.

- Les défaillances en sécurité sont définies par opposition (ici aux défaillances dangereuses), c'est-à-dire par ce qu'elles n'entraînent pas. Il aurait été plus simple de les définir « positivement », ce qui aurait permis de mieux les situer par rapport aux défaillances intempestives (spurious trip failures) qui ne sont même pas citées dans la norme. Ces dernières défaillances correspondent, par exemple, à un déclenchement inopportun d'une action de sécurité. Un exemple illustratif de ce type de défaillance est le cas d'un système de détection de surpression qui envoie un signal à l'unité de décision qui, à son tour commandera la fermeture de vannes de sécurité, alors qu'en réalité il n'y a pas de surpression.

- Cette classification des défaillances conduit à celle des taux de défaillance correspondants, qui est systématiquement utilisée dans la norme. Ceci est une source d'ambiguïté, car si l'on peut en général aisément qualifier de dangereux ou de sûr un taux de défaillance d'un composant, il n'en est pas de même dans le cas d'un système, même simple. C'est pourquoi l'option de définir avec précision les différents états dans lesquels peut se trouver un système est préférable à l'option de définir directement ses taux de défaillance dangereux et sûrs. La définition de ces derniers et des défaillances possibles du système résultera d'ailleurs de l'identification préalable de ses états potentiels, comme nous le verrons bientôt.

2.7.2. Classification proposée par SINTEF

Cet organisme propose, dans son manuel [SIN 06], une classification plus fine et plus réaliste que la précédente, puisqu'elle prend en compte les défaillances intempestives et les défaillances non critiques qui sont définies ci-après. Cette classification est résumée par l'arborescence suivante :

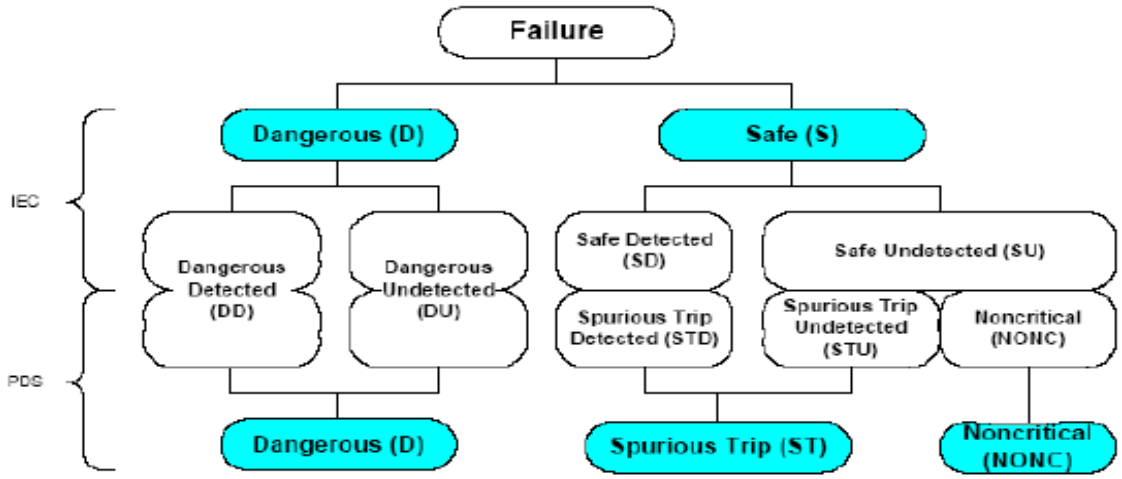


Figure 2.16. Classification des défaillances selon SINTEF [SIN 06].

Pour résumer, la méthode PDS de SINTEF considère, au niveau des composants, trois types de défaillances : dangereuses, intempestives et non critiques.

- Les défaillances dangereuses sont celles de la norme et se divisent donc en défaillances détectées LDD et non détectées LDU.
- Les défaillances intempestives sont un sous-ensemble des défaillances sûres et se divisent également en défaillances détectées LSTD) et non détectées LSTU.
- Les défaillances non critiques LNONC sont celles qui n'ont aucune incidence sur les deux fonctions principales du système EUC, c'est-à-dire son aptitude à produire (disponibilité de production) et son aptitude à ne pas engendrer d'événements redoutés (sécurité).

Défaillances de causes communes :

La norme IEC 61508 introduit également des défaillances de causes communes (DCC) pour les architectures redondantes qui peuvent apparaître dans les canaux suite à une même cause. L'étude des modes communs ont été réalisés par différents auteurs [FLE 74]; [MOS 87]; [HAU 06].

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

Les défaillances de mode commun peuvent être introduites dans les calculs de la PFDavg des SIS de façon directe. On évalue les paramètres de calcul à partir de données issues du retour d'expérience [MEC 11].

2.8. Contraintes architecturales :

Il est écrit dans la norme 61508-2 (paragraphe 7.4.3.1) que, « dans le contexte de l'intégrité de sécurité du matériel le niveau d'intégrité le plus élevé qui peut être annoncé pour la fonction de sécurité donnée est limité par la tolérance aux anomalies du matériel et la proportion de défaillances en sécurité des sous-systèmes qui réalisent la fonction de sécurité ».

La norme définit alors ces deux nouveaux termes :

- Une tolérance aux anomalies du matériel d'indice N signifie que (N+1) anomalies sont susceptibles de provoquer la perte de la fonction de sécurité.

- La proportion de défaillances en sécurité d'un sous-système (Safe Failure Fraction ou SFF) est définie par le rapport du taux moyen des défaillances en sécurité, plus les défaillances dangereuses détectées au taux de défaillance moyen total du sous-système.

La démarche présentée dans l'annexe C de la norme 6 1508-2 s'appuie sur deux tableaux reproduits ci-après (tableaux 2.4 et 2.5).

Proportion de défaillances en sécurité (SFF)	Tolérance aux anomalies matérielles		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
>= 99 %	SIL 3	SIL 4	SIL 4
Un SIS peut être considéré du type A si son comportement en présence d'anomalies est bien déterminé, si les modes de défaillance de ses constituants sont bien définis et si les données concernant leurs défaillances, issues du retour d'expérience, sont connues avec une bonne fiabilité.			

Tableau 2.4. Contraintes architecturales sur les SIS du type A

Proportion de défaillances en sécurité (SFF)	Tolérance aux anomalies matérielles		
	0	1	2
< 60 %	Non autorisé	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
>= 99 %	SIL 3	SIL 4	SIL 4
Un SIS peut être considéré du type B si une des trois conditions régissant le type A n'est pas satisfaite.			

Tableau 2.5. Contraintes architecturales sur les SIS du type B

Pour chaque sous-système d'un SIS qui participe à la réalisation d'une SIF, on calcule la SFF et la tolérance aux anomalies (N = 0 à 2). Le croisement de ces deux entrées orthogonales donne, pour chacun des tableaux précédents, la valeur maximale du SIL qu'on peut annoncer pour chaque sous-système. La valeur maximale autorisée pour le SIL de la fonction de sécurité est obtenue en appliquant les règles de combinaison illustrées au sous paragraphe 7.4.3.1.6 de la norme 61508-2.

L'objectif déclaré dans la norme concernant la prise en compte des contraintes architecturales est qu'elle permet d'obtenir, pour tout sous-système et donc pour le SIS, une architecture robuste qui tienne compte de la complexité. [INN 08]

2.9. 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 sont des 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 utilisée pour analyser et évaluer la sûreté de fonctionnement des systèmes réparables. L'objectif du chapitre suivant est l'évaluation de la performance (en terme probabiliste) des SIS.

3

Évaluation de la Performance des Systèmes Instrumentés de Sécurité

3.1. Introduction :

Pour l'évaluation du niveau d'intégrité de sécurité (SIL) 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 présent chapitre est consacré à la détermination des PFD_{avg} des différentes architectures en utilisant la méthode de graphe de Markov.

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

- 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.

Et lorsque $\begin{cases} \lambda = \lambda_{DD} + \lambda_{DU} \\ \dfrac{1}{\mu_{DD}} = MTTR \\ \lambda_{DU} \prec\prec \mu_{DU} \\ \lambda_{DD} \prec\prec \mu_{DD} \\ \lambda_{DD}\lambda_{DU} \approx 0 \\ \lambda_{DD}\lambda_{DU} \prec\prec \mu_{DD}\mu_{DU} \end{cases}$

On peut déduire les résultats donner parla norme.

3.2. Architecture 1001

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 [IEC61508].

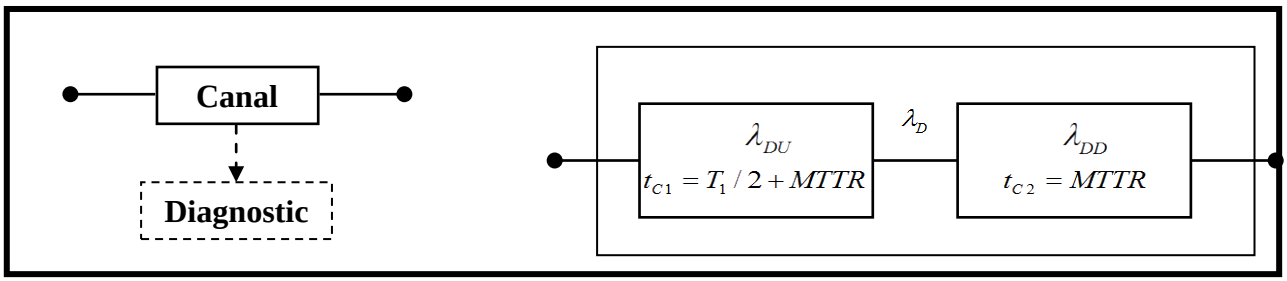


Figure 3.1. Diagrammes blocs physique et de fiabilité 1oo1

La figure (Figure 3.1) 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}.

Ce système étant périodiquement testé (intervalle entre tests égal à T1), son comportement au cours d'une mission de durée donnée est correctement décrit par un modèle markovien multi-phases. [INN 08]

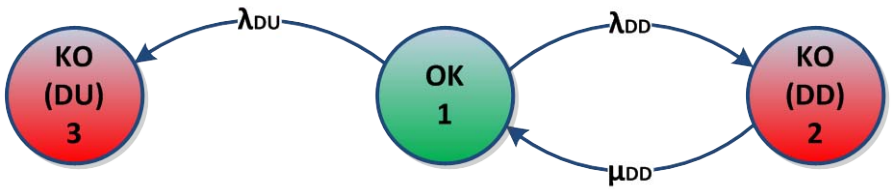


Figure 3.2. Modèle markovien multi-phases de l'architecture 1oo1 [INN 08]

Les formules analytiques déduites de ce modèle sont déjà « lourdes » et les calculs afférents requièrent l'usage d'un logiciel adapté. Ainsi, pour les rendre plus accessibles, il est nécessaire d'approximer le modèle précédent par un modèle markovien classique « continu » donné à la figure 3.3

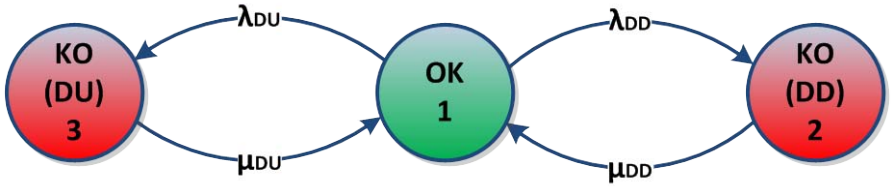


Figure 3.3. Modèle markovien continu de l'architecture 1oo1

3.2.1. 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 [ZHA et al 03].

Donc :

$$t_{C1} = T_1 - t_{DU} + MTTR \qquad (3.1)$$

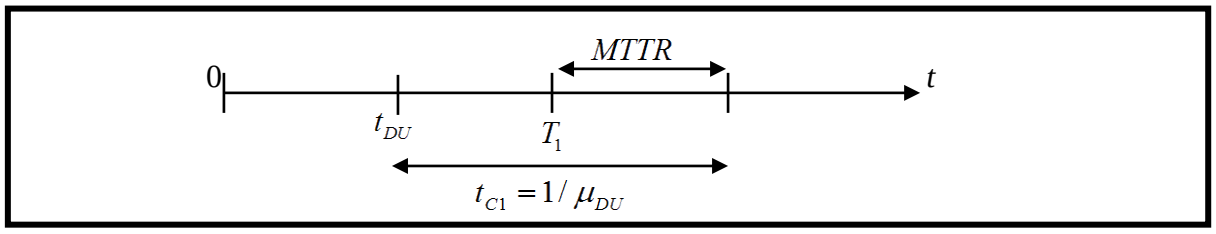


Figure 3.4. Processus d'occurrence d'une défaillance non détectée sur [0, T_1]

L'instant t_{DU} peut être déterminé avec l'utilisation d'une approche barycentrique, en résolvant l'équation suivante [INN et al 05]:

$$t_{DU} = \frac{\int_0^{T_1} t.f(t).dt}{\int_0^{T_1} f(t).dt}$$

$f(t) = \lambda_{DU} \exp(-\lambda_{DU}.t)$ fonction de densité

$$t_{DU} = \frac{\int_0^{T_1} t.\lambda_{DU} \exp(-\lambda_{DU}.t).dt}{\int_0^{T_1} \lambda_{DU} \exp(-\lambda_{DU}.t).dt} = \frac{\int_0^{T_1} t.\lambda_{DU} \exp(-\lambda_{DU}.t).dt}{1-\exp(-\lambda_{DU}.T_1)}$$

On utilise l'intégrale par partie donc on obtient :

$$t_{DU} = \frac{1/\lambda_{DU}(1-\exp(-\lambda_{DU}T_1)) - T_1 \exp(-\lambda_{DU}T_1)}{1-\exp(-\lambda_{DU}T_1)}$$

En approximant $\exp(-\lambda_{DU}T_1)$ par son développement limité au second ordre

$$\exp(-\lambda_{DU}T_1) = 1-\lambda_{DU}T_1 + 1/2\lambda_{DU}{}^2T_1{}^2 - 1/6\lambda_{DU}{}^3T_1{}^3 + ...$$

Et sachant que $\lambda_{DU}T_{1<<1,}$ t_{DU} devient :

$$t_{DU} \approx \frac{\lambda_{DU}T_1^2}{2}(1-\lambda_{DU}T_1)/\lambda_{DU}T_1(1-\frac{\lambda_{DU}T_1}{2}) \approx \frac{T_1}{2}$$

D'où $t_{C1} = T_1 - t_{DU} + MTTR = \frac{T_1}{2} + MTTR$ donc

$$\mu_{DU} = \frac{1}{\frac{T_1}{2} + MTTR} \qquad (3.2)$$

Le comportement du système au cours d'une mission de durée donnée est décrit par un modèle Markovien comme l'indique la figure (figure 3.5)

La figure 3.1 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}.

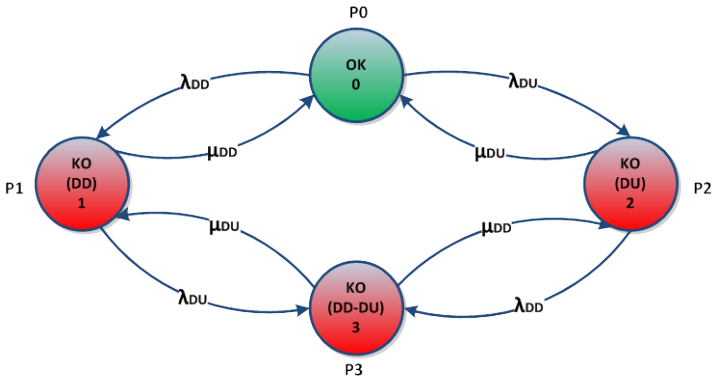


Figure 3.5. Graphe de Markov 1oo1 [ZHA et al 03]

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

Tableau 3.1 : Etats de système

3.2.2. Détermination de la disponibilité de l'architecture 1oo1 :

Les équations différentielles du système :

$$\begin{cases} P_0'(t) = -(\lambda_{DD} + \lambda_{DU})P_0(t) + \mu_{DD}P_1(t) + \mu_{DU}P_2(t) \\ P_1'(t) = \lambda_{DD}P_0(t) - (\lambda_{DU} + \mu_{DD})P_1(t) + \mu_{DU}P_3(t) \\ P_2'(t) = \lambda_{DU}P_0(t) - (\lambda_{DD} + \mu_{DU})P_2(t) + \mu_{DD}P_3(t) \\ P_3'(t) = \lambda_{DU}P_1(t) + \lambda_{DD}P_2(t) - (\mu_{DD} + \mu_{DU})P_3(t) \end{cases} \quad (3.3)$$

Avec $P' = M.P$ est l'équation d'état

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

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

La résolution du système d'équations 3.3, connaissant la distribution initiale $P(0) = [1 \quad 0 \quad 0 \quad 0]$ peut être effectuée par la transformation de LAPLACE.

Donc l'équation de Kolmogorov $P' = M.P$ devient :

$$P'(s) = P(0)[SI - M]^{-1} L^T{}_E \tag{3.4}$$

Où I est la matrice unité.

On en déduit :

$$[SI - M] = \begin{bmatrix} S + (\lambda_{DD} + \lambda_{DU}) & -\mu_{DD} & -\mu_{DU} & 0 \\ -\lambda_{DD} & S + (\lambda_{DU} + \mu_{DD}) & 0 & -\mu_{DU} \\ -\lambda_{DU} & 0 & S + (\lambda_{DD} + \mu_{DU}) & -\mu_{DD} \\ 0 & -\lambda_{DU} & -\lambda_{DD} & S + (\mu_{DD} + \mu_{DU}) \end{bmatrix}$$

Avec

$$[SI - M]^{-1} = \frac{adj[SI - M]}{\det[SI - M]}$$

Les racines du déterminant sont :

$S_1 = 0$, $S2 = -(\lambda_{DD} + \mu_{DD})$, $S3 = -(\lambda_{DU} + \mu_{DU})$, $S4 = -(\lambda_{DD} + \lambda_{DU} + \mu_{DD} + \mu_{DU})$

Nous avons l' $adj[SI - M] = cofacteurde[SI - M]^T$

$$[SI - M]^T = \begin{bmatrix} S + (\lambda_{DD} + \lambda_{DU}) & -\lambda_{DD} & -\lambda_{DU} & 0 \\ -\mu_{DD} & S + (\lambda_{DU} + \mu_{DD}) & 0 & -\lambda_{DU} \\ -\mu_{DU} & 0 & S + (\lambda_{DD} + \mu_{DU}) & -\lambda_{DD} \\ 0 & -\mu_{DU} & -\mu_{DD} & S + (\mu_{DD} + \mu_{DU}) \end{bmatrix}$$

Alors : $P'(s) = \frac{a}{S} + \frac{b}{S + \lambda_{DD} + \mu_{DD}} + \frac{c}{S + \lambda_{DU} + \mu_{DU}} + \frac{d}{S + \lambda_{DD} + \lambda_{DU} + \mu_{DD} + \mu_{DU}}$

Avec :

$$a = \frac{\mu_D \mu_U}{(\lambda_{DD} + \mu_{DD})(\lambda_{DU} + \mu_{DU})} \qquad b = \frac{\lambda_D \mu_U}{(\lambda_{DD} + \mu_{DD})(\lambda_{DU} + \mu_{DU})}$$

$$c = \frac{\lambda_D \mu_D}{(\lambda_{DD} + \mu_{DD})(\lambda_{DU} + \mu_{DU})} \qquad d = \frac{\lambda_D \lambda_U}{(\lambda_{DD} + \mu_{DD})(\lambda_{DU} + \mu_{DU})}$$

Avec l'utilisation de la transformation inverse de LAPLACE on trouve la disponibilité de système :

$$A(t) = \frac{1}{(\lambda_D + \mu_D)(\lambda_U + \mu_U)} \begin{bmatrix} \mu_D \mu_U + \lambda_D \mu_U \exp-(\lambda_D + \mu_D)t + \lambda_U \mu_D \exp-(\lambda_U + \mu_U)t \\ + \lambda_D \lambda_U \exp-(\lambda_D + \lambda_U + \mu_D + \mu_U)t \end{bmatrix} \quad (3.5)$$

3.2.3. Détermination de la durée moyenne globale d'indisponibilité t_{CE} d'un canal :

La fréquence moyenne d'occupation d'un état est donnée par FF [ZHA et al 03] :

$$FF = \sum_{K \in W} P_K . \sum_{J \in F} a_{JK} \quad (3.6)$$

Où

F : est la transition entre les états de défaillance.

W : est la transition entre les états opérationnels.

P_K : est la probabilité de système d'occupation l'état K.

a_{JK} : Élément de la matrice M.

$$FF = P_0.(\lambda_{DD} + \lambda_{DU}) \quad / \quad P_0 = A(\infty) = \frac{\mu_{DD}\mu_{DU}}{(\lambda_{DD} + \mu_{DD})(\lambda_{DU} + \mu_{DU})}$$

$$FF = (\lambda_{DD} + \lambda_{DU}) \frac{\mu_{DD}\mu_{DU}}{(\lambda_{DD} + \mu_{DD})(\lambda_{DU} + \mu_{DU})}$$

Et nous avons :

$$1 - A(\infty) = \frac{\lambda_{DD}\lambda_{DU} + \lambda_{DD}\mu_{DU} + \lambda_{DU}\mu_{DD}}{(\lambda_{DD} + \lambda_{DU})(\mu_{DD} + \mu_{DU})}$$

$$MDT = \frac{1 - A(\infty)}{FF} = \frac{\lambda_{DD}\lambda_{DU} + \lambda_{DD}\mu_{DU} + \lambda_{DU}\mu_{DD}}{(\lambda_{DD} + \lambda_{DU})\mu_{DD}\mu_{DU}}$$

$$MDT = \frac{1 - A(\infty)}{FF} = \frac{1}{(\lambda_{DD} + \lambda_{DU})} \times \frac{\lambda_{DD}\lambda_{DU} + \lambda_{DD}\mu_{DU} + \lambda_{DU}\mu_{DD}}{\mu_{DD}\mu_{DU}}$$

Et lorsque $\begin{cases} \lambda = \lambda_{DD} + \lambda_{DU} \\ \frac{1}{\mu_{DD}} = MTTR \\ \frac{1}{\mu_{DU}} = \frac{T_1}{2} + MTTR \\ \lambda_{DD}\lambda_{DU} \approx 0 \end{cases}$:

Alors $MDT = \frac{\lambda_{DU}}{\lambda_D}\left(T_1/2 + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

Et sachant que

$$MDT = t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(T_1/2 + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \qquad (3.7)$$

3.2.4. Détermination de l'indisponibilité moyenne PFD_{avg} du canal :

Assimiler la *PFD* à l'indisponibilité asymptotique

$$PFD_{avg} = MDT.FF = t_{CE}.FF$$

$$FF = (\lambda_{DD} + \lambda_{DU})\frac{\mu_{DD}\mu_{DU}}{(\lambda_{DD} + \mu_{DD})(\lambda_{DU} + \mu_{DU})} \qquad \text{Sachant que} \quad \begin{cases} \lambda_{DD} \prec\prec \mu_{DD} \\ \lambda_{DU} \prec\prec \mu_{DU} \end{cases}$$

$$FF \approx (\lambda_{DD} + \lambda_{DU}) = \lambda_D$$

Donc pour l'architecture 1001 :

$$PFD_{1001avg} = \lambda_D.t_{CE} = \lambda_D\left[\frac{\lambda_{DU}}{\lambda_D}(T_1/2 + MTTR) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right] \qquad (3.8)$$

Les expressions (3.8) est bien celle données par la norme CEI 61508-6.

Architecture 1001	
t_{CE}	$\frac{\lambda_{DU}}{\lambda_D}\left(T_1/2 + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
PFD_{avg}	$\lambda_D.t_{CE} = \lambda_D\left[\frac{\lambda_{DU}}{\lambda_D}(T_1/2 + MTTR) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$

Tableau 3.2 : PFD_{avg} de l'architecture 1001

3.3. 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 [IEC61508].

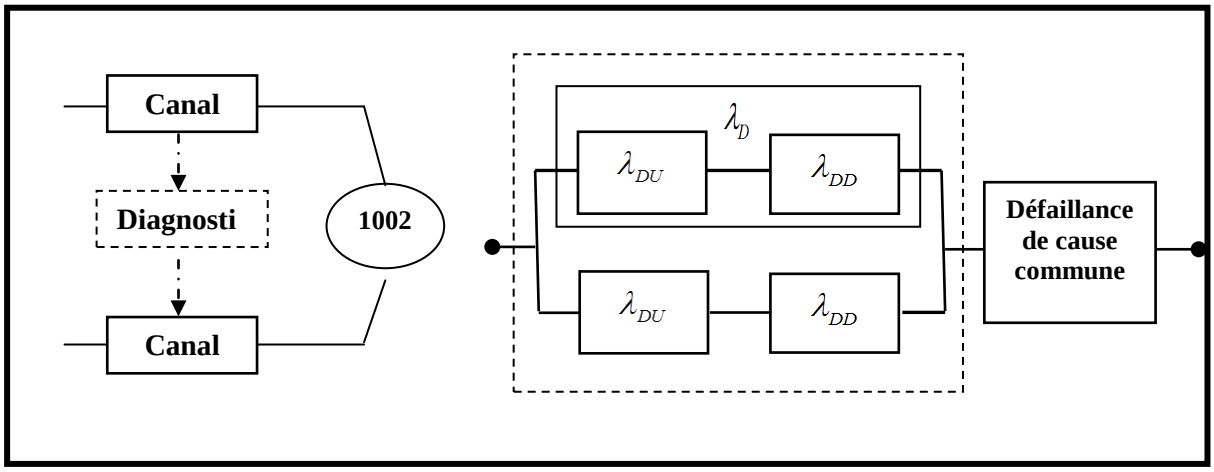


Figure 3.6. Diagrammes blocs physique et de fiabilité 1oo2

Nous suivons la même démarche que précédemment en modélisant le comportement de l'architecture 1002 par un modèle markovien multi-phases que nous approximons ensuite par un modèle markovien continu.

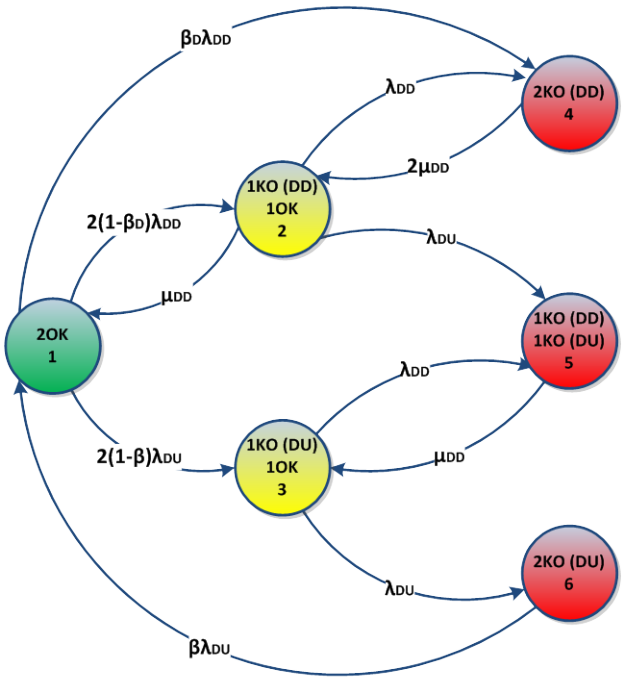


Figure 3.7. Modèle markovien multi-phases de l'architecture 1oo2

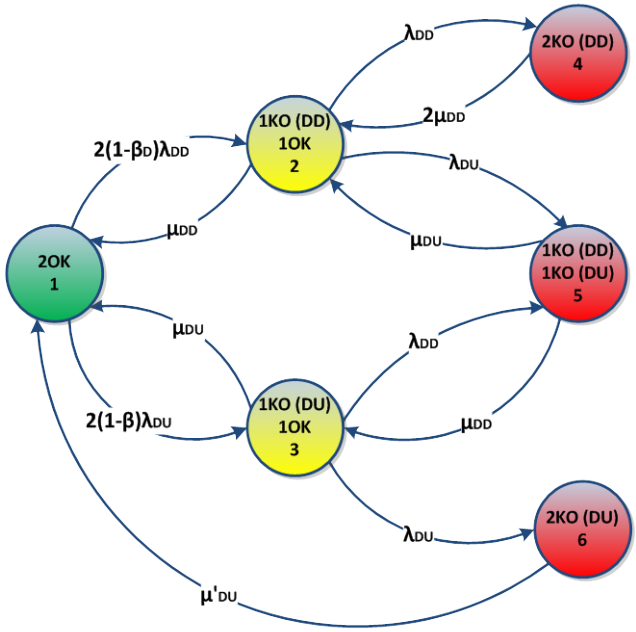


Figure 3.8. Modèle markovien continu de l'architecture 1oo2 [INN 08]

Le taux de μ'_{DU} est différent du μ_{DU}, car elle correspond à la réparation des deux canaux ayant subi successivement une défaillance non détectée [INN 05].

3.3.1. Détermination du taux de réparation μ'_{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 de barycentrique pour déterminer t'_{DU} :

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

$$f(t) = 2\lambda_{DU}\left[1-\exp(-\lambda_{DU}t)\right].\exp(-\lambda_{DU}t)$$

Par un calcule identique au précédent on déduit :

$$t'_{DU} = \frac{\int_0^{T_1} 2\lambda_{DU}.t\left[1-\exp(-\lambda_{DU}t)\right].\exp(-\lambda_{DU}t)dt}{\int_0^{T_1} 2\lambda_{DU}\left[1-\exp(-\lambda_{DU}t)\right].\exp(-\lambda_{DU}t)dt}$$

$$t'_{DU} = \frac{1}{2\lambda_{DU}}.\left[-4\lambda_{DU}T_1 e^{-\lambda_{DU}T_1} - 4\lambda_{DU}e^{-\lambda_{DU}T_1} + 2\lambda_{DU}T_1 e^{-2\lambda_{DU}T_1} + e^{-\lambda_{DU}T_1} + 3\right] / 1 - e^{-\lambda_{DU}T_1}\,]^2$$

On approximant les termes exponentiels par leur développement limité à l'ordre 3 :

$$t'_{DU} = \frac{4\lambda_{DU}{}^3.T_1{}^3}{6\lambda_{DU}{}^3.T_1{}^2} = \frac{2}{3}T_1$$

Soit : puisque $t_{c1} = T_1 - t'_{DU} + MTTR = \frac{T_1}{3} + MTTR$

On trouve $\mu'_{DU} = \frac{1}{t_{c1}} = \frac{1}{\frac{T_1}{3} + MTTR}$ (3.9)

3.3.2. Modèle markovien du 1oo2 :

Nous procédons d'une manière différente de la précédente(1001), nous allons nous baser sur un modèle markovien approché, plus compact que celui que nous aurions déduit du modèle markovien multi-phases de la figure 3.7.

Nous considérons, dans un premier temps, le comportement individuel des deux canaux, et en déduisons leur contribution à la PFD globale de l'architecture 1oo2 [INN 08].

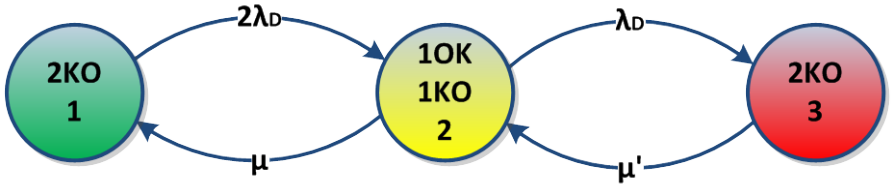


Figure 3.9. Graphe de Markov approché de l'architecture 1oo2

3.3.3. Détermination de la disponibilité de l'architecture 1oo2 :

Les équations différentielles du système :

$$\begin{cases} P_1'(t) = -2\lambda P_1(t) + \mu P_2(t) \\ P_2'(t) = 2\lambda P_1(t) - (\lambda + \mu)P_2(t) + \mu' P_3(t) \\ P_3'(t) = \lambda P_2(t) - \mu' P_3(t) \end{cases} \quad (3.10)$$

Le système (3.10) permet d'écrire :

$$\left[P_1'(t) \quad P_2'(t) \quad \mu P_3'(t)\right] = \left[P_1(t) \quad \lambda P_2(t) \quad P_3(t)\right].\begin{bmatrix} -2\lambda & 2\lambda & 0 \\ & - & + \\ 0\mu & \mu & - \end{bmatrix}$$

On utilise la transformation de LAPLACE on trouve :

Architecture 1002	
t_{CE}	$\frac{\lambda_{DU}}{\lambda_D}\left(T_1/2 + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
t_{GE}	$\left[\frac{\lambda_{DU}}{\lambda_D}(T_1/3 + MTTR) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$
PFD_{avg}	$2\left[\left(1-\beta_D\right)\lambda_{DD} + \left(1-\beta\right)\lambda_{DU}\right]^2 .t_{CE}.t_{GE} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}(\frac{T_1}{2} + MTTR)$

Tableau 3.3 : **PFDavg de l'architecture 1002**

3.4. 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 98].

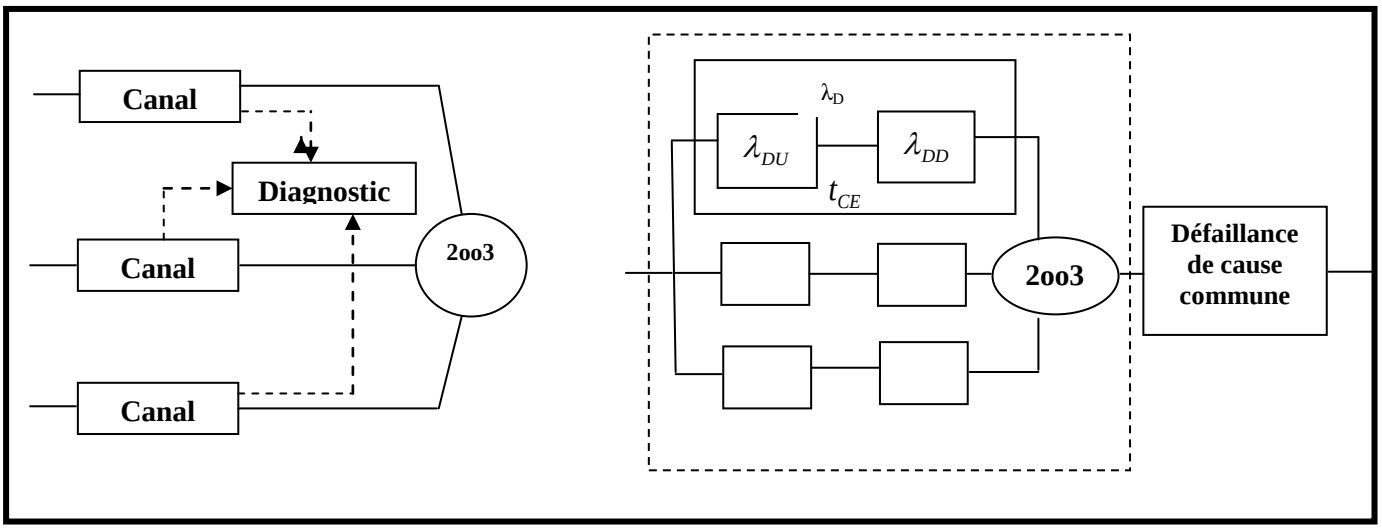


Figure 3.10. Diagrammes blocs physique et de fiabilité 2oo3

Nous suivons la même démarche que précédemment en modélisant le comportement de l'architecture 2003 par un modèle markovien multi-phases que nous approximons ensuite par un modèle markovien continu.

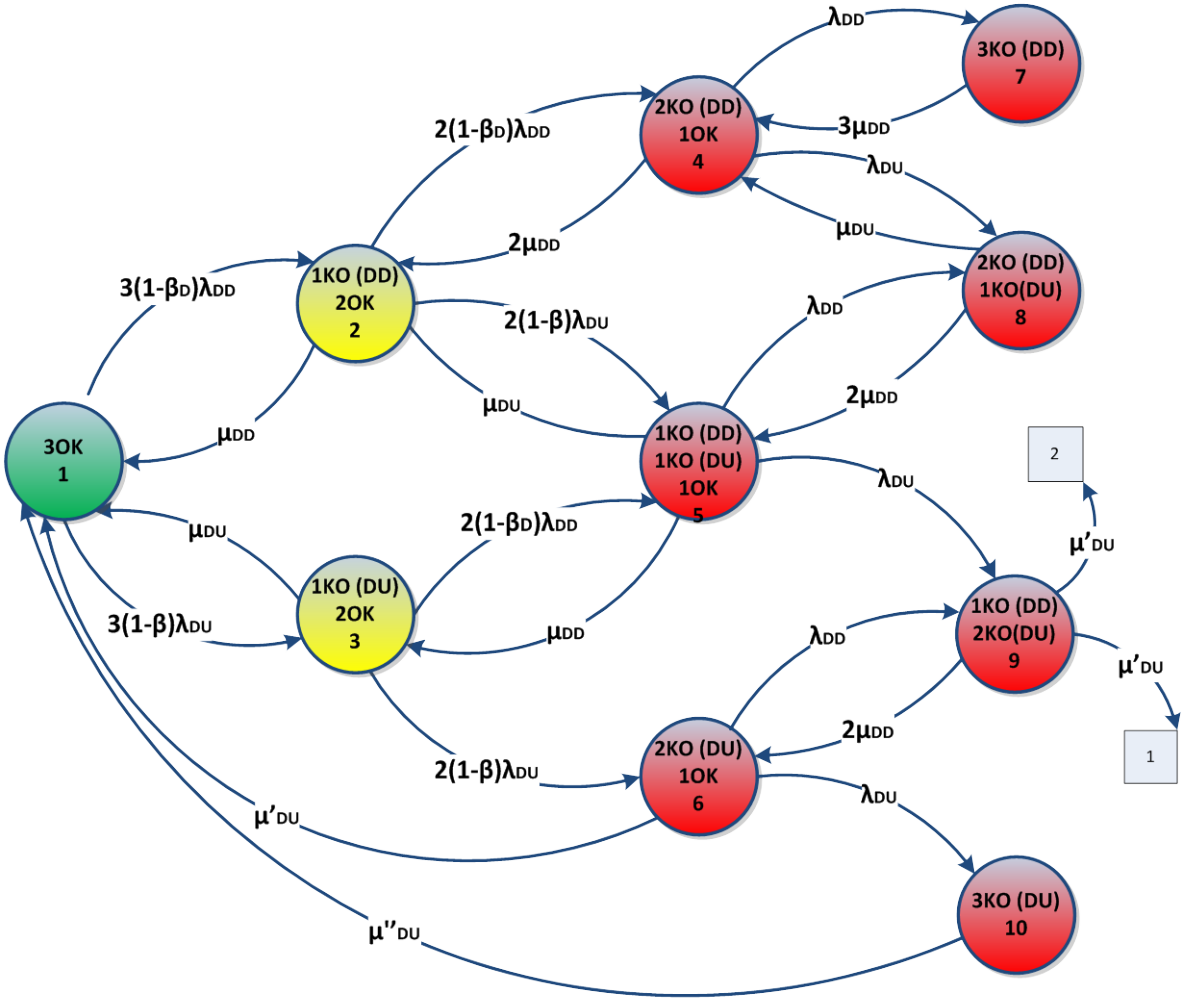


Figure 3.11. Modèle markovien Continu de l'architecture 2003

Le modèle markovien compact « approché », dont on va déduire *PFD* est représenté à la figure 3.12.

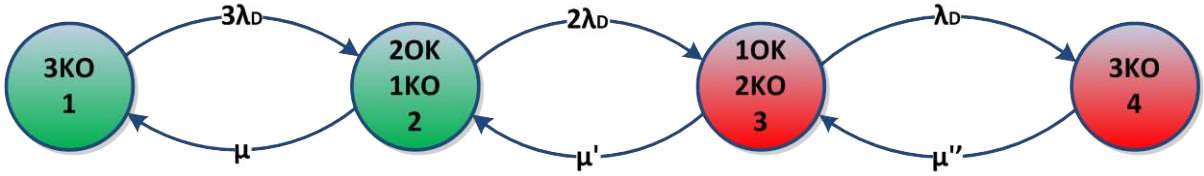


Figure 3.12. Modèle markovien approché de l'architecture 2003 [INN 08]

3.4.1. Détermination de la disponibilité de l'architecture 2oo3 :

Les équations différentielles du système :

$$\begin{cases} P_1'(t) = -3\lambda P_1(t) + \mu P_2(t) \\ P_2'(t) = 3\lambda P_1(t) - (2\lambda + \mu) P_2(t) + \mu' P_3(t) \\ P_3'(t) = 2\lambda P_2(t) - (\lambda + \mu') P_3(t) + \mu'' P_4(t) \\ P_4'(t) = \lambda P_3(t) - \mu'' P_4(t) \end{cases} \quad (3.16)$$

Avec une méthode analogue à celle employée avec l'architecture 1001 et 1002 on obtient alors :

Architecture 2003	
t_{CE}	$\frac{\lambda_{DU}}{\lambda_D}\left(T_1/2 + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
t_{GE}	$\left[\frac{\lambda_{DU}}{\lambda_D}(T_1/3 + MTTR) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$
PFD_{avg}	$6\left[\left(1-\beta_D\right)\lambda_{DD} + \left(1-\beta\right)\lambda_{DU}\right]^2 . t_{CE} . t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} (\frac{T_1}{2} + MTTR)$

Tableau 3.4 : PFD_{avg} de l'architecture 2003

Au terme de cette première partie du chapitre 3 dédié au calcul des probabilités moyennes de défaillance sur demande en utilisons le model markovien, nous pouvons formuler la conclusion suivante :

Les formules analytique, proposées à l'annexe B de la norme CEI 61508-6, pour calculer les PFD_{moy} des différents architectures KooN, sont des formules approchées que l'on peut retrouver, au prix de plusieurs hypothèses restrictives.

3.5. Evaluation des SIL d'un système opérationnel : Four Rebouilleur :

Le module « MPP0 » et le plus ancien des installations pétrolières à Hassi R'Mel. Il est entré en production en 1961.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 différentes installations (ballons de séparation, colonnes de distillation, échangeurs, fours…). Ces dernières sont destinées pour assurer le bon fonctionnement du 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.

Dans ce chapitre notre étude s'intéresse au système four H401 qui est composé des éléments suivantes : four H401, circuit d'alimentation gaz et liquide et le système de contrôle.

3.5.1. 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 [ENS 05]

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, C2)

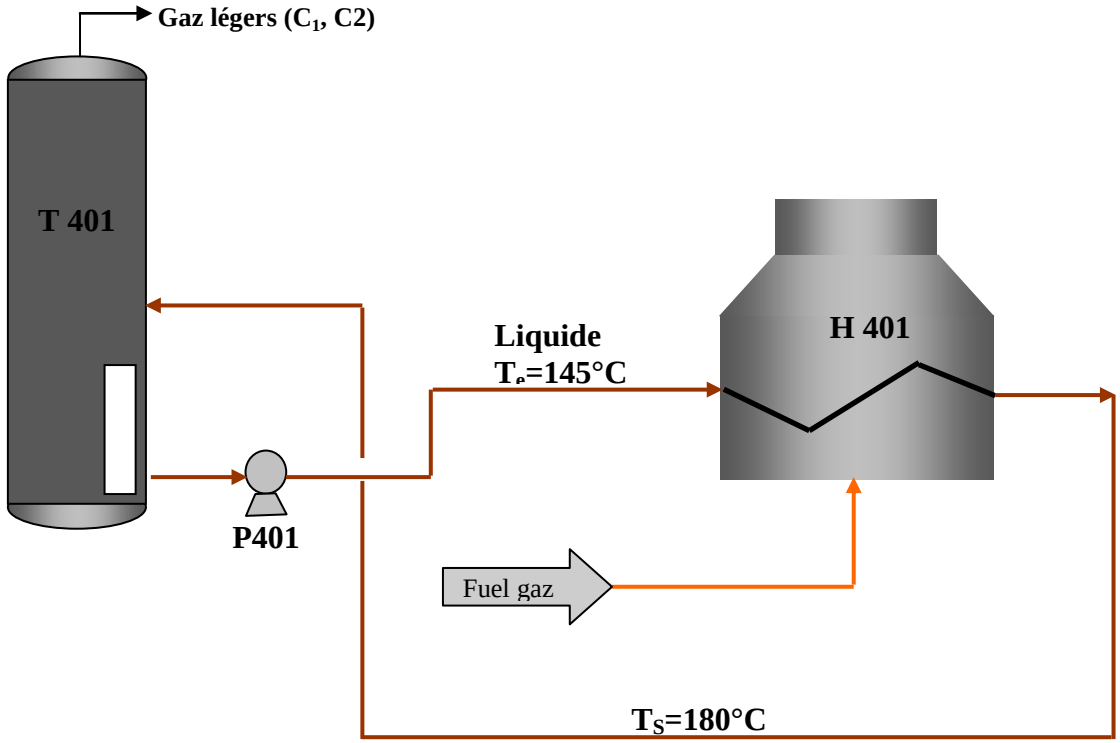


Figure 3.13. Echauffement de liquide par le four H401

3.5.2. Zones de four :

Le four H401 est de type cylindrique vertical composé de deux zones :

3.5.2.1. Zone de radiation (rayonnement) : constituant la chambre de combustion ou foyer dans laquelle des tubes sont exposés à la flamme et reçoivent la chaleur principalement par radiation de produit de combustion (fuel gaz).

3.5.2.2. Zone de convection : installée à la sortie des fumées de la chambre de combustion. Elle est constituée des faisceaux de tubes placés perpendiculairement à la direction des fumées l'échange s'effectue principalement par convection.

3.5.3. Construction de four H401 :

3.5.3.1. Faisceaux tubulaires (Serpentin) :

Le four H401 possède 08 faisceaux tubulaires, les faisceaux tubulaires sont généralement constitués de tubes droits, reliés entre eux par des coudes **à 180 °** soudés sur les tubes.

Le choix du matériau pour les faisceaux des tubes repose sur les critères suivants :

- Résistance à la corrosion par le fluide chauffé.
- Résistance à l'oxydation par les fumées chaudes.
- Résistance mécanique en température.

3.5.3.2. Brûleurs :

Les brûleurs ont pour fonction de réaliser la combustion et donc d'assurer :

- Le mélange du combustible et du comburant
- L'inflammation du mélange.

3.5.3.3. Les pilotes :

Le but des pilotes est de garantir une flamme continue pour l'amorçage du gaz venant des brûleurs.

3.5.3.4. Cheminée : Une cheminée d'évacuation des fumées.

3.5.3.5. Registre :

Le registre introduit sur le circuit des fumées une perte de charge plus ou moins grande selon son ouverture et modifie, c'est l'organe de réglage du tirage

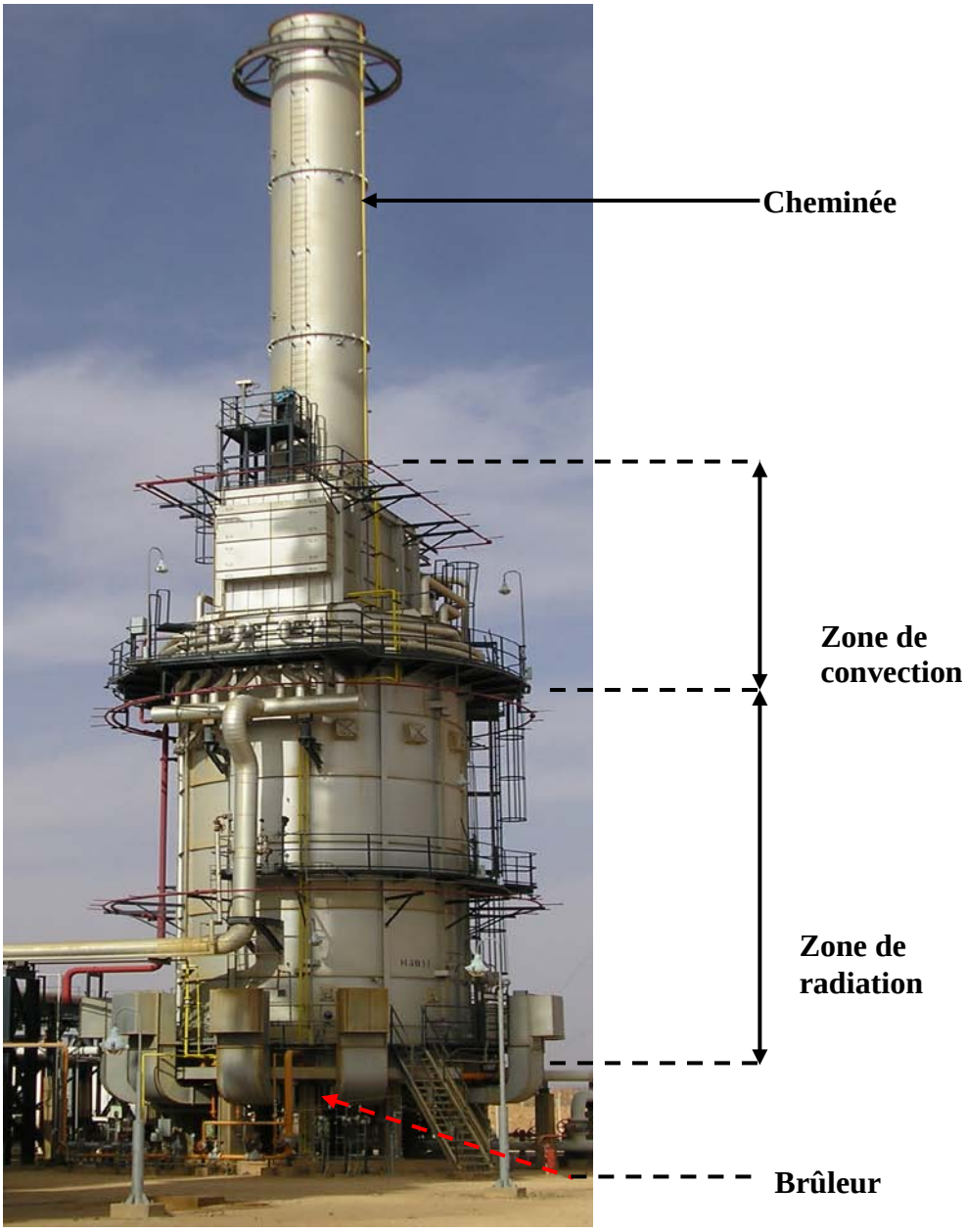


Figure 3.14. Le Four Rebouilleur H401

3.5.4. La décomposition structurelle et fonctionnelle du système four H401 :

3.5.4.1. 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]

Tableau 3.5. Sous-système d'alimentation

3.5.4.2. Sous système de contrôle :

Le contrôle dans le four porte sur les fonctions suivantes :

- 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/h.

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]

Tableau 3.6. Sous-système de contrôle

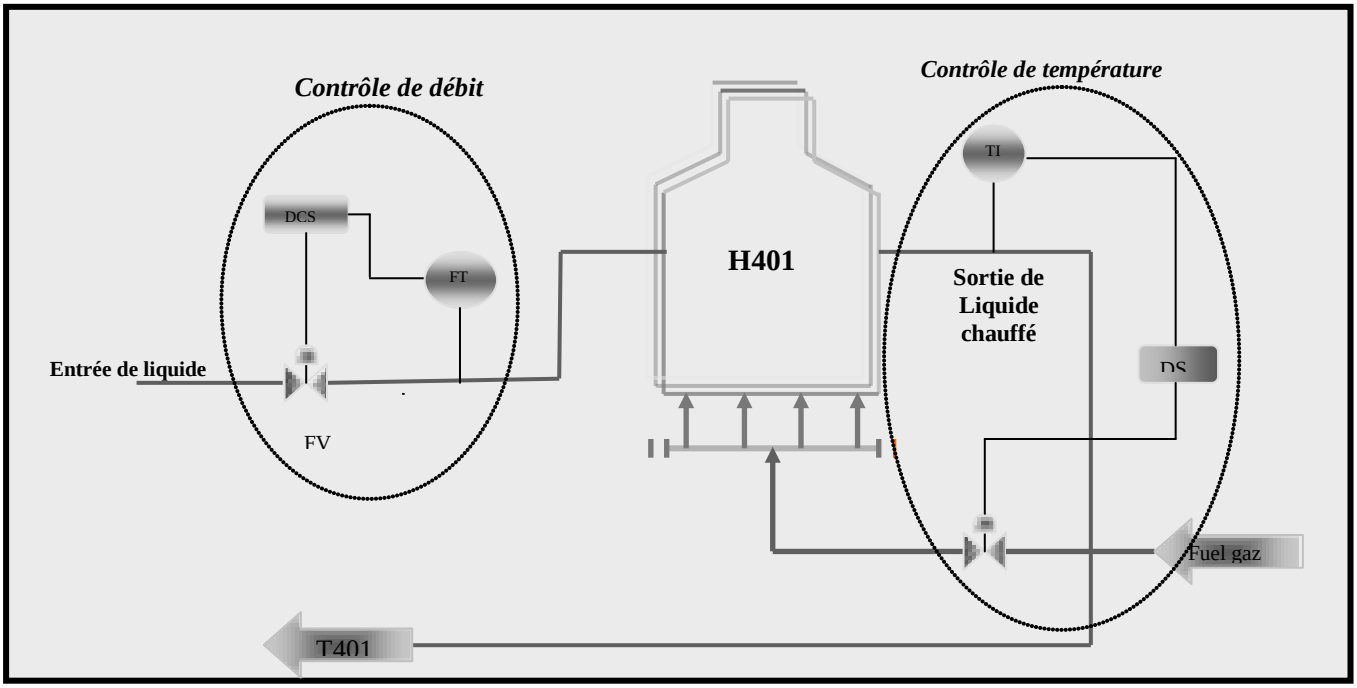


Figure 3.15. Système de contrôle dans le four H401

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

3.5.4.3. 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 peut être utilisé pour alerter les opérateurs pour qu'ils interviennent afin de rendre le système à l'état stable.

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-visuel]

Tableau 3.7. Sous-système d'alarme

3.5.4.4. 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.

3.5.4.4.1. Les 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

3.5.4.4.2. Unité de traitement PLC (TRICONEX) :

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

La technologie TMR (Triple Modular Redundant) 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 out of 3 assure un signal à la sortie s'il y a un signal sur deux voies sur les trois voies.

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 visuell

Figure 3.16. Automate programmable PLC

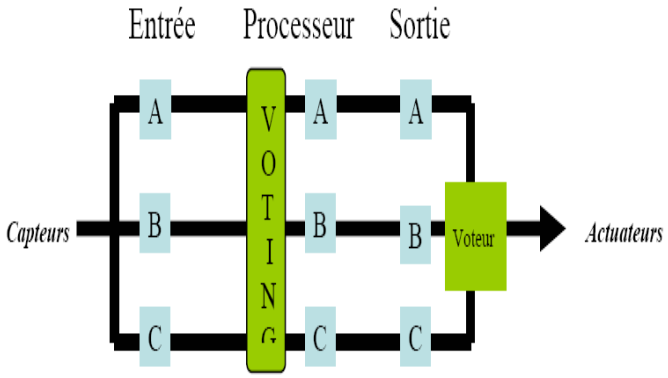


Figure 3.17. Architecture 2oo3 de PLC

3.5.4.4.3. Les actionneurs :

Sont des 02 électrovannes en parallèles (tout ou rien) commandés par le PLC.

En cas d'existence de facteur de déclenchement, on observe la fermeture des vannes (UV1, UV2) pour couper l'alimentation de fuel gaz.

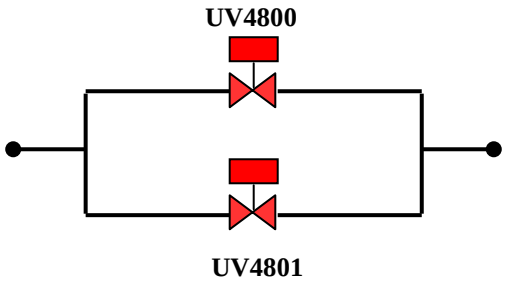


Figure 3.18. Architecture 1oo2 des vannes

3.5.5. Calcul de PFDavg du SIS :

3.5.5.1. Par les équations de modèle Markovien :

Pour calculer la PFDavg de notre SIS, nous avons utilisé les expressions obtenues par le modèle de Markov.

Les différentes données nécessaires au calcul ont été tirées des banques de données [ORE 02], [CCPS 02], [IEEE 84], et [PDS 04].

Par manque de données, nous n'avons pas pris en considération dans les différents calculs des probabilités de défaillance de cause commune ($ß_D$=ß=0).

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

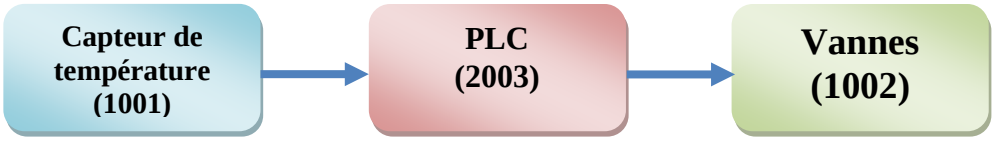


Figure 3.19. Schéma simple du SIS

Les graphes ci-dessus sont obtenus à l'aide du logiciel MATLAB.

Ils consistent à décrire la variation du PFDavg de chaque composant en fonction du temps de proof-test pour un DC fixe.

Sachant que : T1=4380h,

Et pour : le Capteur (1001) : λ_D =1,5.E-6, MTTR=9,8h

Et pour : le PLC (2003) on : λ_D =1.E-10, MTTR=10,2h

Et pour : les vannes (1002) : λ_D =2 ,7.E-6, MTTR=12h

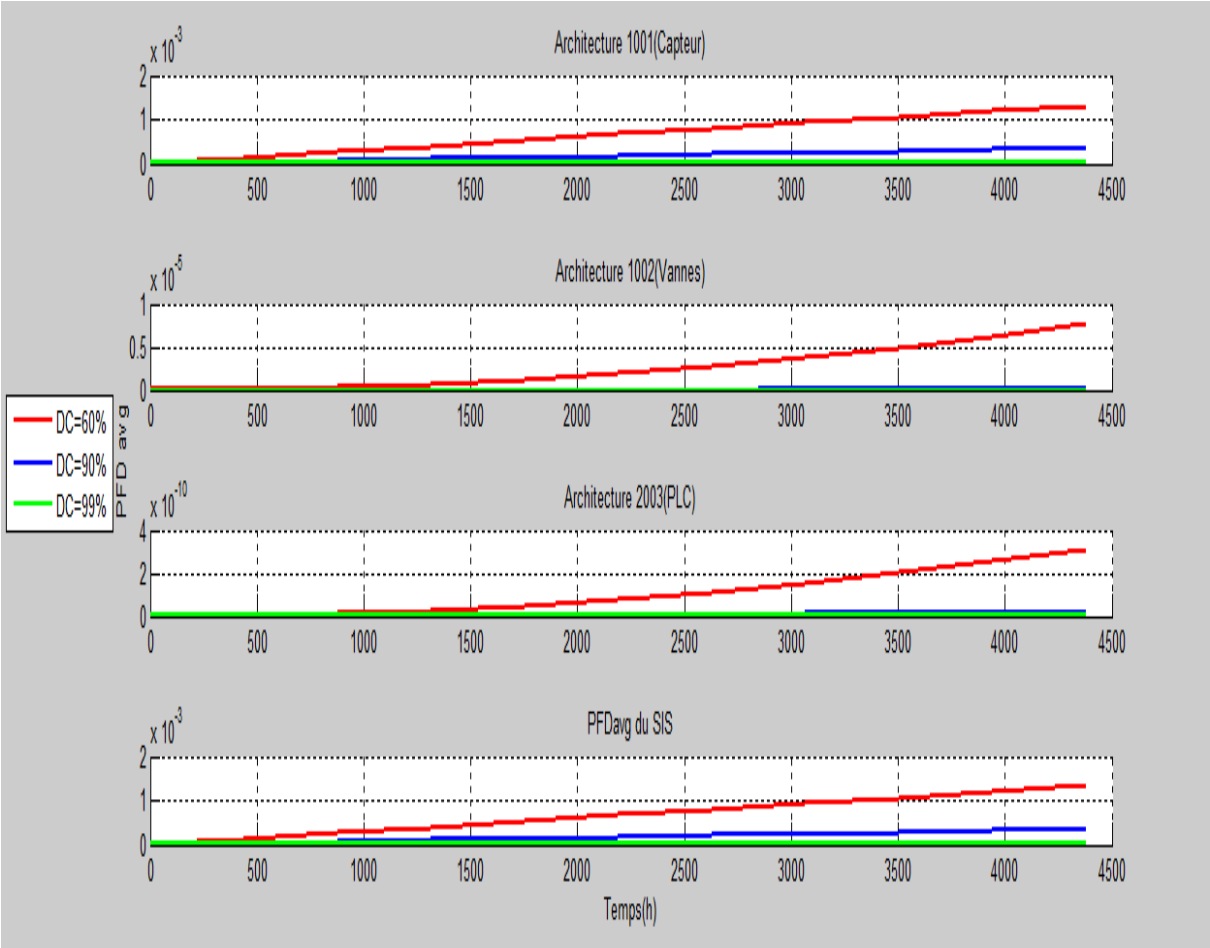


Figure 3.20. Calcul des PFDavg par les équations de modèle markovien T_1=4380h

Commentaires des résultats :

- La PFDavg croit avec le temps de proof test.
- L'augmentation du DC fait diminuer la PFD
- La PFDavg du SIS étudié est influencée par la PFD du capteur car le SIS est composé d'un seul capteur (1oo1)
- L'élément le plus critique dans le SIS est le capteur.

3.5.5.2. Calcul du PFDavg par les équations simplifiées :

La méthode des équations simplifiées est la méthode qui est utilisée par les industriels. Pour pouvoir la comparée avec celle utilisée par le modèle markovien, nous avons gardés des mêmes données nécessaires pour le calcul.

$$PFD_{avg}^{1001} = \lambda_{DU}\frac{T_1}{2} \quad , \qquad PFD_{avg}^{1002} = \frac{1}{3}(\lambda_{DU}.\frac{T_1}{2})^2 \quad , \qquad PFD_{avg}^{2003}avg = (\lambda_{DU}.\frac{T_1}{2})^2$$

	Sensor 1001		**Logic Solver** 2003		**F.Element** 1002		**SIS** System	
	PFD	SIL	PFD	SIL	PFD	SIL	PFD	SIL
DC= 60 %	0.001314	**2**	0.76E-10		1.867E-6		0.0013	**2**
DC= 90 %	3.285E-4	**3**	4.796E-12		1.165E-7		3.285E-4	**3**
DC= 99 %	3.285E-5	**4**	0.47E-13		1.165E-9		3.28E-5	**4**

Tableau 3.8 : Calcul du PFDavg par les équations simplifiées

Les de PFD obtenu par les équations de modèle markovien:

	Sensor 1001		**Logic Solver** 2003		**F.Element** 1002		**SIS** System	
	PFD	SIL	PFD	SIL	PFD	SIL	PFD	SIL
DC= 60 %	0.0013	**2**	1.059E-10		2.589E-6		0.0013	**2**
DC= 90 %	3.432E-4	**3**	7.319E-12		1.819E-7		3.433E-4	**3**
DC= 99 %	4.755E-5	**4**	1.845E-13		1.158E-9		4.755E-5	**4**

Tableau 3.9 : Calcul du PFDavg par les équations de modèle markovien

3.5.5.3. Comparaison des résultats :

Après avoir analysé les résultats obtenus par les deux méthodes, nous pouvons dire que le modèle Markovien est supérieur par rapport à la méthode des équations simplifiées à cause de la rigueur des équations.

3.6. 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.

La méthode des graphes de Markov et celle des équations simplifiées (normes IEC 61508) ont été utilisées pour évaluer la PFDavg du SIS du four rebouilleur. Mais au préalable, une revue détaillée des équations du modèle Markovien pour les architectures constituant ce SIS, est réalisée. Nous avons pu retenir deux principaux résultats :

1) On a constaté une certaine différence entre les résultats issus du modèle Markovien et ceux donnés les équations simplifiés.

2) Selon le concepteur, le SIS du four rebouilleur est certifié SIL2 ; ce qui correspond, selon les résultats obtenus par les deux méthodes utilisées, à une PFDavg de l'ordre de 10^{-3} pour un DC=60%. Or cet ordre est pratiquement donné par la valeur de la PFDavg du capteur qui constitue à cet égard un élément critique pour le SIS.

D'où la nécessité d'augmenter la disponibilité de cet élément. Pratiquement parlant, une architecture 1002 pour le sous-système « capteurs » permet le passage d'un SIL2 vers un SIL3 pour la fonction de sécurité du SIS.

Dans le dernier chapitre, on s'intéresse à simuler le fonctionnement du système (four avec arrêt d'urgence) en utilisant le simulink et une étude expérimentale avec le dSPACE 1103 DS.

4

Simulation et Etude Expérimentale:

Application sur un four rebouilleur

4.1. Introduction :

La complexité des architectures du SIS fait que le diagnostic de leurs défaillances par simulation sur ordinateur devient un outil indispensable. La simulation trouve une application directe dans l'amélioration des performances des SIS. Plus spécifiquement, la simulation en temps réel se révèlera importante pour confirmer que le SIS atteignent les spécifications du niveau d'intégrité exigé en présence de danger. Une simple simulation peut être exécutée sur un ordinateur connecté à un SIS.

Le présent chapitre est consacré à la simulation des défaillances du SIS relatif au four rebouilleur sous l'environnement MATLAB/SIMULINK. Puis une validation des résultats de simulation est effectue sur DSP 1l03 DS.

4.2. Présentation détaillée du système « Four rebouilleur » :

4.2.1. Décomposition du Système :

La figure (4.1) montre un schéma simplifié de la décomposition du système four H401. Le système d'ESD (Emergency Shut Down) consiste à assurer l'arrêt total du four H401 en cas de perturbation du système de contrôle de température (DCS) ou de détection de conditions potentiellement dangereuses, afin de protéger le personnel, les équipements et l'environnement.

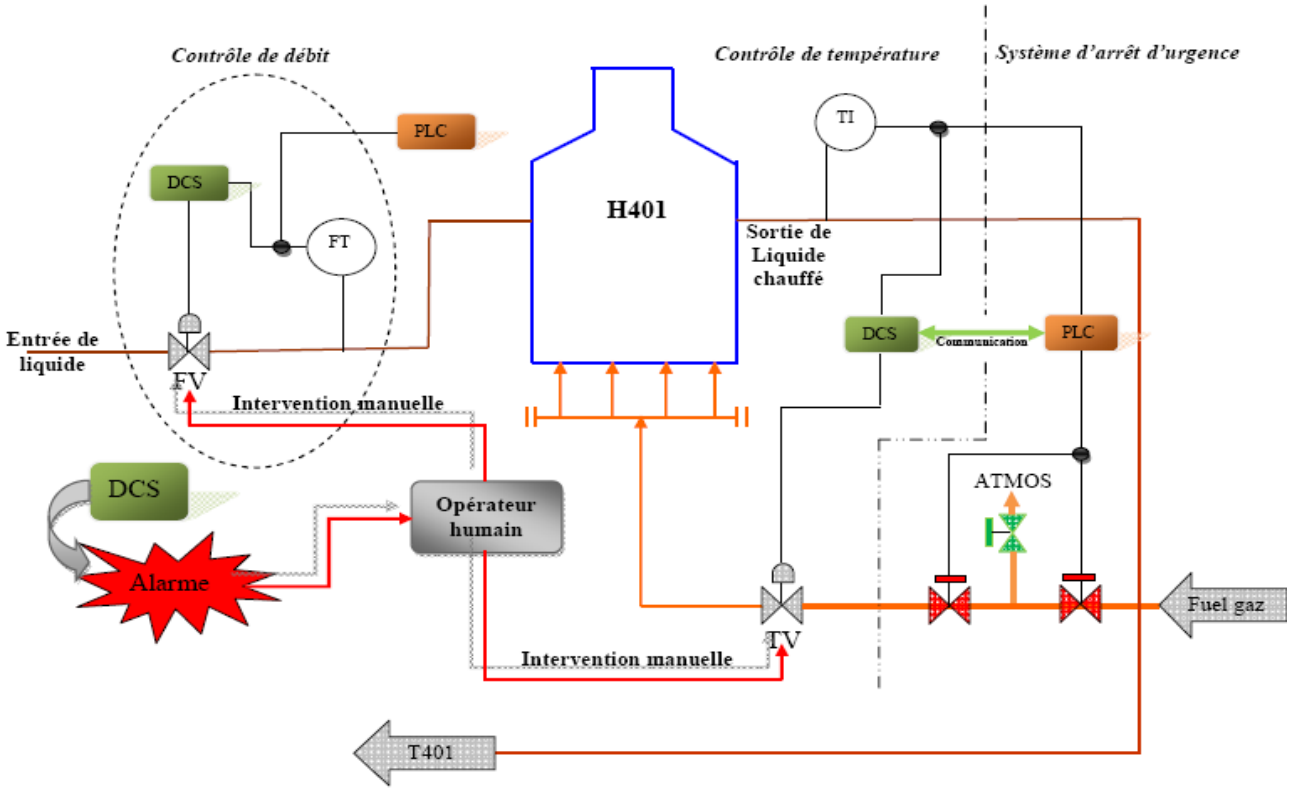


Figure 4.1. Schéma du système four rebouilleur

4.2.2. Sous système d'arrêt d'urgence (SIS) :

Les résultats de simulation que nous avons effectuée par SIMULINK concernent le SIS du four rebouilleur (Fig. 4.1). Un schéma simplifié de ce SIS est donné par la figure (4.2).

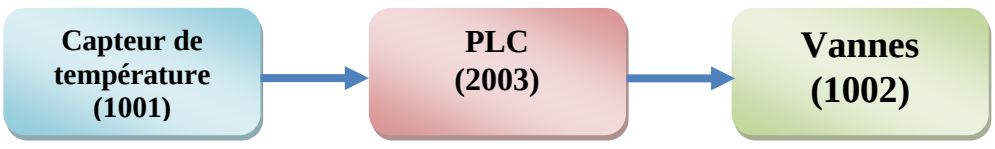


Figure 4.2. Schéma simplifié du SIS

4.3. Simulation et interprétation :

4.3.1. Système avec un seul capteur :

4.3.1.1. Mode de défaillance des composants du SIS :

Le tableau (4.1) montre les principaux modes de défaillances pouvant affecter les composants du SIS.

N°	Composants	Modes de défaillances
1	Capteurs	Indication erronée - Plus que la valeur réelle - Moins que la valeur réelle - Pas d'indication
2	PLC	- Inputs défectueux - Outputs défectueux
3	Vannes	- Bloqué ouverte - Fermeture intempestive

Tableau 4.1. Principaux modes de défaillance des composants

4.3.1.2. Modèle de simulation du système à un seul capteur :

La figure (4.3) montre le schéma de simulation par SIMULINK sous MATLAB du système à un seul capteur.

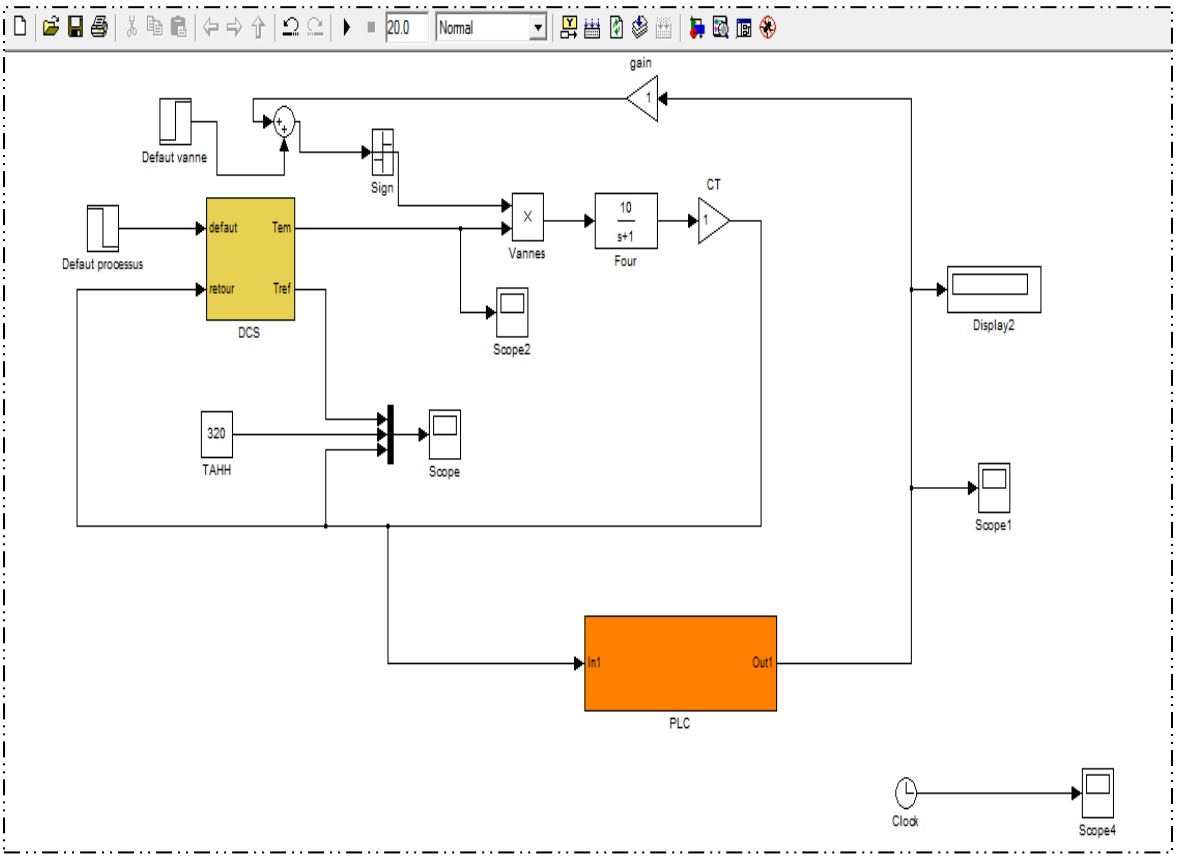


Figure 4.3. Modèle de simulation du système à un seul capteur

4.3.1.3 Résultats et Interprétation :

On a étudié l'influence des défauts du sous système de contrôle et du sous système d'arrêt d'urgence sur le fonctionnement normal du four rebouilleur :

4.3.1.3.1 Sous système de contrôle « DCS » :

La figure (4.4) illustre respectivement les allures de température dans le fonctionnement normal et en cas de défaut dans le sous système de contrôle DCS « régulateur de température ».

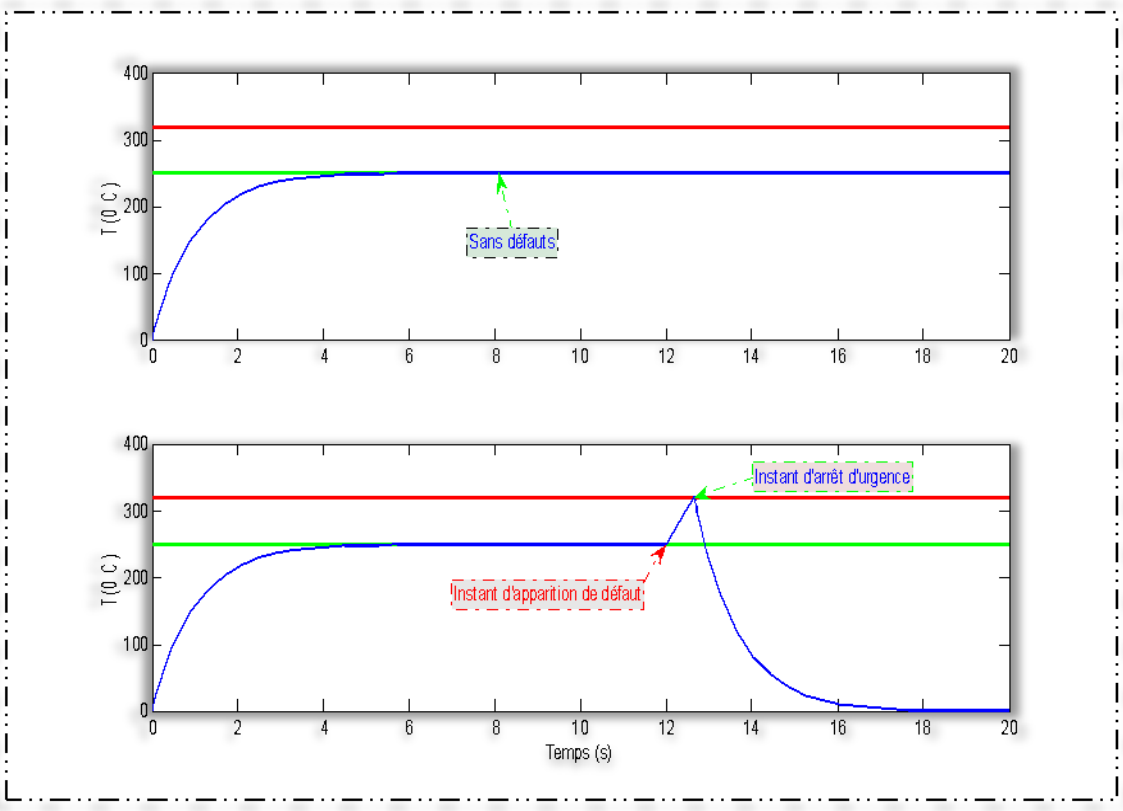


Figure 4.4. Variation de la température en fonction du temps dans le cas normal et défaillant

Interprétation des résultats :

Le régulateur agit en fonctionnement normal en assurant une température de référence. Dans le cas d'apparition de défaut au niveau du sous système de contrôle « DCS », nous constatons que la température augmente jusqu'à 320 ^{0}C, ce qui provoque la coupure de l'alimentation de fuel gaz par le sous système d'arrêt d'urgence pour ramener le système à un état de sécurité.

4.3.1.3.2. Cas de défaillance au niveau de l'unité de traitement (PLC TRICONEX) :

Cette section présente dans un premier temps les résultats de simulation en absence et en présence de défauts au niveau des modules d'I/O.

Les défauts pouvant affecter les modules d'I/O comme le montre la figure (4.5).

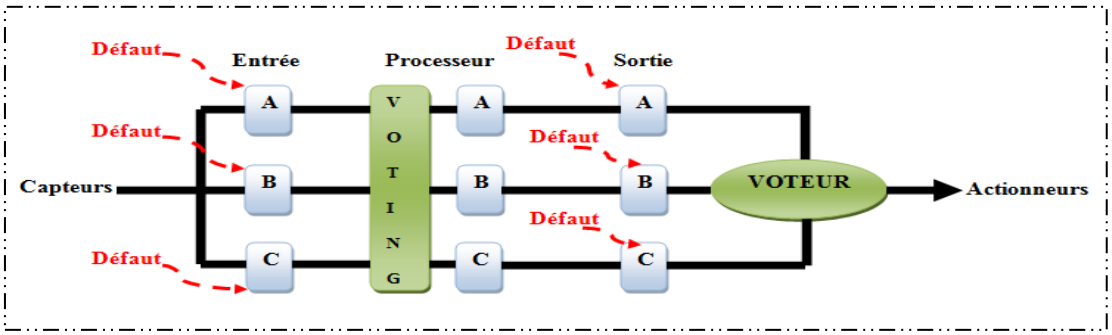


Figure 4.5. Défauts des modules d'I/O

Dans un second temps, nous présentons l'influence de ces défauts sur le fonctionnement du PLC afin de tester les performances de SIS en cas de détection d'une haute température au sein du four H401. La figure (4.6) représente le fonctionnement du système en absence de défauts. On note que les modules d'I/O des trois PLC sont à une logique 1, et le comparateur est à une logique 0, i.e. ne produira aucune alarme pour l'opérateur.

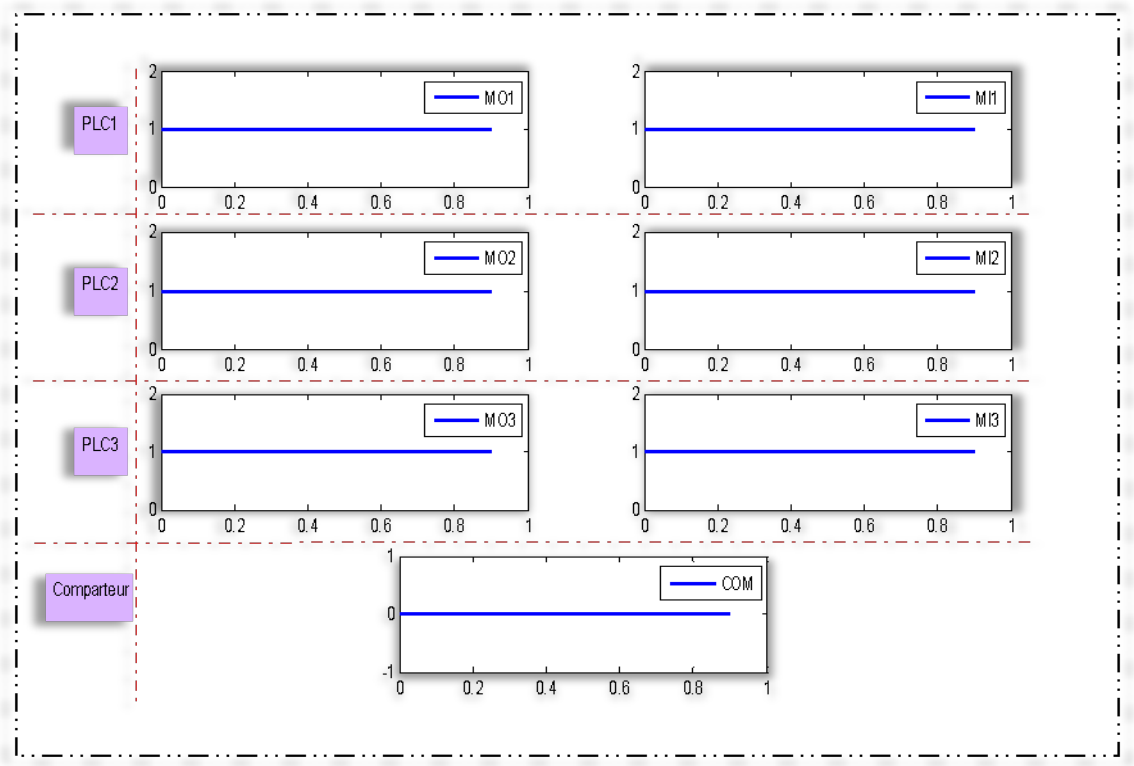


Figure 4.6. Fonctionnement sans défauts

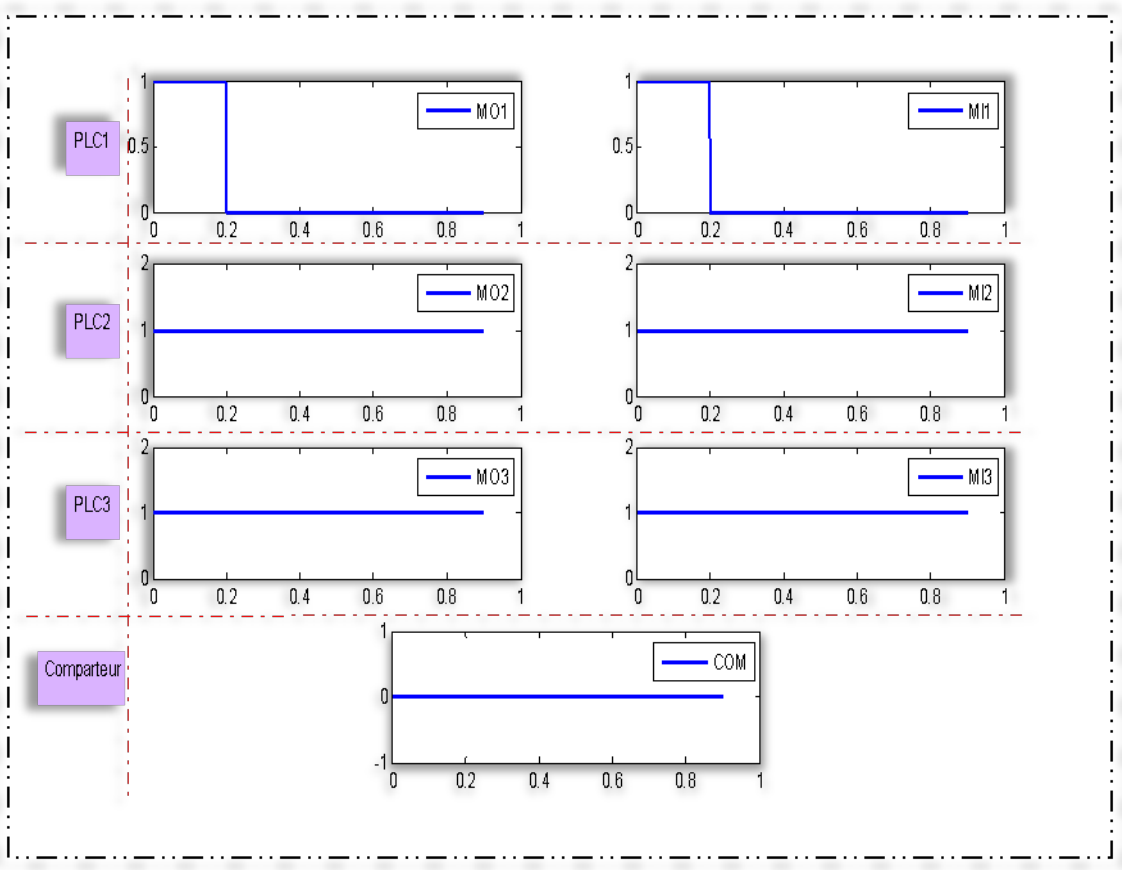


Figure 4.7. Défaillance de PLC1

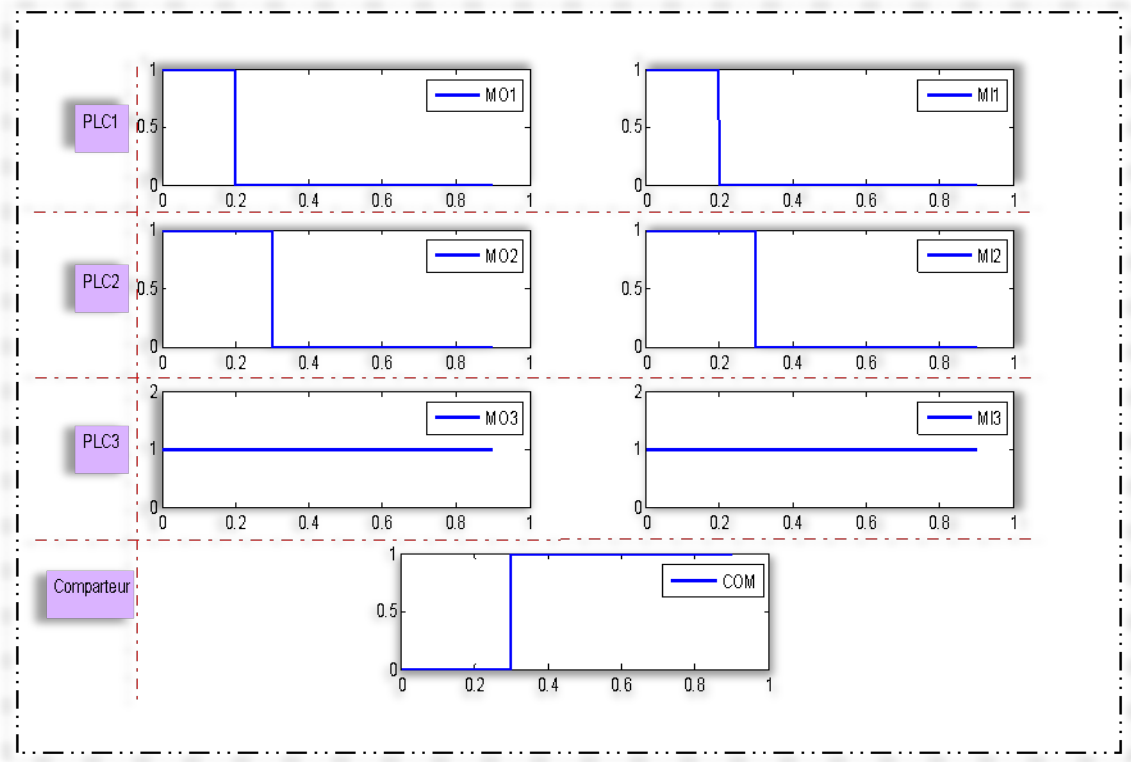


Figure 4.8. Défaillance de PLC1 et PLC2

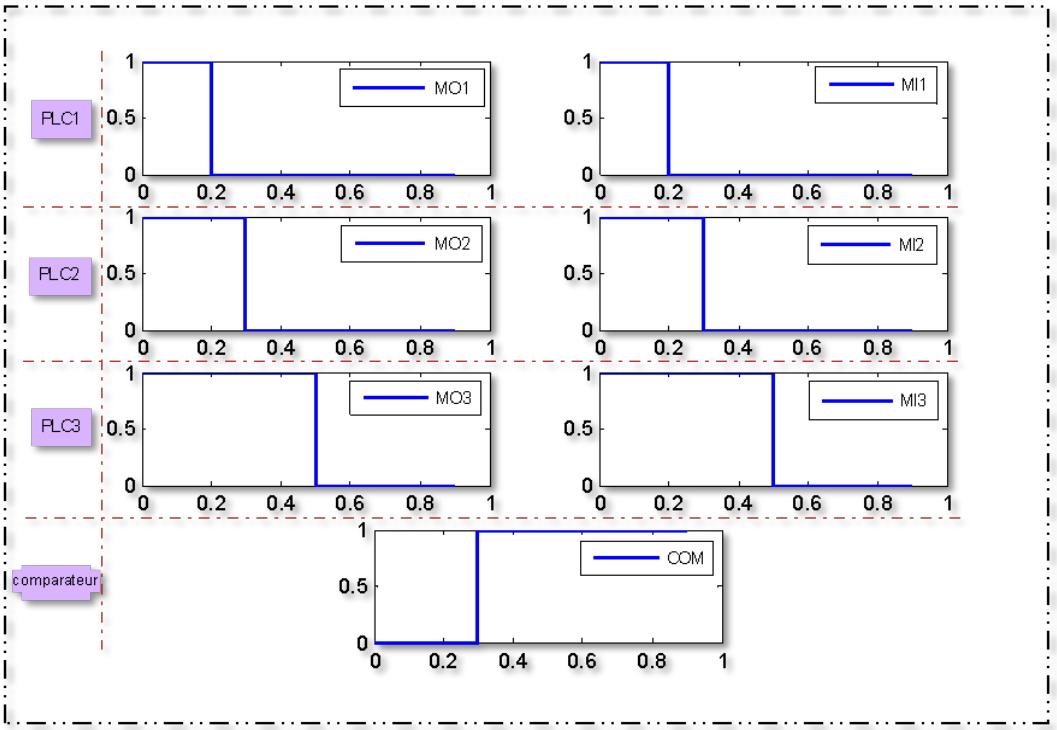


Figure 4.9. Défaillance de PLC1, PLC2 et PLC3

Les figures (4.7), (4.8) et (4.9) représentent le cas d'apparition des défauts au niveau des modules d'I/O. On peut constater que la présence de défaut au niveau d'un seul PLC ne génère aucune alarme puisque les défauts qui se manifestent au niveau d'un seul module sont tolérables. Par contre, l'apparition de défauts au niveau de deux ou trois PLC fait que la logique des modules d'I/O s'écartent notablement de zéro et le comparateur sera à une logique 1, ce qui produira un signal d'alarme.

La figure (4.10) illustre les allures de la température obtenues lors de simulation avec et sans défauts au niveau du PLC. La figure (4.10-A) représente le fonctionnement du SIS en absence de défauts. Nous pouvons constater que la valeur de température s'écarte notablement de 250°C à cause de la défaillance du sous-système de contrôle (DCS) ; le SIS intervient pour couper l'alimentation en fuel gaz et la température diminue graduellement à la valeur nulle dans le but de ramener le procédé à un état sûr. On peut constater aussi qu'en cas d'injection de défauts au niveau d'un seul PLC, l'arrêt d'urgence se produit et le système fonctionne en mode dégradé.

La figure (4.10-B) représente la variation de la température au niveau du four rebouilleur dans le cas d'injection de défauts au niveau de deux ou trois PLC. On peut observer une croissance brutale de la température au-delà 320 ^{0}C, ce qui représente un risque réel pour le personnel et l'environnement. Dans ce cas, d'autres moyens devant être envisagés pour ramener le système à un état de sécurité.

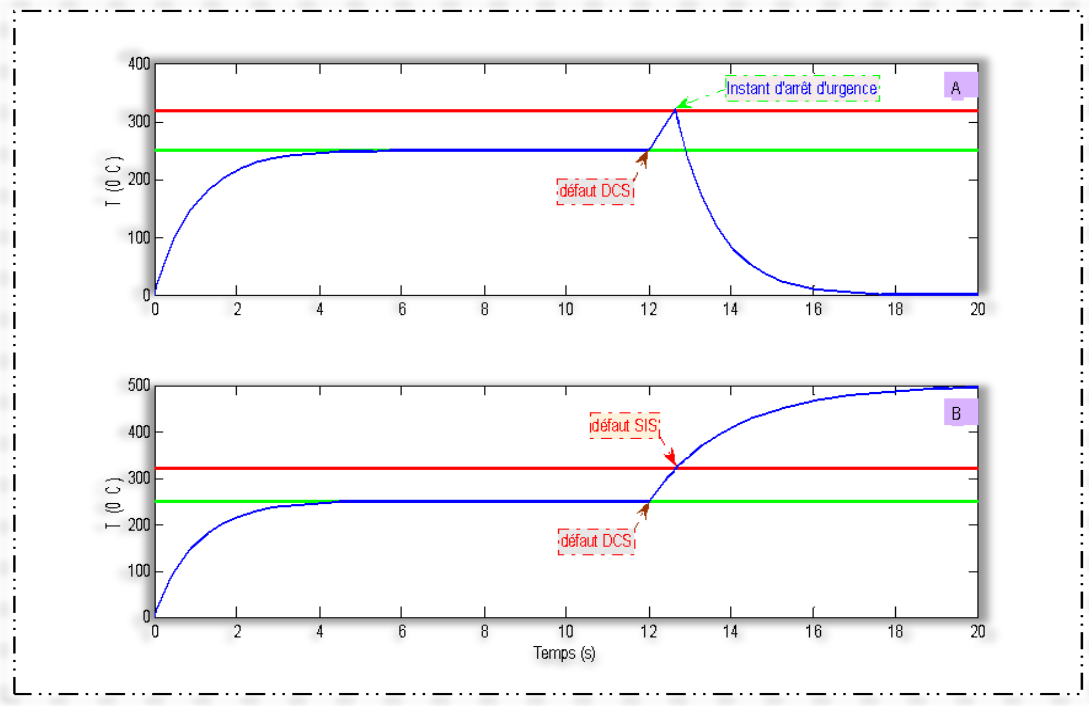


Figure 4.10. Variations de température sans et avec défaillance du PLC (SIS)

4.3.1.3.3. Cas de défaillance des électrovannes:

La figure (4.11), illustre respectivement les variations de la température obtenues par simulation sans et avec défauts au niveau des électrovannes et ce, pour l'effet de leurs défaillances sur le fonctionnement du SIS et sur le processus.

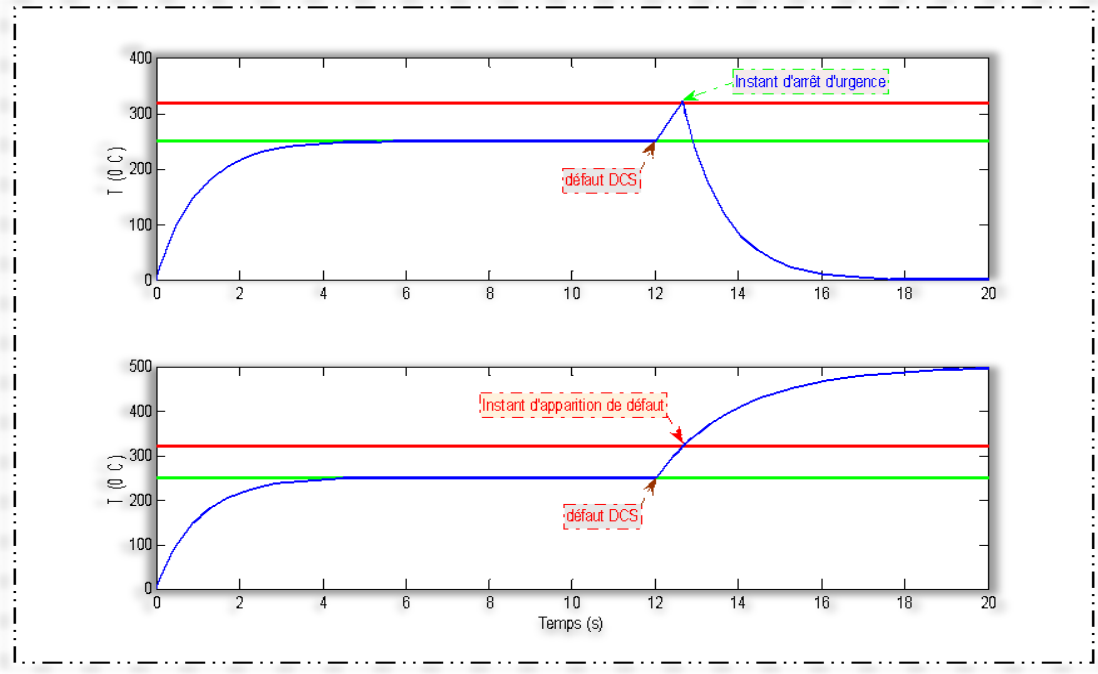


Figure 4.11. Variations de température sans et avec défaillance des électrovannes.

La figure (4.11-A) montre le bon fonctionnement du SIS, qui entraine une diminution progressive de la température jusqu'à zéro à cause de la fermeture des vannes (coupure d'alimentation en fuel gaz). Dans le cas d'apparition de défauts au niveau des deux vannes (bloquées ouvertes) (Fig. 4.11-B), on observe que l'arrêt d'urgence ne s'est pas produit et la température à l'intérieur du four continue à croitre, ce qui met le process dans à un état dangereux.

4.3.1.3.4. Cas de défaillance du Capteur :

La figure (4.12) montre les variations de la température obtenues par simulation sans et avec défauts au niveau du capteur afin de tester l'influence de sa défaillance sur le fonctionnement du SIS et donc, sur le process.

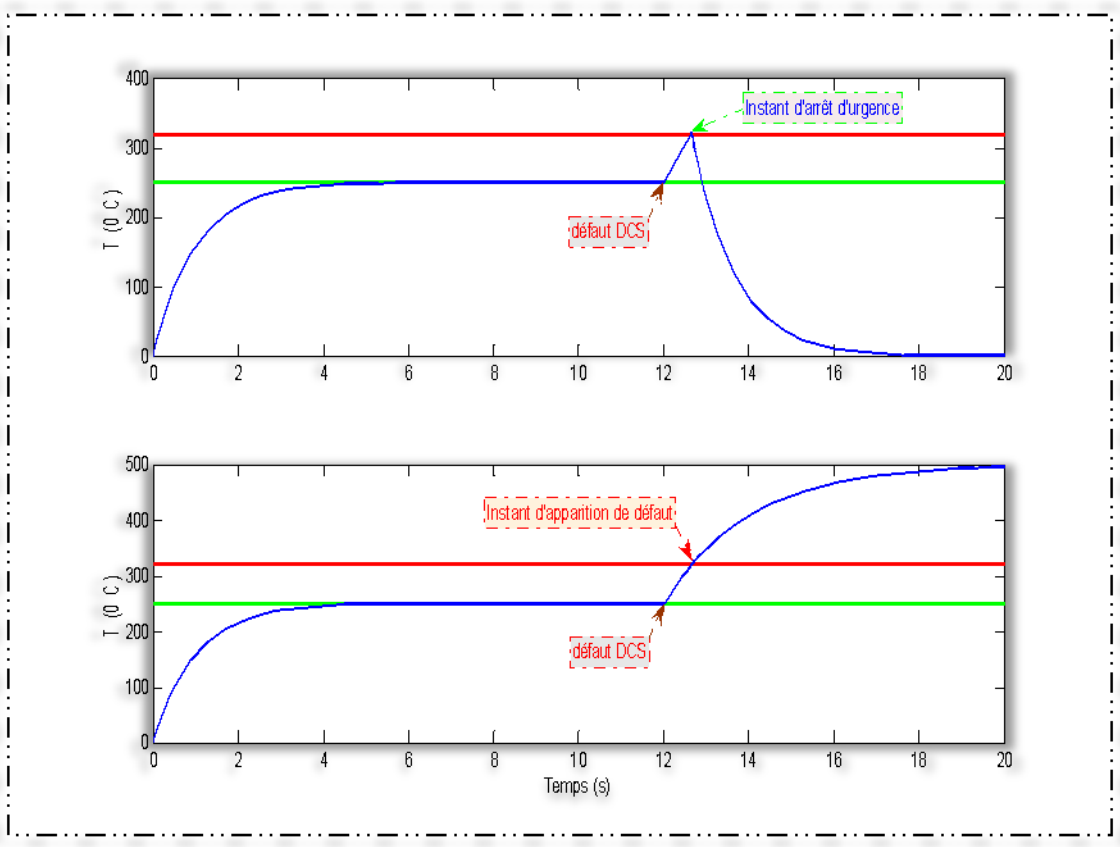


Figure 4.12. Variations de température sans et avec défaillance du capteur.

Comme dans le cas des électrovannes, la défaillance du capteur entraine l'indisponibilité du SIS, d'où l'augmentation de la température au-delà de 320°C à l'intérieur du four.

4.3.2. Simulation du Système avec deux capteurs :

4.3.2.1. Modèle de simulation par SIMULINK :

La figure (4.13) montre le schéma de simulation par SIMULINK du système à deux capteurs.

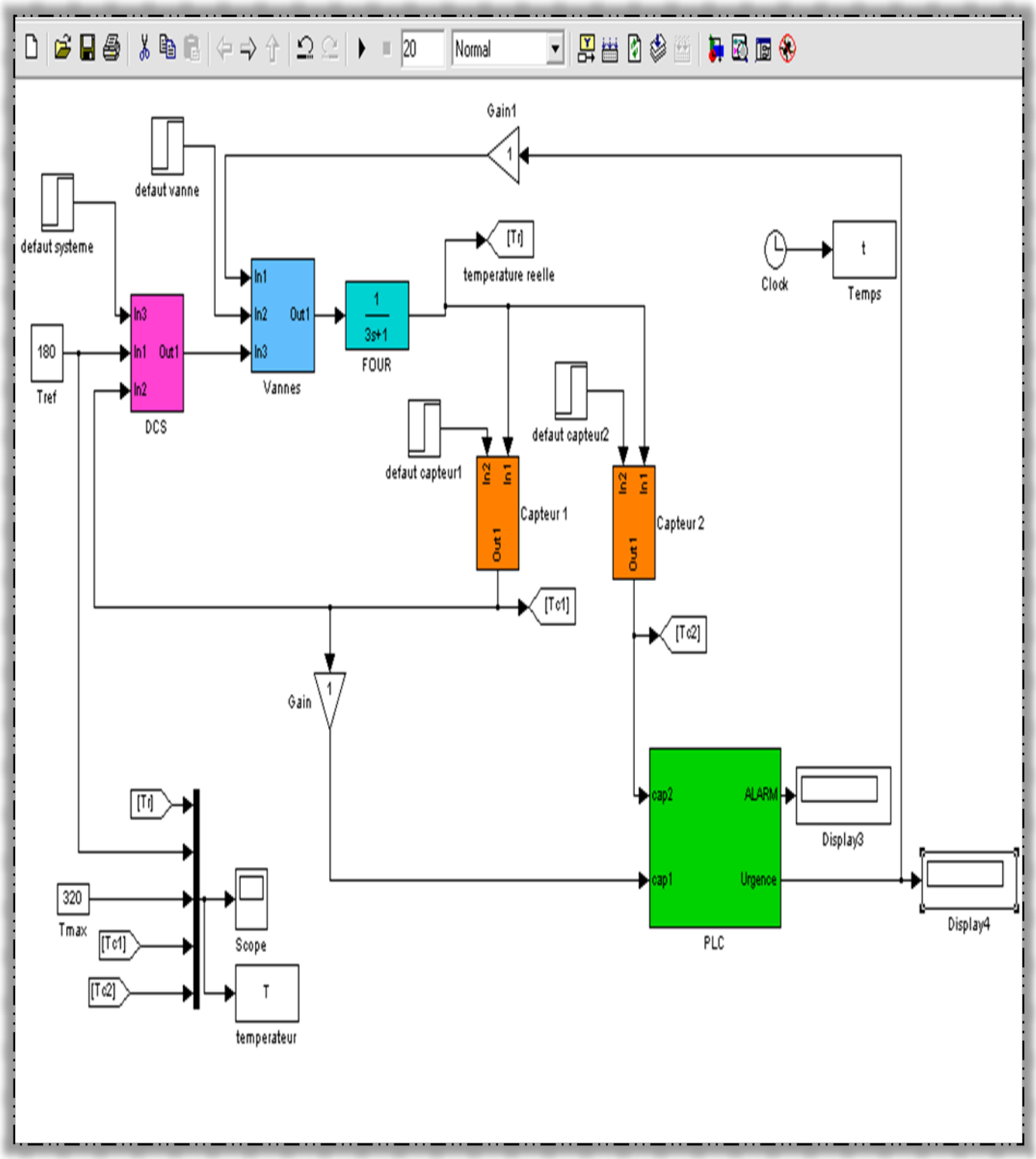


Figure 4.13. Schéma de simulation du système à deux capteurs

Un schéma simplifié du SIS à deux capteurs est donné par la figure (4.14).

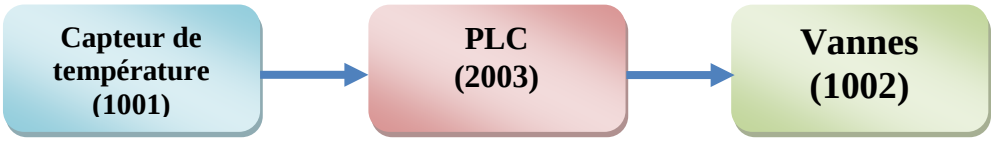


Figure 4.14. Schéma du SIS à deux capteurs

4.3.2.2. Résultats et Interprétation :

A) Système sans et avec Défaut (défaillance du DCS) :

Les figures (4.15) et (4.16) montrent respectivement le système en absence et en présence de défaut au niveau du DCS. Le SIS étant opérationnel, le système est ramené à un état de sécurité par coupure du fuel gaz et diminution progressive de température.

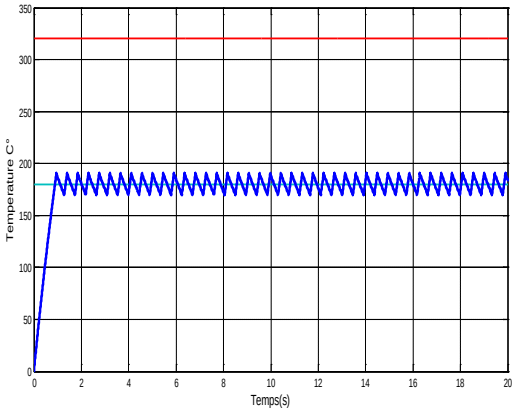


Figure 4.15. Système sans défaut

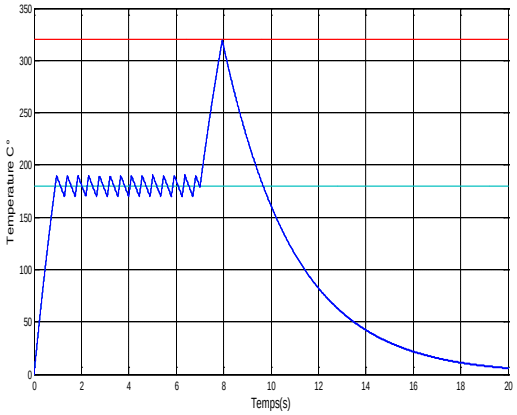


Figure 4.16. Système défaillant

B) Système avec défaillance des capteurs :

La figure (4.17) montre le comportement du système en présence de défaillance du capteur 2 du SIS. Dans ce cas, une alarme se produit, mais le système continue à fonctionner avec un fonctionnement en mode dégradé du SIS.

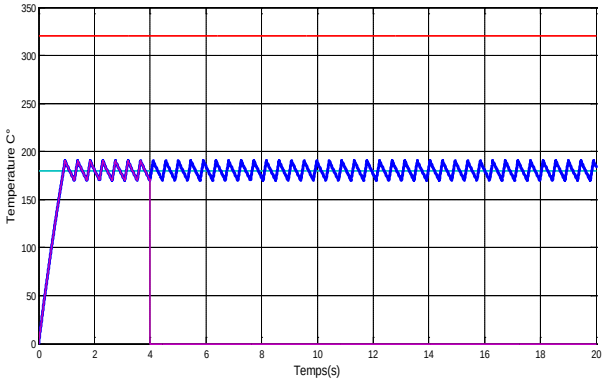


Figure 4.17. Cas de défaillance du Capteur 2 du SIS

Les figures (4.18) et (4.19) montrent les variations de la température dans le cas de défaillance des capteurs du SIS et du DCS. En présence de défaillance du capteur 2 du SIS, le système continue à fonctionner jusqu'à l'apparition de la défaillance du capteur 1 (concernant DCS et SIS) où l'on constatera une augmentation de température au-delà de 320°, ce qui signifie que le SIS est devenu défaillant et l'arrêt d'urgence ne s'est pas produit. Le même résultat est obtenu en cas de défaillance du capteur 1 du DCS puis du capteur 2 du PLC.

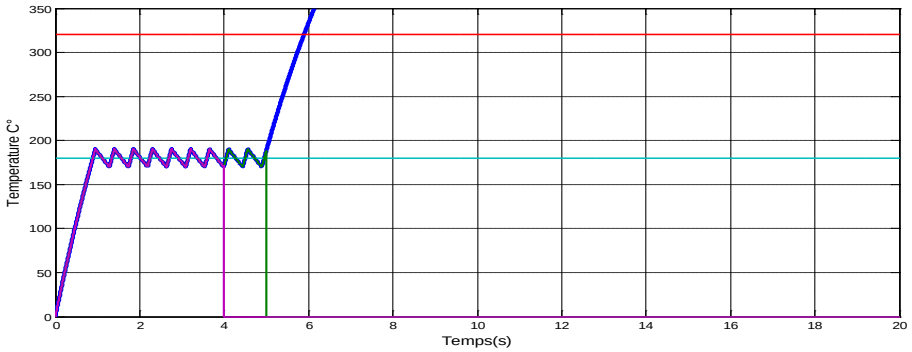


Figure 4.18. Cas de défaillance du Capteur 2 (SIS) et du capteur 1 (DCS)

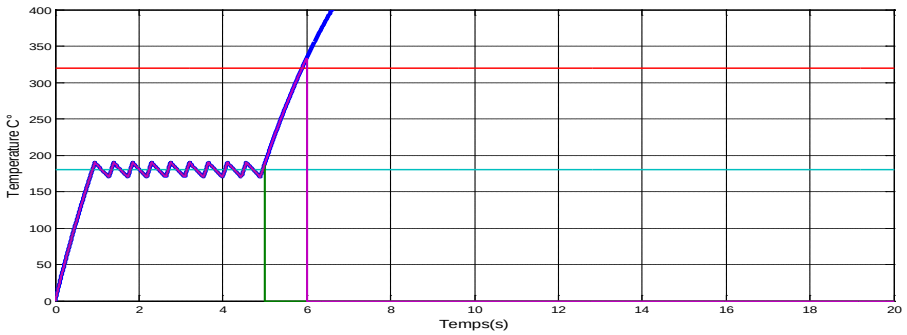


Figure 4.19. Cas de défaillance du capteur1 (DCS) et du capteur 2 (PLC)

Les figures (4.20) et (4.21) montrent le cas où le système est défaillant (défaillance du DCS) et le SIS est opérationnel en mode dégradé (capteur 2 défaillant). Dans ce cas, quelque soit le moment d'apparition de la défaillance du DCS et celle du capteur 2 du SIS, la température est ramenée à la valeur de zéro par ESD (coupure du fuel gaz par le SIS).

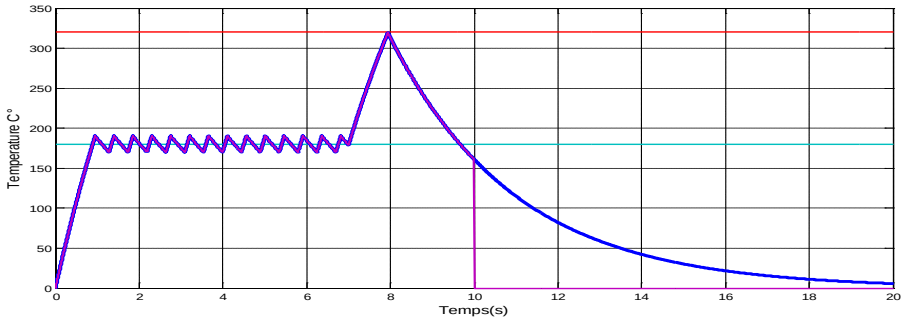


Figure 4.20. Défaillance du système puis défaillance du capteur2 du PLC

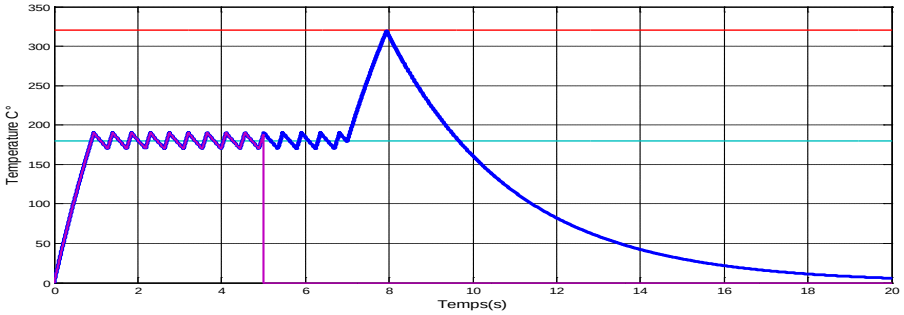


Figure 4.21. Défaillance du capteur2 du PLC puis défaillance du système

4.4. Etude expérimentale :

Dans cette partie, nous présentons les résultats expérimentaux issus de la mise en œuvre pratique des opérations de simulation, objets de vérification et de validation. Précisément, nous avons étudié l'influence des défauts au niveau des composants du SIS (spécifiquement les capteurs) sur le comportement du système.

4.4.1. Présentation du banc d'essais :

Pour la mise en œuvre expérimentale de notre système, un banc d'essais a été monté au laboratoire LSPIE de l'université de Batna. Ce banc d'essais comporte cinq principaux éléments, comme le montre le tableau (4.2). Le DSPACE 1103 est utilisé pour assurer la fonction du PLC du SIS. La carte dSPACE DS1103 est à double processeur de signal ; le PowerPC 604 du constructeur Motorola travaillant autant que maître et le TMS320F240 du constructeur Texas Instruments, travaillant autant qu'esclave (Master–Slave configuration). La carte est logée dans le Bus ISA du PC. Elle dispose d'une interface soft « ControlDesk Ver. 1.2 » qui gère les composants en temps réel (RTI). L'installation correcte de la partie software permet d'exploiter la librairie temps réel « RTI1103 library » de la DS1103 sous l'environnement MATLAB/SIMULINK.

L'étude expérimentale a porté sur le cas du système à deux capteurs de température étant donné que le système à un seul capteur est cas particulier de celui-ci. Le synoptique de l'expérience est donné par la figure (4.22).

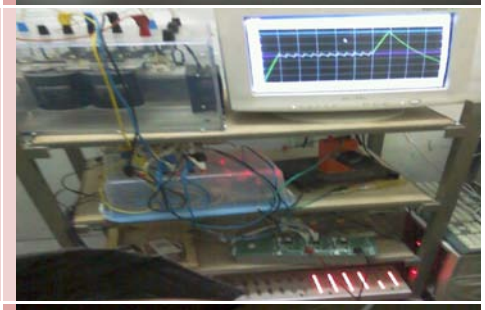
N°	Composant réel	Composant utilisé	Photo
1	Four rebouilleur	Four simple/Résistance	
2	DCS	Régulateur	
3	Capteur de température	Thermocouple	
4	PLC	dSPACE 1103	
5	Vanne	Contacteurs	

Tableau 4.2. Principaux éléments du banc d'essais

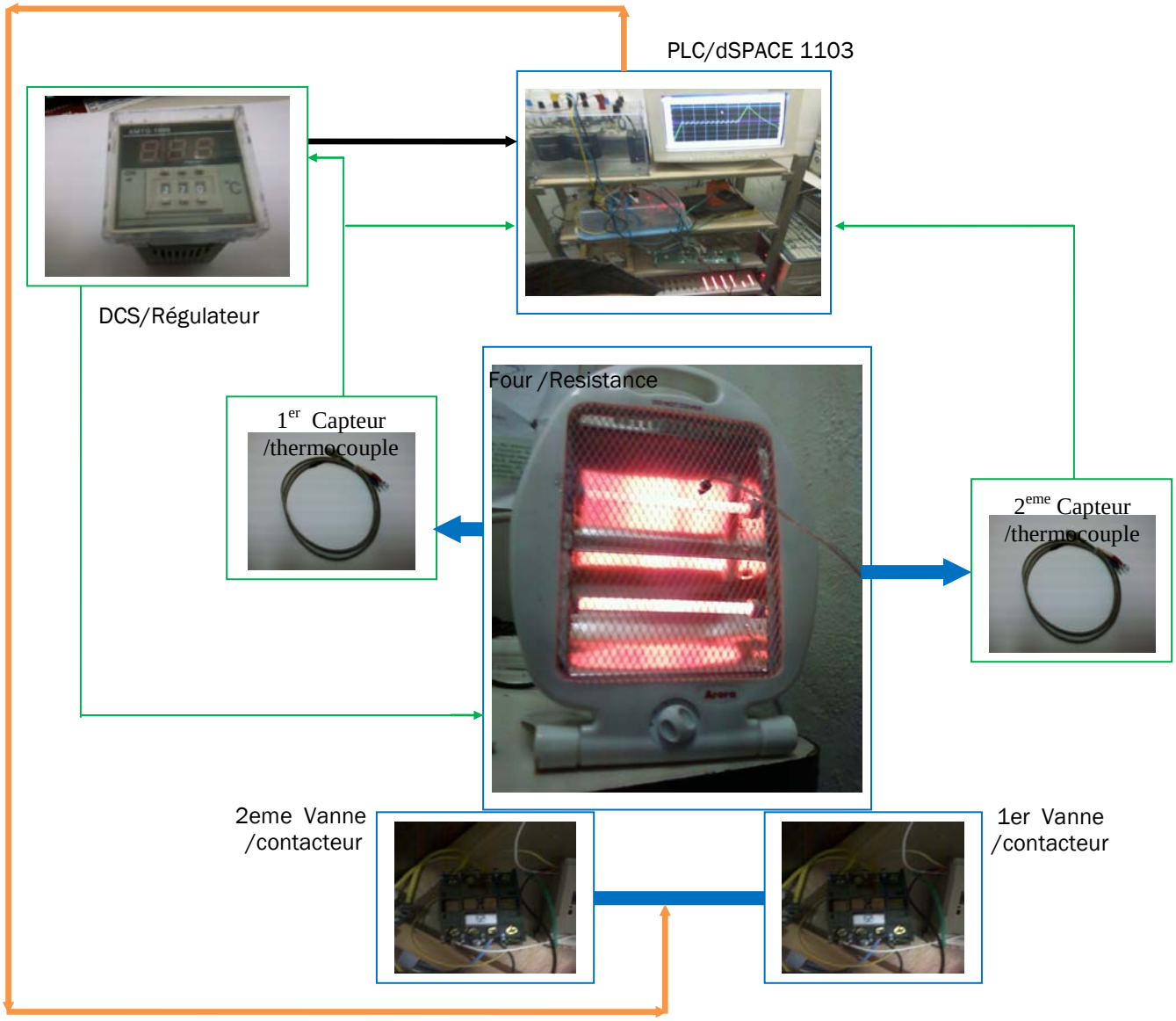


Figure 4.22. Synoptique du banc d'essais à deux capteurs

4.4.2. Résultats et Interprétation :

4.4.2.1. Système sans et avec défaut :

La figure (4.23) décrit la variation de la température à l'intérieur du four dans le cas du fonctionnement normal du système (DCS opérationnel). La figure (4.24) montre l'arrêt d'urgence par intervention du SIS après défaillance du DCS et augmentation de la température jusqu'à 320°C. C'est les mêmes résultats donnés par simulation (voir figures 4.15 et 4.16)

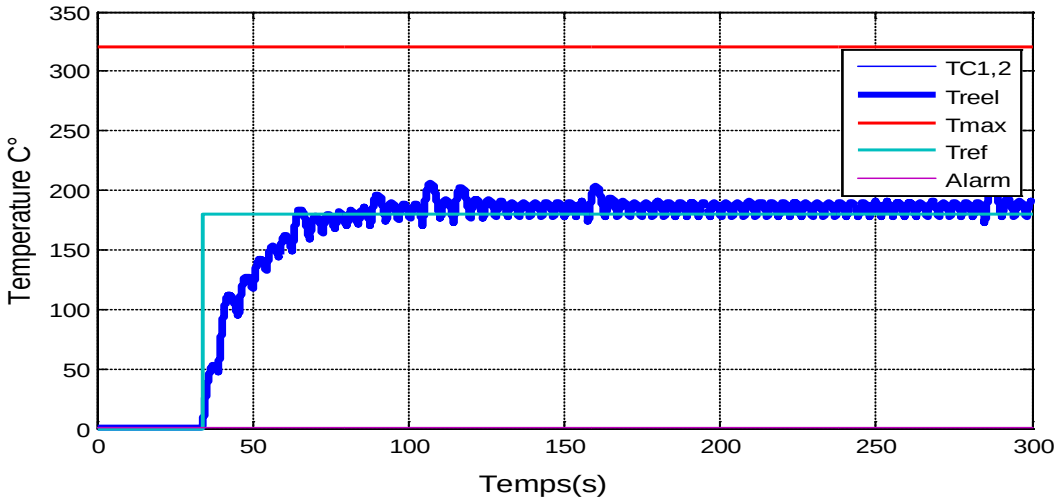


Figure 4.23 : Système sans défaut

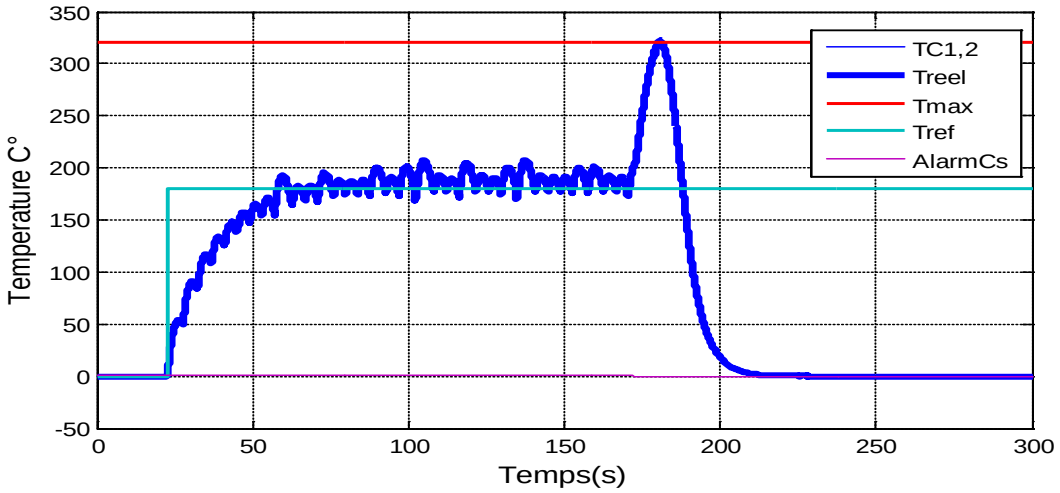


Figure 4.24 : Système défaillant

4.4.2.2. Défaillance des capteurs :

La figure (4.25) montre le cas de défaillance du capteur 1 du DCS. On peut remarquer l'arrêt d'urgence lorsque la température max (320°C) est atteinte. Ce résultat confirme celui de la simulation (voir figure 4.16).

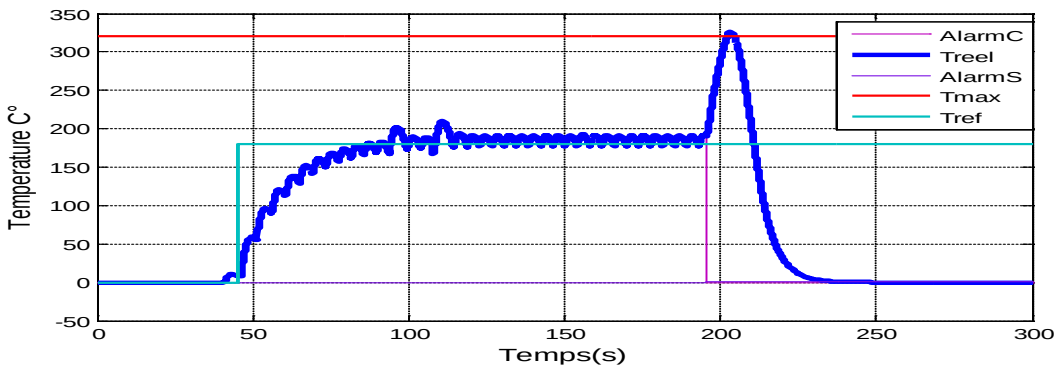


Figure 4.25. Défaillance du capteur 1(DCS)

Le fait que la défaillance du capteur 1 ait lieu avant ou après la défaillance du système (DCS), n'altère en aucun cas la fonction du SIS intervenant pour assurer l'arrêt d'urgence, comme le montre les figures (4.26) et (4.27).

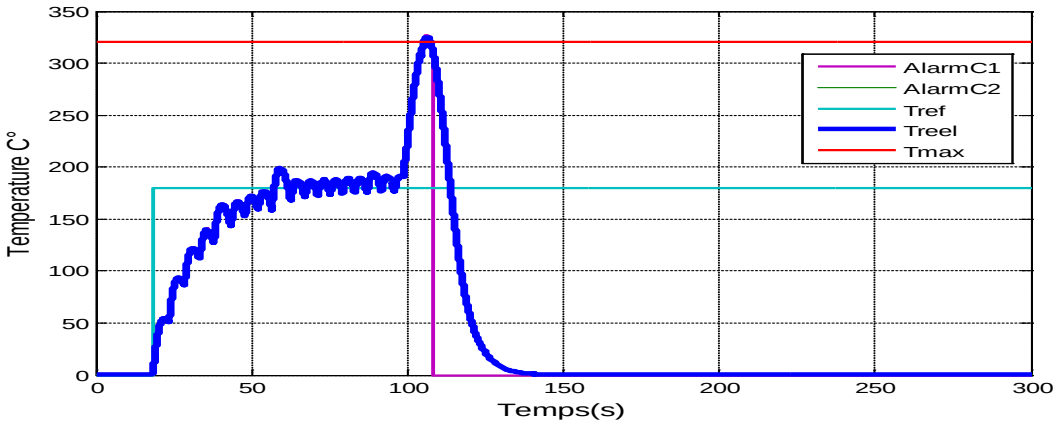


Figure 4.26. Défaillance du capteur 1 après défaillance du Système

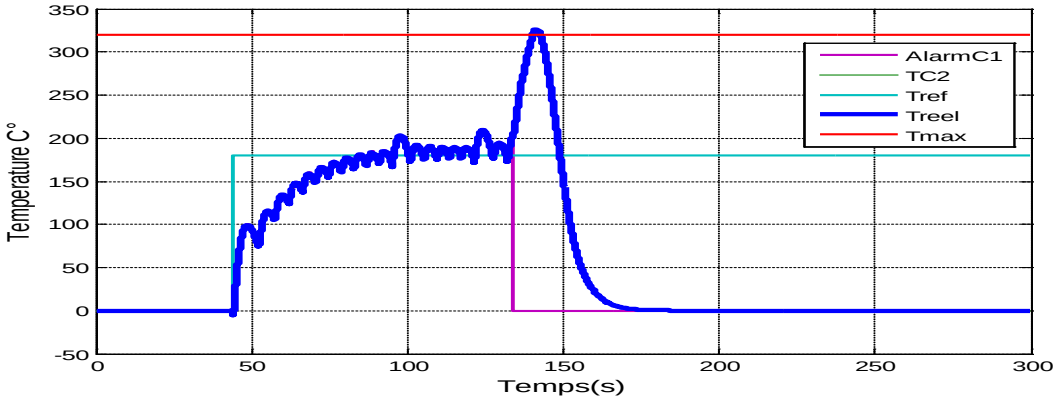


Figure 4.27. Défaillance du capteur 1 avant défaillance du Système

En ca de défaillance du capteur 2 du PLC (SIS), le DCS étant opérationnel, une alarme se produit mais le système continue à fonctionner, comme on peut voir sur la figure (4.28).

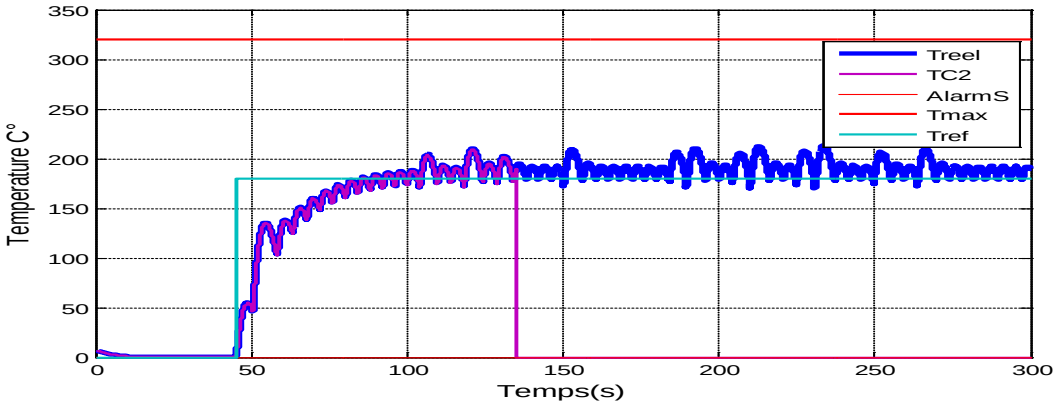


Figure 4.28. Défaillance du capteur 2 (PLC)

Si on plus de la défaillance du capteur 2 du PLC (SIS), on a la réalisation de la défaillance du capteur1 (commun au DCS et PLC), il n'y a pas d'arrêt d'urgence à cause de la défaillance du

SIS et donc, la température dépasse la valeur maximale (320°C), comme le montre la figure (4.29). Ce résultat est le même donné par simulation (voir figures 4.18 et 4.19).

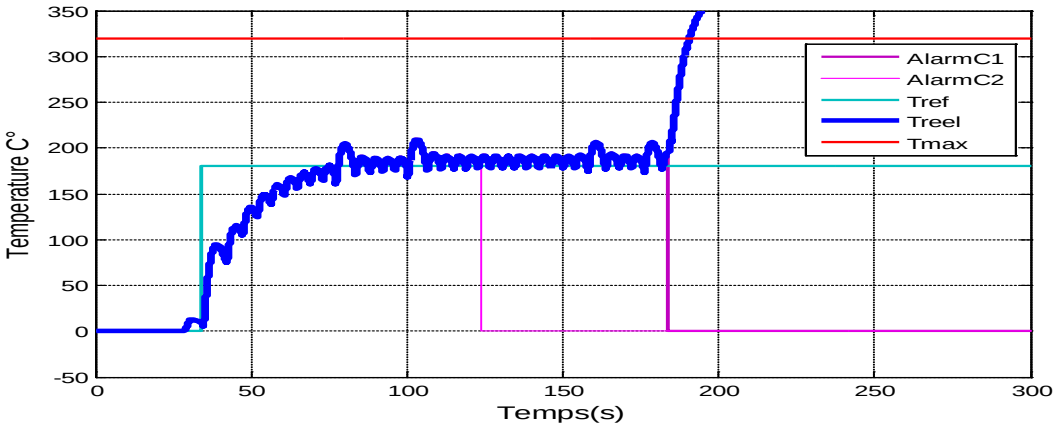


Figure 4.29. Défaillance du capteur 2-PLC et du Capteur 1-DCS

Nous avons pu aussi remarquer que le temps et l'ordre d'apparition des défaillances des composants du SIS (capteurs) et celles du système jouent un rôle important dans la disponibilité du SIS. En effet, si l'on a la défaillance du capteur 2, puis la défaillance du système, puis la défaillance du capteur 1, le SIS procède a l'arrêt d'urgence (par effet de défaillance latente du capteur 1) (voir figure 4.30).

Mais si la défaillance du capteur 2 succède directement celle du capteur 1, puis l'on l'apparition de la défaillance du système, le SIS ne procèdera pas à l'arrêt d'urgence, étant donné que son sous-système de capteurs est déjà défaillant (voir figure 4.31).

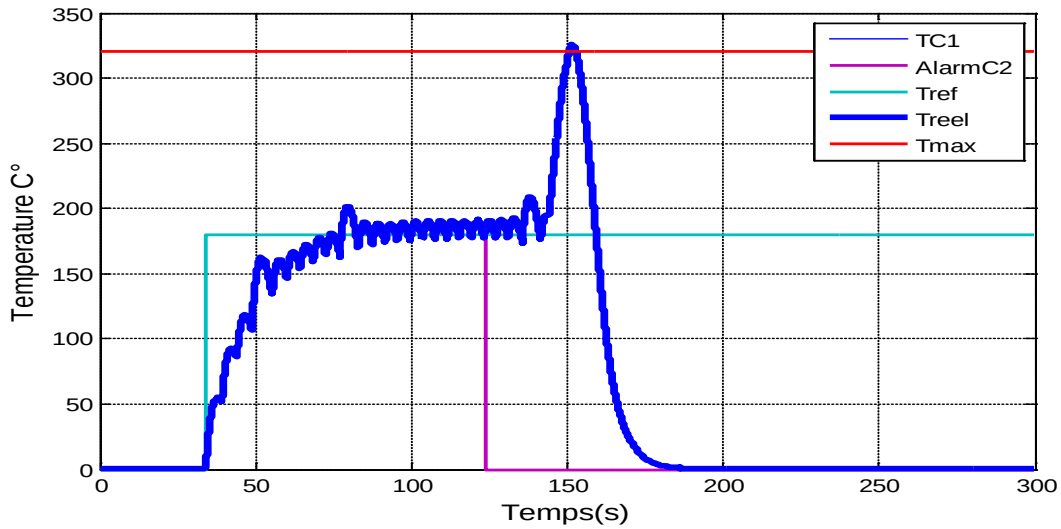


Figure 4.30. Défaillance du capteur 2, puis du Système, puis du capteur 1

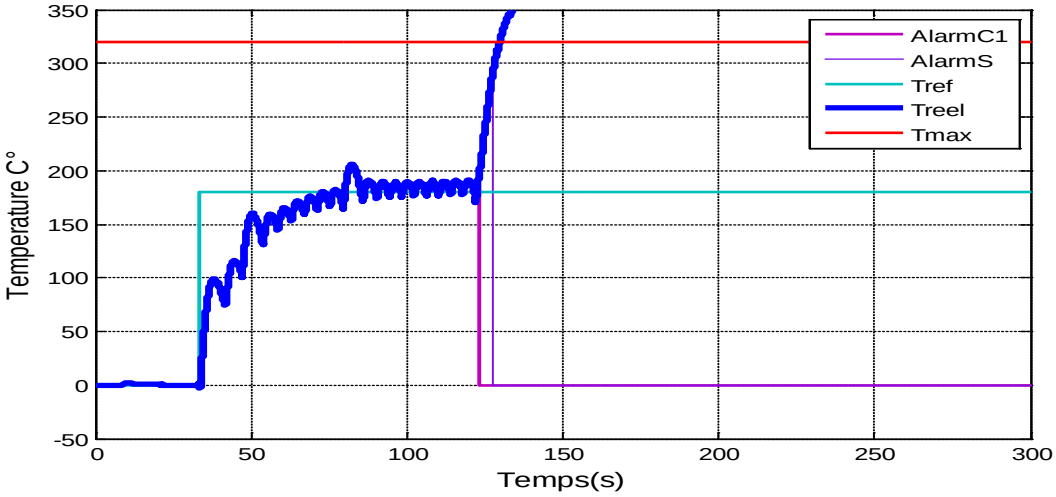


Figure 4.31. Défaillance du capteur 2, puis du capteur 1, puis du Système

4.4.2.3. Défaillance des PLC :

Nous avons aussi testé le cas des défaillances des PLC pris ensemble ou séparément. On a remarqué que la défaillance des PLC n'influent pas sur le fonctionnement du système (voir figures 4.32, 4.33 et 4.34).

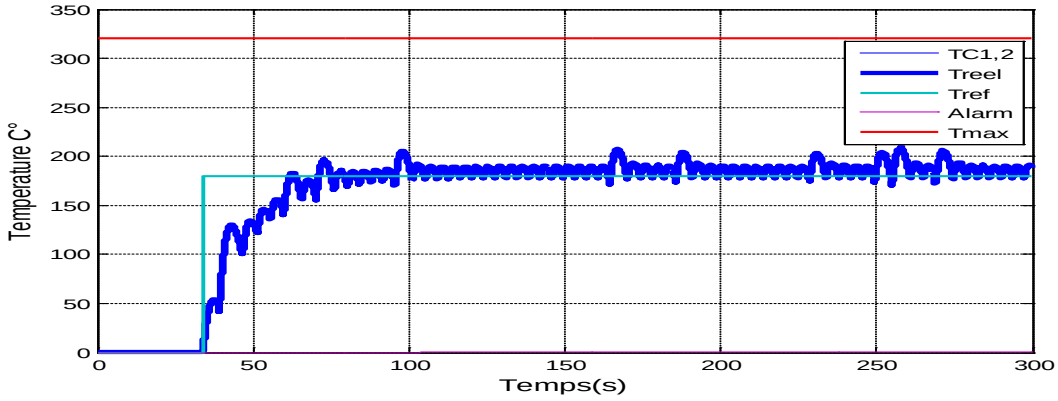


Figure 4.32. Défaillance du PLC 1

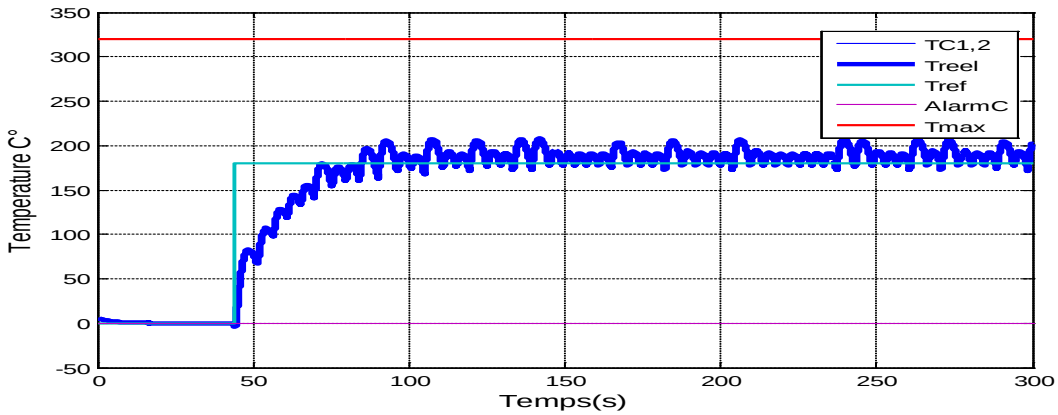


Figure 4.33. Défaillance des PLC 1 et 2

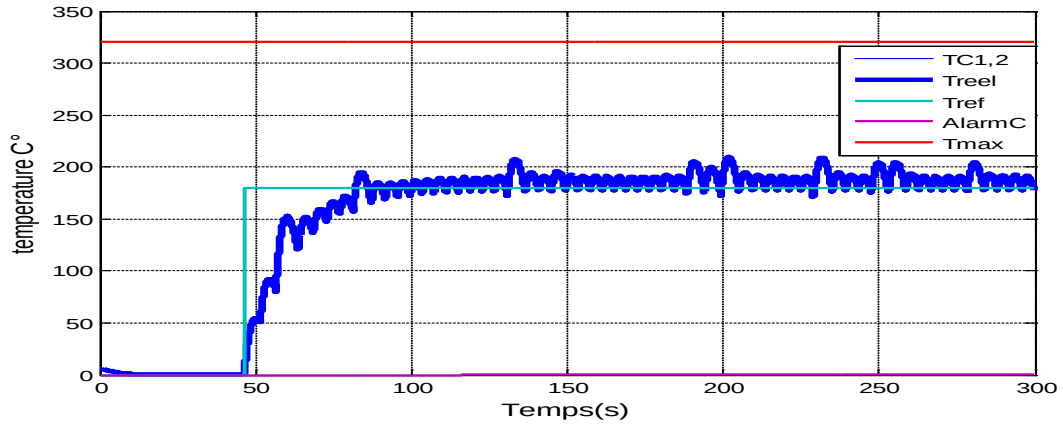


Figure 4.34. Défaillance des PLC 1, 2 et 3

4.4.2.4. Défaillance des vannes :

En présence d'une fermeture intempestive des vannes, on assiste à un arrêt d'urgence du système, comme on peut le voir sur la figure (4.35).

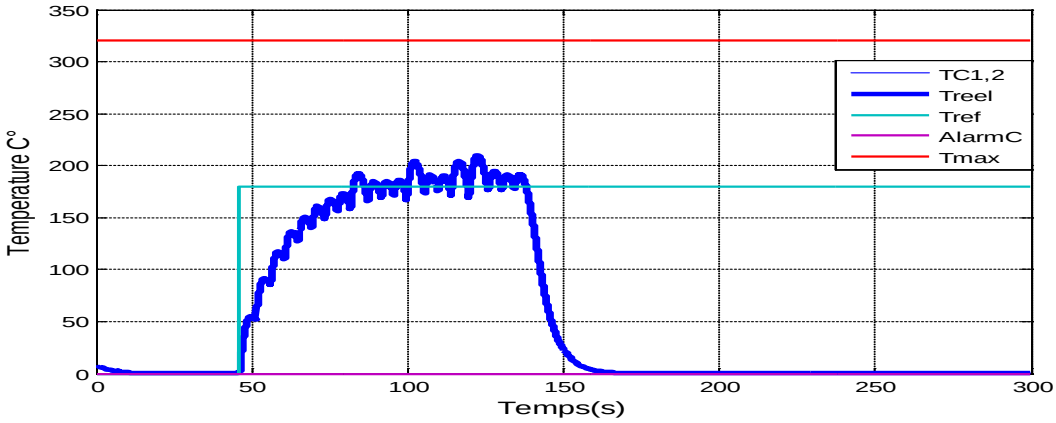


Figure 4.35. Défaillance des Vannes (Fermeture intempestive)

4.5. Conclusion :

Dans ce chapitre, nous avons présenté dans un premier temps les résultats de simulation par SIMULINK des défauts observés sur un système « four rebouilleur », afin de tester la disponibilité d'un SIS en cas d'existence d'un facteur de déclenchement.

Les différentes simulations effectuées montrent que la redondance des composants et la tolérance aux défauts des éléments du SIS sont nécessaires pour compenser les effets de ces défauts sur les performances du système. Ainsi on a pu conclure que l'utilisation d'un seul

capteur de température ne répond aux exigences de sécurité, d'où la nécessité d'association d'un deuxième capteur de température.

Les résultats de simulation en présence et absence de défauts font apparaitre deux situations, en l'occurrence :

- ✓ Si le SIS est opérationnel, la température diminue progressivement à la valeur nulle et le système se met dans un état de sécurité (ESD)
- ✓ Par contre si le SIS est défaillant, l'arrêt d'urgence (ESD) n'est pas assuré et la température continue à croître, d'où la mise en péril de la sûreté du système global.

Dans un second temps, nous avons procédé à une étude expérimentale par montage et exploitation d'un système de réchauffement similaire au système « four rebouilleur ». On a utilisé une résistance, un régulateur de température, des thermocouples et des contacteurs, l'ensemble est connecté à un dSPACE 1103 associé à l'environnement SIMULINK/MATLAB. Cette partie nous a permis de vérifier et valider les résultats obtenus par la simulation. L'utilisation de deux capteurs (dont l'un est commun au SIS et au DCS) a montré que le système à deux capteurs est plus performant par effet de tolérance aux défauts.

Conclusion Générale

A) Travail réalisé

Le travail présenté dans ce mémoire avait un double objectif. Dans une première partie, il était question d'évaluer la performance au sens probabiliste des systèmes instrumentés de sécurité avec une application à un système instrumenté dont la fonction est la coupure de fuel gaz alimentant un système four rebouilleur, en présence de défaillance du système de régulation de température (situation dangereuse). Puis dans une deuxième partie (partie essentielle de ce mémoire), on a abordé le diagnostic des défaillances des systèmes instrumentés de sécurité avec comme application le même système « four rebouilleur ».

La méthode des graphes de Markov et celle des équations simplifiées (normes IEC 61508) ont été utilisée pour évaluer la PFDavg du SIS du four rebouilleur. Mais au préalable, une revue détaillée des équations du modèle Markovien pour les architectures constituant ce SIS, est réalisée. Nous avons pu retenir deux principaux résultats : 1) On a constaté une certaine différence entre les résultats issus du modèle Markovien et ceux donnés les équations simplifiés. 2) Selon le concepteur, le SIS du four rebouilleur est certifié SIL2 ; ce qui correspond, selon les résultats obtenus par les deux méthodes utilisées, à une PFDavg de l'ordre de 10^{-3} pour un DC=60%. Or cet ordre est pratiquement donné par la valeur de la PFDavg du capteur qui constitue à cet égard un élément critique pour le SIS. D'où la nécessité d'augmenter la disponibilité de cet élément. Pratiquement parlant, une architecture 1002 pour le sous-système « capteurs » permet le passage d'un SIL2 vers un SIL3 pour la fonction de sécurité du SIS.

La deuxième partie du présent travail a été consacrée au diagnostic des défaillances des éléments du SIS du four rebouilleur. Dans un premier temps, nous avons procédé à une simulation par SIMULINK/MATLAB des défauts observés sur le système « four

rebouilleur », afin de tester la disponibilité du SIS en cas d'existence d'un facteur de déclenchement. Les résultats de simulation montrent que la redondance des composants et la tolérance aux défauts des éléments du SIS sont nécessaires pour compenser les effets de ces défauts sur les performances du système. A cet égard, on a pu conclure que l'utilisation d'un seul capteur de température ne répond aux exigences de sécurité, d'où la nécessité d'association d'un deuxième capteur de température. Dans un second temps, nous avons procédé à une étude expérimentale par montage et exploitation d'un système de réchauffement similaire au système « four rebouilleur ». Un carte dSPACE 1103 associé à l'environnement SIMULINK/MATLAB est utilisé comme solveur du SIS. Les résultats expérimentaux nous ont permis de vérifier et valider les résultats obtenus par simulation. L'utilisation de deux capteurs (dont l'un est commun au SIS et au DCS) a montré que le système à deux capteurs est plus performant par effet de tolérance aux défauts.

B) Difficultés rencontrées et perspectives

Les principales difficultés rencontrées lors de la réalisation de ce travail sont :

- Le manque des données relatives aux éléments du SIS, en l'occurrence : taux de défaillance et de réparation, temps des tests périodiques, le facteur β des causes communes.
- La difficulté de concevoir un modèle de simulation qui doit gérer des cas de combinaisons de défauts pouvant survenir en même temps.

Nous suggérons donc dans un premier temps, une collecte de données de fiabilité par retour d'expérience et leurs traitements par des méthodes statistiques. Puis nous proposons comme perspective à notre travail, l'étude de l'implantation de deux capteurs pour le SIS qui sont totalement indépendants du système (i.e. sous-système DCS) et ce, pour pouvoir vérifier tous les cas existants réellement.

5

ANNEXE

ANNEXES B :

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 [BAJ 78], [BAJ 80], [PAG 80], [VIL 80]. 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 :

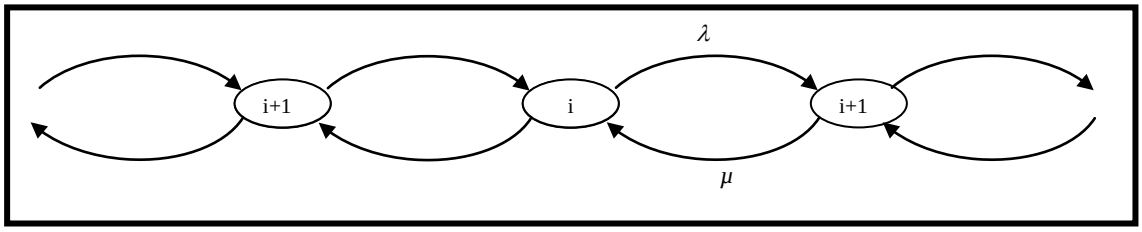


Figure B.1 - Processus markovien

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

Soit :

$$P'_i(t) = \lambda_{i+1,i}(t)\,P_{i+1}(t) - [\,\lambda_{i,i-1}(t) + \mu_{i,i+1}(t)]\,P_i(t) + \mu_{i-1,i}(t)\,P_{i-1}(t) \quad (2)$$

Avec les équations aux limites :

$$P'_n(t) = -\lambda_{n,n-1}(t)\,P_n(t) + \mu_{n-1,n}(t)\,P_{n-1}(t) \quad (3)$$

$$P'o(t) = \lambda_{1,o}(t)\,P_1(t) - \mu_{o,1}(t)\,P_o(t) \quad (4)$$

Et sous forme matricielle :

$$[P'(t)] = [\lambda(t),=\mu(t)]\,[P(t)] \quad avec \quad [P(t)] = \begin{pmatrix} P_n(t) \\ \vdots \\ P_o(t) \end{pmatrix} \quad (5)$$

Sachant que :

$$\Sigma_i\,P_i(t) = 1 \text{ et } Pn(o) = 1 \quad (6)$$

Pour une redondance parallèle.

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

$$\lambda_{i,i-1} = i\,\lambda \text{ et } \mu_{i,i+1} = \mu \quad (7)$$

Et avec *r* réparateurs :

$$\mu_{i,\,i+1} = (n-i)\mu \text{ pour } (n-i) < r \text{ ou } r\mu \text{ pour } n-i \geq r \quad (8)$$

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

$$[P(t)] = [P(o)]\,e^{-[\lambda,\mu]t} \quad (9)$$

2.1.2- Système à deux dispositifs parallèles

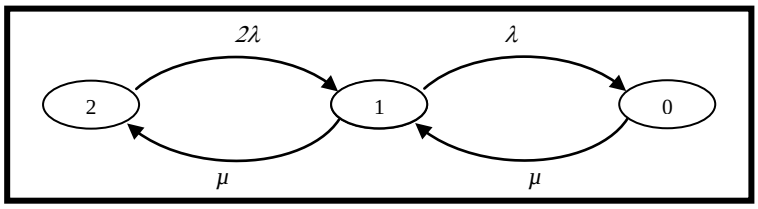


Figure B.2 - Deux dispositifs et un seul réparateur

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

$$\begin{pmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & \mu \\ 0 & \lambda & -\mu \end{pmatrix}$$

$$[P'] = [P(t)] \quad (10)$$

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

$$P_2 + P_1 + P_o = 1 \quad (11)$$

Il vient :

$$P_o = 2\lambda^2 / (2\lambda^2 + 2\lambda\mu + \mu^2) \quad (12)$$

Cette probabilité représente l'indisponibilité moyenne du système.

La disponibilité vaut :

$$A = 1 - P_o = (2\lambda\mu + \mu^2)/(2\lambda^2 + 2\lambda\mu + \mu^2) \quad (13)$$

Et si $\lambda << \mu$:

$$A \approx 1 - 2\lambda^2/\mu^2 \quad (14)$$

L'indisponibilité $1 - A$ vaut :

$$A' \approx 2\lambda^2/\mu^2 \quad (15)$$

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

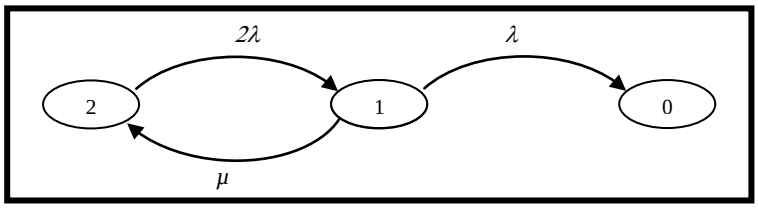


Figure B.3 – Fiabilité

$$[P'] = \begin{pmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{pmatrix} [P(t)] \quad (16)$$

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 :

$$R(t) = 1 - P_o(t) = [\ \lambda_1\ e^{\lambda_2 t} - \lambda 2\ e^{\lambda_1 t}\ ] / (\lambda_1 - \lambda_2) \quad (17)$$

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

$$MTTR = +(3\lambda + \mu)/2\lambda^2 \quad (18)$$

En général $\lambda << \mu$ et $MTTR \approx \mu/ 2\lambda^2$ (19)

Avec deux réparateurs ou plus, il vient :

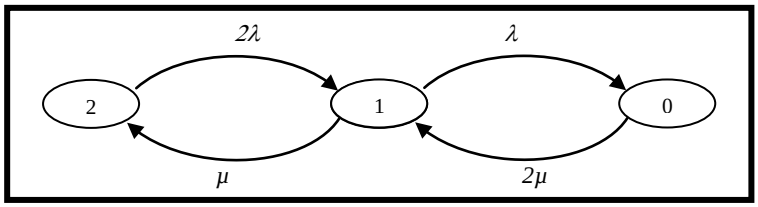


Figure B.4 - Deux dispositifs et deux réparateurs

$$A = (\mu^2 + 2\mu\lambda)/(\lambda + \mu)^2 = 1 - (1-\mu/(\lambda+\mu))^2 \quad (20)$$

$$A \approx 1 - \lambda^2/\mu^2 \quad (21)$$

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

$$A = 3\mu/ (2\lambda + 3\mu) = 1 - 2\lambda/ (2\lambda + 3\mu) \approx 1 - 2\lambda / (3\mu) \quad (22)$$

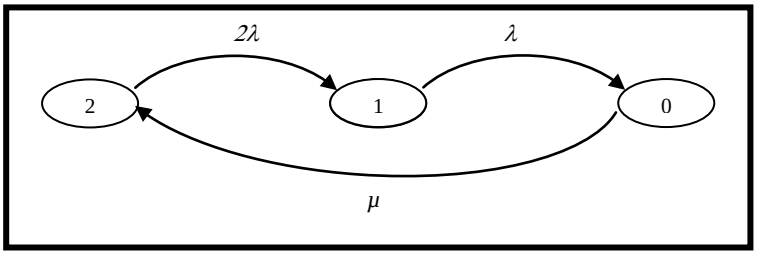


Figure B.5 - Détection de la panne totale

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 :

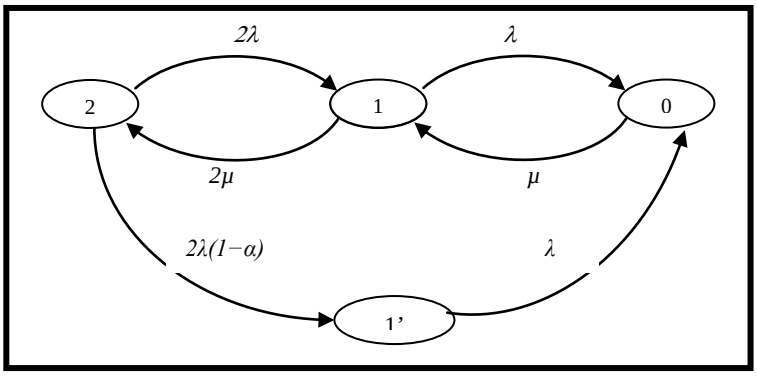


Figure B.6- Détection imparfaite de la panne

$$A' = 2\lambda\,[\lambda + \mu\varpi\,]\,/\mu^2(1 + 2\varpi\,) \qquad (23)$$

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

$$A' \approx 2\lambda\,(\lambda + \mu\varpi\,)/\mu^2 \qquad (24)$$

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 :

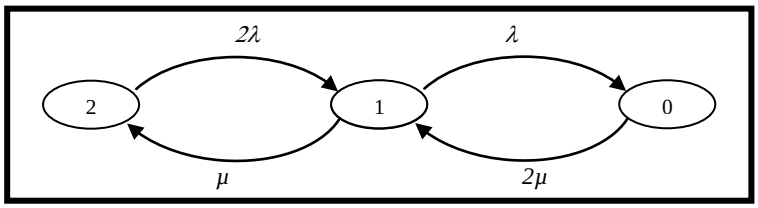


Figure B.7- Fiabilité série

$$[P'(t)] = \begin{pmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 2\mu \\ 0 & \lambda & -2\mu \end{pmatrix} [P(t)] \qquad (25)$$

En régime stationnaire :

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

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

Et la disponibilité moyenne vaut :

$$P_2 = A = 1 - P_o - P_1 = \mu^2/(\lambda+\mu)^2 \approx 1 - 2\lambda/\mu \qquad (26)$$

Ce qui se généralise à des composants en série :

$$A = \Sigma A_i \quad (27)$$

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 :

$$A = A_1^2 (3 - 2A_1) \quad (28)$$

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 :

$$A' = \lambda^2 / (\lambda^2 + \mu\lambda + \mu^2) \approx \lambda^2/\mu^2 \text{ si } \lambda_o = 0 \quad (29)$$

Avec un seul réparateur et :

$$A' \approx \lambda^2 / 2\,\mu^2 \quad (30)$$

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, 02], 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} .

Bibliographie

[ADR 00] O.Adrot. Diagnostic à base de modèles incertains utilisant l'analyse par intervalles : l'approche bornante. Thèse de Doctorat soutenue à l'Université de Nancy, 2000.
[AUB 04] O.Aubry. Sécurité des procédés industriels. Forum ELEC/MESUCORA ELEC 2004.Endress + Hausser. Decembre 2004.

[AYA 05] N.Ayault. Evaluation des barrières techniques de sécurité. INERIS, février 2005.

[BAJ 78] T.Bajenesco. Initiation à la fiabilité électronique, Masson, 1978.

[BAJ 80] T.Bajenesco. Problèmes de fiabilité des composants électroniques actuels, Masson, 1980.

[BAR 10] N.Barkat. Méthodes analytiques de détection des défauts dans les systèmes bouclés : application à un actionneur électrotechnique. Mémoire de Magister soutenu à l'Université de Batna, 2010.

[BEC 01] L. Beckman, Easily assess complex safety loops. Chem Eng Progr 2001.

[BEN 05] T.Bentrcia. Diagnostic et heuristique des systèmes industriels complexe».Mémoire de Magister soutenu à l'Université de Batna, 6 février 2005.

[BEU 06] 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.

[BOU 97] N.Boudaoud .Conception d'un système de diagnostic adaptatif en ligne pour la surveillance des systèmes évolutifs. Thèse de Doctorat soutenue à l'Université de Technologie de Compiègne, France, 1997.

[BUK 95] J. Bukowski, W. Goble. Using Markov models for safety analysis of programmable electronic systems. ISA Trans, 1995.

[BUK 05] J. Bukowski. A comparison of techniques for computing PFD average. In: Proceedings of the annual reliability and maintainability symposium, 2005.

[CCPS 02] CCPS. Offshore reliability data handbook, 4th Edition. 2002.

[COM 91] M.Combacau. Commande et surveillance des systèmes à événements discrets complexes : application aux ateliers flexibles .Thèse de Doctorat soutenue à l'Université de Toulouse, 1991.

[COM 00] M.Combacau, BERRUET P, CHARBONNAUD F, KHATAB A .Réflexions sur la terminologie : Surveillance – Supervision. Groupement pour la Recherche en Productique, Systèmes de Production Sûrs de Fonctionnement, http://www.laas.fr/~combacau/SPSF/sursup.html, 03 mars 2000.

[DAN 97] N.Dangoumau. Commande et Surveillance des Systèmes à Evénements Discrets, Approche par Réseaux de Petri».Thèse de Doctorat soutenue à l'Ecole Centrale de Nantes, 1997.

[DER 09] H.Derbel. Diagnostic à base de modèles des systèmes temporisés et d'une sous classe de systèmes dynamiques hybrides. Thèse de Doctorat soutenue à l'Université de Grenoble, 2009.

[DES et al 03] A. Desroches, A. Leroy, and F. Vallée. La gestion des risques : principes et pratiques. Lavoisier, France, 2003.

[DUB 90] B.Dubuisson. Diagnostic et Reconnaissance de Formes. Hermès Édition, 1990.

[ENS 05] ENSPM. Condition de fonctionnement et construction des fours tubulaires., 2005.

[EN 954-1 96] EN 954-1. Sécurité des machines. Partie des systèmes de commandes relatives à la sécurité. Partie 1 : Principes généraux, décembre 1996.

[FAL 00] E.Fal, J.Ldurka. Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de process industriels. INERIS, 2000

[FLE 74] K.Fleming. A reliability model for common mode failures in redundant systems.Technical report (1974).

[GOB 98] W. Goble, H. Cheddie. Control system safety evaluation and reliability. US: ISA; 1998.

[GRU 98] P.Gruln, J.Pittmann, S.Wiley, T.Leblanc, Quantifying the Impact of partial stroke valve testing of safety instrumented systems. ISA Transactions 37.pp,87-94.1998.

[HAU 06] S.Haug, P.Hokstad, Langseth.Haud, K.Oien.Reliability prediction method for safety instrumented systems, technical report 2006.

[HSE 95] Health and Safety Executive- Out of control HSE book,United Kingdom 1995.

[IEC61061 98] IEC61061. Stratifiés de bois densifiés, non imprégnés, à usages électriques. International Electrotechnical Commission (IEC), 1998.

[IEC 00] CEI 61508. Sécurité fonctionnelle des systèmes électriques/électroniques /électroniques programmables relatifs à la sécurité.Commession Electrotechnique Internationale,Genève,Suisse, 2000.

[IEC61508 02] IEC 61508. Sécurité fonctionnelle des systèmes électriques/électroniques /électroniques programmables relatifs à la sécurité, partie 6, mars 2002.

[IEC61511 03] IEC 61511. Functional safety – Safety instrumented systems for the process industry. International Electrotechnical Commission, Geneva, Switzerland, 2003.

[IEC62061 05] 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 84] 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.

[INN 08] F. Innal, contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances analyse critique de la norme CEI 61508, Thèse de doctorat, Université de bordeaux 1, Soutenu le 03 Juillet 2008.

[INN et al 05] 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 96] ISA-S84. Application of safety instrumented systems for process industries, 01.1996.

[ISA 84.00.01 04] ISA 84.00.01–2004. Functional Safety Instrumented Systems for the Process Industries, Parts 1–3, 2004.

[ISE 97] R Isermann. supervision, fault detection and diagnosis methods-an introduction, Control Eng. Practice, Vol.5, n0 5, pp.639-652, 1997.

[ISO 02] ISO. Management du risque : Vocabulaire, Principes directeurs pour l'utilisation dans les normes. Organisation internationale de normalisation, 2002.

[KEM 04] T.Kempowsky .Surveillance de procédés à base de méthodes de classification : conception d'Un outil d'aide pour la détection et le diagnostic des défaillances .Thèse de Doctorat soutenue à L'institut national des sciences appliquées de Toulouse, le 14 décembre 2004.

[KNE 02] B.Knegtering,Safety lifecycle management in the process industries:the development of a qualitative safety-related information analysis technique.Phd thesis, Technische Universiteit Eindhoven,2002.

[LAL 08] A.Lalami.Diagnostic et approche ensembliste à base des zonotopes.Thèse de Doctorat soutenue à l'Université de Cergy-pontoise, le 15 décembre 2008.

[LAM 02] P.Lamy. Probabilité de défaillance dangereuse d'un système explications et exemple de calcul. INRS, septembre 2002.

[LUN 07] M.A.Lundteigen, M.Rausand. Common cause failure in safety instrumented systems on oil and gas installations :Implementating defense measures through function testing. Journal of loss prevention in the Process Industries, Vol 20, PP218-229, 2007.

[MAC 04] D.Macdonald. Safety in field instruments and devices. Practical Industrial Safety. Risk Assessment and Shutdown Systems. 2004. pp, 200-229.

[MEC 11] W.Mechri. Evaluation de la performance des systèmes instrumentés de sécurité à paramètres imprécis. Thèse de Doctorat. Avril 2011.

[MKH 08] A.Mkhida. Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence».Thèse de Doctorat soutenue à l'Université de Nancy. Le 14 novembre 2008.

[MOH 07] S.Mohamed BOUGUELID. Contribution à l'application de la reconnaissance des formes et la théorie des possibilités au diagnostic adaptatif et prédictif des systèmes dynamiques. Thèse de Doctorat soutenue à l'Université de Reims Champagne-Ardenne, le 12 décembre 2007.

[MOS 87] A.Mosleh, N.Sin.A multiparameter event based common cause failure model. Proceeding of the 9th international conference on structural mechanics in reactor technology, (2) : 147152.(1987).

[NOB 04] T.Nobes. Smart instruments in protective measures, Is your product safe ? IEE Seminar, 2004

[ORA 05] A.Orantes MOLINA .Méthodologie pour le placement des capteurs à base de méthodes de classification en vue du diagnostic. Thèse de Doctorat soutenue à l'Université de Toulouse, 2005.

[ORE 02] Offshore reliability data handbook. OREDA, 2002.

[OUA 09] S.OUARHENT. Diagnostic de panne dans les systèmes roboties, Thest de magister en electronique soutenue a l'université de batna,juin 2009

[PAR 01] V.Paret, On the distribution of weath and income, in roots of the Italian School of Economics and Finance :from Ferrara (1857) to Einaudi (1944),M.Baldassarri and P.Ciocca,(EDS), vol.2, Houndmills,Palgrav.2001.

[PDS 04] Reliability Data for safety instrumented systems.PDS data handbook, september 2004.

[PHI 06] A.Philippot.Contribution au diagnostic décentralisé des systèmes à évènements discrets : application aux systèmes manufacturiers. Thèse de Doctorat soutenue à l'Université de Reims Champagne Ardenne, le 18 juillet 2006.

[RAC 06] D.Racoceanu. Contribution à la surveillance des Systèmes de Production en utilisant les Techniques de l'Intelligence Artificielle. Habilitation à diriger des recherches de l'Université de Franche-Comté de Besançon Soutenue le 19 janvier 2006.

[RAJ 05] C.R.Raju, Strengthening the weak link : the shutdown valve. Scion /05. Sensors for Industry Conference. Houston, Texas, USA. February 2005.

[RIQ 05] 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.

[RIP 99] P.Rippol. Conception d'un système de diagnostic flou appliqué au moteur automobile. Thèse de Doctorat soutenue à l'université de Savoie, 1999.

[ROD 05] M.Rodrigues. Diagnostic et commande active tolérante aux défauts appliqués aux systèmes décrits par des multi-modèles linéaires. Thèse de Doctorat soutenue à l'Université Heinri Poincaré, Nancy 1, 2005.

[SAL 08] N.Salhi. Surveillance et diagnostic d'une chaîne de production par les réseaux de neurones artificiels. Mémoire de Magister soutenu à l'université M'Hamed bougara-boumerdes, le 2 juillet 2008.

[SEL 07] M Sellak.. Évaluation de paramètres de sureté de fonctionnement en présence d'incertitudes et aide à la conception : application aux systèmes instrumentés de sécurité. Thèse de Doctorat soutenue à l'Ecole doctorale IAEM lorraine, 19 octobre 2007.

[SIN 06] Reliability Prediction Method for Safety Instrumented System. PDS Method Handbook, 2006 Edition. SINTEF, Trondheim,Norway.

[SMI 04] 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.

[SUM 00b] A.E.Summers, B.Zachary. Partial-stroke testing of block valves. Control Engineering, 47(12).pp, 87-89.2000.

[SUM 00] A. Summers. Simplified methods and fault tree analysis- Viewpoint on ISA TR84.0.02. ISA Trans 2000;

[VIL 80] A.Villemeur, Sûreté de fonctionnement des systèmes industriels, Eyrolles, 1988.

[ZHA et al 03] T.Zhang, W. Long, Y.Sato. Availability of systems with selfdiagnostic components-applying Markov model to IEC 61508-6. Reliab Eng System Saf, 2003.

[ZWI 95] G.Zwingelstein. Diagnostic des défaillances, théorie et pratique pour les systèmes industriels. traité des nouvelles technologies, diagnostic et maintenance, Hermes, 1995.