République Algérienne Démocratique et Populaire

UNIVERSITE BADJI MOKHTAR ANNABA  **جامعة باجي مختار عنابة**

Faculté des Sciences de l'Ingéniorat

Département d'Electronique

THÈSE

Présentée En Vue de L'obtention du Diplôme De Doctorat

Thème

Sûreté de Fonctionnement : Recherche des Scénarios Critiques dans les Systèmes Mécatroniques

Option
Automatique Industrielle

Présentée et soutenue par :

BOUCERREDJ Leila

Directeur de thèse : Mr DEBBACHE Nasr Eddine Pr U. Annaba

DEVANT LE JURY

Pr BAHI Tahar	Université Annaba	Président
Pr DEBBACHE Nasr Eddine	Université Annaba	Rapporteur
Pr ABBASSI Hadj Ahmed	Université Annaba	Examinateur
Pr MOUSSAOUI Abdelkrim	Université Guelma	Examinateur
Dr MEHENNAOUI Med Lamine	Université Skikda	Examinateur
Dr LALALOU Rachid	Université Skikda	Examinateur

Année : 2015

Remerciements

Je tiens à exprimer toute ma reconnaissance et ma gratitude à mon directeur de thèse Monsieur le Professeur **DEBBACHE Nasr Eddine**, pour avoir dirigé ce travail. Je le remercie pour ses précieux conseils et ses commentaires qui m'ont permis de surmonter mes difficultés et de progresser dans mes études. Qu'il soit remercié pour ses qualités humaines et scientifiques, et ses conseils judicieux sur différents points relatifs à mon projet de thèse. J'ai été honoré de travailler avec lui.

Mes remerciements s'adressent à Monsieur **BAHI Tahar**, Professeur à l'université d'Annaba, d'avoir fait l'honneur de présider mon jury de soutenance.

Je tiens à remercier Monsieur **ABASSI Hadj Ahmed** Professeur à l'université d'Annaba d'avoir accepté d'examiner mon travail de thèse et d'être membre de mon jury de soutenance.

Je tiens à remercier aussi, Monsieur **MOUSSAOUI Abdelkrim** Professeur à l'université de Guelma, de m'avoir fait l'honneur d'examiner mon travail et d'être membre de jury de ma thèse de doctorat.

Je suis très reconnaissante envers Messieurs **MEHENNAOUI Med Lamine** et **LALALOU Rachid,** Maîtres de conférences à l'université de Skikda, qui ont accepté d'examiner ce travail et à participer au jury de soutenance.

Mes respectueux remerciements à monsieur **Hamid DEMMOU** Professeur à LAAS-CNRS ''Université Paul Sabatier de Toulouse'', pour ses aides et conseils précieux ainsi que ses collaborations.

ملخص

***ملخص*:** الأنظمة الميكاترونيكية هي أنظمة هجينة تشمل كلاً من المتغيرات المستمرة والمتقطعة. الديناميكا المستمرة نحصل عليها بفضل معادلات تفاضلية جبرية بينما الجزء المتقطع يكون مندمج من قبل أنظمة التشغيل الذاتي أو التي تمر بمرحلة انتقالية.

الهدف الرئيسي لهذه الأطروحة هو التحليل الكيفي والكمي للحالات الحرجة ، التحليل الكيفي يعتمد على البحث عن الحد الأدنى للحالات الحرجة حيث يقترح هذا العمل نهجا جديدا في مجال أمنية التشغيل للأنظمة الميكاترونيكية. هدفها هو استخراج كافة السيناريوهات الحرجة ذات الحد الأدنى التي تؤدي بالنظام إلى حالة الفشل، وذلك مباشرة من أشجار الدليل للمنطق الخطي لإقامة روابط سببية بين الأحداث غير المرغوب فيها والحالات الطبيعية. أشجار الدليل للمنطق الخطي تحتوي على أحداث التي هي نتيجة لحالة في السيناريو، ولكن ليس سببا ضروريا تماما للإنتاج النهائي للحالة الحرجة، أيضا حجم شجرة الدليل يتناسب مع عدد من التحولات في معبر متتالي يمكن إثباته. لهذا يستند هذا النهج على مفهوم الحد الأدنى لطريقة شجرة الخطأ وتطبيقها على أشجار الدليل للمنطق الخطي لنموذج شبكات بيتري في سياق غير مألوف. الهدف منه هو تقليل حجم أشجار الدليل للمنطق الخطي وتوليد عدد أدنى من السيناريوهات الحرجة.

انطلاقا من نتائج التحليل الكيفي قمنا بالتحليل الكمي وذلك اعتمادا على التشكيلة الهجينة للأنظمة الميكاترونيكية، النمذجة الشكلية المعتمدة هنا هو النموذج الآلي الهجين.

الكلمات المفتاحية *: أمنية التشغيل، الأنظمة الميكاترونيكية، شبكات بيتري، المنطق الخطي، الحد الأدنى للسيناريوهات الحرجة، شجرة الخطأ، الحد الأدنى، الأنظمة الهجينة.*

Résumé

Résumé : Les systèmes mécatroniques sont des systèmes hybrides incluant à la fois des variables continues et discrètes. La dynamique continue est généralement fournie par des équations différentielles et algébriques alors que la partie discrète est modélisée par des automates ou les états à transitions.

L'objectif de cette thèse est d'une part l'analyse qualitative pour la détermination des scénarios redoutés minimaux, et d'autre part l'analyse quantitative basée sur les scénarios minimaux trouvés. Ce travail propose une nouvelle approche d'analyse de la sûreté de fonctionnement des systèmes mécatroniques. Le but est d'extraire les scénarios redoutés minimaux qui conduisent un système vers un état de défaillance, à partir des arbres de preuves de la logique linéaire et établir les liens de causalité entre les événements redoutés et les fonctionnements normaux. Les arbres de preuves de la logique linéaire contiennent des événements qui sont la conséquence d'événements inclus dans le scénario, mais qui ne sont pas strictement nécessaires à l'obtention finale de l'état critique redouté. La taille de l'arbre de preuve est proportionnelle au nombre de franchissement des transitions dans le séquent prouvable. L'approche qualitative proposée est basée sur la notion de coupe minimale de la méthode des arbres de défaillances appliquées aux arbres de preuves de la logique linéaire du modèle réseau de Pétri dans un contexte inconnu. Le but est de réduire la taille des arbres de preuves de la logique linéaire et de générer un nombre minimal de scénarios redoutés.

L'analyse quantitative pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques est basée sur les résultats de l'analyse qualitative. Le formalisme de modélisation adopté pour cette classe de systèmes s'appuie sur les automates hybrides.

Mots clés : *Sûreté de fonctionnement, système mécatronique, réseaux de Petri, logique linéaire, scénario redouté minimale, arbre de défaillance, coupe minimale, automate hybride.*

Abstract

Abstract : Mechatronic systems are hybrid systems include both continuous and discrete variables. Continuous dynamics is usually provided by differential and algebraic while the discrete part is modeled by automata or transitions to states.

The objective of this thesis is the qualitative analysis for determination of minimal feared scenarios, and then a quantitative analysis based on the minimal feared scenarios found. This work proposes a new approach for analysing the dependability of mechatronics systems; its goal is to extract all minimal feared scenarios that lead a system in a state of failure, directly from the proof trees of linear logic to establish the causality between undesirable events and normal operations. The proof trees of linear logic contain events that are the result of event in the scenario, but not strictly necessary for the final production of the critical feared state. The size of the proof tree is proportional to the number of firing transitions in the sequent provable. The proposed approach is based on the concept of minimal cutsets of the fault tree method applied to the proof trees of linear logic of Petri net model in an unknown context. The aim is to reduce the size of the proof trees of linear logic and generate a minimum number of feared scenarios.

The quantitative analysis for analysing the dependability of mechatronic systems is based to the results of qualitative analysis. The modeling formalism adopted for this class of systems is based on the model hybrid automata.

Key words : *Dependability, mechatronic system, Petri net, linear logic, minimal feared scenario, fault tree, cutsets, hybrid automata.*

Tables des matières

Introduction générale **1**

Chapitre 1 Systèmes Mécatroniques : Contexte et Problématique

1.1 Introduction 4

1.2 Les systèmes mécatroniques 4

1.2.1 Contexte historique 4

1.2.2 Exemple des systèmes mécatroniques 6

1.2.3 Ingénierie concourante 9

1.2.4 Cycle de développement 10

1.2.4.1 Analyse/Spécification 11

1.2.4.2 Conception 11

1.2.4.3 Réalisation 12

1.2.4.4 Vérification 12

1.2.4.5 Validation 12

1.3 La mécatronique au centre des préoccupations 13

1.4 Les systèmes mécatroniques et systèmes hybrides 13

1.5 Conclusion 14

Chapitre 2 La Sûreté de Fonctionnement : historique et analyse

2.1 Introduction 15

2.2 Historique de la sûreté de fonctionnement 15

2.3 Concepts et définitions 16

2.3.1 Fiabilité 17

2.3.2 Disponibilité 18

2.3.3 Maintenabilité 18

2.3.4 Sécurité 19

2.4 Quelques indicateurs 19

2.5 Moyens pour la sûreté de fonctionnement 21
2.6 Enjeu de la sûreté de fonctionnement 21
2.7 Les études de sûreté de fonctionnement.....21
2.7.1 Étape par étape 22
2.7.2 Études périphériques 23
2.7.3 En pratique 23
2.8 Les outils utilisés.....24
2.9 Origines des problèmes de sûreté de fonctionnement.....26
2.10 Les données de fiabilité.....27
2.10.1 Les recueils.....27
2.10.2 Le retour d'expérience 28
2.11 La normalisation.....28
2.11.1 ARP-4754.....28
2.11.2 ARP-4761.....28
2.11.3 CEI-61508 et ses dérivées 28
2.12 Conclusion 29

Chapitre 3 Approche de modélisation

3.1 Introduction 30
3.2 Définition des systèmes dynamiques hybrides 30
3.3 Principales classes de phénomènes hybrides 32
3.3.1 Systèmes dynamiques hybrides à commutation autonome "Switching" 32
3.3.2 Systèmes dynamiques hybrides à commutation contrôlée.....34
3.5 Modélisation des systèmes hybrides 35
3.5.1 L'approche continue 35
3.5.2 L'approche évènementielle 35
3.5.3 L'approche mixte 35
3.6 Les automates à états fini 36
3.7 Les automates hybrides.....37
3.7.1 Définition informelle 37
3.7.2 Définition formelle 38

3.8 Simulation d'un système hybride 42
3.9 Les réseaux de Petri 43
3.9.1 Rappel sur les réseaux de Petri 43
3.9.2 Réseaux de Petri t-temporels 43
3.9.3 Réseaux de Petri de haut niveau 43
3.9.4 Les Réseaux de Petri Prédicats-Tansitions Différentiels 44
3.9.5 Les Réseaux de Petri Predicats-Transitions Différentiels et Stochastiques 47
3.10 Relation entre les réseaux de Petri et l'Arbre de défaillance 47
3.11 Conclusion 49

Chapitre 4 Définition de scénario minimal par la notion de coupe minimale

4.1 Introduction 50
4.2 Réseau de Petri et logique linéaire 50
4.2.1 Traductions dans le fragment MILL 51
4.2.1.1 Traduction des marquages 51
4.2.1.2 Traduction des transitions 52
4.2.2 Traduction de l'accessibilité 52
4.3 Preuve d'un séquent 53
4.3.1 Introduction des règles du fragment MILL 53
4.3.2 Calcul des séquents 54
4.3.3 Arbre de preuve canonique 54
4.3.3.1 Étape initiale 55
4.3.3.2 Étape itérative 55
4.3.3.3 Étape finale 56
4.4 Raisonnement avant 57
4.5 Raisonnement arrière 58
4.6 Notion de scénario 59
4.6.1 Evénements et ensembles d'événements 59
4.6.2 Définition d'un scénario 61
4.6.2.1 Cas des réseaux de Petri ordinaires 61
4.6.2.2 Cas des réseaux de Petri temporels 62

4.7 Conditions suffisantes 63
4.7.1 Ensemble suffisant 64
4.7.2 Ensemble suffisant et équation caractéristique 64
4.7.3 Scénario suffisant 65
4.7.3.1 Cas des réseaux de Petri ordinaires 65
4.7.3.2 Cas des réseaux de Petri temporels 66
4.7.4 Ensemble nécessaire 66
4.8 Minimalité des scénarios 67
4.8.1 Propositions et idées fondamentales 67
4.8.1.1 Rappel sur la méthode des Arbres de Défaillances 67
4.8.1.2 Analyse qualitative de la méthode des arbres de défaillances 68
4.8.2 Raisonnement dans un contexte inconnu 70
4.8.3 Notion de scénario minimal sur les arbres de preuve de la logique linéaire 70
4.8.4 Un algorithme pour déterminé les scénarios redoutés minimaux 72
4.9 Méthode de recherche des scénarios redoutés minimaux 73
4.10 Conclusion 74

Chapitre 5 Approche hybride pour la génération des scénarios redoutés minimaux

5.1 Introduction 75
5.2 Système étudié 75
5.3 Analyse qualitative 77
5.3.1 Modélisation 77
5.3.2 Détermination des états normaux et des états cibles 78
5.3.3 Recherche des scénarios redoutés minimaux 78
5.3.3.1 Raisonnement arrière 79
5.3.3.2 Raisonnement avant 80
5.3.3.3 Discussions 83
5.3.4 Recherche des scénarios redoutés minimaux par simulation 83
5.4 Analyse quantitative 85
5.4.1 Modélisation et simulation par automate hybride 85

5.4.2 Algorithme de simulation de l'automate hybride sous Matlab 86
5.4.3 Construction de modèle automate minimal 87
5.4.4 Simulation du modèle hybride 89
5.4.4.1 Modélisation physique du système étudié.....89
5.4.4.2 Bloc Automate (bloc d'événements discrets) 89
5.4.4.3 Résultats et analyses.....92
5.4.4.3.1 Mode de fonctionnement normal où les électrovannes EV 1, EV 2 sont en bon état.....92
5.4.4.3.2 Mode de fonctionnement où EV 1 est bloquée en ouverture et EV 2 en bon état.....93
5.4.4.3.3 Mode de fonctionnement où EV 1 et EV 2 bloqués ouverts et EV 3 en bon état.....94
5.4.4.3.4 Cas de débordement du réservoir 1 et EV 3 hors service.....95
5.4.4.3.5 Cas où EV 1 et EV 2 bloquée en ouverture et EV 3 hors service 96
5.5 Conclusion.....97

***Conclusion générale*.....98**

***Bibliographie*.....100**

Annexe Les étapes de modélisation par le Stateflow

A.1 Modélisation des systèmes dynamiques hybrides par Stateflow.....108
A.2 Utilisation de Stateflow.....109
A.3 Mise en œuvre sur Matlab.....110
A.3.1 Composition d'un diagramme stateflow 110
A.3.2 Modélisation dans Stateflow 114
A.3.3 Exemple sous Stateflow 114

Tables des figures

Figure 1-1 : Système mécatronique 5
Figure 1-2 : Interactions entre systèmes et technologies.....6
Figure 1-3 : Exemple de l'aspect hybride (continu et discret) 7
Figure 1-4 : Exemple des systèmes mécatroniques.....8
Figure 1-5 : Processus de développement d'un système mécatronique.....10
Figure 1-6 : Cycle en V.....11
Figure 1-7 : Cycle de vie et fiabilité 13

Figure 2-1 : Quelques indicateurs 20
Figure 2-2 : Études de la sûreté de fonctionnement d'un système.....22
Figure 2-3 : Analyse de la sûreté de fonctionnement.....23
Figure 2-4 : Relation entre la défaillance et l'état d'un système.....24
Figure 2-5 : Sûreté de Fonctionnement et démarche de conception 27
Figure 2-6 : Norme CEI-61508 et ses dérivées.....29

Figure 3-1 : Comportement des systèmes hybrides 31
Figure 3-2 : Commutation autonome 33
Figure 3-3 : (a)Trajectoire d'une boule de billard et (b) Automate associé.....33
Figure 3-4 : Système hybride à commutation contrôlée 34
Figure 3-5 : Système d'embrayage mécanique 34
Figure 3-6 : Structure mixte d'un système hybride : interaction du continu et du discret.....36
Figure 3-7 : Schéma illustratif d'un automate hybride 37
Figure 3-8 : Schéma général d'un automate hybride 38
Figure 3-9 : Exemple de l'affectation lors du franchissement d'une transition.....38
Figure 3-10 : Modèle du thermostat.....40
Figure 3-11 : Trajectoire de la température.....41
Figure 3-12 : Automate hybride modélisant l'exemple du thermostat.....41
Figure 3-13 : Exemple de RdP PTD.....47

Tableau 3-1 : Modélisation des portes logiques de l'Arbre de Défaillance par leurs réseaux de Petri associés 48

Figure 4-1 : Exemple de réseau de Petri 51
Figure 4-2 : Exemple du modèle réseau de Petri 57
Figure 4-3 : Arbre de preuve du raisonnement arrière 58
Figure 4-4 : Réseau de Petri inversé 58
Figure 4-5 : Arbre de preuve du raisonnement arrière 59
Figure 4-6 : Modèle réseau de Petri 60
Figure 4-7 : Graphe de précédence 62
Figure 4-8 : Exemple de réseau de Petri temporel 63
Figure 4-9 : Scénario généré à partir du réseau de Petri temporel de la figure 4.8 63
Figure 4-10 : Exemple de boucle élémentaire 65
Figure 4-11 : Graphe de précédence du séquent M_0, t_1,t_1,t_2,t_3 ├ M_f 66
Figure 4-12 : Structure de l'arbre de défaillance du système de régulation 68
Figure 4-13: Réduction booléenne de l'Arbre de Défaillance 69
Figure 4-14 : Exemple du modèle RdP pour la notion de coupe minimal 71
Figure 4-15 : Notion de la minimalité sur l'arbre de preuve dans un contexte inconnu 71

Figure 5-1 : Système de régulation des réservoirs 76
Figure 5-2 : Modèle complet du cas d'étude par les RdPPTDS 78
Figure 5-3 : Arbre de preuve du raisonnement arrière 79
Figure 5-4 : Fragment 1 de l'arbre 2 80
Figure 5-5 : Fragment 2 de l'arbre 2 81
Figure 5-6 : Arbre 3 82
Figure 5-7 : Structure du couplage de la plate forme PEMEDIT et le logiciel MATLAB pour la génération des scénarios redoutés minimaux 84
Figure 5-8 : Résultat de simulation sous FSPEMEDIT 84
Figure 5-9 : Matlab / Simulink / Stateflow 85
Figure 5-10 : Le schéma interne du bloc physique du système dans Simulink 89
Figure 5-11 : Structure générale de l'automate hybride du système étudié 90
Figure 5-12 : Schéma interne de l'automate hybride 90

Figure 5-13 : Schéma de simulation globale du système étudié 91
Figure 5-14 : Simulation des volumes V_1, V_2 et V_3, cas de fonctionnement normal 92
Figure 5-15 : Évolution des modes, cas de fonctionnement normal 92
Figure 5-16 : Évolution du volume, cas où l'électrovanne 1 est bloquée en ouverture et l'électrovanne 2, 3 sont en bon état 93
Figure 5-17 : Évolution des modes, cas où l'électrovanne 1 est bloquée en ouverture et l'électrovanne 2, 3 sont en bon état 93
Figure 5-18 : Évolution du volume, cas où EV 1 et EV 2 bloquées ouverts et EV 3 en bon état...94
Figure 5-19 : Évolution des modes, cas où EV 1 et EV 2 bloquées ouverts et EV 3 en bon état....94
Figure 5-20 : Évolution du volume, pour le cas de débordement du réservoir 1 et EV3 hors service…95
Figure 5-21 : Évolution des modes, pour le cas de débordement du réservoir1 et EV3 hors service…95
Figure 5-22 : Évolution du volume dans les trois réservoirs, cas où EV 1 et EV 2 bloquée en ouverture et EV 3 hors service 96
Figure 5-23: Évolution des modes, cas défaillant 96

Figure A-1: Bloc chart / Stateflow 109
Figure A-2 : Modélisation dans Stateflow 114

Introduction générale

La mécatronique est la combinaison synergique et systémique de la mécanique, de l'électronique et de l'informatique. L'intérêt de ce domaine d'ingénierie interdisciplinaire est de concevoir des systèmes automatiques puissants et de permettre le contrôle de systèmes hybrides complexes. La part grandissante de l'électronique et de l'informatique n'est pas sans conséquences sur les méthodes de conception. La complexité croissante des systèmes mécatroniques nécessite une adaptation des processus, méthodes et outils existants par rapport aux spécificités de ces systèmes pour mieux répondre aux exigences, notamment celles liées à la sûreté de fonctionnement. En effet, la préoccupation des industriels est de proposer à leurs clients des produits intégrant les nouvelles innovations technologiques avec une qualité et des performances de plus en plus améliorées mais aussi des produits de plus en plus sûrs. La criticité de ces systèmes nécessite de garantir un niveau de fiabilité et de sécurité convenable. De ce fait, des études de sûreté de fonctionnement doivent être menées tout au long du cycle de développement du système pour permettre une meilleure maîtrise des risques et de la fiabilité. Il doit répondre à des impératifs de criticité, de réactivité, d'autonomie, de robustesse et de fiabilité.

Les méthodes classiques de la sûreté de fonctionnement atteignent vite leurs limites face à la complexité de ces systèmes. Les méthodes combinatoires (arbres de défaillance, arbres d'événements, diagrammes de fiabilité) permettent uniquement d'identifier et d'évaluer les combinaisons des événements menant à l'occurrence d'une catastrophe. Elles ne tiennent pas compte de l'ordre d'occurrence des événements qui les composent. Ceci exclut toute possibilité de prendre en compte la dépendance et les délais entre événements. Pour résoudre le problème de la rareté de ces scénarios auquel sont exposées les méthodes basées sur la simulation, des techniques d'accélération de la simulation ont été développées et largement utilisées, avec succès dans l'ingénierie nucléaire notamment. Les méthodes d'analyse de modèles à événement discrets (automates, réseau de Petri) ont leur contribution dans ce domaine mais l'utilisation de graphe d'accessibilité est vite confrontée au problème de l'explosion combinatoire.

Un moyen d'évaluer la sûreté de fonctionnement des systèmes mécatroniques est la recherche des scénarios redoutés menant à un état catastrophe. L'analyse qualitative visant la mise en évidence des scénarios critiques est confrontée au problème de l'explosion combinatoire du nombre d'états du graphe d'accessibilité à cause de la rareté de ces scénarios. Afin de contourner ce problème, le modèle réseau de Petri semble bien adapté pour extraire les scénarios redoutés sans générer le graphe d'accessibilité associé; l'approche s'appuie sur la logique linéaire comme cadre formel.

Pour représenter les modèles réseaux de Petri et en extraire des scénarios, l'approche de la logique linéaire est adoptée. L'avantage de cette approche est de permettre la construction d'un ordre partiel de franchissement de transitions et focalise la recherche sur les parties intéressantes du modèle pour

l'analyse de la sûreté de fonctionnement. Cette approche est basée sur l'équivalence entre l'accessibilité dans les réseaux de Petri et la prouvabilité du séquent associé en logique linéaire. En effet, grâce à la logique linéaire, il est possible d'extraire les scénarios menant vers un état critique sans avoir à explorer tout le système.

La présence d'une dynamique continue liée à la partie énergétique et d'une dynamique événementielle liée à la commande, aux défaillances et reconfiguration donnent aux systèmes mécatroniques un caractère hybride. Un des problèmes principaux rencontrés lors d'une étude de sûreté de fonctionnement de ces systèmes est la prise en compte de manière efficace l'aspect continu et discret du système. Pour prendre en compte la nature hybride de la dynamique des systèmes mécatroniques, le choix du modèle s'est porté sur les réseaux de Petri associés aux équations différentielles. Le modèle réseau de Petri décrit le fonctionnement nominal, les défaillances et les mécanismes de reconfiguration. Les équations différentielles représentent l'évolution des variables continues de la partie énergétique du système. Pendant la phase de conception des systèmes mécatroniques, les scénarios redoutés sont inconnus du fait de la complexité inhérente à ces systèmes et à la multitude de modules en interaction. L'approche conduit à la génération des scénarios redoutés qui permettent au concepteur de comprendre les raisons de la dérive du système vers l'état critique. Il peut donc prévoir les reconfigurations nécessaires qui permettent d'éviter cet état. A partir d'une connaissance partielle de l'état critique ou redouté, il est possible de revenir en arrière à travers la chaîne des relations de cause à effet et d'extraire tous les scénarios possibles menant vers l'état critique. Chaque scénario est donné sous la forme d'un ordre partiel entre les évènements nécessaires à l'apparition de l'évènement redouté.

Objectif de la thèse

Le but est de développer une approche hybride pour l'étude de la sûreté de fonctionnement des systèmes mécatronique. Pour cela, à partir des travaux présentés précédemment [1], différentes approches ont été étudiées. L'approche retenue pour l'analyse qualitative, est basée sur l'extraction des scénarios redoutés à partir du modèle réseau de Petri à l'aide de la logique linéaire. Les scénarios générés à partir de cette analyse ne sont pas minimaux, d'où le choix de poursuivre des recherches sur cette voie. Pour que les scénarios redoutés générés soient pertinents, ils doivent satisfaire certaines propriétés. La minimalité est une de ces propriétés. La notion de minimalité doit être alors définie dans le cadre des arbres de preuve de la logique linéaire du modèle réseaux de Petri. Une nouvelle notion qui est celle du raisonnement dans un contexte inconnu a été développée. Cette dernière permet de déterminer les scénarios redoutés minimaux, c'est-à-dire, sans entrelacement avec des comportements d'éléments non causalement impliqués dans l'accessibilité de l'état partiel redouté.

L'approche développée pour la recherche des scénarios minimaux est basés sur la notion de coupe minimale de la méthode des arbres de défaillance appliquée directement sur les arbres de preuve de la logique linéaire dans un contexte inconnue. Cette notion est intégrée dans l'algorithme de construction des arbres de preuves pour faciliter la génération des scénarios minimaux. Pour prendre en compte la dynamique continue et devant la limitation des approches classique de cette dynamique, il faut mettre en place une simulation hybride. La simulation hybride est basée sur les scénarios minimaux trouvés à partir de l'analyse qualitative. Ceci permettra d'effectuer une analyse quantitative par les automates hybrides et de réduire considérablement le modèle de la simulation des systèmes mécatronique sûrs de fonctionnement.

Plan de la thèse

La présentation de cette thèse s'articule autour de cinq chapitres.

Le premier chapitre traite des systèmes mécatroniques en présentant leurs contextes et problématiques. Les principales caractéristiques de ces systèmes ainsi que les difficultés liées à leur analyse sont passées en revue. L'objectif du travail en est clairement défini.

Le deuxième chapitre traite l'état de l'art de la sûreté de fonctionnement ainsi que les différentes notions inhérentes. Cette section permet d'exprimer l'origine des problèmes de la sûreté de fonctionnement des systèmes complexes.

Le troisième chapitre est consacré à une étude détaillée des systèmes dynamiques hybrides. Cette étude comprend une large définition de ce type de systèmes, ainsi que la modélisation par les automates hybride qui permettent la prise en charge de l'aspect hybride des systèmes. Des exemples illustratifs sont présentés. On présentera aussi dans ce chapitre les différents formalismes de modélisation à base de réseaux de Petri. Les réseaux de Petri prédicats transitions différentiels stochastiques (RdP PTDS) ont été donc introduits. Ils permettent d'une part de prendre en compte l'aspect hybride des systèmes mécatroniques ainsi que l'aspect stochastique, nécessaire lors des analyses de sûreté de fonctionnement.

Dans le quatrième chapitre, une brève introduction à la logique linéaire ainsi que le rapprochement entre cette logique et les réseaux de Petri ont été présentées. Nous définirons aussi la notion de scénario, utile à l'analyse de la sûreté de fonctionnement des systèmes mécatroniques. La méthodologie pour la recherche des scénarios redoutés minimaux développée dans le cadre de ce travail s'articule autour de la mise en collaboration de deux approches : les arbres de preuve de la logique linéaire du modèle RdP et la notion de coupe minimale de la méthode des arbres de défaillances. Par ailleurs, les deux possibilités de raisonnement avant et arrière dans un contexte inconnu sont aussi présentées.

Le cinquième chapitre quant à lui, traite d'un exemple d'application permettant d'illustrer la méthodologie proposée. Après la présentation du système étudié, nous développons l'analyse qualitative pour l'étude de la sûreté de fonctionnement basée sur la méthodologie proposée. Une simulation du cas d'étude par l'outil graphique PEMEDIT dédié au formalisme réseau de Petri a permis de développer un outil MFSPEMEDIT (Minimal Feared State PEMEDIT), pour simplifier la générations des scénarios redouté minimaux.
Une modélisation par automate hybride est accomplie dans ce chapitre en vue d'une étude quantitative et simulée par l'outil Stateflow qui fonctionne en symbiose avec simulink. Ceci a permis la simulation et la visualisation du comportement réel et dynamique du modèle du système.

Une conclusion générale présentant les différents résultats et les perspectives offertes par ce travail clos la rédaction de cette thèse.

Chapitre 1

Systèmes Mécatroniques : Contexte et Problématique

1.1 Introduction

L'association de différentes technologies, (mécanique, électronique, logiciel) sur un même système a donné naissance à la mécatronique. L'apparition des systèmes mécatroniques est une révolution pour le monde industriel, qui affecte de plus en plus le monde du transport et en particulier le secteur automobile. L'utilisation de ces systèmes se généralise rapidement et influence maintenant tous les secteurs de l'industrie. Ainsi, ce chapitre est dédié à l'état de l'art des systèmes mécatroniques et à la présentation des différents domaines d'application.

1.2 Les systèmes mécatroniques

1.2.1 Contexte historique

Avant de donner les nombreuses définitions et de résumer certaines notions, il est bon de rappeler l'historique des évolutions industrielles ou autres qui ont amené à préciser ces notions. Avant les années 1950, les machines sont des ensembles électromécaniques. Dans les années 50, on assiste à l'apparition des semi-conducteurs, l'électronique est née. Dans les années 60-70, l'apparition de calculateurs fiables permet le contrôle des machines par logiciel. Une étude concernant les innovations technologique publiée en 2002, déclare que sur 100 projets innovants en mécanique, la majorité sont à l'interface de la mécanique et de l'électronique [2].
La mécatronique se définit alors comme la combinaison synergique et systémique de la mécanique, de l'électronique et de l'informatique. L'intérêt de ce domaine d'ingénierie multidisciplinaire est de concevoir des systèmes complexes et de permettre leur contrôle. Le terme *mechatronics* a été introduit pour la première fois par un ingénieur de la compagnie japonaise «YASKAWA» en 1969, pour désigner le contrôle des moteurs électriques par ordinateur [3]. Ce terme a par la suite évolué, pour apparaitre officiellement dans le Larousse en 2005.
Plusieurs définitions sont données pour définir les systèmes mécatroniques. Isermann [4] résume les définitions données à la mécatronique dont « La mécatronique est l'intégration synergique de l'ingénierie mécanique avec l'électronique et le contrôle intelligent de calculateurs dans la conception et la fabrication de produits et processus industriels ». Il estime que toutes les définitions sont d'accord pour dire que la mécatronique est un domaine interdisciplinaire dans lequel les disciplines suivantes agissent ensemble :

- Systèmes mécaniques (éléments mécaniques, machines, mécanique de précision).
- Systèmes électroniques (micro-électronique, électronique de puissance, capteurs et actionneurs).
- Technologie de l'information (théorie des systèmes, automatisation, génie logiciel, intelligence artificielle).

La norme NF E 01-010 [5], définit la mécatronique comme une « démarche visant l'intégration en synergie de la mécanique, l'électronique, l'automatique et l'informatique dans la conception et la fabrication d'un produit en vue d'augmenter et/ou d'optimiser sa fonctionnalité ».
La mécatronique n'est pas intrinsèquement une science ou une technologie, elle doit être considérée comme une attitude, une manière fondamentale de regarder et de faire des choses et exige, par sa nature une approche unifiée [6].

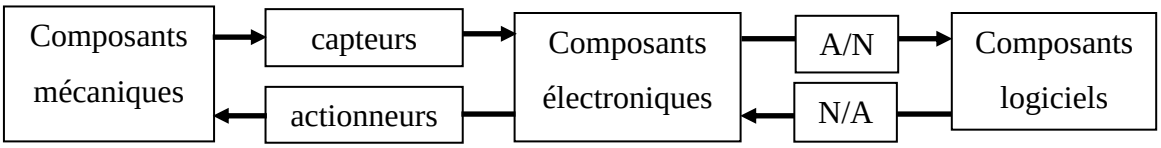


Figure 1-1 : Système mécatronique [6].

Le Système Mécatronique (SM) de la figure 1-1 intègre de la mécanique, de l'électronique et du logiciel, mais également des systèmes hydrauliques, pneumatiques et des systèmes thermiques. Cet exemple montre qu'il est important que le système soit conçu comme un ensemble autant que possible. La synergie induite par les systèmes mécatroniques conduit à une combinaison intelligente de technologies [7], [8], [9]. Elle mène alors à des solutions et à des performances supérieures, qui ne pourraient pas être obtenues par des applications séparées [10].

L'avènement des systèmes mécatroniques dans l'industrie, en particulier dans l'industrie automobile, a entraîné de nouvelles contraintes [11], telles que :

- l'assimilation de plusieurs technologies;
- les interactions entre les différentes entités fonctionnelles;
- la prise en compte de la dynamique du système (le fonctionnement en temps réel, événementiel et l'intégration des nombreux états possibles);
- l'impossibilité de réaliser des tests exhaustifs.

Malgré ces contraintes, la mécatronique apporte des avantages indéniables comme la baisse des coûts, la satisfaction client par les solutions innovantes proposées, la réponse positive à des exigences sociétales de plus en plus importantes - pollution, consommation, sécurité des passagers et piétons [12].
En conclusion, *Un système mécatronique est un système complexe pluridisciplinaire à dominante mécanique et électronique avec contraintes temps réel* [2].
Il est complexe car il est composé d'un grand nombre d'entités en interaction locale et simultanée où il y a des boucles de rétroaction. L'état d'une entité a une influence sur son état futur via l'état

d'autres entités. De plus, c'est un système ouvert et soumis à un extérieur, par le biais des flux d'énergie et d'information sur la frontière.
Il est pluridisciplinaire car plusieurs domaines technologiques sont mis en œuvre pour les parties commande et opérative. Il est composé d'éléments de différents domaines : mécaniques, électroniques ainsi que des technologies de l'information comme c'est indiqué dans la figure 1-2. Finalement la mécatronique est une symbiose de ces différentes disciplines au service de la conception de produits intégrés.

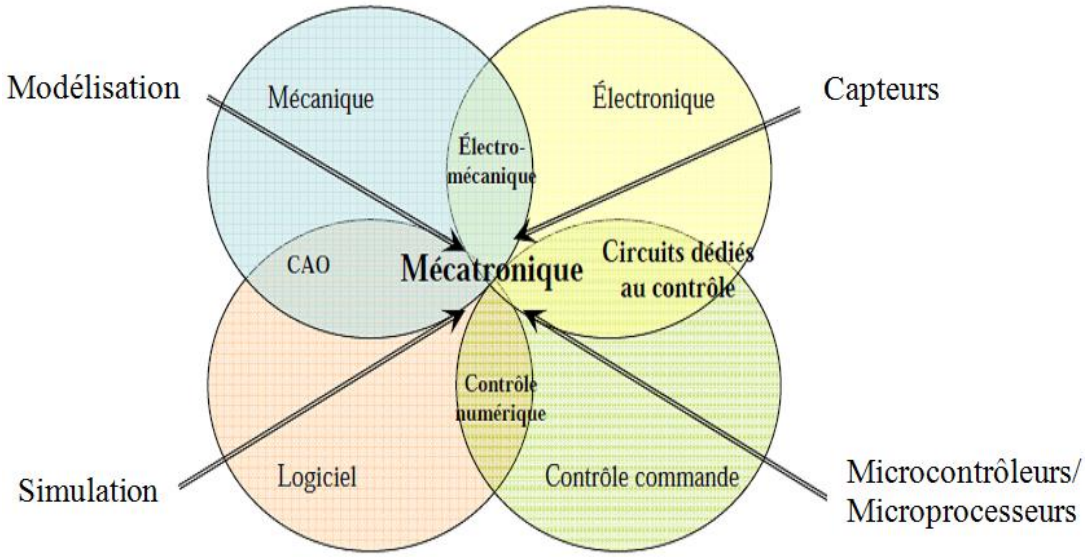


Figure 1- 2 : Interactions entre systèmes et technologies.

Il est à contraintes temps réel car il est le plus souvent immergé dans son environnement et doit permettre une automatisation d'un ensemble de tâches. Le respect des contraintes temporelles dans l'exécution des tâches est aussi important que le résultat de ces tâches pour permettre aux clients de ces derniers de les exploiter correctement [13], [14].

1.2.2 Exemple de systèmes mécatroniques

L'aspect hybride d'un système mécatronique est caractérisé par la présence de phénomènes continus et d'événements discrets.

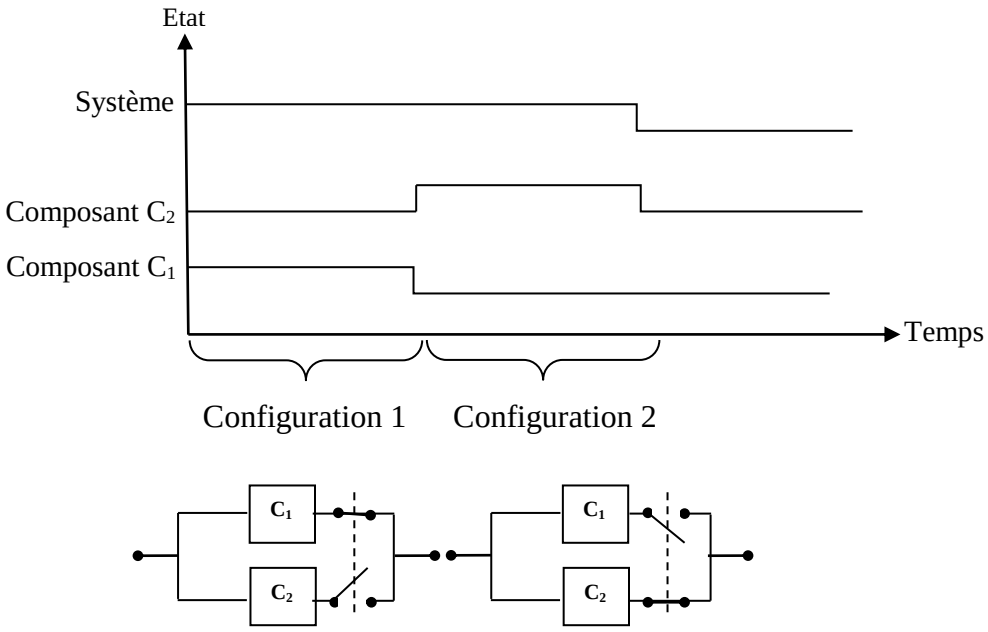


Figure 1-3 : Exemple de l'aspect hybride (continu et discret).

La description de ces systèmes mécatroniques peut faire intervenir explicitement et simultanément un état continu et un état discret tel qu'il est montre sur la figure 1-3. Le système fonctionne en continu alors que l'utilisation des composants C_1 et C_2 est discret. Ainsi, le fonctionnement d'un système comportant une redondance passive est assuré par le composant C_1 alors que le composant C_2 est au repos (pas d'usure de stockage). Lorsque le système détecte la défaillance de C_1, le composant C_2 est actionné pour assurer la continuité de fonctionnement. Sur cet exemple simple, nous mettons en évidence l'aspect hybride (continu = fonctionnement du système, discret = panne de C_1 et démarrage de C_2). On peut ajouter le fait que certaines variables peuvent présenter un caractère aléatoire tel que les défaillances des composants [14].
Par essence, la mécatronique est une conjugaison de technologies différentes, elle requiert pour son développement des équipes pluridisciplinaires avec des langages et des méthodes très différentes entre eux.

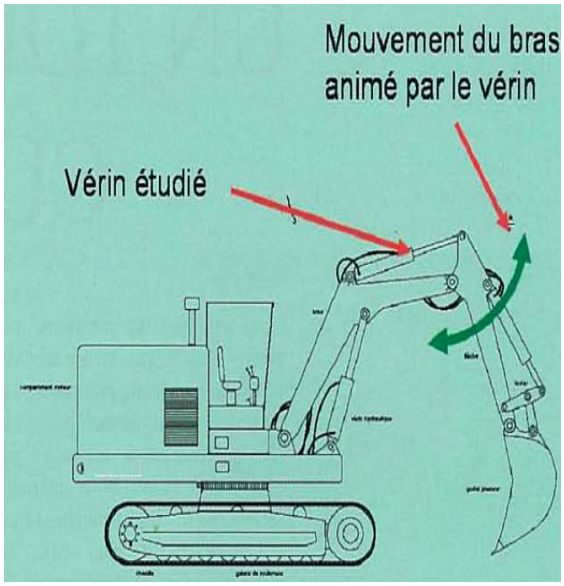
Comme exemples réels de systèmes mécatroniques [12], [15], [16], on peut citer les cas présentés sur le schéma de la figure 1- 4 :

- Véhicule automobile moderne : système anti-blocage (*ABS : Anti Blocking System*), programme de stabilité électronique (*ESP: Electronic Stability Program*), direction assistée, … etc ;
- Avion de chasse;
- Machine-outil à commande numérique;
- Disques durs;
- Les systèmes d'amortissement actif de vérin de pelle mécanique;
- Machines à laver « intelligentes »;
- Ferroviaire;
- ... etc.

Ferroviaire : bogies intelligents (suspension, inclinaison de caisse, essieu radiant, freinage…)

Aéronautique : commandes de vol et actionneur électriques…

Automobile : aides à la conduite, sécurité active, accessoires…



Système d'amortissement actif de vérin de pelle mécanique - parties hydraulique et électronique (*Conception d'une commande électronique pour piloter la vitesse de déplacement d'un vérin hydraulique et amortir ses arrêts en fin de course*).

Figure 1 – 4 : Exemple de systèmes mécatroniques.

Aujourd'hui, pour répondre aux enjeux qualité/coûts/délais imposés par le marché, une nouvelle approche de conception des systèmes est nécessaire pour permettre l'intégration des différentes technologies sûres de fonctionnement dès la première phase de développement. L'ingénierie concourante apparaît comme la méthodologie la plus adaptée au développement des systèmes mécatroniques [17], [18].

1.2.3 Ingénierie concourante

Dans un environnement industriel concurrentiel, la méthode traditionnelle qui consistait à enchaîner séquentiellement les métiers disciplinaires (mécanique, électronique, ...), de la conception, de la fabrication, de l'assemblage, de la distribution n'est plus adaptée.
En effet, ce processus séquentiel est trop coûteux du fait de la définition sectorielle et séquentielle des paramètres inhérents à chaque métier et entraîne, de plus, des délais importants dans la réalisation. La séquentialité des activités programmées et correctrices entraîne également une mauvaise localisation temporelle de certaines décisions.
Face aux enjeux économiques actuels, il devient essentiel de développer des passerelles visant à rendre interopérables les outils et les métiers, propres à chaque discipline, de manière à réduire les temps de développement, donc les coûts, et de rendre l'entreprise plus réactive dans un contexte concurrentiel [19].
D'une manière générale, la nouvelle stratégie de décision nécessite une parallélisation d'un certain nombre d'activités de conception appelé ingénierie concourante.
L'ingénierie concourante est une approche globale multi-métiers, qui consiste à engager en parallèle les activités et les tâches, les services et les métiers nécessaires au développement du système [18], [19]. Elle permet d'optimiser la démarche de conception de projets collaboratifs, et d'assurer la meilleure coordination entre les parties prenantes du projet, ce qui représente un gain de qualité et de temps. Ainsi, l'enchaînement optimal des tâches assure le suivi du cheminement le plus court et permet d'anticiper les problèmes du fait du partage général de l'information entre les membres de l'équipe [20].
L'ingénierie concourante fait intervenir des éléments similaires à ceux des systèmes mécatroniques, tels que:

- le caractère temporel du processus de développement - cycle de développement (décomposition en phases: spécification, conception, fabrication, vérification, validation);
- l'aspect métier - différents corps de métiers interviennent dans le développement : les mécaniciens, les électroniciens, les automaticiens,... ;
- l'aspect multidisciplinaire - mécanique, électronique, logiciel,... ;
- le caractère systémique - système économique, système d'information, système de production, système de distribution.

Du fait de sa complexité, un système mécatronique ne peut pas être créé par une personne; par contre, il peut être conçu par un grand nombre de personnes avec différentes spécialisations à condition que ces personnes constituent une équipe [21], [22]. Nous observons donc une grande analogie entre l'ingénierie concourante et la conception des systèmes mécatroniques.
L'ingénierie concourante permet de faire face plus facilement et plus rapidement aux modifications dans le processus de développement du système. Ce processus fait intervenir des étapes qui s'enchaînent logiquement selon un cycle et qui sont bien adaptées au développement des systèmes mécatroniques.

Le processus de développement d'un système mécatronique [14], s'organise selon le schéma de la figure 1-5 :

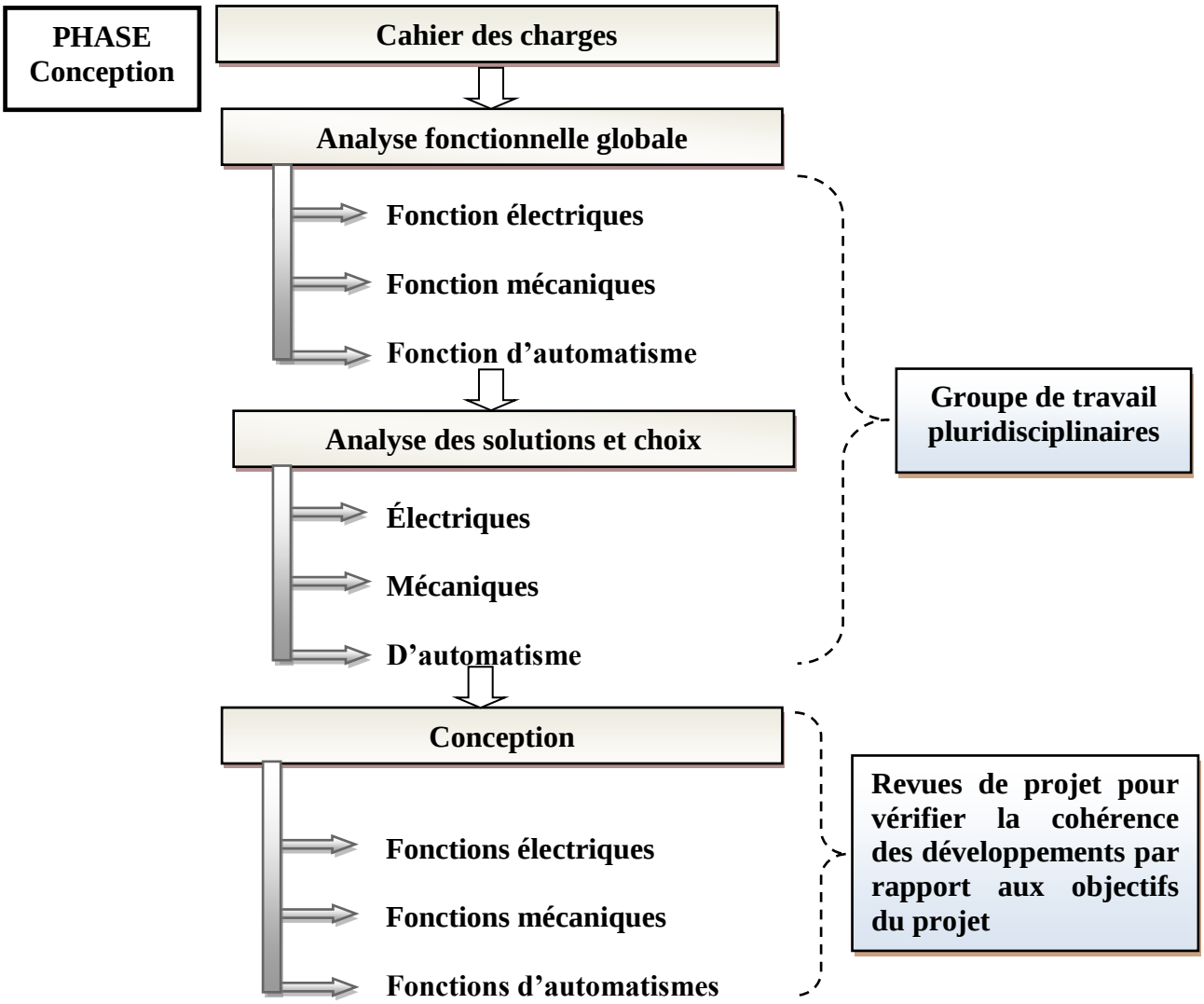


Figure 1-5 : Processus de développement d'un système mécatronique.

1.2.4 Cycle de développement

Les systèmes industriels complexes se caractérisent par le fait qu'ils résultent d'une combinaison de sous-systèmes de technologies différentes. Le cycle en V présenté par la figure 1-6 a d'abord été utilisé comme modèle de développement dans les différentes technologies : la mécanique, l'électronique ou le logiciel. Il a été ensuite généralisé au développement des systèmes complexes, en particulier des systèmes mécatroniques, afin d'avoir une terminologie commune et de proposer une méthodologie globale, avec des étapes communes aux différents technologies. Plusieurs auteurs ont montré l'intérêt du cycle en V [23], [24].
Il existe d'autres types de cycles de développement dont les plus connus sont les cycles en cascade ou en spirale [25]. Le modèle de développement selon le cycle en V positionne les différentes phases de développement, depuis la spécification jusqu'à la validation produit (figure 1- 6).

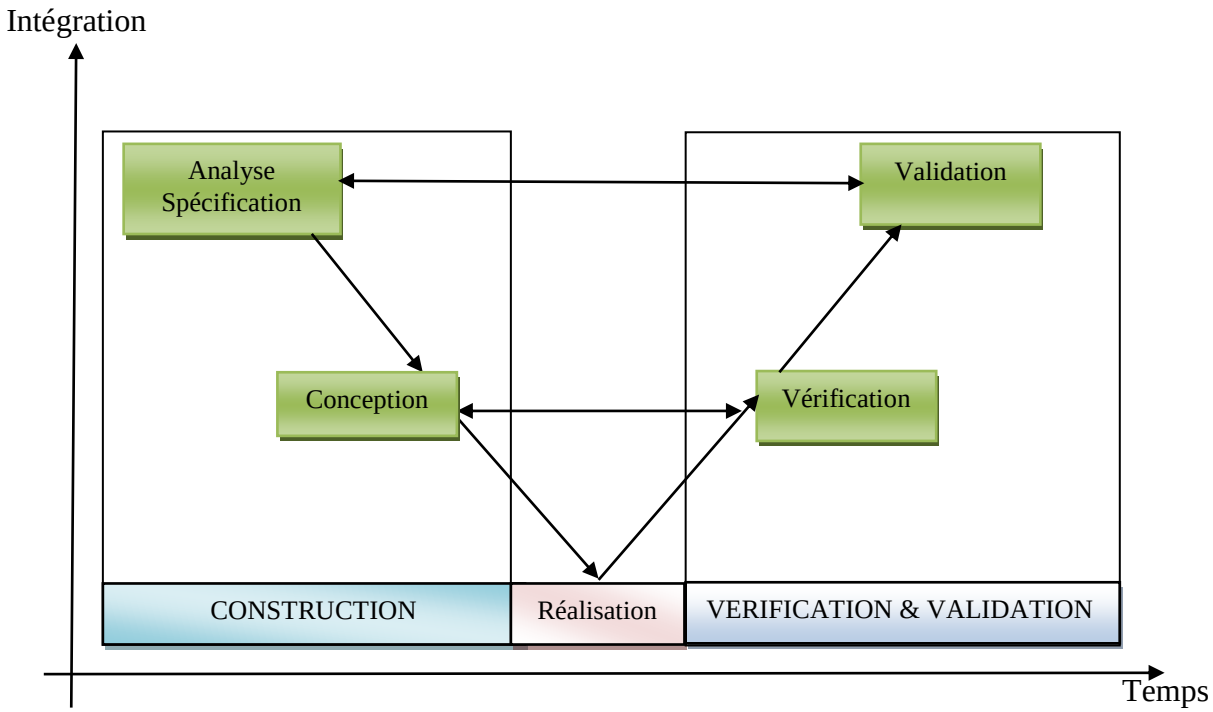


Figure 1-6 : Cycle en V.

Le cycle en V se caractérise par un axe horizontal représentant le temps et par un axe vertical représentant le niveau d'intégration du système. Le développement commence par le bloc de construction du système, la partie descendante du cycle en V, où le système est graduellement décomposé en ses divers sous-systèmes et modules jusqu'au niveau composant.
La partie montante du cycle en V comprend le bloc de Vérification & Validation (V & V) du système où les composants une fois réalisés sont intégrés dans des ensembles et des sous-systèmes graduellement plus grands, jusqu'à ce que le système complet soit construit.
Le cycle en V peut être décrit comme la succession des 5 phases: analyse/spécification, conception, réalisation, vérification et validation [25].

1.2.4.1. Analyse/Spécification

La première phase de développement d'un système consiste dans la réalisation de l'analyse des besoins et des spécifications. Cette phase propose la définition des fonctionnalités, des interfaces, des contraintes et des exigences du système, la préparation du plan qualité, du plan de validation, de l'étude de faisabilité, la définition du niveau de la fiabilité souhaité du système.
Pour un système mécatronique, la difficulté majeure est la traduction de la spécification système en spécifications particulières pour chaque composant selon les différentes technologies.

1.2.4.2 Conception

Suite à l'analyse/spécification, la deuxième phase de développement d'un système est la conception, qui débute par la définition de l'architecture du système, puis des sous systèmes et de leur fonctionnement, du plan de tests et d'essais et de l'analyse des risques.

Dans le cas des systèmes mécatroniques, une simulation du futur système englobant toutes les technologies est effectuée. La complexité du système, l'interprétation des spécifications par les différentes équipes, sont des points sensibles à prendre particulièrement en considération dans la phase de conception.

1.2.4.3 Réalisation

Cette phase de développement consiste à passer du résultat de la conception à un ensemble d'activités d'industrialisation permettant la fabrication et l'assemblage des composants. Même si techniquement les spécifications des composants pour le système mécatronique sont précises, un fournisseur ou un fabricant des composants est toujours susceptible d'interpréter les spécifications légèrement différemment et, en conséquence, de livrer des composants qui ne sont pas conformes aux spécifications.

1.2.4.4 Vérification

Dans cette phase, tous les modules ou sous-systèmes sont vérifiés, testés par rapport à la conception. La vérification est complémentaire avec l'assemblage des modules et des sous-systèmes jusqu'au système final. Dans cette phase, il est difficile de tester la synchronisation des différents modules ou sous-systèmes du système mécatronique. De plus, des ambiguïtés par rapport à la conception peuvent accroître cette difficulté de synchronisation. En même temps, il est extrêmement difficile de détecter des changements de conception (modules ou sous systèmes non conformes à la conception) tant que le système mécatronique n'est pas entièrement construit pour exécuter des essais avec le système complet.

1.2.4.5 Validation

La deuxième phase de V&V est la validation du système final. Il s'agit d'une validation fonctionnelle, une phase importante, où sont constatés les fonctionnalités et le niveau de qualité par rapport aux spécification/analyse de besoins.
Pour un système mécatronique, la validation est un point sensible dû à la combinaison, à la synchronisation et à l'interaction des différentes technologies. Ces contraintes rendent plus difficiles le diagnostic et l'entretien du système mécatronique.
Lors du développement d'un système, le constructeur spécifie non seulement les fonctionnalités, mais aussi les objectifs à atteindre en termes de sûreté de fonctionnement.
Ainsi, il est de plus en plus nécessaire d'intégrer la sûreté de fonctionnement dans l'approche système, très en amont dans les projets, dès la première phase du cycle de développement. Cette intégration conduit non seulement à démultiplier les études de fiabilité, de disponibilité, de maintenabilité et de sécurité, mais aussi à mettre en place une méthodologie transversale qui favorise leur prise en compte dans les projets et à travers les différents métiers liés au développement du système mécatronique. La spécification des objectifs de sûreté de fonctionnement est accompagnée d'une procédure de validation pour vérifier que ces objectifs ont été atteints. Tout au long du développement du système mécatronique, des méthodes et des techniques spécifiques de la sûreté de fonctionnement devront être appliquées pour atteindre les objectifs exigés.

1.3 La mécatronique au centre des préoccupations

L'ingénierie de tels systèmes nécessite la conception simultanée et pluridisciplinaire de trois sous-systèmes : la partie opérative (squelette et muscle du système à dominantes mécanique et électromécanique), la commande (intelligence embarquée du système à dominante électronique et informatique en temps réel), et l'interface entre l'homme et la machine à dominantes ergonomique et esthétique.
Cette approche systémique permet d'obtenir des performances supérieures aux solutions traditionnelles, de réaliser de nouvelles fonctionnalités, de réduire le nombre de composants critiques et de valider la sûreté de fonctionnement du système, mais aussi d'abaisser les coûts, de rendre les produits mécatroniques plus compacts, voire miniaturisés avec le développement des mems (**m**icro**e**lectro**m**echanical **s**ystems), ces systèmes micro-électro-mécaniques à l'échelle du micron, d'ores et déjà présents dans nombre d'appareils électroniques de la vie quotidienne [12], [20], [26], [27].

1.4 Les systèmes mécatroniques et systèmes hybrides

Les systèmes mécatroniques sont de plus en plus complexes et intègrent des quantités croissantes de composants élémentaires. Cette évolution n'aurait pas été possible sans une amélioration considérable de la fiabilité des composants élémentaires et des équipements [26]. Par contre, la testabilité des puces et des cartes électroniques devient de plus en plus difficile à assurer même lorsqu'elle a été prévue dès la conception : un dispositif qui fonctionne initialement fonctionnera longtemps mais il est difficile de savoir s'il ne présente aucun défaut en sortie de fabrication [27]. Les composants électroniques ne sont pas réparables mais leur remplacement permet la remise en service des cartes défectueuses. Une bonne maintenabilité engendre une forte disponibilité pour les systèmes réparables [28], [29].
Toutes ces exigences doivent être prises en compte au cours du cycle de vie : conception, fabrication, utilisation. La prévision de la fiabilité et l'analyse des pannes encadrent la réalisation d'un produit, ce qui est décrit sur le schéma de la Figure 1-7.

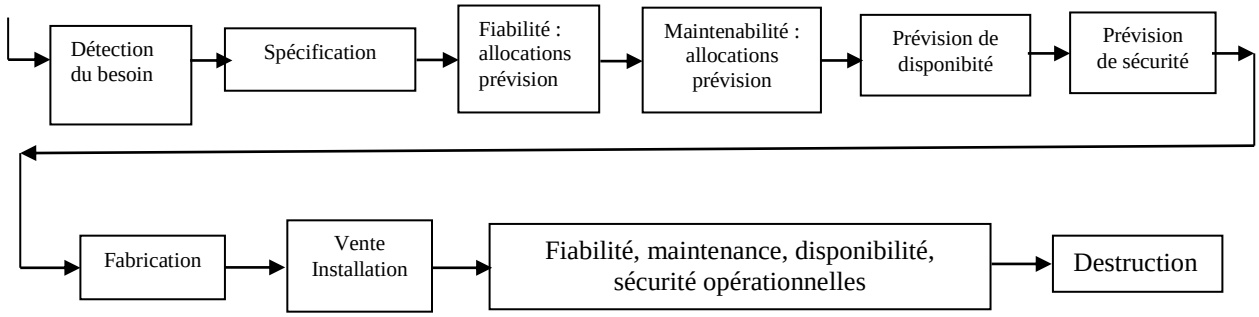


Figure 1-7 : Cycle de vie et fiabilité.

Les problèmes de coût limitent l'amélioration de la fiabilité et de la maintenance et conduisent à la recherche de solutions optimales [30].

Les définitions et les procédures relatives à ces domaines de la fiabilité, maintenabilité, disponibilité (FMD) sont normalisées [31], [32]. Par :

- l'AFNOR (Association Française de NORmalisation);
- l'UTE (Union Technique de l'Electricité);
- le CENELEC (Comité Européen de Normalisation de l'ELECtrotechnique);
- les références militaires MILHDBK (MILitary HanDBooK);
- l'IEC (International Electrotechnics Committee) ou CEI.

1.5 Conclusion

Les systèmes mécatroniques sont de plus en plus utilisés dans l'industrie. Tous les secteurs sont concernés: l'automobile, l'aéronautique, le nucléaire, le spatial et même des domaines comme le bancaire ou le médical. Le développement d'un système mécatronique est envisagé selon l'approche de l'ingénierie concourante dans le cadre d'un cycle de développement, est une démarche méthodologique pour maîtriser la conception des systèmes et produits complexes.
La complexité importante de systèmes mécatroniques et la réduction des coûts de conception et d'exploitation incitent les industriels à maîtriser davantage la sûreté de fonctionnement, ce qui fera l'objet du chapitre suivant.

Chapitre 2

La Sûreté de Fonctionnement : historique et analyse

2.1 Introduction

Les préoccupations dites de sécurité sont très présentes dans le monde des machines outils ou dans les procédés continus comme la pétrochimie. Dans les applications de type manufacturier, les préoccupations sont plutôt liées à la disponibilité. Dès lors que la sécurité ou la disponibilité d'un système est mise en défaut, on incrimine sa fiabilité. Enfin, en cas de dysfonctionnement, il convient de remettre le système en conditions de fonctionnement initial; c'est là qu'intervient la maintenabilité. Ces quatre caractéristiques constituent la sûreté de fonctionnement d'un dispositif, ce à quoi s'attache l'essentiel de ce chapitre, en passant en revue les composantes fondamentales. Par ailleurs quelques événements ou dates clefs permettent de fixer l'évolution chronologique de la sûreté de fonctionnement.

2.2 Historique de la sûreté de fonctionnement

Les problèmes de Sûreté de Fonctionnement (SdF) existent depuis très longtemps, dès qu'un système a pu défaillir ou tomber en panne [33], [34].

A partir des années 1930, les taux de défaillance, utilisés pour comparer des événements passés, sont exploités pour faire des prévisions sur des événements à venir : la théorie de la fiabilité est née [35].

Puis dans les années 1940, des techniques de fiabilité commencèrent à se développer, avec notamment la conception des moteurs de traction des locomotives aux États-Unis [36].
Dans les années 1950, le concept de maintenance fait son apparition [37]. On assiste également aux toutes premières études sur la fiabilité humaine pour les nouvelles centrales nucléaires. A la même époque, des travaux de recueil de données de fiabilité électronique sont entamés.

Dans les années 1960, H. A. Watson des laboratoires Bell [38] met au point la méthode dite des arbres de défauts; grâce à elle, il devient possible de décrire les aléas du fonctionnement de systèmes complexes.

En 1962, l'Académie des Sciences accueille le mot « fiabilité » dans sa terminologie.

A partir de 1970, les premiers travaux sur la fiabilité des logiciels [39] commencent et de nombreuses études sont menées dans le domaine du nucléaire. Nous pouvons citer, par exemple, le rapport américain Rasmussen [40] sur les risques nucléaires. En 1979, la catastrophe nucléaire de Three Miles Island [41] motive encore plus le développement d'outils de sûreté de fonctionnement.

La décennie 80 voit l'approfondissement dans plusieurs directions :

- collecte de données de fiabilité,
- mise au point de nouvelles méthodes d'analyse de la fiabilité, et de la disponibilité, des systèmes (par exemple les réseaux de Pétri),
- méthodes de prise en compte de facteur humain (méthode HCR : "Human Cognitive Response technique", méthode HEART: "Human Error Assessment and Reduction Technique", ...etc).

Puis, progressivement, les techniques de sûreté de fonctionnement vont largement se diffuser et s'étendre à de plus en plus de domaines : la chimie, le ferroviaire, l'automobile, le traitement et l'épuration de l'eau, et l'ensemble des grands secteurs industriels.

Aujourd'hui, des réglementations et des certifications imposent l'utilisation d'outils dédiés à la sûreté de fonctionnement. Parallèlement, la compétitivité croissante force les entreprises à adopter la productivité la meilleure possible, et donc réduisent au maximum les arrêts de production et maximisent la disponibilité de leurs équipements.

Nous allons définir progressivement ces concepts pour mieux cerner la notion générique de la sûreté de fonctionnement.

2.3 Concepts et définitions

Un des grands mérites du concept de sûreté de fonctionnement est l'intégration des méthodes et techniques destinées à garantir l'aptitude d'un système à délivrer un service dans lequel on puisse avoir confiance et à s'assurer que cette confiance est justifiée.

La sureté de fonctionnement est définie par Villemeur [42] comme la science des défaillances. Au sens plus strict, la sureté de fonctionnement est l'aptitude d'une entité à assumer une ou plusieurs fonctions requises dans des conditions données [43], [44].

Selon Laprie [45] la sûreté de fonctionnement d'un système est la propriété qui permet à ses utilisateurs de placer une confiance justifiée dans le service qu'il leur délivre. Cette notion de confiance est fondamentale, étant donné que tout système matériel/logiciel contient des erreurs, la grande majorité d'entre elles étant des erreurs introduites lors des phases de conception. Son objectif est alors de spécifier, concevoir réaliser et exploiter des systèmes où la faute est naturelle, prévue et

tolérable. Une définition alternative donnée par Laprie [45] de la sûreté de fonctionnement est l'aptitude à éviter des défaillances du service délivré plus fréquentes ou plus graves qu'acceptable.

Au sens de la norme CEI 50 (191) [43], la sûreté de fonctionnement recouvre les concepts de fiabilité, maintenabilité et disponibilité (ou FMD). L'équivalent Anglo-Saxons est le terme dependability, (reliability, maintainability, availability) souvent désigné par l'acronyme RAM. La sécurité est souvent traitée à part. Cependant, l'acronyme RAMS (FMDS en français) est utilisé pour désigner l'ensemble des activités liées à ces quatre concepts.

2.3.1 Fiabilité

Dès que les hommes ont inventé les premiers instruments, ils sont devenus dépendants de leur bon fonctionnement. Dans ce sens, le concept de fiabilité était né. Avec l'entrée de l'électronique la fiabilité est entrée dans une nouvelle ère. Cependant, la fiabilité comme un sujet d'étude systématique a débuté dans les années soixante [25].
La fiabilité est un concept populaire qui a été utilisé pendant des années comme un attribut louable d'une personne ou d'un objet façonné. En anglais « reliability » vient de «to rely on » signifiant «compter sur, avoir confiance en… ». Alors que la fiabilité en français vient effectivement du mot «fiable», c'est-à-dire en qui on peut se fier [25].

En 1962, l'Académie de Sciences, l'a définie de la façon suivante : Grandeur caractérisant la sécurité du fonctionnement, ou mesure de la probabilité de fonctionnement d'un appareillage selon les normes prescrites. Plus tard, dans les années soixante dix, le Comité Électrotechnique International propose la définition suivante : Caractéristique d'un dispositif, exprimée par la fiabilité, qu'il accomplisse une fonction requise, dans des conditions données, pendant une durée donnée [46].

Laprie [45] définissent la fiabilité comme la mesure de la continuité de la délivrance d'un service correct ou de façon équivalente, mesure aussi du temps jusqu'à défaillance.

Villemeur [42] et la norme CEI 50 (191) [43] expriment que la fiabilité est l'aptitude d'une entité à accomplir une fonction requise dans des conditions données, pendant une durée donnée. Cette aptitude se mesure par la probabilité qu'une entité réalise une fonction requise dans des conditions données pendant une période de temps donnée [44]. La fiabilité peut être paraphrasée comme la probabilité de la non défaillance de l'entité dans un période de temps donnée.

A l'instant t, la fiabilité se mesure alors par la probabilité que l'entité E accomplisse une fonction requise dans les conditions données pendant l'intervalle de temps $[0; t]$ [43]. Ainsi,

$$R(t) = P[\text{E soit non défaillante sur } [0, t]] \qquad (2.1)$$

ou

$$R(t) = P[E \text{ soit non défaillante sur } [t_1, t_2]] \qquad (2.2)$$

L'aptitude contraire est la probabilité de défaillance de l'entité, quelquefois appelée défiabilité. On écrit :

$$\overline{R}(t)=1-R(t) \qquad (2.3)$$

L'évaluation de cette probabilité peut être faite différemment selon la nature des entités considérées ou selon les moyens dont on dispose pour le faire.

2.3.2 Disponibilité

C'est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données et à un instant donné [42].

La disponibilité est généralement mesurée par la probabilité qu'une entité *E* soit en état d'accomplir une fonction requise dans des conditions données à l'instant *t*.

$$A(t) = P\ [\ E \text{ non défaillante à l'instant } t\ ] \qquad (2.4)$$

Cette caractéristique est appelée disponibilité instantanée. L'aptitude contraire sera dénommée indisponibilité ; sa mesure est notée $\overline{A}(t)$:

$$\overline{A}(t)=1-A(t) \qquad (2.5)$$

La disponibilité ainsi définie ne fait pas appel à l'histoire de l'entité, qu'elle ait été ou non réparée une ou plusieurs fois avant l'instant *t* (c'est en quelque sorte une probabilité non conditionnelle). Il est donc évident que pour un système non réparable, la disponibilité est égale à la fiabilité et que d'une façon générale $A(t) \geq R(t)$. La disponibilité peut se décliner en termes de fiabilité et maintenabilité [47].

2.3.3 Maintenabilité

C'est l'aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits [42].

Elle est généralement mesurée par la probabilité que la maintenance d'une entité *E*, soit achevée au temps *t*, sachant que l'entité est défaillante au temps *t = 0*.
L'évaluation de cette probabilité est bien sûr liée à la manière dont est effectuée la remise en état de fonctionnement de l'entité.

$$M(t)= P\ [\ E \text{ est réparé sur } [\ 0, t\ ]\ ]. \qquad (2.6)$$

2.3.4 Sécurité

Bien que la norme CEI 50 (191) [43] n'intègre pas la sécurité comme composant de la sûreté de fonctionnement, nous considérons qu'il est important de la prendre en compte car l'occurrence d'un événement catastrophique met en péril la vie humaine.

En fait, le concept de sécurité est probablement le plus difficile à définir et à évaluer, car il englobe des aspects très divers. Cependant, la norme EN 292 – 1 [48] sur la sécurité des machines donne cette définition:

Aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue, démontée et mise au rebut dans les conditions d'utilisation normales spécifiées dans la notice d'instructions, sans causer de lésions ou d'atteinte à la santé.

La sécurité peut également s'exprimer sous forme d'une probabilité : probabilité que le système évite de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques [42]. Si on considère que les défaillances d'un système se partagent en deux catégories, celles qui sont dangereuses et celles qui ne le sont pas, la sécurité peut être considérée comme la part de la fiabilité relative aux défaillances dangereuses. Ce concept peut devenir prépondérant dans une analyse de sûreté de fonctionnement, dans la mesure où une défaillance du système peut présenter un risque de dommage corporel à l'encontre des usagers.

Les concepts de la sûreté de fonctionnement correspondent aux propriétés du système liées à la sûreté de fonctionnement. Ils permettent d'apprécier la qualité du système vis-à-vis des services délivrés.

Ces quatre concepts sont les attributs primaires. Il existe également des attributs secondaires, à savoir :

- robustesse : persistance de sûreté de fonctionnement en présence de fautes externes;
- survivabilité : persistance de la sûreté de fonctionnement en présence de fautes actives;
- résilience : persistance de la sûreté de fonctionnement en face de changements fonctionnels, environnementaux, technologiques;
- responsabilité : disponibilité et intégrité de la personne qui a effectué une opération;
- authenticité : intégrité du contenu et de l'origine d'un message, et éventuellement d'autres informations, comme l'instant d'émission;
- non-réfutabilité : disponibilité et intégrité de l'identité de l'émetteur d'un message (non-réfutation de l'origine), ou du destinataire (non-réfutation de la destination);
- confidentialité : absence de divulgations non-autorisées de l'information;
- intégrité : absence d'altérations inappropriées de l'information.

2.4 Quelques indicateurs

Certains indicateurs vont caractériser le fonctionnement prévu du système, tels que le MTTF, le MDT et le MUT.

- Le MTTF (Mean Time To [first] Failure) est la durée moyenne de fonctionnement avant défaillance, espérance mathématique de la durée de fonctionnement avant défaillance. La définition du MTTF est :

$$MTTF = \int_0^{\infty} R(t)\, dt \qquad (2.7)$$

- Le MDT est le temps moyen séparant la survenance d'une panne et la remise en état opérationnel du système. Il se décompose en plusieurs phases lesquelles sont montrées par la figure 2-1 :

- durée de détection de la panne (1);
- durée de diagnostic de la panne (2);
- durée d'intervention jusqu'au début de la réparation (3);
- durée de la réparation (4);
- durée de remise en service du système (5).

- Le MUT est le temps moyen qui sépare une remise en service opérationnelle du système de la survenance de la panne suivante.

Ces deux derniers indicateurs ne sont pertinents que dans le cas de systèmes réparables. Leur somme MUT+MDT représente le temps moyen qui sépare deux pannes consécutives du système. On le note MTBF, comme Mean Time Between Failures.

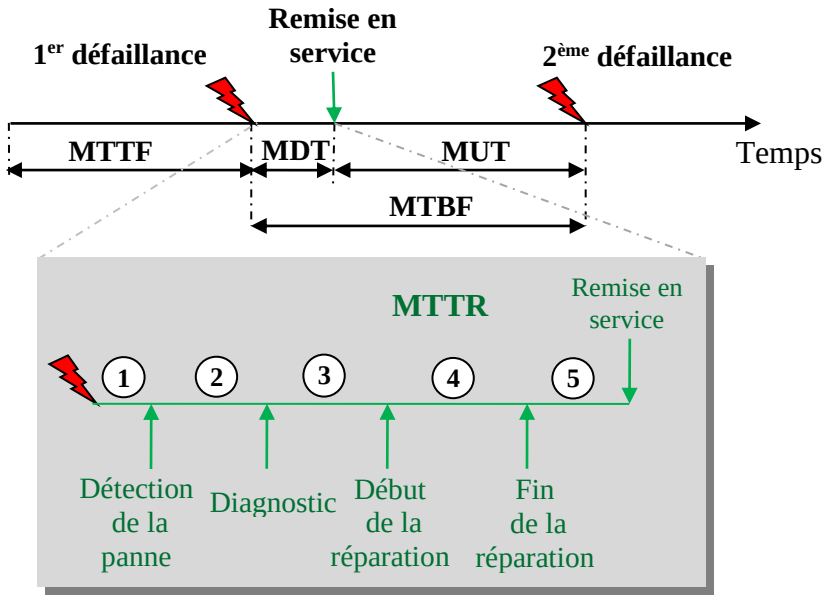


Figure 2-1 : Quelques indicateurs.

2.5 Moyens pour la sûreté de fonctionnement

Le développement d'un système sûr de fonctionnement passe par l'utilisation combinée d'un ensemble de méthodes qui peuvent être classées en :

- prévention des fautes : comment empêcher l'occurrence ou l'introduction de fautes;
- tolérance aux fautes : comment fournir un service à même de remplir la fonction du système en dépit des fautes;
- élimination des fautes : comment réduire la présence (nombre, sévérité) des fautes;
- prévision des fautes : comment estimer la présence, le taux futur, et les possibles conséquences des fautes.

2.6 Enjeu de la sûreté de fonctionnement

L'enjeu de la sûreté de fonctionnement est d'identifier les risques au plus tôt dans la phase de développement du produit.
Plus une erreur de conception est découverte tardivement, plus le risque technique induit peut être lourd et entraîner des surcoûts et des retards considérables pour le projet. L'apparition du risque peut notamment conduire à la mise en cause de la sécurité des personnes et des biens, à la dégradation de l'environnement, à la perte de fonctions.

La sûreté de fonctionnement est une activité d'ingénierie système. Elle peut être qualitative ou quantitative. La part qualitative correspond à l'optimisation des études et elle représente environ 70% de l'activité totale. Les 30% restants représentent la partie quantitative consacrée à la maîtrise des risques avant fabrication à partir des architectures déjà élaborées. C'est donc une phase d'optimisation des architectures des systèmes et de leur mise en œuvre de façon à maximiser, à moindre coût, leur robustesse aux aléas.
En résumé, l'analyse de la sûreté de fonctionnement est une action de réduction des risques et donc du coût à l'achèvement. Elle s'exerce essentiellement pendant les premières phases des projets, jusqu'à la mise en production [53].

2.7 Les études de sûreté de fonctionnement

Les études de sûreté de fonctionnement constituent un préalable indispensable à la conception d'un système voulu sûr [37], et permet d'aider à la prise de décision en (figure 2-2) :

- comprenant et identifiant les risques;
- optimisant l'architecture et comparant des différentes solutions;
- optimisant les moyens de soutien en comparant des solutions;
- justifiant les choix de façon rationnelle et démontrée;
- vérifiant la bonne atteinte des objectifs de sûreté de fonctionnement.

Elles peuvent aussi aider à l'optimisation en :

- diminuant le nombre de pannes qui seront observées durant la vie du système;
- optimisant économiquement la conception par le dimensionnement des équipements et des architectures au "juste nécessaire";
- rendant la maintenance plus ciblée et plus efficace;
- dimensionnant au plus juste les moyens de soutien nécessaires (stocks de pièces de rechange par exemple).

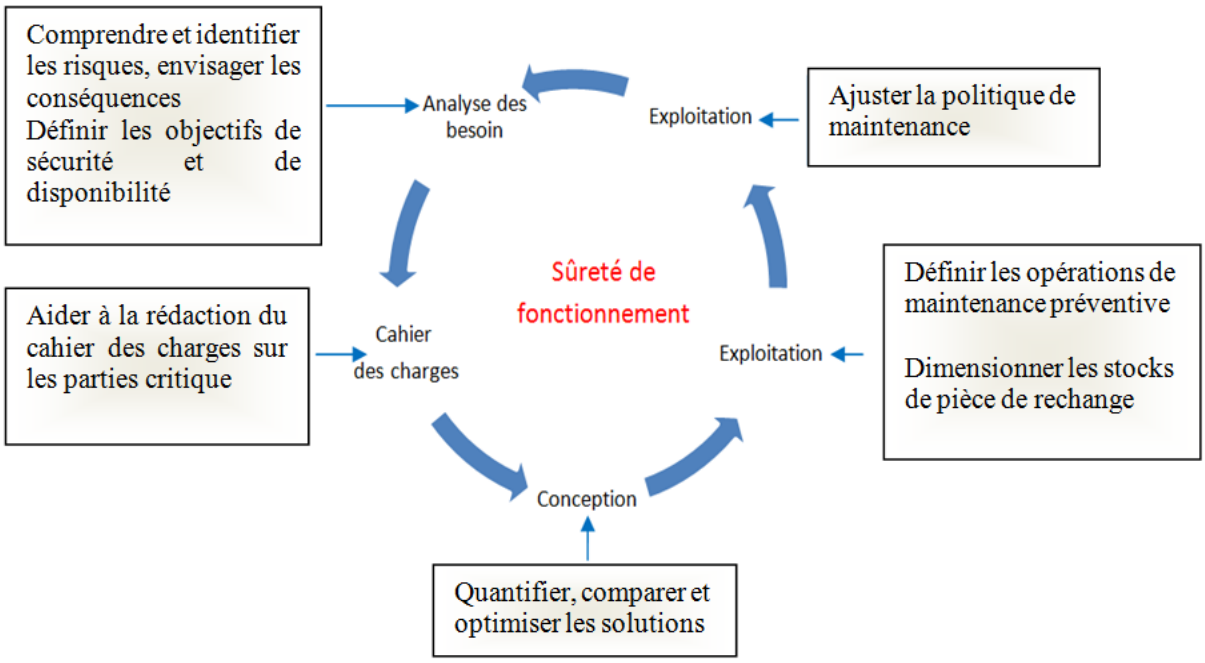


Figure 2-2 : Études de la sûreté de fonctionnement d'un système.

2.7.1 Étape par étape

La première étape consiste à analyser rigoureusement le besoin pour comprendre et identifier l'ensemble des risques, et envisager leurs conséquences. Ensuite, des niveaux d'acceptabilité sont attribués pour ces risques (on parle d'objectifs de F, M, D et/ou S selon les systèmes).

L'identification précise de ces risques va aider à la rédaction du cahier des charges du système, précisément sur ses parties critiques. Il faudra alors imaginer des solutions techniques, des architectures adaptées qui, toutes, seront quantifiées d'un point de vue sûreté de fonctionnement, comparées entre elles et, si nécessaire, optimisées. Une fois la solution retenue, il sera nécessaire de préciser les conditions d'une exploitation la plus efficace possible en :

- définissant les opérations de maintenance préventive nécessaires pour maintenir les caractéristiques de sûreté de fonctionnement au niveau voulu, sans dégradation des équipements préjudiciable à l'une des quatre composantes;
- dimensionnant les stocks de pièces de rechange au plus juste, sans dégrader la disponibilité du système.

2.7.2 Études périphériques

Cette partie, s'intéresse à la recherche d'une méthodologie d'approche globale, complémentaire aux études de sûreté de fonctionnement dans les milieux industriels. Par exemple la recherche de l'optimisation des tailles de stocks de pièces de rechange (suffisamment de pièces en regard de l'aptitude du système à tomber en panne) a fait l'objet d'études particulières où ce souci d'optimisation est couplé avec une démarche analogue sur :

- la maintenance des équipements;
- l'ordonnancement des transports de pièces.

2.7.3 En pratique

L'étude de sûreté de fonctionnement comporte deux volets complémentaires qui sont présentés sur le schéma de la figure 2-3.

- une analyse fonctionnelle, qui va détailler la manière dont le système va opérer dans toutes ses phases de vie ainsi que les autres systèmes avec lesquels il va pouvoir interagir;
- une analyse dysfonctionnelle, qui vise à imaginer l'ensemble des défaillances pouvant survenir n'importe où dans le système, seules ou combinées entre elles, et à analyser l'impact de ces pannes.

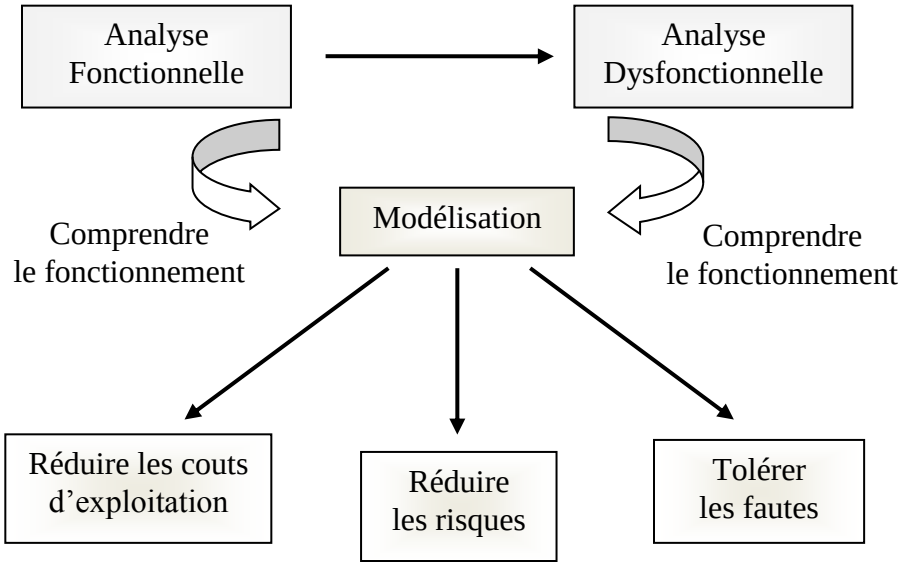


Figure 2-3 : Analyse de la sûreté de fonctionnement.

Les résultats de ces deux études sont mis en commun dans une modélisation du système qui va représenter virtuellement celui-ci avant sa réalisation, tant dans son fonctionnement attendu que dans les pannes susceptibles de lui arriver, comme décrit dans la figure 2-4.

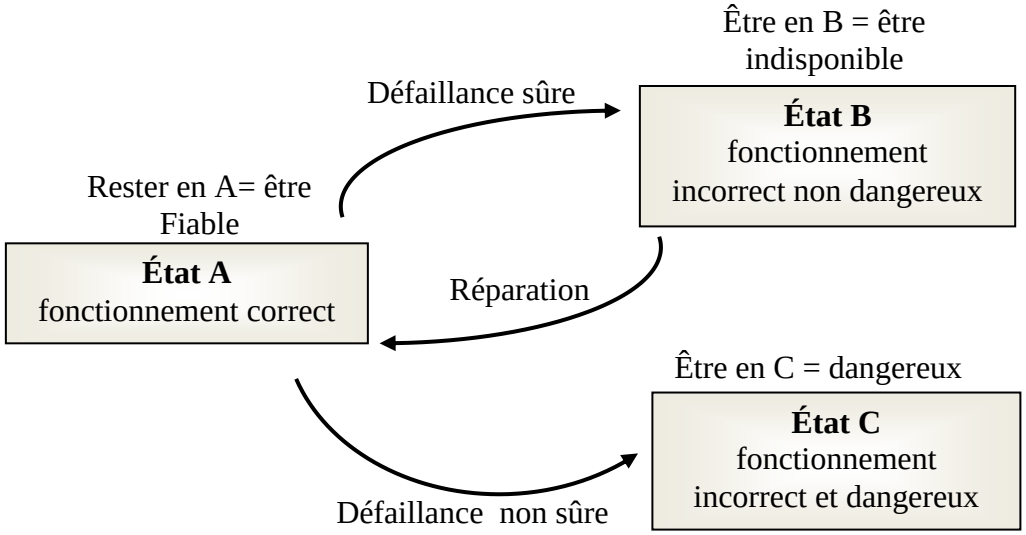


Figure 2-4 : Relation entre la défaillance et l'état d'un système [35].

En étudiant cette modélisation, il devient alors possible de valider ou invalider une solution technique, optimiser des choix architecturaux, remplacer des composants critiques, ceci dont le but de :

- réduire au maximum les risques;
- réduire au maximum les coûts d'exploitation;
- tolérer, dans la mesure du possible, certaines fautes en autorisant un fonctionnement en mode dégradé sous certaines conditions.

2.8 Les outils utilisés

Pour l'analyse fonctionnelle, les principaux outils utilisés sont les suivants [34], [37], [49] :

- SADT (system analysis and design technique), c'est une méthode d'analyse par niveaux successifs d'approche descriptive d'un ensemble, quel qu'il soit. Elle peut l'appliquer aussi bien à la gestion d'une entreprise qu'à un système automatisé.

- BDF (blocs diagrammes fonctionnels), méthode de découpage fonctionnel du système.

Pour l'analyse dysfonctionnelle, on peut recourir à :

- l' APR (analyse préliminaire des risques), qui fournit l'ensemble des événements redoutés prévisionnels dans toutes les phases de vie du système (de la conception au rebut, en passant par la mise en service, l'exploitation et la maintenance) [50];

- l'AMDEC (analyse des modes de défaillance, de leurs effets et de leur criticité), cette méthode exhaustive examine les potentialités de dysfonctionnements de chacun des éléments composant le système, à un niveau de détail choisi à l'avance. Elle permet de quantifier la

probabilité d'apparition de la défaillance et de classer ses effets par ordre de gravité; la combinaison de ces deux estimations fournissant la criticité de l'élément retenu. A l'issue de cette phase, et pour les éléments les plus critiques, il sera procédé à une fiabilisation, ou bien à l'adjonction d'un dispositif de réduction du risque [51], [52];

- l'AEEL (analyse des effets des erreurs logicielles), cette méthode est l'adaptation au logiciel de la méthode AMDEC décrite ci-dessus, le programme étant lui-même décomposé en parties élémentaires de taille prédéfinie [52].

Enfin, pour modéliser le système ainsi analysé, on utilise :

- l'AdD (les arbres de défaillance), en partant d'un événement redouté bien identifié (dit "de tête"), on détermine les sous-événements qui peuvent conduire à l'événement de tête soit par survenance simultanée (il est nécessaire que tous les sous-événements se réalisent pour que l'événement de tête se réalise (on parle de porte ET), soit par survenance d'un quelconque sous événement (porte OU). Chacun des sous-événements est lui-même décomposé ensuite de la même manière, jusqu'à obtenir des éléments suffisamment simples pour estimer directement leur probabilité d'apparition (on parle d'événements de base). En recombinant les probabilités d'apparition de tous les événements de base grâce au schéma logique de l'arbre de décomposition (algèbre booléenne/théorème de Poincaré : équation 2.8) [48], on en déduit la probabilité d'apparition de l'événement de tête [53].

$$P(Uc_i) = \sum_i P(c_i) - \sum_{i \neq j} P(c_i \cap c_j) + \sum_{i \neq j \neq k} P(c_i \cap c_j \cap c_k) - \ldots \qquad (2.8)$$

L'analyse par un arbre des défaillances est fondée sur les principes suivants :

- un événement est une combinaison d'événements de base non décomposables,
- les évènements de base sont indépendants,
- la probabilité d'occurrence des événements de base peut être évaluée.

Les liens entre les différents évènements sont réalisés grâce à des opérateurs logiques (ET, OU, ...etc.). Cette méthode utilise une représentation graphique qui permet de présenter les résultats dans une structure arborescente [53].
La méthode des Arbres de Défaillances, est la plus utilisée pour analyser les défaillances de systèmes complexes.

- Les GM (graphes de Markov), ce sont les différents états du système qui sont représentés. On suppose que le passage d'un état du système à l'autre survient aléatoirement, ou classiquement par la défaillance d'un élément, ou à la fin de la réparation d'un autre élément. Connaissant l'état initial du système, on peut en déduire soit la probabilité d'être dans un état donné après une durée déterminée, soit la probabilité moyenne d'être dans un état donné tout au long de sa durée de vie utile [54], [55].

- Les RdPS (réseaux de Petri stochastiques), cette technique s'apparente à celle des graphes de Markov décrite ci-dessus, à la différence que les transitions entre les différents états peuvent suivre des lois de probabilité autres que la loi exponentielle classique. D'autres

caractéristiques permettent de synchroniser différentes transitions. Le prix à payer étant la nécessité de simuler le fonctionnement du système par des méthodes de Monte Carlo puisque le calcul analytique n'est quasiment jamais possible. Il existe une abondante littérature sur les diverses techniques actuelles d'accélération des simulations pour ce type de systèmes [56].

2.9 Origines des problèmes de sûreté de fonctionnement

L'augmentation de la taille et de la complexité des systèmes actuels (système mécatronique) rend les processus de conception de plus en plus difficiles. Les changements apportés aux systèmes au fil des années font apparaître des limites des approches et techniques relatives à la sûreté [53]. Ils concernent :

- Des évolutions technologiques rapides,
- Des changements dans la nature des accidents,
- De nouveaux types de dangers,
- Une augmentation de la complexité et de l'hétérogénéité,
- Une relation plus complexe entre l'humain et l'automatisation,
- Un changement de la vision des organismes de régulation et des simples utilisateurs sur la sûreté.

Ces changements représentent un challenge pour tous les acteurs académiques et/ou industriels pour la définition de nouveaux processus, méthodes et outils d'analyse et d'évaluation de la sûreté.

Rasmussen [57] a montré que la majorité des accidents sont souvent causés non pas par la composition de défaillances indépendantes mais reflète plutôt d'une migration systématique du comportement organisationnel vers les limites d'un comportement sûr. Ceci est principalement dû aux pressions sur les coûts et sur l'efficacité exigée dans un environnement de plus en plus compétitif.

Somme toute, les faiblesses des processus actuels d'analyse et d'évaluation de la sûreté peuvent être résumées par les points suivants [25] :

- Différents groupes ont besoin de travailler avec différentes vues du système (vue d'ingénieur système et vue d'ingénieur de sûreté par exemple).
- Mauvaise définition des exigences de sûreté et de leur formalisation.
- Absence de traçabilité des exigences de sûreté.
- Les méthodes existantes (traditionnelles) sont insuffisantes vu la complexité des systèmes actuels.
- La description textuelle des modes de défaillance est souvent ambigüe.
- Absence de langage commun entre les différents métiers concernés par le système.
- Besoins mal spécifiés ou exigences mal formulées.
- Evolution des besoins/exigences dans le temps et mauvaise gestion du changement.
- Modification spontanée, parfois faite avec de bonnes intentions.
- Non accumulation de savoir-faire et manque de retour d'expérience.
- Pari technologique trop important.
- Définition erronée d'interface.

- Forte pression de la concurrence.
- Extension d'exigences fonctionnelles.

Nous constatons que les problèmes de sûreté de fonctionnement des systèmes ne proviennent pas nécessairement d'une mauvaise analyse ou mauvaise estimation des attributs de sûreté (fiabilité, maintenabilité, disponibilité, sécurité, confidentialité, intégrité), mais de nombre d'autres aspects liés aux projets et à la démarche de conception. Comme exemple, nous pouvons citer : la gestion des données, les mécanismes de traçabilité, la gestion de configuration, la gestion des risques, la définition d'interface, la formulation d'exigence, …etc.

Ces éléments participent indirectement à la sûreté de fonctionnement du système; la figure 2-5 présente une vue conceptuelle de la sûreté de fonctionnement, cette représentation s'inspirant d'une norme d'ingénierie système, l'EIA-632 [58].

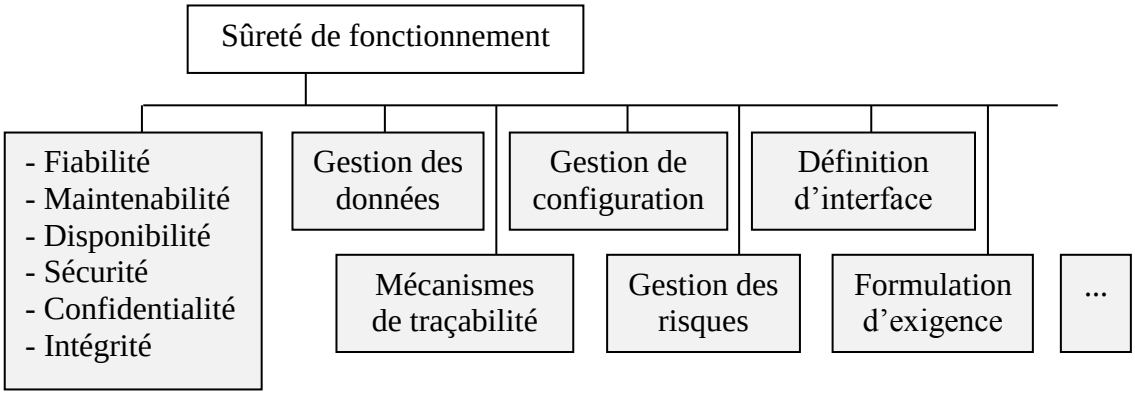


Figure 2-5 : Sûreté de fonctionnement et démarche de conception.

2.10 Les données de fiabilité

Elles sont la base même des études. C'est à partir des données de fiabilité que vont être élaborés les calculs permettant une vision objective des capacités du système en termes de sûreté de fonctionnement [59].

2.10.1 Les recueils

Il existe de nombreux recueils de données collectées et traitées par des organismes privés ou publics à travers le monde, et mises à jour régulièrement. C'est le cas du domaine électronique notamment, qui bénéficie des nombreux travaux des industriels concernés.

2.10.2 Le retour d'expérience

Le retour d'expérience est désigné ainsi l'ensemble des dispositions permettant de recueillir des informations sur la fiabilité opérationnelle des produits et systèmes auxquels on s'intéresse : pannes, défaillances détectées préventivement, maintenances diverses.

Si le recueil de données est fidèle à la réalité, il est possible, grâce à des techniques statistiques adaptées, de calculer les indicateurs de sûreté de fonctionnement correspondant, spécifiques pour le système considéré. Ainsi, ces indicateurs sont plus pertinents aux yeux des clients de ces systèmes.

2.11 La normalisation

Dans cette section, on évoquera quelques normes génériques pour la sûreté de fonctionnement [25].

2.11.1 ARP-4754

La norme de sûreté ARP-4754 [60], dont l'intitulé est « Certification Considerations for Highly-Integrated or Complex Aircraft Systems » et dont une nouvelle version est sortie en décembre 2010, est un standard de la Society of Automotive Engineers (SAE). Elle traite de processus de développement de systèmes aéronautiques en se focalisant sur les aspects de sûreté.
La norme fait référence à d'autres standards bien connus, comme le DO-178B «Software Considerations in Airborne Systems and Equipment Certification» [61], pour le développement de logiciel dans le domaine aéronautique, ou encore le DO-254 «Design Assurance Guidance for Airborne Electronic Hardware Considerations in Airborne Systems and Equipment Certification» [62], pour le développement de matériel.
Pour beaucoup de techniques d'ingénierie pour la sûreté, l'ARP-4754 [60], fait aussi référence à un autre standard l'ARP-4761 présenté dans la section suivante.

2.11.2 ARP-4761

L'ARP-6761 «Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment » [63], il est destiné à être utilisé conjointement avec l'ARP-4754 pour démontrer la conformité du système en court de conception.

2.11.3 CEI-61508 et ses dérivées

La norme CEI-61508 [64], est une norme générique de sûreté de fonctionnement du CEI (International Electrotechnical Commission), elle est utilisée comme référentiel par tous les grands secteurs industriels. Elle traite de la sécurité fonctionnelle des systèmes électriques/électroniques et électroniques programmables (E/E/PE).
En fait, cette norme a révolutionné le monde de la sûreté de fonctionnement, car elle a su amener des nouveautés dans la façon d'intégrer et de réaliser les activités de sûreté de fonctionnement dans le cycle de développement d'un système E/E/PE. Entre autres, la norme a permis de définir des niveaux d'intégrité pour des systèmes E/E/PE qui prennent en compte aussi bien les aspects quantitatifs que qualitatifs dans la gestion du risque.
Par son aspect générique, la norme CEI 61508 reste brève sur la description des outils, méthodes et les techniques à mettre en œuvre. Mais depuis sa création, plusieurs dérivés de cette norme ont vu le jour dans le but de la rendre applicable pour les différents secteurs concernés (figure 2-6) [25].

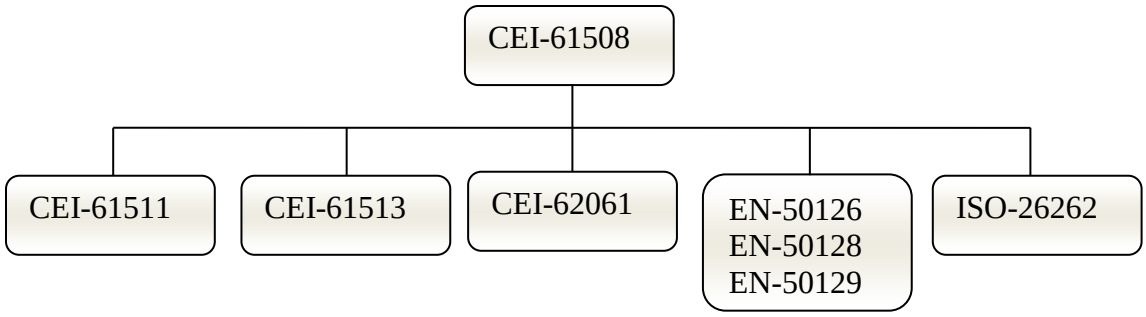


Figure 2-6 : Norme CEI-61508 et ses dérivées

Ces normes dérivées sont les suivantes :

- La norme CEI 61511, créée en 2003, est adaptée pour les procédés industriels.
- La norme CEI 61513, créée en 2001, est adaptée pour le secteur du nucléaire.
- La norme CEI 62061, créée en 2005, est adaptée pour la sécurité des machines.
- Les normes EN 50126/EN 50128/EN 50129, créées respectivement pour les dernières versions, en 1999/2001/2003, sont adaptées pour le secteur du ferroviaire.
- La norme ISO 26262, qui devrait être publiée en tant que standard en 2011, sera adaptée pour le secteur de l'automobile [65].

Cette dernière section a permis de conclu que les normes de sûreté aident énormément à comprendre quels sont les objectifs et les activités pour obtenir un système sûrs. Par exemple, l'ARP-4754 fournit une très bonne vision des activités de sûreté de fonctionnement. Mais en soit, ces normes ne définissent pas une approche globale et unifiée avec les activités de conception nominales. Il était nécessaire de définir une approche globale pour la prise en compte de la sûreté de fonctionnement.

2.12 Conclusion

Après un tour d'horizon sur l'historique de la sûreté de fonctionnement, nous avons passé en revue dans ce chapitre les principaux outils et méthodes d'analyse de la sûreté de fonctionnement des systèmes.
Nous allons exposer la problématique d'intégration de la sûreté de fonctionnement dans les systèmes mécatroniques, qui fait partie de nos domaines d'intérêt. Nous constatons l'absence d'approches globales pour l'analyse de sûreté de fonctionnement qui doit permettre de répondre à la problématique liée aux insuffisances des méthodes statiques limitées par un certains nombre d'hypothèses notamment l'absence de la notion d'ordre entre les événements, ainsi que la notion de l'instant d'apparition des événements. Il nous a paru nécessaire, d'aborder ce problème dans le chapitre suivant.

Conclusion générale

Les travaux développés dans cette thèse ont contribué à l'analyse de la sûreté de fonctionnement des systèmes mécatroniques et plus particulièrement la recherche des scénarios redoutés minimaux. Les systèmes mécatroniques étant des systèmes dynamiques hybrides. Pour modéliser l'aspect hybride, les réseaux de Petri prédicats transitions différentiel stochastique ont été utilisés. Cette modélisation semble bien adaptée à une description fine des systèmes hybrides soumis à des reconfigurations de façon à prendre en compte correctement les défaillances. Cela est nécessaire pour simuler aussi le plus fidèlement possible des scénarios redoutés dont on connaît déjà les événements constitutifs.

Pour mettre en évidence les scénarios redoutés minimaux, on a développé une approche hybride d'extraction de scénarios redoutés à partir d'un modèle réseau de Petri. L'approche est basée sur la logique linéaire et permet de générer les scénarios redoutés minimaux sans avoir à explorer la totalité du système. Elle est basée sur une analyse des relations de cause à effet présentes dans le modèle qui permettent de déterminer les scénarios non pas sous forme de séquence d'événements mais par un ordre partiel entre les événements du scénario.

Un travail théorique a permis de mieux formaliser la notion de scénario. Une définition formelle basée sur la logique linéaire de la notion de scénario a été proposée. Cette définition a permis ensuite de présenter formellement la notion de minimalité dans le cadre des arbres de preuve de la logique linéaire, basée sur la notion de coupe minimale de la méthode des arbres de défaillances. Cette notion a été intégrée dans un algorithme de construction de l'arbre de preuve de la logique linéaire. Un algorithme a été développé pour la génération des scénarios redoutés minimaux dans un contexte inconnu, ce qui facilite l'analyse de recherche des scénarios minimaux. Grâce à cet algorithme, on a développé une méthode de recherche des scénarios minimaux. Le but final est d'en déterminer le scénario redouté minimale globale.

Tout d'abord, au lieu de raisonner d'un état initial vers un état final, nous avons raisonné à partir de l'état redouté et remonter les chaînes de causalité jusqu'à un état normal, il s'agit d'un raisonnement arrière. Le raisonnement arrière pouvait se faire en logique linéaire comme le raisonnement avant, à condition d'avoir inversé les arcs du réseau de Petri.

Le raisonnement arrière, expliquant comment le système peut arriver dans l'état redouté en question. Ce raisonnement est poursuivi jusqu'à ce que l'on arrive à un état de fonctionnement normal. Ensuite un raisonnement avant est mené afin de voir toutes les évolutions possibles à partir de l'état partiel normal obtenu. Ce raisonnement a pour but de mettre en évidence les comportements qui permettent d'éviter d'atteindre l'état redouté. Une bonne caractérisation des bifurcations entre le comportement menant à l'état redouté et ceux qui l'évitent est en effet essentielle pour comprendre les conditions d'occurrence du scénario redouté et pour envisager ensuite une étude qualitative ciblée.

Les perspectives ouvertes par ce travail sont multiples. Elles vont du domaine de la fiabilité dynamique à l'étude systématique des probabilités d'occurrence des événements redoutés. Nous espérons que cette approche débouchera sur des projets de développement dans les axes de recherche et pour des cas plus significatifs et d'aborder certains aspects qui n'ont pas été traités.

Dès que nous sommes en mesure de comprendre une théorie, une autre vient prendre sa place.
[Carl Sagan]

Bibliographie

[1] Boucerredj L., (2006). « Sûreté de fonctionnement: Recherche des scénarios critique dans les systèmes mécatroniques ». Mémoire de magister, à la l'université d'Annaba.

[2] Jallouli M., (2009). « Méthodologie de conception d'architectures de processeur sûres de fonctionnement pour les applications mécatroniques ». Thèse de doctorat, Université Paul Verlaine – Metz, France.

[3] Yaskawa C., (1969). Http : //www.yaskawa.co.jp/en/company/rekisi.htm.

[4] Isermann R., (2000). « Mechatronic systems : concepts and applications ». Transactions of the Institute of Measurement and Control, vol. 22, p. 29-55.

[5] Norme (2008). NF E 01-010 – AFNOR.

[6] Isermann R., (2007). « Mechatronic systems - innovative products with embedded control ». Control Engineering Practice, 10 :16.

[7] Piwonka F., (2001). « Mechatronic systems engineering - from methodology to education ». In 1st Baltic Sea Workshop on Education in Mechatronics : A new Approach to Engineering Education.

[8] Alciatore D., (2006).« Definitions of mechatronics »,
http://www.engr.colostate.edu/mechatronics/definitions.html.

[9] Saviuc V., (2006). « La mécatronique intelligente ». Jitec.

[10] Rzevski G., (2003). « On conceptual design of intelligent mechatronic systems ». Mechatronics, 13(10), pp. 1029–1044.

[11] Chalé H. G., Taofifenua O., Gaudré T., Topa A., Lévy N. & Boulanger J. L., (2011). « Reducing the Gap Between Formal and Informal Worlds in Automotive Safety Critical Systems». 21st Annual INCOSE International Symposium. Denver, USA.

[12] Thesame, (2013). « La mécatronique à l'épreuve du marché ». Jitec.

[13] Breedveld P. C., (2004). « Port-based modeling of mechatronic systems ». Mathematics and Computers in Simulation, 66, pp. 99–127.

[14] Demri A., (2010). « Contribution à l'évaluation de la fiabilité d'un système mécatronique par modélisation fonctionnelle et dysfonctionnelle ». Thèse a l'université d'Angers, 186p.

[15] Ollero A., Boverie S., Goodall R., Sasiadek J., Erbe H., & Zuehlke D., (2006). « Mechatronics robotics and components for automation and control: Ifac milestone report ». Annual Reviews in Control, 30(1), pp. 41–54.

[16] Siemers C., Falsett R., Seyer R., & Ecker K., (2005). « Reliable event-triggered systems for mechatronic applications ». Journal of Systems and Software, 77(1), pp. 17–26.

[17] Cazals F., Meizel D., (2005). « Projects in the pedagogy of mechatronics in engineering education ». In The 6th International Workshop on Research and Education in Mechatronics, pages 453–458, France.

[18] Schoenig R., (2004). « Définition d'une méthodologie de conception des systèmes mécatroniques sûrs de fonctionnement ». Thèse de L'Institut National Polytechnique de Lorraine.

[19] Guillemot M., Noterman D., Bideaux E., Louail G., et Favrel J., (2002). « Ingénierie concourante interdisciplinaire ou inter-métier ». In 4th International Conference on Integrated Design and Manufacturing in Mechanical Engineering, Clermond-Ferrand, France.

[20] Gomes S., Sagot J., Koukam A., Leroy N., (1999). « Manercos a new tool providing ergonomics in a concurrent engineering design life cycle ». In 4th Annual Scientific Conference on Web Technology, New Media, Communications and Telematics - Theory, Methods, Tools and Applications, EUROMEDIA 99, pages 237– 241, Munich.

[21] Dieterle W., (2005). « Mechatronic systems : Automotive applications and modern design methodologies». Annual Reviews in Control, 29(2), pp. 273–277.

[22] Molla J., Jacobsa J., Kustersb R., et Trienekens J., (2004). « Defect detection oriented lifecycle modeling in complex product development ». Information and Software Technology, 46: 665–675.

[23] Fan Z., Sorensen T., Conrad F., Andreasen M., Christensen G., & Hein L. (2005). « Mechatronics education : Conceptual prototype Vs ». Physical realization. In The 6th International Workshop on Research and Education in Mechatronics, pages 397–402, France.

[24] Sell R., et Tamre M., (2005). « Integration of v-model and sysml for advanced mechatronics system design ». In The 6th International Workshop on Research and Education in Mechatronics, pages 276–280, France.

[25] Guillerm R., (2011). « Intégration de la Sûreté de Fonctionnement dans les Processus d'Ingénierie Système ». Thèse de doctorat de l'université de Toulouse III – Paul Sabatier.
[26] Castaneda Pérez G. A., (2009). « Évaluation par simulation de la sûreté de fonctionnement de systèmes en contexte dynamique hybride ». Thèse de L'Institut National Polytechnique de Lorraine.

[27] Jamshidpour E., (2014). « Contribution a l'étude de la sûreté de fonctionnement et de la continuité de service des bus DC ». Thèse de doctorat de l'université de Lorraine.

[28] David P., Idasiak V., Kratz F., (2010). « Reliability study of complex physical systems using SysML ». Reliability Engineering and System Safety, Vol. 95, pp.431- 450.

[29] Brissaud F., (2010). « Contributions à la Modélisation et à l'Évaluation de la Sûreté de Fonctionnement de Systèmes de Sécurité à Fonctionnalités Numériques ». Thèse de doctorat, Université de Technologie de Troyes.

[30] Mkhida A., Thiriet J. M., Aubry J. F., (2008). « Impact de l'utilisation d'un réseau de communication sur les performances en sécurité d'un système instrumente de sécurité ». 7ème Conférence Internationale de Modélisation et Simulation, ''Modélisation, Optimisation et Simulation des Systèmes : Communication, Coopération et Coordination'', MOSIM'08, 8 p.

[31] Chevalier M., (2004). « La Sûreté de Fonctionnement ». Le magazine Schneider Electric, Guide Technique de l'enseignement technologique et professionnel.

[32] CEI / IEC 1025-Norme Internationale, (1990). « Fault Tree Analysis (FTA) ». Bureau Central de la CEI, Genève, Suisse.

[33] Batteux M., (2011). « Développement d'une chaîne de conception outillée d'un système de diagnostic appliquée aux systèmes technologiques pilotés ». Thèse de doctorat, Université Paris-Sud11.

[34] Mkhida A., 2010. « Déficience de la validation d'un capteur intelligent et incidence sûr les performances d'une boucle de sécurité ». Manuscrit auteur, publié dans 17ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda-Mu'2010, La Rochelle : France.

[35] Sylvie L., (2004). « Etudes de sûreté des installations électriques ». Cahier Technique Schneider Electric, n° 184.

[36] Vesely W.E., Goldberg F.F., Roberts N.H., Haasl D.F., (1981). « Fault Tree Handbook ». U.S. Nuclear Regulatory Commission Washington.

[37] Riera D., Clement E., (2012). « Modélisation dynamique en sureté de fonctionnement : une avance pour l'analyse des systèmes complexes ». 18ème congrès de maîtrise des risques et sûreté de fonctionnement, 16 – 18 octobre 2012. Tours.

[38] Watson H.A., (1961). « Launch Control Safety Study ». Section VII, Vol. 1, Bell Labs, Murray Hill, NJ.

[39] Ledoux J., Gaudoin O., (2007). « Modélisation aléatoire en fiabilité des logiciels ». Edition Hermes Science Publications.

[40] Rasmussen N., (1975). « Reactor Safety Study – An Assessment of Accident Risks in U.S ». Commercial Nuclear Power Plants, WASH-1400, October 1975.

[41] Rogovin M., (1979). « Three Mile Island : a report to the commissioners and to the public ». Technical Report, Nuclear Regulatory Commission, Washington, DC (USA), January 1979.

[42] Villemeur A., (1988). « Sûreté de fonctionnement des systèmes industriels ». Edition Eyrolles.

[43] CEI 50 191. (1990). « Vocabulaire Electrotechnique International ». Sûreté de fonctionnement et qualité des services, Chapitre 191.

[44] Belhadaoui H., (2008). « Conception sûre des systèmes mécatroniques intelligents pour des applications critiques ». Thèse de Doctorat. Institut National Polytechnique de Lorraine, Université Paul Verlaine – Metz, France.

[45] Laprie J. C., (2004). « Sûreté de fonctionnement informatique : concepts, défis, directions ». ACI Sécurité et Informatique, CNRS, LAAS, Toulouse, 15 – 17 novembre.

[46] Pagès A., & Gondran M., (1980). « Fiabilité des systèmes ». Collection de la Direction des Études et Recherches d'Électricité de France, Editions Eyrolles.

[47] Smith D. J., (2001). « Reliability, maintainability and risk. Practical methods for engineers ». Sixth Edition, Butterworth Heinemann.

[48] EN 292 – 1, (1991). « Sécurité de machines – Notions fondamentales, principes, généraux de conception – Partie 1 ». Terminologie de base – Méthodologie.

[49] David P., (2009). « Contribution à l'analyse de sûreté de fonctionnement des systèmes complexes en phase de conception : application à l'évaluation des missions d'un réseau de capteurs de présence humaine ». Thèse doctorat, Université d'Orléans.

[50] Desroches A., Baudrin D., Dadoun M., (2009). « L'analyse préliminaire des risques ». Edition Hermès – Lavoisier.

[51] Evrot D., (2008). « Contribution à la vérification d'exigences de sécurité : application au domaine de la machine industrielle ». Thèse de doctorat, Université Henri Poincaré, Nancy I.

[52] Faucher J., (2009). « Pratique de l'AMDEC ». 2ème édition, Editeur Dunod, 17 juin 2009.

[53] Guillerm R., Sadou N., et Demmou H., (2011). « Combining FMECA and Fault Trees for declining safety requirements of complex systems ». European Safety and Reliability Conference.

[54] Schoenig R., Aubry J. F., Cambois T., Hutinet T., (2006). «An aggregation method of Markov graphs for the reliability analysis of hybrid systems ». International Journal on Reliability Engineering and System Safety, Elsevier, Vol 91/2, pp. 137–148.

[55] Zhang H., Gonzalez K., Dufour F., Dutuit Y., (2008). « Piecewise deterministic Markov processes and dynamic reliability ». Journal of Risk and Reliability, Volume 222, number 4, Professional Engineering Publishing, ISSN 1748-006X, 1748-0078.

[56] Florin G., Natkin S., (1985). « Les Réseaux de Petri Stochastiques». Technique et Science Informatiques,Vol A, N°l, pp. 143-160.

[57] Rasmussen J., (1997). « Risk Management in a Dynamic Society : A Modelling Problem ». Safety Science, vol. 27, N° 2, Elsevier Science Ltd., pp. 183-213.

[58] EIA-632, (1999). « Processes for engineering systems, Electronic Industries Alliance standard ». 7 janvier 1999.

[59] Guillerm R., Sadou N., et Demmou H., (2009). « System engineering approach for safety ». European Simulation and Modelling Conference, Leicester (Royaume-Unis), pp. 150-157.

[60] ARP-4754, (1996). « Certification considerations for highly-integrated or complex aircraft systems ». Society of Automotive Engineers (SAE) standard, November 1996.

[61] DO-178B, (1992). « Software considerations in airborne systems and equipment certification ». RTCA et EUROCAE, 1er décembre 1992.

[62] DO-254, (2000). « Design assurance guidance for airborne electronic hardware ». RTCA et EUROCAE, 19 avril 2000.

[63] ARP-4761, (1996). « Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment». Society of Automotive Engineers (SAE) standard.

[64] CEI-61508, (2010). « Functional safety of electrical/electronic/programmable electronic safety-related systems ». International Electrotechnical Commission standard.

[65] ISO-26262, (2008). « Véhicules routiers – sécurité fonctionnelle, version projet de comité ». International Organization of Standardization standard.

[66] Kurovszky M., (2007). « Etude des systèmes dynamiques hybrides par représentation d'état discrète et automate hybride ». Institut National Polytechnique de Grenoble – France.

[67] Brinzei N., Perez Castaneda G. A., et Aubry J. F., (2009). « Sûreté de fonctionnement previsionnelle en contexte dynamique». In 2ème Workshop Surveillance, Sûreté et Sécurité des Grands Systèmes, Nancy, France.

[68] Zaytoon J., (2001). « Systèmes dynamiques hybrides ». Ouvrage collectif sous la direction de collection Hermes Science, ISBN 2-7462-0247-6.

[69] Antsaklis P. J., Koutsoukos X. D., (2002). « Hybrid Systems Control », Encyclopedia of Physical Science and Technology, 3rd edition, Academic Press, vol. 7, p. 445-458.

[70] Olivier-maget N., (2007). « Surveillance des systèmes dynamiques hybrides : Application aux procédés ». Thèse de doctorat, délivré par l'Institut National des Sciences Appliquées de Toulouse.

[71] Demongodin l., Rouibia S., (2003). « Modélisation par réseaux de Petri lots et analyse de l'état stable par automates hybrides ». Modélisation et simulation, 23-25 avril, Toulouse, France.

[72] Diaz M., (2001). « Les réseaux de Pétri, Modèles fondamentaux ». Hermès, Paris.

[73] Antsaklis P., and Koutsoukos X., (1998). « On hybrid control of complex systems : a survey ». European Journa l of Automation, vol. 32, N°. 9-10, pp. 1023-1045.

[74] Alur A., Courcoubetis C., Henzinger T.A., and Ho P.H., (1993), « Hybrid automata : an algorithmic approach to the specification and verification of hybrid systems ». In Hybrid Systems, LNCS, 736, pp. 209-229.

[75] Mokhtari A., (2007) « Diagnostic des systèmes hybrides: développement d'une méthode associant la détection par classification et la simulation dynamique ». Thèse de doctorat. CNRS. Délivré par l'Institut National des Sciences Appliquées de Toulouse.

[76] Baptiste P., Bournez O., (2009). « Programmation et Algorithmique ». Polycopie du cours INF 421, Ecole Polytechnique.

[77] Bourdais R., Yim P., Perruquetti W. (2007). « Time Petri Nets Based Switching Sequences of Hybrid Systems ». International Modeling and Simulation Multiconference, Buenos Aires (Argentine), février 2007.

[78] Medjoudj M., (2006). «Contribution à l'analyse des systèmes pilotés par calculateurs : extraction de scénarios redoutés et vérification de contraintes temporelles». Thèse de doctorat, Universite Paul Sabatier - Toulouse III.

[79] Boucerredj, L., Debbache, N.E., (2007 a), « High-level Petri nets based modelling of hybrid systems». Advancement Modelling and Analysis, International Journal, Vol. 8, Issue1, Published Journal: 2007, Nº 1-2-3.

[80] Genrich H., (1987). « Predicate/transition nets. Petri Nets : Central Models and Their Properties, Advances in Petri Nets ». Lecture Notes in Computer Science 254: 207-247.

[81] Boucerredj L., Debbache N. E., (2008). « Qualitative safety evaluation of mechatronic systems using DPTPN ». Conference international on Tenth International Conference (AEIC), AL-AZHAR ENGINEERING, 24-26 décembre 2008.

[82] Sadou N., (2007). « Aide à la conception des systèmes embarqués sûrs de fonctionnement ». Thèse de doctorat, INSA de Toulouse.

[83] Merle G., Roussel J.M., and Lesage J.J., (2011). « Algebraic Determination of the Structure Function of Dynamic Fault Trees ». Reliability Engineering and System Safety, 96(2), pp. 267-277.

[84] Moncelet G., (1998). « Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile ». Thèse de Doctorat, Université Paul Sabatier, Toulouse.

[85] Khalfaoui S., (2003). « Méthode de recherche des scénarios redoutés pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile ». Thèse de Doctorat, Institut National Polytechnique.

[86] Girault F., (1997). « Formalisation en Logique Linéaire du fonctionnement de réseaux de Petri ». Thèse de Doctorat, Université Paul Sabatier, Toulouse.

[87] Girard J.Y., (1987), « Linear Logic ». Theoretical Computer Science 50, pp.1-102.

[88] Rivière, N., (2003). « Modélisation et analyse temporelle par réseaux de Petri et logique linéaire ». Thèse de l'INSA de Toulouse, le 26 novembre 2003.

[89] Boucerredj L., Debbache N.E., (2007 b). « Modelling of a hybrid system through differential predicate transition Petri nets model and proof tree ». Aircraft Engineering and Aerospace Technology, an International Journal, ISSN 1748-8842. Volume79 Number 3, pages 261 à 267.

[90] Sadou N., Demmou H., Pascal J.C., valette R., (2006). « Fiabilité dynamique des systèmes hybrides : approche basée scénarios ». Conférence Internationale Francophone d'Automatique, Bordeaux, France, 30 Mai - 1er Juin 2006, 6p.

[91] Boucerredj L., Debbache N. E., (2010). « Sûreté de fonctionnement : minimalité des scénarios redoutés ». 3ème Journée sur les Signaux et Systèmes, Université 8 mai 45, Guelma.

[92] Boucerredj L., Debbache N. E., (2011). « Évaluation de la sûreté de fonctionnement des systèmes mécatroniques en utilisant la notion de coupe minimale et la logique linéaire ». Conference International on Systems and Information Processing, Université 8 mai 45 de Guelma.

[93] Boucerredj L., Debbache N. E., (2014 a). « Minimality of Critical Scenarios with linear logic and cutsets ». Revue Synthèse, An international Journal. Volume 29, pages 42-50.

[94] Rauzy A., (2001). « Mathematical foundation of minimal cutsets language ». IEEE Transactions on Reliability, 50(4), pp. 389–396, December 2001.

[95] Merle G., (2010). « Modélisation algébrique des arbres de défaillance dynamiques, contribution aux analyses qualitative et quantitative ». Thèse de doctorat, Ecole normale supérieure de Cachan.

[96] Boucerredj L., Debbache N. E., (2014 b). « Évolution d'une approche analytique pour l'étude des scenarios redoutes ». JD'14, LAIG, Université 8 mai 45 de Guelma.

[97] Boucerredj L., Debbache N. E., (2007 c). « Le raisonnement dans un contexte inconnu pour le diagnostic des systèmes mécatroniques ». Congrès Algérien de Mécanique de Construction, 29-30 Avril 2007 à l'Université des Sciences et de la Technologie Houari Boumediene (U. S. T. H. B), Algérie, IEE.

[98] Pradin-Chézalviel B., Valette R., (2003), « Réseaux de Petri et Logic Linear », chapitre 6 de l'ouvrage ''Vérification et mise en œuvre des réseaux de Petri'' (sous la direction de Michel Diaz), Edition Hermès, ISBN 2-7462-0445-2, pp. 209-229.

[99] Boucerredj L., Debbache N. E., (2014 c). « A novel algorithm to optimize the search of failure ». Joint International Symposium on "the Social impacts of Developments in Information, Manufacturing and Service Systems". CIE'44 & IMSS'14 Proceedings, Turkey.

[100] Hanzalek, (2009). « Matlab toolbox for Petri nets ». Martina Svádová, Zdeněk Hanzálek, Center for Applied Cybernetics, DCE FEE, Czech Technical University in Prague, http://dce.felk.cvut.cz/PN/.

[101] Zhang H., De Saporta B., Dufour F., et Deleuze G., (2013). « Dynamic reliability by using simulink and stateflow ». Chemical Engineering Transactions, 33 : 529–534.

[102] Reicherdt R., and Glesner S., (2012). « Slicing matlab simulink models ». pp. 551–561.

[103] Chunqing C., Sun J., Liu Y., Dong S., Zheng M., (2012). « Formal modeling and validation of Stateflow diagrams ». Int J Softw Tools Technol Transfer 14 : 653–671 DOI 10.1007/s10009-012-0235-0 Published online : 6 June 2012 © Springer-Verlag.

[104] Website, (2003). « Simulink, stateflow and real-time workshop ». http://www.mathworks.com/products.

[105] User guide, (2009). « MathWorks Automotive Advisory Board Control Algorithm Modeling». Guidelines Using M ATLAB, Simulink, and Stateflow.

[106] Site Web de MATLAB et SIMULINK. (2003). http://www.mathworks.com/.