N° Ordre...../FT/UMBB/2020

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université M'Hamed Bougara-Boumerdes

Faculté de Technologie
Laboratoire de Mécanique des Solides et Systèmes

Thèse de Doctorat

Présentée par

AGGAD Maya

En vue de l'obtention du diplôme de doctorat en :

Filière : Génie mécanique

Option : Mécatronique

Titre : Contribution à l'amélioration de la sûreté de fonctionnement des systèmes mécatroniques en phase d'exploitation. Définition d'une approche globale pour l'extraction des scénarii redoutés et le choix de stratégie de maintenance.

Devant le jury :

BENAZZOUZ Djamel	Professeur	UMB Boumerdes	Président
ADJERID Smail	Professeur	UMB Boumerdes	Directeur de thèse
BENFDILA Arezki	Professeur	UMM Tizi-Ouzou	Examinateur 1
BENTARZI Hamid	Professeur	UMB Boumerdes	Examinateur 2
RAHMOUNE Chemsedine	MCA	UMB Boumerdes	Examinateur 3

Année Universitaire : 2020/2021

Remerciements Avant de commencer ce manuscrit je souhaite adresser quelques remerciements à tous ceux qui ont contribué à ce travail et m'ont permis d'aboutir à la fin de ces années de thèse.

Il est de tradition de commencer cette liste par son directeur de thèse. Plus qu'une tradition, j'en ferai un devoir autant qu'un plaisir. Je tiens à exprimer mes vifs remerciements et toute ma reconnaissance à Mr. Adjerid Smail, Professeur à l'université de Boumerdes, pour avoir assuré la direction de mes travaux et pour la qualité de son encadrement. Tout au long de ces années de thèse, il a su m'apporter son expérience et son soutien scientifique et moral.

J'exprime ma profonde reconnaissance à Mr. Benazzouz Djamel, Professeur à l'université de Boumerdes et directeur du Laboratoire de Mécanique des Solides et Systèmes (LMSS) , dont j'ai pu apprécier les qualités tant scientifiques qu'humaines. Merci de m'avoir écouté, de m'avoir fait confiance et surtout merci pour vos remarques très pertinentes.

Je suis très reconnaissant envers les membres du jury, d'avoir acceptés d'étudier mes travaux ainsi que pour l'intérêt et l'attention qu'ils ont accordés à cette étude.

Je souhaite de plus exprimer ma gratitude à Mr. ALLA Hacene, professeur au sein du laboratoire GIPSA LAB , Grenoble, qui m'a accueilli au sein du laboratoire.

Vient le tour de ceux avec qui j'ai partagé le bureau pendant ces années de thèse, merci pour de la bonne entente, la bonne ambiance et pour les nombreuses discussions intéressantes que nous avons eues.

" Sans eux, je ne serais pas là " n'est peut-être pas original au moment de remercier mes deux plus ardents supporteurs, mais c'est le moyen le plus concis que j'ai pu trouver pour rendre hommage à mes parents, les mots ne suffiront jamais à les remercier, ils m'ont accompagnés, soutenus et encadré depuis toujours. Cette thèse est le fruit de votre soutien...

Tous mes remerciements sont à mon frère, ma sœur, mon beau frère et mes amis, qui m'ont soutenus, aidés dans les moments les plus difficiles, sans eux et leur soutien, cette thèse n'aurait pas abouti.

Merci à mon fiancé d'y avoir cru, de m'avoir encouragé, d'avoir contribué à ce que tout se passe pour le mieux.

Je garderai le meilleur pour la fin, c'est à mon grand père que dieu ait son âme que je dédie ce mémoire Tu resteras toujours dans mes pensées grand-père ...

Merci à tous !

Résumé Les systèmes mécatroniques sont de plus en plus intégrés dans les applications actuelles. Cependant, la complexité croissante des systèmes mécatroniques, liée à l'augmentation du nombre de reconfiguration et de la forte interaction entre les composants, nécessite une adaptation des méthodes et outils existants pour mieux répondre aux exigences relatives à la sûreté de fonctionnement. Pour ce faire, une approche de recherche des scénarios critiques basée sur la modélisation préalable d'un système mécatronique sous la forme d'un Réseau de Petri et d'un ensemble d'équations différentielles a été développée, puis, en s'inspirant des concepts de la Logique Linéaire, il a été possible de concevoir un outil d'investigation visant à extraire tous les scénarios critiques. Une simulation Monte Carlo est proposée par la suite afin d'estimer la probabilité d'occurrence de chaque scénario.
Mots clés : Système complexe, sureté de fonctionnement, Réseau de Petri, Logique Linéaire, Simulation Monte Carlo.

Abstract Mechatronic systems are more and more integrated in today's applications. However, the increasing complexity of mechatronic systems, linked to the increasing number of reconfigurations and the strong interaction between components, requires an adaptation of existing methods and tools to meet the dependability requirements. For this purpose, a critical scenario search approach based on a preliminary modeling of a mechatronic system in the form of a Petri net and a set of differential equations has been developed. Then, using the concepts of Linear Logic, it has been possible to design an investigation tool aiming to extract all the critical scenarios. A Monte Carlo simulation is then proposed in order to estimate the occurrence probability of each scenario.
Keywords : Complex system, reliability, Petri nets, Linear Logic, Monte Carlo Simulation.

.

الملخص: أصبحت أنظمة الميكاترونيك أكثر اندماجًا في التطبيقات الحالية. ومع ذلك، فإن التعقيد المتزايد لأنظمة الميكاترونيك، المرتبط بزيادة عدد عمليات إعادة التشكيل والتفاعل القوي بين المكونات، يتطلب تكييف الأساليب والأدوات الحالية لتلبية المتطلبات المتعلقة بالسلامة التشغيلية بشكل أفضل. من أجل ذلك، تم تطوير نهج للبحث في السيناريوهات الحرجة استنادًا إلى التصميم السابق لنظام الميكاترونيك في شكل شبكة بتري ومجموعة من المعادلات التفاضلية، كما ان الاستلهام من مفاهيم المنطق الخطي مكّن من تصميم أداة تحقيق تهدف إلى استخراج جميع السيناريوهات الحرجة. بعد ذلك، ومن أجل تقدير احتمال حدوث كل سيناريو، تم اقتراح محاكاة مونت كارلو.

الكلمات المفتاحية: نظام معقد، سلامة تشغيلية، شبكة بتري، منطق خطي، محاكاة مونت كارلو

Table des matières

Table des figures **vi**

Liste des tableaux **ix**

Introduction generale **1**

I Sûreté de fonctionnement des systemes complexes **4**
I.1 Introduction 4
I.2 Systèmes 4
I.2.1 Systemes mécatroniques 5
I.3 Conception d'un système : Cycle de développement 7
I.3.1 Ingénierie système 9
I.4 Sûreté de fonctionnement des systemes : Concepts et définitions 10
I.5 Sécurité, Risque et Danger 11
I.5.1 Mesure du risque 13
I.6 Conclusion 15

II État de l'art sur les méthodes d'analyse des risques **16**
II.1 Introduction 16
II.2 Méthodes d'analyse des risques 16
II.2.1 Méthodes graphiques 17
II.2.2 Approches à base de modèles transformation 27
II.2.3 Approches basées sur la modélisation utilisant des modèles formels 33
II.3 Synthèse 42
II.4 Conclusion 44

III Modélisation et analyse des risques des systemes mécatroniques **45**
III.1 Introduction 45
III.2 Analyse fonctionnelle 45
III.2.1 Analyse fonctionnelle externe 46
III.2.2 Analyse fonctionnelle interne 48
III.3 Analyse dysfonctionnelle 51
III.4 Modélisation des systemes dynamiques hybrides 51

III.4.1 Extension de techniques de modélisation issue des systèmes continus . . . 52
III.4.2 Extension des techniques de modélisation issue des systèmes discrets . . . 52
III.4.3 Les approches mixtes . . . 53
III.4.4 Exemple de la modélisation d'un système mécatronique . . . 59
III.4.5 Réseau de Petri du système ABS . . . 71
III.5 Analyse qualitative :Extraction des scénarios critiques . . . 76
III.5.1 Scénario Critique . . . 77
III.5.2 Limites des outils d'analyse des RdP . . . 78
III.5.3 Logique linéaire . . . 81
III.5.4 Transcription du RdP en LL . . . 85
III.5.5 Démarche algorithmique . . . 91
III.5.6 Structure de l'algorithme proposé . . . 97
III.6 Analyse quantitative : estimation de la probabilité d'occurrence des scénarios critiques . . . 98
III.6.1 Concepts de base de la simulation Monte Carlo . . . 98
III.7 conclusion . . . 102

IV Application **105**
IV.1 Introduction . . . 105
IV.2 Système de refroidissement des bacs de stockage des fluides inflammables 105
IV.3 Modélisation . . . 107
IV.3.1 Analyse fonctionnelle . . . 107
IV.3.2 Analyse dysfonctionnelle . . . 109
IV.3.3 Détermination des équations différentielles . . . 113
IV.3.4 Modèle RdP du système . . . 116
IV.4 Mise en œuvre de l'algorithme . . . 119
IV.5 Simulation Monte Carlo . . . 123
IV.6 Discussion . . . 126
IV.6.1 Analyse qualitative . . . 126
IV.6.2 Analyse quantitative . . . 129
IV.7 Conclusion . . . 130

V Stratégie de maintenance **132**
V.1 Introduction . . . 132
V.2 Typologie et politique de maintenance . . . 133
V.2.1 La maintenance préventive . . . 133
V.2.2 La maintenance corrective . . . 134
V.2.3 Synthèse . . . 135
V.3 Construction d'une stratégie de maintenance . . . 136
V.3.1 Niveaux de maintenance . . . 136
V.3.2 Recommandations pour la conception d'une stratégie de maintenance . . . 143

V.4 Évaluation d'une stratégie de maintenance 144
V.4.1 Modèles de base d'une stratégie de maintenance 145
V.4.2 Catégorisation des modèles d'évaluation des stratégies de maintenance 147
V.5 Conclusion 148

VI Conclusion générale **149**

Bibliographie **152**

Table des figures

I.1 Éléments constitutifs d'un système mécatronique. 5
I.2 Exemple de l'aspect hybride[1] 6
I.3 Cycle de développement en V 7
I.4 Courbe de Farmer 13

II.1 Arbre de défaillance. 17
II.2 Arbre de défaillance dynamique. 20
II.3 Diagramme état-temps pour la porte PAND 22
II.4 Exemple d'un BDMP 24
II.5 Application de la méthode des graphes des flux dynamiques. 25
(a) Exemple d'un modèle DFM 25
(b) Tableaux de décision 25
(c) Arbre de défaillance temporisé. 25
II.6 Méthode MéDISIS [64] 29
II.7 Exemple d'un graphe de Markov 34
II.8 Exemple d'un automate 36
II.9 Exemple d'un réseau de Petri 38
II.10 Indication de la méthode d'analyse en fonction du modèle RdP. 42

III.1 Formalisation du besoin par une bête à cornes [1] 47
III.2 schéma de pieuvre [1] 47
III.3 Formalisation de l'analyse fonctionnelle externe par le diagramme de cas d'utilisation. 48
III.4 Actigramme [1]. 49
III.5 Analyse fonctionnelle interne par le diagramme de classes 50
III.6 RdP Hybride 52
III.7 Principe des réseaux de Petri Prédicats-Transitions Différentiels 56
III.8 Communication entre les classes du RdP PTDS-OO 59
III.9 Les composants du système ABS. 60
III.10 Principe de fonctionnement du système ABS :freinage normal 61
III.11 Principe de fonctionnement du système ABS :Blocage de roue 61
III.12 Principe de fonctionnement du système ABS :refoulement de liquide de freinage 62

III.13Diagramme de cas d'utilisation du système ABS. 63
III.14Diagramme de classes 64
III.15Efforts agissant sur une roue freinée 71
III.16Glissement en fonction du coefficient de frottement. 73
III.17Classe C1 du Réseau de Petri du système ABS. 74
III.18Réseau de Petri des électrovannes. 75
(a) Réseau de Petri de l'EV 75
(b) Réseau de Petri de l'EV_1 75
(c) Réseau de Petri de l'EV_2 75
III.19Classe C3 du Réseau de Petri du système ABS. 76
III.20a)Exemple d'un RdP. b)Début de construction du graphe des marquages partiel associé au modèle. c)Suite de la construction du graphe des marquage. 79
III.21Règles du calcul des séquents relatives aux connecteurs :$\multimap, \parr, \&$ 84
III.22Franchissement en séquence. 89
III.23Franchissement en parallèle 90
III.24Franchissement en conflit 91
III.25Extraction des transitions dans un RdP. 94
(a) Exemple d'un RdP 94
(b) Extraction détaillée des transitions 94
III.26Organigramme de l'algorithme de la simulation Monté Carlo. 103

IV.1 Les composants du système de refroidissement des bacs de stockage. . . . 107
IV.2 Diagramme de cas d'utilisation du système. 108
IV.3 Diagramme de classes 109
IV.4 Transfert de chaleur entre l'air ambiant et le fluide stocké dans les bacs . 113
IV.5 Écoulement d'eau 115
IV.6 Modèle globale du système de refroidissement des bacs de stockage 117
IV.7 Scénario critique : incendie dans le bac 1 120
IV.8 Scénario critique : incendie dans le bac 2 121
IV.9 Scénario critique : débordement du réservoir 1 121
IV.10Scénario critique : débordement du réservoir 1. 122
IV.11Scénario critique : débordement du réservoir 2. 122
IV.12Scénario critique : débordement du réservoir 2. 123
IV.13Probabilité d'occurrence des scénarios critiques. 124
(a) Sc_1 124
(b) $Sc_{3.1}$ 124
(c) $Sc_{3.2}$ 124
IV.14Probabilité d'occurrence des Scénarios critiques Sc_1, Sc_{31} et Sc_{32} en fonction de la durée T 125
(a) Shéma eclaté 125
(b) Schéma global 125
IV.15Arbres de défaillances. 127
(a) Arbre de défaillance de l'incendie dans le bac de stockage 1 127

(b) Arbre de défaillance du débordement du réservoir 1 127
IV.16Graphe des marquages du modèle RdP du système étudié. 128
IV.17Graphe des marquages partiel associé au modèle du système étudié. . . . 129
(a) Première étape du tracé du graphe d'accessibilité 129
(b) Suite du tracé du graphe d'accessibilité. 129

V.1 Exemple de typologie de maintenance 135
V.2 Fonction d'intensité pour une maintenance ABAO et AGAN 146
(b) maintenance AGAN 146
V.3 Politique de maintenance et ses facteurs d'influence 147

Liste des tableaux

I.1 Matrice de criticité 13
I.2 Échelles de fréquence d'occurrence selon la norme NF EN 50126 14
I.3 Échelles de gravité selon la norme NF EN 50126 15

III.1 Tableau AMDE 51
III.2 L'AMDE du système ABS 66
III.2 L'AMDE du système ABS 67
III.2 L'AMDE du système ABS 68
III.2 L'AMDE du système ABS 69
III.2 L'AMDE du système ABS 70

IV.1 L'AMDE du système de refroidissement des bacs de stockage des fluides inflammables 110
IV.4 Valeurs des paramètres utilisés pour la simulation MC 123
IV.5 Résultats de la simulation MC 125
IV.6 Séquence de chaque scénario 126
IV.7 Comparaison entre la simulation du modèle global et la simulation par sauts 130

V.1 Niveaux de maintenance 138

Acronymes

AADL	Architecture Analysis & Design Language
ABAO	As Bad As Old
ABS	Système d'antiblocage des roues
ADD	Arbre de Défaillance Dynamique
AFE	Analyse Fonctionnelle Externe
AFI	Analyse Fonctionnelle Interne
AGAN	As Good As New
AMDE	Analyse des Modes de Défaillance et de leur Effets
APTE	APplication aux Techniques d'Entreprise
ASH	Automates Stochastiques Hybrides
BDD	Binary Decision Diagram
BDMP	Boolean logic Driven Markov Processes
CCMT	Cell-to-Cell Mapping Technique
DFM	Dynamic Flowgraph Methodology
ECU	Unité de Commande Electronique
EV	Electrovannes
FC	Fonction de Contrainte
FP	Fonction Principale
FS	Fonction Secondaires
MC	Monte Carlo
OCL	Object Constraint Language
OO	Orienté Objets
RdP	Réseau De Petri
RDP PTD	Reseaux de Petri Prédicats Transitions Différentielles
RdP PTDS	Reseaux de Petri Prédicats-Transitions Différentiels stochastiques
RdPS	Réseau de Petri Stochastique
RdPSC	Reseau de petri stochastiques colorés
RdPSG	Réseau de Petri Stochastique Généralisé
RdPSGE	Réseaux de Petri Stochastiques Généralisés étiquetés
RdPT	Réseaux de Petri Temporisés
SADT	Structured Analysis and Design Technique
SC	Scénario Critique
SdF	Sûreté De Fonctionnement
SysML	System Modelling Language
UML	Unified Modeling Language

Introduction

De nos jours, les systèmes mécatroniques envahissent notre quotidien. Beaucoup de fonctions, jadis, réalisées manuellement sont aujourd'hui automatisées grâce à l'électronique et l'informatique. Ceci a apporté des améliorations notables en termes de confort, un confort auquel, il est de plus en plus difficile de renoncer.
Ces systèmes cumulent les avantages de chacune des technologies mécanique, hydraulique et électronique pour réaliser une fonction donnée en gérant au mieux les ressources.

La préoccupation actuelle 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. Cependant, afin de garantir un niveau de sécurité convenable, des études de sûreté de fonctionnement doivent être menées de la phase conception à la phase exploitation.

— Dans la phase conception, afin de valider ou non l'architecture du système en réduisant ainsi le temps et le coût de la conception.En effet, la phase de conception doit être rapide et peu coûteuse (le moins de prototypes possible)avec un niveau de sécurité garanti.De plus, les ressources en moyens matériels étant limitées, pour des raisons de coûts et de mise en œuvre, ces analyses aident les concepteurs à éviter au maximum les redondances matérielles.

— Pendant la phase exploitation, afin de choisir la meilleure stratégie de maintenance possible.

Cependant, la complexité croissante des systèmes mécatroniques, liée à l'augmentation du nombre de reconfiguration et de la forte interaction entre les composants, nécessite une adaptation des méthodes et outils existants pour mieux répondre aux exigences relatives à la sûreté de fonctionnement. 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 et réaliste des dépendances. Dans de tels systèmes, la séquence de fonctionnement normal ou dangereux résulte de l'occurrence commune de deux types d'événements. Les premiers sont liés à l'évolution déterministe des paramètres physiques susmentionnés, alors que les deuxièmes sont dus aux sollicitations et aux défaillances des composants du système et sont donc de nature aléatoire. Les méthodes classiques de 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.Il ne suffit donc plus de composer les défaillances des différents sous-systèmes pour avoir l'ensemble des scénarios critiques du système global mais il faut chercher les scénarios en se basant sur une modélisation du système complet incluant les interactions entre les sous-systèmes.

Objectif de la thèse et contribution Les travaux développés au cours de cette thèse porte sur l'analyse des risques des systèmes mécatroniques. Nous proposons une approche visant l'analyse qualitative et quantitative de ces systèmes en vue de l'obtention des scénarios critiques et de l'estimation de leurs probabilité d'occurrence. La connaissance de ces scénarios permet de les évaluer et de valider les lois de reconfiguration pour orienter le choix des concepteurs quant aux différents types d'architectures possibles proposées pour le système à concevoir mais aussi de choisir la meilleure stratégie de maintenance.
Nous avons développé une approche de recherche des scénarios basée sur la modélisation préalable d'un système mécatronique sous la forme d'un Réseau de Petri et d'un ensemble d'équations différentielles. Cette modélisation hybride présente l'avantage de séparer clairement les aspects discrets et continus. Cependant les outils d'analyse dont ils disposent sont limités dans l'interprétation du modèle pour expliquer les phénomènes indésirables. La contrainte majeure est la difficulté (ou l'impossibilité) de différencier entre les relations de *cause* et de *précédence* à partir du marquage d'accessibilité. La connaissance de ces relations est primordiale car elle favorise largement la compréhension et l'analyse des risques industriels rencontrés. Face a ce constat, en s'inspirant des

concepts de la Logique Linéaire, il est possible de concevoir un outil d'investigation visant à extraire tous les scénarios critiques. À cet effet, nous procédons à la sélection et à l'adaptation de connecteurs et de règles destinés à la transcription de la structure et de la dynamique du Réseau de Petri. Les franchissements des transitions jusqu'au marquage critique génèrent progressivement des arbres d'où seront extraits les scénarios critiques.Par la suite une simulation Monte Carlo est proposée afin d'estimer la probabilité d'occurrence de chaque scénario. L'un des principaux avantages de l'approche proposée est son efficacité dans la sélection et le traitement des seules séquences du modèle ayant effectivement une influence sur l'avènement des situations critiques. Ce qui réduit fortement le nombre de cas à examiner et la durée de la simulation.

Organisation de la thèse Ce manuscrit est composé de cinq chapitres. Nous introduirons dans le premier chapitre quelques notions relatives à la sûreté de fonctionnement ainsi que les caractéristiques des systèmes mécatroniques.
Dans le deuxième chapitre, un état de l'art des méthodes et des travaux réalisés en vue d'une étude d'analyse des risques sont présentés.Ce chapitre se conclut par une synthèse mettant en valeur les point positifs de chaque méthode et permettant ainsi de faire les choix nécessaires pour la conception de l'approche.
Le chapitre trois, présentera les principales méthodes de modélisation des systèmes dynamiques hybride à l'issue duquel nous choisirons le modèle " états-transitions " adéquat pour notre problématique : les réseaux de Petri plus précisément le formalisme Prédicats Transitions Différentiels Stochastiques (RdP PTDS).Nous introduisons ensuite l'approche de recherche de scénarios critiques que nous avons développée. Elle est basée sur l'utilisation des concepts de la logique linaire pour le développement d'un outil d'investigation visant l'extraction des scénarios critiques à partir du modèle Réseau de Petri. Ensuite, sera présentée l'analyse quantitative, associant Réseau de Petri et simulation Monte Carlo pour l'estimation de la probabilité d'occurrence de chaque scénario.
Le quatrième chapitre portera sur l'application de l'approche sur le système de refroidissement des bacs de stockage des fluides inflammables.
Enfin, le cinquième et dernier chapitre est consacré à une réflexion approfondie sur le choix d'une stratégie de maintenance appropriée.

Chapitre I

Sûreté de fonctionnement des systemes complexes

I.1 Introduction

Dans ce chapitre, nous nous intéresserons aux systèmes complexes notamment le cas des systèmes mécatroniques. En passant par une présentation du cycle de développement d'un système où nous exposons brièvement la nouvelle démarche de conception des systèmes complexes, une synthèse des principaux concepts de base de la sûreté de fonctionnement ainsi que différentes notions permettant de préciser le cadre et le contexte de nos travaux sont exposées, à l'image de la sécurité du danger et du risque.

I.2 Systèmes

Depuis toujours, l'homme invente et conçoit des instruments, des équipements, ... pour améliorer ou faciliter sa vie. Ces fabrications, qu'on appelle systèmes, sont un ensemble d'éléments interagissant entre eux selon certains principes ou règles afin de remplir les missions pour lesquelles ils ont été conçus. Dans la littérature, nous pouvons trouver plusieurs définitions sur les systèmes. Parmi lesquelles, on peut citer :

Définition 1 *Système : Un système est un ensemble composé de personnels, de matériels et de logiciels organisés pour que leur inter-fonctionnement permette, dans un environnement donné, de remplir les missions pour lesquelles il a été conçu.*

□

Les premiers systèmes étaient relativement simples. Ainsi, la structure interne de la conception était très facilement compréhensible. Puis, ils ont sans cesse évolué en devenant de plus en plus élaborés et compliqués, surtout depuis le début de l'ère industrielle où les systèmes dit complexes voient le jour.

Définition 2 *Système Complexe : un système complexe est un système composé d'un grand nombre d'éléments de plusieurs types, reliés par des interactions non linéaires.Ces systèmes modifient constamment leur structure interne, en conséquence, ils sont flexibles et s'adaptent facilement à des conditions externes variables.*

□

Parmi les systèmes complexes on peut citer les ***systèmes mécatroniques*** sur lesquels se focalise le travail de la présente thèse.

I.2.1 Systemes mécatroniques

Un système mécatronique est un système combinant des technologies qui relèvent des domaines de la mécanique, de l'hydraulique, de l'électronique et de l'informatique. Il peut être décomposé en quatre entités en interaction (fig I.1) : les capteurs, la partie opérative, le système de commande et de reconfiguration et les actionneurs.

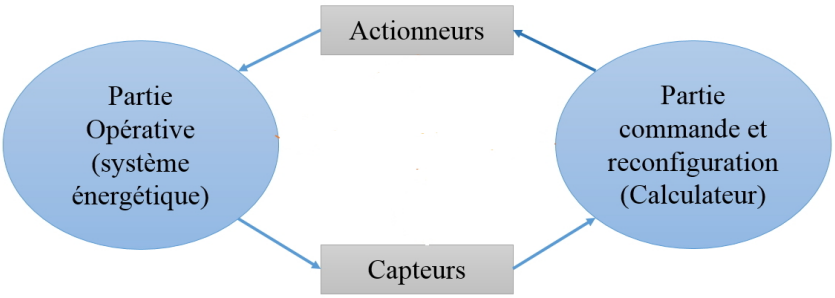


FIGURE I.1: Éléments constitutifs d'un système mécatronique.

Les capteurs mesurent des grandeurs physiques continues caractéristiques de la partie opérative. Le système de commande et de reconfiguration établit en fonction de ces mesures les actions à réaliser. Les actionneurs agissent sur la partie opérative.
Le système de commande a aussi pour objectif d'assurer que certaines grandeurs de la

partie opérative soient maintenues dans un intervalle de sécurité. Lorsque certains événements relatifs à la sécurité du système se produisent, comme le franchissement d'un seuil de sécurité par une variable caractéristique de la partie opérative, des actions sont mises en œuvre de façon à reconfigurer la partie opérative et à ramener les grandeurs caractéristiques de celle-ci dans les limites permises.
Les systèmes mécatroniques sont, par leur nature même, des systemes dynamiques hybrides.

Aspect hybride

L'aspect hybride d'un système mécatronique est caractérisé par la présence de phénomènes continus et d'événements discrets (franchissement de seuil, séquence d'événement ou la combinaison des deux).
La description de ces systèmes mécatroniques peut faire intervenir explicitement et simultanément un état continu et un état discret.

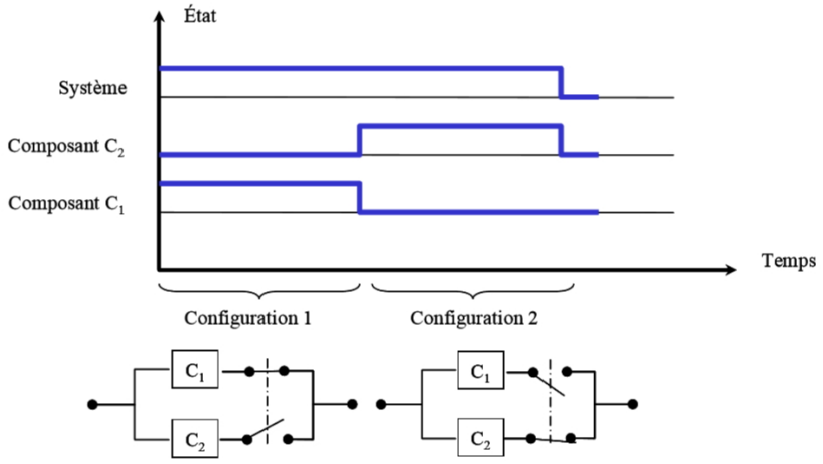


FIGURE I.2: Exemple de l'aspect hybride[1]

Un exemple d'un système hybride [1] (fig I.2) est un système comportant une redondance passive. Le système fonctionne en continu alors que l'utilisation des composants C_1 et C_2 est discrète ou périodique. Le fonctionnement est assuré par le composant C_1 alors que le composant C_2 est au repos. Lorsque le système détecte la défaillance de C_1, le composant C_2 est actionné afin d'assurer la continuité du 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 que

certaines variables peuvent présenter un caractère aléatoire telles que les défaillances des composants.

Aspect dynamique

L'aspect dynamique d'un système mécatronique est caractérisé par l'évolution de son état avec le temps.
Les spécificités des systèmes mécatroniques sont liées au fait qu'ils sont reconfigurables et la décision de reconfiguration est prise par le système lui-même.Ceci consiste à changer sa configuration fonctionnelle afin de maintenir la réalisation de la fonction. Dans certains cas, cette reconfiguration assure le fonctionnement en mode dégradé tout en assurant la sécurité des utilisateurs.

I.3 Conception d'un système : Cycle de développement

Le cycle de développement le plus connu et le cycle en V présenté sur la figure I.3.

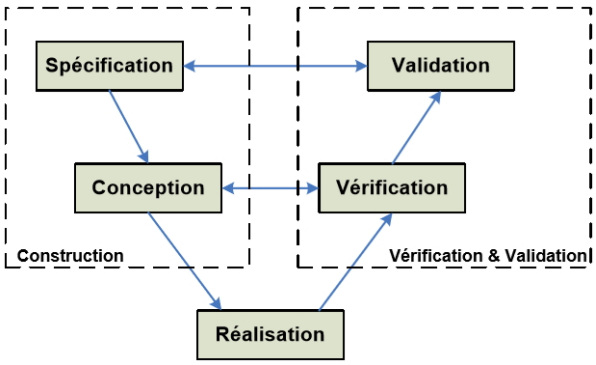


FIGURE I.3: Cycle de développement en V

Le développement commence par la partie construction du système, c'est la partie descendante du cycle en V[2], 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 et Validation 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 (figure I.3).

- **Spécification** : 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 faisabilité souhaitée du système.
- **Conception** :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.
- **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.
- **Vérification** :Dans cette phase tous les modules ou sous-systèmes sont vérifiés et testés par rapport à la conception.
- **Validation** :Il s'agit d'une validation fonctionnelle, une phase importante, où sont constatées les fonctionnalités et le niveau de qualité par rapport aux spécifications/analyse de besoins.

Le piège de ce cycle en V est la linéarité apparente d'une succession séquentielle des opérations. Car il n'en est rien. En pratique, il y a de nombreuses rétroactions des phases aval vers les phases amont, suite à des découvertes tardives d'erreurs obligeant à remettre en question des phases préalablement validées ou suite à une demande de modification d'exigences ou une évolution du marché par exemple [3].
De plus, la complexité des systèmes actuels a forcé les concepteurs à adopter et à s'adapter à une méthode de développement bien plus organisée et rigoureuse. Cette nouvelle façon d'aborder la conception, nécessaire pour maîtriser cette complexité grandissante est l'Ingénierie Système.
Le processus d'Ingénierie Système ordonnance les tâches à réaliser pour obtenir le système désiré. Lors de la conception de nouveaux systèmes complexes, les projets revêtent aujourd'hui un caractère pluridisciplinaire. De plus en plus, les systèmes sont aujourd'hui co-produits par des équipes projets réparties dans plusieurs services de l'entreprise ou associant plusieurs entreprises sur un projet commun.L'ingénierie système aborde la conception dans sa globalité. Partant des souhaits exprimes par le client, elle permet, par étapes successives, validées les unes après les autres, d'aboutir à la définition des

organes et composants prenant place dans une architecture optimisée. Elle permet de faire face plus facilement et plus rapidement aux modifications dans le processus de développement du système.

I.3.1 Ingénierie système

L'Ingénierie Système [4, 5] est une approche méthodologique qui a été développée et est en amélioration continue pour permettre au concepteur de système complexe d'aboutir à une solution équilibrée au moindre coût et délais et répondant au mieux aux besoins des différentes entités concernées par l'utilisation du système (les clients, les agents de maintenance, d'autres systèmes,...). D'après la norme IEEE P1220 [6], l'Ingénierie Système est une approche interdisciplinaire et concerne la capacité de réussir la réalisation des systèmes.
L'approche générale lors de la conception d'un système complexe incluant de nouvelles technologies, se base sur des standards permettant d'accomplir la mission durant le développement. Parmi ces standards, on peut citer : IEEE 1220[6], EIA632[7] et ISO 15288[8].

Lors du développement d'un système, le constructeur spécifie non seulement les fonctionnalités, mais aussi les objectifs à atteindre en terme de sûreté de fonctionnement. Ainsi, il est de plus en plus nécessaire d'intégrer la sûreté de fonctionnement [9] dès la première phase du cycle de développement. Traditionnellement, la satisfaction des exigences de sûreté de fonctionnement est validée après des tests sur des prototypes réels. C'est à ce stade que nous détectons les erreurs de conception et/ou la non-satisfaction des exigences. Afin de diminuer le nombre de prototypes nécessaires à la validation des systèmes conçus, les études de sûreté de fonctionnement doivent être menées au plus tôt dans le cycle de développement avant que les choix de conception ne soient figés.
Il est à préciser que l'étude de la sûreté de fonctionnement ne se limite pas à la seule étape du développement du produit. En effet, elle agit sur tout le cycle de vie du système, depuis la phase de conceptualisation jusqu'à celle de retrait de service. En effet, l'étude de la sûreté de fonctionnement apporte une contribution significative à la prise de décision :

— Lors de la phase développement : l'étude permet de valider la conception du système.

— Pendant le cycle d'exploitation : permet de minimiser le coût de maintenance et

de fournir tous les éléments nécessaires à l'élaboration d'un plan de maintenance préventive pertinent.

I.4 Sûreté de fonctionnement des systemes : Concepts et définitions

Définie par Villmeur [9] comme la science des défaillances, la sûreté de fonctionnement est l'aptitude d'une entité à satisfaire une ou plusieurs fonctions requises dans des conditions données.
Les études de sûreté de fonctionnement (désignée par la suite SdF) ont pour finalité le maintien du bon fonctionnement d'un système, d'un produit ou d'un de ses constituants, tout au long de son cycle de vie.
La SdF d'une entité est caractérisée à travers différents attributs,sur lesquels un concepteur mettra plus ou moins l'accent suivant le type d'utilisation du système : ***la fiabilité, la maintenabilité, la disponibilité, la sécurité.***

Définition 3 ***Fiabilité[10] :*** *La fiabilité est l'aptitude d'une entité à accomplir les fonctions requises dans des conditions données pendant une durée donnée. Elle est caractérisée par la probabilité $R(t)$ que l'entité E accomplisse ces fonctions, dans les conditions données pendant l'intervalle de temps $[0,t]$, sachant que l'entité n'est pas en panne à l'instant 0.*

$$R(t) = P[E \quad non \quad dfaillant \quad sur \quad [0,t]] \tag{I.1}$$

□

Définition 4 ***Disponibilité [10] :*** *La disponibilité est l'aptitude d'une entité à être en état d'accomplir les fonctions requises dans les conditions données et à un instant donné. Elle est caractérisée par la probabilité $A(t)$ que l'entité E soit en état, à l'instant t, d'accomplir les fonctions requises dans des conditions données.*

$$A(t) = P[E \quad non \quad dfaillant \quad \quad l'instant \quad t] \tag{I.2}$$

□

Définition 5 ***Maintenabilité [10] :*** *La maintenabilité 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 réalisée dans des conditions données avec des procédures et des moyens prescrits. Elle est caractérisée par la probabilité $M(t)$ que l'entité E soit en état, à l'instant t, d'accomplir ses fonctions, sachant que l'entité était en panne à l'instant 0.

$$M(t) = P[E \ \ est \ \ rparable \ \ sur \ \ [0,t]] \tag{I.3}$$

□

Définition 6 ***Sécurité [10] :*** *La sécurité est l'aptitude d'une entité à éviter de faire apparaitre, dans des conditions données, des événements critiques ou catastrophiques. Elle est caractérisée par la probabilité $S(t)$ que l'entité E ne laisse pas apparaitre dans des conditions données, des événements critiques ou catastrophiques.*

$$S(t) = P[E \ \ evite \ \ des \ \ evenements \ \ critiques \ \ ou \ \ catastrophiques \ \ sur \ \ [0,t]] \tag{I.4}$$

□

Il est à noter que dans le domaine de l'informatique, la sécurité a souvent deux facettes : la sécurité-innocuité (Safety) qui vise à se protéger des défaillances catastrophiques et la sécurité-confidentialité (Security) qui correspond à la prévention d'accès ou de manipulations non autorisées de l'information.

I.5 Sécurité, Risque et Danger

D'après la norme ISO/IEC GUIDE 51 :2014 [11] qui traite les aspects liés à la sécurité,la définition de sécurité est donnée comme suit :

Définition 7 *Sécurité : absence de risque intolérable.*

□

La considération de la sécurité repose essentiellement sur le concept de risque.En effet, l'évaluation de la sécurité est un exercice qui ne peut être effectué sans la connaissance du risque. Une définition du risque est proposée par Villemeur [9] comme suit : le risque est une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences.

□

Ceci-dit dans la suite de ce manuscrit nous retenons la définition donnée dans la norme PR NF EN 50126-1 [12] :

Définition 8 *Risque : le risque est une combinaison de la probabilité de la survenue d'un dommage et de sa gravité.*

□

Cependant il est essentiel de distinguer entre le risque et le danger. En effet, selon la norme NF EN 50126 [12] la définition du danger est donnée comme suit :

Définition 9 *Le danger est la source potentielle de dommage(blessure physique ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement).*

□

Selon le référentiel OHSAS 18001 [13] :

Définition 10 *Le danger est la source ou une situation pouvant nuire par blessure ou atteinte de la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments*

□

Pour la suite de ce manuscrit, nous proposons la définition suivante :

Définition 11 *Danger : Le danger est une situation pouvant provoquée un dommage.*

□

Synthèse : La sécurité s'articule sur le concept de risque plus précisément des informations relatives à la probabilité d'occurrence et à la gravité d'un dommage.
L'étude de la sécurité se base sur l'analyse du risque, qui consiste en l'identification des dangers c'est-à-dire l'identification des situations pouvant provoquées un dommage.

□

I.5.1 Mesure du risque

En s'appuyant sur la définition 8 retenue, le risque s'articule donc autour de deux concepts qui sont " la probabilité d'occurrence" et "la gravité". Farmer [14]a montré que la probabilité d'occurrence et la gravité étaient liées de façon linéaire. En effet, si nous représentons les mesures des risques des accidents susceptibles de survenir sur une grille nous obtenons la courbe de Farmer présentée dans la figure I.4. Ainsi, nous distinguons deux grandes catégories : les risques acceptables qui sont des risques courants, les risques inacceptables (moyens) et les risques majeurs.

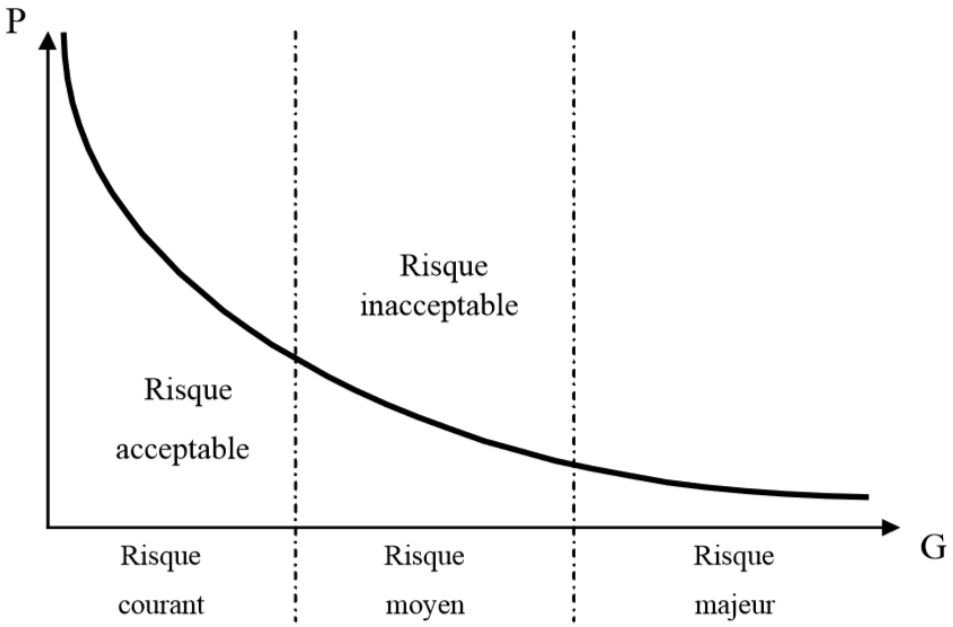


FIGURE I.4: Courbe de Farmer

Le risque peut aussi être mesuré à l'aide d'une matrice de criticité (tableau I.1). Celle-ci s'articule autour de "la fréquence d'occurrence" et de "la gravité".

TABLE I.1: Matrice de criticité

	Insignifiant	Marginal	Critique	Catastrophique
Invraisemblable	Négligeable	Négligeable	Négligeable	Négligeable
Improbable	Négligeable	Négligeable	Acceptable	Acceptable
Rare	Négligeable	Acceptable	Indésirable	Indésirable
Occasionnel	Acceptable	Indésirable	Indésirable	Inacceptable
Probable	Acceptable	Indésirable	Inacceptable	Inacceptable
Fréquent	Indésirable	Inacceptable	Inacceptable	Inacceptable

Afin de positionner les zones de risque, les niveaux de gravité et de fréquence d'occurrence sont croisés dans cette matrice. La matrice Gravité/Occurrence est proposée par la norme NF EN 50126 [12]. La fréquence d'occurrence (frequency)d'un événement est la mesure du nombre moyen d'occurrences attendues en un laps de temps donné dans des conditions connues. Cette fréquence est estimée sur une période de temps donnée (année, jour, heure, etc.).
Les classes de fréquence présentées dans la table suivante (voir TAB I.2) sont proposées dans la norme NF EN 50126 [12].

TABLE I.2: Échelles de fréquence d'occurrence selon la norme NF EN 50126

Niveau	**Description**
Invraisemblable	Extrêmement improbable. On peut supposer que la situation dangereuse ne se produira pas.
Improbable	Peu susceptible de se produire mais possible. On peut supposer que la situation dangereuse peut exceptionnellement se produire.
Rare	Susceptible de se produire à un moment donné du cycle de vie du système. On peut raisonnablement s'attendre à ce que la situation dangereuse se produise
Occasionnel	Susceptible de survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne à plusieurs reprises
Probable	Peut survenir à plusieurs reprises. On peut s'attendre à ce que la situation dangereuse survienne souvent
Fréquent	Susceptible de se produire fréquemment. La situation dangereuse est continuellement présente

La gravité (Severity) est une valeur subjective et est déterminée par la conséquence de l'événement sur les individus, les propriétés et sur l'environnement. Dans la majorité des domaines industriels, la gravité couvre aussi bien les dommages sur l'Homme et le Système, que les nuisances portées à l'Environnement. La norme (NF EN 50126) [12] propose quatre échelles de gravité (voir TAB. I.3) :

TABLE I.3: Échelles de gravité selon la norme NF EN 50126

Gravité	**Conséquences pour les personnes ou l'environnement**	**Conséquences pour le service**
Insignifiant	Éventuellement une personne légèrement blessée	
Marginal	Blessures légères et/ou menace grave pour l'environnement	Perte d'un système important.
Critique	Un mort et/ou une personne grièvement blessée grave et/ou des dommages graves pour l'environnement	Dommages graves pour un (ou plusieurs) système(s)
Catastrophique	Des morts et/ ou plusieurs personnes gravement blessées et/ou des dommages majeurs pour l'environnement	Dommages mineurs pour un système

I.6 Conclusion

Nous avons rappelé dans un premier temps le cycle de développement d'un système ou nous avons introduit brièvement la nouvelle démarche de conception des systèmes complexes. Nous avons présenté par la suite quelques concepts basiques de la sûreté de fonctionnement. Nous nous sommes attardé sur le concept Securité où nous avons repris les notations clés qui lui sont liées tels que le risque et le danger, En vue de bien assimiler le chapitre suivant, consacré aux méthodes de l'analyse des risques.

Chapitre II

État de l'art sur les méthodes d'analyse des risques

II.1 Introduction

L'analyse des risques est essentielle dès la phase conception d'un système, mais la complexité croissante des systèmes dynamiques hybrides, tels que les systèmes mécatroniques entraînent des difficultés liées à cette analyse.
Quand il s'agit d'évaluer le risque d'un système complexe et critique, deux questions sont fondamentales :

— Comment prendre en compte dans un modèle la nature du système étudié : les dépendances multiples entre les composants ainsi que la description du comportement du système en présence de fautes ?

— Comment obtenir des mesures qualitatives et quantitatives des risques à partir de ce modèle ?

Pour répondre à ces deux questions, plusieurs méthodes existes dont quelques-unes seront présentées dans cette section. D'une façon générale, ces méthodes d'analyse passent par une étape de modélisation suivie d'une étape analyse qualitative puis quantitative.

II.2 Méthodes d'analyse des risques

Les méthodes d'analyse des risques peuvent être répertoriées selon trois groupes :

— les méthodes graphiques ;

— les approches basées sur les modèles de transformation ;

— les approches basées sur les modèles formels.

Dans cette section, vont être présentés quelques travaux concernant ces méthodes, ainsi que notre orientation pour l'objectif fixé.

II.2.1 Méthodes graphiques

Méthode d'arbre de défaillance

La méthode de l'arbre de défaillance (Fault Tree en anglais) [9, 15, 16, 17, 18], connue aussi sous le nom d'arbre des causes, arbre des défauts ou arbre des fautes est fréquemment utilisée dans de nombreux domaines industriels (aéronautique, nucléaire, chimique). L'arbre de défaillance est un modèle permettant l'analyse prévisionnelle des risques des systèmes industriels. En effet, à l'aide d'une représentation graphique au moyen d'une structure arborescente et grâce à un raisonnement déductif cette méthode a pour objectif de déterminer les diverses combinaisons possibles d'événements qui entrainent la réalisation d'un événement indésirable préalablement bien défini.
Comme présenté dans la figure II.1, l'arbre de défaillance est formé de niveaux successifs d'événements tel que, chaque événement est généré à partir des événements du niveau inférieur par l'intermédiaire de diverses portes logiques. A la racine de l'arbre se trouve l'événement redouté (ou top event) et les feuilles de l'arbre désignent des évènements pouvant conduire à l'évènement indésirable. Ces événements sont généralement des défauts associés à des défaillances matérielles des composants élémentaires (ou événements de base) du système, des erreurs humaines, des défauts de logiciels...

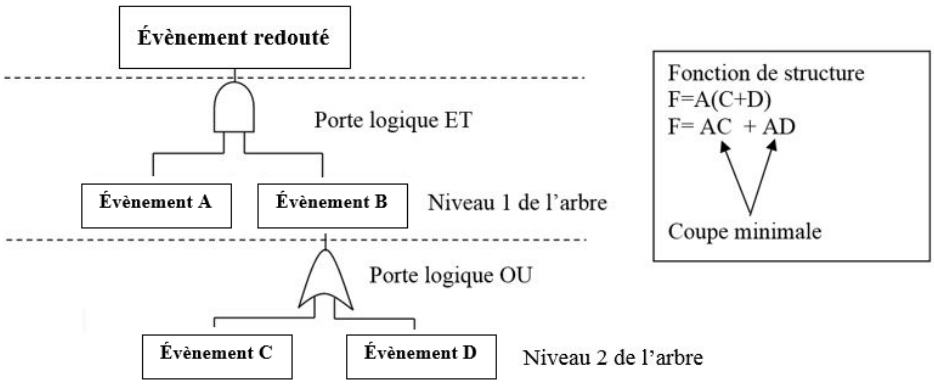


FIGURE II.1: Arbre de défaillance.

Analyse qualitative : L'analyse qualitative consiste en l'extraction des coupes minimales à partir de l'arbre construit. Une coupe est définie par Birnbaum [19] comme un ensemble de composants défaillants conduisant à la défaillance du système ; ces coupes sont un résultat uniquement déterminé par la structure du système. La notion de minimalité a été formalisée par Rauzy [20]. Une coupe minimale est donc la plus petite combinaison d'événements entrainant l'événement redouté, et si un des événements d'une coupe minimale ne se produit pas, l'événement indésirable ne se réalise pas.
La recherche des coupes minimales se fait à partir d'une transformation de l'arbre en une expression booléenne (nommée fonction de structure) entre les événements qui entrainent l'événement indésirable ainsi que par l'utilisation du théorème d'absorption de l'algèbre booléenne pour obtenir une expression booléenne réduite [21, 22].
Due au succès de l'arbre de défaillance, des techniques ont été développées pour l'analyse des arbres de défaillance de très grande taille. Afin d'éviter l'explosion combinatoire, la fonction de structure n'est plus alors représentée par une fonction booléenne mais par un arbre de décision binaire (Binary Decision Diagram, BDD) [23, 24] ou par l'utilisation des zero-suppressed BDD décrite dans [25, 26], dont l'utilisation est illustrée dans [27]. L'interprétation des coupes minimales donne un certain nombre de résultats qualitatifs comme les points faibles du système, les fausses redondances, l'influence d'un élément donné sur la fiabilité du système [4, 24].

Analyse quantitative : L'analyse quantitative permet d'évaluer la probabilité d'occurrence de l'événement redouté et s'effectue, lors de l'utilisation de l'arbre de défaillance, en associant des probabilités d'occurrence aux évènements de base. Une méthode d'évaluation de la probabilité d'occurrence de l'événement sommet(événement redouté), basée sur les diagrammes de décision binaire est présentée dans [23]. L'analyse quantitative permet donc de disposer de critères afin de déterminer les priorités pour la prévention d'accidents potentiels.
Plusieurs outils informatiques de sûreté de fonctionnement basés sur ce modèle sont disponibles : Aralia Fault Tree Analyzer (Dassault Systemes), FaultTree+ (Isograph), CAFTA (Electric Power Research Institute), etc. En général ces outils incluent une interface et des outils d'évaluation afin de calculer les coupes minimales et les probabilités des évènements.

Avantages et limites : Dans de nombreuses situations, le maître d'œuvre chargé de cette étude doit construire un modèle représentatif du comportement du système en présence de défaillances ; ce modèle doit être suffisamment abstrait pour ne contenir que des éléments pertinents et essentiels à l'évaluation recherchée. Ce modèle doit également être conçu afin d'être facilement interprétable par d'autres acteurs participant à la conception. Ainsi, les méthodes graphiques tels que les arbres de défaillance ont eu et ont toujours un succès dans le milieu industriel car la construction d'un modèle dysfonctionnel du système est relativement aisée et permet de visualiser instantanément les coupes minimales de défaillances conduisant à l'occurrence d'événements redoutés.
Cependant, ce type de méthode n'offre qu'une vision statique des combinaisons de défaillances. Basé sur la logique booléenne pour représenter le système étudié, l'arbre de défaillance est adapté à des systèmes à configuration statique, c'est-à-dire des systèmes dont les relations fonctionnelles entre leurs composants restent figées. L'emploi de celle-ci se révèle donc difficile, voir impossible pour l'étude des systèmes en interaction et fortement dépendants du temps.
De plus,cette méthode ne permet pas de différencier les scénarios comportant des ordres d'apparition d'événements différents. En effet, une séquence d'événements peut conduire à un événement redouté alors que les mêmes événements se produisant dans un ordre différent ou à des dates différentes n'y conduisent pas.
Aussi, le temps séparant deux événements n'est pas explicitement pris en compte dans la construction du scénario, on ne peut donc pas représenter les reconfigurations.
Enfin, il n'est pas possible de prendre en compte les défaillances temporaires.
Afin d'illustrer ces limites Moncelet [28] présente un exemple d'un système à deux composants en redondance passive. Ces deux composants (a et b) peuvent tomber en panne en service (défaillances notées respectivement def_a et def_b) et subir des réparations (notées respectivement rep_a et rep_b). La commutation d'un composant à un autre est supposée immédiate et fiable. L'événement redouté du système est l'absence de service. Le composant "a" étant le composant principal, les séquences suivantes ont des conséquences différentes : $s_1 = [def_a, def_b, rep_a]$ et $s_2 = [def_a, rep_a, def_b]$. En effet, la première séquence conduit inévitablement à l'événement redouté puisque les deux composants sont simultanément défaillants pendant un certain temps, par contre, durant (et même après) la séquence s_2, le système continue à délivrer un service. Cet exemple correspond exactement au cas des systèmes avec reconfiguration en l'occurrence les systèmes mécatroniques. Si une deuxième défaillance arrive avant la fin de la reconfiguration il y a

occurrence d'un événement redouté, dans le cas contraire tout se passe comme cela a été prévu.

Méthode d'arbre de défaillance dynamique

Les limites liées à l'utilisation de l'arbre de défaillance ont fait l'objet d'une étude approfondie par Dugan et all [29, 30] et ont proposés une extension de la méthode de l'arbre de défaillance, par l'ajout de nouvelles portes logiques (PAND, SPARE, FDEP, SEQ). Dugan et all [29, 30] proposent l'établissent ainsi de l'arbre de défaillance dynamique (ADD) présenté dans la figure II.2.

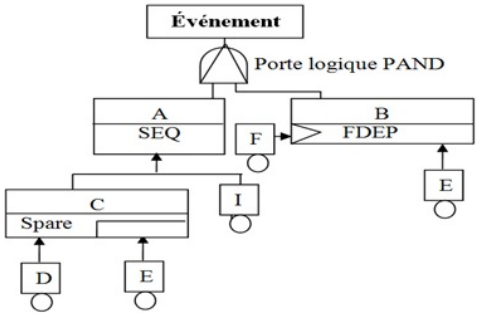


FIGURE II.2: Arbre de défaillance dynamique.

L'arbre de défaillance dynamique (ADD) est capable de représenter l'ordre d'occurrence des défaillances des composants ou des sous-système (porte PAND/ SEQ), de décrire les possibles redondances du système (porte SPARE) et aussi la dépendance entre les composants (porte FDEP). La valeur de sortie de ces nouvelles portes n'est plus seulement fonction de l'ensemble des composants défaillants en entrée de celles-ci, mais également de l'ordre dans lequel ces défaillances sont apparues.
Si on prend l'exemple de la figure II.2 l'événement redouté aura lieu si l'événement A se produit suivie de l'événement B (de gauche à droite). La porte PAND a permis de représenter une défaillance résultant d'une séquence d'événements prédéfinis.
L'événement A (porte SEQ) se produit quand l'événement C est suivie de l'événement I. la porte SEQ peut être comparée avec la porte PAND mais ces deux portes sont toutefois différentes. La PAND détecte en effet si les événements se produisent dans un ordre particulier, mais les événements peuvent se produire dans un autre ordre, au contraire la porte SEQ ne permet que la séquence d'événements qu'elle indique.
La porte Spare décrit de gauche à droite, le composant principal du sous-système, initialement actif suivi du composant de secours qui est initialement non-actives. L'événement

C (porte Spare) se produit quand le composant primaire D est défaillant et la redondance E l'est aussi.
L'événement B (porte FDEP) est déclenché par l'événement F, si l'événement F se produit, il entraine l'événement E.

Analyse qualitative : L'analyse qualitative associée à ce modèle n'a pas encore été développée. L'une des problématiques associées aux systèmes dynamiques dont l'étude des risques est réalisée à l'aide d'arbre de défaillance dynamique est l'inexistence d'une définition universelle, ni même consensuelle, des séquences de coupes minimales.
Tang et all [27] ainsi que Merle et all [31, 32]proposent deux méthodes pour le calcul des séquences de coupe minimales. Par l'application de ces méthodes, les séquences de coupes sont obtenues sous leur forme implicite, ceci par un ensemble de conditions qu'elles doivent respecter, et non sous une forme explicite. De même, aucune réelle définition de ces séquences de coupe n'est proposée quant à leurs propriétés pour l'analyse du système, ce qui peut engendrer des écarts quand aux résultats obtenus [33].

Analyse quantitative : Lors de l'analyse quantitative, la partie statique de l'arbre de défaillance dynamique est traitée de manière classique à l'aide du BDD [34], tandis que pour la partie dynamique, l'analyse consiste en la traduction automatique des ADD vers les chaines de Markov comme parue dans[29, 35] et illustrée dans [36], ou bien par la description de l'ADD sous forme d'un réseau de Petri stochastique (RdPS) [37].

Limites : Par l'utilisation des chaines de Markov, le nombre d'état augmente à chaque fois que le nombre des portes d'entrées augmente. De plus le modèle de Markov est applicable seulement pour des lois de défaillance et de réparation exponentielles. Pour aborder ces difficultés Rao et all [38] présentent une approche basée sur la simulation Monte Carlo [1] en spécifiant le comportement des défaillances temporelles et réparation à travers un diagramme état-temps comme illustré dans la figureII.3 qui prend exemple de la porte PAND ayant deux composants A et B.
Par la définition et l'introduction des nouvelles portes, un ADD permet de modéliser certains types de séquences d'événements (en fonction des portes utilisées dans leur construction) et de calculer leurs probabilités d'occurrence, notamment pour des sys-

1. Méthode qui permet de calculer la valeur numérique d'une variable en utilisant des tirages de nombres aléatoires à partir de distributions statistiques.

tèmes constitués de composants binaires non-réparables. Néanmoins, les séquences d'événements relatives à des systèmes réparables ne peuvent pas être modélisées et évaluées par des arbres de défaillances dynamiques. Pour combler ce manque et permettre la modélisation et l'évaluation de systèmes possédant des politiques de réparation complexes, les arbres de défaillance réparables (ou Repairable Fault Tree) [39] ont été introduits. Ils préservent la simplicité de la modélisation d'ADD et se basent sur l'expressivité des réseaux de Petri pour modéliser les politiques de réparation .Cette approche, consistant à enrichir un modèle booléen basé sur les arbres de défaillances par un modèle de type états-transitions pour prendre en compte des politiques de réparation ou de reconfiguration, est également à l'origine du développement des Boolean logic Driven Markov Processes (BDMP) couplant arbres de défaillances et chaînes de Markov.

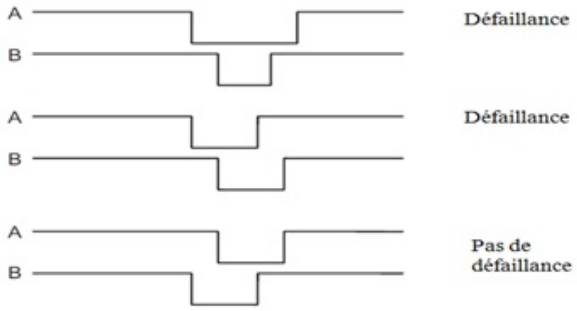


FIGURE II.3: Diagramme état-temps pour la porte PAND

Boolean logic Driven Markov Processes

Une autre alternative proposée dans le cas des systèmes dynamiques est la méthode des Boolean logic Driven Markov Processes (BDMP).
Les BDMP, développés par Bouissou [40] sont une extension des arbres de défaillances combinées avec les graphes de Markov et s'appuient sur le formalisme graphique des arbres de défaillances en y rajoutant ce qu'on appelle des 'gâchettes'.
Les BDMP permettent de modéliser des systèmes avec des interactions très variées entre composants : Les redondances passives, les défaillances de cause commune, les fonctionnements en plusieurs phases....
Dans un BDMP, les sollicitations se propagent tel que dans un arbre de défaillance classique tout au long des branches du BDMP jusqu'à ce qu'elles rencontrent l'arrivée d'une

gâchette. Ceci conditionne le passage du signal de sollicitation d'origine de la gâchette à la cible seulement si l'événement qui est à l'origine de la gâchette est VRAI. Si c'est le cas, la demande est transmise à la porte cible et aux feuilles de l'arbre suivant le même principe.
En termes d'évaluation quantitative, le modèle sous-jacent au BDMP n'est plus une équation booléenne, mais une chaîne de Markov. Par conséquent, la probabilité d'occurrence de l'événement redouté ne pourra plus être calculée par une formule simple (sommes et/ou produits des probabilités des événements de base) mais nécessitera de faire appel à la théorie de chaînes de Markov.
Les BDMP constituent donc un outil efficace pour les études de la Sûreté de Fonctionnement (SdF), proche des arbres de défaillance qui peuvent être considérés comme un sous ensemble de BDMP [33, 41]. Sous certaines hypothèses, le langage Figaro [42, 43] sert à transformer un BDMP dans un processus de Markov en temps continu, donnant ainsi accès à l'évaluation quantitative. Les BDMP sont implémentés dans un ensemble d'outils développés par Electricité de France EDF (KB3) ; un grand nombre des études ont été réalisées avec ces outils, particulièrement dans le domaine des systèmes électriques réparables. Néanmoins, les gâchettes ne considèrent qu'une stratégie de reconfiguration simple (commutation vers un mode de secours sur condition). Aussi, les BDMP ont été conçus dans le but de générer une chaine de Markov par utilisation du langage de description FIGARO. Ils ont donc été plus particulièrement conçus dans l'objectif de conduire des analyses quantitatives plutôt que des analyses qualitatives.

Avantages et Limites : L'explosion combinatoire due aux traitements à effectuer pour quantifier un modèle BDMP à l'aide des graphes de Markov est considérablement limité par l'emploi de la notion d'événement pertinent. En effet, dès qu'un des évènements d'une porte OU est VRAI, les autres événements (et descendants) ne sont plus "pertinentes" (à condition qu'ils ne puissent pas agir ailleurs dans l'arbre) et sont inhibées. On évite ainsi de nombreuses séquences contenant des événements "non pertinents" puisque agissant sur des parties du système déjà perdues.
Par exemple dans le BDMP de la figure II.4 deux défaillances sont possibles à l'état initial. La défaillance d'un des composants de la porte G_1 déclenche la porte G_2 qui transmet le signale aux nouvelles feuilles du sous arbre ce qui rend possible d'autres défaillances (porte G_3). Ainsi la défaillance du deuxième composant de la porte G_1 est considérée comme impertinente et elle est donc inhibée tant que la porte G_1 est vraie

[44]. Ce mécanisme de filtrage des évènements pertinents permet en effet de réduire considérablement la combinatoire dans l'exploration des chemins menant à l'événement redouté, effectuée lors du traitement du modèle.
En outre, on peut citer leur difficulté à prendre en compte des créations/destructions d'éléments en cours de vie du système modélisé, et leur difficulté à modéliser les comportements cycliques/boucles.

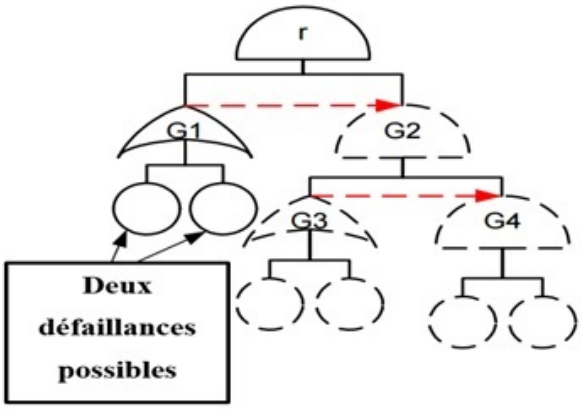


FIGURE II.4: Exemple d'un BDMP

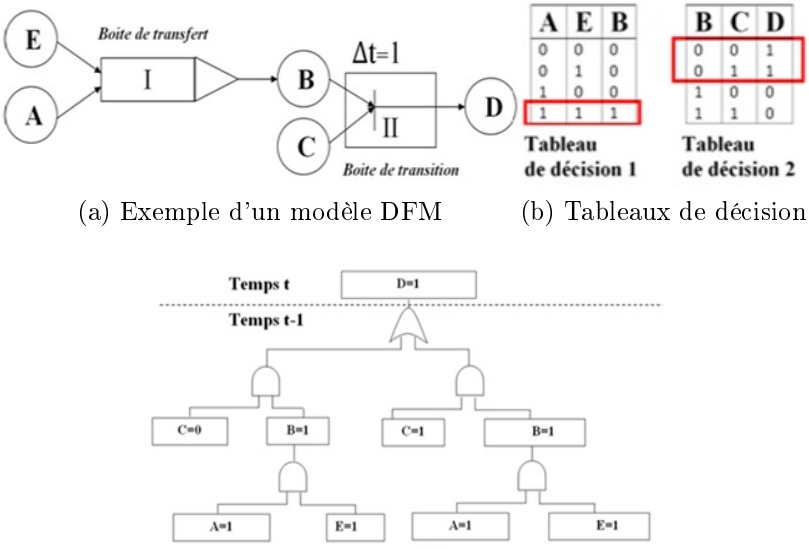
Méthode des graphes des flux dynamiques

La méthode des graphes de flux dynamiques (Dynamic Flowgraph Methodology DFM) proposée par Garret et all [45] a été utilisée dans les études de risque des systèmes aérospatiaux et nucléaires. C'est une technique de modélisation et d'analyse pour étudier les risques des systèmes embarqués [2] qui a pour but d'identifier les scénarios redoutés. Elle permet de prendre en compte l'aspect dynamique des systèmes embarqués et l'interaction entre la partie logicielle et la partie matérielle des systèmes. Des applications de la méthode peuvent être trouvées dans[46, 47, 48, 49, 50].
La méthode est composée de deux étapes : une étape de modélisation suivie d'une étape d'analyse. L'étape de la modélisation a pour objectif la construction d'un modèle décrivant le comportement logique et dynamique du système à l'aide de nœuds (nœuds de variables physiques et nœuds conditionnels) reliés entre eux par des connecteurs (boite de transfert et boite de transition) décrivant ainsi des relations de causalité (relations

2. un système embarqué est un système électronique et informatique autonome dédié à une tâche précise, souvent en temps réel, possédant une taille limitée et ayant une consommation énergétique restreinte.

logiques) et temporelles (comportement dynamique du système) entre les variables physiques de la partie opérative et les paramètres de commande du système de contrôle.

Analyse qualitative L'étape d'analyse qualitative, consiste en la détermination des chemins menant vers un état redouté. Ceci est possible à l'aide d'un arbre de défaillance temporisé construit à partir du modèle DFM.
Les variables physiques sont discrétisées en un nombre fini d'état (il n'existe pas de critère de sélection des états), et à travers une table de décision, toute combinaison de valeurs des nœuds d'entrée lui correspond une valeur pour les nœuds de sortie.
Pour illustrer cette étape d'analyse qualitative, nous avons emprunté de [51] l'exemple de la figure II.5. Pour atteindre l'état D = 1 (Fig II.5a), deux combinaisons sont possibles ce que montre le tableau de décision 2 (Fig.II.5b), soit ($B = 0$ et $C = 0$), soit ($B = 0$ et $C = 1$). Comme B est un nœud de sortie d'une boite de transfert, nous allons chercher les combinaisons possibles pour que $B = 1$. Le tableau de décision 1 de la figure II.5b montre que les causes amenant à l'état $B = 1$ sont ($A = 1$ et $E = 1$). A partir de ces combinaisons, le deuxième niveau de l'arbre peut être construit et s'arrête à ce niveau comme illustré dans la figure II.5c car tous les événements obtenus sont des événements de base.



(a) Exemple d'un modèle DFM (b) Tableaux de décision

(c) Arbre de défaillance temporisé.

FIGURE II.5: Application de la méthode des graphes des flux dynamiques.

Nous obtenons finalement un ensemble de séquences caractérisées par des suites d'états

amenant à l'état $D = 1$:

— $A = 1$ et $E = 1$ et $C = 0$ / $t = t - 1$

— $A = 1$ et $E = 1$ et $C = 1/t = t - 1$

L'arbre de défaillance permet d'exprimer les combinaisons booléennes pouvant amener le système dans un état donné.

Avantages et limites : Une modélisation par DFM permet une prise en compte explicite des interactions entre la partie opérative et la commande de ces systèmes. Un des avantages de cette méthode est qu'elle est basée sur la construction d'arbre de défaillance (temporisés) bien connus dans la communauté des fiabilistes, ce qui rendrait le DFM plus accessible que d'autres méthodes.
Discrétiser systématiquement toutes les variables du système étudié représente un inconvénient majeur de cette méthode quand il s'agit de systèmes de taille industrielle. Cela engendre en effet des modèles de très grande taille. Nous devons faire face à un problème d'explosion combinatoire des états et des séquences qui risque de rendre toute la démarche infaisable. De plus, nous n'avons aucune idée des incertitudes liées à cette discrétisation.
Un deuxième inconvénient est à signaler, il concerne l'incapacité de cette méthode à prendre en compte les caractéristiques stochastiques des composants des systèmes, par exemple leur taux de défaillance[47]. Ceci nous amène vers un autre point qui est celui de la quantification des événements redoutés. Cette méthode produit des arbres de défaillances temporisés montrant comment un système pourrait évoluer vers un état redouté donné. Pour pouvoir déterminer la probabilité d'être dans un tel état, il est indispensable de connaître la dynamique des variables du système c'est-à-dire comment ces variables passent d'un état à un autre et non seulement la probabilité de défaillance des composants du système.
D'autres méthodes peuvent être citées comme :

— **la méthode GO-FLOW** [47, 49] historiquement, c'est l'une des premières méthodes de fiabilité dynamique. Son formalisme graphique s'inspire des diagrammes de fiabilité, tout en étant enrichi d'opérateurs graphiques spécifiques. La méthode GO-FLOW ne s'applique qu'à des systèmes très simples en raison de l'explosion combinatoire qu'elle provoque.

— **la méthode de diagramme de fiabilité dynamique**

— **diagramme des séquences d'évènements**

— ...etc.

L'inconvénient des méthodes graphiques est que les modèles sur lesquels elles sont basées ne sont pas sous-tendus par une démarche d'analyse formelle. Ce qui signifie qu'il est impossible de vérifier le modèle (incohérence, blocage...).

II.2.2 Approches à base de modèles transformation

Le but principal des méthodes à base de modèles transformation est la construction (semi-)automatique des modèles d'analyse de sûreté de fonctionnement.
Le processus commence à partir d'une description du système par les techniques de modélisation issues du domaine de l'informatique. Des lois de transformation et algorithmes sont établies afin d'extraire des modèles d'analyse de sûreté de fonctionnement du modèle conçu.
Ces méthodes peuvent être basées sur les langages de description suivants : Unified Modeling Language (UML)/ System Modelling Language (SysMl), Architecture Analysis & Design Language (AADL) et le langage ALTARICA.

Approches basées sur le langage Unified Modeling Language (UML)

L'UML est considéré comme un standard de-facto pour la conception d'une variété de systèmes allant des petits systèmes de contrôle aux systèmes complexes plus grands. Il est apprécié pour les avantages de l'orienté-objet et a permis de nombreuses modélisations pour la préparation d'analyse de SdF.
Afin de bénéficier de sa souplesse et son expressivité, l'UML est utilisé durant le projet HIDE présenté dans [52][53] et qui a pour objectif de faciliter les études de SdF et ceci par la définition d'un ensemble de transformations automatiques vers des formalismes et outils d'analyses de SdF. Les modèles d'entrée UML expriment le comportement global du système, incluant les comportements défaillants. Afin de rendre possible les transformations de modèle, les auteurs définissent des restrictions d'utilisation d'UML et introduisent leurs propres stéréotypes relatifs à la SdF. Boudavalli et all [54] présentent un passage d'UML aux Réseaux de Petri Temporisés (RdPT), cette transformation passe par plusieurs étapes, oú la première consiste en l'extraction des informations pertinentes de SdF de la masse d'informations disponibles dans une description UML, autrement dit un modèle de sûreté de fonctionnement est construit dans cette étape. L'étape suivante

permet de définir un RdPT pour des fins d'analyse, une dernière étape permet l'analyse du RdPT. Dans ce même contexte Zarras et all [55]ont réalisé un profil UML afin de faciliter la construction d'un modèle capable de prendre en compte les aspects nécessaires pour une analyse de SdF. Les stéréotypes y sont renforcés par l'utilisation de contraintes OCL (Object Constraint Language). Aussi Bernardi et all [56] ainsi que Merseguer et all [57] proposent dans leur article l'utilisation du diagramme de séquence et le statechart de l'UML pour la validation et le calcul des performances de SdF. Comme UML est un langage semi-formel et donc impossible d'appliquer directement les techniques mathématiques pour la validation du système, les auteurs proposent une traduction automatique des statecharts et du diagramme de séquences vers un Réseau de Petri Stochastique Généralisé (RdPSG). Ces travaux sont suivis par Lopez et all [58] qui intègrent l'utilisation des diagrammes d'activité UML pour l'amélioration de l'expressivité afin de générer des Réseaux de Petri Stochastiques Généralisés étiquetés (RdPSGE). Autre alternative proposée par Pai et all [59] qui s'inspirent du projet HIDE permet de générer un arbre de défaillance dynamique à partir d'une description UML. Leangsukun et all [60] proposent de définir de nouveaux stéréotypes afin de décrire le comportement dysfonctionnel du système en utilisant UML. Les modèles utilisant ces stéréotypes sont automatiquement convertis sous le format d'entrée du logiciel SHARPE utilisé pour générer des AdD et chaînes de Markov.

D'autres travaux dans le contexte de l'analyse de la sûreté de fonctionnement, basés sur l'utilisation des digrammes UML peuvent être mentionnés comme ceux dans [61, 62, 63]. Le langage UML a été développé pour répondre aux besoins des ingénieurs logiciel afin d'unifier et généraliser les pratiques de développement. De nombreuses adaptations du langage pour des domaines spécifiques ont vu le jour grâce aux possibilités de stéréotypage et de création de *profils* supportés par la spécification UML 2.0. Néanmoins, UML n'a pas rencontré le succès escompté auprès de la communauté des ingénieurs système, principalement à cause de ses notations trop orientées logiciel et d'un manque d'expressivité pour des problématiques spécifiques aux systèmes physiques [64]. De plus, les profils créés sont réalisés par des groupes restreints de développeurs, pour des applications très ciblées et les outils du marché ne pouvaient notamment pas suivre et implémenter chacune de ces expériences individuelles afin de permettre leur dissémination.

Approches basées sur le langage System Modelling Language (SysML)

Le SysML hérité du langage UML, est construit comme un sous-ensemble des notations UML, augmenté de nouveaux artefacts. SysML est donc constitué d'une partie commune avec UML, et d'une partie spécifique correspondant au profil SysML. Il est conçu à la fois pour aider à l'analyse, la spécification, la conception, la vérification et la validation des systèmes complexes [65]. Le langage offre la possibilité de modéliser des composants physiques ou logiciels, des acteurs humains, des flux de données, des procédures et tout ce qui peut composer un système.
Dans l'article de J. Xiang et all[66], pour des fins d'analyse de SdF, les auteurs proposent de générer automatiquement des arbres de défaillance statiques à partir de modèles de système spécifiés avec SysML.

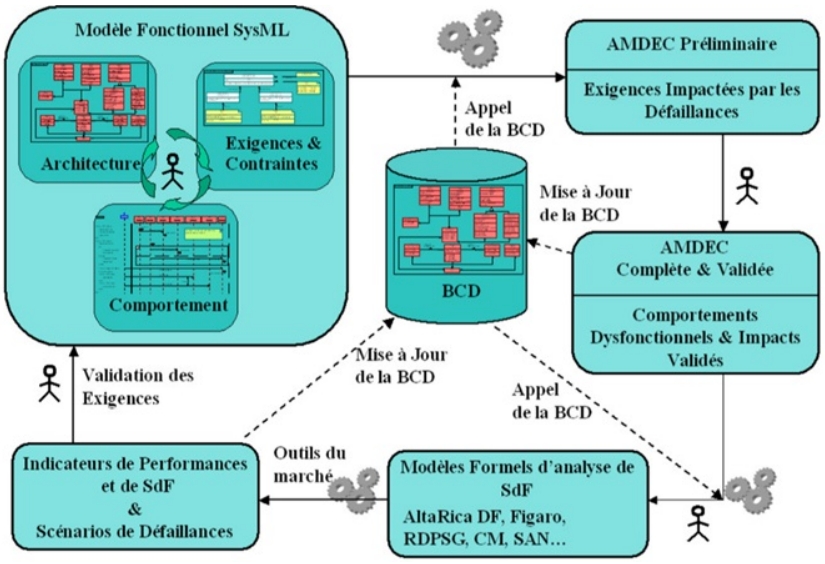


FIGURE II.6: Méthode MéDISIS [64]

Dans sa thèse, P. David [64] s'est intéressé aux systèmes à fortes contraintes de sûreté de fonctionnement. Afin de maîtriser tout au long de la conception la complexité et les performances du système, l'auteur met le point sur la nécessité de l'emploi de techniques rigoureuses d'Ingénierie Système, ainsi que de pratiques avancées d'analyse de sûreté de fonctionnement au cours du développement de ces systèmes. Dans l'optique de faire coopérer les outils employés par chaque communauté, une méthodologie d'intégration des analyses de sûreté de fonctionnement au processus d'Ingénierie Système basée sur les modèles *MéDISIS* et dressée comme le montre la figure II.6. L'auteur considère dans sa thèse les méthodes d'Ingénierie Système basées sur les modèles, en l'occurrence le

SysML comme la meilleure alternative d'ingénierie pour le développement des systèmes complexes à fortes contraintes de sûreté de fonctionnement. D'autre part, en considérant que le langage Altarica comme un langage très puissant et populaire pour la réalisation d'études de sûreté de fonctionnement, une passerelle est proposée afin de traduire des modèles fonctionnels SysML vers le modèle AltaRica Data Flow, permettant une analyse formelle de la SdF du système.

Approches basées sur le langage AltaRica

AltaRica est un langage de modélisation formelle développé dans le but d'établir divers ponts entre la sûreté de fonctionnement et les méthodes formelles [67].
La première version du langage AltaRica a été développée au sein du Laboratoire Bordelais de Recherche en Informatique (LaBRI) en partenariat avec plusieurs industriels afin de permettre une description des systèmes complexes[68, 69].
La sémantique de la première version d'Altarica a été définie en termes d'automates a contraintes [69] qui sont des automates finis pour lequel les variables et les transitions sont soumises à des contraintes.
AltaRica Studio est l'outil basé sur le langage AltaRica permettant de visualiser et d'analyser les modèles. Plusieurs outils d'évaluation ont été développés à partir du langage AltaRica, comme le compilateur de l'arbre de défaillance ou le générateur des séquences d'évènements critiques [70]. Par la suite, une seconde version du langage, Altarica Data-Flow, a été développée à l'Institut de Mathématiques de Luminy (IML) dont la sémantique est basée sur les automates à mode [71] afin de pouvoir traiter les systèmes de taille industrielle [71, 72]. Le langage Altarica Data-Flow a été utilisé comme langage de base par plusieurs ateliers de sûreté de fonctionnement dans l'industrie tels que Cecilia OCAS (Dassault Aviation), Simfia v2 (EADS Apsys) et Safety Designer (Dassault Systemes). Cette version du langage rend possible le développement d'un ensemble d'algorithmes de traitement efficaces comme le compilateur d'arbre des défaillances [71], le générateurs des séquences d'évènements critiques, le compilateur des chaines de Markov [73] les simulateurs stochastiques [74] et pas à pas. Cependant, la large expérience des développeurs de ce langage à monter que le langage ainsi que les outils d'évaluation peuvent être améliorés encore. Pour cela, une troisième version AltaRica 3.0 est proposée par la suite [75]. Afin d'améliorer le langage, Prosvirnova et all[67] utilisent un formalisme pivot (les systèmes de transitions gardées[76]) qui permet de traduire le modèle vers des

outils de traitement tels que le générateur de l'arbre de défaillances, le générateur des chaines de Markov, générateur de séquences critiques...etc.
Le langage formel AltaRica est intéressant pour la modélisation de systèmes en vue d'une analyse de sûreté de fonctionnement car il permet une modélisation à la fois fonctionnelle et dysfonctionnelle. Cette vue dysfonctionnelle est permise grâce à l'introduction d'événements modélisant la défaillance des composants. Un avantage de ce formalisme est sa généricité, et donc la capacité de pouvoir générer de nombreux modèles ayant des objectifs différents à partir d'une description AltaRica d'un système.
D'autres travaux basés sur le langage AltaRica dans le contexte de la sûreté de fonctionnement peuvent être mentionnés, Pagetti [77] a travaillé sur une extension temps réel d'AltaRica, Kehren[78] a identifié des motifs d'architecture de systèmes pour la sûreté de fonctionnement, Humbert [79]s'est intéressée à la définition d'exigences de sécurité pour les systèmes,Khuu [74]a travaillé sur l'accélération de la simulation stochastique pour la sûreté de fonctionnement à partir de modèles décrits en AltaRica Data Flow, Sagaspe [80] a proposé une méthodologie et un outil pour la réalisation de l'allocation de ressources dans le cadre de l'aéronautique tout en s'assurant du respect des exigences de sûreté de fonctionnement, Bernard [81] s'est intéressé à la sûreté de fonctionnement des systèmes critiques, et plus particulièrement quand on considère un système à des niveaux de détails différents, en utilisant la notion de raffinement de modèles AltaRica. David [64] décrit un algorithme afin de générer automatiquement des modèles Altarica Data-Flow, à partir des diagrammes SyML et du tableau AMDEC, Albore et all[82],pour des fins d'analyse de risque, décrivent une approche basée sur une extension du langage AltaRica ou les auteurs associent des contraintes temporelles aux événements .AltaRica a aussi été présent dans le projet européen MISSA (More Integrated and cost efficient System Safety Assessment) d'avril 2008 à mars 2011et qui avait pour but de proposer des méthodes et outils pour aider les ingénieurs sûreté de fonctionnement à effectuer leurs analyses.

Approches basées sur le langage Architecture Analysis & Design Language (AADL)

Le langage AADL est développé et standardisé par la SAE (Society of Automotive Engineers) en 2004 [83], dans le but de modéliser les systèmes embarqués. L'AADL fournit une notation textuelle et graphique standardisée pour décrire des architectures

matérielles et logicielles et pour effectuer différentes analyses du comportement et des performances du système modélisé [84].
En AADL, les systèmes sont modélisés comme des ensembles de composants logiciels qui interagissent via des ports et qui s'exécutent sur des composants matériels.
La plupart des articles publiés autour des analyses basées sur AADL se sont concentrés sur l'extension du langage pour faciliter la vérification formelle, comme dans les cas de [85] et du projet COTRE [86]. Dans [87, 88] les auteurs proposent des méthodes pour effectuer des analyses d'ordonnancement, d'autre part la contribution de [89],qui se rapproche à notre objectif de l'analyse de sûreté de fonctionnement, présente un outil interne de Honeywell qui permet la génération d'arbres de défaillance à partir de modèles AADL.
D'après Rugina [90] d'un point de vue critique, cette contribution ne fournit pas de méthodologie de modélisation et ne guide pas l'utilisateur dans la construction du modèle AADL de sûreté de fonctionnement. En même temps, la transformation de modèle de AADL vers les arbres de défaillance n'est pas détaillée. De plus, cette approche cible uniquement la fiabilité et ne peut pas être utilisée pour évaluer d'autres mesures de sûreté de fonctionnement. Pour répondre a cela Ruguina et all dans [91, 92, 93] guident l'élaboration du modèle AADL de sûreté de fonctionnement par une méthode itérative, qui prend en compte progressivement les dépendances entre les composants permettant ainsi à assister l'utilisateur dans la construction structurée du modèle AADL de sûreté de fonctionnement.Ensuite, les auteurs proposant une transformation de modèle de AADL vers des réseaux de Petri stochastiques généralisés (RdPSG)[94], qui peuvent être traités par des outils existants pour évaluer les mesures de sûreté de fonctionnement. La transformation est basée sur un ensemble des règles conçues pour être mise en œuvre dans un outil de transformation de modèle, de façon transparente à l'utilisateur. De cette manière, la complexité de la génération du modèle RdPSG est masquée aux utilisateurs qui connaissent AADL et qui ont généralement des connaissances limitées dans le domaine des RdPSG. Afin de montrer la faisabilité de l'automatisation, les auteurs ont implémenté un outil de transformation, ADAPT (from AADL Architectural models to stochastic Petri nets through model Transformation), qui s'interface avec OSATE, côté AADL, et avec Surf-2, côté RdPSG.
Dans le même but,Bozzano and al. [95] et Brunel and al.[96] proposent des cadres de modélisation pour l'analyse et l'évaluation de la sûreté de fonctionnement. Ceux-ci tiennent compte des aspects temps réel et sont spécifiques aux systèmes aérospatiaux. Ces mo-

dèles sont transformés vers le langage AltaRica 3.0 [75] pour mener des analyses de sûreté de fonctionnement. Ces travaux ont donné lieu à des applications dans le secteur aérospatial, [96].

L'intérêt que suscite les langages de modélisation ces dernières années, tels que les langages cités ci-dessus, a motivé plusieurs auteurs à les exploiter, ces langages fournissent une notation standardisée pour décrire les systèmes. Par la suite, une transformation de ses modèles vers d'autre modèles pour des fins d'analyse de SdF est réalisée. Ceci dit la question qui se pose est l'efficacité du modèle choisi pour l'analyse de sûreté des systèmes complexes et l'éternel problème de l'explosion combinatoire.

II.2.3 Approches basées sur la modélisation utilisant des modèles formels

Dans cette catégorie, l'étape de modélisation joue un rôle crucial dans l'analyse des systèmes et le formalisme choisi influe sur la manière d'aborder le problème. Une fois que le formalisme est choisi, il limite les méthodes et outils d'analyse. Plusieurs auteurs ont soulignés la nécessité d'utiliser des méthodes plus adaptées à la modélisation et à l'analyse des systèmes dynamiques hybrides tels les modèles états transitions.
Dans cette catégorie peuvent être cités les approches basées sur les réseaux de Petri, les graphes de Markov, les automates finis...

Approche basée sur les Graphes de Markov

Une chaine de Markov [97] sur un espace d'état E est un processus (X_n) tel que :

— Pour tout état i de E l'événement $X_{n+1} = i$ ne dépend que de l'état dans lequel était le processus à l'instant n ("le futur ne dépend que de l'instant présent")

— La probabilité de passer de l'état i à j ne dépend pas de l'instant n

Exemple : une puce se déplace aléatoirement sur les sommets d'un carré $\boldsymbol{ABCD}$. Chaque seconde elle saute sur l'un des sommets voisins d'une façon équiprobable.Après n secondes on note X_n sa position.
Par exemple à l'instant $t = 0$, la puce se trouve sur le sommet C, on écrit alors $X_0 = C$, la seconde d'après soit elle saute sur A ou B ou D. Si elle saute par exemple sur A on écrit $X_1 = A$ et ainsi de suite jusqu'à obtenir : $X_0 = C, X_1 = A, X_2 = B, X_3 = D$... qui est la

suite de variables aléatoires décrivant le système.Cette évolution se fait dans le temps, dans cet exemple c'est de seconde en seconde. A chaque fois, ces variables aléatoires vont prendre une valeur à partir d'un ensemble qui est toujours le même $E = \{A, B, C, D\}$ qu'on appel l'espace des états. Celui-ci liste tous les états possibles que peuvent prendre les variables.

Imaginons qu'on est dans l'état $X_2 = B$, la probabilité de passer à l'état $X_3 = C$ ne dépend que du dernier état qui est $X_2 = B$, la manière dont on est arrivé a $X_2 = B$ n'importe peu. Le faite que la puce était dans le sommet C et A infule absolument pas sur les probabilités de l'instant à venir.On dit qu'un processus de Markov est un processus sans mémoire.Ceci est la propriété la plus importante dans les chaines de Markov. La deuxieme propriété, est que peu importe le temps passé dans un état, la probabilité de passer à l'état suivant reste inchangée.

Une chaîne de Markov, est représentable graphiquement par un graphe orienté $G = (E, \Lambda)$ où E représente les sommets du graphe associés aux états du processus et Λ les arcs orientés reliant les sommets.

Les graphes de Markov sont un outil classique en sûreté de fonctionnement.La construction d'un graphe de Markov consiste à identifier les différents états du système (dégradé, défaillants ou non défaillants) et chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une réparation. A chaque transition, de l'état X_i vers l'état X_j, est associé un taux de transition Aij défini de telle sorte que $Aij.dt$ est égal à la probabilité de passer de X_i vers X_j entre deux instants très proches t et $t + dt$ sachant que l'on est en X_i à l'instant de temps t. En SdF, les transitions stochastiques entre les états sont caractérisées par des taux de défaillance/réparation.

Un exemple d'un graphe de Markov est donné dans la figure II.7 ci-dessous.

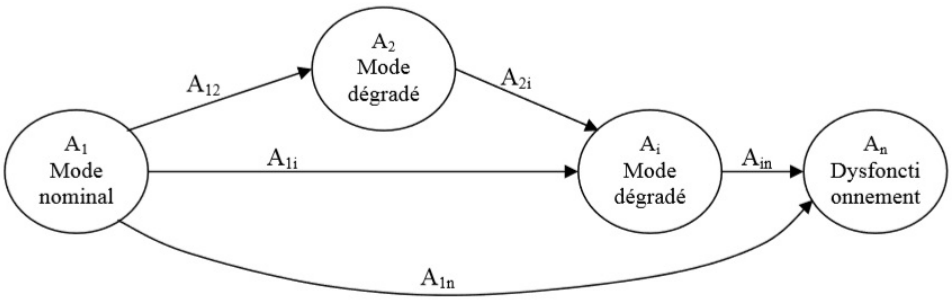


FIGURE II.7: Exemple d'un graphe de Markov

Dans le cadre de la sûreté de fonctionnement cette représentation permet de modéli-

ser les évolutions entre les états d'un système (représentés par les sommets du graphe), ainsi que leurs probabilité d'occurrence.
Pour l'identification des séquences d'événements (scénarios) qui mènent à un événement indésirable spécifié, les travaux récents de Yang et all [98] peuvent être cités. Les auteurs proposent un algorithme implémenté d'une façon déductive pour l'identification des scénarios critiques se basant sur la technique Markov/cell-to-cell Mapping Technique (CCMT)[99].Dans l'article de Aldmir et all [100], les autres illustrent l'application de deux méthodologies d'analyse des risques : graphes de flux dynamique et Markov/cell-to cell Mapping Technique, deux techniques mises en place pour aborder la dynamique des systèmes. L'étude examine la pertinence de deux méthodologies dynamiques pour l'analyser des risques.

En dépit de leur simplicité conceptuelle et leur aptitude à pallier certains handicaps des méthodes classiques, l'inconvénient majeur de ce modèle est la difficulté de construction du graphe, car le processus de modélisation implique l'énumération de tous les états possibles et de toutes les transitions entre ces états. Chaque sommet représentant un état du système, ce modèle est alors très sensible au phénomène d'explosion combinatoire lorsque la taille du système est importante.En effet, de manière générale, pour n composants, la chaîne de Markov peut admettre jusqu'à 2^n sommets. Il est alors quasiment impossible de construire manuellement la chaîne de Markov associée sans introduire d'erreurs.Afin d'éviter ce type de construction et de maitriser l'explosion combinatoire du nombre d'états, il faut avoir recours à des outils de modélisation basés sur des mécanismes tels que l'abstraction, la modularité,l'agrégation et la décomposition hiérarchique. Les travaux de Schoenig [101, 102], utilisant les graphes de Markov agrégés visant une limitation de l'expansion combinatoire peuvent être cités.

Les automates finis

Les automates à états finis [103] constituent le modèle de base pour la représentation des systèmes à événements discrets (SED).
Un automate fini est un quintuplet $M =< Q, \Sigma, \delta, q_0, F >$ où :

- Q est un ensemble fini d'états.
- Σ est un ensemble fini de symboles (un alphabet), ou ensemble des événements.
- $\delta : Q \times \Sigma \longrightarrow Q$ est une fonction de transitions.
- $q_0 \in Q$ est l'état initial.

— $F \subseteq Q$ est l'ensemble (fini) des états finaux.

□

L'exemple de la figure II.8 explique le fonctionnement du l'automate fini.

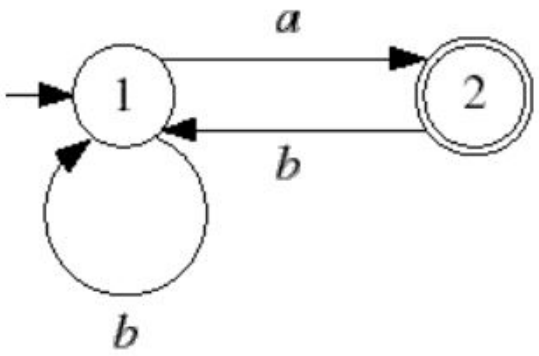


FIGURE II.8: Exemple d'un automate

— $Q = 1, 2$, l'automate fini contient deux états qui sont l'état 1 et l'état 2.

— $i = 1$, état initial noté avec une petite flèche entrante,

— $F = 2$, état final noté avec deux cercles.

— $\delta : Q \times \Sigma \longrightarrow Q$:
$(1, a) \longrightarrow 2$ ceci signifie que si l'automate se trouve dans l'état **1** alors sur l'occurrence de l'événement **a**, l'automate fera une transition vers l'état **2**.
De même pour les autres fonctions :
$(1, b) \longrightarrow 1$
$(2, b) \longrightarrow 1$

L'automate prend en entrée un mot et l'accepte ou la rejette. On dit aussi qu'il le reconnaît ou ne le reconnaît pas.Dans le cas de l'exemple de la figure II.8, on dit que l'automate fini reconnait **a** ou **bba**...
Le langage reconnu (ou accepté) par un automate fini est l'ensemble des mots qui correspondent à un calcul de l'automate partant d'un état initial et s'arrêtant dans un état final.
Lors de l'utilisation d'un automate fini pour la modélisation d'un système, les langages représentent des séquences possibles d'événements : le langage généré représente toutes les séquences possibles, le langage reconnu représente des séquences caractéristiques de

certaines fonctions ou tâches particulières.
Les automates fini existent en plusieurs variantes, comme les automates hybrides[104], les automates stochastiques hybrides[105][106], mais ils sont encore relativement peu utilisés dans le cadre de la SdF. Cependant la méthode utilisant les automates stochastiques hybrides(ASH), décrite en détail dans la thèse Perez [105], est représentée dans le cadre du projet Approdyn [107]. Ce projet avait pour but de modéliser le comportement d'un générateur de vapeur.
Un ASH est un automate à états finis temporisé. Chaque mode (état discret) est associé aux équations différentielles qui représentent l'évolution des variables continues. Le caractère hybride de l'automate est assuré par les transitions. Celles-ci peuvent être déterministes (déclenchées par le passage d'un seuil de la variable physique) ou stochastiques (événement aléatoire telle qu'une défaillance). Perez [105] utilise l'environnement open source Scilab / Scicos pour construire l'ASH global décrivant le système étudié dans son intégralité. Cette étape de composition des ASH élémentaires est délicate car elle peut entraîner l'explosion du nombre de modes de l'ASH global. Afin de contourner cette difficulté, Chraibi [108] utilise des ASH communicant entre eux. Pour l'étape analyse, l'auteur [105] propose un outil de simulation de Monte Carlo permettant d'accéder à l'évaluation des grandeurs de la sûreté de fonctionnement en contexte dynamique. Plus précisément l'auteur évalue la probabilité d'occurrence des deux événements redoutés du son cas test : l'assèchement et le débordement d'un réservoir.

Un autre formalisme graphique utilisé pour des fins d'analyse de SdF et qui se présentes de manière récurrente dans la littérature et le formalisme des réseaux de Petri traités ci-dessous.

Les Réseaux de Petri

Un réseau de Petri (RdP) [109, 110, 111] est un outil graphique et mathématique permettant de modéliser et de vérifier le comportement dynamique des systèmes. C'est un graphe biparti qui se compose de places, de transitions et d'arcs. L'ensemble des places (schématisées par un cercle) permet de représenter l'état du système, l'ensemble des transitions (schématisées par un trait) représente les évènements. Les relations de causalité au sein du système sont représentées par des arcs orientés reliant les places aux transitions.

L'ensemble places, transitions et arcs constitue la structure du réseau de Petri (partie statique). L'évolution du réseau (partie dynamique) est obtenue par les franchissements de transition qui affectent son marquage. Pour qu'une transition soit franchie, il faut qu'elle soit valide ou sensibilisée. Cette présentation intuitive des réseaux de Petri est formalisée par la définition suivante.

Définition 12 ***(Réseau de Petri[110, 109])*** *: Un réseau de Petri R est définit par le 5-tuple* $<P, T, Pre, Post, M_0>$*, avec :*

- $P = P_1, P_2, P_3, ..., P_n$ *est un ensemble fini de places,*
- $T = T_1, T_2, T_3, ..., T_m$ *est un ensemble fini de transitions,*
- $Pre : P \times T \longrightarrow (0, 1)$ *est l'incidence arrière,*
- $Post : P \times T \longrightarrow (0, 1)$ *est l'incidence avant,*
- M_0 *est le marquage initial.*

□

Un exemple du RdP est donnée dans la figure II.9.

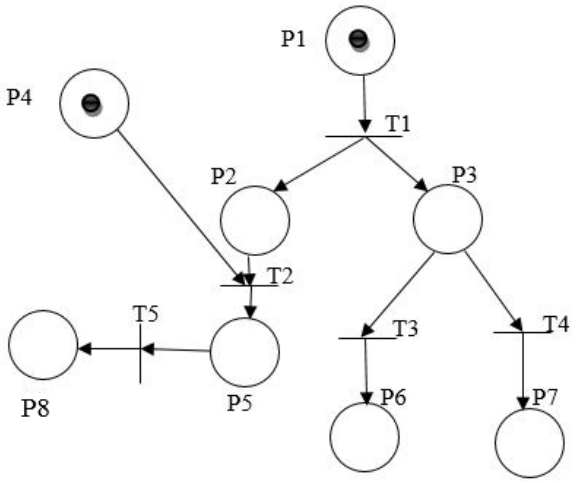


FIGURE II.9: Exemple d'un réseau de Petri

Destinés à modéliser des comportements dynamiques à événement discret, les RdP allient une représentation graphique simple capable de modéliser le parallélisme, la synchronisation et le partage de ressources, à une théorique mathématique riche et procure à ce

formalise un grand pouvoir de modélisation d'où leurs succès.
Depuis son invention [111], le RdP a été enrichi par divers chercheurs pour permettre des descriptions plus condensées et/ou faisant intervenir le facteur temps : RdP temporisés, stochastiques, colorés, continus, hybrides...
Le Reseau de Petri (RdP), comme un outil de l'analyse de la sureté de fonctionnement, est devenu de plus en plus débattus ces dernières années.Ce progrès à été confirmé par les autorités internationales de normalisation qui ont publié le standard IEC 62551 "Analysis techniques for dependability-Petri net techniques-"[112]. Ce standard regroupe les approches utilisant les RdP dans le domaine de la sûreté de fonctionnement.
L'utilisation des RdP pour les analyses de sûreté de fonctionnement est née de la nécessité de considérer les systèmes multi-états reconfigurables. Le principal avantage des RdP est la possibilité d'analyser le comportement d'un système en présence de défaillances. Un RdP permet de modéliser d'une part le fonctionnement normal d'un système et d'autre part les occurrences de défaillances.
Parmi les travaux utilisant les RdP, on peut citer ceux de Dutuit et all [113] utilisant les RdP stochastiques [3] couplés avec la simulation Monte Carlo [4] (MC). Les auteurs proposent une modélisation du système dynamique basée sur le RdP afin d'évaluer certaines grandeurs de sûreté de fonctionnement. L'approche consiste à dresser un ensemble de RdP inter-connectés et les animer en utilisant la technique de simulation de Monte Carlo, ainsi des résultats qualitatifs et quantitatifs des risques ont été déduits au bout de plusieurs itérations.
Si l'estimation des événements rares, pouvant exiger des durées de calcul prohibitives, on peut restreindre leur champ d'application. Selon le standard IEC 61508-6 [114], les RdP sont un parfait support pour l'application de la simulation MC, aussi les RdP ont le grand avantage d'être flexibles et de pouvoir modéliser et traiter presque tous les types de contraintes non seulement des processus non-Markoviens, mais encore des processus concourants et interdépendants.
Dans le même but, Signoret [115] utilise des RdPS développés par l'entreprise "TOTAL" pour modéliser le système dynamique. L'auteur implémente des *prédicats* et des *assertions* dans le RdPS. Les prédicats sont utilisés pour valider une transition et les assertions pour mettre a jour les variables quand la transition est franchis. Cette mo-

3. Un RdP ayant des transitions gérées par des lois probabilistes est dit stochastique.
4. Une méthode algorithmique visant à calculer une valeur numérique approchée en utilisant des procédés aléatoires

délisation a été le support pour une simulation Monte Carlo pour des fins d'analyse quantitative de sûreté de fonctionnement.
Briss et all [116] utilisent les RdP stochastiques colorés [5] (RdPSC) comme modèle de représentation des systèmes dynamiques. Le RdPSC sert de modèle d'entré pour la simulation Monte Carlo afin d'estimer les caractéristiques de sûreté de fonctionnement telles que la probabilité d'occurrence d'un événement non désirable et la fiabilité du système. Les auteurs utilisent un benchmark de la littérature [117]utilisant, pour le même but, les RdP stochastiques généralisés et comparent les résultats obtenus.
Simeu-Abazi et al [118] modélisent le système en utilisant l'arbre de défaillance dynamique qui sera traduit en réseau de Petri haut niveau. La traduction en RdP a montré une grande amélioration dans la flexibilité du modèle et aussi que plusieurs dépendances existantes dans le système peuvent facilement être représentées.
Dans leurs travaux, Venrez et all [119], discutent l'utilisation et l'application courante ainsi que les perspectives des RdP dans le domaine de l'analyse des risques. Après avoir présenté un bref état de l'art sur l'utilisation des RdP pour des fins d'analyse des risques, et estimant que l'analyse quantitative a été largement étudiée, les auteurs se concentrent sur l'analyse qualitative. Afin de prédire les possibles scénarios d'accident dans le métro suisse, Venrez et all [119] utilisent les RdP colorés pour modéliser le système dynamique, ensuite ils utilisent le graphe de marquage pour extraire tous les scénarios d'accident possibles.Les résultats de leurs application montre que malgré l'adéquation des RdP colorés pour la modélisation du système dynamique, ainsi que dans l'analyse quantitative, l'utilisation du graphe de marquage pour des fins d'analyse qualitative souffre de l'explosion combinatoire du nombre d'état, malgré la taille limitée du RdP utilisé. En effet, bien avant les travaux de Venrez et all [119], Moncelet [28] traite l'évaluation qualitative et quantitative de la sûreté de fonctionnement des systèmes mécatroniques automobiles. Plus particulièrement, ces travaux portent sur la détermination des séquences d'événements redoutés et l'estimation de leurs probabilités d'occurrence par la simulation (simulation de Monte Carlo). À partir d'une modélisation et à l'aide des réseaux de Petri colorés, le graphe des marquages accessibles est généré et tous les chemins menant vers un état redouté donné sont identifiés et caractérisés en termes d'enchaînements d'actions et de changement d'états des composants concernés du système. L'estimation de la probabilité d'occurrence de ces scénarios redoutés se fait par une simulation de

5. RdPSC est un RdP stochastique associé avec un RdP coloré.
Un RdP coloré est un RdP dont les jetons sont différencié par des couleurs

Monte Carlo du modèle quantitatif du système.
Cependant, deux limites sont immédiatement évidentes en utilisant cette approche :

— L'analyse qualitative est confrontée au problème de l'explosion combinatoire du nombre d'états du graphe des marquages accessibles .Aussi, le parallélisme est traité par entrelacement ce qui mène a une confusion entre les relations de précédence et celles de cause.

— Lors de l'analyse quantitative, la simulation de Monte Carlo nécessite un temps prohibitif. La rareté des scénarios redoutés rend inefficaces les méthodes basées sur la simulation de Monte Carlo du modèle global. En effet, le système passe la majorité de son temps dans un fonctionnement nominal qui n'apporte aucune information sur la sûreté de fonctionnement.

Pour contourner la première difficulté (l'explosion combinatoire du nombre d'état), Demmou and all[120], Sadou and all[121] ont proposés une méthode d'analyse basée sur la modélisation au préalable du système sous la forme d'un RdP t-temporel [6], dont le raisonnement est fondé sur la prise en compte du dernier ensemble d'événements précédant l'état critique et ignore le reste du réseau. Les conclusions tirées de cette réflexion sont par la suite vérifiées par l'utilisation de la logique linéaire [122, 123] (notée dans la suite LL) de manière à valider la cohérence de leur méthode. Le scénario critique obtenu par cette méthode est constitué certes d'une séquence courte mais insuffisante pour expliquer son historique. Effectivement, les événements influant le dernier état considéré sont tout simplement ignorés et pourtant jouent un rôle essentiel dans la connaissance des causes de son avènement. Néanmoins, Demmou et all [120], Sadou et all [121] ont montré la correspondance parfaite entre les RdP et la LL.

La figureII.10 ci-dessous résume les différentes procédures d'analyse en utilisant les RdP comme modèle de base pour l'analyse des risques.

6. RdP où chaque transition T_i du réseau est associée un intervalle statique de temps $d(T_i) = [d_{imin}(T_i), d_{imax}(T_i)]$qui décrit une durée de sensibilisation.

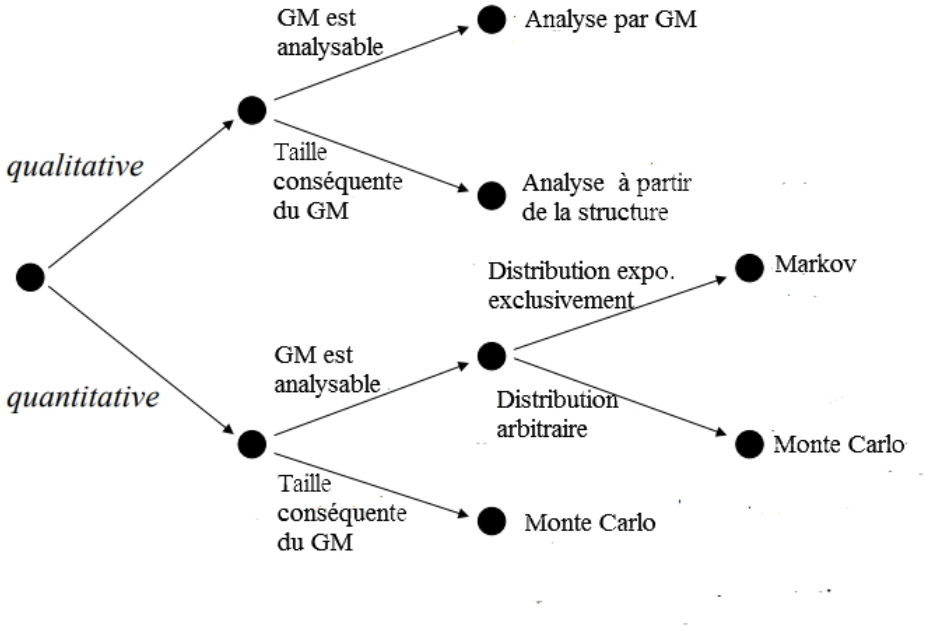


FIGURE II.10: Indication de la méthode d'analyse en fonction du modèle RdP.

II.3 Synthèse

Après ce tour d'horizon sur les principaux travaux récents attraits à la SdF, nous allons résumer leurs principales contributions. Au travers de cette synthèse, nous évoquerons ce que nous avons retenu de ces travaux.

L'analyse de la SdF utilisant ***les arbres de défaillances et leurs extensions*** disposent d'un formalisme de description graphique, commode qui permet de visualiser instantanément les coupes minimales de défaillances conduisant à l'occurrence d'événements redoutés. Par contre l'utilisation de ces formalismes rencontre quelques limites quand il s'agit de les appliquer sur un système dynamique hybride.

A retenir

La description graphique (le modèle) doit permettre de visualiser les chemins menant à l'état critique.

Dans la méthode des Boolean logic Driven Markov Processes (BDMP), l'éternel problème de l'explosion combinatoire est considérablement limitée par l'emploi de la notion d'événement pertinent, puisque des parties du système seront perdues.

A retenir

Détecter les événements pertinents dans le modèle est d'une grande aide pour éviter l'explosion combinatoire

Dans la méthodologie des ***Graphes de Flux Dynamiques***, la prise en compte explicite

des interactions entre la partie logicielle et la partie matérielle lors de la modélisation est un point à retenir. Aussi la méthode montre qu'à partir de la construction d'un seul modèle du système étudié, il est possible de générer automatiquement des arbres de défaillance, et ce, pour chaque événement redouté, ce qui est intéressant. A travers cette méthode, nous constatons aussi que l'analyse des relations de cause à effet (ou relations de causalité) dans le modèle permet une meilleure caractérisation des scénarios redoutés.

Hormis l'incapacité de la méthode à prendre en compte les caractéristiques stochastiques des composants des systèmes, discrétiser systématiquement toutes les variables du système étudié représente un inconvénient majeur de cette méthode quand il s'agit de systèmes de taille industrielle.

A retenir

La prise en compte des interactions existants entre les différentes parties du système est essentielle.
Les liens de causalité doivent être bien mis en évidence

Dans la deuxième catégorie de méthodes,les méthodes à base de modèle transformation, en plus des avantages de la modélisation orienté-objet qui est très appréciée, la notation standardisée pour décrire le système reste un point fort de la méthode. En revanche après une modélisation, une transformation (à l'aide de lois de transformation et algorithmes), vers d'autres modèles d'analyse de sûreté de fonctionnement du modèle conçu est établie, pour effectuer différentes analyses, ceci dit la question qui se pose est l'adéquation des modèles résultants pour l'analyse de SdF des systèmes dynamiques hybrides.

A retenir

Une modélisation orientée objet et une notation standardisée pour décrire le système sont deux points appréciés.

Dans la troisième catégorie nous avons constaté que l'étape de modélisation joue un rôle crucial dans l'analyse de SdF des systèmes. Le formalisme de modélisation choisi, influe sur la manière d'aborder le problème, cette catégorie donne un plus grand choix et une plus grande flexibilité dans l'étape analyse.Procéder en utilisant cette catégorie pour effectuer l'analyse de la sûreté de fonctionnement des systèmes dynamiques hybrides nécessite le choix d'un formalisme capable de représenter le système d'une façon réaliste.

A retenir

Lors de la description, la prise en compte de la nature du système est essentielle.
Les méthodes à base de modèles formels procurent une plus grande flexibilité dans l'étape analyse.

II.4 Conclusion

Après ce tour d'horizon sur les principaux travaux ayant attraient aux méthodes d'analyse de la sûreté de fonctionnement des systèmes complexes, pour les objectifs recherchés dans ce travail de thèse, ont été privilégiées les méthodes basées sur un modèle formel.Cette catégorie nécessite une étape de modélisation suivie d'une étape d'analyse qui sera présentée dans le chapitre suivant.

Chapitre III

Modélisation et analyse des risques des systemes mécatroniques

III.1 Introduction

Comme nous venons de le mentionner dans le chapitre précédent, pour des fins d'analyses des risques, trois étapes sont à considérer : Modélisation,analyse qualitative, analyse quantitative.
L'étape modélisation joue un rôle crucial,cependant, une parfaite connaissance des modèles employés permettra de sasser et d'en tirer un hybride le plus adapté au type des systèmes étudiés.
Une fois le modèle choisi nous passerons à l'étape analyse(qualitative puis quantitative) selon le modèle choisi.
Il est à préciser, que des analyses dites fonctionnelle et dysfonctionnelle précédent une analyse des risques. Dans notre travail ces analyses sont effectuées avant l'étape de modélisation permettant ainsi de mieux caractériser les fonctions offertes par un produit ainsi que de recenser les défaillances possibles.

III.2 Analyse fonctionnelle

L'analyse fonctionnelle établit de façon systématique et exhaustive les relations fonctionnelles à l'intérieur et l'extérieur du système. Une première analyse fonctionnelle dite analyse fonctionnelle externe (AFE) consiste à rechercher les fonctions offertes par un

système pour satisfaire les besoins de son utilisateur et couvre aussi la relation entre le système étudié et son environnement extérieur à travers les limites physiques du système. Par la suite, une analyse fonctionnelle interne (AFI) donne une décomposition hiérarchique et arborescente du système en éléments matériels avec les fonctions techniques de chaque composant du système ainsi que les probables contraintes.

III.2.1 Analyse fonctionnelle externe

Dans l'analyse fonctionnelle externe, en plus de la nécessité de montrer clairement les fonctions principales (FP) et les fonctions secondaires (FS) ainsi que les relations de celles-ci avec le milieu extérieur, il est indispensable également de délimiter les frontières du système étudié.
La méthode APTE (APplication aux Techniques d'Entreprise) est la méthode la plus utilisée pour établir une AFE.

Methode APTE

La démarche de la méthode APTE est divisée en quatre étapes principales :

— La mise en évidence du besoin à satisfaire en utilisant un formalisme nommé ***bête à cornes***. Celle-ci représente la matérialisation du besoin, trois questions sont posées : La première (à qui ?) nous permet de savoir à qui le système rend-il service, la deuxième question (sur quoi ?) consiste à montrer sur qui ou sur quoi le système agit-il et enfin la troisième question (pourquoi ?) illustre l'intérêt de l'action et aussi le besoin du système comme le montre la figure III.1.

— La recherche des milieux extérieurs ;

— La détermination des fonctions principales et des fonctions de contraintes ;

— La schématisation permettant de faire apparaitre les lignes de flux.
Ces trois dernières étapes utilisent le schéma de la ***Pieuvre*** comme montré sur la figure III.2

Comme mentionné au chapitre précédent,de nombreux chercheurs démontrent tous les avantages d'une notation standardisée pour décrire le système[61, 56, 58, 60, 124]. Dans ce contexte, à l'aide des diagrammes UML, il est possible d'établir une AFE. Dans ce travail de thèse, pour une compréhension unique de tous les acteurs du projet, cette

analyse est réalisée par l'utilisation du diagramme cas d'utilisation UML (use case) [125, 126].

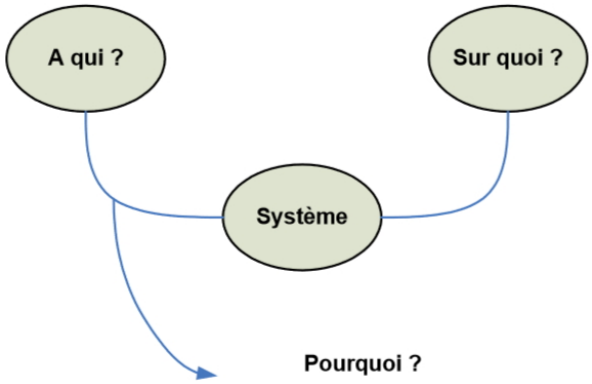


FIGURE III.1: Formalisation du besoin par une bête à cornes [1]

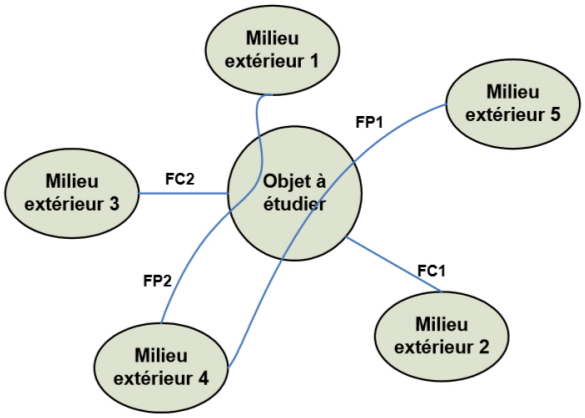


FIGURE III.2: schéma de pieuvre [1]

Digramme cas d'utilisation

Le diagramme de cas d'utilisation UML, représenté par une boîte rectangulaire, permet de visualiser les actions réalisées par un système ou par un acteur (externe ou interne).
Un acteur externe, au sens UML, simule le rôle d'une entité externe (utilisateur humain ou non) interagissant avec le système, et un acteur interne celui d'une entité interne (pouvant être constituée de plusieurs composants du système) réalisant les fonctions du système.

Dans les fonctions d'un système on distingue d'abord les fonctions principales et secondaires. Une fonction principale (la fonction pour laquelle le produit est créé), peut engendrer à son tour une ou plusieurs fonctions internes produites par les acteurs internes.
Une fonction secondaire est une fonction nécessaire, mais elle est considérée comme secondaire par rapport à la fonction principale.
La figure III.3 montre un exemple d'un cas d'utilisation. L'acteur est symbolisé par un bonhomme en fil de fer (en anglais stick man), généralement on trouve à droite l'acteur externe, et à gauche les acteurs internes.

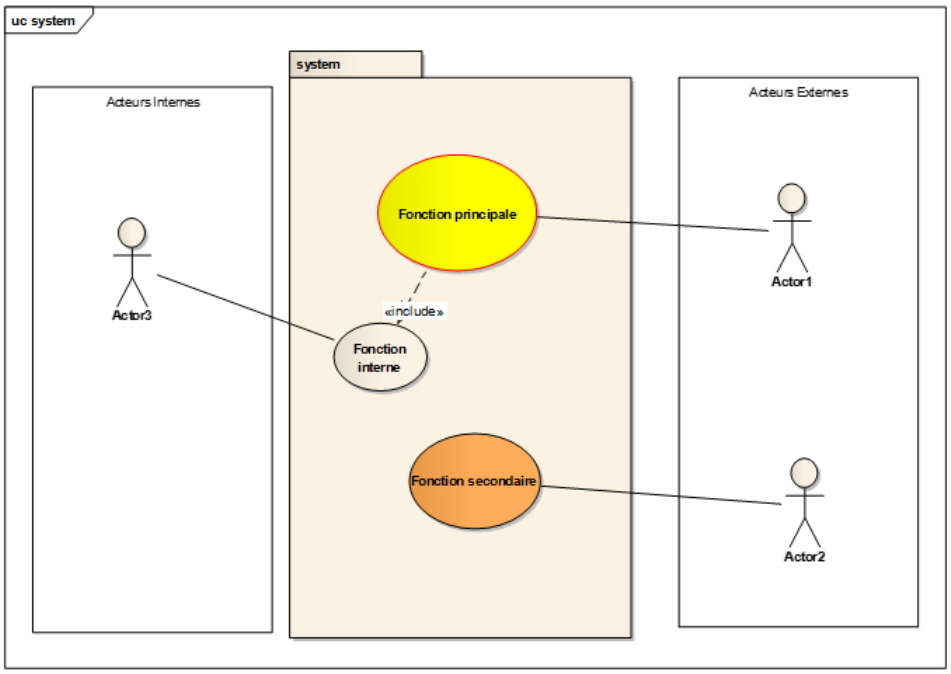


FIGURE III.3: Formalisation de l'analyse fonctionnelle externe par le diagramme de cas d'utilisation.

III.2.2 Analyse fonctionnelle interne

L'AFE est complétée par une analyse fonctionnelle interne (AFI) permettant d'obtenir une décomposition arborescente et hiérarchique du système étudié en éléments matériels et/ou fonctionnels, et aussi de déterminer toutes les fonctions techniques du système. La méthode SADT (Structured Analysis and Design Technique) peut être utilisée pour effectuer cette analyse.

Methode SADT (Structured Analysis and Design Technique)

La méthode SADT consiste à considérer tout système complexe comme une structure composée de systèmes plus simples en interaction.Un modèle SADT est constitué d'un ensemble hiérarchisé de diagrammes permettant de représenter à divers niveaux de détail et sous une forme relativement concise, des systèmes simples à très complexes. Ces diagrammes sont constitués de 5 à 6 boites afin d'éviter que le diagramme soit trop complexe. La méthode propose deux formes de représentation (actigramme et datagramme). La figure III.4 représente une boite d'activité dans laquelle on met l'accent sur les fonctions du système.

— Les entrées connectées à gauche, sont transformées par l'activité pour produire les sorties qui sont connectées à droite.

— Les contrôles connectés en haut ne sont pas modifiés par l'activité mais agissent sur cette dernière en la déclenchant ou en influant fortement sur son comportement.

— Les mécanismes connectés en bas permettent de décrire les éléments physiques et les moyens mis en œuvre pour réaliser la fonction.

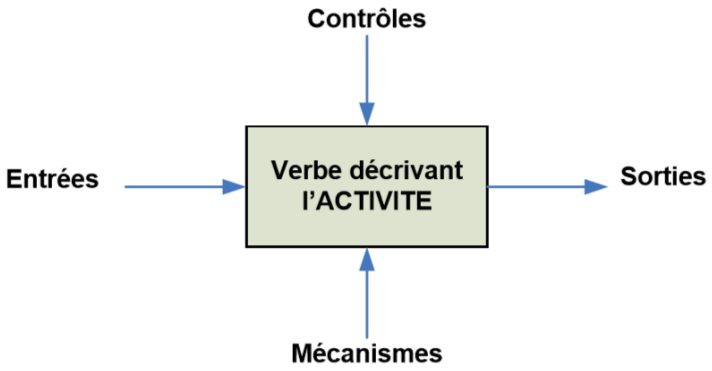


FIGURE III.4: Actigramme [1].

Un diagramme représente une fonction plus ou moins vaste. Afin d'obtenir plus de précision, les diagrammes se construisent selon une approche descendante c'est-à-dire du général vers le particulier. Il n'existe aucune limite théorique à cette décomposition par affinage. Seul le rédacteur et ses interlocuteurs sont à même de juger quand le niveau atteint parait suffisant.
De la même manière,pour une notation standard, dans ce travail de thèse, lors de l'analyse fonctionnelle interne, la décomposition du système en éléments matériels et/ou fonc-

tionnels et la désignation de toutes ses fonctions techniques, se fait à l'aide du diagramme de classes UML.

Digramme de classe

Le diagramme de classes décrit la structure du système. Chaque classe du diagramme identifie un composant ainsi que les fonctions qu'il réalise à travers des attributs et des opérations. Les diverses relations qui peuvent existées entre les classes y sont également représentées, comme le montre la figure III.5.
Le diagramme de classes appartient à la partie statique d'UML car il fait abstraction des aspects temporels et dynamiques[125, 126].

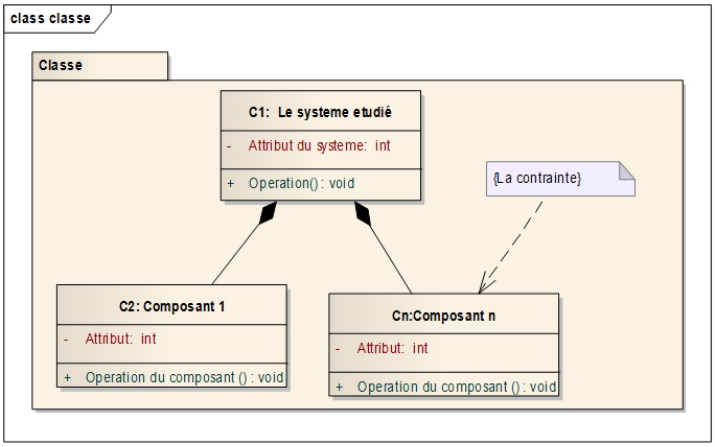


FIGURE III.5: Analyse fonctionnelle interne par le diagramme de classes

Les analyses fonctionnelles externes et internes, sont accompagnées par la définition des contraintes imposées au système par son milieu extérieur. Cela revient à identifier les relations entre les objets d'une classe et un élément du milieu extérieur. Ces relations sont appelées : fonctions de contrainte (FC).
Une contrainte peut être exprimée à l'aide du langage OCL (Object Constraint Language)[127] associé au langage UML en l'insérant entre deux accolades ({}) dans une note (Figure III.5). L'élément pointé par la note est alors le contexte de la contrainte.
Ces analyses fonctionnelles interne et externe ne nous donnent, cependant, aucune information concernant les défaillances, d'ou la nécessité de réaliser une analyse dysfonctionnelle qualitative qui permet de compléter les informations manquantes et de lister tous les dysfonctionnements potentiels que peut subir le système mécatronique.

III.3 Analyse dysfonctionnelle

L'analyse dysfonctionnelle, à son tour, complétera les informations sur le système et son environnement, par l'identification de ses différents états et modes de défaillance.

Methode d'Analyse des Modes de Défaillance et de leur Effets(AMDE)

L'AMDE (Analyse des Modes de Défaillance et de leur Effets) [9, 128] est largement utilisée dans le domaine de la sûreté de fonctionnement. Cette analyse consiste à étudier les unes après les autres les différentes fonctions du système (principales FP, secondaires FS et de contrainte FC) qui ont été identifiées et définies au cours de l'analyse fonctionnelle. Pour chacune d'elles, l'étude consiste à recenser les modes de défaillance conduisant à une dégradation, et à identifier leurs causes et leurs effets.
Une forme tabulaire classique de l'AMDE fonctionnelle est donnée dans le tableau III.1suivant :

TABLE III.1: Tableau AMDE

Fonctions du système (FP+FS+FC)	Fonctions internes	Composants	Modes de défaillance	Causes	Effets

Après la définition des fonctions du système ainsi que toutes les défaillances et les causes pouvant affecter le bon fonctionnement du système nous passons à l'étape de modélisation.

III.4 Modélisation des systemes dynamiques hybrides

Comme mentionné dans le chapitre II, le formalisme choisi influt d'une façon significative dans la suite de nos travaux. Une parfaite connaissance des modèles employés permettra de sasser et d'en tirer un hybride le plus adapté au type des systèmes étudiés. Selon la nature dynamique hybride des systèmes mécatroniques,on présente dans cette section quelques approches de modélisation permettant la description comportementale de ce type de systèmes. De manière générale, ces approches de modélisation peuvent être classées en trois catégories principales[129].

III.4.1 Extension de techniques de modélisation issue des systèmes continus

Cette approche consiste à prendre en compte l'aspect discret par une extension d'un formalisme continu. Ce type d'approche s'adapte bien aux systèmes intégrant quelques aspects discrets mais qui sont fondamentalement continus. Quand l'aspect discret est conséquent l'approche devient inutilisable car très lourde à mettre en œuvre[51]. L'extension du ***formalisme des bonds de graphs*** [130] [131][129] pour la modélisation d'une classe de système hybride en est un exemple.

III.4.2 Extension des techniques de modélisation issue des systèmes discrets

L'exemple type de cette catégorie est celui des ***RdP hybrides*** développés par Alla et all [109]. Contenant des places discrètes et des places continues ils permettent de représenter au sein d'un même formalisme ce couplage entre un fonctionnement discret et un fonctionnement continu (représentation graphique unifiée des variables continues et des variables discrètes). L'exemple dans la figureIII.6 illustre cette interaction entre partie continue et partie discrète.
Ce type d'approche prend en compte que les équations linéaires et ne permet ni de considérer les équations différentielles générales, ni de représenter des équations algébriques.

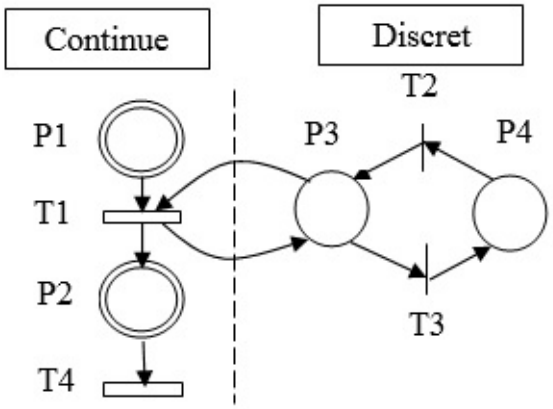


FIGURE III.6: RdP Hybride

III.4.3 Les approches mixtes

Les modèles mixtes reposent sur la collaboration de deux sous modèles, l'un pour l'aspect discret, basé sur les automates d'état fini, les RdP ou les extensions de ces formalismes et l'autre formalisé par des équations d'état pour l'aspect continu. Chacun de ces deux aspects, discret ou continu, est ainsi décrit sous une forme classique et l'aspect hybride est clairement pris en compte dans l'interface entre les deux sous modèles : l'aspect discret influe sur le modèle continu en validant certaines des équations continues en fonction du mode discret actif et inversement, l'aspect continu agit sur le modèle discret en validant ou forçant le franchissement de certaines transitions.
Comme nous favorisons les RdP pour notre étude, nous présentons les RdP capables de prendre en compte la nature dynamique hybride selon l'approche mixte.

Les RdP et l'approche hybride

L'extension des formalismes continus tend à restreindre la flexibilité de modélisation de la partie continue. Ceci est également valable dans le cas de l'extension des formalismes discrets (restriction de la modélisation de la partie discrète). Les approches qui combinent un formalisme continu et un formalisme discret présentent une grande puissance de modélisation et de flexibilité par rapport aux deux premières classes [132].
La modélisation de l'aspect hybride de ces systèmes avec les réseaux de Petri est abordée selon deux tendances : d'une part, la tendance reposant sur l'intégration des aspects continus et discrets au sein du même formalisme, et d'autre part, celle associant un formalisme différent pour chacun des deux aspects. Dans sa thèse Andreu [133] a largement décrit les différentes approches de modélisation de l'aspect hybride : les approches séparée et intégrée.
L'approche intégrée regroupe : les RdP haut niveau et les RdP hybrides ; tandis que l'approche séparée regroupe : les RdP couplés avec des équations différentielles.
L'utilisation de modèles propres à chaque aspect permet de conserver le potentiel de modélisation dans chacun des domaines [134]. Les aspects continu et discret correspondent à deux mondes mathématiques différents offrant deux vues différentes du système. La vue discrète n'est pas seulement une abstraction du phénomène continu ; les deux vues sont complémentaires[133]. L'idée d'associer à chaque partie du système un formalisme différent permet de séparer clairement la partie discrète de la partie continue. Cela permet aussi de conserver le potentiel de modélisation dans chacun des domaines. En effet,

la complexité de la partie continue du modèle hybride est totalement découplée de celle de la partie discrète.
Les réseaux de Pétri associés à des équations différentielles regroupent deux types de réseaux de Pétri : les réseaux de Pétri mixtes [129]et les réseaux de Pétri Prédicats-Transitions Différentiels[135].
Les deux approches, réseaux de Pétri Prédicats-Transitions Différentiels et réseaux de Pétri Mixtes, partagent un même principe de base : l'évolution des variables continues est définie par un ensemble d'équations différentielles et algébriques. L'ensemble des équations est défini à partir du marquage du réseau de Petri et le franchissement de transitions dépend du dépassement de seuils sur les variables continues ou leurs dérivées. Soit les variables continues sont supposées globales (réseaux de Petri Mixtes), soit elles correspondent aux attributs des jetons (Reseaux de Petri Prédicats-Transitions Différentielles$RDPPTD$).
Les RdP Prédicats-Transitions Différentielles sont bien adaptés pour une approche modulaire et compositionnelle de représentation des systèmes complexes, ce qui permet une conception structurée du modèle.

Les réseaux de Petri Prédicats Transitions différentiels Le comportement hybride est pris en compte en associant les variables représentant l'état continu à des jetons et en associant à chaque place un ensemble d'équations algébro-différentielles (algébriques et/ou différentielles), notées EAD. Un jeton mis dans une place déclenche l'intégration des équations correspondantes. Parallèlement à l'intégration, plusieurs seuils sont surveillés. Chaque seuil surveillé est associé à une transition avale d'une place marquée. Quand le seuil est franchi, cela signifie que l'événement attendu correspondant est apparu, et la transition associée à ce seuil est franchie. Un nouveau marquage est calculé et l'intégration du nouveau système démarre. Si deux jetons sont dans la même place, les variables de chacun d'eux évoluent, indépendamment les unes des autres, selon les mêmes équations associées à la place.

Définition 13 ***(RdP Prédicats-Transitions Différentiels)[135] :*** *Le modèle RdP Prédicats-Transitions Différentiels (RdP PTDS)est défini, par le triplet* $< P, T, M >$ *où :*

— $P = \{P_1, P_2, P_3, ..., P_n\}$ *est un ensemble fini de places.Les places de ce modèle sont décrites par la paire* $< P, F >$ *où :*

— *F est un système d'équations différentielles et/ou algébriques associe à chaque place Pi modélisant l'aspect continue du système. F est défini comme suit :*

$$F = \begin{pmatrix} F_i(\dot{x_i}, x_i, t) \\ \vdots \\ F_n(\dot{x_n}, x_n, t) \end{pmatrix} \; i = 1, ..., n$$

— $T = \{T_1, T_2, T_3, ..., T_m\}$ *est un ensemble fini de transitions,décrites par le triplet* $< T, e, J >$ *où :*

— $T = \{T_1, T_2, T_3, ..., T_m\}$ *est un ensemble fini de transitions.*

— $e = \{e_1, e_2, ..., e_m\}$ *est l'ensemble des fonctions de* ***sensibilisation****, associée à chaque transition* T_i*, qui impose des conditions supplémentaires aux franchissements des transitions, elle peut être :*

- *Une condition de franchissement liée à un marquage d'une place,*
- *Une loi de probabilité définissant le processus stochastique de défaillance et de réparation quand elle est associée à une transition stochastique,*
- *Un seuil à atteindre quand elle est associée à une transition déterministe, cad selon la valeur des variables continues associées aux places en amont de la transition* T_i *, la transition est franchie à la date à laquelle le seuil donné par la fonction de sensibilisation est atteint. Cette date est obtenue par la résolution de l'équation attachée à la place en amont de la transition.*

— $J = \{J_1, J_2, ..., J_m\}$ *est l'ensemble des fonctions de* ***jonction*** *associées aux transitions. Lors du franchissement d'une transition, les fonctions de jonction associées sont activées. Lors du franchissement de* T_j *à la date t,la fonction* J_j *associée à la transition* T_j *calcule les valeurs des variables ainsi que leurs dérivées. Ce qui signifie que les valeurs des variables, et de leurs dérivées, juste après t (à t+) sont calculées à partir de valeurs des variables, et de leurs dérivées, juste avant t (à t−). Ceci permet de redéfinir les attributs des jetons en cas de discontinuité.*

□

L'exemple, tiré de l'ouvrage de Zaytoon [129] présenté dans la figure III.7, permet d'illustrer le principe des $RdPPTD$. La partie droite de la figure montre l'évolution des variables associées à deux jetons A et B dans le réseau de Petri PTD de la partie gauche.

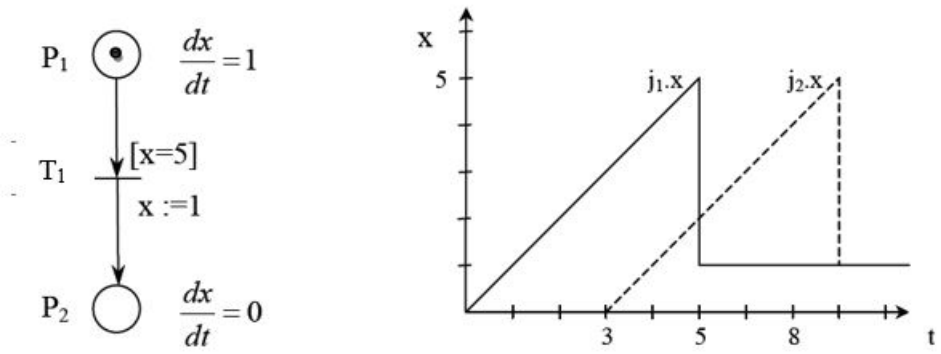


FIGURE III.7: Principe des réseaux de Petri Prédicats-Transitions Différentiels

Ce réseau est constitué de deux places P_1 et P_2 et d'une transition T_1. A chacune des places P_1 et P_2 est associée une équation différentielle.
A la transition T_1 sont associées une fonction de sensibilisation (le seuil$[x = 5]$) et une fonction de jonction $(x := 1)$. Le premier jeton est introduit dans la place P_1 à l'instant $t = 0$ et le second à l'instant $t = 3$. A l'instant $t = 5$, la transition T_1 devient franchissable pour le premier jeton qui la franchit en subissant le saut $(x := 1)$ alors que le second jeton franchit cette même transition à l'instant $t = 8$.

Nous avons passé en revue les différents formalismes de modélisation des systèmes dynamiques hybrides, parmi lesquels les formalismes dérivés des RdP ont été privilégiés. D'une part en raison des avantages et de la capacité des RdP à modéliser le parallélisme, la synchronisation et le partage de ressources mais aussi ont connus depuis leur invention un réel succès en raison de leur simplicité mathématique, des avantages de la représentation graphique et de leur compacité, et d'autre part pour la bonne adéquation des réseaux de Petri à la modélisation de systèmes dynamiques hybrides.
Ainsi, notre choix s'est porté sur les réseaux de Petri Prédicats Transitions différentiels, modèle qui combine deux formalismes distincts, les réseaux de Petri pour la modélisation des aspects discrets et les équations différentielles pour la partie continue.
La motivation qui nous a poussés à faire ce choix est que les réseaux de Petri Prédicats Transitions Différentiels sont plus appropriés que les réseaux de Petri mixtes en raison de l'absence de variables globales. Toutefois, pour étudier la sûreté de fonctionnement de ces systèmes, nous avons besoin de prendre en compte l'aspect stochastique. Cet aspect est lié aux mécanismes de défaillances et de reconfigurations inhérents aux systèmes méca-

troniques. Pour cette raison, nous introduisant le formalisme RdP Prédicats-Transitions Différentiels stochastiques ($RdPPTDS$) intégrant ces aspects non déterministes.
Aussi, le formalisme n'offre pas la possibilité d'une décomposition du système ou une modélisation progressive, ce qui rend la tâche de modélisation mais aussi l'analyse des systèmes de taille conséquente difficile. Une solution pour faciliter la modélisation de ces systèmes complexes est d'introduire le paradigme Orienté Objets (OO) dans le formalisme [136]. Le principe du paradigme orienté objets consiste à décomposer le système en un certain nombre d'objets qui interagissent entre eux. Ceci permet de structurer la décomposition du système et maîtriser sa complexité. Le modèle $RdPPTDS-OO$qui en résulte, grâce à sa structure modulaire fournit une flexibilité dans la modélisation mais aussi dans l'analyse des systèmes complexes. En effet, le $RdPPDTS-OO$d'un système complexe est facilement établi suite à sa décomposition en classes et objets. Un autre avantage de l'approche objets est la réutilisation des modèles. Lors de l'analyse de sûreté de fonctionnement le concepteur aura à tester plusieurs configurations, plusieurs architectures. Grâce à la réutilisabilité offerte par l'approche objets, en cas de modification d'architecture, certains composants du modèle initial pourront être réutilisés, le modèle initial ne sera pas complètement remis en cause.
La définition de ce formalisme de modélisation est donnée comme suit :

Définition 14 ***(RdP Prédicats-Transitions Différentiels stochastiques Orienté Objets)[136]*** *: Un RdP Prédicats-Transitions Différentiels stochastiques Orienté Objets ($RdPPTDS-OO$)est un ensemble fini Nde sous $RdPPTDS-OO-i$. Avec$N = \{PDTS-OO-1, PDTS-OO-2, ..., PDTS-OO-C\}$, où C est le nombre de classes décrivant le comportement dynamique des sous-systèmes.*

□

Définition 15 ***(Sous RdP PTDS-OO)*** *: Un sous $RdPPTDS-OO-i$ est un 4-tuple, avec $RdPPTDS-OO-i =< C_i, R_i, A_i, M_{0-i} >$, où :*

- *C_i est le nom de la classe,*
- *R_i est un réseau de Petri définit par le 4-tuple $< P_i, T_i, Pre_i, Post_i >$avec :*
  - *$P_i = \{P_{1-i}, P_{2-i}, P_{3-i}, ..., P_{n-i}\}$ est un ensemble fini de places,*
  - *$T_i = \{T_{1-i}, T_{2-i}, T_{3-i}, ..., T_{m-i}\}$ est un ensemble fini de transitions avec $T_i = T_s \cup T_d$ où T_s sont les transitions stochastiques (modélisant un mécanisme de*

défaillance où de réparation) et T_d les transitions déterministes (modélisant le fonctionnement du système)

- $Pre_i : P \times T \longrightarrow (0,1)$ *est l'incidence arrière,*
- $Post_i : P \times T \longrightarrow (0,1)$ *est l'incidence avant,*

— A_i *est l'annotation de chaque classe* C_i, $A_i =< X_i, e_{k_i}, j_{k_i}, F_{k_i} >$ *avec :*

- X_i est l'ensemble des variables utilisées pour décrire la partie continue du système.
- e_{k_i} est une fonction de sensibilisation associée à chaque transition T_{k_i}, qui impose des conditions supplémentaire aux franchissements des transitions,
- j_{k_i} une fonction de jonction associée à chaque transition T_{k_i} qui impose un saut discret sur la valeur des variables continues.
- F_{k_i} un système d'équations différentielles et/ou algébriques associe à chaque place P_{k_i} modélisant l'aspect continue du système.

— M_{0_i} le marquage initial du sous-réseau.

□

Un concept-clé pour définir la communication entre objets est l'encapsulation. La communication entre les objets est possible grâce à des appels de méthodes ou bien grâce aux fonctions de sensibilisation.
Le modèle RdP est composé de deux ensembles de transitions, les transitions offertes et les transitions utilisées. Chaque transition utilisée dans une classe, ex : classe C_1 dispose dans une autre classe ex : classe C_2 d'une transition offerte correspondante, comme le montre la figure III.8. Dans la figure III.8, lorsque la transition utilisée (T_{11}) de la classe C_1 est sensibilisée, la classe C_1 appelle la transition offerte correspondante (T_{12}) dans la classe C_2. La communication entre les deux classes a lieu par fusion de leurs transitions mutuelles permettant un franchissement commun. On représente les méthodes utilisées par un rectangle noir et les méthodes offertes par un rectangle transparent.
La communication entre les objets peut se faire aussi grâce à la condition imposée par les fonctions de sensibilisation quand cette condition est liée au marquage d'une place dans une classe du RdP. Par exemple dans une classe C_i le franchissement d'une transition T_{i-k} est associée à la fonction de sensibilisation $e_{i-k} : P_{o_k} = 1$, ceci signifie que T_{i_k} est franchie seulement si la place P_{o_k}de la classe C_o est marquée.

Par exemple dans la figure III.8, le franchissement d'une transition T_{11} de la classe C_1 est associé à la fonction de sensibilisation $e_{11} : P_{13} = 1$, ceci signifie qu'une des conditions du franchissement de T_{11} est le marquage de la place P_{13} de la classe C_2.

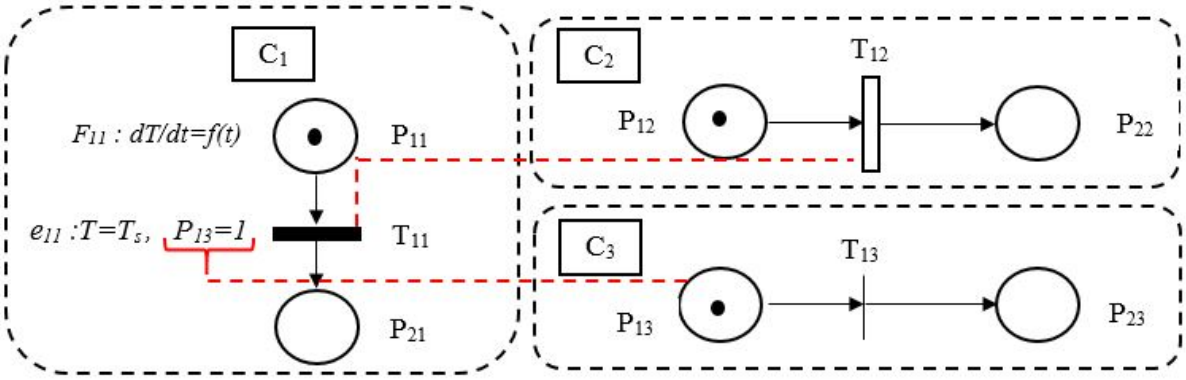


FIGURE III.8: Communication entre les classes du RdP PTDS-OO

III.4.4 Exemple de la modélisation d'un système mécatronique

Système d'anti blocage des roues (ABS)

Pour arrêter ou ralentir un véhicule, il faut dissiper son énergie cinétique. Actuellement, cela se réalise sous forme thermique en serrant un élément monté sur l'arbre de roue (disque ou tambour) avec une plaque (plaquette ou garniture) munie d'un matériau de friction et reliée au châssis via les éléments de suspension. Généralement, les constructeurs utilisent des disques de freins qui sont serrés par des mâchoires équipées de plaquettes montées sur des étriers. Ces étriers sont actionnés par un ou plusieurs pistons hydrauliques dans lesquels le fluide hydraulique applique la pression engendrée par le maître-cylindre actionné par la pédale de frein. Depuis 2004, tous les véhicules livrés par les constructeurs sont équipés de l'ABS qui n'est donc plus une option. L'ABS module la pression de freinage indépendamment de la force agissant sur la pédale, pour ramener la vitesse de la roue dans la plage où le niveau de glissement est nécessaire pour une performance de freinage optimale. Tout dérapage au freinage allonge la distance d'arrêt et met en danger la stabilité du véhicule. L'ABS constitue donc un plus indéniable pour le confort de conduite et pour la sécurité. Ce dispositif a été introduit pour la première fois en 1978 sur la Mercedes Class S [1, 137, 138]. Lorsque l'adhérence sur la chaussée n'est pas suffisante au freinage, la roue se bloque et s'arrête de tourner alors que le véhicule

continue sur sa lancée. L'efficacité du freinage est nettement amoindrie et le conducteur perd tout pouvoir directionnel. L'ABS permet, lorsque le blocage d'une roue est détecté, de relâcher la pression du circuit hydraulique sur celle-ci, puis, de l'augmenter à nouveau jusqu'à un nouveau blocage éventuel, auquel cas le cycle recommence. Les ABS actuels permettent une fréquence de l'ordre de 60 cycles par seconde.
La figure III.9 montre les différents composants du système ABS. C'est un système qui s'intercale entre le maitre-cylindre et les freins de roue.Le système est composé d'un capteur(1) d'un modulateur composé de deux électrovannes (électrovanne de maintien de pression et électrovanne de diminution de pression) et une pompe (2), et d'un calculateur (ECU)(3).

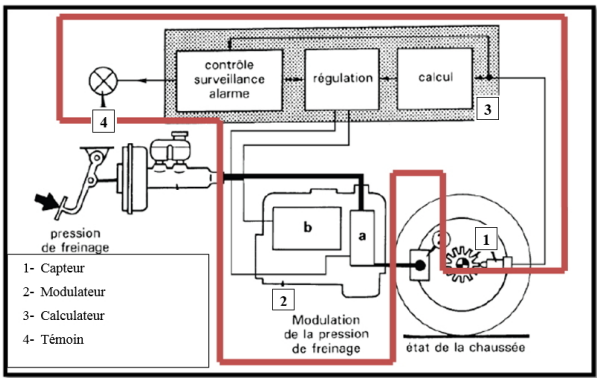


FIGURE III.9: Les composants du système ABS.

Principe de fonctionnement du système ABS

Durant un freinage normal, le conducteur applique une pression hydraulique dans le maitre-cylindre quand il appuie sur la pédale cette pression est transmise intégralement aux 4 freins du véhicule lorsque l'ABS est déconnecté électriquement ou en mode surveillance active des vitesses de roue sans activité hydraulique. Autrement dit, le liquide de frein se déplace du maître-cylindre jusqu'au modulateur. Une fois dans l'unité, le liquide se déplace à travers l'électrovanne de maintien de pression normalement ouverte (N.O) et puis, s'écoule dans les étriers afin de freiner la roue comme le montre la figureIII.10.
Quand le système détecte un blocage de roue, l'ABS agit hydrauliquement :
Ferme l'électrovanne de maintien pour abaisser la pression dans l'étrier, *Ouvre* l'électrovanne de diminution de pression en libérant la pression vers un accumulateur interne.

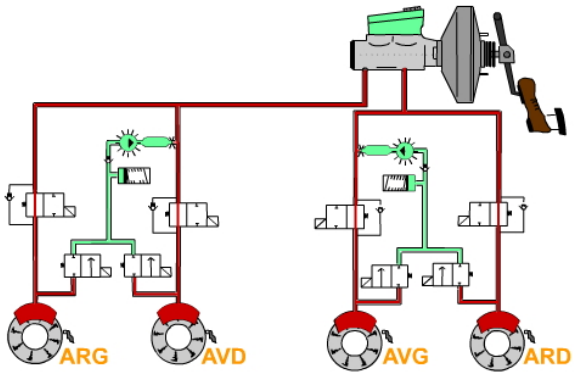


FIGURE III.10: Principe de fonctionnement du système ABS :freinage normal

Dans le schéma suivant(figureIII.11), la roue qui se bloque est la roue avant droite.

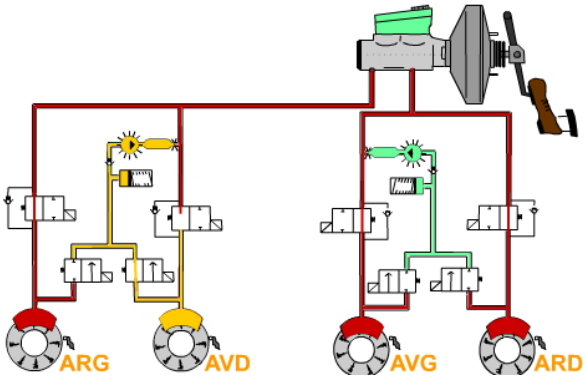


FIGURE III.11: Principe de fonctionnement du système ABS :Blocage de roue

Ensuite, la pompe de l'ABS vide l'accumulateur en renvoyant le liquide vers le maitre-cylindre (figure III.12) .Quand la roue est libérée , le système revient à son état hydraulique initial (communication complète entre le maitre-cylindre et le frein). Si la roue se rebloque à nouveau ce cycle est répété autant que nécessaire ; le temps moyen d'un cycle blocage /déblocage est de l'ordre de $0.1s$.

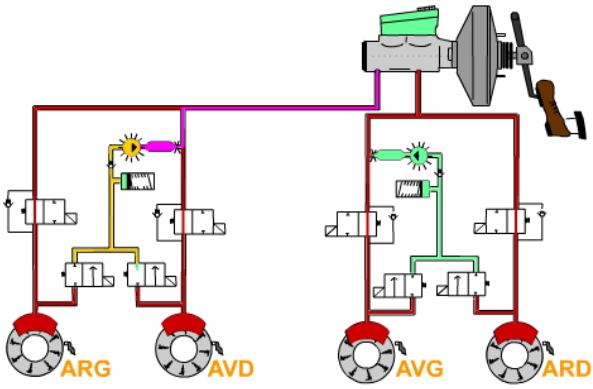


FIGURE III.12: Principe de fonctionnement du système ABS :refoulement de liquide de freinage

Modélisation du système ABS

Comme nous l'avons déjà mentionné, une construction efficace du modèle utilisant le RdP peut être réalisée que si les informations tels que les fonctions du système, l'environnement externe, tous les composants ainsi que leurs interactions, les contraintes imposées et les possibles défaillances des composants sont soigneusement compris. Pour cette raison une analyse fonctionnelle et dysfonctionnelle doit nécessairement précéder l'étape de construction du RdP.

Analyse Fonctionnelle Cette analyse permet une description synthétique des modes de fonctionnement du système ABS, ainsi que la connaissance des fonctions qu'il doit garantir.
La réalisation de cette analyse fonctionnelle se déroule principalement en deux étapes :

- L'Analyse Fonctionnelle Externe qui a pour objectif de formaliser et de valider l'analyse du besoin ;
- L'Analyse Fonctionnelle Interne dans le but d'identifier les fonctions techniques du système à étudier.

Analyse Fonctionnelle Externe L'analyse fonctionnelle externe pratiquée sur le système ABS a conduit au diagramme de cas d'utilisation de la figure III.13.
À gauche, dans le diagramme sont représentés les acteurs internes qui sont : les électrovannes, la pompe, le capteur et l'ECU.
De même, à droite sont représentés les acteurs externes : le maître-cylindre, l'étrier, l'indicateur et la roue.

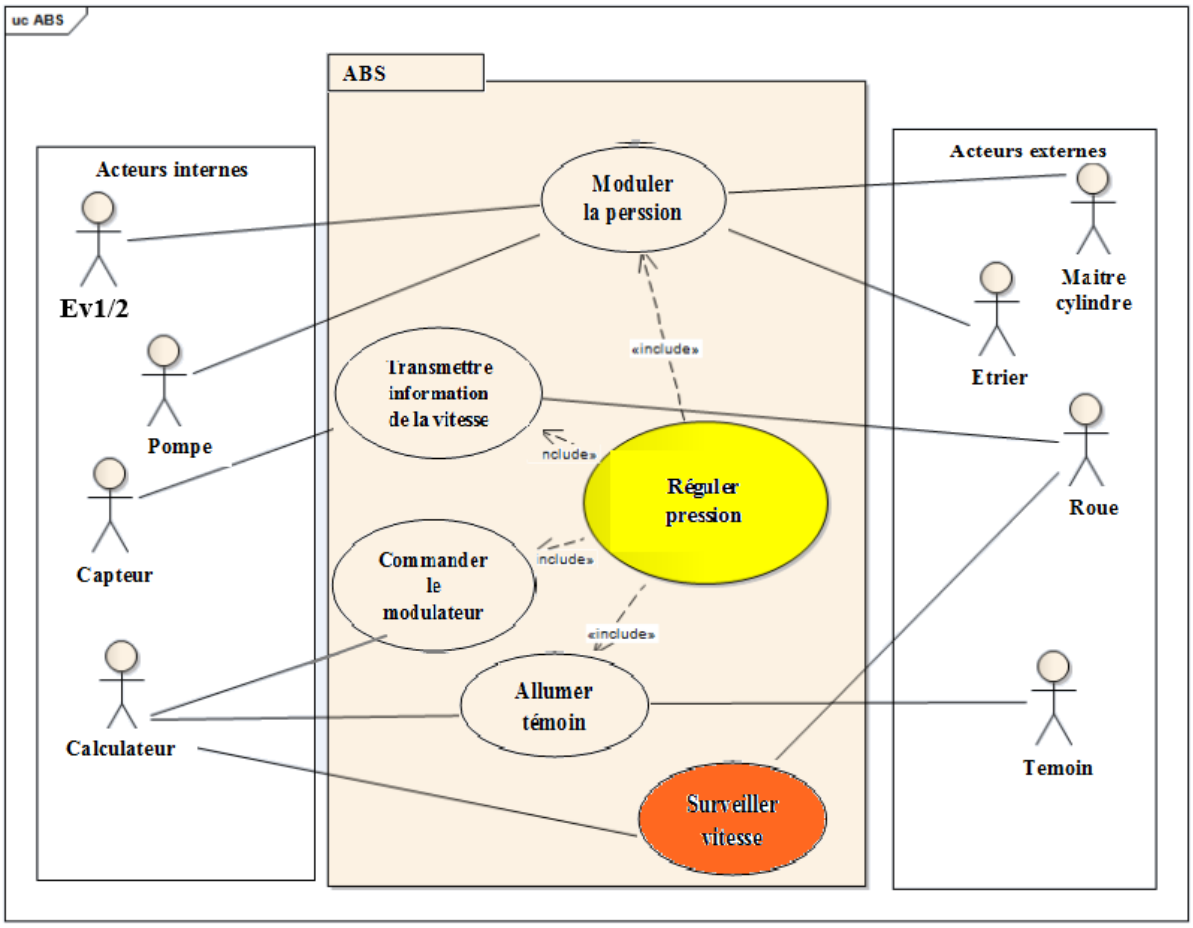


FIGURE III.13: Diagramme de cas d'utilisation du système ABS.

Au centre de la figure on retrouve les fonctions du système. La fonction principale du système ABS est de **réguler** la pression exercée sur l'étrier de frein.
Divers fonctions internes sont effectuées pour y parvenir :

- Transmettre de la vitesse de la roue à l'ECU (unité de commande électronique),
- Commander le modulateur,
- Moduler la pression sur l'étrier,
- Allumer l'indicateur.

La fonction secondaire du système est la suivante :
Surveiller la vitesse de la roue sans activité hydraulique.
Ainsi, il est facile de distinguer les différentes fonctions du système étudié.

Analyse fonctionnelle interne Pour l'analyse fonctionnelle interne, il est considéré que le système comprend un calculateur de commande du modulateur en fonction de la vitesse de la roue fournie par le capteur.
Le digramme de classes de la figure III.14 indique la décomposition arborescente et hiérarchique du système étudié, également il permet de visualiser les différentes fonctions de contrainte.

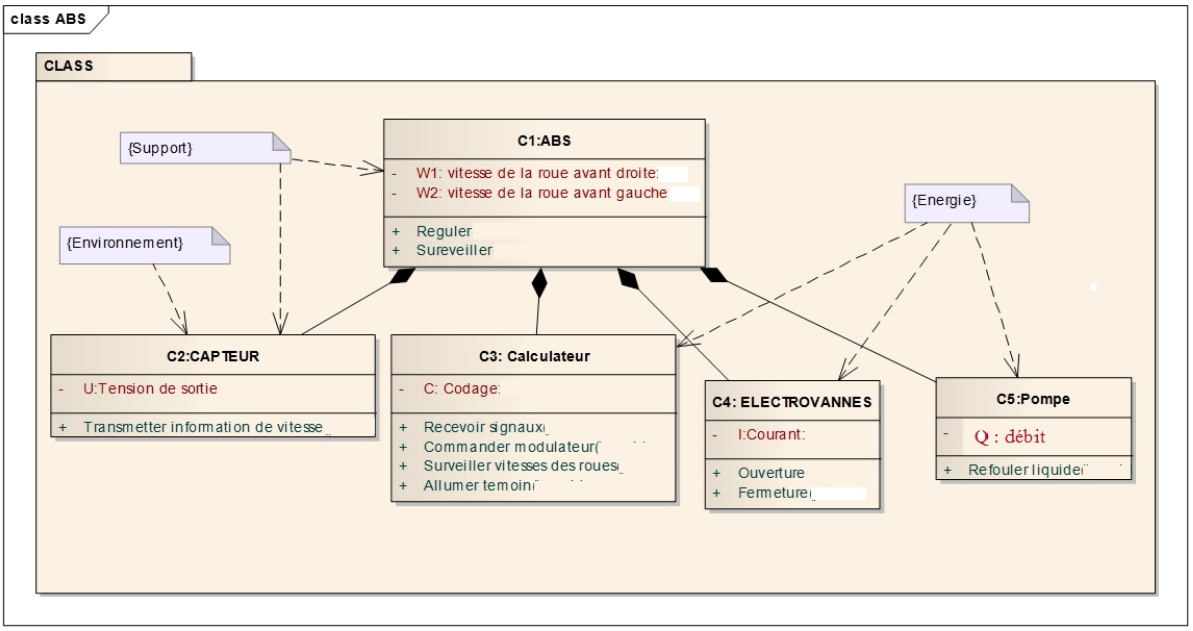


FIGURE III.14: Diagramme de classes

Le diagramme comporte cinq classes :

— La classe C_1 (classe ABS) qui représente le système, a le rapport de glissement S comme attribut, c'est-à-dire en fonction de la valeur de S le système régule la pression sur l'étrier ou surveille la vitesse de roue.

— La classe C_2 (classe de capteur) modélise le capteur de la roue. Cette classe a comme attribut la tension U. Le capteur délivre un signal de tension proportionnel à la vitesse de roue et l'envoie à l'ECU.

— La classe C_3 (classe d'ECU) décrit l'ECU du système. L'ECU reçoit des signaux envoyés par le capteur, commande le modulateur, surveille la vitesse des roues et allume l'indicateur du freinage anti-blocage.

— La classe C_4(classe électrovanne) a le courant comme attribut. Un courant circule dans la bobine de l'électrovanne, soit pour l'ouvrir ou la fermer.

— La classe C_5 (classe de pompe) décrit la pompe du système qui permet de refouler le liquide de frein au maître-cylindre.

Une relation de composition relie la classe C_1 aux classes C_2, C_3, C_4et C_5 afin de distinguer le système de ses divers composants.
Il existe trois fonctions de contraintes qui sont :

— L'énergie : **alimenter** en énergie électrique la pompe, l'électrovanne et l'ECU pour fonctionner.

— Le soutien : **soutenir** le système et le capteur.

— L'environnement : **résister** à l'environnement externe.

Analyse dysfonctionnelle de l'ABS L'analyse fonctionnelle précédemment effectuée n'apporte aucune information sur les défaillances potentielles que peut rencontrer le système ABS. Pour cette raison l'analyse dysfonctionnelle est nécessaire dans le but de nous fournir les informations et obtenir ainsi les causes de défaillance de ce même système.
L'application de l'AMDE sur le système ABS est donnée dans le tableau III.2. A chaque fonction sont décrits les modes de défaillance possibles, les causes probables et les effets redoutés.

TABLE III.2: L'AMDE du système ABS

Fonctions	Fonctions externes	Fonctions internes	Composants	Mode de défaillance	Causes	Effet
FONCTION PRINCIPALE	Refouler le liquide vers le MC	Transmettre l'information relative à la vitesse	Capteur	Pas de transmission	Capteur défaillant	Risque de blocage des roues
					Cible cassée	
					Présence de calamine	
					Pas de connexion des connecteurs	
					Coupure des connecteurs	
				Transmission altérée	Cible cassée	
					Mauvaise connexion	
					Coupure des connecteurs	
					Capteur défaillant	

TABLE III.2: L'AMDE du système ABS

FONCTION PRINCIPALE	Refouler le liquide vers le MC	Transmettre l'information relative à la vitesse	Capteur	Perte de transmission	Coupure des connecteurs	Risque de blocage des roues
					Mauvaise connexion	
					Capteur défaillant	
		Commander le modulateur	Calculateur	Pas de commande	Calculateur défaillant	
					Perte de connexion	
					Pas de connexion des connecteurs	
				Commande altérée	Faible tension	
					Calculateur défaillant	
					Coupure des connecteurs	

TABLE III.2: L'AMDE du système ABS

FONCTION PRINCIPALE	Refouler le liquide vers le MC	Commander le modulateur	Calculateur	Commande altérée	Mauvaise connexion	Risque de blocage des roues
		Ouverture ou fermeture des EV	Modulateur	Pas d'ouverture et de fermeture des EV	EV défaillante	Surpression et risque de blocage des roues /pas de freinage
					EV bloquée	
					Mauvaise connexion des EV	
					Pas de connexion des connecteurs	
		Transmettre le liquide du MC à l'étrier		Pas de transmission	Tuyauterie écrasée	Pas de freinage
					EV défaillante	
					Fuites internes	
					Niveau d'huile bas	

TABLE III.2: L'AMDE du système ABS

FONCTION PRINCIPALE	Refouler le liquide vers le MC	Transmission du liquide du MC a l'étrier	Modulateur	Mauvaise transmission	Tuyauterie écrasée	Pas de freinage
					EV défaillante	
					Fuites internes	
					Niveau d'huile bas	
		Récupérer le surplus du liquide		Pas de récupération	Présence d'air	Surpression et risque de blocage des roues
					Ev défaillante	
					Fuites internes	
					AC défaillant	
		Refouler le liquide vers le MC		Pas de refoulement	Présence d'air	
					Fuites internes	
					Pompe défaillante	
FONCTION SECONDAIRE	Surveiller la vitesse des roues	Recevoir le signal du capteur	Calculateur	Pas de réception	Usure des connecteurs	Blocage des roues
				Réception altérée		

TABLE III.2: L'AMDE du système ABS

FONCTION SECONDAIRE	Surveiller la vitesse des roues	Analyser les informations reçues	Calculateur	Pas d'analyse	Calculateur défaillant	Blocage des roues
				Analyse intempestive		
FONCTION DE CONTRAINTE	Alimenter le système	Brancher les connecteurs	Batterie	Perte de contacte électrique	Vibrations du véhicule	Pas d'assistance ABS
					Usure des connecteurs	

Dans un premier temps nous avons listé les fonctions du système : fonction principale, fonction secondaire et fonction de contrainte. Pour chaque fonction ont été établies les fonctions internes ainsi que les composants réalisant chacune d'elles. Dans un deuxième temps nous avons imaginé toutes les défaillances possibles pour chaque élément.

III.4.5 Réseau de Petri du système ABS

Détermination des équations différentielles

Pour obtenir ces équations différentielles, une roue freinée du véhicule avec tous les efforts qui s'appliquent sur cette dernière est représentée comme dans la figure III.15. ω représente la vitesse angulaire, $T_t$est le moment de frottement, $T_b$le moment de freinage, I le moment d'inertie, av représente l'accélération du véhicule, F_{fr} est la force de frottement, M_v la masse du véhicule, μ le coefficient de frottement, F_N est l'effort normal agissant sur la roue, V_v représente la vitesse du véhicule et enfin R représente le rayon de la roue. À partir des efforts appliqués sur une des quatre roues du véhicule comme le montre la figure III.15 nous pouvons donc écrire les équations suivantes :

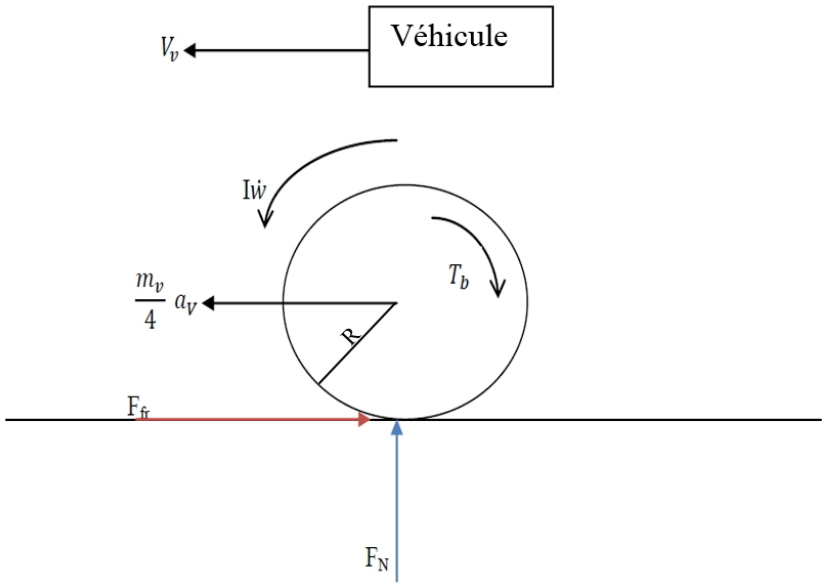


FIGURE III.15: Efforts agissant sur une roue freinée

La somme des forces suivant l'axe y nous donne l'expression (équation III.2) :

$$\Sigma F = \frac{m_v}{4}.g \tag{III.1}$$

$$F_N = \frac{m_v}{4}.g \tag{III.2}$$

La somme des forces suivant l'axe $x$nous permet d'avoir l'expression de la force de frottement (équation III.3) :

$$-F_{fr} = \frac{m_v}{4}.a_v \tag{III.3}$$

L'expression de la vitesse s'écrira alors comme suit :

$$V_v = \int a_v.dt + V_{v0} = \int \frac{-4F_{fr}}{m_v}.dt + V_{v0} \tag{III.4}$$

D'un autre coté :

$$F_{fr} = KF_N \tag{III.5}$$

En substituant l'équation III.3 dans III.5 :

$$KF_N = -\frac{m_v}{4}.a_v \tag{III.6}$$

La somme des moments agissant sur la roue s'écrivent de la manière suivante (équation III.8) :

$$\Sigma T = I\dot{\omega} \tag{III.7}$$

$$T_t - T_b = I\dot{\omega} \tag{III.8}$$

Le moment généré par la force de frottement s'écrit comme montré dans l'équation III.9 :

$$T_t = F_{fr}.R = \frac{Km_v.g}{4}.R \tag{III.9}$$

En remplaçant III.9 dans III.8 on obtient l'équation III.10 :

$$\frac{Km_v.g}{4}.R - T_b = I\dot{\omega} \tag{III.10}$$

L'expression de la vitesse angulaire ω s'écrit de la manière suivante (équation III.11) :

$$\omega = \int \dot{\omega}.dt + \omega_0 = \int \frac{1}{I}(\frac{Km_v.g}{4} * R - T_b).dt + \omega_0 \tag{III.11}$$

Le taux de glissement est défini comme suit (équation III.12) :

$$S = \frac{V_v - R\omega}{V_v} \tag{III.12}$$

Le taux de glissement varie suivant le coefficient de frottement comme le montre la figure III.16.

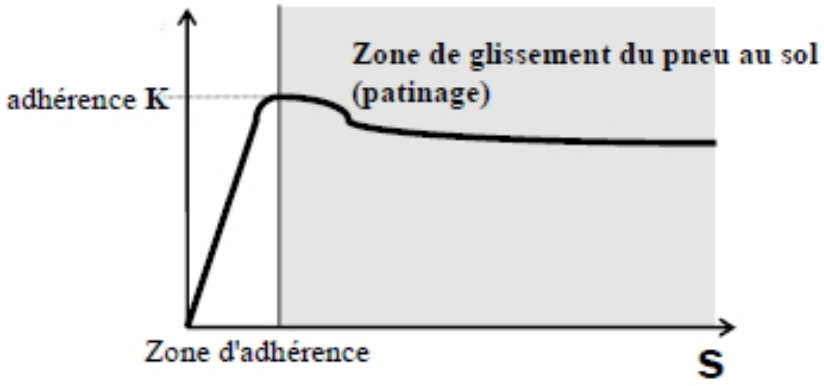


FIGURE III.16: Glissement en fonction du coefficient de frottement.

Modèle Réseau de Petri

La dynamique du système ABS décrit le phénomène physique du système. Il est modélisé par des équations mathématiques qui représentent la partie continue du système. La partie discrète est modélisée par le réseau de Petri lui-même. La combinaison du réseau de Petri et les équations mathématiques proposées par le RdP PTDS-OO a permis une modélisation hybride du système ABS.
Pour éviter d'encombrer le modèle RdP du système, seules les électrovannes et la pompe sont prises en considération. La Figure III.17 montre la modélisation du système ABS à l'aide des réseaux de Petri PTDS-OO.

La place $P1.1$ désigne la vitesse du véhicule dont la dynamique continue est prise en compte par l'équation $F1.1$, celle-ci est suivie de la transition $T1.1$. Par franchissement de cette transition la place $P2.1$ sera marquée et correspondra à la mise en marche du capteur et à la détection de la vitesse de la roue.

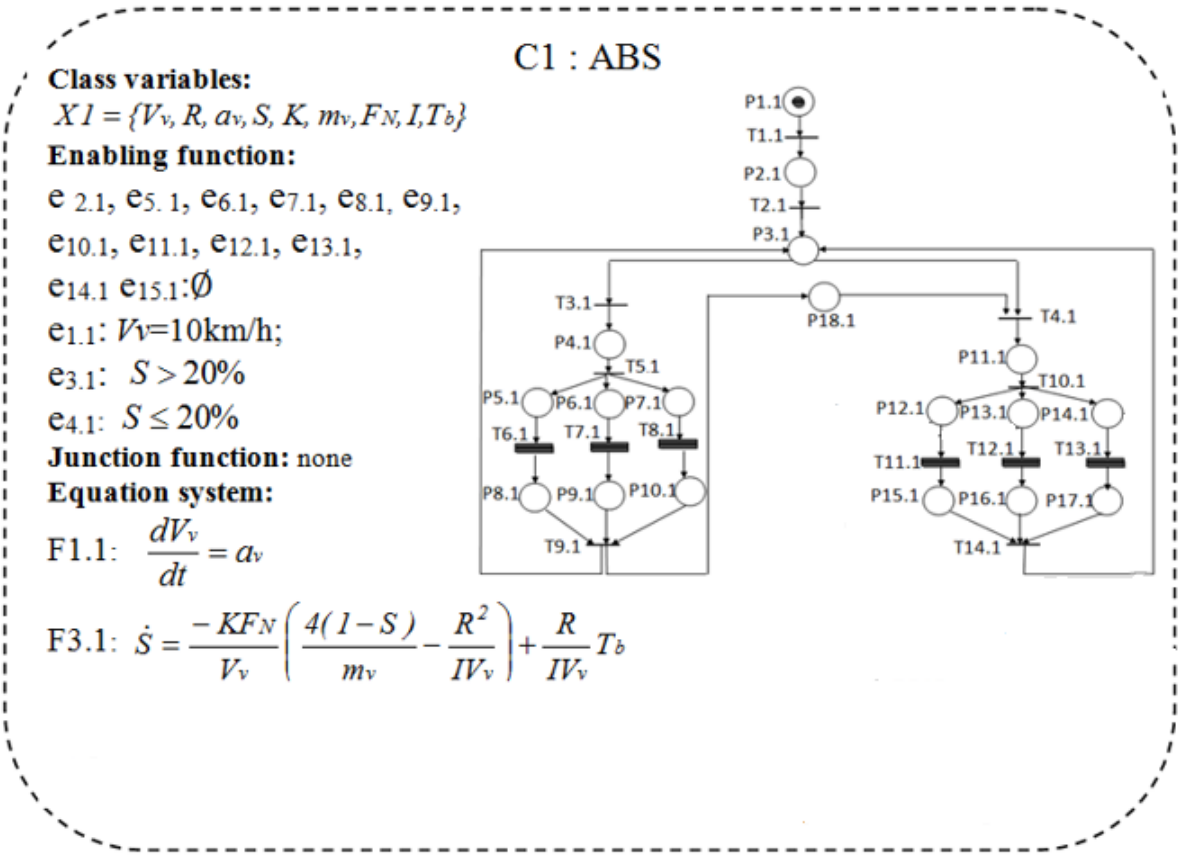
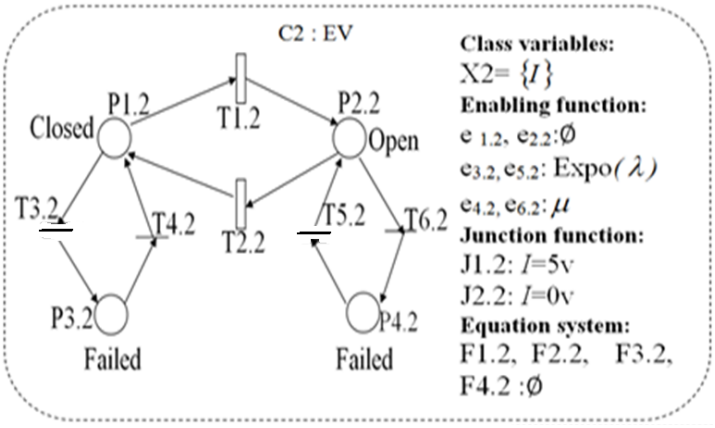


FIGURE III.17: Classe C1 du Réseau de Petri du système ABS.

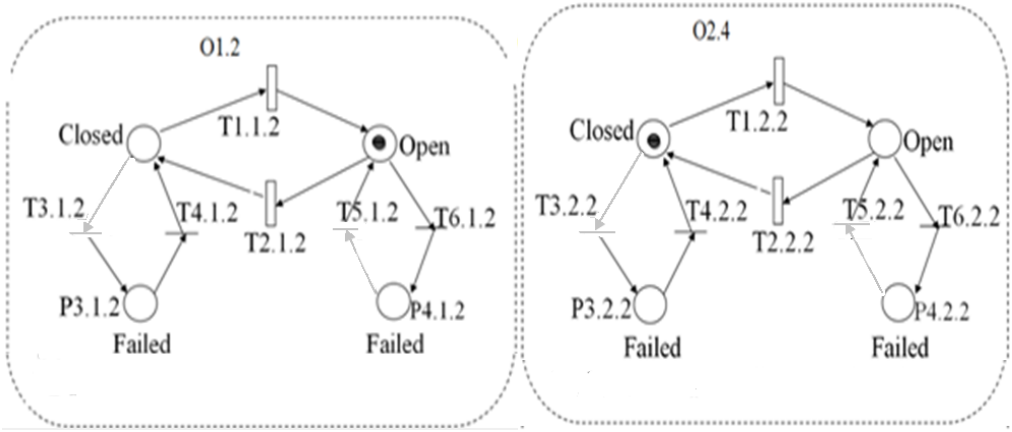
La place $P3.1$ reçoit le jeton venant de la place $P2.1$. Elle correspond à la place de surveillance des vitesses, en d'autre termes, en fonction du signal reçu par le capteur le calculateur évalue le glissement (S) de la roue suivant l'équation $F3.1$, si un blocage est détecté ($S > 20\%$) la transition $T3.1$ sera franchie et la place $P4.1$ qui correspond au mode commande du calculateur, sera marquée permettant ainsi le marquage des $P5.1, P6.1, P7.1$. Ces places appellent aux méthodes offertes par les classes C_2 et C_3 liées à la demande de fermeture de l'EV_1, d'ouverture de l'EV_2 et de mise en marche de la pompe via un relais électromagnétique. Une fois les méthodes exécutées le calculateur reviendra en mode surveillance c'est-à-dire à la place $P3.1$ par le franchissement de la transition $T9.1$. Quand le glissement $S < 20\%$, autrement dit plus de blocage, la transition $T4.1$ est franchie pour le passage du calculateur en mode commande, ainsi les places $P12.1, P13.1, P14.1$ seront marquées et les transitions en aval de ces places feront appel à la méthode d'ouverture de l'EV_1, de fermeture de l'EV_2 et de l'ouverture du contact du relais de la pompe. Une fois les méthodes exécutées, l'ECU retourne à son

état initial, par le franchissement de $T14.1$.

Pour chaque roue, deux électrovannes permettent de moduler la pression sur l'étrier (Figure III.18) : l'EV_1, ouverte en son état initial est modélisée par l'objet $O_{1.2}$ dans la figureIII.18(b), et l'EV_2, fermée en son état initial est modélisée par l'objet $O_{2.2}$ dans la Figure III.18(c).



(a) Réseau de Petri de l'EV



(b) Réseau de Petri de l'EV_1 (c) Réseau de Petri de l'EV_2

FIGURE III.18: Réseau de Petri des électrovannes.

Le tir de la transition déterministe $T2.1.2$ (transition offerte par cette classe) suite à l'appel effectué par la classe C_1 permet de fermer l'EV_1 et le tir de la transition $T1.2.2$ (transition offerte) permet d'ouvrir l'EV_2. Aussi, Le tir de la transition déterministe $T1.1.2$ (transition offerte par cette classe) suite à l'appel effectué par la classe C_1 permet d'ouvrir l'EV_1 et le tir de la transition $T2.2.2$ (transition offerte) permet de fermer l'EV_2.

Le processus de fermeture de l'EV_1et d'ouverture de l'EV_2 s'effectue si un courant$I = 5A$ traverse leurs bobines.

Le franchissement des transitions stochastiques $T_{3.1.2}$, $T_{5.1.2}$ pour l'EV_1 et des transitions stochastiques $T3.2.2, T5.2.2$ pour l'EV_2 correspond à l'état défaillant de l'EV avec un taux de réparation λ. Les transitions $T4.1.2$ et $T6.1.2$ pour l'objet $O_{1.2}$ et les transitions $T4.2.2$ et $T6.2.2$ représentent la réparation de l'électrovanne EV1 avec un taux de réparation μ.

La pompe du système ABS est modélisé par quatre places dans la figure III.19. La place $P1.3$ correspond à l'état initial c.à.d le contact du relais est ouvert. Suite à l'appel effectué par la classe $C1$, Le franchissement de la transition déterministe $T1.3$ permet le marquage de la place $P2.3$ désignant l'état fermé du contact du relais de la pompe. La pompe suit une loi de défaillance de Weibull pour cela aux transitions stochastiques $T3.5$ Et $T5.5$ seront affectés les taux de défaillance β et τ. Le tir de ces transitions correspondra à l'état défaillant.

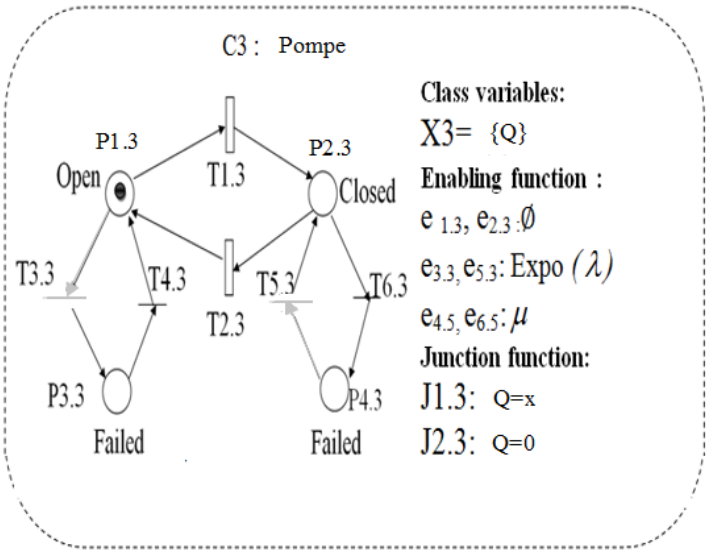


FIGURE III.19: Classe C3 du Réseau de Petri du système ABS.

III.5 Analyse qualitative :Extraction des scénarios critiques

Une fois l'étape de modélisation terminée, l'analyse qualitative prend place. Cette analyse vise à mettre en évidence tous les types de comportement amenant à des états

pour lesquels la sécurité n'est plus assurée. Elle a pour but d'extraire tous les enchainements d'évènements menant à l'état critique (dangereux), à partir d'un état de bon fonctionnement.
L'analyse qualitative des risques ou bien l'extraction des scénarios critiques, est un outil de prise de décision pour le concepteur et l'utilisateur :

— Choisir l'architecture adéquate pour un système à la phase conception.

— Établir un plan maintenance au stade exploitation.

L'objectif de cette section est de présenter une méthode permettant de trouver les scénarios critiques et de les caractériser par des relations de causalité entre événements. Nous commencerons tout d'abord par définir de manière formelle la notion de scénario critique. Ensuite, nous présenterons les limites des outils d'analyse des RdP pour l'extraction des scénarios critiques, avant d'introduire des notions de logique linéaire comme moyen pour contourner ces limites. Nous présenterons, enfin, la méthode proposée de recherche de scénarios critiques qui est basée sur la logique Linéaire.

III.5.1 Scénario Critique

Définissons tout d'abord ce que c'est qu'un scénario. Un scénario sous-entend un début, une fin et une histoire qui décrit l'évolution d'un système. Dans le contexte de la sûreté de fonctionnement, un scénario critique mène à un état catastrophique ou dangereux : c'est l'état final (dit état critique). L'état initial est un état de bon fonctionnement du système. Le scénario critique décrit de manière précise (ce qui est nécessaire pour la compréhension) et concise (causalité) comment le système quitte le bon fonctionnement pour évoluer vers un fonctionnement jugé dangereux. C'est en effet une description du système sous la forme de changements d'états et de suites d'événements qui mènent vers l'état critique. C'est une explication claire des raisons pour lesquelles le système s'est trouvé ou risque de se trouver dans un état critique donné. Ce n'est donc pas simplement une suite d'événements sans liens de causalité entre eux mais nous les considérons comme un ensemble de relations d'ordre qui peuvent être interprétées comme des relations de causalité entre certains événements, ceux qui ne sont pas reliés par une relation d'ordre étant considérés comme des événements parallèles. En résumé, un scénario critique est une description de l'évolution de certains composants du système global à partir d'un état de bon fonctionnement jusqu'à l'occurrence de l'événement critique. Ce scénario fait donc intervenir uniquement les composants ayant un lien de causalité avec l'occurrence de

l'événement critique. Les combinaisons de défaillances des composants élémentaires d'un système forment la majeure partie des causes possibles pouvant provoquer les scénarios critiques. Ces combinaisons peuvent être identifiées par un raisonnement en parcourant l'ensemble des combinaisons possibles des défaillances élémentaires. Dans certains cas, ces défaillances élémentaires sont bénignes pour le fonctionnement du système mais, combinées avec des interactions entre certains sous-systèmes (partage de ressource ou partage de variable continue), ces défaillances peuvent être à l'origine des scénarios critiques. L'objectif de notre méthode est d'identifier ces scénarios de façon exhaustive,à partir du modèle du système en réseau de Petri. Commençons tout d'abord par formaliser ces scénarios par rapport au formalisme des réseaux de Petri. Dans le cadre des réseaux de Petri, l'occurrence des événements est modélisée par le tir des transitions et les états partiels sont les marquages partiels. Ainsi, un scénario est interprété, dans un RdP, comme la(les) séquence(s) de franchissement menant du marquage M_g (modélisant l'état de bon fonctionnement)au marquage M_c (modélisant l'état critique).

Définition 16 ***(Scénario critique)***[7] *:Un Scénario critique associé à un RdP, est un ensemble de séquence de franchissements S'à partir d'un marquage M_g menant au marquage critiqueM_c : $\forall S \in S'$ tel que$M_g \xrightarrow{S} M_c$ Où :*
S est la séquence de franchissements,
M_g le marquage correspondant à un état de bon fonctionnement.

□

Après avoir défini les scénarios critiques, nous allons introduire les outils RdP permettant l'extraction de ces séquences de franchissement ainsi que leur limites.

III.5.2 Limites des outils d'analyse des RdP

L'extraction de la(les) séquence(s) de franchissement menant du marquages M_g (modélisant l'état de bon fonctionnement)au marquage M_c (modélisant l'état critique),peut être traitée de deux façons différentes [109, 110] :

— La première permet d'aborder ce problème en faisant appel à l'algèbre linéaire en résolvant l'équation caractéristique : $M_f = M_0 + W.s$,

  — M_f, M_0 sont respectivement le marquage final et le marquage initial

7. Définition proposée par l'auteur

— West une matrice d'incidence qui représente le nombre de jetons modifiés à la place i lorsqu'une transition j est tirée une fois.

— s est le vecteur caractéristique. C'est un vecteur de m-composants dont le numéro de composant $j$correspond au nombre de fois que la transition T_j doit être tirée pour transformer M_0 en M_f.

— La seconde, fait appel au graphe des marquages accessibles. A partir du marquage initial M_0, on essaye de trouver toutes les séquences permettant d'accéder au marquage final M_f.

L'exemple de la figureIII.20, met en évidence les limites des outils d'analyse des RdP.

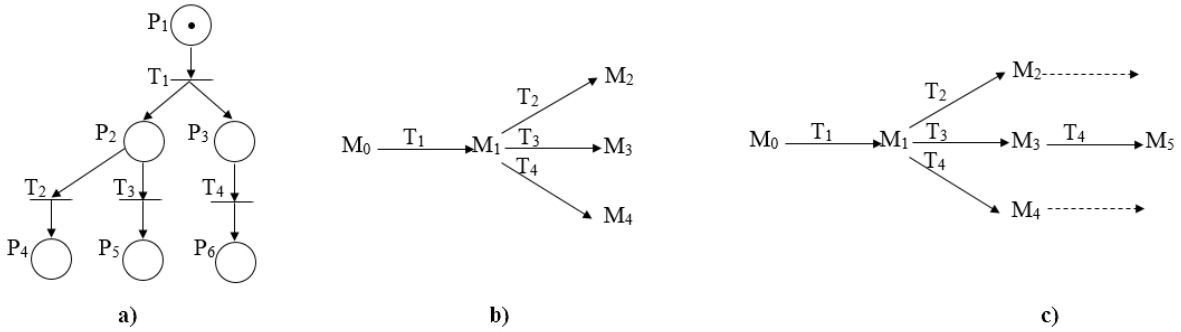


FIGURE III.20: a)Exemple d'un RdP. b)Début de construction du graphe des marquages partiel associé au modèle. c)Suite de la construction du graphe des marquage.

À partir du marquage initial$M_0 = M_g = P1$ du réseau de Petri de la figureIII.20a, la connaissance d'un marquage final partiel, n'est pas suffisante pour calculer le vecteur caractéristique s. Aussi, la résolution de cette équation permet de déterminer une condition nécessaire mais non suffisante d'accessibilité. Le vecteur caractéristique s ne donne aucun ordre de franchissement des transitions mais uniquement le multi-ensemble (non ordonné) des transitions à franchir. Cette condition nécessaire, mais non suffisante, peut s'interpréter de la sorte : s'il existe un chemin entre les marquages M_0 et M_f, il passera forcément par le multi-ensemble s calculé. Par contre, l'algèbre linéaire ne définit ni l'ordre des franchissements ni la possibilité effective de ces franchissements (qui dépend du marquage initial). Dans notre exemple $s = [1101]^T$détermine la condition nécessaire pour atteindre le marquage final ou les places modélisant l'état critique sont marquées, c'est-à-dire, il faudra franchir une fois chacune des transitions T_1, T_2 et T_4. Le vecteur caractéristique indique les transitions à franchir mais ne spécifie aucun ordre de franchissement.

Quant au procédé du graphe des marquages, son utilisation conduit à une génération d'un grand nombre d'états et ne montre pas la relation réelle entre les événements (la relation de précédence est confondue avec celle de cause). Ceci est explicitée par la configuration obtenue du graphe des marquages associé au modèle RdP (Fig.III.20b), de là on remarque deux situations :

— T_2 et T_3 sont en conflit (le tir de T_2 est la cause de blocage du tir de T_3 et inversement), constituant ainsi une relation de cause,

— et, T_3 et T_4 sont en parallèle (leur tir est indépendant), constituant ainsi une relation de précédence,

La première incohérence est constatée dès la première étape du tracé du graphe (Fig.III.20b), c'est-à-dire le conflit (entre T_2 et T_3) exprimant une relation de cause est représentée de la même manière que le parallélisme (T_3 et T_4) exprimant une relation de précédence.
La deuxième incohérence est enregistrée dans la suite du tracé (Fig.III.20c). Par exemple, la séquence $T_1T_3T_4$ menant au marquage M_5, fait ressortir une relation de cause entre T_1 et T_3, ceci est confirmé dans le modèle RdP de la Figure III.20 où la succession de ces deux transitions est mise en évidence. En même temps, T_3 et T_4, appartenant à la même séquence, se succèdent mais dans le modèle du système elles vont se retrouver en parallèle ce qui implique une relation de précédence entre elles.
En définitif, dans un graphe des marquages, outre le problème de l'explosion combinatoire du nombre d'états due à la complexité des systèmes mécatronique, une même structure peut exprimer des relations différentes et induire, par conséquent, une confusion entre les liens de causalité et de précédence.
Un moyen de contourner le problème et de concevoir un outil d'investigation substituant le graphe des marquages applicable à l'ensemble du réseau et capable d'établir les scénarios critiques possibles.La correspondance parfaite entre les RdP et la LL nous a inspiré pour proposer cet outil, en interprétant les modèles réseaux de Petri. A cet effet on a procédé à la sélection et à l'adaptation de connecteurs et de règles destinés à la transcription de la structure et de la dynamique du RdP. Une fois l'outil conçu, la démarche d'extraction est organisée autour d'un algorithme comprenant deux sub-algorithmes : un sub-algorithme pour l'extraction des transitions menant au marquage critique, définie des techniques de RdP et sub-algorithme pour l'extraction des scénarios utilisant les règles de franchissement proposées.
Avant d'introduire la démarche nous donnons des notions de logique linaire dans la

section qui suit.

III.5.3 Logique linéaire

La logique Linéaire a été proposée par le logicien et mathématicien J.Y. Girard comme une restriction de la logique propositionnelle classique pour prendre en compte la notion de **ressource**, comme l'explique dans sa publication [122] :"[...] focaliser l'attention sur les propositions qui s'usent quand on s'en sert, par opposition aux vérités universelles de la logique classique"
Les règles de syntaxe de la logique linéaire différent de celles de la logique classique, de telle sorte que les propositions logiques sont considérées, non plus comme des vérités pérennes (comme en logique classique),mais sont gérées comme des choses *périssables*, des *ressources* consommées et produites pendant les preuves.
Une déduction en Logique Linéaire consomme les propositions qu'elle prend pour prémisses, et produit les propositions qui forment sa conclusion. Cela signifie que pour réutiliser une prémisse qui vient d'être consommée, soit il aurait fallu initialement poser deux fois cette prémisse, soit il faut préalablement la produire à nouveau, par le biais d'une autre déduction.
Prenons un exemple afin d'illustrer la différence fondamentale entre la logique classique et la logique Linéaire : le principe de consommation / production. Considérons le raisonnement suivant :
Pour $10DA$ j'ai un pain $[A \Rightarrow B]$
j'ai $10DA$ $[A]$
(donc) j'ai un pain $[B]$
Ce raisonnement ne serait pas réaliste s'il était formulé en logique classique. En effet, les valeurs de vérité des propositions classiques ne sont pas révocables. Cela pourrait nous mener à la conclusion suivante : l'achat d'un pain est gratuit puisqu'on aura toujours, après achat, $10DA$.
Afin de pouvoir prendre en compte ce principe de consommation / production, Girard a été amené à refaire intégralement le système des connecteurs classiques et à introduire quatre nouveaux connecteurs au lieu de deux (le "*et* " et le " *ou* "). Une des principales raisons de cette refonte est que l'idée de conjonction de ressources ne vérifie pas une propriété fondamentale de la conjonction classique : **l'idempotence** [8]. Cette propriété

8. L'idempotence signifie qu'une opération a le même effet qu'on l'applique une ou plusieurs fois.

est le fait que toute proposition A est équivalente à sa conjonction avec elle-même A et$A$. Le passage des connecteurs classiques aux connecteurs linéaires s'effectue donc par le rejet de la propriété d'idempotence.Reprenons l'exemple et supposons que l'acheteur ait deux pièces de $10DA$.Pour exprimer ce fait il faudrait que la conjection "*j'ai* $10DA$ *et j'ai* $10DA$ " ne se réduit pas à "*j'ai* $10DA$" mais à "*j'ai* $20DA$". C'est pourquoi le connecteur classique *et* et remplacer par un autre en logique linéaire et de la même manière pour le connecteur "*ou* ". Tous les connecteurs logiques étant en relation, ce rejet n'a de sens qu'au prix d'une refonte intégrale du système. C'est seulement après avoir établie la syntaxe des nouveaux connecteurs dans le calcul du séquent [9] que Girard a perçu le sens dynamique de ces nouveaux connecteurs a savoir qu'ils permettent de formuler des raisonnements en utilisant des proposions comme ressources.

Quelques connecteurs de la logique linéaire

L'ensemble des connecteurs de la logique linéaire est réparti en 3 groupes : les connecteurs multiplicatifs, additifs et exponentiels. Nous ne présenterons ici que ceux (le connecteur *entraine*, le connecteur *par*, le connecteur *avec*) qui concernent notre travail sur les réseaux de Petri. Le lecteur intéressé pourra trouver une présentation détaillée des autres connecteurs dans[123].

Implication linéaire Nommée *entraine* et notée $\multimap$, l'implication linéaire exprime la possibilité d'une déduction.Nous interprétons la formule $A \multimap B$, comme l'action qui exprime la possibilité de produire un exemplaire de la ressource B en consommant un exemplaire de la ressource A.
La possibilité de cette action ($A \multimap B$) dépend de la consommabilité, de la ressource A.Illustrant ceci concrètement en reprenant l'exemple précédent : pour qu'un client puisse acheter du pain (pour produire la ressource pain B) il doit avoir de l'argent(consommation de la ressource argent A). On écrit alors :$A, A \multimap B$.

Disjonction multiplicatif Nommé *par* et noté $\parr$, ce connecteur exprime une notion de cumul disjoint (en parallèle) de deux exemplaires de ressource.Avec le cumul en parallèle tous se passe comme si les exemplaires cumulés ($A \parr B$)sont séparés par

9. Un séquent est une expression logique de la forme : $H \vdash C$. cad l'hypothèse H permet de déduire la conclusion C.Le calcul des séquents est un système de déduction.

une barrière empêchant de les utiliser conjointement dans une action mais rien n'opposent leur utilisation dans deux actions indépendantes $(A \multimap C), (B \multimap D)$. On écrira : $A \parr B, (A \multimap C), (B \multimap D)$.
Pour bien comprendre la notion de cumul en parallèle, nous reprenons l'exemple précédent : imaginons deux clients dans une boulangerie. Supposant que le premier client ait$12DA$ et le deuxième $20DA$ et que le pain coute toujours $10DA$.Avec le point de vue commun des actions des deux clients,la ressource argent du premier client et la ressource argent du deuxième client sont utilisées disjointement pour réaliser l'action d'achat pour chacun des clients.

Conjonction additif Le connecteur se nomme *avec* et se note &.Au sens des ressources, consommer un exemplaire $A \,\&\, B$ permet de produire soit un exemplaire de$A$ soit un exemplaire de B mais pas les deux en même temps ni conjointement ni disjointement. Le connecteur & exprime donc un conflit.
Pour illustrer cette interprétation,prenons l'exemple d'un distributeur automatique de boissons chaudes. Supposons que la machine serve pour la somme de $25DA$ (ressource A) un gobelet de thé (ressource B) ou de café(ressource C). L'action du client qui introduit l'appoint dans le distributeur s'écrit donc : $A, A \multimap B \,\&\, C$. Selon le point de vu du client la ressource $B \,\&\, C$ correspond bien a une chose virtuelle vis-à-vis de laquelle il possède un degré de liberté quant à sa matérialisation, il peut choisir entre deux possibilités de production.

Calcul du séquent et arbre de preuve

Toutes les déductions de la Logique Linéaire se font dans un cadre clair et formel : le calcul des séquents. Introduit par Gentzen en 1934, le calcul des séquents est un formalisme syntaxique permettant d'étudier les lois de la logique. Girard a montré qu'il était parfaitement adapté pour définir la logique linéaire et l'a repris pour en définir la syntaxe.

Notions de séquent Un séquent est une déduction qui exprime que d'un ensemble de prémisses on peut déduire un ensemble de conclusion. Sa forme générale est la suivante :

$$A, B... \vdash E, F$$

— A, B, E, F sont des variables de formules propositionnelles. Ce sont donc des méta-variables, elles peuvent se substituer avec toute formule propositionnelle.

— Le symbole $\vdash$ appelé *tourniquet*, est un méta-connecteur qui sépare le membre droit contenant les prémisses, du membre gauche contenant les conclusions.

Notions de règle Pour prouver la correction de la déduction exprimée par un séquent on applique les règles du calcul des séquents. Ces règles sont réparties en 3 groupes : le groupe identité, le groupe structurel et le groupe logique.

Règle logique pour le connecteur implique

$$\frac{\Gamma \vdash F, \Delta \quad \Gamma', G \vdash \Delta'}{\Gamma, \Gamma', F \multimap G \vdash \Delta, \Delta'} \multimap_L$$

Règle logique pour le connecteur par

$$\frac{\Gamma, F \vdash \Delta \quad \Gamma', G \vdash \Delta'}{\Gamma, \Gamma', F \parr G \vdash \Delta, \Delta'} \parr_L$$

Règle logique pour le connecteur Avec

$$\frac{\Gamma, F \vdash \Delta}{\Gamma, F \& G \vdash \Delta} \&_{L_1} \qquad \frac{\Gamma, G \vdash \Delta}{\Gamma, F \& G \vdash \Delta} \&_{L_2}$$

FIGURE III.21: Règles du calcul des séquents relatives aux connecteurs :$\multimap, \parr, \&$

Pour chaque règle, le séquent à prouver est écrit en dessous de la barre tandis que le (ou les) séquent(s) utilisé(s) pour cette preuve est (sont) écrit(s) au-dessus. L'attribut indique que l'on applique la règle à gauche (indice L comme Left) ou à droite (indice R comme Right) du tourniquet du séquent concerné.

$\frac{Squent \quad premisse1 \qquad Squent \quad premisse2}{Squent \quad conclusion} Nom \quad regle_{attribut}$

Partant de ces règles, une preuve est conduite de bas en haut en posant comme racine de l'arbre de preuve le séquent à démontrer. On applique ensuite une à une les règles logiques pour éliminer successivement les connecteurs du séquent. Chaque nœud de l'arborescence est alors un séquent prémisse plus simple que celui dont il est conclusion.

Ce séquent est prouvé si chaque feuille de l'arbre se termine par un séquent axiome de type $A \vdash A$. On dit qu'un séquent est prouvable si et seulement s'il existe une preuve dont il est la racine. Nous pressentons dans la figure III.21 les règles logiques qui nous intéressent dans la suite de ce manuscrite.
Par exemple, la démonstration du séquent $A, A \multimap B \vdash B$, est donnée par l'arbre de preuve suivant :

$$\frac{A \vdash A \quad B \vdash B}{A, A \multimap B \vdash B} \multimap L$$

III.5.4 Transcription du RdP en LL

L'idée d'associer RdP à LL est que les RdP produisent et consomment des ressources de manière dynamique, et les règles de syntaxe de la logique linéaire acceptent cette représentation de telle sorte qu'une déduction dans LL consomme une proposition et produit une nouvelle proposition. Dans LL, les propositions ne sont pas considérées comme une vérité éternelle contrairement à la logique classique, ce qui justifie l'adéquation parfaite entre RdP et LL. En considérant les propriétés de la LL, nous avons dans notre démarche, procédés à la sélection et à l'adaptation de connecteurs et des règles destinés à la transcription de la structure et de la dynamique du RdP. Nous avons développé notre modèle basé sur ces propriétés en traitant la sélection et en adaptant les connecteurs de la LL à la structure RdP, puis en adaptant les règles appropriées au comportement dynamique du modèle. La technique consiste en la transcription des transitions selon le type de franchissement, elles peuvent être en séquence, en parallèle et en conflit, à l'aide d'un connecteur particulier.Chaque connecteur est associé à sa propre règle permettant de décrire l'évolution du RdP en différenciant les relations de cause et de précédence existantes entre les transitions. Chaque type de franchissement exprime une relation : le franchissement de deux transitions en séquence (T_1 suivie de T_2) exprime une relation de cause c.à.d. T_1 est la cause du franchissement de T_2. Le franchissent de deux transitions en parallèle (T_1 et T_2) exprime une relation de précédence c.à.d. le franchissement de T_1 en premier n'est pas la cause du franchissement de T_2 et vice versa et enfin le franchissement de deux transitions en conflit (T_1 et T_2) exprime une relation de cause c.à.d. le franchissement de T_1 est la cause du blocage de T_2 et vice-versa.
Avant d'entamer la section suivante quelques notations sont nécessaires.

Notation 1 $^\circ T_j = \{P_i \in P | Pre(P_i, T_j) > 0\}$ *ensemble des places d'entrer de* T_j *;*

$T_j^\circ = \{P_i \in P | Post(P_i, T_j) > 0\}$ *ensemble des places de sortie de* T_j ;
$^\circ P_i = \{T_j \in T | Post(P_i, T_j) > 0\}$ *ensemble des transitions d'entrer de*P_i ;
$P_i^\circ = \{T_j \in T | Pre(P_i, T_j) > 0\}$ *ensemble des transitions de sortie de*P_i ;

□

Définition 17 ***(Transition franchissable)****[139] : Étant donné un RdP* $N =< P, T, Pre, Post, M_0 >$, *une transition est franchissable pour un marquage* M *si :* $M \geq W^-(P, T_i)$ *où :*
$W^-(P, T_i)$ *est le marquage minimum pour franchir* T_i *et correspond à la* i^{th} *colonne de la matrice d'incidence arrière* W^-.

□

Définition 18 ***(Transitions en conflit)[140]*** *: deux transitons* T_i *et* T_j *sont en conflit structurel si elles ont au moins une place d'entrée commune :*
$W^-(P, T_i)^T \times W^-(P, T_j) \neq 0$

□

Définition 19 ***(Transitions en parallèles)[140]*** *: deux transitons* T_i *et* T_j *sont structurellement parallèles si elles n'ont aucune place d'entrée commune :*
$W^-(P, T_i)^T \times W^-(P, T_j) = 0$

□

Transcription de la structure du RdP

Les connecteurs empruntés de la logique linéaire pour transcrire la structure du *RdP* sont : $entraine(\multimap), par(⅋), avec(\&)$.

Transition seule Le franchissement d'une transition est assimilé à une action qui produit des jetons en en consommant. l'implication lineaire ($\multimap$) permet de transcrire ceci, en posant a gauche le marquage minimal pour franchir la transition, tandis que a droit le marquage atteint après le franchissement de cette transition à partir du marquage minimal.
Le connecteur *entraine* ($\multimap$) est donc utilisé pour transcrire une transition $T_i \in T$ en décrivant sa structure amont et avale.
Pour cette transcription, nous donnons la définition suivante :

Définition 20 ***(Transition seule[141])*** *: Le connecteur entraine ($\multimap$) décrit la structure amont et aval de la transition $T_i \in T$*
$T_i : ({}^\circ T_i \multimap T_i^\circ) \Leftrightarrow^\circ T_i, T_i^\circ$

□

La transcription de l'attribution du connecteur *entraine*, comporte deux membres par rapport au symbole d'équivalence : l'écriture du membre gauche est équivalente à l'écriture située au membre droit.

Transitions en parallèles Le franchissement de deux transitions en parallèle T_i, T_j est équivalent a deux actions indépendantes, la première correspond au franchissement de T_i : $({}^\circ T_i \multimap T_i^\circ)$ et la deuxième de T_j : $({}^\circ T_j \multimap T_j^\circ)$.Afin de transcrire ceci en LL, nous ne raisonnons pas en termes de ressources mais en termes d'action.Il devient donc possible d'utiliser le connecteur *par*, modélisant l'évolution en parallèle des ressources pour transcrire l'évolution en parallèle de deux actions cad le parallélisme.

Définition 21 ***(Transition en parallèle[141])*** *: Le parallélisme structurel est décrit par le connecteur* ***par*** *($\parr$). Le connecteur ($\parr$) exprime la possibilité de franchir deux transitions en parallèle T_i, T_j :*

$$M_k({}^\circ T_i \multimap T_i^\circ) \parr ({}^\circ T_j \multimap T_j^\circ) \iff M_k \overset{\nearrow^{T_i}}{\underset{\searrow_{T_j}}{\overset{[T_i\,T_j]}{\rightarrow}}}$$

M_k, est le marquage avant franchissement de la transition T_i et T_j, $k \geq 0$

□

L'écriture du membre gauche est équivalente au graphe situé à droite : le franchissement de T_i et T_j peut être simultané ou alternatif.

Transitions en conflit Contrairement au parallélisme, le franchissement de deux transitions en conflit T_i, T_j correspondent a deux actions dépendantes.Choisir l'action de franchir T_i : $({}^\circ T_i \multimap T_i^\circ)$ empêche celle de franchir T_j : $({}^\circ T_j \multimap T_j^\circ)$ et vice versa.En

raisonnant en terme d'action et non de ressource, le connecteur *avec* modélisant le choix de production de ressource, sera utilisé pour transcrire le conflit cad le choix de réalisation d'une action.

Définition 22 ***(Transition en conflit[141])*** *: Le conflit structurel est décrit par le connecteur* ***Avec*** *(&) et exprime la possibilité de franchir deux transitions en conflit* T_i, T_j *:*

$$M_k(^\circ T_i \multimap T_i^\circ)\&(^\circ T_j \multimap T_j^\circ) \iff \begin{cases} M_k \xrightarrow{T_i} \\ M_k \xrightarrow[T_j]{} \end{cases}$$

M_k, est le marquage avant franchissement de la transition T_i ou T_j, $k \geq 0$

□

L'écriture du membre gauche est équivalente au graphe situé au membre à droite : l'utilisation du connecteur & autorise le franchissement d'une seule transition à la fois T_i ou T_j

Transcription de la dynamique du RdP

Les règles de calcul du séquent empruntées de la logique linéaire sont également adaptées pour fournir les règles de franchissement des transitions décrivant l'évolution du RdP. Chaque connecteur est donc associé avec sa propre règle. D'une manière générale, une règle comprend dans sa partie inférieure le marquage avant franchissement des transitions suivi des transitions transcrites par le connecteur associé et dans sa partie supérieure le nouveau marquage obtenu après franchissement des transitions. Le franchissement effectif d'une transition s'effectue donc en éliminant le connecteur associé à celle-ci en appliquant la règle appropriée.

Règle 1 : Franchissement en séquence La règle d'élimination du connecteur *entraine* adaptée pour exprimer un franchissement en séquence d'une transition T_i, est donnée comme suit :

$$\frac{M_{k+1}T'_{k+1}}{M_k(^\circ T_i \multimap T_i^\circ)} \multimap (T_i)$$

M_{k+1} est le marquage après le franchissement de la transition T_i.
T'_{k+1} est l'ensemble des transitions nouvellement franchissables à partir du marquage M_{k+1}.

□

La règle 1, appliquée au RdP de la FigureIII.22, montre ci-dessous la transcription de la transition $T_1 : (P_1P_2P_3 \multimap P_1P_6)$, franchissable à partir du marquage $M_k = P_1P_2P_3$.

$$\frac{P_1P_6T_2}{P_1P_2P_3(P_1P_2P_3 \multimap P_1P_6)} \multimap T_1$$

Le franchissement effectif deT_1 s'effectue donc par élimination du connecteur *entraine* et produit deux jetons dans$P_1P_6(M_{k+1} = P_1P_6)$ et active T_2.

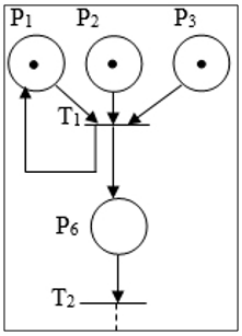


FIGURE III.22: Franchissement en séquence.

Règle 2 : Franchissement en parallèle La règle d'élimination du connecteur *par* adaptée pour exprimer un franchissement en parallèle de deux transitions T_i etT_j, est donnée comme suit :

$$\frac{M_{k+1}T'_{k+1}}{M_k(^\circ T_i \multimap T_i^\circ) \parr (^\circ T_j \multimap T_j^\circ)} \parr (\multimap T_iT_j)$$

M_{k+1} : est le marquage après le franchissement des transitions T_iT_j.

□

La transcription de la règle 2 appliquée au réseau RdP de la figure III.23, montre ci-dessous la traduction des transitions parallèles $T_1 : (P_1 \multimap P_2)$ et $T_2 : (P_3 \multimap P_4)$ franchies à partir du marquage$M_k = P_1P_3$.

$$\frac{P_2P_4T_3T_4}{P_1P_3(P_1 \multimap P_2) \parr (P_3 \multimap P_4)} \parr(\multimap T_1T_2)$$

Le franchissement combiné de T_1T_2 s'effectue donc par élimination du connecteur *par*. Ce franchissement produit deux jetons dans $P_2P_4(M_{k+1} = P_2P_4)$ et active T_3, T_4 $(T'_{k+1} = T_3, T_4)$.

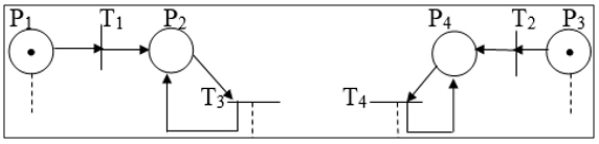


FIGURE III.23: Franchissement en parallèle

Règle 3 :franchissement en conflit La règle d'élimination du connecteur *avec* adaptée pour exprimer un franchissement en conflit de deux transitions T_i et T_j est donnée comme suit :

$$\frac{M_{k+1}T'_{k+1}}{M_k(\circ T_i \multimap T_i^\circ)\&(\circ T_j \multimap T_j^\circ)}\&(\multimap T_i) \qquad \frac{M_{k+2}T'_{k+2}}{M_k(\circ T_i \multimap T_i^\circ)\&(\circ T_j \multimap T_j^\circ)}\&(\multimap T_j)$$

M_{k+1}, est le marquage après le franchissement de la transition T_i.
M_{k+2}, est le marquage après le franchissement de la transition T_j.
T'_{k+1},T'_{k+2}sont respectivement l'ensemble des transitions nouvellement franchissables à partir de M_{k+1} et M_{k+2}.

□

La règle 3, appliquée au RdP de la Figure III.24, montre ci-dessous la transcription, en deux arbres, des deux transitions en conflit $T_1 : (P_1P_2P_3 \multimap P_1P_4)$ et $T_2 : (P_3 \multimap P_5)$, franchissables à partir du marquage $M_k = P_1P_2P_3$.

$$\frac{P_1P_4T_4}{P_1P_2P_3(P_1P_2P_3 \multimap P_1P_4)\&(P_3 \multimap P_5)} \&(\multimap T_1)$$

$$\frac{P_1P_2P_5T_3}{P_1P_2P_3(P_1P_2P_3 \multimap P_1P_4)\&(P_3 \multimap P_5)}\ \&(\multimap T_2)$$

L'arbre 1 donne le résultat du tir de T_1 et produit deux jetons dans $P_1P_4(M_{k+1} = P_1P_4)$ et active$T'_{k+1} = T_4$.
L'arbre 2 donne le résultat du tir de T_2 et produit un jeton dans $(M_{k+2} = P_1P_2P_5)$ et active $T'_{k+2} = T_3$.

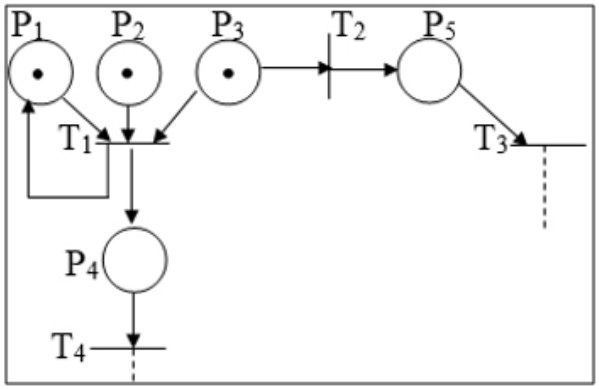


FIGURE III.24: Franchissement en conflit

III.5.5 Démarche algorithmique

Après la démonstration, relative à la distinction structurelle des trois types de franchissements, la suite du travail consiste en la détermination des scénarios critiques. Le but est de caractériser les scénarios critiques par des relations de causalité entre les événements menant vers un état critique donné. Dans les systèmes mécatroniques, les scénarios critiques sont, en effet, inconnus du fait de la complexité inhérente à ces systèmes et à la multitude de modules en interaction.
L'extraction des scénarios critiques s'effectue par application des règles de franchissement jusqu'à atteindre le marquage critique : les franchissements des transitions jusqu'au marquage critique génèrent progressivement des arbres d'où seront extraits les scénarios critiques.
La technique d'extraction utilisée est un algorithme utilisant deux sub algorithmes : le premier intitulé extraction-transitions, qui traite l'exposition combinatoire.Cet algorithme utilise le concept du raisonnement arrière pour isoler la partie intéressante du modèle. Le second intitulé extraction-scénarios, traite la confusion entre les relations de

précédence et de causalité qui existe entre les événements. Cet algorithme utilise les trois règles proposées pour extraire les scénarios critiques sans aucune confusion.

Définition du sub algorithme Extraction-Transitions

Le sub algorithme Extraction-Transitions est définit dans l'algorithme 1 ci-desous.

Algorithm 1: Extraction-Transitions sub algorithme

Function *Extraction-transitions (T'')*
- Input : M_g, M_c,W^+, W^-, T''
- Output : T''
- **Étape 1** : Début de l'extraction des transitions appartenant à l'ensemble T''
- **for** *pour chaque place* $P_i \in M_c$ **do**
  - **Étape 1.1** : Identifier $^\circ P_i$,en repérant dans la matrice W^+, les éléments non nuls de la ième ligne.
  - **Étape 1.2** Eliminer les $T_j \in^\circ P_i$ en boucle, les transitions retenues seront introduites dans T''
  - **for** *pour chaque transition* $T_j \in^\circ P_i$ **do**
    - **if** $Post(P_i, T_j) = Pre(P_i, T_j)$ **then**
      - Eliminer la transition T_j
    - **else**
      - Retenir T_j
      - Affecter T_j to T''
  - **Étape 2** : Extraction des places appartenant à l'ensemble P'
  - **for** *pour chaque transition* T_j *retenue dans l'étape 1.2* **do**
    - ***Step 2.1*** Identifier $^\circ T_j$,en repérant dans la matrice W^-, les éléments non nuls de la jème ligne.
    - **for** *pour chaque* $P_i \in^\circ T_j$ **do**
      - **if** $P_i \in M_g$ **then**
        - Eliminer la place P_i
      - **else**
        - Affecter P_i à P'
    - **Étape 3** : Finalisation de la composition de T''
    - **if** $P' = \emptyset$ **then**
      - Revenir à l'étape 2 avec la transition Tj suivante T_j
    - **else**
      - Appliquer la fonction *Extracion-Transition* pour chaque $P_i \in P'$
  - Revenir à l'étape 1 avec la place suivante de M M_c
- Afficher T''

Le sub algorithme Extraction-Transitions, est nécessaire pour extraire du RdP seules les transitions menant au marquage critique évitant le traitement de tout le réseau. Le sub algorithme utilise les matrices d'incidence avantW^- et arrière W^+ de façon interposée. C'est-à-dire, W^+ est utilisée pour la détermination des transitions en amont de chaque place du marquage M_c. Ensuite,W^- est à son tour utilisée pour la détermination des places situées en amont des transitions déterminées juste préalablement. Cette manipulation se poursuit de la même manière jusqu'à la détermination complète des transitions survenant du marquage M_g. Ainsi, l'ensemble des places identifié est désigné par P' et l'ensemble des transitions extraites est désigné par T''.

Explication de l'algorithme 1 à travers l'exemple de la figure III.25 En se basant sur l'algorithme 1 proposé et l'exemple donné de la figure III.25, où $M_g = P_1$ et $Mc = P_{11}$. On commence par P_{11}, et on associe à M_c la matrice d'incidence de sortie W^+(figure III.25b1). On cherche l'élément non nul dans la 11^{me} ligne de cette matrice. Le "1" correspond à la transition T_8. Cette transition obtenue sera stockée dans l'ensemble T''. Ceci est exprimé comme suit.

Étape 1 : $P_{11} \rightarrow W_{b1}^{+} \rightarrow T_8 \rightarrow stored \ \ in \ \ T''$

De même, nous adoptons cette structure pour exprimer les prochaines étapes.

Étape 2 : $T_8 \rightarrow W_{b2}^{-} \begin{array}{l} \nearrow P_8 \\ \searrow P_9 \end{array}$

Étape 1 (2^{nd} **itération**)

$P_8 \rightarrow W_{b3}^{+} \rightarrow T_5 \rightarrow stockee\ dans\ T''$

$P_9 \rightarrow W_{b3}^{+} \rightarrow T_6 \rightarrow stockee\ dans\ T''$

Étape 2 (2^{nd} **itération**)

$T_5 \rightarrow W_{b4}^{-} \rightarrow P_5$

$T_6 \rightarrow W_{b4}^{-} \rightarrow P_6$

Étape 1 (3^{rd} **itération**)

$P_5 \rightarrow W_{b5}^{+} \rightarrow T_3 \longrightarrow stockee\ dans\ T''$

$P_6 \rightarrow W_{b5}^{+} \rightarrow T_3 \longrightarrow stockee\ dans\ T''$

Étape 2 (3^{rd} **itération**)

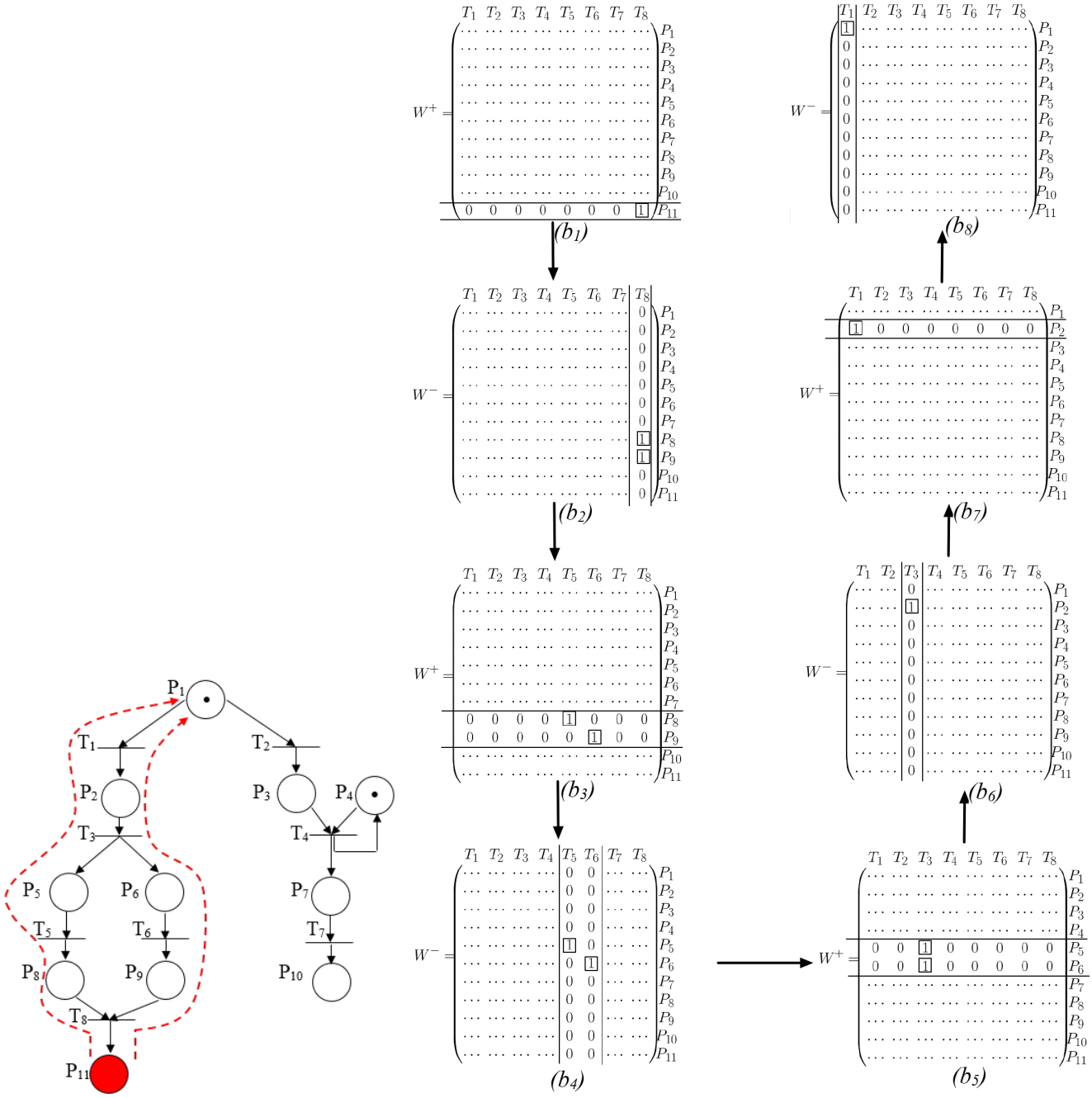
$T_3 \rightarrow W_{b6}^{-} \rightarrow P_2$

Étape 1 (4^{th} **itération**)

$P_2 \rightarrow W_{b7}^{+} \rightarrow T_1 \longrightarrow stockee\ dans\ T''$

Étape 2 (4^{th} **itération**)

$T_1 \rightarrow W_{b8}^{-} \rightarrow P_1 \in M_g \rightarrow T'' = \{T_1, T_3, T_5, T_6, T_8\}$.



(a) (b) Extraction détaillée des transitions

FIGURE III.25: Extraction des transitions dans un RdP.

Définition de la fonction Extraction-Scénarios

Le sub algorithme Extraction-Scénarios est présenté dans l'algorithme 2 ci-dessous.

Algorithm 2: Extraction-Scénarios sub algorithme

Function *extraction-scénarios (Sc)*

Input : M_g, M_c, W^-, T''

Output : Cs

Étape 1 : Détermination des transitions franchissables

Déterminer à partir de $M_g$les transitions franchissables $T_i \in T''$

for *chaque* $T_i \in T''$ **do**

if $M_g \geq W^-(P, T_i)$ [10] **then**

T_i est franchissable

Retenir T_i

Étape 2 : Franchissement des transitions

if *une seule transition* T_i *est retenue dans l'étape 1* **then**

Franchissement en séquence

Appliquer la règle 1

Vérifier si le marquage critique est atteint

if $M_c \leq M_{k+1}$ [11] **then**

Donner le scenario critique Cs

else

$M_g = M_{k+1}$

Appliquer la fonction Extraction-Scenario (Sc)

else

Deux transitions T_i et T_j (ou plusieurs) sont retenues

if $W^-(P, T_i)^T \times W^-(P, T_j) = 0$ [12] **then**

Franchissement en parallèle

Appliquer la règle 2

Vérifier si le marquage critique est atteint

if $M_c \leq M_{k+1}$ **then**

Donner le scenario critique Sc

else

$M_g = M_{k+1}$

Appliquer la fonction Extraction-Scenario (Sc)

else

Franchissement en conflit

Appliquer la règle 3

Vérifier si le marquage critique est atteint M_{k+1},M_{k+2}

if $M_c \leq M_{k+1}$ **then**

Donner le scenario critique Sc

else

$M_g = M_{k+1}$

Appliquer la fonction Extraction-Scenario (Sc)

if $M_c \leq M_{k+2}$ **then**

Donner le scenario critique Sc

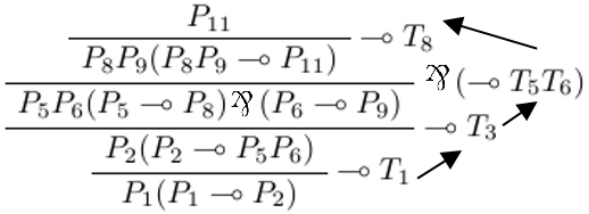
else

$M_g = M_{k+2}$

Appliquer la fonction Extraction-Scenario (Sc)

À ce stade nous connaissons effectivement les événements qui ont accompagné l'évolution du système vers l'état critique, toutefois, nous n'avons obtenu aucune information sur les relations existantes entre ces événements.En effet, pour les transitions extraites par le sub algorithme Extraction-Transitions aucun ordre de franchissement n'est encore spécifié, pour cela l'analyse se poursuit par l'application du sub algorithme Extraction-Scénarios Le sub algorithme Extraction-Scénarios proposé est présenté dans l'algorithme 2. Le sub algorithme d'Extraction-Scénarios commence par franchir séquentiellement les transitions de "T''" par l'application des règles de franchissement. Cela génère un arbre à partir duquel nous pouvons identifier la séquence menant à M_c. Cette séquence représente le scénario critique.

Explication de l'algorithme 2 à travers l'exemple de la figure III.25 L'arbre généré est lu de bas en haut.



Étape 1 : l'algorithme commence de $M_g = P_1$ et la transition franchissable $T_1 \in T''$. La construction de l'arbre commence donc par la transcription $P_1(P_1 \multimap P_2)$ décrivant l'etat initial du système avec $M_0 = M_g = P_1$ suivi par la transition franchissable $T_1 \in T''$,où $T_1 : (P_1 \multimap P_2)$

Étape 2 : application de la règle 1 vu qu'une seule transition est franchissable. Son application décrit le franchissement de T_1 et permet d'obtenir le marquage courant P_2 et la transition nouvellement franchissable $T_3 : (P_2 \multimap P_5P_6)$ comme le montre le second niveau de l'arbre.

P_2 ne correspond pas au marquage critique $M_c = P_{11}$, et $T_3 \in T''$, l'étape 2 est alors appliquée une deuxième fois.

Étape 2 (2^{eme} itération) : on continue d'appliquer la règle 1 tant qu'il n'y a qu'une transition pour obtenir le troisième niveau de l'arbre "$P_5P_6(P_5 \multimap P_8) \parr (P_6 \multimap P_9)$",

4. Définition 7
5. $M_c \leq M_{k+1}$ if $M_c(i) \leq M_{k+1}(i)$ $i \in \{1, 2...n\}$
6. Définition 8

décrivant le marquage courant P_5P_6 suivi par les transitions nouvellement franchissables $T_5 : (P_5 \multimap P_8)$ et $T_6 : (P_6 \multimap P_9)$. Le marquage critique n'est pas encore atteint, et les deux transitions nouvellement franchissables $\{T_5, T_6\} \in T''$. l'Étape 2 et alors répétée.

Étape 2 (3^{eme} itération) : application de la règle 2 vu que maintenant deux transitions sont en parallèle. Ceci permet d'obtenir le quatrième niveau de l'arbre "$P_8P_9(P_8P_9 \multimap P_{11})$", décrivant le marquage courant P_8P_9 suivi par la nouvelle transition franchissable $T_8 : (P_8P_9 \multimap P_{11})$. Le marquage critique n'est pas encore atteint et $T_8 \in T''$.L'étape 2 est alors répétée.

Étape 2 (4^{eme} itération) : Application de la règle 1, vu qu'une seule transition est franchissable.La construction de l'arbre est terminée par ce franchissement qui donne le marquage critique $M_c = P_{11}$.

Au final, nous nous retrouvons avec un arbre où l'on peut extraire la séquence ordonnée conduisant M_c à partir de M_g qui représente le scénario critique.

$$T_1 \longrightarrow T_3 \longrightarrow \begin{bmatrix} T_5 \\ T_6 \end{bmatrix} \longrightarrow T_8$$

III.5.6 Structure de l'algorithme proposé

L'algorithme proposé (algorithme 3)est structuré en trois étapes. La première étape concerne l'initialisation en définissant le RdP et les matrices d'incidence du modèle. La deuxième étape représente l'application du sub-algorithme 1 pour extraire "T'''". La dernière étape représente l'application du sub-algorithme 2 pour identifier les scénarios critiques.

Algorithm 3: Algorithme général

Étape 1 : Initialisation
Définir le marquage M_g et M_c à partir du réseau
Définir les matrice d'incidence avant et arrière (W^- et W^+)
$T'' = \emptyset$
Étape 2 : Extraction de l'ensemble des transitions T'' menant au marquage critique.
Application du sub-algorithme extraction-transitions
Étape 3 : Extraction des scénarios critiques
Application du sub-algorithme extraction scenario

III.6 Analyse quantitative : estimation de la probabilité d'occurrence des scénarios critiques

l'étude bibliographique décrite au Chapitre II a permis de montrer que parmi les différents possibilités d'analyse quantitative,l'association des RdP avec la simulation de type Monte-Carlo constitue un outil d'évaluation numérique performant.En effet, les RdP sont un parfait support pour l'application de la simulation Monte-Carlo.Selon [47, 142, 143]l'avantage de ce type d'approche est la quasi-insensibilité par rapport à la complexité et à la taille des systèmes modélisés. Cependant, son principal inconvénient est la durée de traitement qui est très importante, pour palier a ce problème la quantification recherchée est réalisée à l'aide d'une simulation Monte-Carlo par sauts.
Juste avant de passer à la présentation proprement dite de la démarche suivie pour la simulation, nous allons expliquer le concepts de base de la méthode Monte Carlo.

III.6.1 Concepts de base de la simulation Monte Carlo

Présentation de la méthode

La simulation de Monte Carlo est une méthode très répandue. Historiquement, la méthode de Monte Carlo a été inventée au milieu du XX^{eme} siècle pour estimer des intégrales. Cette technique est à présent utilisée dans de nombreux domaines comme la résolution d'équations aux dérivées partielles, la simulation de files d'attente mais aussi dans le management du risque, que ce soit dans les secteurs de la sûreté de fonctionnement ou dans celui de la finance.
La méthode de Monte Carlo est définie au sens large comme étant une technique de résolution d'un modèle en utilisant des nombres aléatoires ou pseudo-aléatoires [144, 145]. Les nombres aléatoires sont des variables stochastiques qui sont uniformément distribuées sur l'intervalle $[0, 1]$ et qui montrent une indépendance stochastique [144]. Cela veut dire que les variables peuvent prendre n'importe quelle valeur entre 0 et 1 avec la même probabilité. L'indépendance implique que si nous connaissons les nombres aléatoires $r_1, r_2, ..., r_{i-1}$ nous n'avons aucune information sur r_i. Les nombres pseudo-aléatoires sont générés en appliquant des algorithmes déterministes appelés générateurs de nombres aléatoires. Dans un but pratique, le comportement de ces nombres est considéré comme rigoureusement aléatoire. On considère alors qu'ils sont distribués uniformément et indépendants. Les algorithmes les plus répandus pour la génération de nombres

aléatoires sont : le générateur congruentiel multiplicatif et le générateur congruentiel mixte [146, 147]

Principe

Utilisant la méthode Monte Carlo, La quantité que l'on désire estimer correspond à l'espérance mathématique [13] d'une variable aléatoire. Le principe consiste à étudier l'évolution d'un système en simulant un modèle générique, représentant le comportement du système, au cours de ce qu'on appelle une *histoire*.
Le principe de la simulation de Monte Carlo est donc le suivant [148] :

- établissement d'un modèle fonctionnel et dysfonctionnel du système à étudier ;
- animation du modèle par tirage de nombres au hasard pour réaliser des histoires possibles du système étudié ;
- récupération et exploitation des résultats statistiques intéressants.

Du principe ci-dessus, il résulte plusieurs remarques très importantes :

- Le modèle doit être suffisamment détaillé pour représenter tous les modes de fonctionnement et de dysfonctionnement significatifs ;
- Le modèle doit être capable de représenter tous les changements d'état pour tenir compte des événements aléatoires mais aussi déterministes (liés à l'évolution continue) ;
- Un générateur de nombres aléatoires est nécessaire pour animer le modèle ;
- Comme nous parlons de statistiques, cela sous-entend que de nombreuses histoires devront être réalisées afin de rassembler des échantillons statistiquement représentatifs et suffisants pour la précision recherchée.

Le RdP choisi permet de représenter les modes de fonctionnement et dysfonctionnement mais aussi de tenir compte des événements aléatoires et déterministes, donc il présente un bon support pour appliquer la simulation MC.Cette association sera présentée dans la section suivante.

13. En théorie des probabilités, l'espérance mathématique d'une variable aléatoire réelle est, intuitivement, la valeur que l'on s'attend à trouver, en moyenne, si l'on répète un grand nombre de fois la même expérience aléatoire. Elle se note $E(X)$ et se lit "espérance de X "

Association RdP et simulation Monte Carlo L'association des RdP à la simulation du type Monte-Carlo constitue un outil d'évaluation numérique performant pour l'étude des systèmes complexes, encore inaccessibles aux méthodes analytiques.
Dans le domaine de la sûreté de fonctionnement, la quantification de la grandeur recherchée (par exemple la fiabilité, ou la probabilité d'apparition d'un événement critique en ce qui nous concerne) est alors basée sur l'étude d'un certain nombre d'histoires différentes, permettant d'en extraire des résultats statistiques (estimateurs).
Pour effectuer une estimation de la probabilité d'apparition d'un événement critique, on peut associer un estimateur de type binaire à cette probabilité et incrémenter un compteur d'une unité pour chaque histoire dans laquelle l'événement critique se produit. L'estimation de la probabilité est alors obtenue en faisant le rapport entre le nombre d'histoires ayant connu un événement critique et le nombre total d'histoires [47] :

$$Pr = \frac{nombre\ d'histoires\ ayant\ connu\ un\ evenement\ critique}{nombre\ d'histoires\ simules} \tag{III.13}$$

plus précisément,nous rappelons que le RdP utilisé dans notre approche contient des transitions déterministes et des transitions stochastiques suivant différentes lois de probabilité (exponentielle, weibull..).
D'abord,pour la détermination de la valeur du délai d attaché aux transitions stochastiques, lors d'une simulation Monte Carlo, par exemple celles qui suivent une loi exponentielle de paramètre λ ; on opère de cette manière[149] :

— On procède au tirage aléatoire d'un nombre X selon une loi uniforme sur $[0, 1]$,

— On pose

$$X = F(t) = 1 - e^{(-\lambda t)} \tag{III.14}$$

— On déduit la valeur cherchée

$$t = -(\frac{1}{\lambda}).ln(1 - x) \tag{III.15}$$

On simule ainsi le RdP suivant son évolution sur une durée préfixée T qu'on appelle durée d'une histoire, la durée T est choisie en fonction du type de système à étudier. Ce

peut être la durée de vie opérationnelle de ce système, la durée moyenne d'une mission, ou encore la durée qui s'écoule entre deux révisions (totales ou partielles) du système. On réitère un grand nombre de fois N une telle histoire en partant chaque fois des mêmes conditions initiales et en conservant en mémoire les données numériques obtenues. Au terme de ces N histoires, on exploite d'une manière statistique l'ensemble des données accumulées pour déterminer les estimations désirées. La valeur du nombre$N$ d'histoires à effectuer dépend de la précision de l'estimation souhaitée du paramètre à observer.
Au fur et à mesure du déroulement des histoires des échantillons statistiques, des paramètres d'intérêt sont constitués. Lorsque N histoires sont réalisées, des formules statistiques classiques permettent d'estimer la moyenne m_N et la variance σ_N^2 de chacun de ces échantillons :

$$m_N = \frac{1}{N}\sum_{i=1}^{N} X_i \tag{III.16}$$

$$\sigma_N^2 = \frac{1}{N}\sum_{i=1}^{N}(X_i - m_N)^2 \tag{III.17}$$

Sachant que :
$m_N \approx \mu$ pour N grand, où μ est l'espérance mathématique.
La racine carrée de la variance σ est appelée *écart type* de l'échantillon. Au fur et à mesure que le nombre d'histoires grandit, l'échantillon grandit aussi et les paramètres m_N et σ_N convergent vers des valeurs limites m et σ qui correspondent aux résultats recherchés. Plus σ est petit, moins la variable aléatoire correspondante est dispersée autour de sa moyenne et plus sa densité de probabilité est pointue.
La qualité de l'estimation peut donc être mesurée par la fourchette dans laquelle se trouve l'estimation m_N par rapport à la valeur vraie m. Cela s'exprime à l'aide de la notion de confiance à $\alpha\%$ qui exprime la probabilité que la moyenne estimée m_N se trouve dans un intervalle de confiance autour de la valeur " vraie " m. Un intervalle de confiance à 95% (La probabilité pour que l'espérance cherchée se trouve dans cet intervalle est de 0.95) est donné par :

$$C = [m_N - \frac{1.96\sqrt{\sigma_N}}{\sqrt{N}}, m_N + \frac{1.96\sqrt{\sigma_N}}{\sqrt{N}}] \tag{III.18}$$

Plus l'intervalle de confiance est petit et α grand, plus l'estimation m_N de m est précise.

Cependant, dans le cadre de la sûreté de fonctionnement, le modèle simulé est régi par des événements très rares (les défaillances) et des événements très fréquents (fonctionnement normal du système), et ce, simultanément. La simulation est alors cadencée par de nombreuses occurrences d'événements fréquents qui ne reflètent pas le comportement du système en présence de défaillances. C'est le problème de simulation des événements rares. Un nombre important d'histoires sont nécessaires pour voir apparaître un événement redouté, ce qui implique des temps de calcul importants. Pour pallier à ce problème, dans notre approche l'évaluation est centrée seulement aux séquences critiques déterminées précédemment au cours de l'analyse quantitative. Nous procédons à une simulation Monte Carlo par sauts ; c.à.d ne lancer la simulation qu'à partir du moment ou une défaillance apparait, d'évaluer l'état du système à l'issue de la reconfiguration, et de reprendre la simulation à la défaillance suivante, et ce jusqu'à ce qu'un évènement critique ou la fin de la mission soit atteint. L'algorithme suivi pour effectuer la simulation Monte Carlo est donné dans l'organigramme III.26 suivant :

III.7 conclusion

Au cours de ce chapitre ont été présentés différents modèles pour la modélisation des systèmes dynamiques hybrides permettant de déterminer le modèle le plus approprié pour les objectifs recherchés dans notre étude, en l'occurrence les RdP Prédicats-Transitions Différentiels stochastiques, un formalisme décrivant parfaitement la nature dynamique hybride des systèmes étudiés, l'évolution comportementale est assez mise en évidence. Cependant les outils d'analyse dont ils disposent sont limités dans l'interprétation du modèle pour expliquer les phénomènes indésirables. La contrainte majeure est la difficulté (ou l'impossibilité) de différencier entre les relations de cause et de précédence à partir du marquage des marquages. La connaissance de ces relations est primordiale car elle favorise largement la compréhension et l'analyse des risques industriels rencontrés. D'où l'idée de substituer le graphe des marquages en introduisant dans une démarche analytique, des connecteurs et des règles empruntés de la logique linéaire mais adaptés à notre démarche. Ainsi, profitant de l'association intelligente des modèles des RdP et de la LL, il a été possible de concevoir un algorithme original permettant l'extraction optimale des scenarios critiques. L'un des principaux avantages de l'algorithme proposé est son efficacité dans la sélection et le traitement des seules séquences du modèle ayant effectivement une influence sur l'avènement des situations critiques. Ce qui réduit forte-

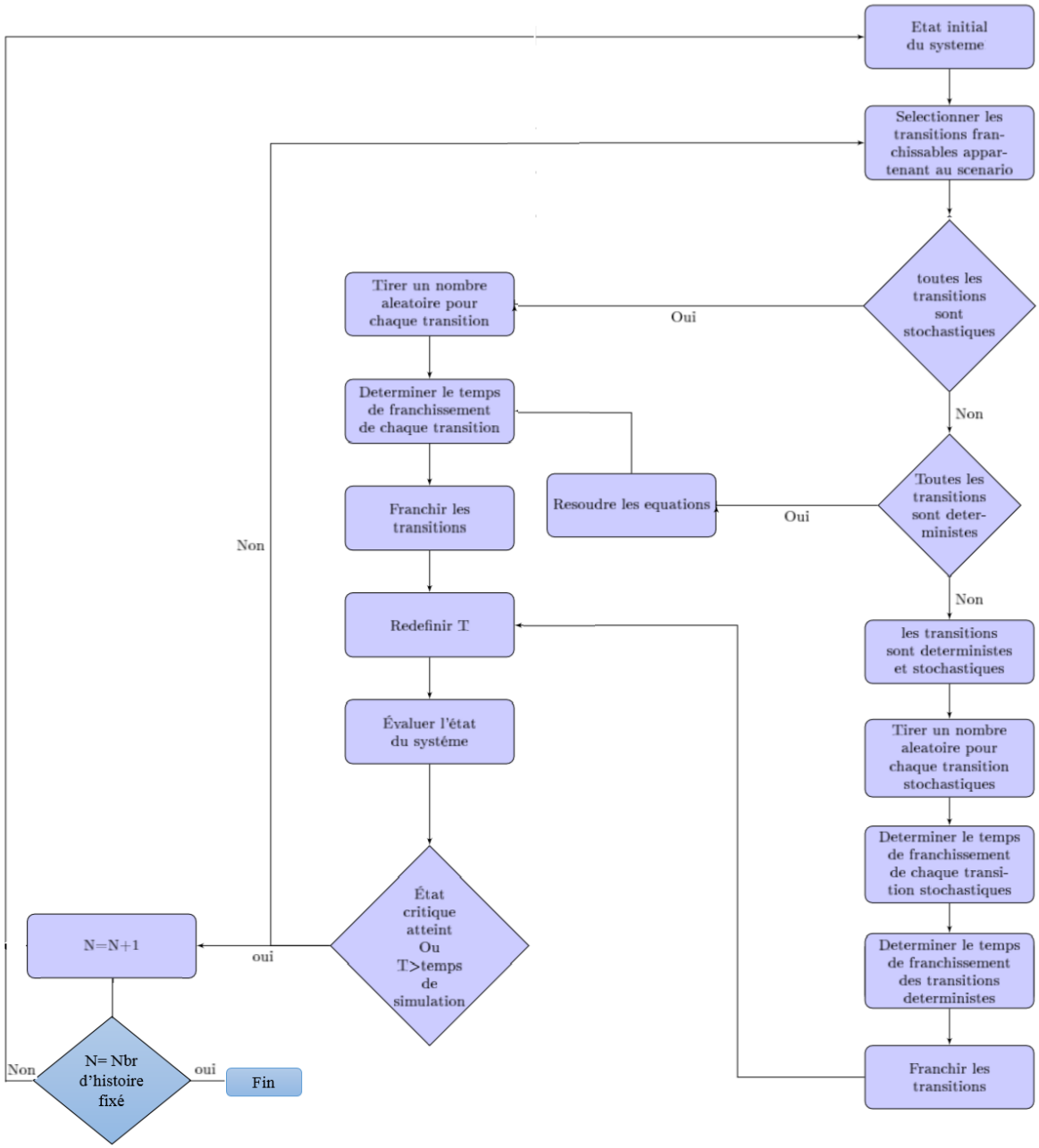


FIGURE III.26: Organigramme de l'algorithme de la simulation Monté Carlo.

ment le nombre de cas à examiner et la durée de la simulation.

L'algorithme comporte 3 étapes incluant deux sub-algorithmes itératives dédiées à l'extraction des transitions et des scénarios critiques en recourant à la prospection et l'isolation des seules séquences utiles dans l'analyse.

L'analyse qualitative a été complétée par une analyse quantitative dans le but d'éva-

luer la probabilité d'occurrence de chaque scénario critique. Celle-ci utilise l'association du RdP et de la simulation Monte Carlo qui constitue un outil d'évaluation numérique performant pour l'étude des systèmes complexes selon divers auteurs cités dans l'étude bibliographique. Cependant, la méthode souffre d'une durée de calcul qui peut être très importante, pour palier a ce problème, nous avons proposé d'effectuer la quantification a l'aide d'une simulation Monte-Carlo par sauts réduisant ainsi le temps de calcul.
Dans le chapitre suivant, nous allons présenter les résultats de l'application de notre méthode de recherche et de quantification de la probabilité d'occurrence des scénarios critiques sur un exemple de système.

Chapitre IV

Application

IV.1 Introduction

Dans le chapitre précédent, nous avons présenté une méthode de recherche de scénarios critiques suivie d'une démarche de quantification de la probabilité d'occurrence de chaque scénario. Ceci a été rendu automatique grâce aux algorithmes que nous avons proposé. Cette méthode est à appliquer à partir d'un modèle réseau de Petri. L'anlyse qualitative est appliquée sur le modèle réseau de Petri ordinaire sous-jacent au réseau de Petri Prédicats Transitions Différentiels Stochastiques du système étudié et l'analyse quantitative sur le Prédicats Transitions Différentiels Stochastiques. Au travers d'un exemple simple de système mécatronique, nous allons mettre en application notre méthode de recherche et de quantification de la probabilité d'occurrence des scénarios. Nous en présenterons les résultats sur le système choisi et nous en signalerons également les limites et les perspectives d'amélioration. Nous traiterons le système de refroidissement des bacs de stockage des fluides inflammables qui illustre parfaitement la problématique des systèmes mécatroniques.

IV.2 Système de refroidissement des bacs de stockage des fluides inflammables

Le système de refroidissement des bacs de stockage des fluides inflammables a été considéré comme un cas d'étude (figure IV.1). Le système comprend : deux bacs de stockage de fluide inflammable, deux réservoirs d'eau pour le refroidissement, reliés chacun

à une cuve destinée à la récupération de l'eau utilisée, d'une unité de commande électronique,deux capteurs, de trois électrovannes et de deux pompes. Ce système consiste en la réduction par l'eau, de la chaleur excédentaire du fluide inflammable stocké dans les bacs, résultant de l'élévation de la température de l'air ambiant. La réduction de la température du fluide à une température acceptable empêche un incendie probable.
D'une manière simple, le fonctionnement normal de ce système est le suivant : l'unité de commande électronique (ECU) reçoit l'information sur la température du fluide (T_F) stocké dans chaque bac. Si la température du fluide d'un bac atteint la température limite ($T_L = 45^oC$), l'ECU commande l'ouverture de l'électrovanne concernée (Ev_1 pour le bac 1 et Ev_2 pour le bac 2) permettant à une quantité d'eau (du réservoir d'eau 1 ou 2) de circuler à travers la paroi du bac pour refroidir le fluide stocké par le principe d'échange de chaleur. Une fois le bac refroidi, l'ECU contrôle la fermeture de l'électrovanne et l'eau utilisée pour le refroidissement est récupérée instantanément dans la cuve correspondante. Ensuite, l'ECU commande la mise en marche de la pompe pour ajuster le volume d'eau du réservoir à partir de la cuve et son arrêt dès que le volume $V = V_{max}$.
Si la température du fluide (T_F) atteint la température limite (T_L) dans un bac et que l'électrovanne associée est défaillante, l'ECU commande l'ouverture de la troisième électrovanne (Ev_3) en remplacement de l'électrovanne défaillante.
En ce qui concerne les pompes, la défaillance envisagée est le refus de s'arrêter. Dans ce cas, l'ECU contrôle l'ouverture de l'électrovanne correspondante pour faciliter la circulation de l'eau et donc éviter le débordement du réservoir d'eau. Le système fonctionne alors en mode dégradé.
Dans tous les cas, la sécurité des bacs de stockage est privilégiée. Ev_3 ne peut pas remplacer Ev_1 ou Ev_2 pour défaillance des pompes.
Le déclenchement d'un incendie dans le bac de stockage et le débordement du réservoir d'eau 1 ou 2 sont les deux états critiques à prendre en compte dans le système. Le débordement du réservoir est considéré critique pour des raisons économique et écologique.

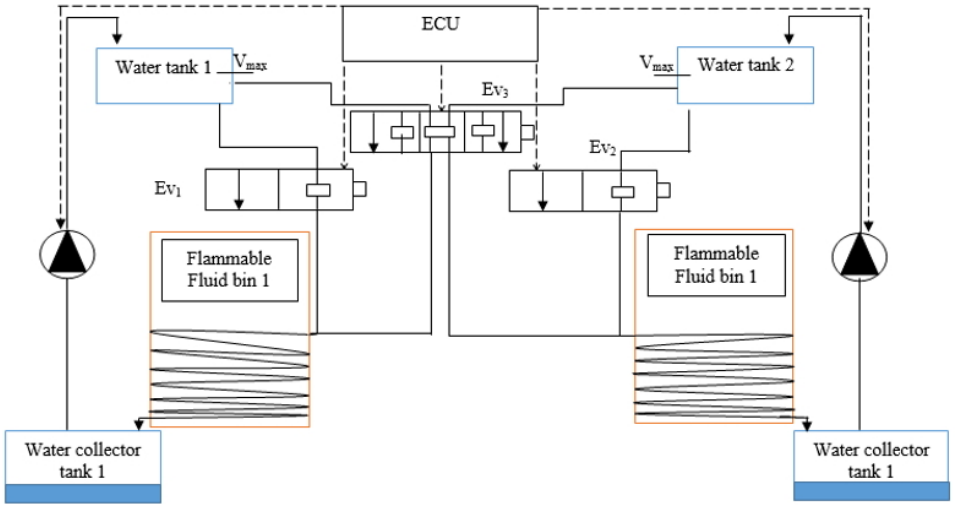


FIGURE IV.1: Les composants du système de refroidissement des bacs de stockage.

IV.3 Modélisation

IV.3.1 Analyse fonctionnelle

Cette analyse permet une description synthétique des modes de fonctionnement du système, ainsi que la connaissance des fonctions qu'il doit garantir.
La réalisation de cette analyse fonctionnelle se déroule principalement en deux étapes :

- L'Analyse Fonctionnelle Externe qui a pour objectif de formaliser et de valider l'analyse du besoin ;
- L'Analyse Fonctionnelle Interne dans le but d'identifier les fonctions techniques du système à étudier.

Analyse Fonctionnelle Externe L'analyse fonctionnelle externe pratiquée sur le système a conduit au diagramme de cas d'utilisation de la figure IV.2.
A gauche, dans le diagramme sont représentés les acteurs internes qui sont : les électrovannes, la pompe, le capteur et l'ECU.
Au centre de la figure on retrouve les fonctions du système. La fonction principale du système est de **Refroidir** les bac de stockage.
Diverses fonctions internes sont effectuées pour y parvenir :

- Transmettre la température ambiante à l'ECU (unité de commande électronique),
- Commander les électrovannes,

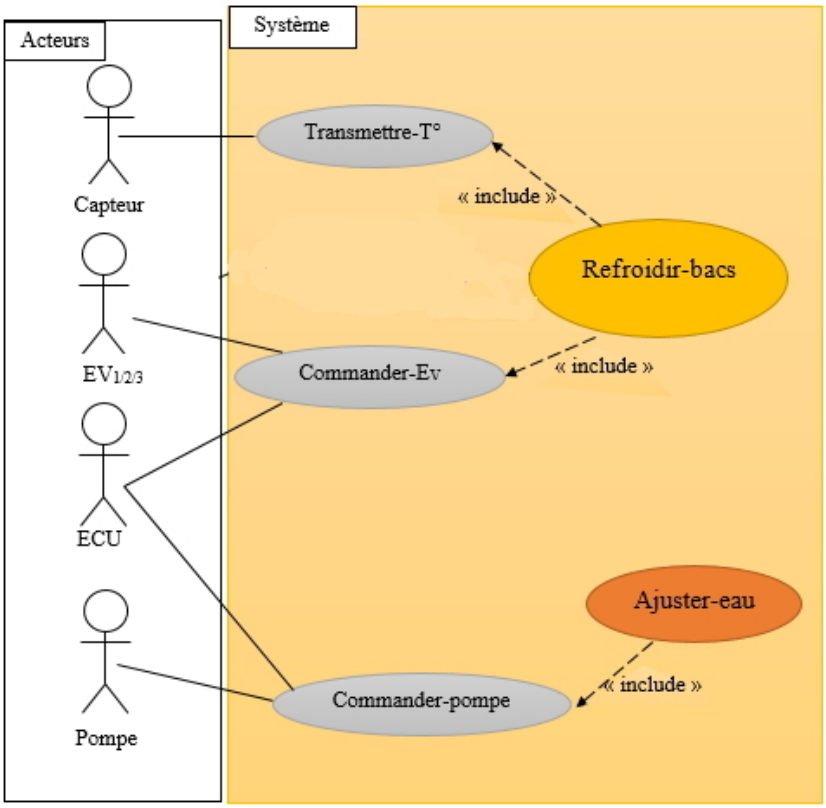


FIGURE IV.2: Diagramme de cas d'utilisation du système.

La fonction secondaire du système est la suivante :
Ajuster le niveau d'eau dans le reservoir d'eau.
Ainsi, il est facile de distinguer les différentes fonctions du système étudié.

Analyse fonctionnelle interne Pour l'analyse fonctionnelle interne, il est considéré que le système comprend un calculateur, deux pompes, trois électrovannes et deux capteurs.
Le digramme de classes de la figure IV.3 indique la décomposition arborescente et hiérarchique du système étudié et également il permet de visualiser les différentes fonctions de contrainte. Le diagramme comporte cinq classes :

— La classe C_1 (classe système) qui représente le système, a la température T_F comme attribut, c'est à dire en fonction de la valeur de T_F le système refroidi les bacs.
— La classe C_2 (classe de capteur) modélise le capteur de température. Cette classe a comme attribut la résistance R. Le capteur délivre une résistance proportionnelle

à la température ambiante.

— La classe C_3 (classe d'ECU) décrit l'ECU du système. L'ECU reçoit l'information du capteur, surveille la température et commande l'électrovanne.

— La classe C_4(classe électrovanne) a le courant comme attribut. Un courant circule dans la bobine de l'électrovanne, soit pour l'ouvrir ou la fermer.

— La classe C_5 (classe de pompe) décrit la pompe du système qui permet d'ajuster le volume d'eau du réservoir.

Une relation de composition relie la classe C_1 aux classes C_2, C_3, C_4et C_5 afin de distinguer le système et de ses divers composants.

Il existe deux fonctions de contraintes qui sont :

— L'énergie : alimenter en énergie électrique la pompe, l'électrovanne et l'ECU pour fonctionner.

— L'environnement : résister à l'environnement externe.

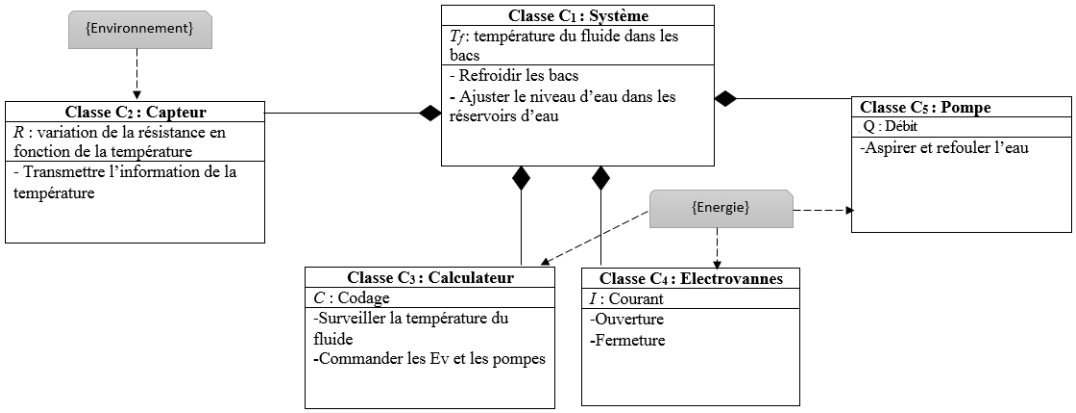


FIGURE IV.3: Diagramme de classes

IV.3.2 Analyse dysfonctionnelle

L'analyse fonctionnelle précédemment effectuée n'apporte aucune information sur les défaillances potentielles que peut rencontrer le système que nous avons choisi d'étudier. Pour cette raison l'analyse dysfonctionnelle est nécessaire dans le but de nous fournir les informations sur l'état du système et obtenir ainsi les causes de défaillance de ce même système. L'application de l'AMDE sur le système est donnée dans le tableau IV.1. À chaque fonction sont décrits les modes de défaillance possibles, les causes probables et les effets redoutés.

TABLE IV.1: L'AMDE du système de refroidissement des bacs de stockage des fluides inflammables

Fonctions	Fonctions externes	Fonctions internes	Composants	Mode de défaillance	Causes	Effets
FONCTION PRINCIPALE	Refroidir les bacs	Transmettre l'information relative à la température	Capteur	Pas de transmission	Capteur défaillant	Augmentation de la température et risque d'incendie
					Présence de calamine	
					Pas de connexion des connecteurs	
					Coupure des connecteurs	
				Transmission altérée	Mauvaise connexion	
					Coupure des connecteurs	
					Capteur défaillant	
				Perte de transmission	Coupure des connecteurs	
					Mauvaise connexion	
					Capteur défaillant	

FONCTION PRINCIPALE	Refroidir les bacs	Commander les électrovannes	Calculateur	Pas de commande	Calculateur défaillant	Augmentation de la température et risque d'incendie
					Perte de connexion entre les EV et le calculateur	
					Pas de connexion des connecteurs	
				Commande altérée	Calculateur défaillant	
					Coupure des connecteurs	
					Mauvaise connexion	
			Électrovannes	Pas d'ouverture et de fermeture des EV	EV défaillantes	
					EV bloquées	
					Mauvaise connexion des EV	
FONCTION SECONDAIRE	Ajuster le niveau d'eau dans les réservoirs d'eau	Commander les pompes	Calculateur	Pas de commande	Calculateur défaillant	Risque de débordement des bacs
					Perte de connexion entre la pompe et le calculateur	
					Pas de connexion des connecteurs	

FONCTION SECONDAIRE	Ajuster le niveau d'eau dans les réservoirs d'eau	Commander les pompes	Calculateur	Commande altérée	Calculateur défaillant	Risque de débordement des bacs
					Coupure des connecteurs	
					Mauvaise connexion	
			Pompes	Pas d'enclenchement /d'arrêt des pompes	Pompes défaillantes	
					Mauvaise connexion	
					Pas de connexion des connecteurs	
FONCTION DE CONTRAINTE	Alimenter le système	Brancher le système électrique	Système électrique	Perte de contact électrique	Usure des connecteurs	Risque d'incendie/ débordement des bacs

IV.3.3 Détermination des équations différentielles

Les parois d'un bac ainsi que les différents phénomènes de transfert de chaleur existants sont présentés dans la FigureIV.4. Ceci permet d'obtenir les équations différentielles représentant la partie continue du système.

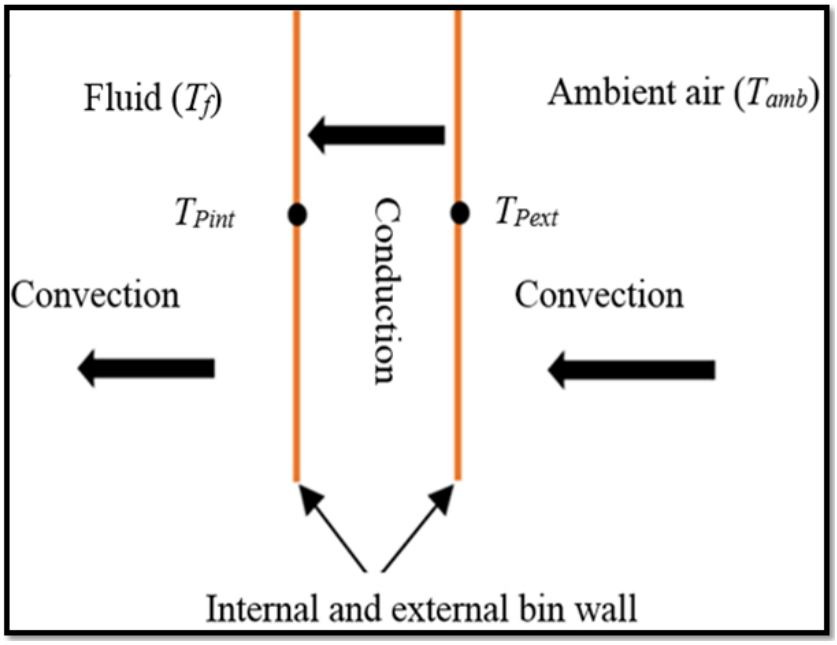


FIGURE IV.4: Transfert de chaleur entre l'air ambiant et le fluide stocké dans les bacs

Le flux de chaleur est transmis de l'air ambiant jusqu'au fluide suivant deux mechanismes de transfèrt de chaleur : ***convection***(air/paroi extérieur du bac(P_{ext})) suivie d'une **conduction** (paroi extérieur du bac(P_{ext})/paroi interne du bac(P_{int}))et finalement une ***convection***(paroi interne du bac/fluide).
L'équation décrivant la variation du flux en fonction de la température ambiante et la température de la paroi externe du bac et donnée comme suit :

$$\Phi = \Phi_{convection(air/Pext)} = \Phi_{conduction(Pext/Pint)} = \Phi_{convection(Pint/fluide)} \tag{IV.1}$$

En remplaçant chaque flux de chaleur par son expression on obtient l'équation suivante :

$$\Phi = h_{ext}(T_{amb} - T_{Pext}) = KS(T_{ext} - T_{Pint}) = h_{int}(T_{int} - T_f) \tag{IV.2}$$

avec :
Φ : flux de chaleur(w/m^2)

h_{ext}, h_{int} : coefficient de convection $(w/m^2.k)$
T_{amb} : température ambiante (K)
T_{Pext} : température de la paroi externe du bac (K)
T_{Pint} : température de la paroi interne (K)
T_f : température du fluide (K)
K : conductivité thermal du matériaux $(w.m^{-1}.K^{-1})$
S : surface du bac
La température du fluide varie de dT, donc :

$$dQ = \rho.C.V.dT_f \tag{IV.3}$$

avec :
Q :quantité de chaleur
ρ : La masse volumique du fluide $(kg.m^{-3})$,
C :la capacité thermique du fluide $(J.kg^{-1}.K^{-1})$,
V :le volume du fluide (m^3),
Sachant que :

$$\Phi = \frac{dQ}{dt} \tag{IV.4}$$

Et en posant :
$T_{Pext} = T_{amb}; T_{Pint} = T_f$
Nous obtenons :

$$\rho.C.V.dT_f = KS(T_{amb} - T_f)dt \tag{IV.5}$$

Pour alléger l'écriture, posons :$\tau = \dfrac{\rho.C.V}{KS}$
L'équation différentielle s'écrit donc :

$$\frac{dT_f}{dt} + \frac{T_f}{\tau} = \frac{T_{amb}}{\tau} \tag{IV.6}$$

L'équation différentielle obtenue est une équation différentielle du premier ordre à coefficient constants avec second membre.
Le refroidissement est effectué par l'écoulement d'une quantité d'eau a travers la paroi du bac.Nous présentons la figureIV.5 afin de déterminer le temps nécessaire de l'écoulement de cette quantité d'eau.

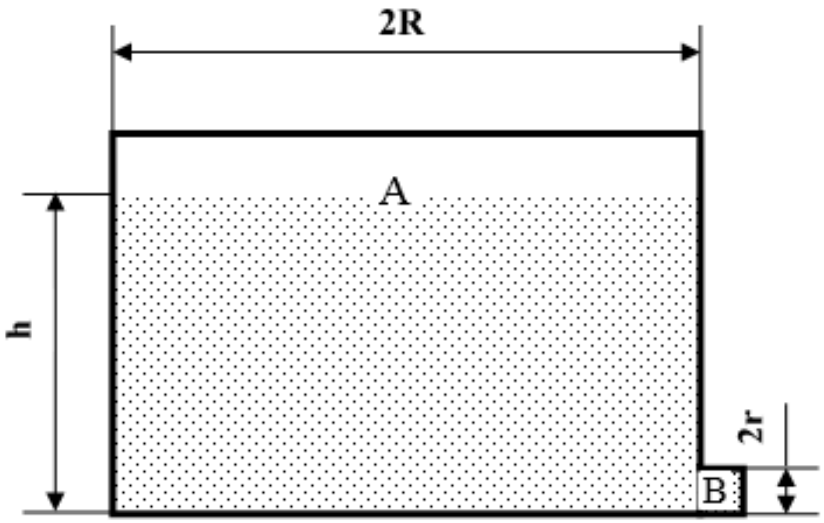


FIGURE IV.5: Écoulement d'eau

D'après la loi de conservation du débit :

$$Q_A = Q_B \tag{IV.7}$$

or :

$$Q = S.V \tag{IV.8}$$

alors :

$$S_A.V_A = S_B.V_B \tag{IV.9}$$

donc :

$$V_A = \frac{S_B.V_B}{S_A} \tag{IV.10}$$

D'après la loi de Torricelli :

$$V_B = \sqrt{2gh} \tag{IV.11}$$

En remplaçons IV.11 dans IV.10 on obtient :

$$V_A = (\frac{r}{R})^2\sqrt{2gh} \tag{IV.12}$$

Sachant que :

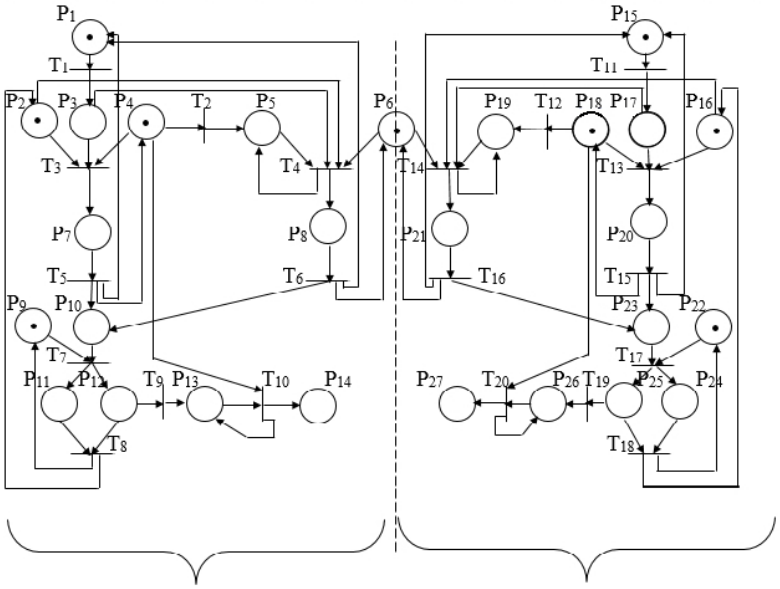
$$V_A = \frac{dh}{dt} \tag{IV.13}$$

$$\frac{dh}{dt} = -(\frac{r}{R})^2\sqrt{2gh} \tag{IV.14}$$

Nous obtenons une équation différentielle du 1^{ere} ordre qui nous donne l'évolution de la hauteur du liquide h dans le reservoir en fonction du temps t.
Une fois l'étape de refroidissement terminée, une pompe sert à ajuster le niveau d'eau dans le reservoir d'eau avec un débit $Q(l/s)$.

IV.3.4 Modèle RdP du système

Les composants du système de refroidissement décrits précédemment, sont disposés symétriquement, en deux sous-systèmes, par rapport à l'ECU et à l'Ev_3. Ainsi il est plus facile de modéliser d'abord un sous-système (par exemple celui constitué avec le bac 1) et le dupliquer par la suite pour concevoir le modèle global du système de refroidissement en entier (Fig. IV.6).
Le modèle du sous système du premier bac a été obtenu de la manière suivante.
À l'état initial, cinq places sont marquées : $M_0 = P_1P_2P_4P_6P_9$. La place P_1 modélise la présence du fluide inflammable dans le bac 1 a une température acceptable. Celle-ci est associée avec l'équation IV.6 (F_1) décrivant l'évolution de la température du fluide dans le bac.
La place P_2 modélise la présence d'eau dans le réservoir 1.
Les places P_4, P_6 et P_9 signifient respectivement que les électrovannes (Ev_1 et Ev_3) et la pompe 1 sont opérationnelles.



Fonctions du système

$F_1 : \frac{dT_{f1}}{dt} + \frac{T_{f1}}{\tau} = \frac{T_{amb}}{\tau}$;$F_7 = F_8 = \frac{dh}{dt} = -(\frac{r_1}{R_1})^2\sqrt{2gh}$;$F_{12} = Q_1$;$F_{15} : \frac{dT_{f2}}{dt} + \frac{T_{f2}}{\tau} = \frac{T_{amb}}{\tau}$;$F_{20} = F_{21} = \frac{dh}{dt} = -(\frac{r_2}{R_2})^2\sqrt{2gh}$; $F_{25} = Q_2$

$F_2 = F_3 = F_4 = F_5 = F_6 = F_9 = F_{10} = F_{11} = F_{13} = F_{14} = F_{16} = F_{17} = F_{18} = F_{19} = F_{22} = F_{23} = F_{24} = F_{26} = F_{27} = \varnothing$

Fonction de sensibilisation

$e_1 : T_{f1} > 45^o c$;$e_2 : \lambda$;$e_3 = e_4 = e_7 = e_{13} = e_{14} = e_{17} = \varnothing$;$e_5 = e_6 : h_1 = h_{1req}$;$e_8 = e_{10} : V_1 = V_{1max}$;$e_9 : \lambda$;$e_{11} : T_{f2} > 45^o c$;$e_{12} = e_{19} : \lambda$; $e_{15} = e_{16} : h_2 = h_{2req}$;$e_{18} = e_{20} : V_2 = V_{2max}$

Fonction de jonction

$j_5 = j_6 : h = h_I - h_{1req}$;$j_{15} = j_{16} : h = h_I - h_{2req}$;$j_8 : T_{f1} = 30^o c$

$j_{18} : T_{f2} = 30^o c$;$j_1 = j_2 = j_3 = j_4 = j_7 = j_9 = j_{10} = j_{11} = j_{12} = j_{13} = j_{14} = j_{17} = j_{19} = j_{20} = \varnothing$

FIGURE IV.6: Modèle globale du système de refroidissement des bacs de stockage

A partir de ce marquage, deux transitions peuvent être franchies T_1 etT_2 :

— La transition T_1, modélisant l'élévation de la température jusqu'à la température seuil, consomme le jeton dans P_1 par son tir, quand $T_{f1} > 45^o c$ ($e_1 : T_{f1} > 45^o c$). Ceci marque la place P_3, signifiant que le fluide a atteint sa température limite ($T_L = 45^o C$). DeP_3, T_3 est franchissable et consomme les jetons dans P_2, P_3, P_4 par son tir. Ceci marque la place P_7, ce qui signifie que Ev_1 est ouverte permettant ainsi d'écouler une quantité requise d'eau froide à travers la paroi du bac pour refroidir le fluide stocké (T_F doit être $< 45^o C$).La place P_7 est associée a l'équation IV.14 décrivant cet écoulement. De P_7, T_5 est franchissable quand toute la quantité d'eau nécessaire a été déversée($e_5 : h = h_{1req}$) pour marquer les places P_{10} et P_4 signifiant respectivement que l'eau utilisée est récupérée dans la cuve 1 et l'Ev_1 reprend son état initial (fermé).À cet instant le niveau d'eau dans le reservoir est équivalent à la différence entre le niveau initial h_I et h_{1req} ($j_5 : h = h_I - h_{1req}$).

— La transition T_2 modélise la défaillance de l'Ev_1 ($e_2 : \lambda$)et son franchissement marque la place P_5. P_5 active la transition T_4, modélisant l'ouverture de l'Ev_3 lorsque la température limite est atteinte. Ce franchissement consomme les jetons P_5 et P_6 pour produire un jeton dans P_8, indiquant que l'Ev_3 est ouverte pour assurer le processus de refroidissement du bac.La place P_8 est associée a l'équation IV.14 décrivant cet écoulement. À partir de P_8, T_6 est franchissable, lorsque toute la quantité d'eau requise est déversée($e_6 : h = h_{1req}$) pour marquer les places P_{10} et P_6 signifiant respectivement que l'eau utilisée est récupérée dans la cuve 1 et l'Ev_3 a repris son état initial (fermé).A cette instant le niveau d'eau dans le reservoir est équivalent à la différence entre le niveau initial h_I et h_{1req} ($j_6 : h = h_I - h_{1req}$).

Des places P_9 et P_{10}, la transition T_7 modélisant le déclenchement de la pompe 1 est franchissable pour marquer les places P_{12} et P_{11} indiquant que la pompe est déclenchée et le remplissage du réservoir d'eau a commencé, avec un débit de le pompe Q_1 ($F_{12} : Q_1$).P_{11} etP_{12} activent la transition T_8 dont le tir modélise l'arrêt de la pompe dès que le volume d'eau dans le réservoir $e_8 : V = V_{max}$, et marque les places P_2 et P_9 signifiant respectivement que le remplissage du réservoir d'eau est fini et la pompe est retournée à son état initial. À cet instant la température du fluide est a une température acceptable ($j_8 : T_{f1} = 30^o c$)

P_{12} seule active la transition T_9, son franchissement modélise la défaillance de la pompe ($e_9 : \lambda$) et marque la place P_{13} qui active la transition T_{10}. T_{10} est franchie, dès que

le volume d'eau dans le réservoir $e_{10} : V = V_{max}$, en consommant les jetons de P_{13} et P_4 pour marquer P_{14} signifiant que le système fonctionne en mode dégradé. C'est-à-dire lorsque la pompe 1 est défaillante (refus de s'arrêter), l'ECU actionne Ev_1 pour permettre la circulation de l'eau en circuit fermé.
Le modèle du premier bac de stockage est maintenant configuré, le modèle du second bac est simplement dupliqué pour obtenir le modèle global du système.
Pour une meilleure lisibilité, les différentes matrices M_c représentant les différents états critiques ne seront représentées que par les places concernées. Cette modélisation fait apparaître les marquages critiques suivants :
Incendie dans le bac 1 $Mc_1 = [P_3 P_5 P_{21}]$ cette représentation signifie qu'il y a une marque en P_3, P_5, P_{21} et le reste des places ne sont pas concernées. De même pour les autres matrices : incendie dans le bac de stockage 2 $Mc_2 = [P_8 P_{17} P_{19}]$, débordement du reservoir 1 $Mc_3 = [P_5 P_{13}]$ et débordement dans le reservoir 2 $Mc_4 = [P_{19} P_{26}]$

IV.4 Mise en œuvre de l'algorithme

Comme on peut le constater, la lecture seule du modèle (Fig.IV.6) n'est pas suffisante pour se prononcer sur les transitions impliquées dans le processus de l'avènement de chaque scénario critique. Par contre, la simulation proposée parvient à un résultat arborant clairement le franchissement ordonné des transitions constituant les différents scénarios critiques issus du marquage $M_g = M_0$. L'applicabilité de la méthode est établie par la programmation sous Matlab de l'algorithme sur RdP modélisant le système de refroidissement des bacs de stockage des fluides inflammables de la figure IV.6 en considérant les quatre marquages critiques.
De Mc_1 nous obtenons le scénario critique Sc_1. De Mc_2, nous obtenons Sc_2. À partir de Mc_3, nous obtenons deux scénarios critiques $Sc_{3.1}$ et $Sc_{3.2}$. De même pour Mc_4, nous obtenons $Sc_{4.1}$ et $Sc_{4.2}$.
La description de ces scénarios et les résultats obtenus sont détaillés comme suit :
Marquage $Mc_1 = P_3 P_5 P_{21}$
Sc_1 : Ce scénario retrace la succession des événements à l'origine de l'incendie dans le bac 1. Il est représenté sous forme de suite de changements d'états qui mène d'un état de bon fonctionnement à l'état critique où les relations de précédence et de cause sont bien mises en évidence (Fig. IV.7). D'abord, les événements sur les apparitions des défaillances des électrovannes Ev_1 et Ev_2 (T_2, T_{12}) et de l'élévation de température du fluide

dans les deux bacs (T_1, T_{11}) surviennent d'une façon indépendante et aléatoire ; ensuite, par hypothèse, de l'indisponibilité de Ev_3 (T_{14}) utilisée en secours par le bac 2. Ainsi, l'ordre de franchissement établi entre les quatre transitions (T_1, T_2, T_{11}, T_{12}) n'est pas une obligation puisqu'elles sont indépendantes et expriment une relation de précédence et non une relation de cause (la défaillance de Ev_1 n'est pas la cause de la défaillance de Ev_2 ni de l'élévation de température et vice versa). Par contre, le franchissement de T_{14} suit inévitablement ceux de T_{12} et T_{11} exprimant une relation de cause, c'est-à-dire la défaillance de Ev_2 et l'élévation de la température du fluide du bac 2 sont la cause de l'utilisation de Ev_3.
Ce résultat est corroboré par le RdP (Fig. IV.6) dans lequel on peut maintenant distinguer les seules transitions indispensables menant de Mg à Mc_1.

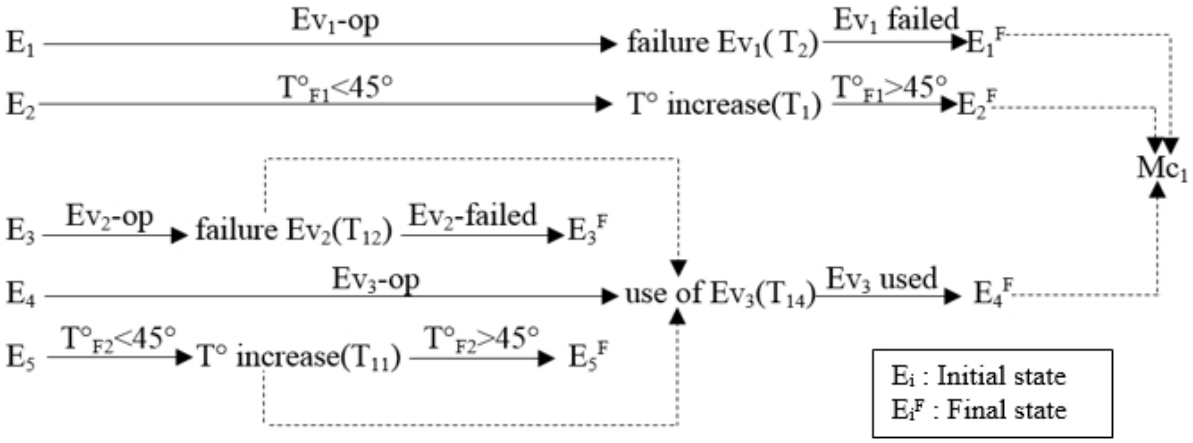


FIGURE IV.7: Scénario critique : incendie dans le bac 1

Marquage $Mc_2 = P_8P_{17}P_{19}$

Sc_2 : "incendie dans le bac de stockage 2" (Fig.IV.8), scénario similaire au précédent : les événements sur les apparitions des défaillances des électrovannes Ev_1 et Ev_2 (T_2, T_{12}) et de l'élévation de température du fluide dans les deux bacs (T_1, T_{11}) surviennent d'une façon indépendante et aléatoire ; ensuite, par hypothèse, de l'indisponibilité de Ev_3 (T_4) utilisée en secours par le bac 1.
Ce résultat est corroboré par le RdP (Fig. IV.6) dans lequel on peut maintenant distinguer les seules transitions indispensables menant de M_g à Mc_2.

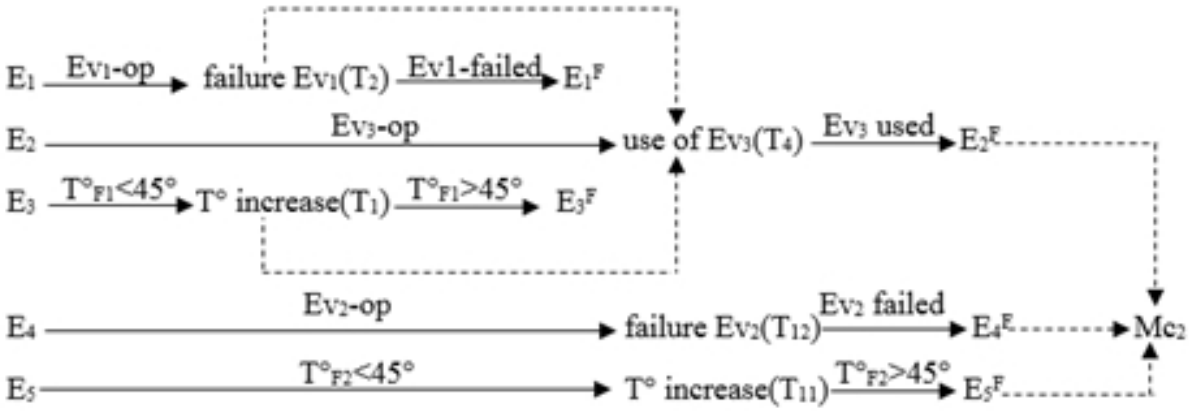


FIGURE IV.8: Scénario critique : incendie dans le bac 2

Marquage $Mc_3 = P_5P_{13}$ Deux scénarios se produisent pour atteindre l'état critique "débordement du réservoir 1".

$Sc_{3.1}$: Après refroidissement du bac 1 et la fermeture de Ev_1 (événements représentés par la succession de T_1, T_3etT_5), la pompe 1 est enclenchée (T_7) et maintenue en fonctionnement jusqu'à la fin du remplissage du réservoir 1. A l'issue de cette opération, si la pompe refuse de s'arrêter(T_9), l'ECU commande la réouverture de Ev_1 pour faciliter la circulation de l'eau évitant ainsi le débordement du réservoir. Cependant, il est possible qu'à cet instant Ev_1 soit également défaillante(T_2), par conséquent le dysfonctionnement de la pompe et de l'électrovanne provoque le scénario critique (Fig.IV.9). En rappelant que dans cette situation Ev_3 ne peut pas être sollicitée, le refroidissement des bacs est privilégié.

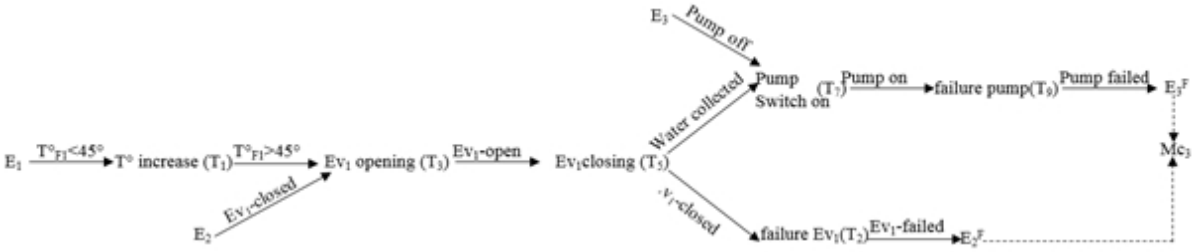


FIGURE IV.9: Scénario critique : débordement du réservoir 1

$Sc_{3.2}$: Suite à l'élévation de la température du fluide dans le bac 1 (T_1) et la défaillance de $Ev_1(T_2)$, Ev_3 est actionnée (T_4) pour libérer la quantité d'eau indispensable au refroidissement du bac 1. Après refroidissement (T_6), la pompe 1 est enclenchée (T_7) et

maintenue en fonctionnement jusqu'à la fin du remplissage du réservoir 1. Si à cet instant, la pompe refuse de s'arrêter (T_9) le scénario critique est inévitable (Fig.IV.10).

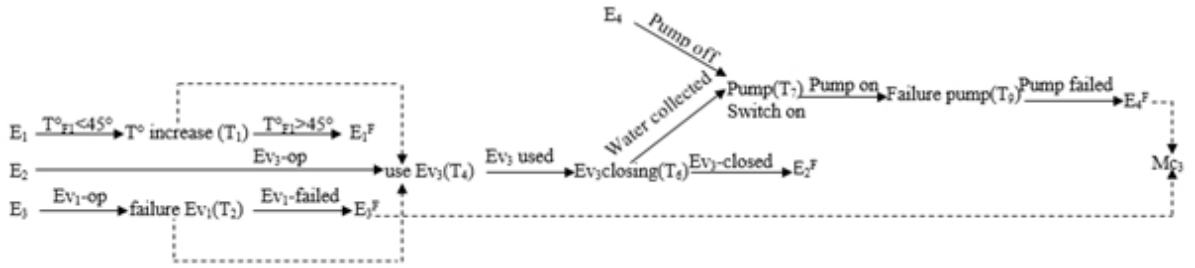


FIGURE IV.10: Scénario critique : débordement du réservoir 1.

Marquage $Mc_4 = P_{19}P_{26}$ Deux scénarios se produisent pour atteindre l'état critique "débordement du réservoir 2".

$Sc_{4.1}$: Après refroidissement du bac 2 et fermeture de Ev_2 (événements représentés par la succession de T_{11}, T_{13} et T_{15}), la pompe 2 est enclenchée (T_{17}) et maintenue en fonctionnement jusqu'à la fin du remplissage du réservoir 2. A l'issue de cette opération, si la pompe refuse de s'arrêter(T_{19}), l'ECU commande la réouverture de Ev_2 pour faciliter la circulation de l'eau évitant ainsi le débordement du réservoir. Cependant, il est possible qu'à cet instant Ev_2soit également défaillante(T_{12}), par conséquent le dysfonctionnement de la pompe et de l'électrovanne provoque le scénario critique (Fig.IV.11). En rappelant que dans cette situation Ev_3 ne peut pas être sollicitée, le refroidissement des bacs est privilégié.

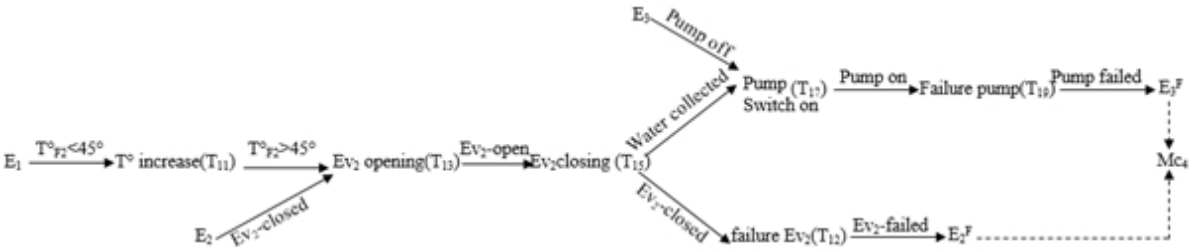


FIGURE IV.11: Scénario critique : débordement du réservoir 2.

$Sc_{4.2}$: Suite à l'élévation de la température du fluide dans le bac 2 (T_{11}) et la défaillance de $Ev_2(T_{12})$, Ev_3 est actionnée (T_{14}) pour libérer la quantité d'eau indispensable au refroidissement du bac 2.

Après refroidissement(T_{16}), la pompe 2 est enclenchée (T_{17}) et maintenue en fonctionnement jusqu'à la fin du remplissage du réservoir 2. Si à cet instant, la pompe refuse de s'arrêter (T_{19}) le scénario critique est inévitable (Fig.IV.12).

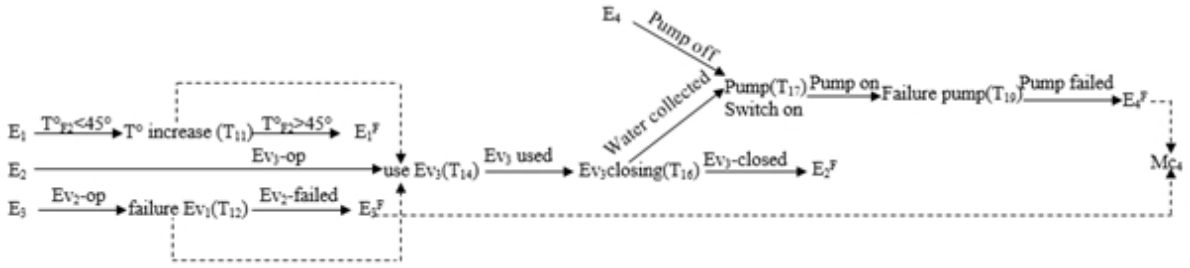


FIGURE IV.12: Scénario critique : débordement du réservoir 2.

IV.5 Simulation Monte Carlo

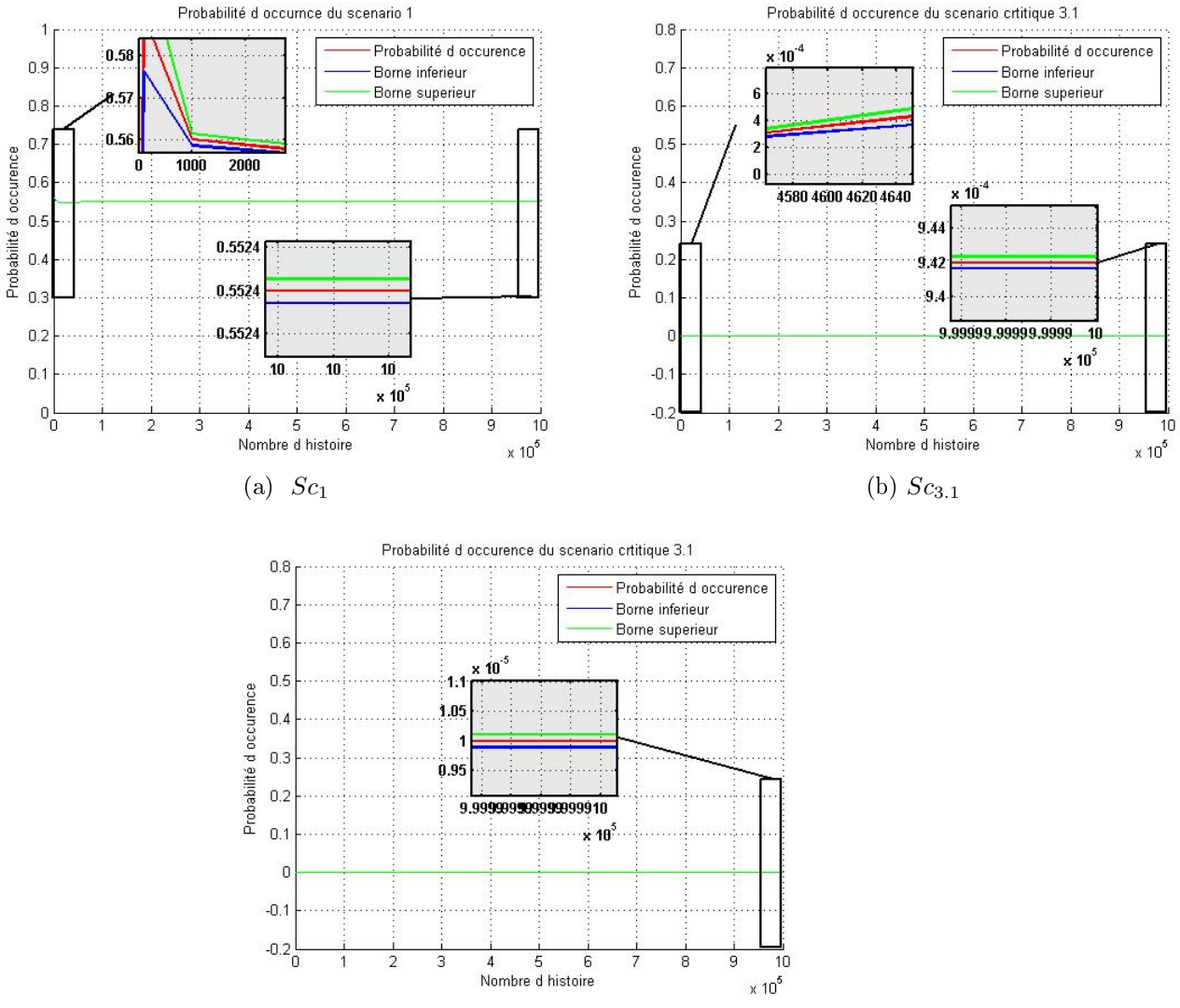
La dernière étape de notre méthodologie consiste à effectuer des simulations du réseau de Petri de la figure IV.6 en considérant les lois de distribution du tableau IV.4 avec les paramètres qui leur sont associés.
Le formalisme RdP utilisé permet de bien décrire les aspects fonctionnel et dysfonctionnelle du système étudié. Le modèle RdP de la figure IV.6 présente donc un bon support pour appliquer la simulation Mc.

TABLE IV.4: Valeurs des paramètres utilisés pour la simulation MC

Composants	**Loi**	**Paramètre**
Électrovanne 1/2	Exponentielle	$\lambda = 3.10^{-4}(h^{-1})$
Pompe 1/2	Weibull	$\beta = 1.2, \eta = 1000(cycles), \gamma = 0$

L'estimation de la probabilité d'occurrence de chaque scénario est alors basée sur l'étude d'un certain nombre de d'histoires, permettant d'en extraire des résultats statistiques. Nous avons associé un estimateur de type binaire à cette probabilité et incrémenter un compteur d'une unité pour chaque histoire dans laquelle le scénario critique se produit. L'estimation de la probabilité est alors obtenue en faisant le rapport entre le nombre d'histoires ayant connu un événement critique et le nombre total d'histoires.
On simule ainsi le RdP suivant son évolution sur une durée d'histoire $T = 1an$ correspondante à la durée qui s'écoule entre deux révisions du système.

On réitère une telle histoire 10^6 fois en partant chaque fois des mêmes conditions initiales et en conservant en mémoire les données numériques obtenues. Comme nous l'avons déjà mentionné au chapitre précédent, nous procédons à une simulation Monte Carlo par sauts concentrée seulement sur les scénarios critiques extrait dans l'analyse qualitative précédemment effectuée suivant l'organigramme présenté dans la section III.6.1.
Après simulation pour l'estimation de la probabilité d'occurrence des scénarios critiques nous obtenons les résultats présentés dans sur la figure IV.13.



(a) Sc_1 (b) $Sc_{3.1}$

(c) $Sc_{3.2}$

FIGURE IV.13: Probabilité d'occurrence des scénarios critiques.

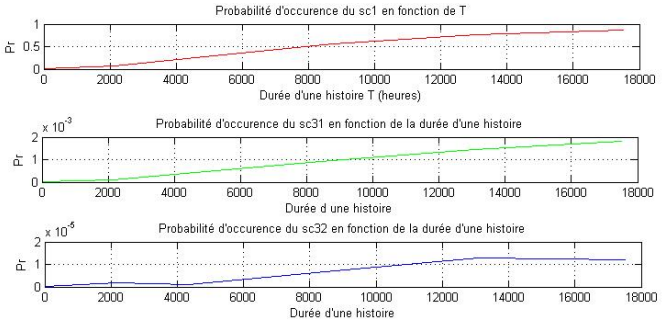
Sur la figureIV.13 nous avons tracé, la probabilité d'occurrence des scénarios Sc_1 (Fig.IV.13a), $Sc_{3.1}$ (Fig.IV.13b),$Sc_{3.2}$ (Fig.IV.13c), ainsi que l'intervalle de confiance en fonction du

nombre d'histoires.Nous constatons sur le graphe que la probabilité fluctue quand le nombre d'histoires n'est pas conséquent, mais celle-ci se stabilise vers la fin où le nombre d'histoires atteint 10^6.Les résultats des probabilités d'occurrence des scénarios critiques, ou bout de 10^6, sont regroupés dans le tableau IV.5.

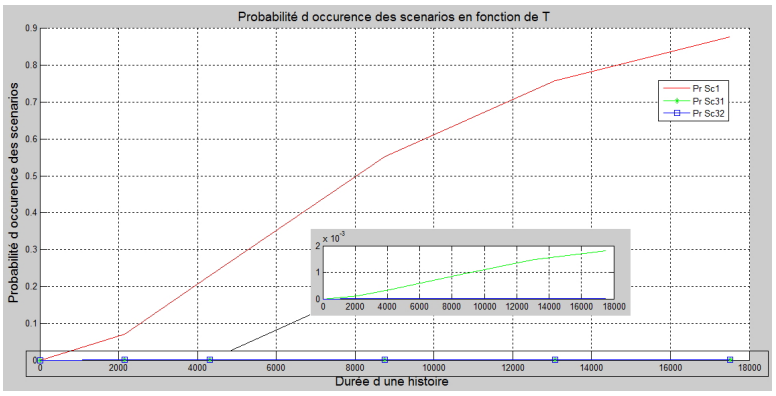
TABLE IV.5: Résultats de la simulation MC

Scénario	**Probabilité d'occurrence**	**intervalle de confiance**	**Temps de simulation(seconds)**
Sc_1	0.5524	$C = [0.5523, 0.5524]$	119.53
$Sc_{3.1}$	$9.42.10^{-4}$	$C = [9.4166.10^{-4}, 9.4234.10^{-4}]$	335.47
$Sc_{3.2}$	1.10^{-5}	$C = [0.9889.10^{-5}, 1.0110.10^{-5}]$	538.93

En utilisant la matrice de criticité, nous constatons qu'avec une probabilité d'occurrence de $9.42.10^{-4}$ pour $Sc_{3.1}$ et de 7.10^{-6} pour $Sc_{3.2}$ le risque est acceptable. Nous préconisons ainsi d'augmenter la durée qui s'écoule entre deux révisions du système. Ceci revient a augmenter la durée d'histoire T, comme il est présenté dans la figure IV.14.



(a) Shéma eclaté



(b) Schéma global

FIGURE IV.14: Probabilité d'occurrence des Scénarios critiques Sc_1, Sc_{31} et Sc_{32} en fonction de la durée T

Sur la figureIV.14a nous avons tracé, la probabilité d'occurrence de chaque scénarios en

fonction de la durée d'une histoire T. Nous regroupons les trois tracés dans la figure IV.14b afin de visualiser la durée de révision qui convient au mieux au système étudié. Même avec une durée d'histoire $T = 2ans$ la probabilité des deux scénarios Sc_{13} et Sc_{23} reste faible.Ces scénarios sont très rares et peuvent donc être supprimés de l'ensemble des scénarios critiques. Par contre, le Sc_1 reste le plus probable à survenir et sur lequel nous nous baserons pour choisir la meilleure échéance de la révision de maintenance.

IV.6 Discussion

IV.6.1 Analyse qualitative

L'approche proposée a permis de procéder, à partir du marquage initial du modèle RdP, à l'extraction optimale des scénarios critiques pouvant entraîner de graves dommages sur les personnes, l'installation et l'environnement. Ainsi, seules les séquences menant à chaque marquage critique ont été déduites (Tabl.IV.6).

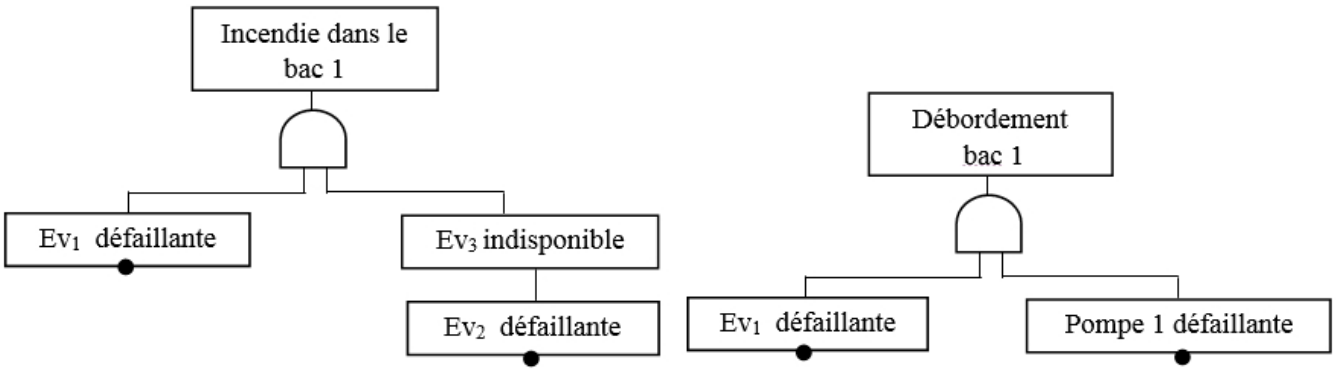
TABLE IV.6: Séquence de chaque scénario

Marquage	**Scenario**	**Sequence**	**nombre de transitions**
Mc_1	Sc_1	$Cs_1 : \begin{bmatrix} T_1 \\ T_2 \\ T_{11} \\ T_{12} \end{bmatrix} \begin{matrix} \longrightarrow \\ \\ \\ \longrightarrow \end{matrix} T_{14}$	5/20
Mc_2	Sc_2	$Cs_2 : \begin{bmatrix} T_1 \\ T_2 \\ T_{11} \\ T_{12} \end{bmatrix} \begin{matrix} \longrightarrow \\ \longrightarrow \\ \\ \end{matrix} T_4$	5/20
Mc_3	$Sc_{3.1}$	$Cs_{3.1} : T_1 \longrightarrow T_3 \longrightarrow T_5 \longrightarrow \begin{bmatrix} T_2 \\ T_7 \end{bmatrix} \longrightarrow T_9$	6/20
	$Sc_{3.2}$	$Cs_{3.2} : \begin{bmatrix} T_1 \\ T_2 \end{bmatrix} \longrightarrow T_4 \longrightarrow T_6 \longrightarrow T_7 \longrightarrow T_9$	6/20
Mc_4	$Sc_{4.1}$	$Cs_{4.1} : T_{11} \longrightarrow T_{13} \longrightarrow T_{15} \longrightarrow \begin{bmatrix} T_{12} \\ T_{17} \end{bmatrix} \longrightarrow T_{19}$	6/20
	$Sc_{4.2}$	$Cs_{3.2} : \begin{bmatrix} T_{11} \\ T_{12} \end{bmatrix} \longrightarrow T_{14} \longrightarrow T_{16} \longrightarrow T_{17} \longrightarrow T_{19}$	6/20

Lors de l'analyse qualitative, en plus d'éviter la propagation du nombre d'états, l'approche a distinctement mis en exergue les relations de précédence et de cause des sé-

quences examinées. Cette connaissance aura par la suite un rôle clé dans l'aide à la prise de décision sur les actions à mener pour anticiper la survenance de catastrophes.
Nous avons également enregistré pour l'analyse du système étudié, une durée de moins d'une minute.

En vue de son évaluation, notre approche a été comparée avec d'autres méthodes. La méthode d'analyse de risque la plus utilisée est l'arbre de défaillance classique. Cette méthode appliquée à l'exemple étudié ne fournit qu'une combinaison d'évènements conduisant à l'état critique envisagé. La figure IV.15 présente deux cas : le premier décrit l'état critique incendie dans le bac 1 dû aux défaillances de EV_1 et EV_2 (Fig. IV.15a) et le deuxième cas décrit l'état critique débordement du réservoir 1 dû aux défaillances de EV_1 et de la pompe 1 (Fig. IV.15b). Le constat majeur relevé est que l'arbre de défaillance ne fournit pas de scénario décrivant dans ses moindres détails les processus de dégradation de l'état de l'installation comme le préconise notre démarche (Sc_1, $Sc_{3.1}$ et $Sc_{3.2}$). On peut connaître le problème sans pour autant expliquer clairement son histoire, c'est-à-dire l'ordre et les relations entre les évènements ne sont pas pris en charge par AdD. Dans ce cas, les résultats sont insuffisants.



(a) Arbre de défaillance de l'incendie dans le bac de stockage 1

(b) Arbre de défaillance du débordement du réservoir 1

FIGURE IV.15: Arbres de défaillances.

Quant au procédé du graphe des marquages, son utilisation conduit à une génération d'un grand nombre d'états.Un aperçu du graphe des marquages est présenté dans la figure IV.16.

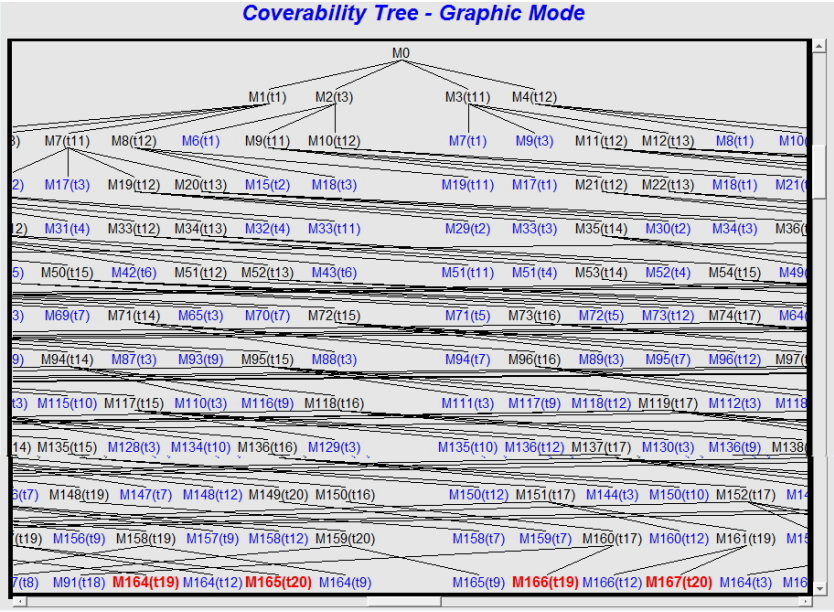


FIGURE IV.16: Graphe des marquages du modèle RdP du système étudié.

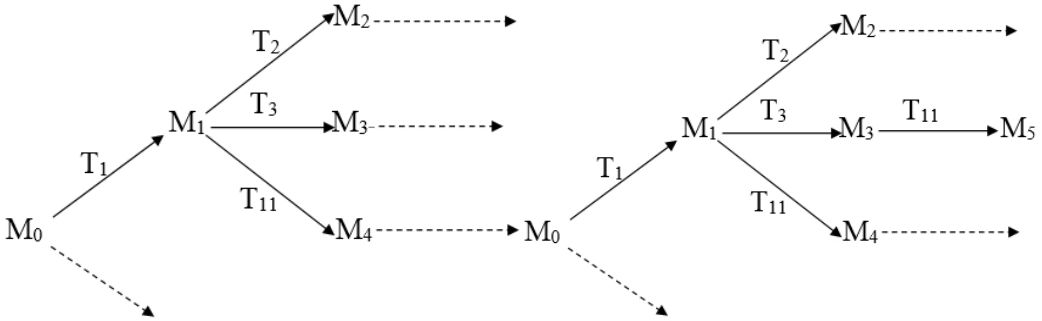
Aussi, on peut remarquer que le graphe ne montre pas la relation réelle entre les événements (la relation de précédence est confondue avec celle de cause). En effet, dans le modèle RdP du système IV.6 on remarque deux situations :

— T_2 et T_3 sont en conflit (le tir de T_2 est la cause de blocage du tir de T_3 et inversement), constituant ainsi une relation de cause,

— et, T_3 et T_{11} sont en parallèle (leur tir est indépendant), constituant ainsi une relation de précédence,

La première incohérence est constatée dès la première étape du tracé du graphe (Fig. IV.17a), c'est-à-dire le conflit (entre T_2 et T_3) exprimant une relation de cause est représenté de la même manière que le parallélisme (T_3 et T_{11}) exprimant une relation de précédence.
La deuxième incohérence est enregistrée dans la suite du tracé (Fig.IV.17b). Par exemple, la séquence $T_1T_3T_{11}$ menant au marquage M_5, fait ressortir une relation de cause entre T_1 et T_3, ceci est confirmé dans le modèle du système (Fig. IV.6) où la succession de ces deux transitions est mise en évidence. En même temps, T_3 et T_{11}, appartenant à la même séquence, se succèdent mais dans le modèle du système elles vont se retrouver en parallèle ce qui implique une relation de précédence entre elles.
En définitif, dans un graphe d'accessibilité, une même structure peut exprimer des relations différentes et induire, par conséquent, une confusion entre les liens de causalité et

de précédence. Alors que la démarche que nous proposons ne rencontre pas ce type de difficulté.



(a) Première étape du tracé du graphe d'accessibilité

(b) Suite du tracé du graphe d'accessibilité.

FIGURE IV.17: Graphe des marquages partiel associé au modèle du système étudié.

IV.6.2 Analyse quantitative

L'analyse qualitative a été complétée par une analyse quantitative, estimant la probabilité d'occurrence de chaque scénario.

En utilisant AdD pour estimer la probabilité d'occurrence d'un évènement critique, seule la connaissance des probabilités des évènements de base ne suffit pas pour déduire la probabilité d'apparition de l'état critique. En effet, pour estimer la probabilité d'occurrence d'un événement, l'arbre de défaillance suppose que tous les événements de base sont indépendants. Ceci revient à dire que par exemple, la probabilité d'occurrence de l'événement *"débordement du bac1"* (fig.IV.15b) est estimée comme suit :

$Pr(debordement) = Pr(defaillanceEV_1).Pr(defaillance\ \ pompe1)$

donc :

$Pr(debordement) = (1 - R_1(t)).(1 - R_2(t))$

où :

$R_1(t)$: est la fiabilité de l'Ev_1 sur une période de 1ans.

$R_1(t)$: est la fiabilité de la pompe sur une période de 1ans.

Dans ce cas, en utilisant les mêmes valeurs des paramètres utilisés lors de la simulation Monte Carlo la probabilité d'occurrence est égale à $Pr = 0.11$, une valeur nettement plus élevée que celle trouvée lors de la simulation. Cette différence s'explique par la justesse

de notre démarche qui se prend en compte l'aspect continue du système étudié.
Afin d'éviter des temps de calcul importants, la simulation Monte Carlo a été réalisée par sauts, l'évaluation est centrée seulement aux séquences critiques déterminées précédemment au cours de l'analyse qualitative. Les résultats obtenus, pour les scénarios Sc_1,Sc_{31} et Sc_{32}, par la simulation par sauts et celle du modèle globale sont présentés dans le tableau IV.7suivant :

TABLE IV.7: Comparaison entre la simulation du modèle global et la simulation par sauts

	Sc1		Sc3.1		Sc3.2	
	Simulation modèle global	Simulation par saut	Simulation modèle global	Simulation par saut	Simulation modèle global	Simulation par saut
Probabilité d'occurrence	0.5502	0.5524	$9.45.10^{(-4)}$	$9.42.10^{(-4)}$	$1.10^{(-5)}$	$1.10^{(-5)}$
Temps	13 min	2.50 min	34 min	7.92 min	20,85min	8,98 min

Pour chaque scénario,et dans les deux cas (simulation du modèle global et par sauts), 10^6 histoires ont été effectuées pour obtenir l'estimation de la probabilité présentée dans le tableau IV.7. Les résultats obtenus en simulant le modèle globale avoisine ceux de la simulation par sauts avec mais avec des écarts dans le temps de calcul. En effet, le temps de calcul pour l'estimation de la probabilité d'occurrence sur le modèle global est jusqu'à 6 fois plus grand que celui par simulation par sauts (cas du scénario 1). Cela signifie que la simulation par sauts a permis une réduction considérable du temps d'environ 80%.

IV.7 Conclusion

Nous avons appliqué, au cours de ce chapitre,l'approche proposée d'extraction des scénarios critiques et d'estimation de la probabilité d'occurrence de chaque scénario, au système de refroidissement des bacs de stockage des fluides inflammables. Ce système utilise une reconfiguration de type partage de ressources. L'électrovanne de secours peut être utilisée en effet par les deux réservoirs mais un seul à la fois. Ce partage de ressources permet certes d'optimiser le nombre d'électrovannes de secours, mais pourrait également générer des scénarios critiques inattendus. Ces scénarios peuvent échapper à la méthode des arbres de défaillances, basée uniquement sur la prise en compte des états de défaillance des composants. Notre approche permet de déterminer les scénarios critiques de manière systématique car basée sur une modélisation adéquate.
Aussi, par son application , nous avons constaté l'efficacité de l'approche dans la sélec-

tion et le traitement des seules séquences du modèle ayant effectivement une influence sur l'avènement des situations critiques. Ce qui réduit fortement le nombre de cas à examiner et la durée de la simulation comparée au graphe des marquages.
Nous avons poursuivi l'analyse par une estimation de la probabilité d'occurrence de chaque scénario. Celle-ci utilise l'association des RdP avec la simulation monte Carlo. La simulation a été réalisée par sauts, donnant ainsi des résultats satisfaisants, avec un temps de calcul moindre par rapport à la simulation du modèle global.
L'utilisation de notre approche sur des exemples plus complexes nécessite le développement d'un logiciel qui sera couplé avec un joueur de réseaux de Petri.

Chapitre V

Stratégie de maintenance

V.1 Introduction

La maintenance est définie selon la norme NF EN 13306 (2010) "Ensemble de toutes les actions techniques, administratives et de management durant le cycle de vie d'un bien, destinées à le maintenir ou à le rétablir dans un état dans lequel il peut accomplir la fonction requise ".
Se rajoute à ces différentes missions professionnelles, une mission majeure et indispensable : " expertise ".
L'enchainement d'évènements non désirables peuvent entrainer des défaillances majeures voire critiques. Leur expertise permet la préparation et la mise en œuvre des mesures appropriées en fonction des enjeux socio-économiques étroitement liés à l'activité et à la qualité des interventions de maintenance. Autrement dit, disposer d'une stratégie de maintenance suffisante pour contrer toute éventuelle défaillance d'un système. La stratégie de maintenance, qui résulte de la politique de maintenance, impose des choix pour atteindre, voire dépasser, les objectifs fixés (Norme AFNOR FDX 60-000 mai 2002).
Ces choix sont à faire pour :

- développer, adapter ou mettre en place des méthodes de maintenance,
- élaborer et optimiser les gammes de maintenance,
- organiser les équipes de maintenance,
- internaliser et/ou externaliser partiellement ou totalement les tâches de maintenance, définir, gérer et optimiser les stocks de pièces de rechange et de consommables,

— étudier l'impact économique (temps de retour sur investissement) de la modernisation ou de l'amélioration de l'outil de production en matière de productivité et de maintenabilité.

La stratégie de maintenance implique la mise en œuvre d'un plan de maintenance avec des objectifs chiffrés et des indicateurs mesurables.
Les résultats mesurés sont comparés aux objectifs et font l'objet d'analyses.
Une partie importante de la stratégie de maintenance concerne les ressources humaines aussi bien chez les intervenants extérieurs à l'entreprise que dans le personnel de l'entreprise elle-même :

— sélection, recrutement,

— formation du personnel,

— gestion des compétences et des habilitations,

— communication,

— etc.

V.2 Typologie et politique de maintenance

De la définition de la maintenance citée précédemment deux notions fondamentales sont à mettre en évidence. La première notion "Maintenir" se rapporte à la maintenance préventive et la deuxième notion "Rétablir" se rapporte à la maintenance corrective.

V.2.1 La maintenance préventive

La maintenance préventive est une maintenance exécutée à des intervalles prédéterminés ou selon des critères prescrits et destinés à réduire la probabilité de défaillance ou la dégradation du fonctionnement d'un bien. Elle est subdivisée en :

La maintenance conditionnelle : maintenance préventive basée sur une surveillance du fonctionnement du bien et/ou des paramètres significatifs de ce fonctionnement et intégrant les actions qui en découlent. Ce type de maintenance, appelé également maintenance prédictive, connait un essor très significatif grâce aux différents travaux de recherche et aux technologies de diagnostic et de contrôle (analyse de huiles, analyse

vibratoire, contrôle non destructif (CND), thermographie IR etc...) et est très largement appréciée auprès des industries manufacturières du moins pour minimiser les coûts de maintenance et optimiser les moyens de maintenance en fonction des objectifs de production.

La maintenance systématique : maintenance préventive exécutée à des intervalles de temps préétablis ou selon un nombre défini d'unités d'usage mais sans contrôle préalable de l'état du bien. La maintenance préventive systématique est sans aucun doute la plus efficace pour éviter la dégradation du bien et l'apparition d'une défaillance le plus longtemps possible, mais très coûteuse. De ce fait, elle trouve son utilisation essentiellement pour les biens nécessitant un niveau de sécurité élevé des domaines du nucléaire, aéronautique ... et les secteurs d'industries stratégiques de pétrochimies, centrales électriques .... Les opérations (actions) menées en maintenance préventive conditionnelle et en maintenance préventive systématique sont techniquement les mêmes (quelques-unes sont citées plus bas). Seulement, sur une période donnée, le nombre (la fréquence) des interventions de la maintenance systématique est supérieur ce qui explique ses coûts importants.

V.2.2 La maintenance corrective

Est une maintenance exécutée après détection d'une panne et destinée à remettre un bien dans un état dans lequel il peut accomplir une fonction requise.
Évidemment, quelques que soient les moyens de la maintenance utilisés, la dégradation et/ou l'apparition devient inévitable à un moment donné. Les opérations de maintenance, dans ce cas sont différentes et indispensables pour remettre le matériel en bon état de marche. Généralement, une telle maintenance est plus sollicitée pour les équipements ayant déjà un certain nombre d'années d'usage. Cependant, il n'est pas rare de constater l'application de la maintenance corrective sur des équipements encore jeunes mais surexploités où la maintenance préventive devient déficiente.
Le choix entre les méthodes de maintenance s'effectue dans le cadre de la politique de la maintenance et doit s'opérer en accord avec la direction de l'entreprise. Pour choisir, il faut donc connaitre :

— les objectifs de la direction,

— les orientations politiques de maintenance,

— le comportement du matériel en exploitation,

— les moyens disponibles d'application de chaque méthode,

— les coûts de maintenance,

— les coûts de perte de production.

V.2.3 Synthèse

En définitif, la maintenance dispose de différentes méthodes (Fig. V.1) et une panoplie d'opérations techniques à mettre en œuvre selon les circonstances auxquelles est confronté le maintenancier et la politique de maintenance adoptée.

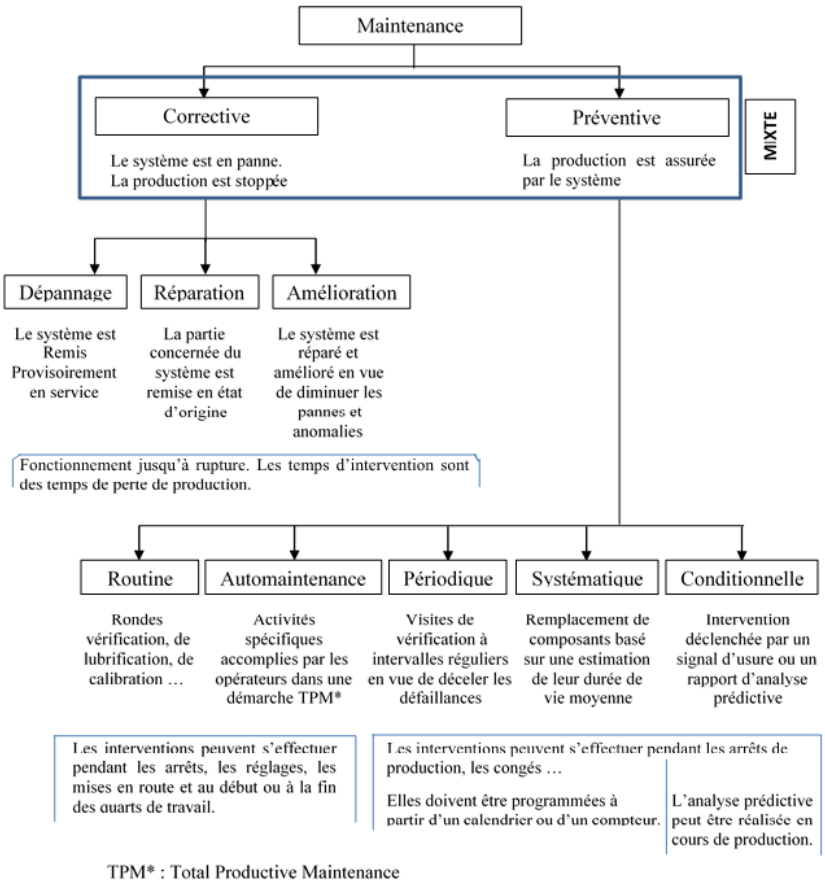


FIGURE V.1: Exemple de typologie de maintenance

V.3 Construction d'une stratégie de maintenance

Une maintenance préventive systématique est certes plus couteuse mais peut s'avérer plus rentable et judicieuse qu'une maintenance conditionnelle pour une chaîne de production particulière dont l'arrêt peut provoquer des pertes financières significatives, des retards de livraison du produit aux clients impactant l'image de marque de l'entreprise ou entrainant des pénalités ou encore une détérioration de la matière première en amont de la chaîne de production, etc ...

Pour les équipements en fin de vie, les soins de prévention ne s'y prêtent plus et seule la maintenance corrective peut encore les garder en survie. D'autres situations sont également envisageables.

Ainsi, au fil de sa perpétuelle évolution, la maintenance a intégré dans ses stratégies des critères technico-économiques fiables pour justifier la pertinence de ses prises de décision sur le choix approprié des opérations de maintenance à mener. Les qualifications et le potentiel disponible du personnel, la sous-traitance, etc... sont également à considérer.

Une stratégie de maintenance standard, du genre "prête à l'emploi", ne saurait exister sachant que chaque équipement durant son fonctionnement a son propre comportement, sa propre pathologie et par conséquent son propre remède.

Pour faire simple, une stratégie de maintenance, est une recette de cuisine concoctée par la cuisinière selon la disponibilité, le dosage des différents ingrédients, le temps de réalisation (préparation, cuisson ...) etc...pour satisfaire les consommateurs. Autrement dit, une bonne stratégie n'est pas constituée totalement par des opérations de la maintenance préventive systématique, ou des opérations de la maintenance conditionnelle ou par des opérations de maintenance corrective. C'est plutôt une combinaison réfléchie de différentes opérations techniques, déterminées en fonction des enjeux en place et en mesure d'optimiser les performances de la stratégie proposée. Selon les situations, les objectifs d'un programme de maintenance sont souvent variés et la définition préalable des critères de choix d'une stratégie de maintenance est indispensable tels que le risque, le coût, la fiabilité et la disponibilité.

V.3.1 Niveaux de maintenance

Dans le tableau ci-dessous sont regroupées quelques actions de maintenance dont le maintenancier puisera pour construire sa stratégie. Ces exemples d'actions de main-

tenance préventive et de maintenance corrective sont présentés selon l'ordre de leur niveau de complexité. Ces actions sont classées en cinq niveaux de maintenance (norme $FDX-60-000$). Les exemples d'actions de maintenance citées ci-dessous sont destinées aux équipements industriels.

TABLE V.1: Niveaux de maintenance

Maintenance préventive	Maintenance corrective
1^{er} niveau de maintenance	
Actions simples nécessaires à l'exploitation et réalisées sur des éléments facilement accessibles en toute sécurité à l'aide d'équipements de soutien intégrés au bien. Ce type d'opération peut être effectué par l'utilisateur du bien avec, le cas échéant, les équipements de soutien intégrés au bien et à l'aide des instructions d'utilisation.	
— Ronde de surveillance d'état, — Graissages journaliers, — Manoeuvre manuelle d'organes mécaniques, — Relevés de valeurs d'état ou d'unités d'usage, — Test de lampes sur pupitre, — Purge d'éléments filtrants, — Contrôle d'encrassement des filtres.	— Remplacement des ampoules, — Opérations de serrurerie courantes sur caractérisation, racleurs, bavettes, frotteurs, — Ajustage, remplacement d'éléments d'usure ou détériorés, sur des éléments composants simples et accessibles.
2^{e} niveau de maintenance	
Actions qui nécessitent des procédures simples et/ou des équipements de soutien (intégrés au bien ou extérieurs) d'utilisation ou de mise en œuvre simple. Ce type d'actions de maintenance est effectué par un personnel qualifié avec les procédures détaillées et les équipements de soutien définis dans les instructions de maintenance.	

— Contrôle de paramètres sur équipements en fonctionnement, à l'aide de moyens de mesure intégrés au bien, — Réglages simples (alignement de poulies, alignement pompe-moteur, etc.), — Contrôle des organes de coupure (capteurs, disjoncteurs, fusibles), de sécurité, etc., — Détartrage de surface de ruissellement (tour aéroréfrigérante), — Graissage à faible périodicité (hebdomadaire, mensuelle), — Remplacement de filtres difficiles d'accès.	— Remplacement par échange standard de pièces : fusibles, courroies, filtres à air, etc., — Remplacement de tresses, de presse-étoupe, etc. — Lecture de logigrammes de dépannage pour remise en cycle, — Remplacement de composants individuels d'usure ou détériorés par échange standard (rail, glissière, galet, rouleaux, chaîne, fusible, courroie ...).
3^e niveau de maintenance	
Opérations qui nécessitent des procédures complexes et/ou des équipements de soutien portatifs, d'utilisation ou de mise en œuvre complexes. Ce type d'opération de maintenance peut être effectué par un technicien qualifié, à l'aide de procédures détaillées et des équipements de soutien prévus dans les instructions de maintenance.	

— Contrôle et réglages impliquant l'utilisation d'appareils de mesure externes aux biens, — Visite de maintenance préventive sur les équipements complexes, — Contrôle d'allumage et de combustion (chaudières), — Intervention de maintenance préventive intrusive, — Relevé de paramètres techniques d'état de biens à l'aide de mesures effectuées d'équipements de mesure individuels (prélèvement de fluides ou de matière...).	— Diagnostic, — Réparation d'une fuite de fluide frigorigène (groupe de froid), — Reprise de calorifuge, — Diagnostic d'état avec usage d'équipements de soutien portatifs et individuels (pocket automate, multimètre), — Remplacement d'organes et de composants par échange standard de technicité générale, sans usage de moyens de soutien communs ou spécialisés (carte automate, vérin, pompe, moteurs, engrenage, roulement...), — Dépannage de moyens de production par usage de moyens de mesure et de diagnostics individuels.

4^e niveau de maintenance	
Opérations dont les procédures impliquent la maîtrise d'une technique ou technologie particulière et/ou la mise en œuvre d'équipements de soutien spécialisés. Ce type d'opération de maintenance est effectué par un technicien ou une équipe spécialisée à l'aide de toutes instructions de maintenance générales ou particulières.	
— Révisions partielles ou générales ne nécessitant pas le démontage complet de la machine, — Analyse vibratoire, — Analyse des lubrifiants, — Thermographie infrarouge (installations électriques, mécanique, thermique...), — Relevé de paramètres techniques nécessitant des moyens de mesure collectifs (oscilloscope, collecteur de données vibratoires) avec analyse des données, — Révision d'une pompe en atelier, suite à dépose préventive	— Remplacement de clapets de compresseur — Remplacement de tête de câble en BTA, — Révision d'une pompe en atelier spécialisé suite à dépose préventive, — Réparation d'une pompe sur site, suite à une défaillance, — Dépannage de moyens de production par usage de moyens de mesure ou de diagnostics collectifs et/ou de forte complexité (valise de programmation automate, système de régulation et de contrôle des commandes numériques, variateurs...).

5^e niveau de maintenance	
Opérations dont les procédures impliquent un savoir-faire, faisant appel à des techniques ou technologies particulières, des processus et/ou des équipements de soutien industriels. Par définition, ce type d'opérations de maintenance (rénovation, reconstruction, etc.) est effectué par le constructeur ou par un service ou société spécialisée avec des équipements de soutien définis par le constructeur et donc proches de la fabrication du bien concerné.	
— Révisions générales avec le démontage complet de la machine, — Reprise dimensionnelle et géométrique, — Réparations importantes réalisées par le constructeur ou le reconditionnement de ses biens, — Remplacement de biens obsolètes ou en limite d'usure.	

V.3.2 Recommandations pour la conception d'une stratégie de maintenance

Pour la conception d'une stratégie de maintenance quelques recommandations sont proposées :

- **décomposition arborescente d'un bien :** une décomposition arborescente d'une part du bien et d'autre part de ses fonctions devra être réalisée en vue des actions de maintenance. Il appartient à chacun de définir selon ses besoins les différents niveaux de cette décomposition arborescente.
  Certaines professions peuvent développer, pour leur propre usage et en fonction de leurs spécificités, des guides standards ou des normes sectorielles facilitant cette décomposition.
- **description et codification d'un bien :** chaque site est décomposé en systèmes qui réalisent des fonctions. Un système est composé d'un ensemble de matériels ou d'équipements eux-mêmes décomposables. La désignation et la codification de ces matériels ou équipements sont à définir en préalable et sont la base de toute la gestion de la maintenance, de l'exploitation, de l'historique, de la documentation, de la gestion de stock, de la gestion économique, de la gestion du patrimoine, etc.
- **plan de maintenance :** chaque matériel ou équipement est constitué d'un certain nombre d'éléments pour lesquels sont définies des actions de maintenance préventive systématique ou préventive conditionnelle à réaliser. Il convient de prendre en considération, si elles existent, les recommandations des constructeurs, complétées des données de retour d'expérience du site ou d'autres sites utilisateurs de mêmes équipements.
- **échéancier :** les actions de maintenance préventive sélectionnées sont par la suite échelonnées dans le temps avec un échéancier en tenant compte de la charge du personnel (interne et externe) et des moyens techniques existants.
  Note : les actions de la maintenance corrective ne peuvent être programmées par anticipation. La survenue des défaillances des systèmes, par définition imprévisible, conditionnera les interventions des maintenanciers et la définition des opérations les plus appropriées pour la remise en bon état du système. Elles seront déterminées en fonction de la nature, des causes et des effets des anomalies constatées. Ces opérations seront enclenchées selon les urgences signalées avec les moyens disponibles.

— **réalisation suivant mode opératoire :** afin de garantir une qualité constante d'exécution des prestations en toute sécurité, la maintenance doit disposer de ressources nécessaires en termes de personnel (nombre, spécialisation et qualification) accompagnées d'outillage, de pièces de rechange et de manuel des instructions de maintenance explicitant l'objectif de l'opération, les procédures et les moyens à mettre en œuvre.
Ce manuel fait partie de la documentation de maintenance.

— **suivi et contrôle des travaux :** le suivi du déroulement des opérations nécessite la mise en œuvre d'un planning prenant en compte les contraintes liées à l'exploitation et les ressources disponibles, de tableaux de bord avec des indicateurs et de ratios pertinents indiquant le niveau de l'état d'avancement des travaux et constituent une aide à la prise de décisions. Ces tableaux de bord seront des outils.

V.4 Évaluation d'une stratégie de maintenance

Le développement de la maintenance s'effectue constamment grâce aux nombreux travaux de recherche réalisés à ce jour. Des méthodologies de plus en plus fiables sont proposées par exemple pour la modélisation de dégradations, de diagnostic, de pronostic et d'aide à la décision. Ce qui fait défaut actuellement c'est l'insuffisance de méthodes et d'outils d'évaluation de performances des orientations de maintenance pour la mise en œuvre industrielle de nouvelles stratégies de maintenance. Tel est le défi scientifique majeur lancé aux chercheurs du domaine.
Toute organisation de maintenance peut définir sa stratégie de maintenance selon trois critères principaux :

— assurer la disponibilité de l'ensemble des systèmes de production pour les fonctions requises, au coût optimum,

— tenir compte des exigences de sécurité relatives aux systèmes à la fois pour le personnel de maintenance et le personnel d'exploitation en tenant compte des conséquences sur l'environnement,

— améliorer la durabilité du système et/ou la qualité du produit ou du service fourni, au coût optimum.

V.4.1 Modèles de base d'une stratégie de maintenance

Chaque stratégie de maintenance adoptée, comprenant différentes actions de maintenance, a un impact sur le taux de défaillance (λ) du système. Il est défini comme étant la probabilité conditionnelle que l'équipement tombe en panne entre l'instant t et $t + \delta t$ sachant qu'il a survécu jusqu'à l'instant t. La variable est le "temps" et est considérée comme une unité d'usage, comme elle peut être une distance parcourue, un nombre de tours, un nombre de sollicitations.... Donc, l'évolution de la fonction d'intensité $\lambda(t)$ est déterminée par l'efficacité des opérations de maintenance.
Ainsi, en raison de l'impact des opérations de maintenance sélectionnées, les stratégies de maintenance peuvent être classées en trois catégories :

— Minimale : le modèle de maintenance minimale suppose que l'effet de la maintenance est de remettre le système en fonctionnement dans l'état exact où il était juste avant la défaillance. Cela caractérise un effet de maintenance neutre (n'améliore pas et ne dégrade pas le système). Le système après maintenance est dit aussi mauvais que vieux et cet état est connu dans la littérature par "As Bad As Old " (ABAO).

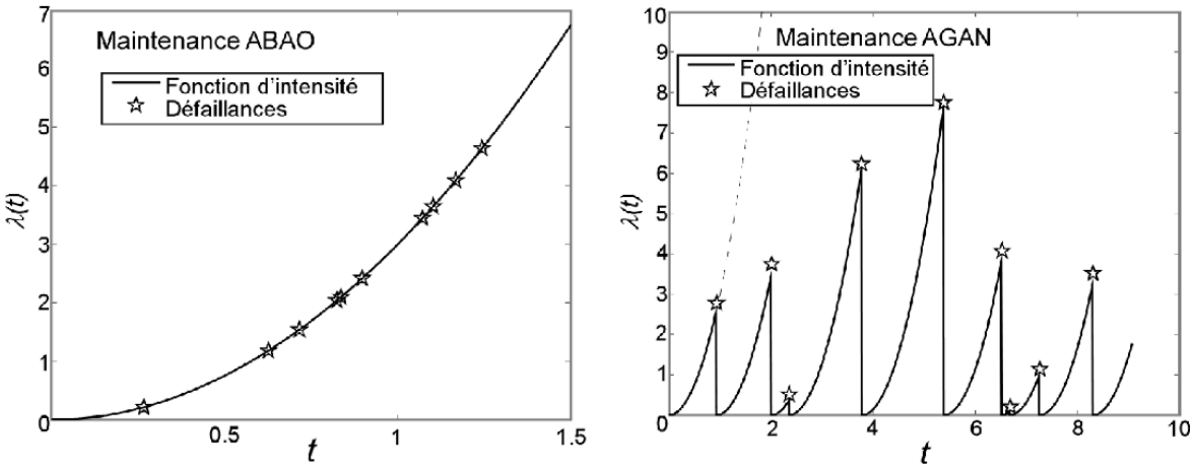
  L'intensité de défaillance est alors une fonction uniquement du temps et ne dépend donc pas du passé du processus.

  La figure V.2a illustre cette propriété et représente l'intensité de défaillance d'un système pour des maintenances ABAO. Les étoiles sur l'axe des abscisses symbolisent les instants de défaillance.

  Barlow and Proschan [151] ont été les premiers à étudier ce type de maintenance. Après une action de maintenance minimale, le taux de défaillance reste inchangé. De ce fait, ce type de maintenance minimale n'est utilisé que pour modéliser des actions de maintenance correctives.

— la maintenance parfaite : si la maintenance remet le système dans un état aussi bon que neuf " As Good As New " (AGAN). En théorie, les durées de vie et la fonction du taux de défaillance sont les mêmes que celles d'un système neuf.

  La figure V.2b représente une trajectoire de l'intensité de défaillance d'un système pour des maintenances AGAN. Les instants de défaillance sont les instants de saut de l'intensité. Après une maintenance, l'intensité repart de zéro parallèlement à la courbe d'intensité initiale.



(a) maintenance ABAO (b) maintenance AGAN

FIGURE V.2: Fonction d'intensité pour une maintenance ABAO et AGAN

Ce type de problème, a fait l'objet de nombreux développements ultérieurs incluant diverses variantes.

— la maintenance imparfaite : est apparue pour modéliser un état intermédiaire [152]. En pratique, la maintenance imparfaite est située entre la maintenance parfaite (AGAN) et la maintenance minimale (ABAO). Effectivement, il est techniquement invraisemblable qu'une maintenance remette un système industriel en exploitation à l'état neuf, mais il est très probable que l'état obtenu soit meilleur que celui d'avant ayant entrainé sa détérioration. Plusieurs causes peuvent être à l'origine d'une action de maintenance imparfaite comme par exemple :

  — un changement partiel des composants du même système,

  — une intervention non préparée (procédures de maintenance, personnel non qualifié ...) peut réduire l'efficacité de l'intervention des opérateurs et la réparation ne sera qu'approximative,

  — une utilisation des pièces de rechange non appropriées,

  — etc ...

-

V.4.2 Catégorisation des modèles d'évaluation des stratégies de maintenance

Ces trois modèles de stratégie de maintenance sont des modèles de base. En effet, l'évaluation des stratégies de maintenance a fait l'objet de divers travaux de recherche parmi lesquels on peut citer [153, 154, 155]. Beaucoup de travaux de recherche ont porté sur la modélisation de la maintenance dans le but de minimiser les coûts de maintenance et maximiser la durée de bon fonctionnement des systèmes de production.
La figure V.3 résume les différentes politiques de maintenance et ses facteurs d'influence sur le choix d'une stratégie de maintenance.

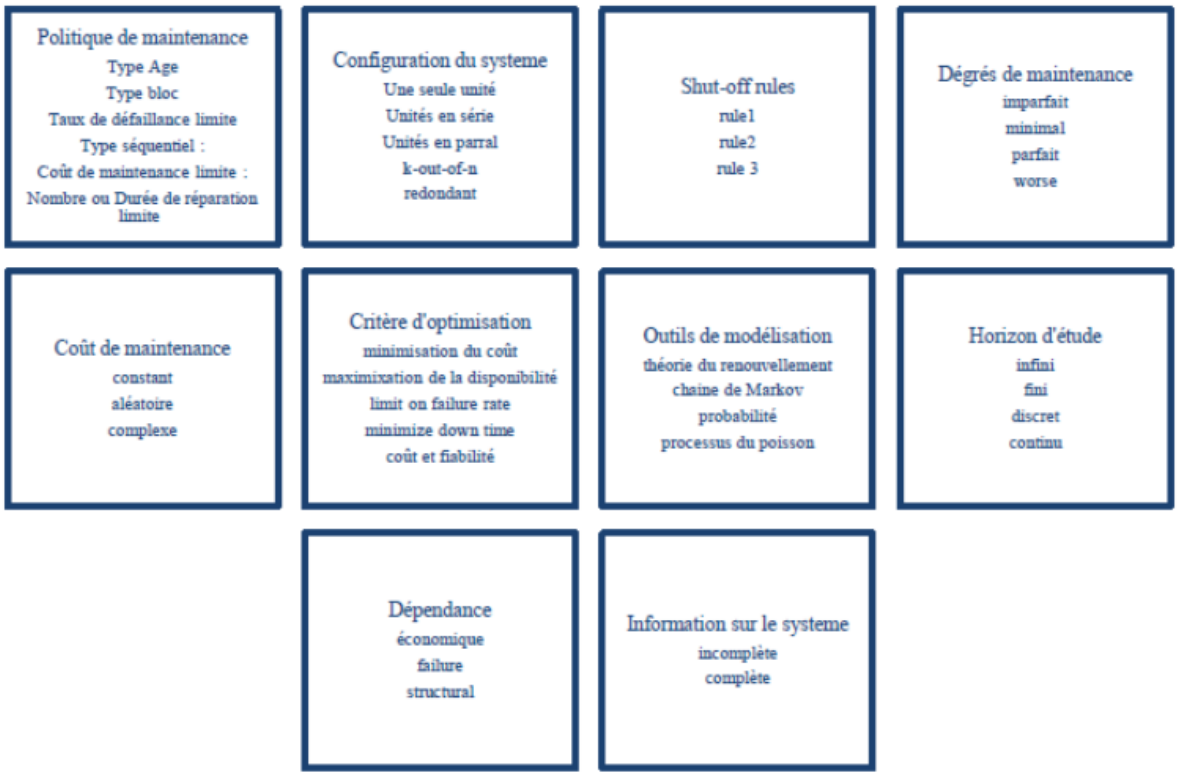


FIGURE V.3: Politique de maintenance et ses facteurs d'influence

D'une manière générale, les méthodes présentées dans la littérature peuvent être classées en trois catégories : les méthodes basées sur une réduction du taux de défaillance, les méthodes basées sur une réduction arithmétique d'âge et les modèles hybrides qui représentent une combinaison entre les deux méthodes précédemment citées.
Dans la catégorie méthodes basées sur une réduction du taux de défaillance, les modèles proposés [155] suggèrent que l'action de maintenance préventive n'est effectuée que

lorsque le taux de panne atteint une limite prédéterminée et en cas de panne, des actions de réparations seront effectuées. Les auteurs [156] ont proposé un modèle de maintenance où des actions de maintenance préventive sont effectuées quand le système atteint la limite prédéterminée et en cas de panne des actions de réparation seront effectuées. Il existe d'autres travaux traitant le problème de stratégies de maintenance basées sur la limitation du taux de défaillance. On peut citer, à titre d'exemple, [157, 158, 159, 160]. D'autres travaux et plus de détails peuvent être trouvés dans la revue de littérature de [155].

V.5 Conclusion

D'une manière générale, une stratégie de maintenance doit permettre d'une part de maximiser la disponibilité et la fiabilité (pour produire la quantité désirée de produits, avec les spécifications de qualité requises, dans les meilleurs délais, par exemple) et d'autre part d'atteindre une certaine efficacité en termes de coût dans tout le cycle de vie du système.

Nombres de stratégies de maintenance ont été développées pour différentes industries manufacturières au cours des dernières décennies. Il est donc difficile d'identifier une stratégie optimale universelle qui est réellement appropriée pour la maintenance d'un système.

Entre l'état de marche parfaite et l'état de panne totale, les systèmes industriels présentent généralement un grand nombre d'états dégradés qui continuent à assurer un service, même si celui-ci n'est pas égal à 100 %. " Ces états dégradés sont donc à prendre en compte pour évaluer correctement le niveau de service des systèmes industriels et cela est plus particulièrement vrai en ce qui concerne les systèmes de production ".

Ainsi, dans ce chapitre nous avons présenté un aperçu d'une recherche bibliographique sur les concepts fondamentaux, les critères à considérer pour la conception et l'évaluation d'une stratégie de maintenance. Ensuite, il a été constaté que parmi les outils mathématiques de modélisation de l'impact des actions de maintenance existants, les Modèles de Markov Cachés (MMC) s'y prêtent facilement à l'analyse des risques des systèmes dynamiques et à la modélisation des phénomènes aléatoires ce qui est le cas des dégradations des systèmes mécatroniques.

Chapitre VI

Conclusion générale

Les systèmes mécatroniques sont utilisés dans de nombreuses applications, aussi bien dans les domaines militaires, l'avionique, spatial, l'automobile, que dans celui du nucléaire. Ce sont des systèmes dynamiques hybrides car ils combinent dans leur structure des technologies mécaniques, hydrauliques, électroniques et informatiques. La dynamique continue est associée à la partie énergétique et la dynamique discrète est liée à la commande numérique et à l'existence d'événements discrets (défaillances, dépassements de seuils). La flexibilité matérielle de ces systèmes a permis au concepteur de rajouter progressivement des composants électroniques pour assurer de nouvelles fonctions, ce qui les rend de plus en plus complexes et pose des problèmes de sûreté de fonctionnement. L'analyse des risques de ces systémes est rendue difficile.

Les travaux développés durant cette thèse nous ont permis de contribuer à l'analyse des risques des systèmes mécatroniques, plus particulièrement à la recherche des scénarios critiques et à l'estimation de leurs probabilité d'occurrence. La nature dynamique et hybride des systèmes mécatroniques nous a conduit au choix d'une modélisation à l'aide des réseaux de Petri et d'équations algébro-différentielles. Pour cela, nous avons repris l'approche développée par Ronan Champagnat [135] et compléter par Sarhane Khalfaoui[51]. Le modèle RdP 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.Aussi, à travers un exemple nous avons monté comment le modèle choisi peut être utilisé en orienté objet pour plus de flexibilité quand il s'agit d'un système industriel imposant.

Cependant, les outils d'analyse dont disposent les RdP sont limités dans l'interprétation du modèle pour expliquer les phénomènes indésirables. La contrainte majeure est la dif-

ficulté (ou l'impossibilité) de différencier entre les relations de cause et de précédence à partir du graphe des marquages. La connaissance de ces relations est primordiale car elle favorise largement la compréhension et l'analyse des risques industriels rencontrés. Pour extraire donc les scénarios critiques, nous nous sommes appuyés sur la logique linéaire afin d'exploiter les relations de cause à effet présentes dans le modèle. Nous avons choisi d'utiliser la logique Linéaire à cause de l'équivalence entre accessibilité dans un réseau de Petri et prouvabilité dans cette logique. Où l'idée est de substituer le graphe des marquages en introduisant dans une démarche analytique, des connecteurs et des règles empruntés de la logique linéaire mais adaptés à notre démarche.Ainsi, profitant de l'association intelligente des modèles des RdP et de la LL, il a été possible de concevoir un algorithme original permettant l'extraction optimale des scénarios critiques. L'un des principaux avantages de l'algorithme proposé est son efficacité dans la sélection et le traitement des seules séquences du modèle ayant effectivement une influence sur l'avènement des situations critiques. Ce qui réduit fortement le nombre de cas à examiner.
L'algorithme comporte 3 étapes incluant deux sub algorithmes itératifs dédiés à l'extraction des transitions et des scénarios critiques en recourant à la prospection et l'isolation des seules séquences utiles dans l'analyse.D'abord, l'algorithme extrait du RdP seulement les transitions menant au marquage critique évitant le traitement de tout le réseau.Ensuite,il consiste en l'application des règles de franchissement pour déterminer l'ordre de passage des transitions, justifiant les relations existantes entre les événements conduisant au scénario critique.
Une fois l'extraction des scénarios critiques faite, nous avons poursuivi le travail pour l'estimation de la probabilité d'occurrence de chaque scénario. L'idée était d'associer un RdP et une simulation Monte Carlo qui a montré son efficacité dans des travaux précédents. Cependant, afin d'éviter des temps de calcul important nous avons pensé à effectuer une simulation par sauts. L'originalité de cette estimation consiste en ce qu'elle est basée sur ces scénarios, préalablement identifiés, ce qui évite donc d'effectuer une simulation globale basée sur tout le réseau de Petri. En effet, nous avons pu optimiser la simulation Monte Carlo en forçant les histoires tirées au sort à suivre ces scénarios pré-identifiés. Cette idée a été appliquée sur le système étudié et a donné des résultats satisfaisants en comparaison avec la simulation classique cad du modèle globale.
Avant de penser à utiliser l'algorithme de recherche de scénario dans un contexte industriel, il reste du travail à faire. Le premier travail va consister à le mettre en oeuvre sous la forme d'un logiciel afin de pouvoir traiter des exemples plus conséquents.Pour

ce faire, il sera de toute façon nécessaire de mettre en œuvre une approche de modélisation structurée et modulaire, comme présentée au chapitre 3. Ce n'est qu'ainsi que nous pourrons éclaircir des points restés encore imprécis dans l'algorithme. Ces systèmes vont également nous poser des problèmes de modélisation. En effet, un même système peut être modélisé de diverses façons avec des réseaux de Petri Prédicats Transitions Différentiels et Stochastiques.Il est clair que seuls les scénarios induits par le modèle sont trouvés et que l'exhaustivité par rapport au système réel dépend de la modélisation qui reste et restera longtemps un problème ouvert.

Depuis plus de 30 ans, les réseaux de Petri se sont avérés très puissants pour effectuer des études et développer de nouvelles approches liées à la sécurité / fiabilité. Néanmoins, la diffusion est lente et les RdP ne sont pas encore couramment utilisés par les ingénieurs de fiabilité. En fait, les RdP actuels sont souvent complexes et difficiles à comprendre même si, en réalité, ils modélisent les systèmes très simplement. C'est décourageant à la fois pour les concepteurs et les lecteurs des RdP.La tendance actuelle est de mettre en œuvre des démarches et outils afin de réaliser une modélisation par RdP des grands systèmes industriels tout en gardant la lisibilité et la compréhensibilité tout au long du processus de construction.

Bibliographie

[1] Demri, A. *ontribution a l'évaluation de la fiabilite d'un systeme mecatronique par modelisation fonctionnelle et dysfonctionnelle.* Ph.D. thesis, Ecole doctorale d'Angers (2009).

[2] Forsberg, K. & Mooz, H. Application of the vee to incremental and evolutionary development. *Proceedings of the Fifth Annual International Symposium of the National Council on Systems Engineering, St. Louis, MO* (1995).

[3] Guillerm, R. *Intégration de la Sûretè de fonctionnement dans les Processus d'Ingènierie Systéme* . Ph.D. thesis, Université de Toulouse (2011).

[4] Mihlech, A. *Modélisation et évaluation de la fiabilité des systémes mécatroniques : application sur systéme embarqué.* Ph.D. thesis, École doctorale d'Angers,France (2007).

[5] AFIS. Ingenierie systeme. pourquoi comment. Tech. Rep., association française d'ingenierie systeme (2016).

[6] IEEEP1220. standard for system engineering-a commercial standard for improving competitiveness. Tech. Rep., Digital Avionics Systems Conference (1993).

[7] EIA-632. Processes for engineering a system. Tech. Rep., ELECTRONIC INDUSTRIES ALLIANCE (2003).

[8] ISO15288. Systems and software engineering - system life cycle processes. Tech. Rep., ISO Software and systems engineering (2015).

[9] villmeur, A. *Sûreté de fonctionnement des systémes industriels : fiabilité - facteurs humains - informatisation* (Eyrolles, 1988).

[10] Mihalache, A. *Modelisation et evaluation de la fiabilite des systemes mecatroniques : Application sur systemes embarque.* Ph.D. thesis, Universite d'Angers (2007).

[11] ISO/IEC51. Safety aspects – guidelines for their inclusion in standards. Tech. Rep., ISO Committee on consumer policy (2014).

[12] EN50126-1. Railway applications - the specification and demonstration of reliability, availability, maintainability and safety (rams) - part 1 : Generic rams process. Tech. Rep., British Standards Institution (2017).

[13] BSI/OHSAS18001. Occupational health and safety management systems- specification. Tech. Rep. (2005).

[14] Framer, F. Siting criteria : a new approach . *Atom* **128**, 152–166 (1967).

[15] Vesely, W., Goldberg, F., Roberts, N. & Haasl, D. *Fault Tree Handbook*, vol. NUREG-0492 (U.S Nuclear Regulatory Commission, 1981).

[16] M.Rausand. Risk Assessment : Theory, Methods, and Applications. *Wiley, New Jersey* (2011).

[17] E.Ruijters & M.Stoelinga. Fault tree analysis : a survey of the state of the art in modeling, analysis and tools. *Computer science Review* **15**, 29–62 (2015).

[18] S.Kabir. An overview of fault tree analysis and its application in model based dependability analysis. *Expert Systems With Applications* **77**, 114–135 (2017).

[19] Birnbaum, Z., Esary, J. & Saunders, S. Multi-component systems and structures and their reliability. *Technometrics* **3**, 55–77 (1961).

[20] Rauzy, A. Mathematical foundations of minimal cutsets. *IEEE Transactions on Reliability.* **50**, 389–396 (2001).

[21] Dutuit, Y. & Rauzy, A. Efficient algorithms to assess component and gate importance in fault tree analysis. *Reliability Engineering and System Safety* **72**, 213–222 (2001).

[22] Dutuit, Y. & Rauzy, A. Approximate estimation of system reliability via fault trees. *Reliability Engineering and System Safety* **87**, 163–172 (2005).

[23] Rauzy, A. & Dutuit, Y. Exact and truncated computations of prime implicants of coherent and non-coherent fault trees within Aralia. *Reliability Engineering and System Safety* **58**, 127–144 (1997).

[24] Deng, Y., Wang, H. & Guo, B. Bdd algorithms based on modularization for fault tree analysis. *Progress in Nuclear Energy* **85**, 192 – 199 (2015). URL `http://www.sciencedirect.com/science/article/pii/S014919701530024X`.

[25] Minato, S. Zero-suppressed bdds for set manipulation in combinatorial problems. *30th Conference on Design Automation,Dallas (USA)* (1993).

[26] Minato, S. Zero-suppressed BDDs and their applications. *International Journal on Software Tools for Technology Transfer* **3**, 156–170 (2001).

[27] Tang, Z. & Dugan, J. Minimal cut set/Sequence generation for dynamic fault trees. *Annual Symposium of Reliability and Maintainability,Los Angeles (USA)* 207–213 (2004).

[28] Moncelet, G. *Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systémes mécatroniques du monde automobile.* Ph.D. thesis, Université Paul Sabatier, Toulouse (1998).

[29] Dugan, J., Bavuso, S. & Boyd, M. Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Trans on Reliability* **41**, 363–377 (1992).

[30] Dugan, J., Sullivan, K. & Coppit, D. Developing a low-cost highquality software tool for dynamic fault-tree analysis. *IEEE Transactions on Reliability* **49**, 49–59 (2000).

[31] Merle, G., Roussel, J., Lesage, J. & Bobbio, A. Probabilistic algebraic analysis of fault trees with priority dynamic gates and repeated events. *IEEE Transactions on Reliability* **59**, 250–261 (2010).

[32] Merle, G., Roussel, J. & Lesage, J. Algebraic determination of the structure function of dynamic fault trees. *Reliability Engineering and System Safety* **96**, 267–277 (2011).

[33] Chaux, P. *Formalisation de la cohérence et calcul des séquences de coupe minimales pour les systémes binaires dynamiques réparables.* Ph.D. thesis, École normale supérieure de Cachan (2013).

[34] Bryant, R. Graph based algorithms for boolean function manipulation. *ieee transaction on computers* **35**, 677–691 (1986).

[35] Dugan, J., Sullivan, K. & Bechta, J. Fault trees and Markov models for reliability analysis of fault-tolerant digital systems. *Reliability Engineering and System Safety* **39**, 291–307 (1993).

[36] Coppit, D., Sullivan, K. & Dugan, J. Formal semantics of models for computational engineering : a casestudy on dynamic fault trees. *11th International Symposium on Software Reliability Engineering, San Jose (USA)* 270–282 (2000).

[37] Bobbio, A. & Raiteri, D. Parametric fault trees with dynamic gates and repair boxes. *Annual Symposium of Reliability and Maintainability (USA)* **3**, 459–465 (2004).

[38] Rao, K. *et al.* Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. *Reliability Engineering and System Safety* **94**, 872–883 (2009).

[39] F.Flammini. *Model-based dependability evaluation of complex critical control systems.* Ph.D. thesis, Dipartimento di Informatica e Sistemistica (2006).

[40] Bouissou, M. & Bon, J. A new formalism that combines advantages of fault trees and markov models : Boolean logic driven markov processes. *Reliability Engineering and System Safety* **82**, 149–163 (2003).

[41] Bouissou, M. *Gestion de la complexite dans les etudes quantitatives de surete de fonctionnement de systemes* (Editions Lavoisier, 2008).

[42] Bouissou, M., Bouhadana, H., Bannelier, M. & Villatte, N. Knowledge modelling and reliability processing : Presentation of the FIGARO language and associated tools. *IFAC/IFIP/EWICS/SRE Symposium,Trondheim (Norvege)* 69–75 (1991).

[43] Bouissou, M. The figaro dependability evaluation workbench in use : Case studies for fault-tolerant computer systems. In *FTCS-23 The Twenty-Third International Symposium on Fault-Tolerant Computing*, 680–685 (1993).

[44] Bouissou, M. Automated dependability analysis of complex systems with the kb3 workbench : the experience of edf r&d (2005).

[45] Garret, C., Guarro, S. & Apostolakis, G. Development of a methodology for assessing the safety of embedded software systems (1993).

[46] Al-Dabbagh, W. & Lixuan, L. Reliability modeling of networked control systems using dynamic flowgraph methodology. *Reliability Engineering and System Safety* **95**, 1202–1209 (2010).

[47] Labeau, P., Smidts, C. & Swaminathan, S. Dynamic reliability : towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety* **68**, 213–254 (2000).

[48] Yau, M., Guarro, S. & Apostolakis, G. Demonstration of the Dynamic Flowgraph Methodology using the Titan II Space Launch Vehicle Digital Flight Control System. *Reliability Engineering and System Safety* **49**, 335–353 (1995).

[49] Aldemir, T. *et al.* probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies. *reliability engineering and system safety* **95**, 1011–1039 (2010).

[50] Yau, M., Dixon, S. & Guarro, S. Application of the dynamic flowgraph methodology to the space propulsion system benchmark problem. *PSAM 2014 - Probabilistic Safety Assessment and Management* (2014).

[51] Khalfaoui, S. *Modélisation et validation par simulation des systémes hybrides.* Ph.D. thesis, Rapport de DEA, INP-ENSEEIHT (2000).

[52] Bondavalli, A., M Dal Ci and, D. L. & Pataricza, A. High-level Integrated Design Environment for dependability (HIDE). *the 5th International Workshop on Object-Oriented Real-Time Dependable Systems,Guadalajara, Mexico* 87–92 (1999).

[53] Bondavalli, A. *et al.* Dependability analysis in the early phases of UML-based system design. *International Journal of Computer Systems Science and Engineering* **16**, 265–275 (2001).

[54] Bondavalli, A., Majzik, I. & Mura, I. Automated dependability analysis of uml designs. *Proceedings of the 2nd IEEE International Symposium on Object oriented Real time distributed Computing Saint Malo France* (1999).

[55] Zarras, A. & Isarny, V. A UML Based Framework for Assessing the Reliability of Software Systems. *the 1st ICSE workshop on describing software architecture with UML toronto* 36–40 (2001).

[56] Bernardi, S., Donatelli, S. & Merseguer, J. From UML Sequence Diagrams and StateCharts to analyzable Petri Net models. *the 3rd Int workshop on software on performance,Rome, Italy* (2002).

[57] Merseguer, J., Campos, J., Bernardi, S. & Donatelli, S. A Compositional Semantics for UML State Machines Aimed at Performance Evaluation. *the 6th Int Workshop on Discrete Event Systems, Zaragoza, Spain* (2002).

[58] JP Lopez Grao and J Merseguer and J Campos. From uml activity diagrams to stochastic petri nets application to software performance engineering. *Proceedings of the fourth Int workshop on software and performance Redwood shores, USA* (2004).

[59] Pai, G. & Dugan, J. Automatic Synthesis of Dynamic Fault Trees from UML System Models. *the 13th International Symposium on Software Reliability Engineering, Annapolis, USA* 243–254 (2002).

[60] Leangsukun, C., Song, H. & Shen, L. Reliability modeling using UML. *the International conference on software engineering research and practice, Las Vegas, USA* (2003).

[61] Iwu, F., Galloway, A., McDermid, J. & Toyn, I. Integrating safety and formal analyses using UML and PFS. *Reliability engineering and system safety* **92**, 156–170 (2007).

[62] Gilmore, S. & Kloul, L. A unified tool for performance modelling and prediction. *Reliability engineering and system safety* **89**, 17–32 (2005).

[63] Pap, Z., Majzik, I., Pataricza, A. & Szegi, A. Methods of checking general safety criteria in UML StateChart specifications. *Reliability engineering and system safety* **87**, 89–107 (2005).

[64] David, P. *Contribution á l'analyse de sûreté de fonctionnement des systémes complexes en phase de conception : application á l'évaluation des missions d'un réseau de capteurs de présence humaine.* Ph.D. thesis, Université d'Orléans (2009).

[65] OMG. OMG Systems Modeling Language (OMG SysML), Version 1.5 (2017). URL `http://www.omg.org/spec/SysML/1.5/`.

[66] Xiang, J., Yanoo, K., Maeno, Y. & Tadano, K. Automatic synthesis of static fault trees from system models. In *2011 Fifth International Conference on Secure Software Integration and Reliability Improvement*, 127–136 (2011).

[67] Prosvirnova, T. & Rauzy, A. Guarded transition system : pivot modelling formalism for safety analysis. *18eme congress de maitrise des risques et sûreté de fonctionnement, Tours, France* (2012).

[68] Point, G. & Rauzy, A. AltaRica : Constraint automata as a description language. *Journal Européen des Systémes Automatisés* **33**, 1033–1052 (1999).

[69] Arnold, A., Griffault, A., Point, G. & Rauzy, A. The altarica language for describing concurrent systems. *Fundamenta Informaticae* **34**, 109–124 (2000).

[70] Griffault, A., Point, G., Kuntz, F. & Vincent, A. Symbolic computation of minimal cuts for AltaRica models. Tech. Rep. (2011). URL `https://hal.archives-ouvertes.fr/hal-00634022`. 65 pages.

[71] Rauzy, A. Mode automata and their compilation into fault trees. *Reliability Engineering and System Safety* **78**, 1–12 (2002).

[72] Boiteau, M., Dutuit, Y., Rauzy, A. & Signoret, J. the AltaRica Data-Flow Language in Use : Assessment of Production Availability of a MultiStates System. *Reliability Engineering and System Safety* **91**, 747–755 (2006).

[73] Rauzy, A. An experimental study on iterative methods to compute transient solutions of large Markov models. *Reliability Engineering and System Safety* **86**, 105–115 (2004).

[74] Khuu, M. *Contribution á l'accélération de la simulation stochastique sur des modèles AltaRica Data-Flow.* Ph.D. thesis, Université de la Méditerranée (Aix-Marseille II) (2008).

[75] Prosvirnova, T. *AltaRica 3.0 : une approche orientée modèles pour la Sûreté de Fonctionnement.* Ph.D. thesis, École polytechnique, université paris saclay (2014).

[76] Rauzy, A. Guarded Transition Systems : a new States/Events Formalism for Reliability Studies. *Reliability Engineering and System Safety* **222**, 495–505 (2008).

[77] Pagetti, C. *Extension temps réel du langage AltaRica.* Ph.D. thesis, École Centrale de Nantes et de Université de Nantes (2004).

[78] Kehren, C. *Motifs formels d'architectures de systémes pour la sûreté de fonctionnement.* Ph.D. thesis, École Nationale Supérieure de l'aéronautique et de l'Espace (2005).

[79] Humbert, S. *Déclinaison d'exigences de sécurité, du niveau système vers le niveau logiciel, assistée par des modèles formels.* Ph.D. thesis, Université de Bordeaux I (2008).

[80] Sagaspe, L. *Allocation sûre dans les systémes aéronautiques : modèlisation, vérification et génération.* Ph.D. thesis, Université de Bordeaux (2008).

[81] Bernard, R. *Analyse de Sécurité multi systémes.* Ph.D. thesis, Université de Bordeaux (2009).

[82] A.Albore, Zilio, S., G.Infantes, C.Seguin & P.Virelizier. A model-checking approach to analyse temporal failure propagation with altarica 147–162 (2017).

[83] SAE-AS5506. SAE Architecture Analysis and Design Language (AADL). *International Society of Automotive Engineers* (2004).

[84] Feiler, P., Gluch, D., Hudak, J. & Lewis, B. Pattern-based analysis of an embedded real-time system architecture. *18th IFIP World Computer Congress, ADL Workshop, (Toulouse, France)* (2004).

[85] Hugues, J., Kordon, F., Pautet, L. & Vergnaud, T. *"A Factory To Design and Build Tailorable and Verifiable Middleware",in Workshop on Neworked Systems : Realization of Reliable Systems on Top of Unreliable Networked Platforms*, 123–144 (2007).

[86] Farines, J. *et al.* The cotre project : rigorous software development for real time systems in avionics. *27th IFAC/IFIP/IEEE Workshop on Real Time Programming, Zielona Gora(Poland)* (2003).

[87] Singhoff, F., Legrand, J., Nana, L. & Marc, L. Scheduling and memory requirements analysis with aadl. *SIGAda Int. Conf. on Ada, Atlanta (USA)* (2005).

[88] Sokolsky, O., Lee, I. & Clarke, D. Scedulability analysis of aadl models. *20th Parallel and Distributed Processing Symposium, Rhodes Island (Greece)* (2006).

[89] Joshi, A., Vestal, S. & Binns, P. Automatic generation of static fault trees. *Workshop on Architecting Dependable Systems of The 37th Annual IEEE/IFIP Int. Conference on Dependable Systems and Networks, Edinburgh (UK)* (2007).

[90] Rugina, A. *Dependability modeling and evaluation :From AADL to stochastic Petri nets.* Ph.D. thesis, l'Institut National Polytechnique de Toulouse (2007).

[91] Rugina, A., Feiler, P., Kanoun, K. & Kaâniche, M. "software dependability modeling using an industry-standard architecture description language",Research Report,LAAS CNRS (2006).

[92] Rugina, A., Feiler, P., Kanoun, K. & Kaâniche, M. An architecture-based dependability modeling framework using aadl. *10th IASTED Int. Conf. on Software Engineering and Applications, Dallas (USA)* (2006).

[93] Rugina, A., Feiler, P., Kanoun, K. & Kaâniche, M. Modélisation de la sûreté de fonctionnement à partir du langage AADL. *15éme Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lille (France)* (2006).

[94] A.Rugina, K.Kanoun & Kaâniche, M. The ADAPT tool : From AADL architectural models to stochastic petri nets through model transformation. *CoRR* (2008). URL `http://arxiv.org/abs/0809.4108`.

[95] Bozzano, M. *et al.* Safety, dependability and performance analysis of extended aadl models. *Comput. J.* **54**, 754–775 (2011). URL `http://dx.doi.org/10.1093/comjnl/bxq024`.

[96] Bozzano, M. & Papadopoulos, Y. *Model-Based Safety and Assessment : 5th International Symposium, IMBSA 2017, Trento, Italy, September 11–13, 2017, Proceedings* (2017).

[97] Howard, R. A. *Dynamic Programming and Markov Processes* (MIT Press, Cambridge, MA, 1960).

[98] Yang, J. & Aldemir, T. An algorithm for the computationally efficient deductive implementation of the markov/cell-to-cell-mapping technique for risk significant scenario identification. *Reliability Engineering and System Safety* **145**, 1 – 8 (2016). URL `http://www.sciencedirect.com/science/article/pii/S0951832015002550`.

[99] Tombuyses, B. & Aldemir, T. Computational efficiency of the continuous cell-to-cell mapping technique as a function of integration schemes. *Reliability Engineering and System Safety* **58**, 215 – 223 (1997). URL `http://www.sciencedirect.com/science/article/pii/S0951832097000756`.

[100] Aldemir, T. *et al.* Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies. *Reliability Engineering and System Safety* **95**, 1011 – 1039 (2010). URL `http://www.sciencedirect.com/science/article/pii/S0951832010000967`.

[101] Schoenig, R. *Définition d'une méthodologie de conception des systémes mécatroniques surs de fonctionnement.* Ph.D. thesis, Institut National Polytechnique de Lorraine (2004).

[102] Schoenig, R., Aubry, J., Cambois, T. & Hutinet, T. An aggregation method of markov graphs for the reliability analysis of hybrid systems. *International Journal on Reliability Engineering and System Safety RESS* **91**, 137–148 (2006).

[103] Hopcroft, J. E., Motwani, R. & Ullman, J. D. *Introduction to Automata Theory, Languages, and Computation (3rd Edition)* (Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2006).

[104] Alur, R. *et al.* The algorithmic analysis of hybrid systems. *Theoretical Computer Science* **138**, 3–34 (1995).

[105] Perez, C. *Évaluation par simulation de la sûreté de fonctionnement de systémes en contexte dynamique hybride.* Ph.D. thesis, Institut National Polytechnique de Lorraine-INPL (2009).

[106] Castaneda, G. P., Aubry, J. & Brinzei, N. Modélisation et simulation d'un systéme dynamique hybride pour calculer sa fiabilité dynamique en utilisant le toolbox scicos de scilab. *7éme édition du Congrés International pluridisciplinaire Qualita Tanger (Maroc)* 311–318 (2007).

[107] Aubry, J. *et al.* Approches de la fiabilité dynamique pour modéliser des systémes critiques. *Rapport final du projet APPRODYN* (2012).

[108] Chraibi, H. Dynamic reliability modeling and assessment with pycatshoo : Application to a test case. *In PSAM Topical Conference,Tokyo(Japan)* (2013).

[109] David, R. & Alla, H. *Discrete, Continuous, and Hybrid Petri Nets* (Springer, Berlin, 2010), 2 edn.

[110] Murata, T. Petri nets : Properties, analysis and applications. *Proceedings of the IEEE* **77**, 541–580 (1989).

[111] Petrii, C. *Kommumkatio n mit Automates* (1992).

[112] 62551, I. Analysis techniques for dependability-petri net techniques. Tech. Rep. (2012).

[113] Dutuit, Y., Châtelet, E., Signoret, J. & Thomas, P. Dependability modelling and evaluation by using stochastic Petri nets : application to two test cases. *Reliab Eng Syst Saf 1997* **55**, 117–124 (1997).

[114] 61508-6, I. Functional safety of electrical,electronic,programmable electronic safety related systems. Tech. Rep., the International Standards for electrical, electronic and programmable electronic safety related systems (2013).

[115] Signoret, J. Dependability and safety modeling and calculation : Petri nets . *2nd IFAC Workshop on Dependable Control of Discrete Systems DCDS'09 Bari, Italy* 203–208 (2009).

[116] P Škňouřilová and R Briš. Coloured Petri nets and a dynamic reliability problem. *Proc Inst Mech Eng Part O J Risk Reliab* **222**, 635–642 (2008).

[117] Marseguerra, M. & Zio, E. Monte carlo approach to psa for dynamic process systems. *Reliability Engng and Saf. System* **52**, 227–241 (1996).

[118] Simeu-Abazi, Z., Lefebvre, A. & Derain, J.-P. A methodology of alarm filtering using dynamic fault tree. *Reliability Engineering and System Safety* **96**, 257 – 266 (2011). URL `http://www.sciencedirect.com/science/article/pii/S0951832010002085`.

[119] Vernez, D., Buchs, D. & Pierrehumbert, G. Perspectives in the use of colored petri nets for the risk analysis and accident modelling. *Safety science* **41**, 445–463 (2003).

[120] Demmou, H., Khalfaoui, S., Guilhem, E. & Valette, R. Critical scenarios derivation methodology for mechatronic systems. *Reliab Eng Syst Saf* **84**, 33–44 (2004).

[121] Sadou, N. & Demmou, H. Reliability analysis of discrete event dynamic systems with petri nets. *Reliab Eng Syst Saf* **94**, 1848–1861 (2009).

[122] Girard, J. Linear logic. *Theor Comput Sci* **50** (1987).

[123] Girault, F. *Formalisation en Logique Linéaire du fonctionnement des réseaux de Petri.* Ph.D. thesis, université de Toulouse (1997).

[124] H Lykins and S Friedenthal and A Meilich. dapting uml for an objectoriented systems engineering method (oosem). *Proceedings of the 10th annual INCOSE symposium* (2000).

[125] Muller, P. *Modelisation objet avec UML* (Edition Eyrolles, 1997).

[126] Gabay, J. *UML2 analyse et conception* (Edition DUNOD, 2008).

[127] Clark, T. *Object Modeling with the OCL* (Springer, 2002).

[128] Faucher, J. *pratique de l'AMDEC* (Edition DUNOD, 2004).

[129] Zaytoon, J. *Systemes dynamiques hybrides* (Hermes Science, 2001).

[130] Karnopp, D., Rosenberg, R. & S. Perelson, A. System dynamics : A unified approach. *Systems, Man and Cybernetics, IEEE Transactions on* **6**, 724–724 (1976).

[131] Rosenberg, R. & Karnopp, D. introduction to physical system dynamics. *McGraw-Hill,Londres,New York* (1983).

[132] Gueguen, H. & Lefebvre, M. A comparison of mixed specification formalisms. *Journal Européen des Systémes Automatisés* **34**, 381–394 (2001).

[133] Andreu, D. *Commande et supervision des procédés discontinus.* Ph.D. thesis, Laboratoire d'analyse et d'architecture des systémes,Toulouse (1996).

[134] Valentin, C. *Contribution á la modélisation et á la conduite des procédés mixtes (continues-discrets) : application á l'industrie papetiére.* Ph.D. thesis, l'Institut Polytechnique de Grenoble (1993).

[135] Champagnat, R. *Supervision des systémes discontinus : définition d'un modéle hybride et pilotage en temps-réel.* Ph.D. thesis, Université Paul Sabatier de Toulouse (1998).

[136] Villani, E. Object oriented approach for cane sugar production : modelling and analysis. *Control Engineering Practice* **12**, 1279–1289 (2004).

[137] J.Chen & G.Tan. Study of Anti-lock Brake System Control Strategy in Automobile, Communications in Computer and Information Science. *Springer Berlin Heidelberg* (2011).

[138] Goga, V., Jediny, T., Kralovic, V. & Klucik, M. Mechatronic model of anti-lock braking system (abs). *Springer Berlin Heidelberg* (2012).

[139] Comlan, M., Delfieu, D., Sogbohossou, M. & Vianou, A. Embedding time petri nets. In *2017 4th International Conference on Control, Decision and Information Technologies (CoDIT)*, 0404–0409 (2017).

[140] N.Bennis. Lecture notes : Reseaux de petri (2002).

[141] Aggad, M., Adjerid, S. & Benazzouz, D. Development of a new strategy to extract dangerous scenarios from petrochemical industry installation. *Arabian Journal for Science and Engineering* **45**, 7077–7090 (2020).

[142] Smidts, C. & Devooght, J. Probabilistic reactor dynamics - ii : A monte carlo study of a fast reactor transient. *Nuclear science and engineering* **111**, 241–256 (1992).

[143] A.Cabarbaye & Laulheret, R. Evaluation de la surete de fonctionnement des systemes dynamiques par modelisation recursive. *6eme Congres International pluridisciplinaire, qualite et surete de fonctionnement, Qualita,Bordeaux* (2005).

[144] Kleijnen, J. P. C. Statistical Techniques in Simulation, Part I, New York (1974).

[145] Billinton, R. & Alan, R. Reliability evaluation of engineering systems. *Plenum Press,2nd Edition,New York* (1992).

[146] Billinton, R. & Li, W. Reliability assessment of electric power systems using monte carlo methods. *Plenum Press, New York* (1994).

[147] Ocnasu, A. *Evaluation de la surete de fonctionnement des reseaux de distribution par la simulation Monte Carlo : application a des strategies de maintenance optimales.* Ph.D. thesis, Université de Grenoble (2008).

[148] Niel, E. & Craye, E. Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment. *Maîtrise des risques et sûreté de fonctionnement des systémes de production. Productique : information, commande, communication. Lavoisier* (2002).

[149] Chabot, J., Dutuit, Y. & Rauzy, A. De l'usage de la simulation de monte-carlo couplee aux reseaux de petri en surete de fonctionnement. *3e Conference Francophone de MOdelisation et SIMulation "Conception, Analyse et Gestion des Systemes Industriels, Troyes (France)* (2001).

[150] Vrignat, P. Generation d'indicateurs de maintenance par une approche semi-parametrique et par une approche markovienne. *Revue Sciences et Maintenance, Association franc caise des ingenieurs et responsables de maintenance (AFIM)* 1 – 28 (2012).

[151] Basile, O. *Prise en compte de l'incertitude dans les modeles fiabilistes de maintenance industrielle. Extension aux sollicitations variables.* Ph.D. thesis, Faculté Polytechnique de Mons (2007).

[152] Schutz, J. *Contribution a l'optimisation des plans d'exploitation et de maintenance, selon une approche basee sur le pronostic : application au domaine naval.* Ph.D. thesis, Universite Paul Verlaine - Metz (2009).

[153] Dekker, R. Applications of maintenance optimization models : a review and analysis. *Reliability Engineering and System Safety* **51**, 229 – 240 (1996). URL `http://www.sciencedirect.com/science/article/pii/0951832095000763`. Maintenance and reliability.

[154] Scarf, P. A. On the application of mathematical models in maintenance. *European Journal of Operational Research* **99**, 493 – 506 (1997). URL http://www.sciencedirect.com/science/article/pii/S0377221796003165. Eleventh EURO Summer Institute : Operational Research Models in Maintenance.

[155] Wang, H. A survey of maintenance policies of deteriorating systems. *European Journal of Operational Research* **139**, 469 – 489 (2002). URL http://www.sciencedirect.com/science/article/pii/S0377221701001977.

[156] Lie, C. H. & Chun, Y. H. An algorithm for preventive maintenance policy. *IEEE Transactions on Reliability* **35**, 71–75 (1986).

[157] Malik, M. A. K. Reliable preventive maintenance scheduling. *A I I E Transactions* **11**, 221–228 (1979). URL https://doi.org/10.1080/05695557908974463. https://doi.org/10.1080/05695557908974463.

[158] Pham, H. & Wang, H. Imperfect maintenance. *European Journal of Operational Research* **94**, 425 – 438 (1996). URL http://www.sciencedirect.com/science/article/pii/S0377221796000999.

[159] Monga, A., Zuo, M. & Toogood, R. Reliability-based design of systems considering preventive maintenance and minimal repair. *International Journal of Reliability, Quality and Safety Engineering* **04**, 55–71 (1997).

[160] Chan, J. . & Shaw, L. Modeling repairable systems with failure rates that depend on age and maintenance. *IEEE Transactions on Reliability* **42**, 566–571 (1993).