Contribution à l'évaluation de la fiabilité d'un système mécatronique par modélisation fonctionnelle et dysfonctionnelle

Amel Demri

UNIVERSITE D'ANGERS **Année 2009**
N°991

Contribution à l'évaluation de la fiabilité d'un système mécatronique par modélisation fonctionnelle et dysfonctionnelle

THESE DE DOCTORAT
Spécialité : Sciences de l'ingénieur
ECOLE DOCTORALE D'ANGERS

Présentée et soutenue publiquement
Le xx septembre 2009
A l'Institut des Sciences et Techniques de l'Ingénieur d'Angers

Par Amel DEMRI

Devant le jury ci-dessous :

Patrick LYONNET	Rapporteur	Professeur à l'ENI St Étienne
Abdelkhalak EL HAMI	Rapporteur	Professeur à l'INSA Rouen
Améziane AOUSSAT	Examinateur	Professeur à l'ENSAM Paris
Yasser ALAYLI	Examinateur	Professeur à l'Université de Versailles St Quentin
Fabrice GUERIN	Examinateur	Professeur à l'Université d'Angers
Abdérafi CHARKI	Examinateur	Maître de conférences à l'Université d'Angers
Hervé CHRISTOFOL	Examinateur	Maître de conférences à l'Université d'Angers

Directeur de thèse : **Fabrice GUERIN**
Co-encadrants : **Abdérafi CHARKI & Hervé CHRISTOFOL**

Laboratoire : **Laboratoire en Sûreté de fonctionnement, Qualité et Organisation**
62, avenue Notre Dame du Lac
49000 ANGERS

ED 503

Remerciements

Le travail de recherche exposé dans ce mémoire de thèse a été réalisé au sein du LAboratoire en Sûreté de fonctionnement, QUalité et Organisation (LASQUO) de l'Institut des Sciences et Techniques de l'ingénieur d'Angers (ISTIA).

Je tiens à exprimer mes vifs remerciements et toute ma reconnaissance au Professeur Fabrice Guérin 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.

J'adresse également mes remerciements à Abdérafi Charki et Hervé Christofol pour leur aide et leur disponibilité pendant toute la durée de ma thèse.

Je remercie Monsieur Patrick Lyonnet, Professeur à l'Ecole Nationale d'Ingénieurs de Saint Étienne ainsi que Monsieur Abdelkhalak El Hami, Professeur à l'Institut National des Sciences Appliquées de Rouen, d'avoir accepté de rapporter mon mémoire et pour l'intérêt qu'ils ont bien voulu porter à ce travail.

Mes remerciements s'adressent également à Monsieur Améziane Aoussat, Professeur à l'Ecole Nationale Supérieure d'Arts et Métiers de Paris, ainsi qu'à Monsieur Yasser Alayli, Professeur à l'Université de Versailles St Quentin, pour avoir accepté de prendre part au jury.

Je remercie la Région Pays de la Loire d'avoir financé mes recherches durant ces années de thèse et permis de travailler dans de bonnes conditions.

Mes remerciements vont à tout le personnel du laboratoire LASQUO qui m'a accueillie durant ces années. L'ambiance chaleureuse est propice à un travail efficace.

Je remercie particulièrement Bertrand pour la compréhension des impératifs qu'entraîne un tel travail, et pour ses encouragements et son soutien. Finalement, je tiens à remercier du fond du cœur ma famille sans qui je ne serais jamais arrivée là.

Un grand merci, aussi, à tous mes amis.

A la mémoire de mon père.

Table des matières

Table des figures

Introduction générale

La mécatronique est un néologisme qui caractérise l'utilisation simultanée et en étroite symbiose de la mécanique, de l'électronique et de l'informatique pour envisager de nouvelles façons de concevoir, de produire et de créer de nouveaux produits plus performants. Certaines applications s'imposent naturellement depuis de nombreuses années dans le secteur de l'automobile (accélération sans patinage, direction à assistance variable, freinage sans blocage des roues) en réponse à des contraintes physiques et de dimensionnement des équipements. Cette tendance va encore s'accélérer dans le secteur de l'automobile avec l'évolution prévue vers des solutions plus complètes. La mécatronique joue un rôle fondamental dans la maîtrise des risques et des coûts d'exploitation des véhicules.

La conception de ces éléments, comportant une intégration poussée de composants de technologies différentes, nécessite dès le début de l'étude l'intégration harmonieuse de celles-ci afin de réaliser un produit industriel compétitif et de qualité. L'approche intégrant ces différentes technologies semble évidente mais elle est, en réalité, pleine d'embûches du fait de l'accroissement significatif de la complexité résultant du processus d'intégration. Tout changement dans le niveau de cette complexité introduit des problèmes émergents dont la nature et l'importance va dépendre de la profondeur du processus d'intégration et de l'accroissement des fonctionnalités du produit mécatronique final. Tout déploiement d'un processus d'intégration va donc nécessiter, à son tour, le déploiement du principe du double-action (intégration et correction). Cela passe par l'utilisation du prototypage numérique rapide permettant de simuler sans risque et rapidement le fonctionnement de systèmes complexes et de tester (en termes fonctionnel et dysfonctionnel) une grande variété de solutions en phase de conception.

Ainsi, il est nécessaire que les industriels disposent d'outils d'analyse performants permettant de prendre en compte les aspects événementiels (temps réel), de reconfigurations (possibilité de fonction en mode dégradé) fonctionnelles (besoins client) et dysfonctionnelles (défaillances de composants). L'efficacité de ces outils doit considérer les spécificités associées aux différentes technologies utilisées afin de contribuer à l'ingénierie simultanée et favoriser le travail collaboratif de tous les acteurs (mécaniciens, électronicien, program-

meur, fiabiliste, etc.) en partageant des outils communs.

Un des plus grands problèmes des systèmes mécatroniques concerne l'évaluation de leur fiabilité. Les méthodes d'estimation de cette fiabilité dans les différents domaines des composants qui constituent les systèmes mécatroniques (mécanique, électronique et logiciel), sont très différentes les unes des autres et il n'existe pas, à l'heure actuelle, une méthodologie permettant de mesurer la fiabilité de ces systèmes. De plus, les systèmes mécatroniques sont des systèmes complexes qui intègrent des aspects dynamiques, hybrides et reconfigurables.

Les systèmes mécatroniques et plus généralement les systèmes hybrides ont fait l'objet de nombreux travaux. Ils ont principalement consisté à proposer des modèles fonctionnels et/ou dysfonctionnels permettant de mesurer la performance d'une architecture donnée. On peut distinguer deux catégories de modèles :

- modèle statique : L'arbre de défaillances est le plus utilisé pour décrire des scénarios de dysfonctionnement ou de défaillance. Toutefois, ce modèle ne permet pas de modéliser correctement les systèmes temps réels et/ou reconfigurables (possibilité de fonctionnement en mode dégradé).
- modèle dynamique : Les réseaux de Petri stochastiques et les chaînes de Markov sont les plus utilisés pour décrire les aspects fonctionnels ou/et dysfonctionnels des systèmes mécatroniques. Les études menées utilisent principalement l'hypothèse de taux de défaillance constant pour caractériser une transition vers une place caractérisant un état de défaillance. Cette hypothèse ne peut pas être prise dans le cas de défaillance de composants mécaniques. En phase de conception, la fiabilité des composants mécaniques est couramment estimée à l'aide de la méthode Résistance-Contrainte.

Ainsi, pour étudier le plus précisément possible les systèmes mécatroniques en intégrant les aspects fonctionnels et dysfonctionnels il est nécessaire d'intégrer des méthodes d'analyse hétérogènes.

L'objectif de cette thèse consiste à développer une méthodologie globale permettant de :

- réaliser l'analyse fonctionnelle du produit permettant de définir une architecture fonctionnelle en phase avant-projet et matérielle si les technologies sont choisies en intégrant les spécificités de chacune d'elle ;
- effectuer l'analyse des risques permettant de réduire le nombre de solutions d'architecture en intégrant les différents outils classiques mais distincts en fonction des technologies ;
- modéliser les comportements dynamiques fonctionnel et dysfonctionnel d'une ar-

chitecture en prenant compte de la physique associé aux différentes technologies. Ce point portera en particulier sur la physique de défaillance en mécanique qui est relativement complexe mais qui permettra d'obtenir un prototype numérique plus proche du comportement réel du produit ;

– simuler le modèle comportemental du système mécatronique afin d'étudier et d'optimiser les performances des différentes solutions retenues.

Ce mémoire comporte trois chapitres :

Le premier chapitre est consacré au contexte actuel des systèmes mécatroniques en tenant compte de leurs différents aspects (dynamique, hybride et reconfigurable) et de montrer qu'ils doivent être conçus et développés de manière collaborative pour obtenir des systèmes sûrs de fonctionnement. L'approche systémique, qui est une démarche d'aide à l'étude des systèmes complexes, est définie dans ce premier chapitre. Nous abordons, par la suite, l'ingénierie système qui apportera un gain de qualité et de temps. Enfin nous terminons par un dernier paragraphe qui présente les différentes méthodes d'analyse de la sûreté de fonctionnement des systèmes complexes et, par conséquent, des systèmes mécatroniques.

Le deuxième chapitre présente, dans un premier temps, des généralités sur la sûreté de fonctionnement. Les différentes méthodes adaptées à chaque étape du cycle de développement, défini dans le premier chapitre, sont présentées. L'analyse qualitative est, ensuite, abordées où on met l'accent sur l'analyse fonctionnelle et l'analyse dysfonctionnelle ainsi qu'aux différentes méthodes qui leurs sont associées. La construction du modèle dynamique d'un système mécatronique est importante. C'est pourquoi nous présentons, dans cette partie, les différentes méthodes dédiées à la modélisation dynamique. Un point important aussi de ce chapitre concerne la présentation des différents mécanismes de défaillances des composants constituant le système mécatronique et les lois de fiabilité associées à ces différents composants. Pour finir, nous abordons la fiabilité dynamique et la fiabilité mécanique en fonction du temps ainsi qu'une synthèse sur les travaux précédemment réalisés.

Le dernier chapitre est dédié à la méthodologie que nous avons mise au point pour résoudre les différents problèmes que peuvent engendrer les systèmes mécatroniques ainsi qu'à son application sur un système ABS. La première partie de ce chapitre expose la problématique de ces systèmes dynamiques, hybrides, reconfigurables et multitechnologies. La seconde partie explique le principe de la démarche que nous avons mis en place. Cette méthodologie est constituée de deux grandes étapes qui sont l'analyse qualitative et l'analyse quantitative. L'analyse qualitative (analyse fonctionnelle et dysfonctionnelle) permet d'obtenir les fonctions internes du système mécatronique ainsi que les différents

modes de défaillance qu'il peut rencontrer. L'analyse quantitative permet de déterminer les variables physiques internes du système ainsi que sa fiabilité. Pour finir, la troisième partie est dédiée à l'application de cette méthodologie sur un système ABS.

Pour clore ce mémoire, une conclusion générale permet de préciser les apports de la méthodologie que nous avons développée et les perspectives à cette dernière.

Chapitre 1

Contexte

Sommaire

1.1 Introduction

Il y a quelques années, le domaine de la sûreté de fonctionnement s'est repositionné par l'arrivée de pannes dues à l'accroissement et à la généralisation des systèmes embarqués, notamment dans les véhicules. Ces systèmes plongés dans des environnements perturbants et inadaptés, ont généré des problèmes dont on ne pouvait pas soupçonner l'existence.

Depuis, une nouvelle démarche d'étude de sûreté de fonctionnement de ces systèmes s'est mise en place dans le but de tenir compte de leur complexité.

1.2 Approche systémique

La systémique est une discipline qui regroupe les démarches théoriques, pratiques et méthodologiques, relatives à l'étude de ce qui est reconnu comme trop complexe pour pouvoir être abordé de façon plus simple, et qui pose des problèmes de frontières, de relations internes et externes, de structure, de lois ou de propriétés émergentes caractérisant le système comme tel, ou des problèmes de mode d'observation, de représentation, de modélisation ou de simulation d'une totalité complexe [22].

Pour appréhender la complexité d'un système, la systémique fait appel à un certain nombre de concepts spécifiques que l'on peut regrouper de la manière suivante :

- quatre concepts de base à caractère général, articulés entre eux et pouvant donner lieu en préalable à une présentation simple ;
- une dizaine de concepts complémentaires plus techniques et orientés vers l'action.

Les quatre concepts de base sont schématisés sur la figure 1.1. Ces concepts sont : la complexité, le système, l'interaction et la globalité.

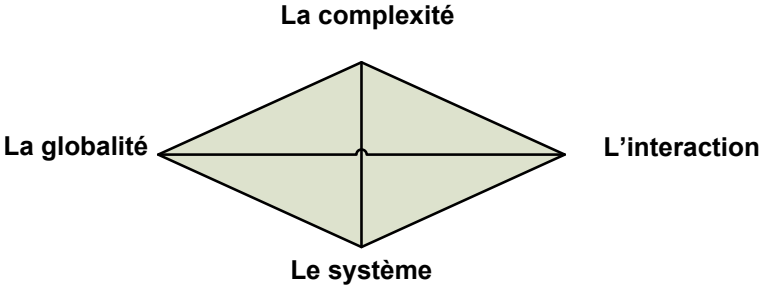

FIGURE 1.1 – Les quatre concepts de base de la systémique [33]

- **La complexité** : C'est une hypothèse qui conduit à postuler que les méthodes analytiques sont insuffisantes pour appréhender le phénomène étudié.
- **Le système** : Ce concept représente le socle sur lequel repose la systémique. Il est l'objet de l'étude et le champ de responsabilité du modélisateur.
- **La globalité** : Il s'agit d'une propriété des systèmes complexes et selon laquelle on ne peut les connaître vraiment sans les considérer dans leur ensemble. Cette globalité exprime à la fois l'interdépendance des éléments du système et la cohérence de l'ensemble. Sous le nom d'approche globale, le concept désigne également la voie d'entrée dans la démarche systémique. On entend par là qu'il convient d'aborder tous

les aspects d'un problème progressivement, mais non séquentiellement : partir d'une vue générale (globale) pour approfondir les détails, avec de nombreuses itérations et retours en arrière pour compléter ou corriger la vision antérieure.

– **L'interaction** : Ce concept, un des plus riches de la systémique, complète celui de globalité car il s'intéresse à la complexité au niveau élémentaire de chaque relation entre les constituants du système complexe. Initialement emprunté à la mécanique où l'interaction se réduit alors à un jeu de forces, la relation entre constituants se traduit le plus souvent dans les systèmes complexes, par un rapport d'influence ou d'échange portant aussi bien sur des flux de matière, d'énergie et d'information.

Ces quatre concepts sont essentiels. Cependant il est nécessaire d'en connaître d'autres tels que l'information, la finalité, la rétroaction (feedback), etc.

La systémique est non seulement un savoir mais aussi une démarche et une manière de rentrer dans la complexité. Cette démarche se déroule en plusieurs étapes comme le montre la figure 1.2 :

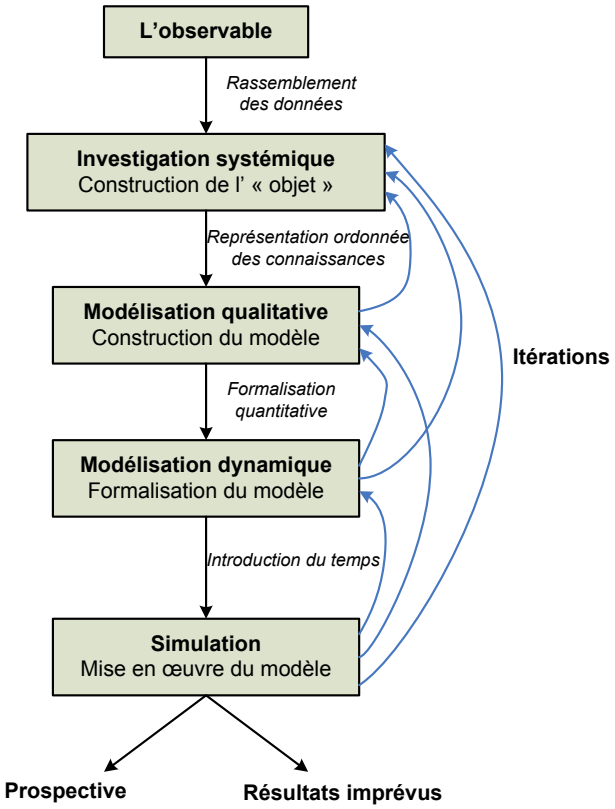

FIGURE 1.2 – Les étapes de la démarche systémique [33]

– l'observation du système par divers observateurs et sous divers aspects ;
– l'analyse des interactions et des chaînes de régulation ;
– la modélisation en tenant compte des enseignements issus de l'évolution du système ;

– simulation et confrontation à la réalité pour obtenir un consensus.

Dans le cadre de cette thèse nous nous sommes intéressés aux systèmes complexes multitechnologies et en particulier aux systèmes mécatroniques.

1.3 La mécatronique

Le terme mécatronique (*mechatronic*) a été proposé, pour la première fois, par un ingénieur d'une compagnie japonaise ; Yaskawa en 1969, comme étant une combinaison de *mecha* pour désigner la mécanique et *tronic* pour l'électronique [50, 20].

Depuis, une multitude de définitions de la mécatronique existent du fait que l'électronique est de plus en plus présente dans les systèmes et dans des domaines aussi variés que le transport, la domotique, la médecine, la robotique, etc.

Selon le Comité Consultatif de Recherche Industrielle et de Développement de la Communauté Européenne (Industrial Research and Development Advistory Comittee of the European Communoty), la mécatronique est la combinaison synergique de l'ingénierie mécanique de précision, de la commande électronique et du système informatique dans la conception des produits et des processus de fabrication. Selon les professionnels, c'est le processus d'intégration pluridisciplinaire combinant synergie de l'ingénierie mécanique, électronique et informatique [69, 95, 61, 60].

La mécatronique est ainsi une démarche rigoureuse, adaptée et focalisée sur l'optimisation des systèmes du point de vue de l'ingénieur. Cette approche globale permet aussi de réduire les coûts, d'augmenter la fiabilité des systèmes exposés à des environnements éprouvants. C'est avant tout une démarche et un état d'esprit [9].

Étant donné la présence de l'électronique dans de nombreux domaines, les équipes de conception mécanique et électronique sont amenés à fusionner et développer des synergies et des nouvelles méthodes de travail pour faire face aux problèmes qui se manifestent lors de toute rupture technologique.

Un des plus grands problèmes de ces systèmes mécatroniques concerne l'évaluation de leur fiabilité qui est une préoccupation qui prend une place de plus en plus importante, poussées à la fois par l'évolution des technologies et par les demandes du marché. Cette fiabilité est souvent ressentie, par les industriels, comme étant l'un des points les moins bien maîtrisés et, pour certains, comme étant le point critique pour le déploiement et l'avenir des technologies mécatroniques.

Les méthodes d'évaluation de cette fiabilité dans ces différents domaines (mécanique, électronique et logiciel) sont en effet très différentes les unes des autres et il n'existe pas, à l'heure actuelle, de procédé permettant de mesurer la fiabilité des systèmes intégrant plu-

sieurs technologies, notamment ceux mêlant hydraulique et électronique où l'expérience accumulée par l'industrie est faible [95]. Les problèmes de ces systèmes mécatroniques résident aussi dans l'incompréhension et le manque de dialogue entre les différents domaines impliqués dans un développement mécatronique et sont souvent identifiés comme la cause principale des délais ou des erreurs commises.

Cependant, un constat se dégage des enquêtes menées : l'augmentation de la profondeur d'intégration mécatronique augmente la fiabilité d'un dispositif isolé de son environnement. Le problème de fiabilité se pose lorsque le dispositif est intégré dans un environnement complexe. C'est la nature mécatronique de l'interface qui est en effet la plus délicate à contrôler [95].

Pour résoudre le problème majeur des systèmes mécatroniques, les concepteurs et les utilisateurs montrent un grand intérêt pour l'évaluation de la fiabilité du système global, c'est-à-dire pour la partie matérielle et pour la partie logicielle. A ce jour, la modélisation de la fiabilité du matériel et celle du logiciel ont pris des orientations différentes et sont souvent conduites séparément [69].

Pour un matériel comme pour un logiciel, la fiabilité décroît avec le temps si on ne répare pas mais elle croît avec le temps, dans le cas du logiciel, si on corrige les défauts [38].

1.3.1 L'aspect dynamique des systèmes mécatroniques

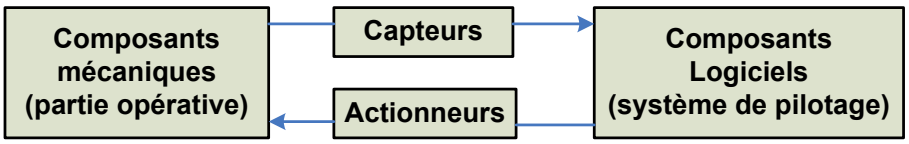

FIGURE 1.3 – Schéma d'un système mécatronique

Le système mécatronique de la figure 1.3 intègre de la mécanique, de l'électronique et du logiciel. Il peut être décomposé en quatre entités en interactions : les capteurs, la partie opérative, le système de commande et de reconfiguration et les actionneurs.

Les capteurs mesurent des grandeurs physiques continues caractéristiques de la partie opérative. Le système de pilotage ou 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 également 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 pour ramener les grandeurs caractéristiques de celle-ci dans les limites permises. Ainsi pour ce type de système, la sécurité est assurée par des reconfigurations sans interruption de la mission. Ces systèmes mécatroniques sont des systèmes à reconfigurations dynamiques [67, 73].

1.3.2 L'aspect hybride des systèmes mécatroniques

L'aspect hybride des systèmes mécatronique réside dans la présence de phénomènes continus et d'événements discrets (franchissement de seuils, séquence d'événements, ou combinaison des deux). On peut ajouter que certaines de ces variables peuvent présenter un caractère aléatoire telle que les défaillances d'un des composants par exemple.

1.3.3 L'aspect reconfigurable des systèmes mécatroniques

Un système est constitué de composants. Le fonctionnement de ce système est assuré par les interactions entre ces composants. Si les relations fonctionnelles entre ces composants restent figées tout au long de la mission du système, il sera dit statique. Il conserve la même configuration tout au long de son cycle de vie et remplit toujours la même fonction.

Un système est dit reconfigurable s'il est prévu pour remplir plusieurs fonctions alternativement ou remplir une fonction en utilisant ses ressources de plusieurs façons différentes.

Si le système peut changer la configuration des relations fonctionnelles entre certains de ses composants sans interrompre sa mission, le système sera dit à configuration dynamique.

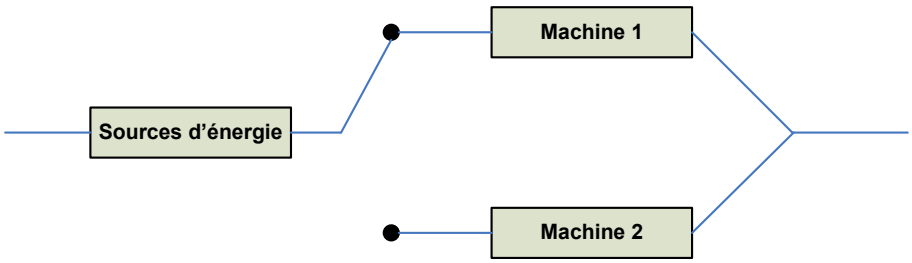

FIGURE 1.4 – Exemple d'un système reconfigurable [73]

La reconfiguration peut être de type matérielle ou logicielle. La reconfiguration matérielle consiste à réparer un équipement ou à choisir une nouvelle architecture physique pour réaliser la fonction considérée. La reconfiguration logicielle se base sur la redondance. La différence entre ces deux types de reconfiguration est dans la vitesse d'exécution et le coût : un changement de configuration matérielle est toujours plus long et plus risqué. Une telle reconfiguration a une probabilité d'échec généralement non négligeable [67].

La conception de tel système nécessite de recourir à des processus d'ingénierie adaptées.

1.4 L'ingénierie système

Lors de la conception de nouveaux systèmes, 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. En utilisant un processus efficace de développement de produits, dans un environnement d'équipes multifonctionnelles performantes et créatives, il est possible de développer rapidement des produits de qualité à des coûts compétitifs [69, 1].

D'une manière générale, la nouvelle stratégie de décision nécessite une parallélisation d'un certain nombre d'activités de conception appelé ingénierie système.

C'est une approche globale multi-métiers qui consiste à engager en parallèle les activités et les tâches, les services et les métiers nécessaires au développement du système.

L'ingénierie système permet d'optimiser la démarche de conception de projets collaboratifs, et d'assurer la meilleure coordination entre les parties prenantes du projet. L'apport de l'ingénierie système est avant tout un gain de qualité et de temps. Ainsi l'enchaînement optimal des tâches assure le suivi du cheminement le plus court et permet d'anticiper les problèmes du fait du partage général de l'information entre les membres de l'équipe.

L'ingénierie système fait intervenir des éléments similaires à ceux des systèmes mécatroniques, tels que [69] :

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

Du fait de sa complexité, un système mécatronique ne peut pas être créé par une personne par contre, il peut être conçu par un grand nombre de personnes avec différentes spécialisations à condition que ces personnes constituent une équipe.

L'ingénierie système aborde la conception dans sa globalité. Partant des souhaits exprimés 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. Ce processus fait intervenir des étapes qui s'enchaînent logiquement selon un cycle et qui sont bien adaptées au développement des systèmes mécatroniques.

1.4.1 Cycle de développement

Les systèmes industriels complexes se caractérisent par le fait qu'ils résultent d'une combinaison de sous-systèmes de technologies différentes.

Le cycle en V, présenté sur la figure 1.5, a d'abord été utilisé comme modèle de développement dans les différentes technologies : la mécanique, l'électronique ou le logiciel.

Le cycle en V a été ensuite généralisé au développement des systèmes complexes, en particulier des systèmes mécatroniques, afin d'avoir une terminologie commune et de proposer une méthodologie globale, avec des étapes communes aux différents technologies. Plusieurs auteurs ont montré l'intérêt du cycle en V [96, 48].

Il existe d'autres types de cycles de développement, les plus connus étant les cycles en W, en cascade ou en spirale.

Le modèle de développement selon le cycle en V positionne les différentes phases de développement, depuis la spécification jusqu'à la validation produit comme le montre la figure 1.5 [48]

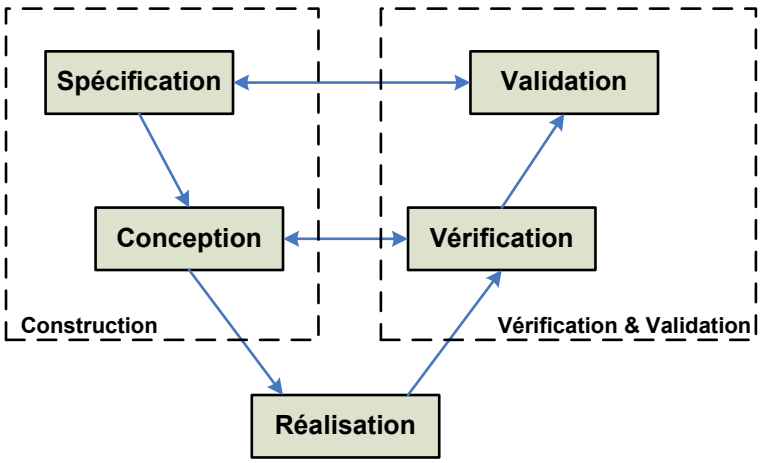

FIGURE 1.5 – Cycle en V

Le développement commence par la partie construction du système, la partie descendante du cycle en V, où le système est graduellement décomposé en ses divers sous-systèmes et modules jusqu'au niveau composant. La partie montante du cycle en V com-

prend le bloc de Vérification & 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.

1.4.2 Analyse/Spécification

La première phase de développement d'un système consiste dans la réalisation de l'analyse des besoins et des spécifications. Cette phase propose la définition des fonctionnalités, des interfaces, des contraintes et des exigences du système, la préparation du plan qualité, du plan de validation, de l'étude de faisabilité, la définition du niveau de la fiabilité souhaité du système.

Pour un système mécatronique la difficulté majeure est la traduction de la spécification système en spécifications particulières pour chaque composant selon les différentes technologies.

1.4.3 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, du plan de tests et d'essais et de l'analyse des risques.

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

1.4.4 Réalisation

Cette phase de développement consiste à passer du résultat de la conception à un ensemble d'activités d'industrialisation permettant la fabrication et l'assemblage des composants.

Même si techniquement les spécifications des composants pour le système mécatronique sont précises, un fournisseur ou un fabricant des composants est toujours susceptible d'interpréter les spécifications légèrement différemment et, en conséquence, de livrer des composants qui ne sont pas conformes aux spécifications.

1.4.5 Vérification

Dans cette phase tous les modules ou sous-systèmes sont vérifiés et testés par rapport à la conception. La vérification est complémentaire avec l'assemblage des modules et des sous-systèmes jusqu'au système final.

Dans cette phase, il est difficile de tester la synchronisation des différents modules ou sous-systèmes du système mécatronique. De plus, des ambiguïtés par rapport à la conception peuvent accroître cette difficulté de synchronisation. En même temps, il est extrêmement difficile de détecter des changements de conception (modules ou sous-systèmes non conformes à la conception) tant que le système mécatronique n'est pas entièrement construit pour exécuter des essais avec le système complet.

1.4.6 Validation

La deuxième phase de V&V est la validation du système final. Il s'agit d'une validation fonctionnelle, une phase importante, où sont constatées les fonctionnalités et le niveau de qualité par rapport aux spécification/analyse de besoins. Pour un système mécatronique, la validation est un point sensible dû à la combinaison, à la synchronisation et à l'interaction des différentes technologies. Ces contraintes rendent plus difficiles le diagnostic et l'entretien du système mécatronique.

Lors du développement d'un système, le constructeur spécifie non seulement les fonctionnalités, mais aussi les objectifs à atteindre en terme de sûreté de fonctionnement. Ainsi, il est de plus en plus nécessaire d'intégrer la sûreté de fonctionnement dans l'approche système, très en amont dans les projets, dès la première phase du cycle de développement. Cette intégration conduit non seulement à démultiplier les études de fiabilité, de disponibilité, de maintenabilité et de sécurité, mais aussi à mettre en place une méthodologie transversale qui favorise leur prise en compte dans les projets et à travers les différents métiers liés au développement du système mécatronique.

La spécification des objectifs de sûreté de fonctionnement est accompagnée d'une procédure de validation pour vérifier que ces objectifs ont été atteints. Tout au long du développement du système mécatronique, des méthodes et des techniques spécifiques de la sûreté de fonctionnement devront être appliquées pour atteindre les objectifs exigés.

Notre objectif est d'évaluer quantitativement la sûreté de fonctionnement des systèmes mécatroniques en phase de conception afin de comparer les différents types d'architectures possibles proposées à l'issue des études en avance de phase.

1.5 Méthodes d'analyse de la sûreté de fonctionnement d'un système complexe

Dans le processus de développement des systèmes complexes, la sûreté de fonctionnement est devenue une caractéristique essentielle [75]. Ainsi, afin d'optimiser le développement de ces systèmes, il est impératif de disposer de méthodes permettant d'évaluer la sûreté de fonctionnement en cours de développement.

L'évaluation de la sûreté de fonctionnement d'un système consiste à analyser les défaillances des composants pour estimer leurs conséquences sur le service rendu par le système. Les principales méthodes utilisées lors d'une analyse de la sûreté de fonctionnement sont : l'Analyse Préliminaire des Risques (APR), l'Analyse des Modes de Défaillance, de leur Effets et de leurs Criticités (AMDEC), le Diagramme de Fiabilité (DdF), les Arbres de Défaillances (AdD), la Méthode de l'Espace des États (MEE), etc.

Les méthodes classiques de la sûreté de fonctionnement, comme celles citées précédemment, sont statiques. Ces méthodes basées sur la logique booléenne pour représenter le système étudié sont adaptées à des systèmes à configuration statique, c'est-à-dire des systèmes dont les relations fonctionnelles entre leurs composants restent figées.

Dans le cadre de nos travaux, la prise en compte des mécanismes de reconfiguration dans les systèmes pilotés par calculateurs est essentielle. Cet aspect n'est pas pris en compte par les méthodes classiques de sûreté de fonctionnement ce qui les rend inefficaces. Ces méthodes restent combinatoires et incapables de prendre en compte les changements d'états et les reconfigurations dans les scénarios redoutés.

Les méthodes les plus adaptées à la modélisation et à l'analyse des systèmes dynamiques hybrides sont les modèles *états-transitions* tels que les graphes d'états (les graphes de Markov et les automates) et les approches basées sur les réseaux de Petri [67].

Ces méthodes seront présentées en détail dans le chapitre 2.

1.6 Conclusion

Les systèmes mécatroniques sont de plus en plus utilisés dans l'industrie. Tous les secteurs sont concernés : l'automobile, l'aéronautique, le nucléaire, le spatial et même les domaines comme le bancaire ou le médical. La complexité importante des systèmes mécatroniques et la réduction des coûts de conception et d'exploitation incitent les industriels à maîtriser davantage la sûreté de fonctionnement de ces systèmes.

Comme nous l'avons présenté dans ce chapitre, les systèmes mécatroniques sont des systèmes complexes caractérisés par leur :

- aspect dynamique où les relations fonctionnelles entre ses composants changent au court du temps ;
- aspect hybride où on retrouve la présence de phénomènes continus et d'événements discrets ainsi que la présence de phénomènes aléatoires dûs au défaillances des composants par exemple ;
- aspect reconfigurable dont l'objectif est de concevoir des systèmes les plus stables possible.

Pour l'étude des systèmes complexes tels que les systèmes mécatronique, la systémique constitue un outil très intéressant. Cette approche systémique peut être définie comme étant une approche logique, centrée sur le but à atteindre, rationnelle et globale, orientée par le présent-futur (prospective), ouverte sur la diversité des réalités et la pluralité des solutions, etc. Par ce fait, l'approche systémique est particulièrement apte à éclairer et à orienter l'action des décideurs.

Plusieurs méthodes d'analyse de sûreté de fonctionnement existent, mais les plus adaptées à la modélisation et à l'analyse des systèmes dynamiques hybrides sont les modèles *états-transitions*. Ces modèles sont détaillés dans le chapitre suivant.

Chapitre 2

Sûreté de Fonctionnement des systèmes mécatroniques

Sommaire

2.1 Généralités sur la Sûreté de Fonctionnement

La complexité croissante des systèmes, la réduction de leurs coûts de conception et d'exploitation, leur utilisation de plus en plus importante dans la vie quotidienne font que la sûreté de fonctionnement est devenue incontournable dans le développement de tout système industriel.

La Sûreté de Fonctionnement (SdF) fait partie des enjeux majeurs de ces dernières années et des années à venir. Cette notion désigne à la fois un ensemble de moyens et un ensemble de résultats produits par ces moyens :

- des méthodes et des outils pour caractériser et maîtriser les effets des aléas, des pannes et des erreurs ;
- la quantification des caractéristiques des systèmes pour exprimer la conformité dans le temps de leurs comportements et de leurs actions.

Différents auteurs [102, 75, 38, 84, 58] définissent la sûreté de fonctionnement comme :

- la fiabilité, la disponibilité, la maintenabilité et la sécurité ;
- la science des défaillances ;
- la confiance justifiée dans le service délivré ;
- le maintien de la qualité dans le temps.

La définition « Fiabilité, Disponibilité, Maintenabilité et Sécurité » qu'on retrouve dans l'acronyme FDMS, fait référence aux définitions de ces termes et met en avant leur complémentarité. Si la fiabilité, la maintenabilité, la disponibilité ou la sécurité sont aussi des performances d'un système, la sureté de fonctionnement ne se réduit pas uniquement à une de ces performances, elle se construit à travers toutes ces dernières [38].

La définition « science des défaillances » suppose la connaissance, l'évaluation, la prévision, la mesure et la maîtrise des défaillances. Ainsi la sûreté de fonctionnement apparaît davantage comme l'aptitude d'une entité à satisfaire une ou plusieurs fonctions requises dans des conditions données [102].

La définition « confiance justifiée dans le service délivré » dépend principalement de la perception des utilisateurs. Le service délivré par un système est son comportement perçu par son, ou ses utilisateurs, sachant qu'un utilisateur est un autre système (humain ou physique) qui interagit avec le système considéré.

La définition « maintien de la qualité dans le temps » prend en compte la conformité aux exigences (explicites ou non). Elle présente le défaut de laisser supposer qu'une activité SdF se conduit nécessairement dans le cadre d'une démarche qualité, ce qui est insuffisant [75].

La définition de la SdF sera considérée globalement comme la conjugaison de ces quatre

définitions. L'ensemble de ces définitions est cohérent et fournit une image plus complète de la SdF prise selon plusieurs points de vue.

Dans ce chapitre, on s'intéresse uniquement aux principales grandeurs de la SdF qui sont la fiabilité, la disponibilité, la maintenabilité et la sécurité.

2.1.1 Fiabilité

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.

$$R(t) = P[E \text{ non defaillant sur } [0,t]] \tag{2.1}$$

Pour certains appareils, il peut être plus judicieux de prendre une autre variable : nombre de cycles d'ouverture-fermeture pour un relais, nombre de tours pour un moteur, nombre de kilomètres pour une voiture, etc.

2.1.2 Disponibilité

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.

$$A(t) = P[E \text{ non defaillant a l}'\text{instant } t] \tag{2.2}$$

2.1.3 Maintenabilité

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.

$$M(t) = P[E \text{ est reparable sur } [0,t]] \tag{2.3}$$

2.1.4 Sécurité

La sécurité est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques. Elle est caractérisée par la probabilité *S(t)* que l'entité E ne laisse pas apparaître dans des conditions données, des événements critiques ou catastrophiques.

$$S(t) = P[E \text{ evite des evenements critiques ou catastrophiques sur } [0, t]] \tag{2.4}$$

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 et concerne la lutte contre les fautes intentionnelles [38].

2.1.5 Métriques de la Sûreté de Fonctionnement

Des grandeurs associées à la sûreté de fonctionnement peuvent être calculées à partir des mesures de probabilités. Ces grandeurs suivantes caractérisent des durées moyennes [102] :

- MTTF (Mean Time To Failure) : Durée moyenne de fonctionnement d'une entité avant la première défaillance.

$$MTTF = \int_0^\infty R(t)\, dt \tag{2.5}$$

- MTTR (Mean Time To Repair) : Durée moyenne de réparation

$$MTTR = \int_0^\infty [1 - M(t)]\, dt \tag{2.6}$$

- MUT (Mean Up Time) : Durée moyenne de fonctionnement après réparation
- MDT (Mean Down Time) : Durée moyenne d'indisponibilité après défaillance
- MTBF (Mean Time Between Failure) : Durée moyenne entre deux défaillances

$$MTBF = MDT + MUT \tag{2.7}$$

Ces durées sont représentées dans la figure :

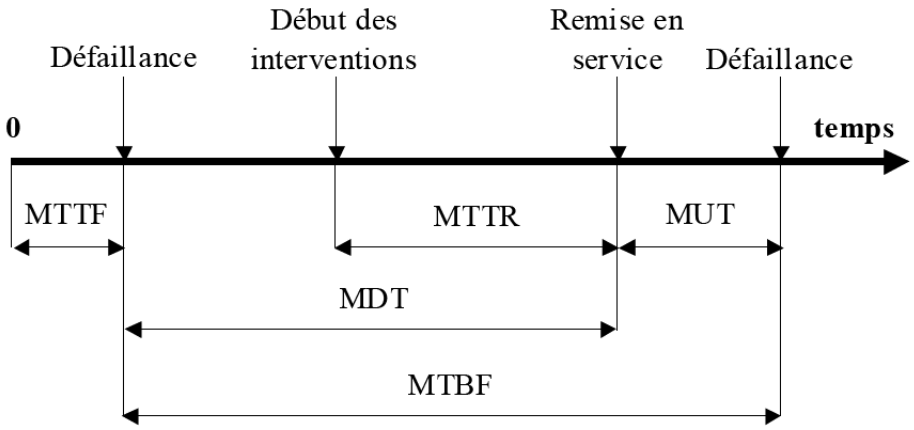

FIGURE 2.1 – Durées moyennes associées à la SdF

2.1.5.1 Mesure de performances

On considère un système pouvant se trouver dans différents états. Cet ensemble d'états, noté `E`, se décompose en deux sous ensembles formant une partition : le sous-ensemble `M` des états de marche et le sous-ensemble `D` des états de défaillance.

On appelle également fiabilité, la probabilité associée *R(t)* définie par :

R(t) = Prob(qu'une entité *E* soit non défaillante sur la durée *[0,t]*, en supposant qu'elle n'est pas défaillante à l'instant $t = 0$).

La caractéristique contraire est appelée défiabilité ou probabilité de défaillance. Elle est telle que :

$$\overline{R(t)} = 1 - R(t) \tag{2.8}$$

La figure 2.2 présente une allure de la fonction *R(t)* en fonction du temps

Pour compléter l'approche théorique de la notion de fiabilité, il est nécessaire de définir aussi les notions suivantes, qui sont issues de la théorie des probabilités.

La fonction F(t) représente la fonction de répartition de la variable aléatoire T (instant de défaillance). C'est la défiabilité $\overline{R(t)}$ (la probabilité de défaillance du système) ou la probabilité complémentaire à 1 de la fiabilité R(t) définie par :

$$F(t) = \overline{R(t)} = 1 - R(t) \tag{2.9}$$

La fonction f(t) désigne la densité de probabilité de t et elle est donnée par :

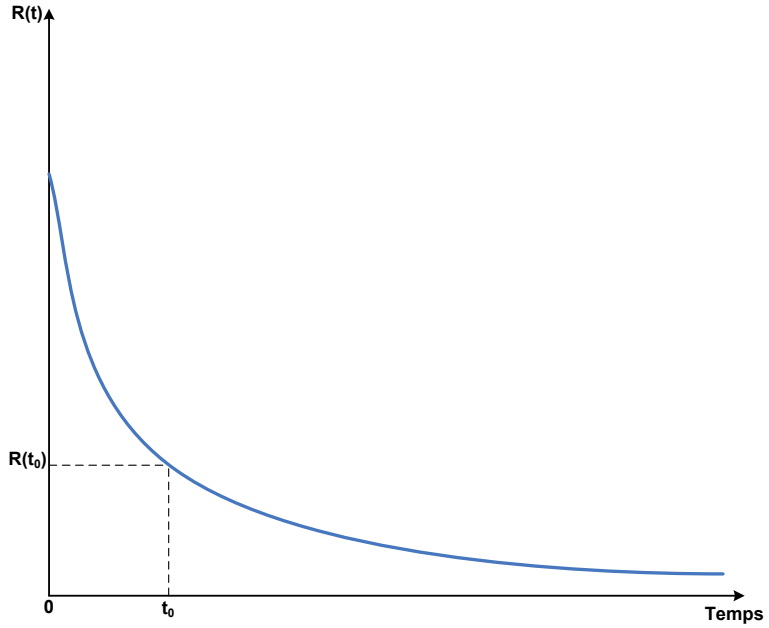

FIGURE 2.2 – Courbe de survie ou de fiabilité

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \tag{2.10}$$

Taux de défaillance instantané : Le taux instantané de défaillance, λ(t), est une des mesures caractéristiques de la fiabilité. La valeur $\lambda(t)dt$ représente la probabilité conditionnelle d'avoir une défaillance dans l'intervalle de temps *[t,t+dt]*, sachant qu'il n'y a pas eu de défaillance dans l'intervalle de temps *[0,t]*.

Ainsi, en appliquant le théorème des probabilités conditionnelles, puis le théorème des probabilités totales, λ(t) s'écrit :

$$\lambda(t)\,dt = \frac{\text{Prob}\left(\text{defaillant sur } [t, t+dt] \text{ sans defaillance sur } [0,t]\right)}{\text{Prob}\left(\text{non defaillant sur } [0,t]\right)} \tag{2.11}$$

$$\lambda(t)\,dt = \frac{\text{Prob}\left(\text{defaillant sur } [0, t+dt]\right) - \text{Prob}\left(\text{defaillant sur } [0,t]\right)}{\text{Prob}\left(\text{non defaillant sur } [0,t]\right)} \tag{2.12}$$

$$\lambda(t) = \frac{f(t)}{R(t)} = -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \tag{2.13}$$

Il est fréquent de représenter l'évolution du taux de défaillance $\lambda(t)$ au cours du temps t selon une courbe caractéristique dite en *baignoire* qui sera abordée plus loin dans ce chapitre..

Taux de réparation instantané : La valeur $\mu(t)dt$ représente la probabilité pour que le système n'étant pas réparé à t le soit à $t+dt$. Le taux de défaillance $\mu(t)$ s'écrit alors :

$$\mu(t) = \frac{1}{1 - M(t)} \cdot \frac{dM(t)}{dt} \tag{2.14}$$

2.1.6 Quelques lois de probabilité

2.1.6.1 Loi exponentielle

La loi exponentielle a de nombreuses applications dans plusieurs domaines. Elle décrit la vie des matériels qui subissent des défaillances brutales. La loi exponentielle est la plus couramment utilisée en fiabilité électronique pour décrire la période durant laquelle le taux de défaillance des équipements est considéré comme constant (défaillance aléatoire). Elle décrit le temps écoulé jusqu'à une défaillance, ou l'intervalle de temps entre deux défaillances. Elle est définie par un seul paramètre, le taux de défaillance, λ [32].

Elle est caractérisée par :

La fiabilité

$$R(t) = e^{-\lambda t} \tag{2.15}$$

La densité de probabilité :

$$f(t) = \lambda e^{-\lambda t} \tag{2.16}$$

Le taux de défaillance :

$$\lambda(t) = \lambda \tag{2.17}$$

2.1.6.2 Loi Weibull

La loi de Weibull est souvent utilisée en mécanique ; elle caractérise bien le comportement du produit dans les trois phases de vie selon la valeur du paramètre de forme β : période de jeunesse ($\beta < 1$), période de vie utile ($\beta = 1$) et période d'usure ou vieillissement ($\beta > 1$). La loi de Weibull est définie par deux paramètres η (paramètre d'échelle) et β (paramètre de forme) [32].

Elle est caractérisée par :

La fiabilité :

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{2.18}$$

La densité de probabilité :

$$f(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{2.19}$$

Le taux de défaillance :

$$\lambda(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} \tag{2.20}$$

2.1.6.3 Loi normale

La loi normale est très répandue parmi les lois de probabilité car elle s'applique à de nombreux phénomènes. La loi normale est définie par une moyenne μ et un écart type σ :

La fonction de répartition :

$$F(t) = \frac{1}{\sigma\sqrt{2\pi}}\int_{-\infty}^{t} e^{-\frac{1}{2}\left(\frac{(x-\mu)}{\sigma}\right)^2} dx \tag{2.21}$$

La densité de probabilité :

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{(t-\mu)}{\sigma}\right)^2} \tag{2.22}$$

2.1.6.4 Loi lognormale

Loi lognormale Une variable aléatoire continue et positive t est distribuée selon une loi lognormale si son logarithme est distribué suivant une loi normale. Cette distribution est utilisée en fiabilité pour modéliser les défaillances par fatigue. La loi lognormale a deux paramètres μ et σ [32] :

La fiabilité :

$$R(t) = 1 - \Phi\left(\frac{\log(t) - \mu}{\sigma}\right) \tag{2.23}$$

La densité de probabilité :

$$f(t) = \frac{1}{t\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\log(t)-\mu}{\sigma}\right)^2} \tag{2.24}$$

Le taux de défaillance :

$$\lambda(t) = \frac{e^{-\frac{1}{2}\left(\frac{\log(t)-\mu}{\sigma}\right)^2}}{t\int_0^{\infty}\sigma\sqrt{2\pi}f(t)\,dt} \tag{2.25}$$

2.2 Méthodes utilisées au cours du cycle de développement en V

Les méthodes de validation dépendent de la phase du cycle de développement dans laquelle elles sont utilisées. Cet impact a été déterminé à partir d'une étude qualitative

sur l'utilisation des méthodes dans le processus de développement, à travers des références bibliographiques.

2.2.1 Les méthodes actuelles de validation dans la partie construction

Pendant les activités de construction d'un système, correspondant aux phases descendantes du cycle en V, certaines ont directement un impact sur la fiabilité du système. L'efficacité des méthodes dépend de la connaissance du système et des exigences de fiabilité préalablement définies.

2.2.1.1 Phase d'Analyse/Spécification

Cette phase commence par l'analyse fonctionnelle, une démarche qui consiste à rechercher, ordonner, caractériser, hiérarchiser et/ou valoriser les fonctions du système attendu par l'utilisateur.

L'analyse fonctionnelle est la base de l'élaboration d'un cahier des charges fonctionnelles (CdCF), représentant l'expression des besoins (voir annexe A).

Un CdCF est, par définition, un document dans lequel le demandeur exprime son besoin en terme de fonctions de service et de contraintes. Pour chacune des fonctions, des critères d'appréciation et leurs niveaux sont définis. Chacun de ces niveaux est assorti d'une tolérance.

L'analyse des besoins qui est l'activité essentielle au début du processus de développement donne lieu à l'élaboration de plusieurs documents :

- un recueil d'informations pertinentes sur toutes les phases de la vie du produit envisagé ;
- une analyse systématique et aussi exhaustive que possible du besoin et sa traduction en termes de fonctions ;
- une réflexion approfondie sur l'importance relative des fonctions ;
- une définition pertinente des critères d'appréciation de chaque fonction ;
- une évaluation des niveaux estimés nécessaires pour chaque critère d'appréciation (qualité, performances, etc.).

Les spécifications du système ont pour but d'établir une première description du futur système. Pour la réalisation des spécifications, le constructeur système doit disposer comme données d'entrées des résultats de l'analyse des besoins et des considérations techniques et de faisabilité. En phase de spécification, il est nécessaire de recenser toutes les exigences liées à la fiabilité du système :

1. exigences qualitatives :
   - listes d'événements redoutés, classification des défaillances ;
   - définition des modes dégradés et des conditions de passage entre modes, comportement dans chacun des modes ;
   - type de fautes à considérer et stratégie de tolérances aux fautes ;
   - méthodes à employer et normes à respecter ;
2. exigences quantitatives :
   - probabilité de bon fonctionnement ;
   - durée de fonctionnement ;
   - MTTF (ou MTBF) ;
   - taux de défaillance ;
   - taux de réparation.

Les principales méthodes utilisées pour fiabiliser un système dès la phase de l'analyse/spécification du cycle de développement sont : l'Analyse Préliminaire des Risques (APR), l'Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticités (AMDEC), le Diagramme de Fiabilité (DF), les Arbres de Défaillances (AdD), la Méthode de l'Espace des États (MEE), les Réseaux de Petri (RdP), les Arbres d'Événement (AE), la Méthode des Combinaisons de Pannes Résumées (MCPR), etc.

Certaines de ces méthodes sont présentées dans le paragraphe 2.3. Pour le reste des méthodes, le lecteur peut les retrouver en annexe.

2.2.1.2 Phase de conception

Dans cette phase, la démarche SdF commence par une analyse préliminaire de risques du système, afin d'identifier les fonctions et les composants à risque. Cette analyse permettra de prendre en compte les nécessités d'isoler les parties à risques dans le choix de l'architecture.

La démarche repose essentiellement sur une analyse prévisionnelle des risques dont le but est d'identifier les parties critiques du système complexe et les actions pour réduire les risques associés.

L'analyse des risques peut être réalisée au moyen d'une analyse inductive ou d'une analyse déductive. L'analyse inductive correspond à une approche montante, où l'on identifie toutes les combinaisons d'événements élémentaires possibles qui entraînent la réalisation d'un événement unique indésirable. Pour l'analyse déductive la démarche est inversée, puisque l'on part de l'événement indésirable et l'on recherche ensuite par une approche descendante toutes les causes possibles [107]. Ces analyses qui s'appuient sur la description

du système sont dites techniques d'analyse statique. Des techniques d'analyse dynamique sont également utilisées en complément.

Ces analyses se déroulent en parallèle et en liaison étroite avec les activités d'analyse/spécification et de conception, de manière continue et itérative.

L'analyse statique nécessite de disposer en entrée :

- des événements redoutés pour le système ;
- d'une description du système (au niveau de spécifications, puis au niveau de l'architecture, afin de comprendre les interactions entre les différents sous-systèmes).

Ces analyses mettent en évidence les scénarios susceptibles de conduire à la réalisation d'un événement redouté. A partir de ces scénarios, des actions de réduction des risques sont ensuite identifiées, telles que :

- la spécification des modes de fonctionnement dégradé pour supprimer ou diminuer la gravité des conséquences du dysfonctionnement considéré. La spécification de ces modes de fonctionnement dégradé doit être cohérente avec les exigences de tolérance aux fautes ;
- les études complémentaires spécifiques visant à démontrer l'improbabilité du risque (modélisation, simulation) ;
- l'identification d'essais de validation spécifiques visant à démontrer que le scénario ne va pas se produire ;
- les contraintes sur l'architecture matériel et logiciel ;
- les contraintes sur la testabilité et l'observabilité en opération ;
- l'implantation de mécanismes de détection et de traitement de défauts ;
- le choix de conception minimisant les risques (choix d'architecture, de structures de données, etc.) ;
- l'identification de tests permettant de démontrer l'efficacité des mécanismes implémentés.

Une analyse dynamique du comportement d'un système, la modélisation dynamique permet de vérifier des propriétés supplémentaires de cohérence, de complétude, etc. Elle permet aussi de tester les modes dégradés du système et l'efficacité des techniques de tolérance aux fautes. Les analyses dynamiques ou de performances permettent de mettre en évidence des problèmes de :

- définition incorrecte ou incomplète des modes de fonctionnement ou des transitions entre modes et donc des spécifications ;
- dimensionnement et partage de ressources ;
- synchronisation des traitements et des entrées/sorties ;
- ordonnancement des tâches ;

– protocole de communication.

Ce type de modélisation est surtout utile pour aider ou valider le choix entre plusieurs développements possibles.

Les principales méthodes utilisées pour fiabiliser un système dès la phase de la conception du cycle de développement sont : l'Analyse Préliminaire des Risques (APR), l'Analyse des Modes de Défaillance, de leur Effets et de leurs Criticités (AMDEC), le Diagramme de Fiabilité (DF), les Arbres de Défaillances (AdD), la Méthode de l'Espace des Etats (MEE), les Réseaux de Petri (RdP), les Arbres d'Événement (AE), la Méthode des Combinaisons de Pannes Résumées (MCPR), la Méthode de Diagramme Causes-Conséquences(MDCC), etc.

2.2.2 Les méthodes actuelles de validation dans la partie Vérification & Validation

Les activités de V&V sont des activités continues et mises en place dès le début du projet, afin de détecter au plus tôt les risques de non fiabilité et s'assurer que les dispositions prises et les analyses effectuées répondent aux exigences définies.

Un manque de fiabilité constaté en phase finale du développement peut être irrémédiable pour le système.

Pendant les activités de V&V d'un système, effectuées dans les étapes montantes du cycle en V, la fiabilité a un impact sur :

– la confirmation des choix effectués lors des activités de construction dans les étapes analyse/spécification et conception ;
– la vérification de l'efficacité des dispositions prises, par des actions spécifiques, notamment lors des étapes de validation du système complexe ;
– la finalisation des principes liés à l'exploitation opérationnelle du système en s'assurant de l'efficacité des moyens et procédures mis en place pour le diagnostic et/ou les reconfigurations.

2.2.2.1 Phase de vérification

La vérification exhaustive du comportement du système est souvent impossible, car elle se heurte aux limites des outils existants.

La vérification consiste en des essais et des tests au niveau module (unitaire) et au niveau système (intégration).

La vérification au niveau module (unitaire) entraîne :

– l'exécution de l'ensemble des tests unitaires définis et la vérification de la conformité des résultats obtenus aux objectifs ;
– l'exécution des tests des mécanismes relatifs à la fiabilité ;
– l'évaluation de la robustesse des modules du système.

La vérification au niveau module système (intégration) entraîne :

– l'exécution de l'ensemble des tests d'intégration définis et la vérification de la conformité des résultats obtenus aux résultats attendus ;
– l'exécution des tests des mécanismes inter-modules relatifs à la fiabilité ;
– l'évaluation de la robustesse des interfaces entre modules système.

Dans cette phase, les méthodes d'évaluation de la fiabilité sont peu nombreuses : la Méthode de l'Espace des États (MEE), les Réseaux de Petri (RdP) ou la Table de Vérité (TV).

2.2.2.2 Phase de validation

La validation du système est prononcée à la suite de :

– l'exécution de l'ensemble de tests de validation définis et la vérification de la conformité des résultats obtenus aux résultats attendus ;
– l'évaluation du taux de couverture fonctionnelle ;
– l'exécution des tests de robustesse du système (incluant les cas de fonctionnement dégradé du système) ;
– la conformité aux exigences de fiabilité du système ;
– l'évaluation de la robustesse du système et du niveau de fiabilité atteint.

L'évaluation de la fiabilité d'un système vis-à-vis des fautes physiques affecte ses composants matériels en phase opérationnelle. Cette évaluation repose sur une analyse basée sur la structure du système, de l'influence des probabilités de défaillance de ses composants sur la probabilité de défaillance globale du système.

La démarche consiste alors à observer le comportement du système considéré et à effectuer les traitements statistiques sur les données relatives aux défaillances observées.

La collecte des données de défaillance est déterminante dans une telle démarche et elle doit être prévue dès le début du projet.

Pour que ces relevés de défaillance puissent être utiles, il est important que l'utilisation du système soit la plus représentative possible des conditions de sollicitation réelle du système dans son environnement opérationnel. L'objectif principal de cette observation est d'évaluer le niveau de fiabilité du système dans les conditions d'utilisation prévues.

Pour obtenir une bonne étude statistique, il est nécessaire de recueillir un nombre suffisant de données, afin d'en déduire la ou les lois de modélisation les plus proches de

ce que l'on a pu constater pendant la période de temps considérée.

Les méthodes d'évaluation de la fiabilité utilisées dans cette phase sont les même que pour la phase de validation : la Méthode de l'Espace des États (MEE), les Réseaux de Petri (RdP) ou la Table de Vérité (TV).

2.3 Présentation des méthodes qualitatives

Comme nous l'avons déjà cité dans le chapitre précédent (chapitre 1), les systèmes mécatroniques sont difficiles à étudier à cause des différents composants et domaines qui interagissent entre eux. Pour l'étude de sûreté de fonctionnement de ces systèmes il est, donc, important de bien connaître le système à étudier dès la phase de conception.

Pour cela, il est nécessaire d'effectuer tout d'abord une analyse qualitative [52] comme montré sur la figure 1.2 qui représente les différentes étapes de la démarche systémique à suivre pour l'étude des systèmes complexes. Cette analyse qualitative a pour objectif l'identification de toutes les causes de défaillance pouvant affecter le bon fonctionnement d'un système. Les scénarios redoutés sont caractérisés par des changements d'états et des enchaînements d'événements qui conduisent le système vers un état dit redouté [102, 67, 82].

L'analyse qualitative est généralement précédée par une analyse fonctionnelle [73]. Une première analyse fonctionnelle, dite externe (AFE), nous permet de connaître les relations entre le système mécatronique étudié et son milieu extérieur, et de définir les limites matérielles du système, ses différentes fonctions de service et opérations réalisées ainsi que ses diverses configurations d'exploitation.

L'AFE est complétée par une analyse fonctionnelle interne (AFI) permetant d'obtenir une décomposition arborescente et hiérarchique du système mécatronique étudié en éléments matériels et/ou fonctionnels, et aussi de déterminer toutes les fonctions techniques du système.

Ces analyses fonctionnelles interne et externe ne nous donnent, cependant, aucune information concernant les défaillances, d'où 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.

2.3.1 Analyse fonctionnelle

Les techniques de l'analyse fonctionnelle ont été appliquées à partir des années 60 dans le domaine industriel, pour la conception dans le secteur aéronautique, spatiaux et

nucléaire pour prendre en compte les attentes des utilisateurs ainsi que les paramètres de fiabilité, de maintenabilité, de disponibilité, de sécurité et de sûreté du système.

L'analyse fonctionnelle permet la description synthétique des modes de fonctionnement d'un système et la connaissance des fonctions à garantir. Elle établit de façon systématique et exhaustive les relations fonctionnelles à l'intérieur et à l'extérieur de ce système. En d'autres termes, l'analyse fonctionnelle consiste à rechercher et à caractériser les fonctions offertes par un système pour satisfaire les besoins de son utilisateur [82, 65, 93].

Selon la norme NF X50-150, une fonction est définie comme les actions d'un produit ou de l'un de ses constituants exprimées en terme de finalité. Au sens de la même norme, l'analyse fonctionnelle est alors définie comme une démarche qui consiste à recenser, ordonner, caractériser, hiérarchiser et/ou valoriser les fonctions [82].

Les concepts fondamentaux introduits dans les méthodes d'analyse fonctionnelle sont : [106]

- La description du besoin de l'utilisateur par rapport à un système en terme de fonctions à garantir ;
- La description des choix technologiques imposés au système en terme de contraintes ;
- La description du système en terme de fonctions de service ou d'usage (satisfaction du besoin) et de fonctions de contraintes (solutions techniques retenues qui répondent aux contraintes) ;
- L'optimisation du besoin sur le plan économique et technique.

La réalisation d'une analyse fonctionnelle se déroule en trois principales étapes (figure 2.3) :

1. L'analyse fonctionnelle externe qui a pour objectif de formaliser et de valider l'analyse du besoin. Le système est considéré comme une boîte noire recevant des entrées et fournissant des sorties ;
2. L'analyse fonctionnelle interne permet d'identifier les fonctions techniques et les solutions technologiques nécessaires pour la réalisation de la boîte noire ;
3. L'optimisation du couple besoin/produit.

La figure 2.3 représente les principales étapes, citées précédemment, de l'analyse fonctionnelle qui illustre les deux types d'analyse fonctionnelle l'AFE et l'AFI. Après ces deux analyses et l'optimisation du couple besoin/produit, le système est réalisé si les objectifs sont atteints.

De nombreux outils ont été développés pour la réalisation de l'analyse fonctionnelle et, pour la plupart, ils peuvent s'adapter aux domaines biologiques, mécatroniques, pharmaceutiques, médicales, etc [65]. Voici quelques méthodes utilisées pour l'analyse fonction-

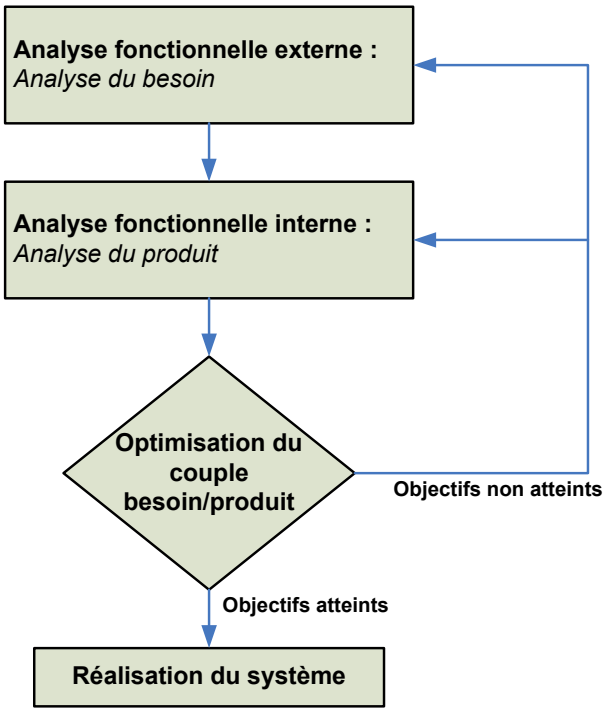

FIGURE 2.3 – Démarche générale de l'analyse fonctionnelle

nelle d'un système.

2.3.1.1 Analyse fonctionnelle externe (méthode APTE)

Le cabinet conseil APTE a développé une méthode d'analyse de la valeur appliquée à l'organisation des entreprises et à la rédaction des frais généraux [107]. C'est une des méthodes les plus utilisée en sûreté de fonctionnement et elle est généralement employée en vue d'une analyse AMDE ultérieure.

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

1. La mise en évidence du besoin à satisfaire en utilisant un formalisme nommée *bête à cornes* (figure 2.4) ;
2. La recherche des milieux extérieurs ;
3. La détermination des fonctions principales et des fonctions de contraintes ;
4. La contribution d'un schéma général de raisonnement permettant de faire apparaître les lignes de flux.

Les fonctions de base sont déduites après une étude des milieux extérieurs. Cette étude met en relation le système et ses milieux extérieurs. Chaque fonction devra être validée.

Sur la figure 2.4 qui 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

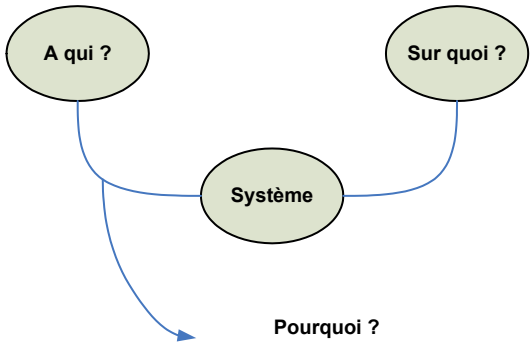

FIGURE 2.4 – Formalisation du besoin par une *bête à cornes*

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.

Après la formalisation du besoin, il est important d'établir les relations entre le système et les éléments de son milieu extérieur. Pour cela on utilise le schéma de la *Pieuvre* comme montré sur la figure 2.5. (FP : Fonction Principale, FC : Fonction de contrainte).

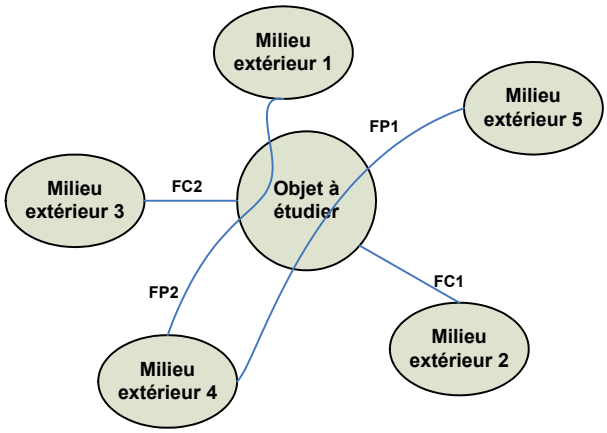

FIGURE 2.5 – Schéma de la Pieuvre

Comme le montre la figure 2.3, l'Analyse Fonctionnelle Interne (AFI) constitue la deuxième étape de la démarche générale de l'analyse fonctionnelle. Voici quelques méthodes utilisées dans l'AFI.

2.3.1.2 Structured Analysis and Design Technique (SADT)

Bien plus qu'une méthode d'analyse, SADT est un langage pluridisciplinaire, qui cherche à favoriser la communication entre les utilisateurs et les concepteurs. C'est une méthode d'analyse et de conception des systèmes développée en 1977 par *Douglas T.Ross* fondateur de la société américaine Softech. C'est essentiellement une méthode de représentation structurée conçue à partir de concepts simples, et basée sur un formalisme

graphique et textuel facile à apprendre. Elle consiste à considérer tout système complexe comme une structure composée de systèmes plus simples en interaction [105, 49, 64].

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 boîtes afin d'éviter que le diagramme soit trop complexe. La méthode propose deux formes de représentation (actigramme et datagramme).

Un actigramme représente une activité par un verbe dans une boite alors que le datagramme identifie une donnée par un nom dans une boite. Nous nous intéresserons uniquement aux actigrammes plus utilisés et mieux adaptés à une approche fonctionnelle [17, 97, 107].

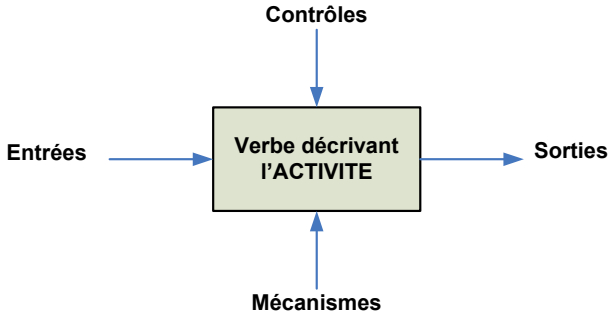

FIGURE 2.6 – Actigramme

La figure 2.6 représente une boîte 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.

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 paraît suffisant.

La méthode SADT est une méthode de spécification d'un système. Cependant, il nous est indispensable de représenter l'aspect dynamique d'un système mécatronique. C'est pourquoi on comble cette lacune de la méthode SADT par l'utilisation de la méthode SA-RT qui est une méthode de spécification dynamique d'un logiciel. La méthode SA-RT est présentée ci-dessous.

2.3.1.3 Structured Analysis - Real Time (SA-RT)

L'accroissement très important de la taille des logiciels développés dans les années 70 a conduit à mettre en place des méthodes d'analyse et de conception permettant une meilleure réalisation et aussi une maintenance plus efficace dans l'exploitation des logiciels. Par conséquent, une extension temps réel a été proposée à la méthode d'analyse structurée par Paul Ward et Stephen Mellor en 1985, ce qui a donné naissance à la méthode SA-RT qui est l'une des méthodes d'analyse structurée de logiciel pour les applications temps réel les plus utilisées dans le monde [24, 49]. C'est une méthode d'analyse fonctionnelle et opérationnelle qui permet de réaliser une description graphique et textuelle de l'application en termes de besoins.

Une première étape extrêmement importante est le diagramme de contexte qui va définir le contexte et l'environnement extérieur du système. Nous pouvons considérer cette étape comme le contrat de réalisation entre le concepteur et son client.

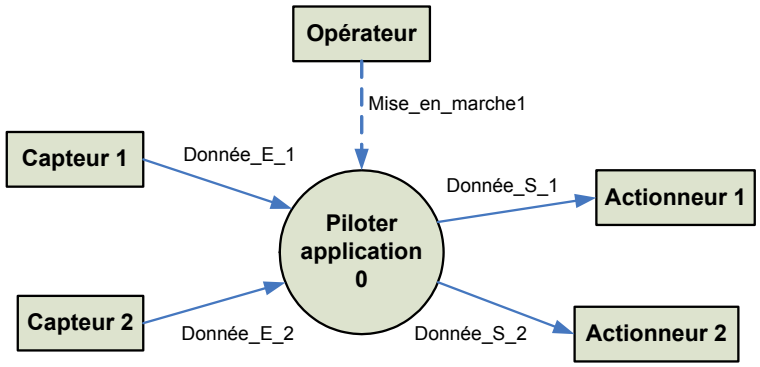

FIGURE 2.7 – Diagramme de contexte de la méthode SA-RT

La figure 2.7 représente un exemple d'un diagramme de contexte de la méthode SA-RT sur lequel un seul processus fonctionnel *Piloter l'application* est présent, numéroté 0 et qui traduit l'application à réaliser par le concepteur. On distingue deux données d'entrée ou capteurs et deux données de sortie ou actionneurs. Il est souvent nécessaire d'ajouter un événement de démarrage lié à l'opérateur qui est la *mise-en-marche*.

La deuxième étape représente le diagramme préliminaire qui constitue une décomposition du processus fonctionnel initial 0 et ne contient qu'un seul processus de contrôle. Pour avoir une meilleure lisibilité, le nombre de processus fonctionnels, composant ce diagramme préliminaire, doit être limité à 9 maximum.

La figure 2.8 représente une décomposition du diagramme de contexte illustrée sur la figure 2.7. Cette analyse fait apparaître trois processus fonctionnels de base (1,2,3) et un processus de contrôle (4) permettant de séquencer l'ensemble. L'événement *E/D* est

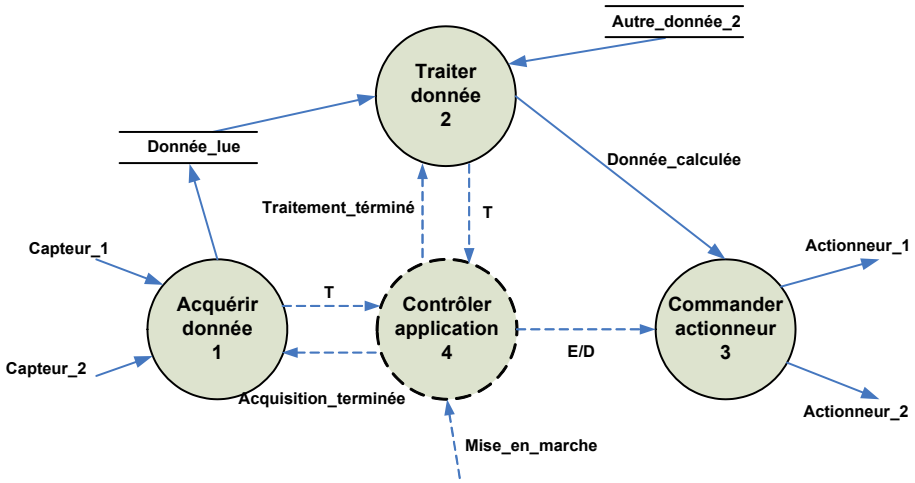

FIGURE 2.8 – Diagramme préliminaire de la méthode SA-RT

utilisé pour piloter un processus fonctionnel de type *Boucle sans fin* et l'événement T est utilisé pour activer un processus fonctionnel de type *début-fin*.
E (Enable) : pour indiquer un flot de contrôle d'activation, D (Disable) : pour un flot de désactivation et T (Trigger) : pour un flot de déclenchement.

On distingue dans cette figure deux processus fonctionnels supposés de type *début-fin*. Ils sont activés l'un après l'autre par le processus de contrôle par un événement T et envoient à leurs tour un événement de fin d'exécution vers ce même processus de contrôle. Le troisième et dernier processus fonctionnel, activé par un événement E/D, est lié à la commande des actionneurs qui doit être faite en continu, c'est-à-dire de type *Boucle sans fin*.

La troisième étape dans la réalisation de la méthode SA-RT consiste à construire un diagramme état/transition qui explique le fonctionnement du processus de contrôle. Reprenons l'exemple du diagramme préliminaire de la figure 2.8 qui représente la coordination d'un système acquisition-traitement-commande par un processus de contrôle.

La figure 2.9 représente un diagramme état/transition du processus de contrôle du diagramme préliminaire tracé sur la figure 2.8.

A partir de la méthode SA-RT, nous pouvons avoir une traduction ou une correspondance avec les réseaux de Petri. Cette correspondance sera illustrée dans la partie consacrée à la méthodologie.

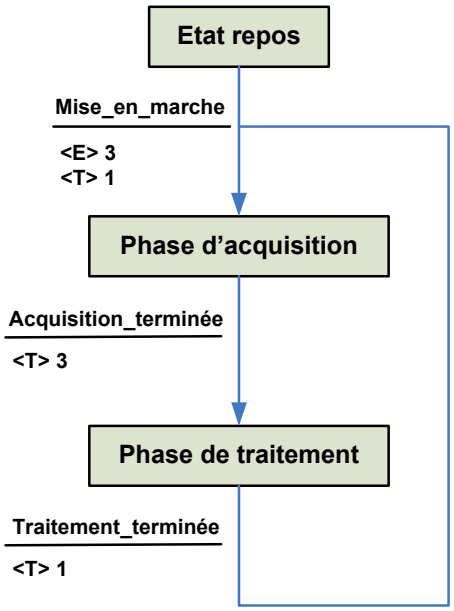

FIGURE 2.9 – Représentation du diagramme état/transition du processus de contrôle

2.3.2 Analyse dysfonctionnelle qualitative

L'analyse fonctionnelle précédemment étudiée, n'apporte aucune information sur les défaillances potentielles que peut rencontrer un système mécatronique. Pour cette raison l'utilisation de l'analyse dysfonctionnelle est nécessaire dans le but de nous fournir ces informations manquantes. Ceci nous permet de déterminer les causes de défaillance ainsi que de spécifier les différents états du système.

2.3.2.1 Analyse des Modes de Défaillance et de leur Effets (AMDE)

L'AMDE est la méthode la plus utilisée et est devenue le symbole de la sûreté de fonctionnement. Elle est née dans l'industrie aéronautique américaine au début des années 60 et prend un nouvel essor dans les années 70 lorsque certaines industries européennes la récupèrent et y ajoutent la notion de criticité pour arriver à l'AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) [77, 102, 107, 39, 40].

C'est une méthode inductive qui part des défaillances élémentaires des composants pour en déduire ce qui en résulte. Elle est destinée à prévenir les défaillances potentielles d'un système. Pour cela, elle s'appuie sur une analyse méthodique des risques potentiels qui permet de les hiérarchiser afin de traiter les plus importants de manière préventive.

Cette méthode prend toute sa valeur quand elle est appliquée dès la conception des systèmes. Elle permet alors de gérer au mieux les risques liés à leur utilisation.

L'AMDE s'applique au produit d'un fabricant dans le but d'améliorer la conception

de ce produit et d'avoir la meilleure satisfaction possible des exigences du client. Elle s'applique aussi au processus de fabrication ainsi qu'à chacun des moyens de production.

Le principe de l'analyse AMDE est présenté sur la figure 2.10 :

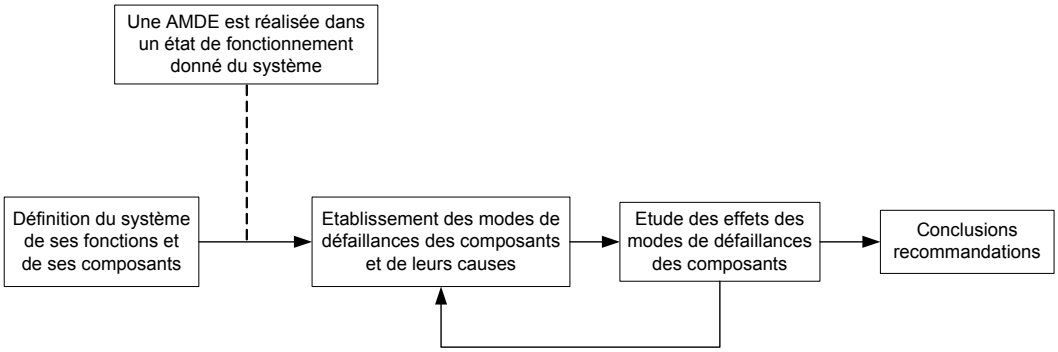

FIGURE 2.10 – Étapes de l'élaboration de l'AMDE

L'élaboration de l'AMDE, comme le montre la figure 2.10, est réalisée en quatre étapes qui sont présentées ci-dessous :

- décomposition du système en composants ;
- recensement des modes de défaillance des composants ;
- effets et conséquences des modes de défaillance des composants ;
- risques découlant des défaillances des composants.

Dans un premier temps, il est important de décomposer le système en éléments plus petits. Cette décomposition doit être assez fine pour savoir identifier tous les modes de défaillance attachés à chaque élément. Cette première étape aboutit donc à une liste de composants à laquelle on associe différents modes de défaillance possibles.

Dans un deuxième temps, il est nécessaire de décrire ce qui va se passer dans le système quand le mode de défaillance étudié est apparu. On doit indiquer, dans cette partie, les effets vue de l'extérieur du système ainsi que les effets sur l'accomplissement des fonctions du cahier des charges. Ce travail d'analyse est généralement présenté dans des tableaux comme celui présenté ci-dessous :

Composant	Modes de défaillance	Causes	Effets

TABLE 2.1 – Tableau de l'AMDE

Pour finir une analyse AMDE, il est important de faire une synthèse structurée selon les besoins pour lesquels l'AMDE doit répondre et en même temps, ne rien perdre de ce que l'analyse a mis en valeur.

L'AMDE est particulièrement pertinente lorsqu'elle est appliquée aux systèmes mécaniques et/ou électroniques, ce qui n'est pas le cas lorsqu'elle est appliquée au logiciel. Il existe donc une méthode spécifique à ce dernier et qui a été développée dans l'esprit de l'AMDE et qui s'appelle l'AEEL (Analyse des Effets des Erreurs du Logiciel).

2.3.2.2 Analyse des Effets des Erreurs du Logiciel (AEEL)

L'AEEL est une analyse de risque issue d'une adaptation de l'AMDE au niveau du logiciel car on parle d'erreurs du logiciel et non pas de modes de défaillance [39, 81].

Cette analyse a pour but d'exposer aux concepteurs les points critiques identifiés et de permettre aux personnes chargées de la validation d'affiner leur démarche.

Le principe de l'AEEL, tout comme l'AMDE, consiste à observer les effets d'une erreur dans un logiciel. Cette analyse doit être entreprise dès la phase de conception afin que les propositions de modification du logiciel soient prises au plus tôt.

Le tableau 2.2 présente un exemple de formulaire d'AEEL :

Module	Erreurs	Effets sur le module	Effets sur le système

TABLE 2.2 – Tableau de l'AEEL

Cette analyse dysfonctionnelle termine l'étape de l'analyse qualitative et nous permet d'entamer la partie de la modélisation dynamique et de l'analyse quantitative.

2.4 Présentation des méthodes de modélisation dynamique

Parmi les étapes de la démarche systémique illustrée sur la figure 1.2, on retrouve, après l'analyse qualitative, la modélisation dynamique. Cette étape nous permet de construire un modèle dynamique qui représente le système étudié et qui se rapproche le plus possible de la réalité et de l'aspect dynamique des systèmes mécatroniques.

2.4.1 Modèles de fiabilité des systèmes mécatroniques

Une particularité caractérisant de nombreux systèmes industriels est que leurs comportements varient en fonction du temps en raison des interactions entre les composants de ce système ou avec l'environnement. On parle donc de systèmes dynamiques. Chaque comportement du système est défini par les lois de la physique qui lui sont propres. Le

passage d'un comportement à un autre peut être dû à plusieurs causes : l'intervention humaine, l'action de l'organe de contrôle agissant sous l'influence des variables physiques qui décrivent l'état du système, une discontinuité propre au système ou encore une défaillance de composant.

En plus de l'hybridité (continu + événements discrets), il faut aussi tenir compte du caractère stochastique du système imposé par les défaillances des composants ou par les incertitudes sur la connaissance du système [14, 15, 16].

Comme nous l'avons déjà défini dans le chapitre 1, les systèmes mécatroniques sont des systèmes constitués de composants mécaniques, électroniques et logiciels. Ils peuvent être décomposés en quatre entités en interaction : les capteurs, la partie opérative, le système de commande et de reconfiguration et les actionneurs.

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 actionneur agissent sur la partie opérative.

Le système de commande a 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 pour ramener les grandeurs caractéristiques de celle-ci dans les limites permises. Ainsi, pour ce type de système, la sécurité est assurée par des reconfigurations sans interruption de la mission. Ces systèmes sont donc des systèmes à reconfiguration dynamique.

2.4.2 Méthodes de fiabilité dynamique

Pour aborder la problématique que pose l'évaluation de la fiabilité dynamique d'un système, plusieurs méthodes sont couramment utilisées pour modéliser les différents états de fonctionnement et de dysfonctionnement d'un système dynamique.

2.4.2.1 Fiabilité dynamique

La fiabilité dynamique est l'évaluation prévisionnelle de la fiabilité d'un système dont la structure fiabiliste évolue dans le temps. On peut dire que la fiabilité dynamique est le problème de l'évaluation probabiliste de la défaillance d'un système dynamique hybride [14, 15, 16, 23, 85].

Ainsi, le système évolue entre plusieurs états discrets, chacun d'eux étant caractérisé par une évolution propre au cours du temps des variables physiques, décrites par

un système d'équations différentielles dont les coefficients sont propres à cet état du système. C'est ce qu'on appelle un modèle de fiabilité dynamique qui permet de prendre en compte des modélisations hybrides, c'est-à-dire, d'étudier des phénomènes dans lesquels interagissent des variables discrètes et continues.

Les systèmes dynamiques hybrides sont caractérisés par la présence de phénomènes continus et d'événements discrets (franchissement de seuils, séquence d'événements, ou combinaison des deux, etc.). La description de ces systèmes peut faire intervenir explicitement et simultanément un état continu X(t) et un état discret Q(t). On peut ajouter que certaines de ces variables peuvent présenter un caractère aléatoire (perturbation d'une variable continue, défaillance d'un composant, etc.)[14, 12].

On entend par fiabilité dynamique, l'évaluation prévisionnelle de la fiabilité d'un système dont la structure fiabiliste évolue dans le temps. Cette fiabilité peut donc s'écrire sous la forme suivante :

$$R_S(t) = \mathrm{P}\left[f_S(t, X, Q, U) = 1\right]_{[0,t]} \tag{2.26}$$

L'équation 2.26 exprime que la fiabilité d'un système R_S se mesure par la probabilité que le système fonctionne pendant un intervalle de temps [0,t]. f_S est la fonction de structure du système qui vaut 1 si le système fonctionne et 0 dans le cas contraire, X et Q les vecteurs d'état continu et discret, U le vecteur état de fonctionnement des composants.

Le calcul de cette fiabilité dynamique n'est pas simple et plusieurs problèmes sont à considérer :

- Le premier problème à considérer dans le calcul de la fiabilité dynamique d'un système est de prendre en compte, de façon réaliste et effective les interactions dynamiques existant entre les paramètres physiques et le comportement fonctionnel ou dysfonctionnel des composants du système lui-même. Cela signifie qu'il y a deux types d'événements : les premiers sont liés à l'évolution déterministe du système (les variables physiques) et les seconds sont liés aux sollicitations ou aux défaillances des composants du système. Ces derniers sont généralement de nature probabiliste.
- Le deuxième problème (parfois lié au précédent) consiste à prendre en compte le temps et notamment l'ordre d'occurrence des événements notamment des défaillances. Cela permettra la construction des différents chemins critiques représentant l'évolution du système vers des états non désirés ou dangereux.
- Le troisième problème est la complexité de la formulation mathématique de la fiabilité dynamique. Le calcul de cette fiabilité dynamique nécessite l'intégration dans le modèle de fiabilité des interactions entre les phénomènes de défaillance et le

processus physique. Une formulation mathématique rigoureuse de la fiabilité dynamique impliquerait de connaître l'expression analytique des variables évoluant dans le temps, puis d'exprimer les grandeurs de sûreté de fonctionnement recherchées en fonction de toutes ces variables. Cela demande un effort considérable pour développer les modèles physiques appropriés pour chaque configuration. Il est parfois nécessaire de connaître le comportement physique du système associé à chaque état de défaillance des composants [87]. La transcription mathématique complète du processus stochastique en un système d'équations différentielles devient vite impossible car sa dimension est infinie. Par discrétisation du modèle continu, on peut réduire la complexité pour obtenir une solution, mais on doit trouver un compromis entre temps de calcul et précision des résultats.

– Pour surmonter cette difficulté et en l'absence de solution analytique, on ne peut que recourir à la simulation. Le quatrième problème consiste à intégrer, dans une même simulation, le comportement continu et discret d'une part, déterministe et stochastique d'autre part. Quelques méthodologies utilisent deux simulations, l'une qui contient l'aspect numérique et l'autre le code pour coupler les comportements probabilistes et physiques du système. Pour cela, il est bien sûr important de réduire le temps de calcul.
– Le cinquième problème, problème plus complexe, consiste à prendre en compte les défaillances progressives des composants dues à l'usure.

2.4.2.2 Chaînes de Markov

Les chaînes de Markov ou Méthode de l'Espace des États (MEE) ont été développés dans les années 50 pour l'analyse de fiabilité des systèmes réparables [102, 107, 82].

Cette méthode consiste à représenter le comportement d'un système par un ensemble de composants pouvant se trouver dans un nombre fini d'états de fonctionnement et de panne. Un support graphique appelé *graphe des états*, permet de visualiser les différents états d'un système qui sont représentés par des cercles et relier entre eux par des arcs orientés qui représentent la transition d'états de départ vers des états d'arrivée. Un modèle Markovien est présenté sur la figure 2.11 :

Pour effectuer cette analyse, il est indispensable dans un premier temps de recenser et de classer tous les états du système (fonctionnement ou panne) et chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une réparation. A chaque transition, de l'état E_i vers l'état E_j, est associé un taux de transition L_{ij} défini de telle sorte que L_{ij}.dt est égal à la probabilité de passer de E_i vers E_j entre deux instants très proches t et t+dt sachant que l'on est en E_i à l'instant de temps t [67]. Enfin, la dernière étape

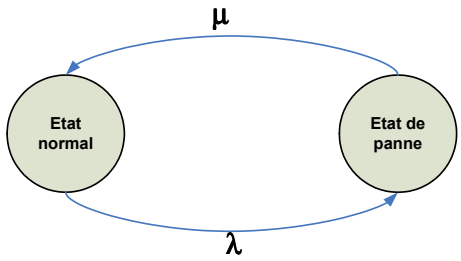

FIGURE 2.11 – Un modèle Markovien

consiste à calculer les probabilités d'apparition des différents états du système ainsi que les caractéristiques de sûreté de fonctionnement (MTTF, MTBF,MTTR, etc.) [102, 44].

Les **Processus Markoviens Déterministes par Morceaux** sont présentés dans le but de surmonter les difficultés de la fiabilité dynamique : le système suit une trajectoire déterministe, décrite par exemple à travers une équation différentielle ordinaire, jusqu'à un premier temps de saut arrivant soit spontanément de manière aléatoire, soit quand la trajectoire atteint un seuil. A partir de cet instant, un nouveau point est sélectionné à travers un opérateur aléatoire et le processus repart de ce nouveau point. Entre deux sauts le système suit une trajectoire déterministe. Alors, il existe deux types de saut : déterministes, par exemple dus à un changement de mode de fonctionnement par le franchissement d'un seuil et stochastiques modélisant les défaillances de composants ou les entrées qui modifient le mode de fonctionnement du système [35].

La modélisation avec les graphes de Markov permet de prendre en compte les dépendances temporelles et stochastiques plus largement que les méthodes classiques. En dépit de leur simplicité conceptuelle et leur aptitude à pallier certains handicaps des méthodes classiques, les graphes de Markov souffrent de l'explosion du nombre des états, car le processus de modélisation implique l'énumération de tous les états possibles et de toutes les transitions entre ces états. Ce problème peut se poser même dans le cas de la modélisation du seul aspect dysfonctionnel, mais il devient un handicap énorme si on souhaite rajouter la description de l'aspect fonctionnel à celui de l'aspect dysfonctionnel. Pour surmonter ce problème, on peut alors s'orienter vers les réseaux de Petri.

2.4.2.3 Les automates

Les automates sont l'un des formalismes *états-transitions* les plus utilisés dans la description des systèmes à événements discrets. Ce formalisme a été étendu sous la forme des automates hybrides pour modéliser correctement les systèmes dynamiques hybrides. Les automates hybrides sont une extension des automates temporisés. Informellement, un automate hybride est l'association d'un automate à états finis et d'un ensemble d'équations

dynamiques continues pilotées par ce dernier.

L'automate stochastique hybride prend en compte les différents modes continus de fonctionnements du système et le passage de l'un à l'autre sur l'occurrence des événements déterministes et stochastiques. Les premiers sont produits par franchissement de seuils des variables continues, les seconds sont produits par défaillances des composants simulées par un générateur aléatoire en fonction de leurs lois de probabilités. Les dynamiques continues du système sont définit à travers des équations différentielles ordinaires [16, 8].

Un automate stochastique hybride est défini comme un 11-tuple (équation 2.27) :

$$ASH = (\chi, E, A, X, A', H, F, p, \chi_0, x_0, p_0) \tag{2.27}$$

Dans lequel :

- χ est un ensemble fini d'états discrets ;
- E est un ensemble fini d'événements ;
- A est un ensemble fini d'arcs de la forme (χ_O,e,G,R,χ_B) où :
- χ_O et χ_B sont les états origine et but de l'arc, G la condition de garde et R est la fonction de réinitialisation. Sur occurrence de e si la condition de garde G est vérifiée, le système bascule de l'état χ_O à l'état χ_B dans lequel R définit les valeurs initiales des variables continues du système ;
- X est un ensemble fini des variables réelles ;
- A' : $\chi \times X \rightarrow (\Re^+ \rightarrow \Re)$ est une fonction des *activités*, qui associe un élément de $\chi \times X$ une fonction définie sur $\Re^+$ et à valeur dans $\Re$;
- H est un ensemble fini d'horloges ;
- $F : H \rightarrow (\Re \rightarrow [0,1])$ est une application qui associe à chaque horloge une fonction de répartition de probabilité ;
- p est une distribution de probabilité de transition d'état $p(\chi_B|\chi,e)$. Par exemple, si on a le même événement e définissant les transitions de l'état discret χ_O vers les états discrets χ_B et χ_j (l'automate à état sous jacent n'est pas déterministe), on peut définir la probabilité p de passer de l'état χ_O à l'état χ_B et la probabilité $(1\text{-}p)$ de passer de l'état χ_O à l'état χ_j ;
- χ_0,x_0 *et* p_0 correspondent, respectivement, à l'état discret initial, à la valeur initiale du vecteur d'état continu et à la distribution initiale des probabilités de transition.

Les éléments χ,E et A de l'automate stochastique hybride correspondent à l'automate à états finis définissant sa partie événementielle. En revanche X et A' définissent sa partie continue. Finalement, H et p exprime son aspect temporel et stochastique.

Dans le cas de la modélisation des systèmes complexes pouvant être découpés en sous-systèmes, il est possible de construire un modèle d'automate pour chacun d'eux et

de les composer ensuite pour élaborer l'automate correspondant au système global. La composition se fait par synchronisation entre les automates des différents sous-systèmes, soit par messages, soit par variable partagées. Toutefois cette composition entre automates rend difficile l'analyse de leurs propriétés. D'où le besoin de disposer de mécanismes de structurations plus puissants offerts par des modèles de plus haut niveau.

Les relations de cause à effet menant vers l'état redouté ne sont pas représentées d'une façon claire et homogène avec les automates. En effet au sein d'un automate représentant un objet séquentiel (élément d'un produit d'automates ou d'un ensemble d'automates communicants), les relations de cause à effet sont représentées par les événements qui relient, chacun, un état origine et un état destination. Chaque événement correspond à une causalité explicite entre deux états. Par contre entre deux automates, ces relations de cause à effet sont la conséquence directe ou indirecte de synchronisations par messages ou de communication par variables partagées. L'existence d'une relation de causalité ou non dépendra de la valeur du message ou de la façon suivant laquelle la variable partagée est modifiée et testée. Cela donne une représentation non unifiée des relations de cause à effet inter et intra automates ce qui n'est pas le cas avec les réseaux de Petri.

2.4.2.4 Réseaux Bayésiens Dynamiques

Le problème de la modélisation et de l'analyse de la fiabilité dynamique se pose dès lors que l'état de fonctionnement du système et l'état des variables fonctionnelles du système lui même s'influencent mutuellement [94].Les Réseaux Bayésiens Dynamiques (DBN) semblent constituer un outil mathématique intéressant pour modéliser ce problème en permettant une représentation graphique des processus stochastiques. Ces DBN sont utilisés pour représenter l'interaction complexe entre l'état du système et l'état des variables processus, d'une part, et le processus et la perturbation externe, d'autre part. Si l'intérêt de l'approche est évident, son application à des problèmes physiques réels reste difficile [12, 94].

2.4.2.5 Réseaux de Petri

Les réseaux de Petri ont été inventés en 1962 par Carl Adam Petri [73, 52, 53]. Ils sont basés sur la théorie des automates. Ces réseaux permettent de représenter le comportement des systèmes dans les conditions de fonctionnement normal ainsi que leur comportement en cas de défaillance de leurs composants [41, 57, 25, 74, 101, 65, 69, 19, 46]. Les réseaux de Petri sont décrits par un 7-tuplé, $(P, T, A, W, M_0, Pre, Post)$, défini par :

– L'ensemble des places p_i de P, tel que $p_i \in P$, est fini et non vide ;

- L'ensemble des transitions t_i de T, tel que $t_i \in T$, est fini et non vide ;
- L'ensemble des arcs a_i de A, tel que $a_i \in A$;
- L'ensemble des poids w_i affectés aux arcs a_i, tel que $w_i \in W$, souvent égale à 1 pour les réseaux déterministes, évalué à partir de probabilité pour les réseaux stochastiques ;
- Le marquage initial M_0 avec ses jetons J. C'est le caractère dynamique du réseaux de Petri et sa capacité à supplanter les chaînes de Markov, dans son utilisation en fiabilité des systèmes ;
- $Pre(P,T)$ est l'application d'incidence avant, de type $P \times T \longrightarrow N$ correspond aux arcs allant d'une place vers une transition ;
- $Post(P,T)$ est l'application d'incidence arrière, de type $T \times P \longrightarrow N$ correspond aux arcs allant d'une transition vers une place.

Pour les fonctions avant et arrière, nous utiliserons les notations suivantes :
${}^{\circ}T_j = \{P_i \in P | Pre(P_i, T_j) > 0\}$ = ensemble des places d'entrée de T_j
$T^{\circ}{}_j = \{P_i \in P | Post(P_i, T_j) > 0\}$ = 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'entrée de P_i
$P^{\circ}{}_i = \{T_j \in T | Pre(P_i, T_j) > 0\}$ = ensemble des transitions de sortie de P_i

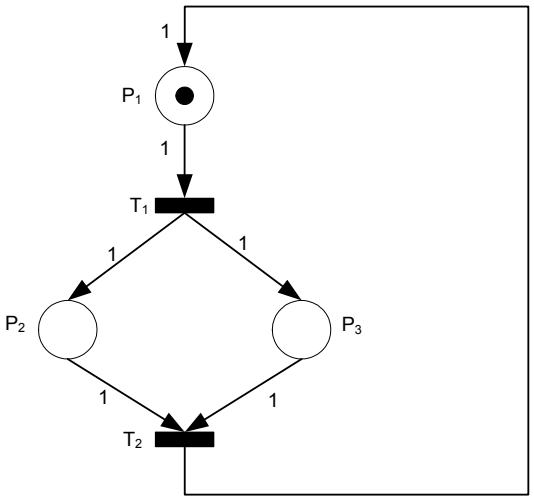

FIGURE 2.12 – Réseau de Petri

La figure 2.12 illustre un exemple d'un réseau de Petri. Le marquage de ce réseau est déterminé par le nombre de jetons $M(P)$ dans chaque place P. Le marquage initial M_0 qui correspond à l'état initial du système, s'écrit :

$$M_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \tag{2.28}$$

L'évolution du réseau de Petri est obtenue par des franchissements (tirs) de transitions. Ce franchissement n'est possible, que si chacune des transitions en amont possède un nombre de jetons correspondant au poids de l'arc qui lui est associé. Ceci génère des jetons dans les places en aval. Plusieurs transitions peuvent être sollicitées en même temps, le choix du franchissement se portera sur la transition qui a le délai le plus court.

A partir de ce marquage initial M_0, nous pouvons déterminer une séquence de franchissements. Cette séquence est une suite de transitions qui sont franchissables successivement (sans autres franchissements de transitions) [25]. Le franchissement de ces séquences conduit au passage d'un marquage à un autre, ce qui correspond au passage du système d'un état à un autre.

L'ensemble des marquages accessible à partir d'un marquage initial représente le graphe de marquage de la figure 2.13 associé au réseau de Petri de la figure 2.12.

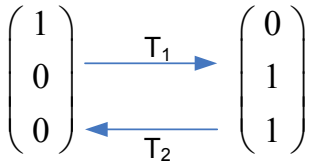

FIGURE 2.13 – Graphe de marquage

Ce graphe de marquage est composé de noeuds qui correspondent aux marquages accessibles, et d'arc correspondant aux franchissements de transitions faisant passer d'un marquage à un autre. Il nous aidera à déterminer la matrice d'incidence $W_m \times n$ équivalente au réseau de Petri (m correspond aux nombre de places et n aux nombre de transitions) qui s'écrit de la manière suivante :

$$W = W^+ - W^- = [w_{ij}] \tag{2.29}$$

$$\begin{cases} W^+ = \left[w_{ij}^+\right] = [Post\,(P_i, T_j)] \\ W^- = \left[w_{ij}^-\right] = [Pre\,(P_i, T_j)] \end{cases} \tag{2.30}$$

Considérons l'exemple de réseau de Petri traité dans la figure 2.12. Les matrices d'incidences avant et arrière s'écrivent :

$$W^- = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad W^+ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix} \tag{2.31}$$

La matrice d'incidence W est de la forme :

$$W = \begin{pmatrix} -1 & 1 \\ 1 & -1 \\ 1 & -1 \end{pmatrix} \tag{2.32}$$

Les réseaux de Petri sont très utilisés dans la modélisation des systèmes à événements discrets et dans les études de sûreté de fonctionnement des systèmes dynamiques. Ils sont caractérisés par une évolution asynchrone dans laquelle les transitions des composantes parallèles sont franchies les unes après les autres, et par une représentation explicite des synchronisations et des mécanismes d'allocation. Plusieurs extensions des réseaux de Petri ont été élaborées pour répondre à la modélisation des problèmes spécifiques et pour maîtriser la taille et la lisibilité des modèles. L'un des points forts des réseaux de Petri par rapport aux autres formalismes, repose sur ses fondements théoriques qui lui permettent de vérifier les propriétés générales d'un modèle (vivant, réinitialisable, sans blocage ou borné, etc.,) ainsi que l'accessibilité de certains marquages. Les méthodes de recherche de propriétés dans les réseaux de Petri sont basées sur l'élaboration du graphe des marquages accessibles, sur l'algèbre linéaire (calcul des invariants de places et des transitions), la réduction des réseaux ainsi que sur la logique linéaire qui permet de caractériser les relations d'ordre partiel [57, 74, 69, 19, 46, 55].

Les **réseaux de Petri stochastiques** sont obtenus à partir des réseaux de Petri classiques en associant des durées de franchissement aléatoires aux transitions. Ils permettent de prendre en compte, de manière plus structurée que les graphes de Markov, l'occurrence des défaillances et leur influence sur le comportement du système. En effet, le parallélisme étant pris en compte ils permettent d'expliciter l'architecture du système en décrivant indépendamment les états des divers objets composant le système et leurs interactions.

Une extension nommée **Réseaux de Petri Stochastiques Généralisés (RDPSG)** permet de prendre en compte, en plus de transitions avec des lois exponentielles, d'autres transitions dites *immédiates* tirées sans délai et qui sont prioritaires par rapport aux transitions à délai aléatoire.

On peut citer d'autres extensions telles que les **Réseaux de Petri Stochastiques et Déterministes (RdPSD)**. Dans ces RdPSD, les délais associés aux transitions temporisées suivent des lois de distribution exponentielle ou autre et certaines transitions sont

immédiates.

Parmi les diverses extensions des réseaux de Petri pour prendre en compte l'aspect hybride, on peut citer aussi les **réseaux de Petri de haut niveau**, les **réseaux de Petri hybrides** et les **réseaux de Petri couplés avec les équations algébro-différentielles**.

Le principal avantage des réseaux de Petri est la possibilité d'analyser le comportement d'un système en présence de défaillances. Cette modélisation dynamique permet d'obtenir des mesures en terme de fiabilité, en assignant des valeurs numériques aux paramètres du modèle. Un réseau de Petri permet de modéliser d'une part le fonctionnement normal d'un système et d'autre part les occurrences de défaillances [69].

Il existe d'autre méthodes pour aborder la problématique que pose l'évaluation de la fiabilité dynamique. Ces méthodes sont présentées en annexe.

2.4.3 Fiabilité des composants

Dans la paragraphe précédent, nous avons présenté plusieurs méthodes de fiabilité dynamique. Toutes nécessite de connaître l'architecture du système (fonctions, composant, etc.), une description physique du fonctionnement et les différentes modalité de dysfonctionnement. La plupart du temps, le dysfonctionnement du système est provoqué par la défaillance de un ou plusieurs composants. Aussi, nous présentons dans la suite de ce paragraphe les différent mécanismes de défaillance, les lois statistiques applicables et les moyens d'obtenir les paramètre de ces lois.

Les systèmes mécatroniques sont des systèmes complexes qui regroupent différentes technologies. Voilà pourquoi notre intérêt se porte, dans cette partie, sur la fiabilité des différents types de composants qui constituent le système mécatronique.

2.4.3.1 Rappels sur les fondements de la fiabilité

Très tôt, de grandes entreprises ont montré un grand intérêt pour la fiabilité : General Motors, depuis les années 1940, la NASA, le Department of Defense au Etats-Unis, depuis les années 1950, Airbus, Air Force, Bell Telephone Laboratoires, depuis les années 1960, Thomson, Philips, Kodak, Citroën, ... depuis les années 1970 [102].

La recherche de la diminution du coût des défaillances en exploitation a entraîné une augmentation des exigences de fiabilité sur les systèmes. Ainsi, en 1995, General Electric a estimé que les coûts de non-fiabilité représentaient de 8 à 12 milliards dollars et a décidé d'augmenter le niveau de qualité de ses produits dans le cadre de la politique Six Sigma.

La maîtrise de la fiabilité d'un système représente un enjeu économique important pour toute entreprise. La mesure de cette grandeur est un premier pas indispensable vers

sa maîtrise.

La fiabilité recouvre de multiples aspects : l'analyse de défaillance des systèmes, la fiabilité prévisionnelle, les banques de données de fiabilité, les essais de fiabilité, la fiabilité opérationnelle, les méthodes prévisionnelles de fiabilité et de sécurité, l'assurance de la fiabilité et de la qualité [102].

2.4.3.2 Mécanisme de défaillance

En ce qui concerne l'origine de la défaillance, les causes de défaillances prennent naissance pendant leur conception et leur production pour le matériel et également pour le logiciel. Outre les manipulations et les défauts de conception et de fabrication, les causes de défaillances pour un matériel en utilisation sont aussi dues aux phénomènes de dégradations. Si contrairement au matériel, le logiciel n'est pas soumis aux contraintes de dégradations, le phénomène de vieillissement du logiciel se traduit non pas par un changement de ses performances intrinsèques, mais par un changement de son environnement. Il s'agit en l'occurrence de la contrainte *durée de vie* du logiciel. Néanmoins, il apparaît que l'application de la courbe en *baignoire* du matériel dans le cas du logiciel est réaliste.

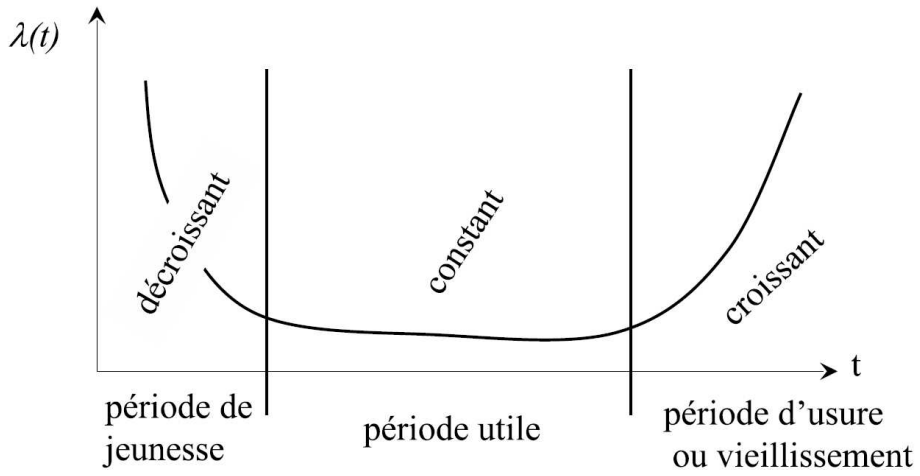

FIGURE 2.14 – Courbe en baignoire

Rappelons la forme en baignoire de cette courbe sur la figure 2.14 où l'on observe la période de jeunesse qui est considérée comme la phase de correction, suivie de la phase de vie utile qui est la période où le taux de défaillance est constant et finalement la période de fin de vie utile lorsque l'usure et le vieillissement font sentir leurs effets.

La période de jeunesse concerne les défaillances précoces dues à des problèmes de conception ou de production. La période utile, plus au moins importante selon le type de matériel, est caractéristique des défaillances aléatoires. Enfin la période d'usure ou de

vieillissement correspond aux défaillances dues à des phénomènes d'usure, de vieillissement, etc. [69].

Les composants logiciels Le cycle de développement du logiciel peut être comparé avec le cycle de vie du matériel. Ainsi, pendant ce cycle de développement, le taux de défaillance logiciel est caractérisé par la courbe en baignoire illustrée sur la figure 2.14 :

- La première phase définit la phase de jeunesse et est caractérisée par une décroissance rapide du taux de défaillance. Cette phase commence avec les tests et est considérée comme la phase de correction. Les erreurs de programmation ou les opérations non conformes aux spécifications sont identifiées et corrigées [70].
- La deuxième phase représente la période de vie utile du logiciel dans laquelle le taux de défaillance est constant. La distribution utilisée lors de cette phase est la loi exponentielle [70].
- La dernière phase commence à la fin de vie utile. La majorité des erreurs observées durant cette phase sont dues à l'incapacité du logiciel à satisfaire les nouveaux besoins du client, sans modification des spécifications initiales. Par conséquent, nous pouvons considérer ce phénomène comme *l'usure* du logiciel.

Les composants électroniques Le taux de défaillance des composants électroniques est représenté par la courbe 2.14 qui est composée de trois phases :

- La période de jeunesse du composant électronique s'explique par l'élimination progressive des défauts dus aux processus de conception ou de fabrication mal maîtrisé ou à un lot de composant défectueux. Aujourd'hui cette période est réduite, compte tenu de la grande qualité des composants. Les distribution utilisées pour cette phase sont la loi de Weibull ($\beta < 1$) et la loi Lognormale ($\sigma > 1$).
- La phase de vie utile est généralement très longue. Le taux de défaillance est quasiment constant. Les défaillances, durant cette phase, sont aléatoires et sont dues à d'autres mécanismes d'endommagement. Le choix de la loi est tout à fait satisfaisant dans cette phase.
- La période de vieillissement, dans ce cas, est due à des phénomènes tels que l'usure, l'érosion, etc. Les distributions de probabilité utilisées pour cette phase sont la loi de Weibull ($\beta > 1$) et la loi Lognormale ($\sigma < 1$) et la loi Normale.

Les composants mécaniques Dès le début de leur vie, les composants mécaniques sont soumis aux phénomènes d'usure ou de vieillissement. Si la courbe du taux de défaillance en fonction du temps est tracée, on constate que le plateau présent dans la figure 2.14 est

réduit ou inexistant. La courbe possède ainsi deux phases :

- La première phase est décrite par une décroissance progressive du taux de défaillance en fonction du temps dû à une amélioration des caractéristiques internes et des interfaces par un rodage préalable des pièces. Les lois de probabilité utilisées pour cette phase sont la loi de Weibull ($\beta < 1$) et la loi Lognormale ($\sigma > 1$).
- La dernière phase représente la période de vieillissement qui recouvre la majeur partie de la vie du composant. Elle est caractérisée par une augmentation progressive du taux de défaillance. Les distributions de probabilité utilisées pour cette phase sont la loi de Weibull ($\beta > 1$) et la loi Lognormale ($\sigma < 1$) et la loi Normale.

Comme on vient de le citer dans le paragraphe ci-dessus, la période de vie utile est caractérisée par les défaillances aléatoires. Pour représenter cette période, le choix de la loi exponentielle (voir annexe) est toute à fait satisfaisant dans le cas des composants électroniques et logiciels.

Dans le cas des composants mécaniques, il est possible d'utiliser une loi de Weibull. Cependant, nous allons construire, par la suite, une loi qui décrira l'évolution de la fiabilité d'un composant mécanique en fonction du temps dans le paragraphe 2.4.3.5.

Avant d'entamer la fiabilité mécanique en fonction du temps, faisant tout d'abord quelques rappels sur les méthodes classiques de fiabilité mécanique.

2.4.3.3 Les modèles composants

Lorsqu'une équipe de conception développe un nouveau système, elle doit disposer d'un certain nombre de recommandations ou de règles, issues du savoir-faire et de l'expérience acquise qui sont indispensables à une conception sûre de fonctionnement. Les recueils de données sont des outils incontournables et indispensables.

Ces recueils sont des ensembles de données validées et/ou élaborées après un long processus d'expertise et de traitement, relatif à un domaine de connaissance et organisé pour être offert aux consultations d'utilisateurs.

En électronique, un domaine où le calcul de fiabilité est pratiquée depuis de nombreuses années, les bases de données de fiabilité sont disponibles et nombreuses. En mécanique, l'utilisation des recueils est plus récentes. Il y a une certaine difficulté à constituer ces recueils, compte tenu de la complexité des composants, néanmoins ils sont de plus en plus utilisés. Pour le logiciel, il existe peu de de recueils de données du faite de la difficulté de réutiliser les mêmes lignes de code.

Dans la majorité des recueils, les informations disponibles sont : la dénomination du composant, la moyenne des temps de bon fonctionnement (MTTF), le taux de défaillance moyen ou calculé avec l'hypothèse qu'il est constant, l'intervalle de confiance associé et

un coefficient multiplicateur du taux de défaillance dépendant de l'environnement.

En électronique, les recueils de données sont souvent exhaustifs sachant que les composants suivent une loi exponentielle.

En mécanique, l'hypothèse du taux de défaillance constant est rarement justifié.

Dans le cas du logiciel, il y a peu de recueils de données. Les erreurs sont introduites lors de la conception ou bien lors de la programmation. Microsoft a estimé un programmeur introduisant environ 6 défaillance par 1000 ligne de code [65].

Fiabilité logicielle Deux modèles de fiabilité logiciel sont présentés dans cette partie

- **Le modèle de temps d'exécution de Musa :** est un des premiers modèles de fiabilité logiciel. Il estime le taux de défaillance initiale λ_0 du logiciel, à partir d'une loi exponentielle, au début des tests.
  Le taux de défaillance de ce modèle s'écrit :

$$\lambda = kpN_0 \tag{2.33}$$

  k représente une constante qui dépend de la structure dynamique du programme et de la machine sur laquelle il est installé (k = 4.2 10^{-7}), p est le nombre d'exécutions par unité de temps ($p = r/SLOC/ER$), r est une constante qui représente le taux d'exécution d'instruction, $SLOC$ représente les lignes de source de code (ne comprenant pas le code réutilisé), ER est le rapport d'expansion, une constante sur le langage de programmation ($ER = 1$ pour Assembleur, 1.5 pour Macro Assembleur, $ER = 2.5$ pour le C, $ER = 3$ pour COBAL, FORTRAN et $ER = 4.5$ pour Ada) et enfin N_0 représente l'évaluation du nombre initial de défauts dans le programme.
- **Modèle de Putnam :** Putnam a affecté la distribution de Rayleigh pour décrire la fiabilité observée du logiciel, où k et a sont des constantes estimées à partir des données et t est le temps exprimé en mois :
  La fiabilité s'écrit :

$$R(t) = ke^{-at^2} \tag{2.34}$$

  N_0 représente le nombre initial de défauts (k = N_0), t_D est la base de référence (a = $3/t^2{}_D$).
  La densité de probabilité s'écrit alors de la manière suivante :

$$f(t) = \left(\frac{6N_0}{t_D^2}\right) te^{-\frac{3t^2}{t_D^2}} \tag{2.35}$$

Fiabilité électronique Les recueils de données les plus utilisées pour les composants électroniques sont : FIDES, IEEE STD, MIL-HDBK-217, BT-HDR, etc. La durée de vie des données fournies par ces recueils est relativement courte et elle varie entre 3 et 6 ans. Nous nous intéressons, dans notre travail, au modèle FIDES.

Modèle FIDES : L'expression du taux de défaillance dépend de plusieurs facteurs dont la technologie de conception, la technologie de fabrication et l'environnement de fonctionnement du composant [37, 21]. Ainsi, le taux de défaillance dépend d'un taux de défaillance de base, pondéré par des facteurs de technologie, de conception, de fabrication, d'utilisation, d'environnement, etc.

Le taux de défaillance s'écrit comme suit :

$$\lambda = \lambda_{\text{Physique}} \Pi_{\text{Part-manufacturing}} \Pi_{\text{Process}} \tag{2.36}$$

$\lambda_{Physique}$ représente la contribution physique à la défaillance, $\lambda_{Part-manufacturing}$ est la contribution qualité et maîtrise de la fabrication et $\lambda_{Process}$ représente la contribution développement, conception et utilisation du produit.

Exemple de disques durs (EIDE, SCSI) dans le guide FIDES [37] : le modèle général associé à la famille est écrite sur l'équation 2.36 avec :

$$\lambda_{Physique} = \sum_{i}^{Phases} \left(\frac{t_{annuel}}{8760}\right)_i \cdot \left(\lambda_{Disque-dur-Thermique} \cdot \Pi_{Thermique} + \lambda_{Disque-dur-Mcanique} \cdot \Pi_{Mcanique}\right)_i \cdot \Pi_{Induit-i} \tag{2.37}$$

Les taux de défaillance associés au sous-ensemble sont présenté sur le tableau 2.3 :

Description du sous-ensemble	$\lambda_{Disque-dur-Mecanique}$ **(FIT)**	$\lambda_{Disque-dur-Thermique}$ (FIT)
Disque dur EIDE	Π_S.[120-60.ln(Ft)]	Π_S.(5.1+($\frac{T_a}{9.6}$)$^{5.0}$)
Disque dur SCSI	Π_S.[60-29.ln(Ft)]	Π_S.(2.6+($\frac{T_a}{11}$)$^{5.0}$)

TABLE 2.3 – Taux de défaillance

Ft représente le format du disque dur (en pouce) avec $1 < Ft < 5.25$ et T_a le temps d'accès moyen (en ms), $T_a < 20$ms.

Le facteur de sollicitation Π_S s'écrit :

$$\Pi_S\left(Pc, Dc\right) = \frac{Pc \cdot Dc + 3}{Pc + 3} \tag{2.38}$$

Dc représente le taux de sollicitation (Duty Cycle) définit par :

$$Dc = \frac{\left(\sum_a Temps\_acces + \sum_b Temps\_Lecture + \sum_c Temps\_ecriture\right)}{Temps\_Utilisation} \tag{2.39}$$

Pc est le nombre de plateau (de disque) (Platter Count). Si Pc est inconnu alors il faut prendre :

$$Pc = Part\_entiere\left(\frac{1+Nt}{2}\right) \tag{2.40}$$

Nt représente le nombre de têtes. Dans le cas de la durée de vie il faut se reporter aux données fabricants.

Voici quelques renseignements liés au profil de mission :

t_{annuel} est le temps associé à chaque phase sur une année (heures), $T_{ambiante}$ représente la température ambiante moyenne associée à une phase (°C) et G_{RMS} est le stress associé à chaque phase de vibration aléatoire (Grms).

$\Pi_{Thermique}$	En phase de fonctionnement : $e^{11604\times 0.785\times\left[\frac{1}{293}-\frac{1}{T_{ambiante}+273}\right]_i}$ En phase de non-fonctionnement : $\Pi_{Thermique} = 0$
$\Pi_{Mcanique}$	$(\frac{G_{RMS}}{0.5})^{2.5}{}_i$

TABLE 2.4 – Taux de défaillance associé au sous-ensemble

Fiabilité mécanique Lorsqu'il s'agit d'un composant mécanique standard, les recueils de données peuvent être utilisés. Parmi ces recueils nous pouvons citer : AVCO, NPRD, NSWC, EIREDA, etc. La durée de vie de ces recueils dans le cas de la mécanique, contrairement à l'électronique, est plus longue et varie entre 30 et 40 ans.

– **Modèle de fiabilité de composants mécaniques standards :** Considérons un exemple d'un composant mécanique standard tel que les roulements. La fiabilité de ce composant s'écrit alors de la manière suivante :

$$R = e^{\left(-\left(\frac{L/L_{10}-0.02}{4,439}\right)^{1.483}\right)}, \quad L_{10} = \left(\frac{C}{P}\right)^n \tag{2.41}$$

L_{10} représente la durée de vie du roulement en millions de tours, C est la charge dynamique de base, P représente la charge équivalente exercée sur le roulement et n est égale à 3 pour un roulement à billes et 10/3 pour les roulements à rouleaux.

La durée de vie d'un ensemble de roulements s'écrit :

$$L_{E10} = \left(\left(\frac{1}{L_{1.10}} \right)^{1.5} + \left(\frac{1}{L_{2.10}} \right)^{1.5} + \cdots + \left(\frac{1}{L_{n.10}} \right)^{1.5} \right)^{\frac{1}{1.5}} \tag{2.42}$$

– **Fiabilité de composants mécaniques spécifiques :** Dans le cas d'un composant mécanique spécifique, il est nécessaire d'utiliser les méthodes probabilistes afin d'estimer la fiabilité de ce composant. Ces méthodes sont présentées dans le paragraphe ci-dessous.

2.4.3.4 Fiabilité mécanique d'un composant spécifique

De manière générale, le dimensionnement de structure se fait en considérant un mode de défaillance donné et basé sur l'établissement d'une relation mécanique caractérisant son état en fonction des variables de la structure. Cette relation mécanique est composée de 2 termes : un premier donnant l'état de sollicitation de la structure (efforts internes s'exerçant dans la structure) en fonction d'un mode de ruine donné (statique, fatigue, ...) noté S, et un deuxième caractérisant la résistance à la contrainte exercée noté R.

Dans un problème de fiabilité, les variables d'entrée sont considérées comme des variables aléatoires. Ces variables d'entrée sont généralement regroupées dans un vecteur appelé vecteur des variables de base noté X. La fonction de performance notée $G(X)$ permet la réalisation d'une partition de l'espace physique en deux domaines, appelés domaines de sécurité et de défaillance pour le quel nous avons respectivement $G(X)>0$ et $G(X)<0$. Il existe donc une frontière appelée *état limite* sur laquelle $G(X)=0$ [72, 59, 68, 90, 42].

La première étape vers l'évaluation de la fiabilité d'une structure consiste à établir la relation fonctionnelle liant la variable aléatoire X du problème afin d'obtenir une fonction d'état qui s'écrira :

$$G(X) = G(X_1, X_2, \ldots, X_n) \tag{2.43}$$

Cette fonction $G(X)$ peut être implicite ou explicite. La fiabilité de la structure P_R est la probabilité que l'état de la structure à un moment donné, se situe dans la zone sûre ($G(X)>0$). Complémentairement, la probabilité de défaillance P_f est :

$$P_f = 1 - P_R \tag{2.44}$$

Dans le cas élémentaire d'une structure ayant une résistance mécanique R soumise à un chargement S, la probabilité de défaillance est alors égale à la probabilité que le chargement soit supérieur à la résistance soit :

$$P_f = P\left(R - S \leq 0\right) = P\left(\frac{R}{S} \leq 1\right) = F_R\left(S\right) \tag{2.45}$$

D'une manière générale R et S sont des variables aléatoires définies, respectivement, par une fonction de répartition F_R et F_S, et une densité de probabilité f_R et f_S.

Les méthodes classiques de dimensionnement de structure définissent un coefficient de sécurité qui est égal au rapport de la résistance R et de la contrainte S. Mais lorsque l'on cherche, par exemple, à alléger une structure (c'est-à-dire à diminuer le coefficient de sécurité), quel risque prenons-nous ? Dans ce cas ces méthodes ne peuvent pas répondre à cette interrogation. C'est pourquoi nous nous tournons vers les méthodes probabilistes qui consistent à déterminer la probabilité de défaillance. Cette probabilité de défaillance est déterminée en prenant en compte toutes les valeurs possibles des variables R et S, et caractérise la probabilité que la contrainte S soit supérieur à la résistance R. Cette relation est nommée Résistance/Contrainte.

$$P_f = P\left(R - S \leq 0\right) = \int\int_D f_{RS}\left(r, s\right) drds \tag{2.46}$$

où D est le domaine d'intégration des variables, c'est-à-dire la région où $G(R,S)<0$, et $f_{RS}(r,s)$ est la densité de probabilité jointe de R et S.

Dans le cas de n variables aléatoires quelconques, l'équation 2.46 prend la forme suivante :

$$P_f = \int\limits_{G(X)\leq 0} f_X\left(x_1, x_2, \ldots, x_n\right) dx_1, \ldots, dx_n \tag{2.47}$$

Pour résoudre un problème de fiabilité, plusieurs approches peuvent être mises en avant ; parmi elles les méthodes où la forme de la fonction d'état limite est essentielle. Ceci implique de disposer de l'écriture explicite de cet état limite où à défaut d'une approximation. La probabilité de défaillance peut être estimée par différentes méthodes comme la simulation de Monte Carlo, les méthodes FORM/SORM (First/Second Order Reliability Method) ou la méthode de surface de réponse.

Simulation de Monte Carlo : La simulation de Monte Carlo est une méthode universelle pour l'évaluation des intégrales comme celle de l'équation 2.47.

La fonction indicatrice du domaine de défaillance notée γ_F(X) prend une valeur égale à 0 dans le domaine sûr et 1 dans le domaine de défaillance.

$$P_f = \int_{R^d} \gamma_F(x)\, f_X(x)\, dx = E\left[\gamma_F(x)\right] \tag{2.48}$$

E[γ_F(X)] représente l'espérance de γ_F(X), il est donc possible de faire appel à l'estimateur empirique :

$$P_f = \frac{1}{n}\sum_{i=1}^{n} \gamma_F(x_i) = \frac{n_d}{n} \tag{2.49}$$

n_d représente le nombre de tirages se trouvant dans le domaine de défaillance et n le nombre de tirages total [90, 72, 68].

En résumé, la simulation de Monte Carlo telle qu'elle est décrite dans ce paragraphe est, en principe, appliquée quelle que soit la complexité du modèle déterministe. Cependant, son coût de calcul peut la rendre irréalisable.

Méthode FORM : La méthode FORM (First Order Reliability Method) est introduite dans le but de faire une approximation de la probabilité de défaillance à moindre coûts comparé à la simulation de Monte Carlo, où le coût est mesuré en termes du nombre d'évaluation de la fonction d'état limite [90].

La première étape consiste à retraiter le problème dans l'espace normal standard en utilisant les transformations isoprobabilistes. Pour cela, les variables physiques X, qui suivent a priori une loi quelconque et qui sont a priori corrélées, sont transformées en des variables aléatoires centrées réduites et indépendantes U. Ces dernières définissent les vecteurs de base de l'espace normé. Cet espace est parfaitement adapté à une conduite simple de calculs. D'une part, les difficultés liées aux domaines de définition des densités des variables physiques sont ainsi évitées étant donné que la densité gaussienne est à support infini. D'autre part, celles liées à une différence trop importante entre les ordres de grandeurs des valeurs moyennes des variables en jeu ne se posent plus.

Deux types de transformation sont principalement utilisés c'est la transformation de Rosenblatt et celle de Nataf

- **Transformations de Rosenblatt :** Cette transformation permet d'opérer une transformation marginale des variables de l'espace normé vers l'espace physique. La transformation de Rosenblatt n'est applicable que si la densité conjointe de toutes les variables aléatoires est connue. Son principe réside dans l'hypothèse que la distribution multivariable $F_{X_1,X_2\cdots X_n}(X_1,X_2,\ldots,X_n)$ est équivalente à :

$$F_{X_1}(x_1)\, F_{X_2|X_1}(x_2\,|x_1)\ldots F_{X_n|X_1,\ldots,X_{n-1}}(x_n\,|x_1,\ldots,x_{n-1}) \tag{2.50}$$

La transformation de Rosenblatt est donnée par :

$$\begin{cases} U_1 = \Phi^{-1}\left(F_1\left(X_1\right)\right) \\ U_2 = \Phi^{-1}\left(F_2\left(X_2\left|X_1\right.\right)\right) \\ \vdots \\ U_n = \Phi^{-1}\left(F_n\left(X_n\left|X_{n-1}, \ldots X_1\right.\right)\right) \end{cases} \tag{2.51}$$

Dans la pratique, la difficulté majeure dans l'application de cette transformation réside dans la détermination des probabilités conditionnelles en jeu. De plus, la densité conjointe des variables physiques n'est pas toujours connue [59, 72].

– **Transformations de Nataf :** Elle ne requiert pas la connaissance de la densité conjointe des variables physiques. En revanche, leurs densités marginales ainsi que la matrice de corrélation ρ_{ij} sont connues. Son principe consiste à considérer une suite des variables centrées réduites, mais corrélées, $U = (u_1, \ldots u_n)$, issue de la transformation 2.52, où Φ représente la fonction de répartition de la loi normale centrée réduite.

$$u_i = \Phi^{-1}\left(F_{X_i}\left(x_i\right)\right) \tag{2.52}$$

Les corrélations ${\rho_{ij}}^*$ des variables U sont solution de l'intégrale 2.53, dans laquelle ϕ_2 représente la densité de la loi binormale :

$$\rho_{ij} = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{x_i - \mu_i x_j}{\sigma_i} \cdot \frac{x_j - \mu_j}{\sigma_j} \phi_2\left(u_i, u_j, \rho_{ij}^*\right) du_i du_j \tag{2.53}$$

Dans la pratique, des relations empiriques fournissant des estimations acceptables des corrélations des variables intermédiaires sont utilisées. La matrice de décorrélation des variables physiques est alors construite à partir de la matrice de corrélation des variables intermédiaires en considérant sa décomposition spectrale, ou encore sa décomposition de Cholesky. Les coordonnées des variables physiques dans l'espace normé peuvent alors être déterminées [68, 72].

La deuxième étape de la méthode FORM consiste à déterminer le point u^* appelé point de conception, qui est le point de défaillance le plus probable. Ce point appartient à la surface d'état limite et a pour caractéristique d'être le plus proche de l'origine. La fonction d'état limite pour la méthode FORM du premier ordre autour du point de conception s'écrit :

$$G_U\left(U\right) = 0 \approx \nabla g_U\left(u^*\right)^T \left(u - u^*\right) \tag{2.54}$$

Ce point de conception est solution du problème d'optimisation qui résoud :

$$\begin{cases} \beta = \min\left(\sqrt{u^T u}\right) \\ tel\ que : G_U(u) = 0 \end{cases} \tag{2.55}$$

Dans l'équation 2.55, u^T est la transposée de u et β représente l'indice de fiabilité au sens de Hasofer et Lind, β_{HL} qui est la distance entre l'origine et le point de conception. Cet indice diffère de celui de Basler et Cornell qui est basée sur une linéarisation autour du point moyen. Celle proposée par ces deux derniers auteurs est rarement retenue dans la pratique en raison du manque d'invariance quant à la manière de formuler la fonction d'état limite [72].

Troisième et dernière étape de cette méthode d'approximation consiste à estimer la probabilité de défaillance à partir de l'indice de fiabilité. C'est une grandeur scalaire, qui permet de rendre compte de la fiabilité d'un mode de performance donné. En effet, plus cet indice est élevé, plus la probabilité de défaillance sera faible. La relation entre l'indice de fiabilité et la probabilité de défaillance s'écrit de la manière suivante :

$$P_f \approx \Phi(-\beta) \tag{2.56}$$

Il est à noter que dans le cas d'une fonction d'état limite possédant une forte courbure, l'approximation au point de conception par un hyperplan tangent n'est évidemment plus adaptée. Il est alors nécessaire de recourir à une approximation au second ordre.

Méthode SORM La méthode de fiabilité du second ordre SORM (Second Order Reliability Method) est basée sur une approximation plus précise de la surface d'état limite, puisque cette dernière est approchée par une surface quadratique ayant le même rayon de courbure que la surface réelle au point de conception. Il est nécessaire de trouver une approximation de la fonction d'état limite par un développement en série de Taylor du second ordre autour du point de conception. La surface d'état limite s'écrit de la forme suivante :

$$G_U(U) = 0 \approx \nabla g_U(u^*)^T (u - u^*) + \frac{1}{2}(u - u^*)^T D(u^*)(u - u^*) \tag{2.57}$$

D est la matrice Hessienne symétrique de la fonction G_U qui est la matrice des dérivées partielles du second ordre au point de conception :

$$D_{ij}(u^*) = \frac{\partial^2 g_u(u^*)}{\partial u_i \partial u_j} \tag{2.58}$$

Avec une telle approximation, la probabilité de défaillance peut être approchée par plusieurs approches. La probabilité de défaillance est [72, 90] :

$$P_f = \Phi(-\beta) \prod_{i=1}^{n-1} (1 - \beta k_i)^{-1/2} \tag{2.59}$$

Il apparait clairement dans l'équation 2.59 que l'approximation SORM de la probabilité de défaillance est obtenue par une correction de celle obtenue par l'approximation FORM exprimé dans l'équation 2.56 [90].

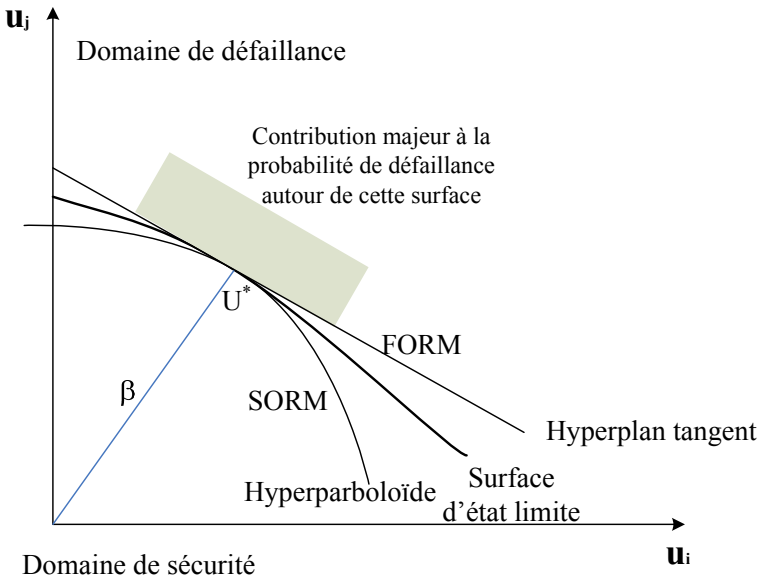

FIGURE 2.15 – Méthode FORM/SORM

L'évaluation de la performance des structures par les méthodes classiques de la théorie de la fiabilité (méthodes FORM, SORM) nécessite la définition d'une fonction d'état limite qui caractérise le dysfonctionnement d'une structure. Or, dans le cas de structures complexes cette fonction n'admet pas nécessairement de forme explicite. Le calcul de la probabilité de défaillance nécessite alors de recourir à des simulations numériques de type Monte-Carlo. Les probabilités très faibles à estimer impliquent cependant des tirages en grand nombre ou des techniques de simulations adaptées.

Une méthode alternative consiste à construire artificiellement la fonction d'état limite en utilisant un polynôme ajusté aux résultats d'un nombre limité de calculs aux éléments finis [72]. Cette fonction peut être utilisée pour évaluer la probabilité de défaillance. Ce type d'approche est appelé méthode par surfaces de réponse (MSR).

Méthode de Surface de Réponse La méthode des surfaces de réponse est un outil utilisé depuis le début des années cinquante dans plusieurs domaines scientifiques tels que la biologie animale et végétale, les sciences humaines, la chimie, l'industrie et l'ingénierie. En développant des logiciels relatifs à la fiabilité des structures, la méthode des surfaces de réponse est rapidement devenue une des plus puissantes pour évaluer la fiabilité des structures complexes [103].

Un des objectifs des surfaces de réponse est d'obtenir un modèle mathématique explicite qui :

- représente la surface de défaillance de structures complexes pour des éléments particuliers (modes de défaillance) ;
- représente une bonne approximation du comportement du modèle étudié ;
- est une technique d'approximation permettant de diminuer les temps de calcul et de réaliser une étude fiabiliste des structures complexes ;
- est construit sur un couplage entre un code de calcul éléments finis et un outil numérique de fiabilité.

La réponse d'une structure est généralement représentée par une fonction d'état limite $G(X)$ qui caractérise la défaillance de la structure. Cette fonction dépend de $X=(x_1,...,x_n)$, vecteur des variables intervenant dans le problème étudié (en termes de résistances et de sollicitations). Dans le cas de structures complexes, la fonction implicite $G(X)$ peut être évaluée seulement de manière discrète par des réalisations $X^k=(x^k{}_1,...,x^k{}_n)$, $k=1,...,n$ des variables.

L'idée d'origine de la méthode des surfaces de réponse est de remplacer la fonction $G(X)$ qui est une fonction a priori inconnue, par une fonction explicite équivalente $G(X)$. Les méthodes de surfaces de réponse recherchent donc une fonction, généralement une surface polynomiale, dont les coefficients sont déterminés de manière à minimiser l'erreur d'approximation dans la région autour du point de conception (point de l'état limite admettant la plus forte densité). L'évaluation de ces coefficients nécessite la réalisation de séries d'expériences numériques qui correspondent à des calculs numériques avec des paramètres d'entrée sélectionnés conformément à un plan d'expérience.

Une structure dans son environnement réel, subit des charges qui varient en fonction du temps tout au long de la durée de vie d'un système. Cela signifie que l'analyse probabiliste n'inclue pas uniquement des variables aléatoires, comme dans les cas standards, mais aussi des variables aléatoires en fonction du temps, généralement qualifiés de processus stochastique ou aléatoire en fonction du temps [11, 68].

2.4.3.5 Fiabilité mécanique en fonction du temps

Dans un problème de fiabilité dynamique, la charge à tendance à croître alors que la résistance à tendance à décroître. Cela signifie que le problème général de la fiabilité dynamique peut être représenté, si l'on considère un cas simple, comme montré sur la figure 2.16.

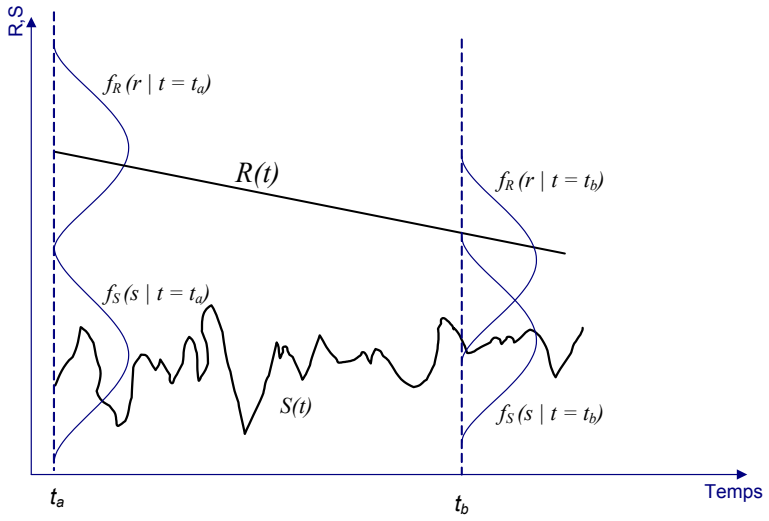

FIGURE 2.16 – Schéma d'un problème de fiabilité dynamique [68]

En conséquent, la probabilité de défaillance $P_f(t)$ en fonction du temps t s'écrira de la manière suivante :

$$P_f(t) = R(t) - S(t) < 0 \tag{2.60}$$

Cette probabilité de défaillance peut être représenté par le chevauchement des deux fonctions de densité de probabilité de la résistance et de la contrainte f_R et f_S. Dès que cette intersection varie avec le temps la probabilité de défaillance P_f peut varier alors en fonction du temps.

Si la fonction de densité de probabilité instantanée $f_R(t)$ et $f_S(t)$, respectivement, de $R(t)$ et $S(t)$ sont connues, la probabilité de défaillance instantanée $P_f(t)$ peut être obtenue par l'intégrale suivante :

$$P_f(t) = P(R(t) - S(t) \leq 0) = \int_{-\infty}^{+\infty} F_R(x(t))\, f_S(x(t))\, dx(t) \tag{2.61}$$

Schématiquement, les changements de $F_R(t)$, $f_S(t)$ et $P_f(t)$ en fonction du temps peuvent être décrit dans la figure 2.16.

Si le caractère aléatoire des variables de conception ne provient que d'un aléa ω, alors

elles sont modélisées par des variables aléatoires. Si elles sont aussi indexées sur le temps t, elles sont modélisées par des processus stochastiques dont la propriété essentielle est de posséder une corrélation entre deux instants [3, 4].

Dans une étude de dégradation, l'état-limite ne comporte souvent que des fonctions du temps décrivant la cinétique du processus et des variables aléatoires $R(\omega)$ modélisant l'aléa des paramètres de ce processus d'où $X(t,\omega) = R(\omega)$.

Dans une étude d'actions aléatoires, l'état-limite comporte uniquement des processus aléatoires $S(t,\omega)$, d'où $X(t,\omega)=S(t,\omega)$.

Dans une étude plus générale, l'état-limite peut comporter une combinaison des deux champs : $R(\omega)$ et $S(t,\omega)$ sont présents simultanément dans l'état-limite d'où $X(t,\omega)= (R(\omega),S(t,\omega))$.

Probabilité instantanée de défaillance En utilisant une analyse probabiliste à un instant t, nous pouvons calculer la probabilité d'avoir une défaillance à cet instant donné. La probabilité instantanée de défaillance s'écrit alors :

$$P_{f,i}(t) = \text{Prob}\left(G\left(t, X\left(t,\omega\right)\right) \leq 0\right) \tag{2.62}$$

$X(t,\omega)$ représente le vecteur des variables de conception, t le temps, ω l'aléa et $P_{f,i}(t)$ est la probabilité que la structure soit défaillante à l'instant t.

Probabilité cumulée de défaillance La probabilité cumulée de défaillance est définie de la manière suivante :

$$P_{f,c}(t_1, t_2) = \text{Prob}\left(\exists t \in [t_1, t_2], tq\ G\left(t, X\left(t,\omega\right)\right) \leq 0\right) \tag{2.63}$$

L'équation 2.63 est vrai dans le cas où on a un seul passage de l'état sûr à l'état défaillant (un seul franchissement) dans l'intervalle de temps [t,t+Δt]

Dans le cas de la fiabilité en fonction du temps les méthodes classiques d'estimation de la fiabilité telles que FORM ou SORM ne sont plus adaptées. C'est pourquoi nous nous tournons vers une autre méthode qui permet de calculer la probabilité de défaillance en fonction du temps. Cette méthode a été présentée par [3, 2, 5] en 2002 et est connue sous le nom de PHI2.

Méthode PHI2 Le calcul de la probabilité cumulée de défaillance est classiquement basé sur la formule de Rice qui permet de déterminer le taux de franchissement, ou sur

le calcul de l'espérance du nombre de franchissements en utilisant des formules asymptotiques.

La méthode proposée par [3, 2, 5, 92, 18] consiste à utiliser une approche qui permet de calculer le taux de franchissement en utilisant la loi binormale. Ce taux de franchissement est intégré par rapport au temps et calculer, ainsi, la probabilité de défaillance cumulée grâce aux outils classiques (indépendants du temps) de la fiabilité.

Avant de détailler la méthode PHI2, il est nécessaire de faire quelques rappels sur le taux de franchissement.

Taux de franchissement Soit $X(t,\omega)$ le vecteur des variables de conception, t le temps et ω l'aléa. $G(t,X(t,\omega))$ représente la fonction de performance d'une structure selon un mode de fonctionnement donné. L'événement :

$$E = \{\exists t \in [t_1, t_2]\,, tq.\ G\left(t, X\left(t, \omega\right)\right) \leq 0\} \tag{2.64}$$

traduit un franchissement de l'état-limite $G(t,X(t,\omega)) = 0$ dans le domaine de défaillance comme montré sur la figure 2.17

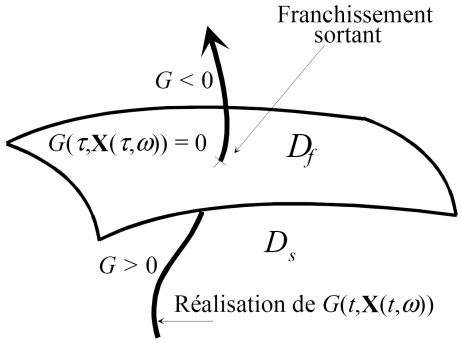

FIGURE 2.17 – Franchissement sortant [3]

On note E[$N^+(t_1,t_2)$] l'espérance du nombre de franchissement sortant $N^+(t_1,t_2)$ sur l'intervalle [t_1,t_2].

Le taux de franchissements $\nu(t)$ est lié au nombre de franchissement $N^+(t_1,t_2)$ par la relation :

$$\nu\left(t\right) = \lim_{\Delta t \to 0} \frac{P\left(N^+\left(t, t+\Delta t\right) = 1\right)}{\Delta t} \tag{2.65}$$

Le nombre moyen de franchissements sur l'intervalle de temps $[t_1,t_2]$ est alors :

$$E\left[N^+\left(t_1, t_2\right)\right] = \int_{t_1}^{t_2} \nu\left(t\right) dt = \nu \cdot \left(t_2 - t_1\right) \tag{2.66}$$

La probabilité de défaillance instantanée s'écrit de la manière suivante :

$$P_{f,i}(t_1) \leq P_f(t_1, t_2) \leq P_{f,i}(t_1) + \nu \cdot (t_2 - t_1) \tag{2.67}$$

Le taux de franchissement peut être calculé de façons différentes :

Analytiquement par la formule de Rice qui est développée pour calculer le taux de franchissement et la probabilité cumulée de défaillance.

Plusieurs cas étaient traité dans [3, 2, 5, 90]. On s'intéressera uniquement aux deux premiers cas qui sont : *R(ω)-S(t,ω)* et *R(ω)-δ.t-S(t,ω)*.

Cas stationnaire : *R(ω)-S(t,ω)* Le taux de franchissement pour ce cas est donné par l'équation 2.68 :

$$\nu(t) = \frac{\omega_0}{\sqrt{2\pi}} \frac{\sigma_S}{\sqrt{\sigma_R^2 + \sigma_S^2}} \phi\left(\frac{m_R - m_S}{\sqrt{\sigma_R^2 + \sigma_S^2}}\right) \tag{2.68}$$

Les étapes permettant d'aboutir à ce taux de défaillance sont détaillés dans [90, 3].
ϕ représente la densité de probabilité de la loi normale centrée réduite et ω_0 la pulsation qui définit comme suit :

$$\omega_0^2 = \left.\frac{\partial^2 \rho_{SS}(t_1, t_2)}{\partial t_1 \partial t_2}\right|_{t_1 = t_2} \tag{2.69}$$

et la corrélation s'écrit :

$$\rho_{SS}(t_1, t_2) = \exp\left(-\frac{(t_2 - t_1)^2}{l^2}\right) \tag{2.70}$$

Le taux étant indépendant du temps, il vient :

$$E\left[N^+(t_1, t_2)\right] = \nu(t).(t_1 - t_2) = \nu.(t_1 - t_2) \tag{2.71}$$

Cas instationnaire : *R(ω) - δ.t - S(t,ω)* Pour traiter ce cas, il faut connaître la probabilité cumulée de défaillance pour une fonction de performance de la forme *G(t,ω)=a(t)-S(t,ω)* où *a(t)* est un seuil dépendant du temps.

Le taux de franchissement s'écrit de la manière suivante :

$$\nu(t) = \omega_0 \phi(b(t)) \Psi\left(\frac{\dot{b}(t)}{\omega_0}\right) \tag{2.72}$$

Le nombre moyen de franchissements, dans ce cas, entre t_1 et t_2 est donné par la relation :

$$E\left[N^{+}\left(t_1,t_2\right)\right]=\int_{t_1}^{t_2}\omega_0\phi\left(b\left(t\right)\right)\Psi\left(\frac{\dot{b}\left(t\right)}{\omega_0}\right)dt \tag{2.73}$$

Sachant que Ψ(x)=ϕ(x)-xΦ(x).
ϕ représente la densité de probabilité de la loi normale centrée réduite et Φ la fonction de répartition da la loi normale centrée réduite.
b(t) est un seuil normalisé et est définit comme suit :

$$b\left(t\right)=\frac{r-\delta t-m_S}{\sigma_S} \tag{2.74}$$

r représente un seuil déterministe.

Le calcul de l'équation 2.73 nous donne le résultat suivant :

$$E\left[N^{+}\left(t_1,t_2\right)\right]=\omega_0\frac{\sigma_S}{\delta}\Psi\left(\frac{-\delta}{\sigma_S\omega_0}\right)\left\{\Phi\left(\frac{m_R-\delta t_1-m_S}{\sqrt{\sigma_R^2+\sigma_S^2}}\right)-\Phi\left(\frac{m_R-\delta t_2-m_S}{\sqrt{\sigma_R^2+\sigma_S^2}}\right)\right\} \tag{2.75}$$

Par la méthode PHI2

Le taux de franchissements $\nu(t)$ est défini par la formule :

$$\nu\left(\tau\right)=\frac{\text{Prob}\left(\text{A}\cap\text{B}\right)}{\Delta\tau} \tag{2.76}$$

où les événements sont :
A = la structure est dans le domaine de sûreté à t
B = la structure est dans le domaine de défaillance à t+Δt

En introduisant la fonction de performance G, la relation précédente devient :

$$\nu\left(\tau\right)=\frac{\text{Prob}\left(A'\cap B'\right)}{\Delta\tau} \tag{2.77}$$

avec :

$$A'=\left\{G\left(t,X\left(t,\omega\right)\right)>0\right\}$$
$$B'=\left\{G\left(t+\Delta t,X\left(t+\Delta t,\omega\right)\right)\leq 0\right\}$$

Dans le contexte d'une approximation FORM, ce type de calcul nécessite l'utilisation de la fonction de distribution Φ_2, qui donne son nom à la présente méthode.

La démarche de calcul est la suivante :

– L'indice de fiabilité $\beta(t)$ associé à G(t,X(t,ω))$\leq$ 0 est calculé après avoir gelé le temps (qui devient un simple paramètre) dans toutes les fonctions dépendantes du temps et en ayant remplacé les processus aléatoires $S_j(t,\omega)$ par les variables

aléatoires correspondantes $S_j{}^{(1)}(\omega)$. Cette approximation de premier ordre FORM nous permet de calculer l'indice de fiabilité β(t)

- L'indice de fiabilité $\beta(t+\Delta t)$ associé à G(t+Δt,X(t+Δt,ω)) ≤ 0 est calculé par une seconde analyse FORM. Les processus aléatoires $S_j(t,\omega)$ sont remplacés par un autre jeu de variables aléatoires $S_j{}^{(2)}(\omega)$ mais corrélées avec $S_j{}^{(1)}(\omega)$.
- Le taux de franchissement est approximé par :

$$\nu(t)_{PHI2} = \frac{\Phi_2\left(\beta(t), -\beta(t+\Delta t); \rho_{GG}(t, t+\Delta t)\right)}{\Delta t} \tag{2.78}$$

Dans l'équation 2.78, Φ_2 est la fonction de répartition de la loi binormale, $\beta(t)$ (respectivement $\beta(t+\Delta t)$) représente l'indice de fiabilité à l'instant t (respectivement $t+\Delta t$) et ρ_{GG} (t,t+Δ t) est le produit des cosinus directeurs calculer par l'approximation FORM.

La probabilité de défaillance $P_{f,c}(t_1,t_2)$ est enfin calculée en intégrant le taux de franchissements :

$$P_{f,c}(t_1, t_2) \leq P_{f,i}(t_1) + \int_{t_1}^{t_2} \nu(t)\, dt \tag{2.79}$$

Calcul de Φ_2 La fonction de distribution cumulée de la loi binormale Φ_2 peut être calculée de différentes façons [3] en utilisant :

- la forme intégrale :

$$I = \Phi_2\left(\beta(t), -\beta(t+\Delta t); \rho_{GG}(t, t+\Delta t)\right) \tag{2.80}$$

$$I = \int_{-\infty}^{\beta(t)} \int_{-\infty}^{\beta(t+\Delta t)} \phi_2\left(x, y; \rho_{GG}(t, t+\Delta t)\right) dxdy \tag{2.81}$$

$$I = \Phi(\beta(t))\,\Phi(-\beta(t+\Delta t)) + \int_0^{\rho_{GG}(t,t+\Delta t)} \frac{1}{2\pi\sqrt{1-z^2}} \left(\beta(t)^2 + \beta(t+\Delta t)^2 + 2\beta(t)\,\beta(t+\Delta t)\, z\right) dz \tag{2.82}$$

- l'expression de Φ_2 lorsque ρ_{GG}(t,t+Δt)=-1 :

$$\Phi_2\left(\beta(t), -\beta(t+\Delta t); -1\right) = \begin{cases} \Phi(\beta(t)) - \Phi(\beta(t+\Delta t)) & si\ \beta(t) > \beta(t+\Delta t) \\ 0 & \text{sinon} \end{cases} \tag{2.83}$$

Par la suite, Sudret a proposé une autre expression pour le calcul du taux de franchissements qui s'écrit de la manière suivante [89, 90] :

Dans le cas stationnaire

$$\nu^{+}_{PHI2} = \frac{\phi(\beta)}{\sqrt{2\pi}} \frac{\|\alpha(t+\Delta t) - \alpha(t)\|}{\Delta t} \tag{2.84}$$

et dans le cas instationnaire :

$$\nu^{+}_{PHI2}(t) = \frac{\|\alpha(t+\Delta t) - \alpha(t)\|}{\Delta t} \phi(\beta(t)) \Psi\left(\frac{\beta(t+\Delta t) - \beta(t)}{\|\alpha(t+\Delta t) - \alpha(t)\|}\right) \tag{2.85}$$

2.5 Synthèse

Au regard des méthodes et techniques présentées dans ce chapitre, nous pouvons observer qu'il est possible de traiter en grande partie la problématique de la sûreté de fonctionnement des systèmes mécatroniques. Toutefois, en analysant les travaux réalisés jusqu'à présent, elles ne permettent pas d'appréhender, dans sa globalité, la modélisation et l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques.

Ainsi, les travaux de thèse de Christian Ziegler [73] proposent une approche globale de la conception des systèmes embarqués en étudiant plusieurs architectures. La comparaison qualitative des architectures, au niveau de la sûreté de fonctionnement, est basée sur une méthode quantitative qui fait appel à une modélisation par des réseaux de Petri stochastiques généralisés. Cette étude concerne des systèmes embarqués dans l'automobile et se déroule dans les phases de spécification et de conception de systèmes embarqués pour l'automobile. L'originalité des travaux consiste dans la description des aspects fonctionnels indépendamment de l'architecture du système. La méthode est appliquée sur deux équipements de l'automobile, le coussin gonflable (Airbag) et la direction électrique, et permet la simplification du choix de l'architecture.

Les travaux de thèse de Gilles Moncelet [73] traitent de l'évaluation qualitative et quantitative de la sûreté de fonctionnement des systèmes mécatroniques. Il propose une méthode pour déterminer les séquences d'événements redoutés et pour estimer leurs probabilités d'occurrence à l'aide de la simulation de Monte Carlo. La modélisation dynamique et l'analyse qualitative du système mécatronique sont réalisées avec le formalisme des réseaux de Petri colorés qui génère le graphe d'occurrence nécessaire pour identifier et caractériser tous les chemins menant vers un état redouté. La simulation de Monte Carlo du modèle du système permet d'estimer la probabilité d'occurrence de ces scénarios redoutés. L'originalité des travaux provient de ces deux types de modélisation. La simulation

de Monte Carlo du modèle nécessite cependant un temps de calcul prohibitif. La méthode est appliquée dans le domaine de l'automobile sur le dispositif de contrôle de pression et sur la suspension active.

Les travaux de thèse de Sarhane Khalfaoui [52] sont centrés sur l'analyse qualitative de la sécurité des systèmes mécatroniques en vue de l'obtention des scénarios redoutés. Il a développé une méthode de recherche de scénarios redoutés basée sur la logique linéaire et le formalisme de réseau de Petri à prédicats et transitions différentielles stochastiques, afin d'évaluer les probabilités d'occurrence pour les scénarios et d'orienter le choix des concepteurs. La méthode permet de revenir en arrière à travers la chaîne des relations de cause à effet, en partant de l'état redouté vers l'état initial de fonctionnement normal, et d'extraire tous les scénarios possibles menant vers cet état. L'originalité des travaux consiste dans l'extraction des scénarios directement à partir d'un modèle RdP du système sans passer par le graphe d'accessibilité et en s'appuyant sur les arbres de preuves en logique linéaire qui permettent de gérer les ordres partiels. La méthode est appliquée dans le domaine de l'automobile sur le conjoncteur-disjoncteur électromécanique et le système des réservoirs.

Les travaux de thèse de Raphaël Schoenig [87] traitent de la sûreté de fonctionnement des systèmes mécatroniques. Ces travaux consistent à définir une méthodologie de conception des systèmes mécatroniques intégrant, dès les premières phases du cycle de développement, les aspects sûreté de fonctionnement. La méthodologie s'appuie sur les réseaux de Petri interprétés, orientés vers la méthode graphique et analytique, les graphes de Markov, qui apportent une garantie sur la qualité des systèmes développés, en tenant compte des contraintes de coût et de temps. Le graphe de Markov permet de modéliser les différents modes de fonctionnement existant (modes nominaux, dégradés, états redoutés). L'originalité des travaux consiste dans la représentation et l'évaluation de la fiabilité des systèmes dynamiques hybrides. Les principales étapes consistent à découpler la dynamique du système et la dynamique du processus de défaillance grâce à la théorie des perturbations singulières, puis d'identifier et d'estimer les grandeurs du système influençant la dynamique des défaillances. La méthode est appliquée sur un système de réservoir.

Les travaux de thèse de Alin Mihalache [69] traitent de la modélisation et de l'évaluation de la fiabilité des systèmes mécatroniques. Il a développé, dans ces travaux, une méthodologie d'évaluation de la fiabilité prévisionnelle, expérimentale et opérationnelle. Les systèmes mécatroniques sont représentés par des Réseaux de Petri Stochastiques Déterministes (RdPSD). La méthodologie d'évaluation de la fiabilité prévisionnelle s'appuie sur une modélisation fonctionnelle et dysfonctionnelle ainsi que l'utilisation des recueils de données pour les différents composants. Dans le cas de l'évaluation des fiabilité ex-

périmentale et opérationnelle, les données des essais de fiabilité ainsi que les données de retour d'expérience sont utilisées. Cette méthodologie, intégrant la démarche bayésienne, permet d'observer une nette amélioration des estimateurs et une réduction importante de l'intervalle de confiance pour la fiabilité expérimentale et opérationnelle par rapport aux estimateurs et aux intervalles de confiance obtenus par d'autres méthodes. La méthode est appliquée dans le domaine de l'automobile sur un système ABS.

Le but de notre travail consiste à estimer la fiabilité des systèmes mécatroniques qui constituent des systèmes dynamiques hybrides, reconfigurables et multitechnologie (mécanique, électronique et logiciel) ainsi que de proposer une démarche globale qui permet d'étudier les systèmes mécatroniques. Cette méthodologie doit comprendre plusieurs phases pour mieux traiter ces systèmes complexes :

1. L'analyse qualitative
   - Analyse fonctionnelle
   - Analyse dysfonctionnelle
2. L'analyse quantitative
   - Modélisation fonctionnelle et dysfonctionnelle
   - Simulations

Comme nous l'avons vu précédemment, l'analyse qualitative comporte deux types d'analyses : une fonctionnelle et une autre dysfonctionnelle.

Parmi les méthodes d'analyse fonctionnelle notre choix s'est arrêté sur la méthode SADT pour une raison en particulier : cette méthode s'applique à tout le système mécatronique, c'est à dire qu'elle s'adapte aussi bien aux composants mécaniques et électroniques qu'au logiciel. Ce qui n'est pas le cas des autres méthodes telles que le Bloc diagramme Fonctionnel (BdF), le Tableau d'Analyse Fonctionnelle (TAF), Reliasep, Functional Analysis System Technique (FAST) qui sont présentés en Annexe A. Cependant l'aspect dynamique des systèmes mécatroniques n'est pas pris en compte par la méthode SADT. C'est pourquoi nous nous intéressons à la méthode SA-RT qui est une extension temps réel à l'analyse structurée et qui comblera la lacune de la méthode SADT.

Dans l'analyse dysfonctionnelle, plusieurs méthodes existent et permettent de déterminer les dysfonctionnements d'un système. Pour en choisir une méthode parmi ces nombreuses méthodes d'analyse dysfonctionnelle, notre critère est de trouver une méthode qui s'applique aux différentes familles des composants d'un système mécatronique. Certaines des méthodes citées dans la partie dédiée à l'analyse dysfonctionnelle, telles que la méthode Table de Vérité (TV), Méthode du Diagramme Causes-Conséquences (MDCC), Méthode des Combinaisons de Pannes Résumées (MCPR) etc., deviennent lourdes lorsque le système est trop complexe et comporte un grand nombre de composants. Ces méthodes sont

présentées en Annexe B. D'autre part, ces méthodes citées s'appliquent principalement pour le matériel et non au logiciel ce qui n'est pas notre objectif recherché. Une des méthodes étudiées possède un équivalent qui s'adapte parfaitement à la partie logicielle c'est la méthode AMDE et l'AEEL. La combinaison de ces deux techniques nous permettrait de déterminer les défaillances des différents composants matériels (composants mécaniques et électroniques) ainsi que les dysfonctionnements que peut rencontrer le logiciel. Voilà pourquoi notre choix s'est concentré sur l'AMDE et son équivalent l'AEEL.

Après la détermination des fonctions d'un système et la mise en évidence de ces différents modes de défaillance, il est important de construire une architecture tolérante aux fautes et d'estimer les fiabilités système, composants et fonctions. C'est l'objectif principal des méthodes de modélisation et d'analyse quantitative telles que les chaînes de Markov, les réseaux de Petri, les réseaux Bayésiens, les réseaux de neurones, etc. Les réseaux de Petri Stochastiques Déterministes permettent d'analyser le comportement d'un système en présence de défaillances ainsi que d'effectuer une modélisation fonctionnelle et dysfonctionnelle. Cette modélisation dynamique permet de quantifier la fiabilité en assignant des valeurs numériques aux paramètres du modèle.

2.6 Conclusion

Dans ce chapitre, nous avons mis l'accent sur deux types d'analyses complémentaires qui sont l'analyse qualitative et l'analyse quantitative.

Dans la partie analyse qualitative, on retrouve deux groupes de méthodes : des méthodes d'analyse fonctionnelle qui permettent de lister toutes les fonctions d'un système complexe après avoir effectué une première analyse fonctionnelle externe, ainsi que des méthodes d'analyse dysfonctionnelle grâce auxquelles il est possible de mettre en évidence tous les modes de défaillance que peut subir un système. Les techniques d'analyse fonctionnelle sont indispensables pour identifier les fonctions des systèmes et de leurs composants. La méthode SADT est la plus intéressante pour étudier les systèmes mécatroniques car elle permet de décomposer n'importe quel système de manière hiérarchique. Cette méthode s'applique à tous les domaines qui nous intéressent à savoir la mécanique, l'électronique et le logiciel. L'aspect dynamique d'un tel système est traité, également, avec une méthode d'analyse structurée (SA) avec une extension temps réel. La méthode SA-RT nous permet d'approfondir, ainsi, notre connaissance du système à étudier.

En ce qui concerne l'analyse dysfonctionnelle, les méthodes AMDE et AEEL permettent d'étudier les différents composants que peut contenir un système mécatronique. Ces méthodes ont un avantage majeur qui consiste à détecter les défaillances des éléments

conduisant à la défaillance globale du système. Elles sont particulièrement pertinentes lorsqu'elles sont appliquées pour les composants mécaniques et électroniques dans le cas de l'AMDE et pour le logiciel dans le cas de l'AEEL.

La dernière étape caractérise la modélisation fonctionnelle et dysfonctionnelle d'un système mécatronique ainsi que l'estimation de sa fiabilité. Les réseaux de Petri Stochastiques Déterministes sont bien adaptés à nos critères recherchés et prennent en compte le comportement dynamique lié à ce système. Un autre point important pour ces réseaux réside dans leur facilité d'utilisation et de compréhension.

On s'intéresse aussi, dans ce chapitre, à la fiabilité dynamique ainsi qu'aux méthodes qui sont utilisées pour l'estimer. Les méthodes analytiques amènent à résoudre des systèmes mathématiques de taille considérable et la résolution de ces systèmes n'est possible qu'au niveau de cas-tests. Dans le cas des méthodes semi-analytiques, on sera confronté à un important problème de dimensions ce qui rend ces deux méthodes inapplicables dans le cas d'un système mécatronique. L'arbre d'événements dynamique discret a été l'outil le plus développé pour faire face aux problèmes de fiabilité dynamique, cependant comme son nom générique le suggère, il se prête plus spécifiquement aux études probabilistes de sûreté. Les réseaux Bayésiens dynamiques semblent constituer un outil mathématique intéressant pour modéliser ce problème en permettant une représentation graphique des processus stochastiques. Cependant si l'intérêt de l'approche est évident, son application à des problèmes physiques réels reste difficile. Les réseaux de Petri et automates stochastiques hybrides semblent être des outils bien adaptés pour traiter les problèmes générés par les systèmes dynamiques.

La troisième partie de ce chapitre consiste à présenter la fiabilité dans les différents domaines que combine un système mécatronique (fiabilité logicielle, fiabilité électronique et fiabilité mécanique). Mais comme on l'a déjà cité, un système mécatronique est un système dynamique dont la structure évolue au court du temps, il est donc nécessaire de présenter la fiabilité en fonction du temps et en particulier pour les composants mécaniques. Pour traiter ce problème, la méthode PHI2 apporte une solution au calcul de la fiabilité en fonction du temps basée uniquement sur les outils classiques de fiabilité instantanée. Son principal avantage est qu'elle permet de traiter des cas dont la dépendance envers le temps peut provenir aussi bien du chargement que de la dégradation des propriétés des matériaux. Elle repose sur une approximation FORM de deux états-limites successifs.

Enfin, la dernière partie de ce chapitre représente une synthèse sur les travaux précédemment réalisés ainsi qu'une comparaison entre les différentes méthodes utilisées durant les différentes étapes la méthodologie proposée (analyse fonctionnelle, analyse dysfonc-

tionnelle, modélisation, etc.). Cette comparaison a pour objectif de choisir les méthodes à utiliser dans la démarche globale pour l'étude des systèmes mécatroniques. La méthodologie est présentée dans le chapitre suivant.

Chapitre 3

Méthodologie proposée et application

Sommaire

3.1 Introduction

Comme nous l'avons déjà cité dans le premier chapitre, un des plus grands problèmes des systèmes mécatroniques concerne l'évaluation de leur fiabilité. Les méthodes d'estimation de cette fiabilité dans les différents domaines des composants qui constituent les systèmes mécatroniques (mécanique, électronique et logiciel), sont très différentes les unes des autres et il n'existe pas, à l'heure actuelle, une méthodologie permettant de mesurer la fiabilité de ces systèmes. De plus, les systèmes mécatroniques sont des systèmes complexes qui intègrent des aspects dynamiques, hybrides et reconfigurables.

Ainsi, ce chapitre est consacré à la méthodologie que nous avons développée pour résoudre les différents problèmes que peuvent engendrer les systèmes mécatroniques. La première partie de ce chapitre expose la problématique de ces systèmes dynamiques hybrides, la seconde partie explique le principe de la démarche que nous avons mis en place et pour finir la troisième partie est dédiée à l'application de cette méthodologie sur un système ABS.

3.2 Problématique

Un équipement mécatronique, tel qu'il est présenté dans le premier chapitre est, d'une part, un système caractérisé par son fonctionnement hybride, dynamique et reconfigurable et d'autre part, un système intégrant des composants de technologies différentes.

Le calcul de la fiabilité des systèmes mécatroniques n'est pas simple et plusieurs problèmes sont à considérer. Le premier problème consiste à prendre en compte de façon réaliste les interactions dynamiques existant entre les variables physiques et le comportement fonctionnel et dysfonctionnel du système ou de ses composants. Le calcul de cette fiabilité est complexe et nécessite l'intégration, dans le modèle de fiabilité, des interactions entre les phénomènes de défaillance et le profil de mission du système. Une formulation mathématique rigoureuse de la fiabilité dynamique impliquerait de connaître l'expression analytique des variables évoluant dans le temps puis d'exprimer les grandeurs recherchées en fonction de toutes ces variables.

De plus, les systèmes mécatroniques intègrent différentes technologies (électronique, mécanique, logiciel, etc.) et les méthodes et outils de travail changent en fonction du domaine du composant.

Tous ces aspects doivent être pris en compte lors du développement afin d'assurer la fiabilité de ces systèmes. Dans un premier temps, nous rappelons ces différents aspects qui caractérisent les systèmes mécatroniques.

3.2.1 Système 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).

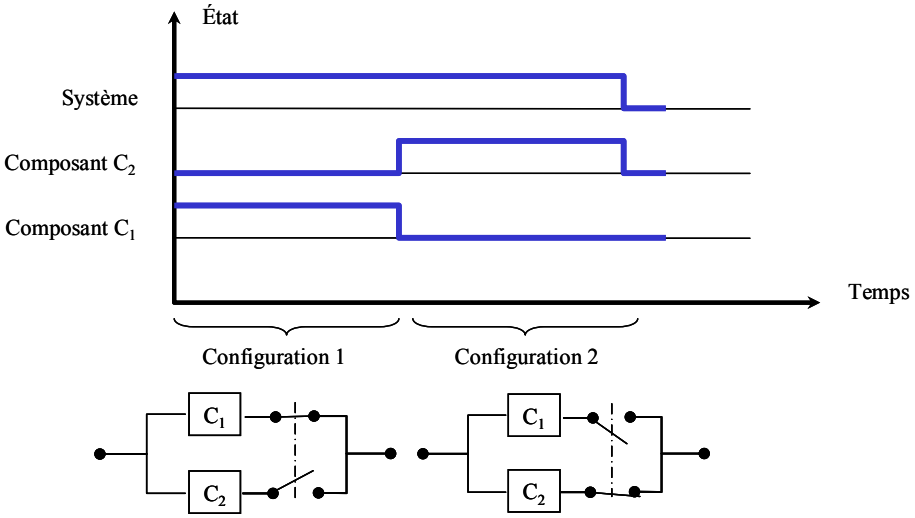

FIGURE 3.1 – Exemple de l'aspect hybride (continu et discret)

La description de ces systèmes mécatroniques peut faire intervenir explicitement et simultanément un état continu et un état discret tel qu'est montré sur la figure 3.1. Le système fonctionne en continu alors que l'utilisation des composants C_1 et C_2 est discrète ou périodique.

Ainsi, le fonctionnement d'un système comportant une redondance passive est assuré par le composant C_1 alors que le composant C_2 est au repos (a priori pas d'usure de celui-ci). 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 tel que les défaillances des composants.

3.2.2 Système dynamique

L'aspect dynamique d'un système mécatronique est caractérisé par les relations fonctionnelles entre les composants qui le constituent.

Si ces relations reste figées tout au long de la mission du système, il sera dit statique.

Si, au contraire, ces relations changent au court de la mission, il sera dit dynamique. Ce système dynamique est prévu pour remplir plusieurs fonctions alternativement ou remplir une fonction en utilisant ses ressources de plusieurs manières différentes.

Les changements de ces relations sont liés au profil de mission du système qui est influencé par différents paramètres tels que les utilisateurs qui l'utilisent, les sollicitations externes qu'il subit ou encore l'environnement où il se trouve (figure 3.2).

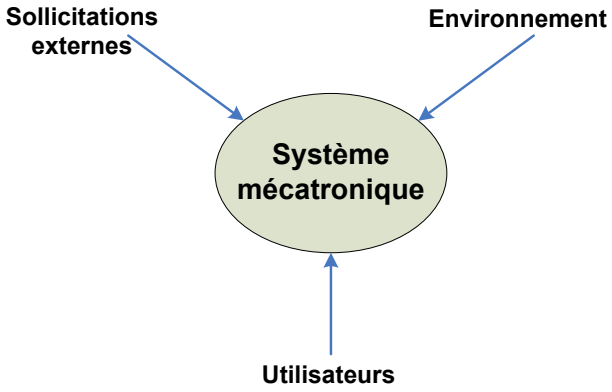

FIGURE 3.2 – Paramètres influant sur le profil de mission d'un système

En effet, le système subit des sollicitations externes qui jouent un rôle important dans le profil de mission. Ces sollicitations externes (charges, vitesse, etc.) peuvent influencer le passage d'un état du système à un autre. Notre intérêt, dans ce travail, se portera particulièrement sur ces sollicitations externes.

Les utilisateurs peuvent influencer le profil de mission d'un système car chaque utilisateur a son propre mode d'utilisation et chaque utilisation peut modifier le profil de mission de ce système.

Pour finir, l'environnement dans lequel le système se trouve (humidité, température, etc.) agit également sur le profil de mission.

3.2.3 Système reconfigurable

Comme nous l'avons présenté dans le premier chapitre, la systémique est une démarche permettant l'étude des systèmes complexes tels que les systèmes mécatroniques. Cette approche vise à maintenir un état stable des objectifs désirés.

Ainsi, le contrôle d'un système 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. En d'autre termes, la reconfiguration dynamique permet d'améliorer la stabilité des systèmes.

La stabilité d'un système peut être représentée comme sur la figure 3.3 :

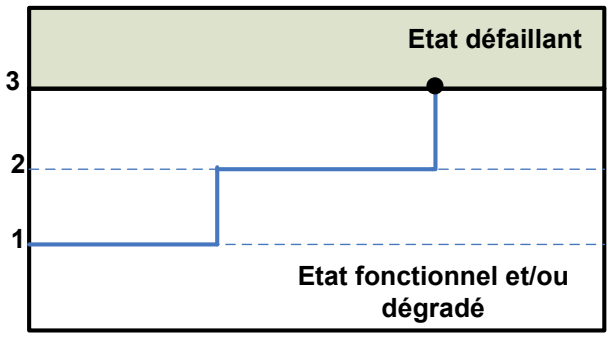

FIGURE 3.3 – Exemple de représentation de l'évolution de la stabilité d'un système

Considérant l'exemple présenté sur la figure 3.1, l'état 1 représente le fonctionnement nominal du système (aucune défaillance des composants C_1 et C_2), l'état 2 illustre le fonctionnement du système en présence d'une défaillance (composant C_1) et l'état 3 représente le cas où les deux composants C_1 et C_2 sont défaillants.

On cherche donc à maintenir la configuration dans les états 1 et 2 où le système est stable, et ne pas se trouver dans l'état 3, où le système est défaillant.

Pour maintenir la stabilité d'un système, il est impératif de construire une architecture tolérante aux fautes. Cette architecture représente un système qui peut changer la configuration des relations fonctionnelles entre certains de ses composants sans interrompre sa mission. Il est donc appelé système à configuration dynamique ou système reconfigurable.

Un exemple d'une architecture tolérante aux fautes est montré sur la figure 3.4 :

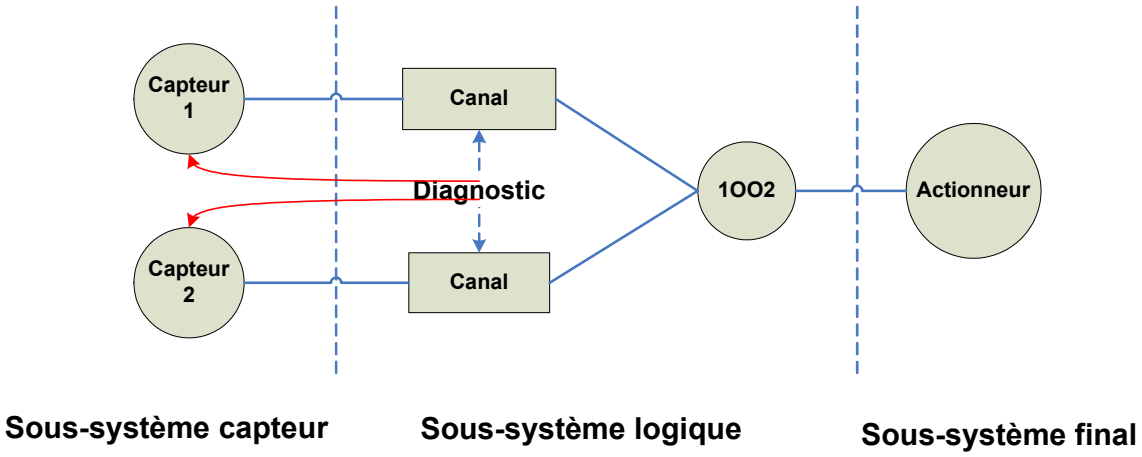

FIGURE 3.4 – Architecture tolérante aux fautes d'un système mécatronique

Cette architecture comprend deux canaux connectés en parallèle et il faudra, au moins, qu'un capteur sur deux fonctionne. Ce qui permettrait, en cas de défaillance d'un des deux capteurs, d'avoir un système fonctionnel. Cette redondance a pour objectif d'augmenter

la disponibilité du système et ainsi d'améliorer sa performance. On pourrait également faire un programme de diagnostic qui permettrait de comparer les deux valeurs envoyées par les capteurs lorsqu'ils sont tous les deux en fonctionnement. Si une différence entre les deux valeurs des capteurs est diagnostiquée , une valeur test est envoyée aux deux capteurs afin d'identifier laquelle de ces deux valeurs est erronée.

A travers cet exemple, nous avons expliqué comment construire des systèmes stables et qui peuvent fonctionner même en présence de fautes en changeant leur configuration et en basculant vers un autre état fonctionnel.

Voici un schéma (chronogramme) qui permet d'illustrer l'aspect hybride, dynamique et reconfigurable que nous venons d'exposer (figure 3.5) :

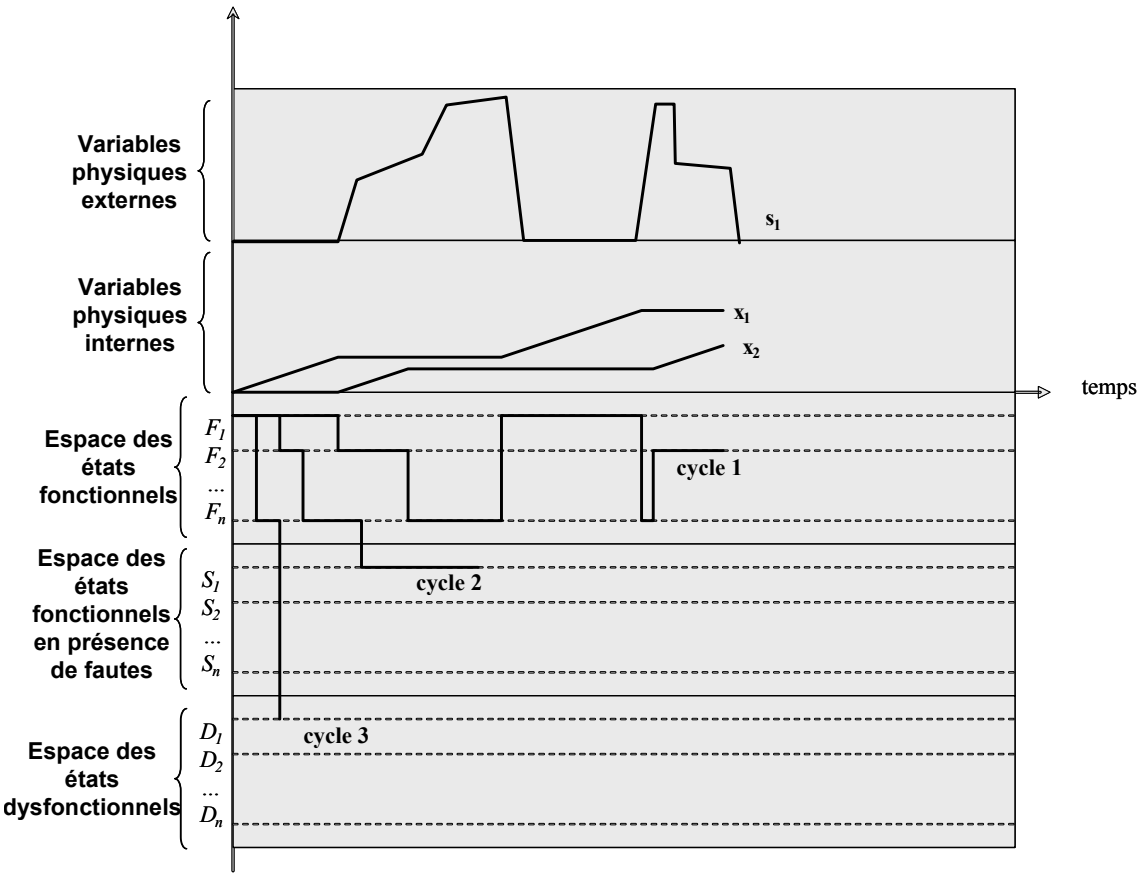

FIGURE 3.5 – Chronogramme

Sur la figure 3.5 on retrouve les variables physiques internes x_i (grandeurs physiques caractéristiques du fonctionnement du système) et les variables physiques externes s_i (sollicitations externes au système qui agissent sur l'état de celui-ci). Ces variables internes et externes représentent le coté hybride (continu + discret) d'un système mécatronique.

Ces variables physiques peuvent engendrer 3 principaux états où le système mécatro-

nique peut se trouver :

- Le premier état représente l'état fonctionnel F_i du système. Dans cet état le système fonctionne normalement et ne rencontre aucun problème ;
- Le deuxième état S_i correspond au fonctionnement en présence de fautes. Lorsque l'on construit un système stable grâce à une architecture tolérante aux fautes, le système peut changer de configuration afin d'éviter l'effet de la défaillance sur le système. En d'autre terme le système continue à fonctionner malgré la présence de fautes.
- Enfin le troisième état concerne l'état de dysfonctionnement D_i où le système mécatronique est défaillant.

Ces variables internes et externes peuvent provoquer plusieurs cycles de fonctionnement différents. Considérons, par exemple, les trois cycles de fonctionnement illustrés sur la figure 3.5 :

- Le cycle 1 correspond au fonctionnement classique du système associé à la sollicitation s_1. En fonction du niveau de sollicitation s_i, le système change d'état. Les variables internes x_1 et x_2 correspondent aux temps de fonctionnement du système dans les états F_1 et F_2 ;
- Le cycle 2 représente le système basculant d'un fonctionnement nominal à un fonctionnement dégradé. Dans ce cas le système remplit sa fonction malgré la présence de fautes et ce grâce à la construction d'architectures tolérantes aux fautes. C'est l'aspect reconfigurable des systèmes mécatroniques ;
- Le cycle 3 illustre le cas d'un système passant d'un fonctionnement nominal à un état dysfonctionnel. Ce dysfonctionnement peut être dû à la défaillance de plusieurs composants par exemple.

Prenons un exemple d'une variable interne x_1 telle que l'usure d'une pièce mécanique.

La variable x_1 augmente en fonction du temps comme montré sur la figure 3.6. X_1 représente le seuil de l'usure de la pièce mécanique à ne pas dépasser.

Le franchissement de ce seuil provoque la défaillance du système. C'est-à-dire que le cycle 1 (figure 3.6) passe d'un état de fonctionnement F_i à un état dysfonctionnel D_i.

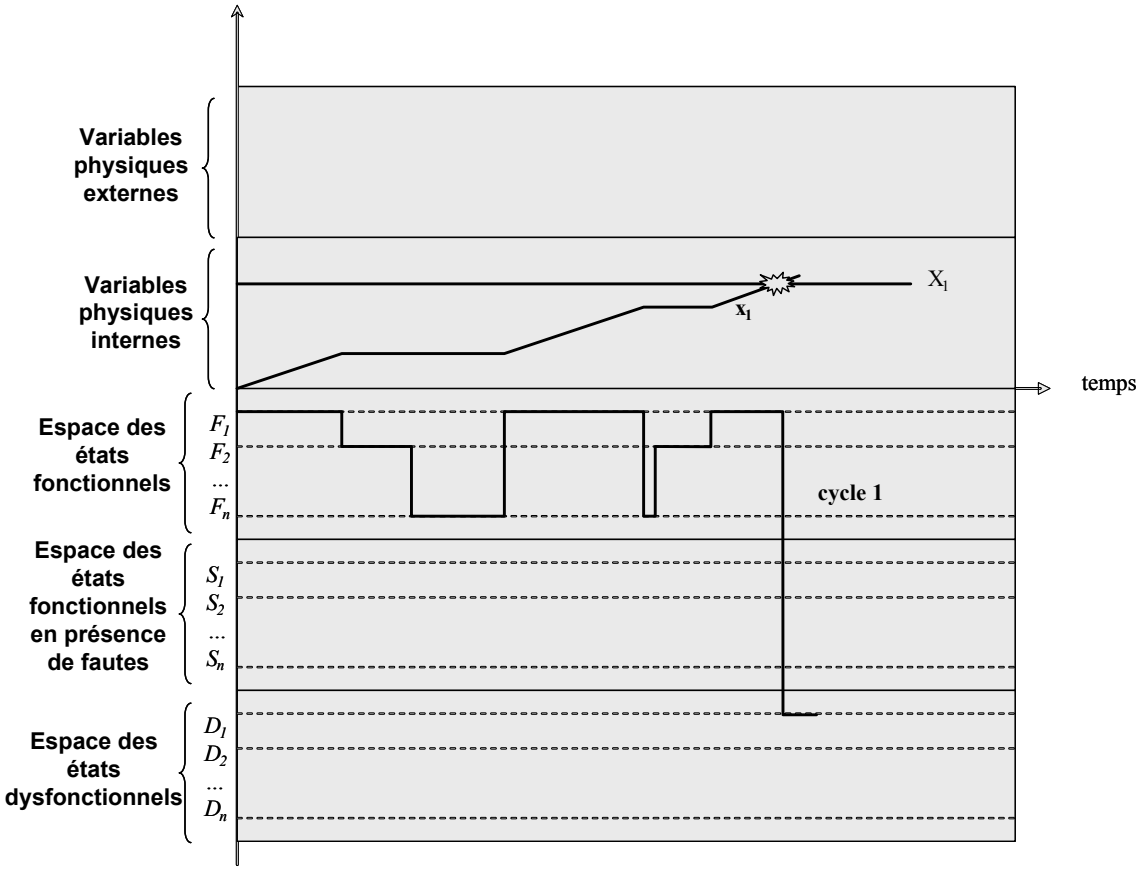

FIGURE 3.6 – Exemple d'un franchissement de seuil

3.2.4 Système intégrant plusieurs technologies

Les systèmes mécatroniques intègrent des composants de technologies différentes : mécanique, hydraulique, électromécanique, électronique, logiciel, etc. Cette hétérogénéité se traduit par des démarches d'analyse de fiabilité distinctes. En particulier, les composants mécaniques spécifiques font l'objet de techniques particulières d'estimation de fiabilité (Monte Carlo, FORM/SORM, PHI2, etc.). En plus, l'aspect dynamique et hybride d'un tel système fait que certains composants fonctionnent que périodiquement par rapport à d'autres qui le sont tout le temps.

Aussi, la conception des systèmes mécatroniques, comportant une intégration élevée de composants de technologies différentes et relevant de plusieurs disciplines, nécessite, dès le début de l'étude, un travail collaboratif entre les différents acteurs du développement, afin de réaliser un produit industriel compétitif et de qualité. La difficulté principale réside dans la pluridisciplinarité se traduisant par des modélisations distinctes et ne permettant pas un développement intégré. Pourtant, il est nécessaire de disposer d'une démarche unique qui permet de construire la fiabilité.

La problématique étant exposée, dans le paragraphe suivant nous proposons une méthodologie permettant l'estimation de la fiabilité des systèmes mécatroniques en tenant compte de tous ses aspects (hybride, dynamique, reconfigurable et multitechnologies) présentés précédemment.

3.3 Principe de la démarche

A l'heure actuelle, il n'existe pas de méthodologie globale qui permet d'estimer la fiabilité des systèmes mécatroniques en tenant compte des différents aspects de ces systèmes : hybride, dynamique, reconfigurable et multitechnologies.

Aussi, nous proposons une méthodologie de construction de la fiabilité en abordant les points suivants :

- les fonctions à remplir ;
- les profils de mission (utilisation et environnement) ;
- effets des défaillances des composants sur le système ;
- les mécanismes de tolérance aux fautes (architecture matériel et logiciel) ;
- hétérogénéité technologique des composants (mécanique, électronique, logiciel, etc.) ;
- dynamique de fonctionnement (description physique du fonctionnement) ;
- défaillance des composants (lois de fiabilité pour chaque composant) ;
- modèle fonctionnel et dysfonctionnel (modèle unifié) ;
- Estimation de la fiabilité aux niveaux système, fonction et composant.

En se basant sur l'approche systémique, définie dans le chapitre 1, ainsi que sur les points que nous venons de citer, nous avons développé une méthodologie globale dans le but d'estimer la fiabilité des systèmes mécatroniques (figure 3.7).

Le principe de cette méthodologie que nous proposons, comme le montre la figure 3.7, est fondé sur deux grande étapes : une étape d'analyse qualitative et une autre d'analyse quantitative.

Comme nous l'avons déjà cité, il est important de construire des systèmes stables afin d'assurer la continuité des objectifs à atteindre. C'est pour cette raison que la première étape de notre méthodologie concerne l'analyse qualitative grâce à laquelle nous pourrons construire cette architecture. L'analyse qualitative se déroule en 3 étapes (l'observable, l'investigation systémique et la modélisation qualitative) qui seront présentées dans le paragraphe suivant.

La deuxième étape représente l'analyse quantitative durant laquelle nous traiterons la fiabilité dynamique du système mécatronique. Cette partie d'analyse quantitative est, elle aussi, décomposée en plusieurs étapes (modélisation dynamique et simulation) et sera

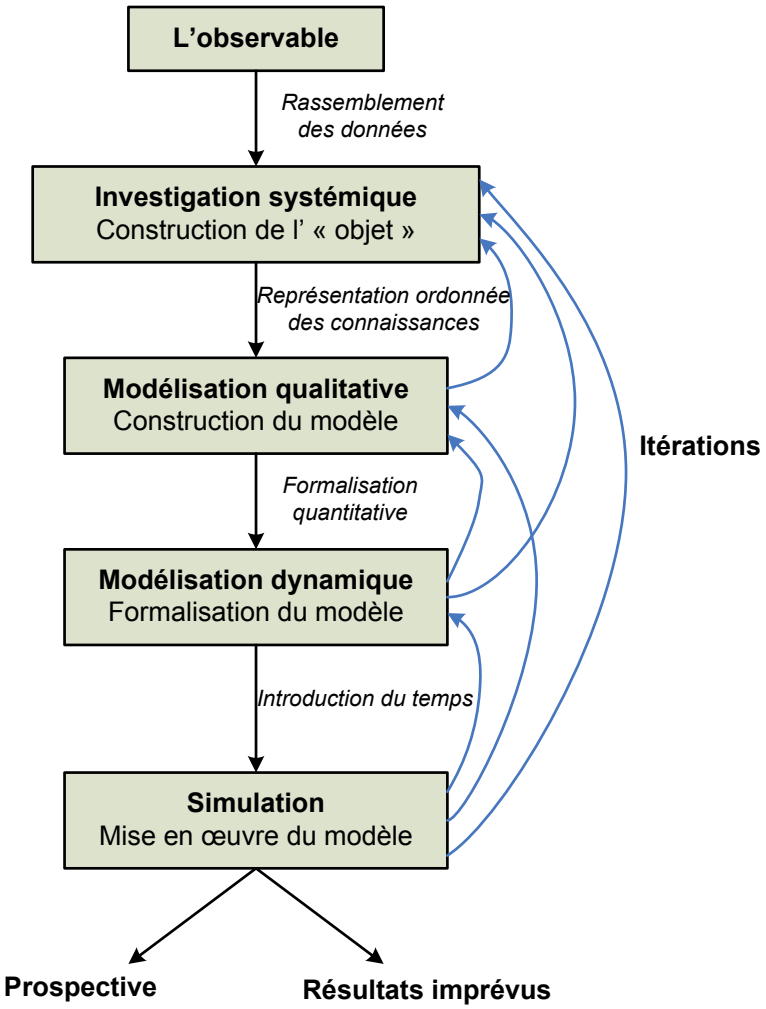

FIGURE 3.7 – Démarche globale pour l'évaluation, la modélisation et l'estimation de la fiabilité d'un système mécatronique [33]

développée plus loin dans ce chapitre.

Nous proposons une démarche systémique imbriquant les différentes phases suivantes (figure 3.7) :

1. **L'observable :** Cette phase nous permet de rassembler les données liées au système mécatronique à concevoir à travers un cahier des charges afin de spécifier les besoins des clients.

2. **Investigation systémique :** Cette phase consiste à obtenir une représentation ordonnée des connaissances. Elle englobe deux étapes importantes qui sont l'analyse fonctionnelle et l'analyse dysfonctionnelle. Ces deux analyses fournissent des connaissances en ce qui concerne les fonctions internes du système (fonctionnement nominal) ainsi que les différents modes de défaillance que ce système peut rencontrer.

3. **Modélisation qualitative :** Elle permet de construire le modèle représentant le système à étudier en tenant compte des informations obtenues grâce aux étapes précédentes.
4. **Modélisation dynamique :** Cette modélisation consiste, d'une part, à construire un modèle physique qui prend en compte l'aspect dynamique du système mécatronique afin d'obtenir les variables physiques internes à partir d'un profil de mission. D'autre part, de construire les loi de fiabilité des composants constituant le système mécatronique.
5. **Simulation :** Cette dernière phase consiste à simuler le modèle dynamique construit grâce à l'enchaînement des différentes étapes citées précédemment afin d'estimer la fiabilité des systèmes complexes et analyser les résultats obtenus dans le but d'améliorer la qualité de ce système.

La phase de l'observable, représentant l'étape de spécification des besoins par les clients, constitue les données d'entrée nécessaires pour l'étude d'un système mécatronique. Les quatre étapes restantes qui sont : l'investigation systémique, la modélisation qualitative, la modélisation dynamique et la simulation sont détaillées dans le paragraphe suivant.

3.3.1 Investigation systémique

L'objectif de l'investigation systémique (ou l'analyse qualitative) est, comme déjà défini dans le chapitre 2, d'identifier toutes les fonctions d'un système ainsi que toutes les causes de défaillance pouvant affecter son bon fonctionnement. Cette analyse qualitative est généralement composée de deux grandes étapes qui sont l'analyse fonctionnelle et l'analyse dysfonctionnelle (figure 3.8).

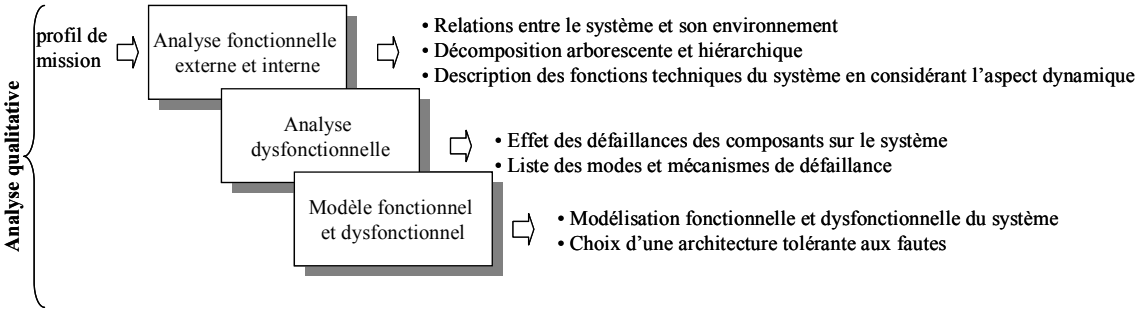

FIGURE 3.8 – Etapes de l'analyse qualitative d'un système mécatronique

La figure 3.8 représente les différentes étapes de l'analyse qualitative. A partir du profil de mission et des besoins formulés par les clients, une première étape représentant l'analyse

fonctionnelle (interne + externe) est effectuée. Cette analyse fonctionnelle nous permet d'identifier les relations entre le système et son environnement ainsi que les différentes fonctions du système à concevoir.

Les résultats obtenus par cette première analyse sont indispensables pour effectuer l'analyse dysfonctionnelle qui constitue la deuxième étape de l'analyse qualitative. Cette analyse dysfonctionnelle a pour objectifs d'identifier les modes et les mécanismes de défaillance ainsi que leurs effets sur le système.

La dernière étape de l'analyse qualitative consiste à construire un modèle fonctionnel et dysfonctionnel en tenant compte des informations obtenues à partir de l'analyse fonctionnelle et de l'analyse dysfonctionnelle effectuées précédemment. Cette dernière étape nous permet de modéliser le système dans le but de construire des systèmes stables.

3.3.1.1 Analyse fonctionnelle

L'analyse fonctionnelle permet la description synthétique des modes de fonctionnement d'un système et la connaissance des fonctions à garantir. En d'autres termes, elle consiste à rechercher et à caractériser les fonctions offertes par un système pour satisfaire les besoins de son utilisateur (figure 3.9)

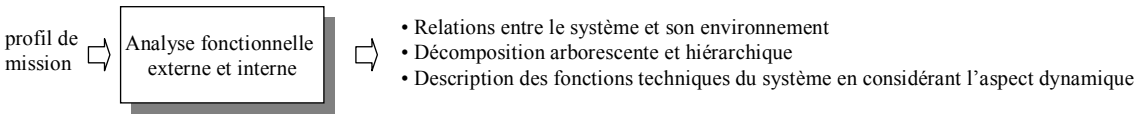

FIGURE 3.9 – Analyse fonctionnelle

Comme le montre la figure 3.9, l'analyse fonctionnelle est décomposée en deux parties :

- **Analyse Fonctionnelle Externe (AFE) :** Cette Analyse Fonctionnelle Externe permet d'illustrer les relations entre un système et son milieu extérieur. Nous avons choisi d'utiliser la méthode développée par le cabinet APTE détaillée dans le chapitre 2. Après cette analyse, les fonctions internes au système ne sont pas déterminées et l'application d'une Analyse Fonctionnelle Interne est nécessaire.
- **Analyse Fonctionnelle Interne (AFI)** : L'Analyse Fonctionnelle Interne permet de réaliser une décomposition arborescente et hiérarchique du système en éléments. Elle décrit également les fonctions techniques du système. Parmi les méthodes d'analyse fonctionnelle notre choix s'est arrêté sur la méthode SADT pour une raison en particulier : cette méthode s'applique à tout le système mécatronique, c'est à dire qu'elle s'adapte aussi bien aux composants mécaniques et électroniques qu'au logiciel. Nous nous intéressons aussi à la méthode SA-RT qui est une extension temps-réel à l'analyse structurée. C'est une des méthodes les plus utilisées et elle permet

de prendre en compte l'aspect dynamique, qui manque à la méthode SADT, d'un système mécatronique. De plus, à partir de la méthode SA-RT nous pouvons avoir une traduction ou une correspondance avec les réseaux de Petri comme le montre la figure 3.10.

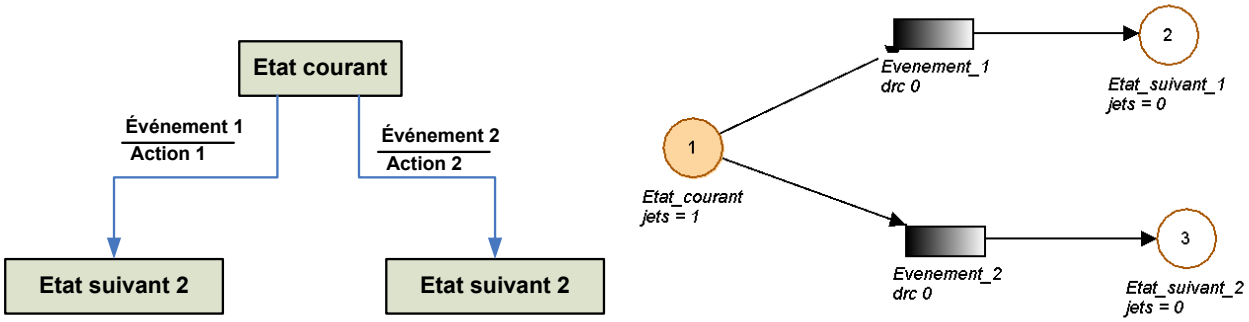

FIGURE 3.10 – Correspondance entre le diagramme état/transition de la méthode SA-RT et les réseaux de Petri

3.3.1.2 Analyse dysfonctionnelle

L'analyse fonctionnelle précédemment étudiée, n'apporte aucune information sur les défaillances potentielles que peut rencontrer un système mécatronique. Pour cette raison l'utilisation de l'analyse dysfonctionnelle est nécessaire dans le but de nous fournir ces informations manquantes. Ceci nous permet de déterminer les causes de défaillance ainsi que de spécifier les différents états du système.

Pour effectuer l'analyse dysfonctionnelle, nous avons besoin des informations obtenues après l'analyse fonctionnelle. En d'autre termes, les sorties ou les résultats de l'analyse fonctionnelle (figure 3.9) constituent les entrées ou les bases de l'analyse dysfonctionnelle comme le montre la figure 3.11.

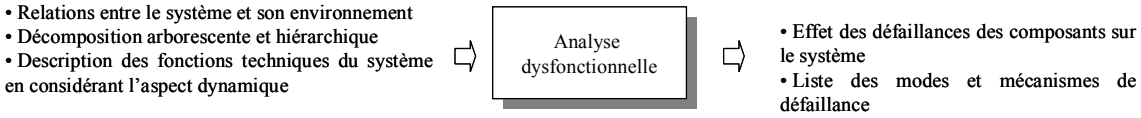

FIGURE 3.11 – Analyse dysfonctionnelle

Il existe plusieurs méthodes permettant de déterminer les dysfonctionnements d'un système. Cependant, la majorité de ces méthodes s'appliquent uniquement pour la partie matérielle (composants mécaniques, électroniques, etc.). Une de ces méthodes d'analyse dysfonctionnelle (AMDE) possède un équivalent qui s'adapte parfaitement à la partie logicielle c'est l'AEEL. La combinaison de ces deux techniques (AMDE + AEEL) nous permet de traiter un système mécatronique en tenant compte de l'aspect multitechnologies.

3.3.2 Modélisation qualitative

Comme nous l'avons déjà présenté dans le chapitre 2, les réseaux de Petri sont très utilisés dans la modélisation et l'étude de sûreté de fonctionnement des systèmes dynamiques. De plus, ces réseaux de Petri permettent de modéliser, d'une part, le fonctionnement normal d'un système et, d'autre part, son comportement en présence de fautes. Voilà pourquoi nous avons choisi d'utiliser les réseaux de Petri pour la modélisation fonctionnelle et dysfonctionnelle d'un système mécatronique ainsi que pour l'estimation de sa fiabilité.

Afin de construire un modèle fonctionnel et dysfonctionnel, il est impératif de passer par les deux étapes que nous venons d'exposer qui sont : l'analyse fonctionnelle et l'analyse dysfonctionnelle (l'investigation systémique). Les résultats de ces deux analyses constituent le point de départ dans la construction du modèle comme illustré sur la figure 3.12.

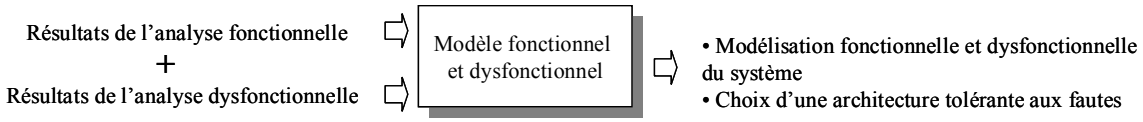

FIGURE 3.12 – Modélisation fonctionnelle et dysfonctionnelle

Cette étape de la méthodologie nous permet d'avoir, d'une part, un modèle fonctionnel et dysfonctionnel et ainsi représenter le comportement du système durant son fonctionnement nominal et son comportement en présence de fautes, et d'autre part, de construire une architecture tolérante aux fautes dans le but de construire des systèmes stables.

L'analyse fonctionnelle précédemment effectuée, nous donne la possibilité de modéliser un système pour représenter son fonctionnement nominal. C'est ce que l'on nomme par *modélisation fonctionnelle*. Les informations que fournitè cette analyse fonctionnelle seront ainsi utilisées pour construire le modèle fonctionnel tel qu'il est présenté sur l'exemple de la figure 3.13.

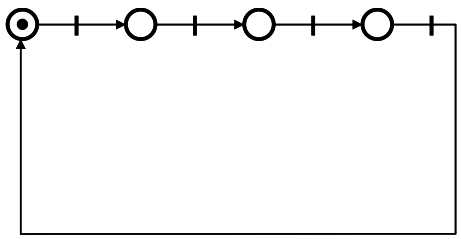

FIGURE 3.13 – Exemple d'un réseau de Petri fonctionnel

Les différents modes de défaillance obtenus grâce à l'analyse dysfonctionnelle sont

utilisés pour compléter le réseau de Petri de la figure 3.13 ce qui donne naissance au nouveau réseau montré sur la figure 3.14.

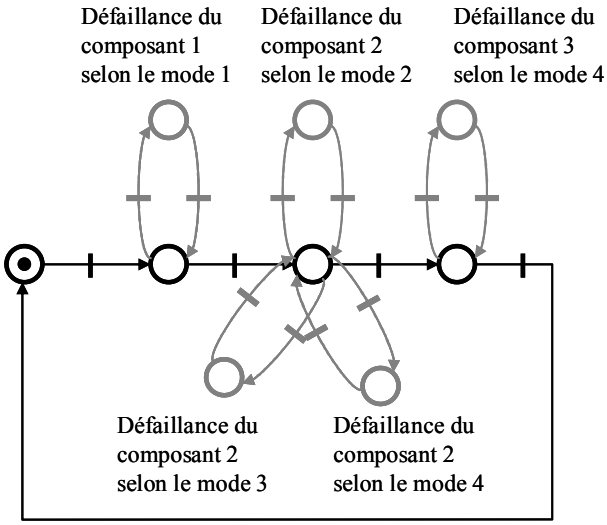

FIGURE 3.14 – Exemple d'un réseau de Petri fonctionnel et dysfonctionnel

Cette figure 3.14 représente, donc, une *modélisation fonctionnelle et dysfonctionnelle* du système mécatronique. En effet, le réseau de Petri que montre cette figure, représente le fonctionnement nominal du système ainsi que ses dysfonctionnements. On constate sur ce réseau que le composant 2 possède plusieurs modes de défaillance. Ces modes de défaillance ont été mis en évidence grâce à l'analyse dysfonctionnelle (AMDE, AEEL).

En résumé, l'analyse qualitative fournit des informations sur le fonctionnement et le dysfonctionnement d'un système mécatronique, mais ne donne aucune information sur les quantités telle que la probabilité de défaillance. Afin de la compléter, on se doit de faire une analyse quantitative qui aura pour données d'entrée les informations obtenues après l'analyse qualitative. L'analyse quantitative constitue la deuxième partie de notre méthodologie et permet d'estimer la probabilité de défaillance du système étudié.

3.3.3 Modélisation dynamique

La phase de la modélisation dynamique constitue la première étape de l'analyse quantitative. Cette analyse quantitative consiste à évaluer la probabilité d'apparition d'un événement qui peut se produire sur un système. Les étape de l'analyse quantitative sont montrées sur la figure 3.15.

Ces deux étapes qui constituent l'analyse quantitative sont détaillées et peuvent être organisées de la manière suivante (figure 3.16) :

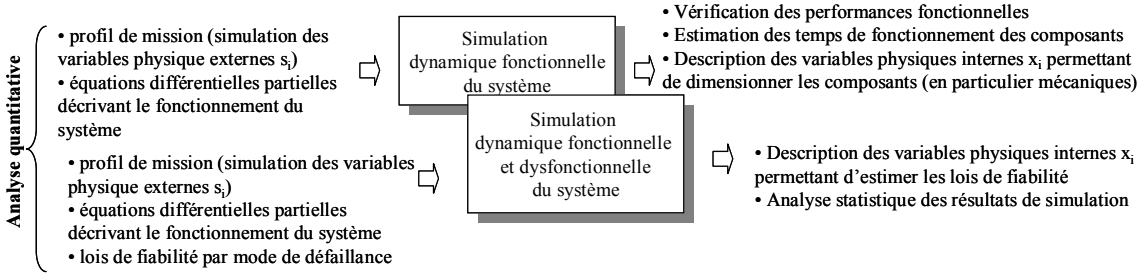

FIGURE 3.15 – Analyse quantitative

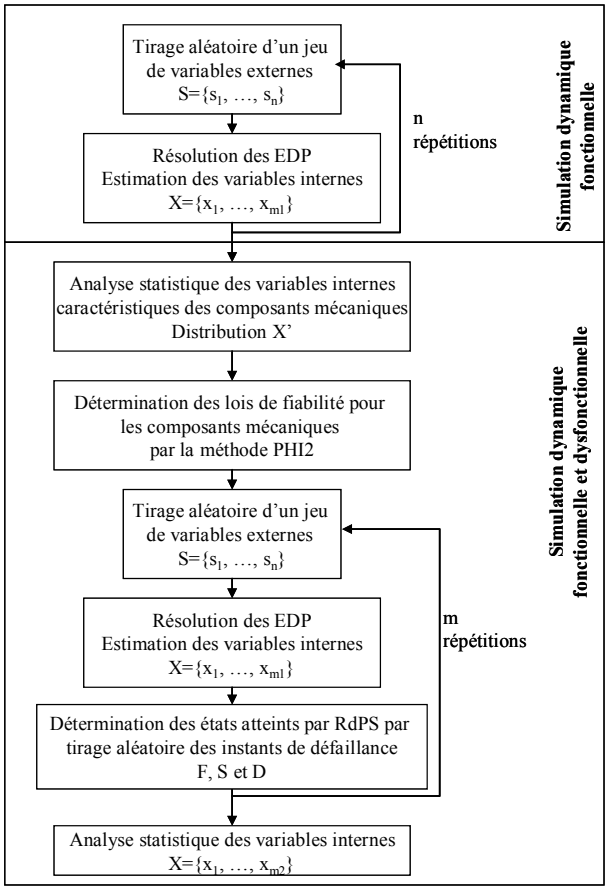

FIGURE 3.16 – Différentes étapes de l'analyse quantitative

Dans la partie analyse qualitative, nous avons modélisé le système à étudier grâce au réseaux de Petri. Ces réseaux sont décrits par un 5-tuplé *(P,T,M_0,Pré,Post)* sachant que P représente les places du réseau de Petri, T ses transitions, M_0 le marquage initial, *pré* l'application d'incidence avant et *Post* l'application d'incidence arrière.

P, *Pré* et *Post* sont associés à la structure du réseau de Petri, M_0 représente l'état du système à l'instant $t = 0$. L'évolution de ce marquage initial M_0 représente la dynamique du système mécatronique. Cette dynamique est pilotée par les transitions T de ce réseau

auxquelles il faut associer des informations obtenues par la simulation dynamique.

La première étape consiste à effectuer des simulations dynamiques fonctionnelles du système en tenant compte du profil de mission (simulations des variables physiques externes s_i) et en utilisant les équations différentielles partielles décrivant le fonctionnement du système. Ces simulations dynamiques fonctionnelles nous permettent de connaître le temps de fonctionnement de chaque composant, la description des variables internes x_i, etc.

La deuxième étape consiste à réaliser des simulations dynamiques fonctionnelles et dysfonctionnelles. Après avoir déterminé les variables physiques internes x_i, on se doit de faire une analyse statistique sur les résultats obtenus et prendre en compte uniquement les variables physiques internes caractéristiques des composants mécaniques nommées X'

A partir des ces variables physiques internes X', nous pouvons déterminer les lois de fiabilité pour les composants mécaniques par la méthode PHI2.

Une autre étape de l'analyse quantitative concerne la détermination des états atteints par le réseau de Petri qui sont F, S ou D (F : fonctionnement normal, S : fonctionnement dégradé, D : dysfonctionnement). Pour cela, on utilise les variables physiques internes du système qui sont obtenues à partir d'un tirage aléatoire des variables physiques externes s_i (profil de mission) afin de simuler le comportement du réseau de Petri construit précédemment.

Ainsi, le but de cette analyse quantitative consiste à estimer la fiabilité dynamique d'un système mécatronique. Comme nous l'avons déjà vu dans le chapitre 2, la fiabilité dynamique s'écrit sous la forme suivante (équation 3.1) :

$$R_S(t) = P\left[f_S(t, F, S, D) = 1\right]_{[0,t]} \tag{3.1}$$

Pour finir, une analyse statistique des résultats obtenus nous permettra d'estimer la fiabilité système, composants et fonctions.

Avant de présenter les différentes parties de l'analyse quantitative, faisons tout d'abord un petit rappel concernant les équations différentielles qui nous permettent d'obtenir une description physique du fonctionnement d'un système.

3.3.3.1 Equations différentielles

Les équations différentielles sont utilisées pour construire des modèles mathématiques de phénomènes physiques. Ces équations expriment le mouvement ou la dynamique d'un système en tenant compte de la variabilité de son profil de mission qui peu être due à des variabilités de la charge, de la vitesse, etc.

Une des plus célèbres équations différentielles est la relation fondamentale de la dynamique de Newton $\sum f = m.a.$ f représente la force, m la masse et a l'accélération.

Considérons l'exemple masse-ressort présenté sur la figure 3.17

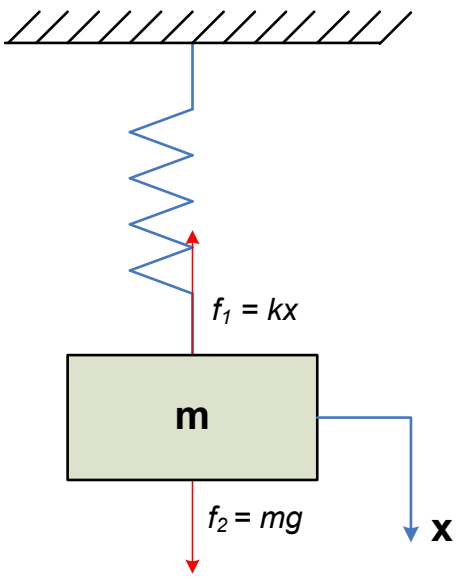

FIGURE 3.17 – Exemple d'un système physique

La relation de Newton est (équation 3.2) :

$$\sum f = m \cdot a = m \cdot \frac{dv}{dt} = m \cdot \dot{v} \tag{3.2}$$

Pour les deux forces f_1 et f_2, l'équation 3.2 devient (équation 3.3) :

$$f_1 - f_2 = m \cdot \dot{v} \tag{3.3}$$

La vitesse est donc égale à (équation 3.4) :

$$\dot{v} = \frac{f_1 - f_2}{m} \Rightarrow v = \int \frac{f_1 - f_2}{m} \cdot dt + v_0 \tag{3.4}$$

Pour résoudre ces équations différentielles nous passons par Simulink. C'est un outil qui permet de modéliser, de simuler et d'analyser les systèmes dynamiques. A partir de ces équations, construisons le modèle physique dans Simulink comme montré sur la figure 3.18 :

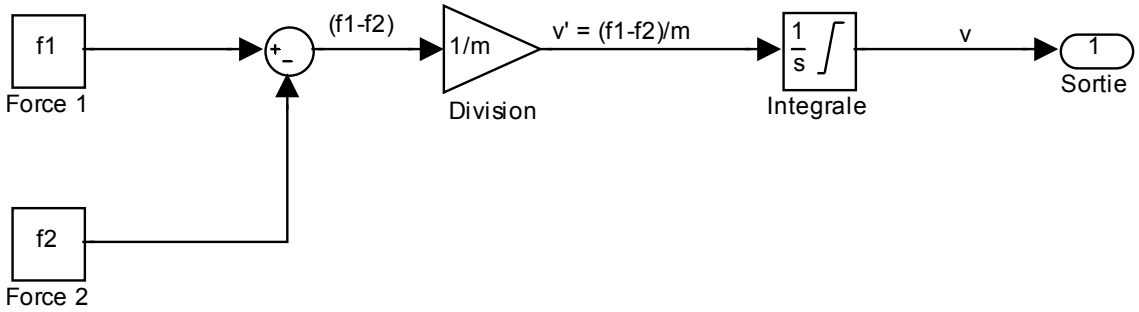

FIGURE 3.18 – Exemple d'une modélisation dynamique dans Simulink

Ce modèle physique permet de déterminer les variables physiques internes en faisant des simulations de celui-ci. Pour effectuer ces simulations nous considérons les valeurs données dans le tableau 3.1

Données	**Valeurs**
k	20 (N/m)
g	10 (m/s^2)
m	100 (g)

TABLE 3.1 – Données de simulations de l'exemple (figure 3.18)

k est le coefficient de raideur du ressort, g la gravité et m représente la masse du solide. La force f_1 et f_2 sont données par :

$$f_1 = m \cdot g \; et \; f_2 = k \cdot x \tag{3.5}$$

La force f_1 est considérée comme constante alors que f_2 varie en fonction du déplacement x (variabilité du profil de mission). Cette force f_2 est présentée sur la figure 3.19.

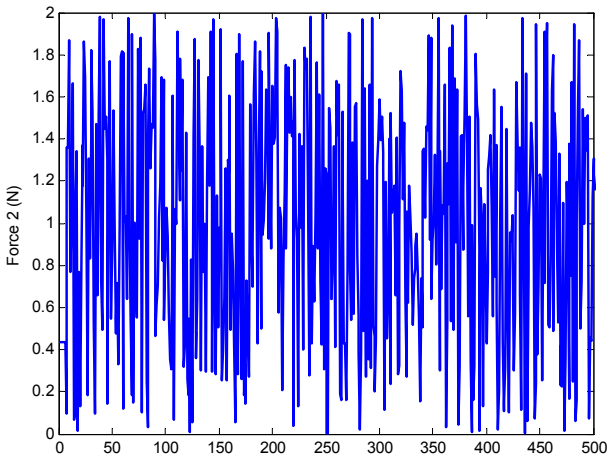

FIGURE 3.19 – Valeurs aléatoires de de la force f_2 en N

Etant donné la variabilité du profil de mission et de la force f_2 nous obtenons une variabilité dans les résultats des simulations. Nous avons représenté, sur la figure 3.20, la vitesse du solide.

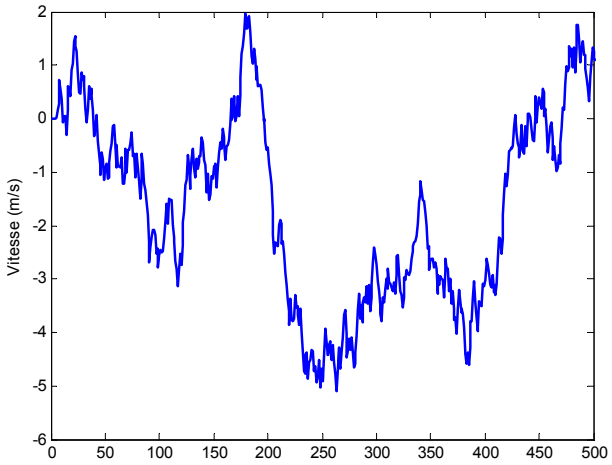

FIGURE 3.20 – Résultats obtenues pour la vitesse en (m/s)

3.3.3.2 Estimation des variables internes $\mathbf{x}_i$

La première partie des étapes constituant l'analyse quantitative de la figure 3.16 concerne la simulation dynamique fonctionnelle qui est présentée sur la figure 3.21. Cette partie nous permet d'estimer les variables physiques internes x_i du système mécatronique, les temps de fonctionnement de ses différents composants, etc.

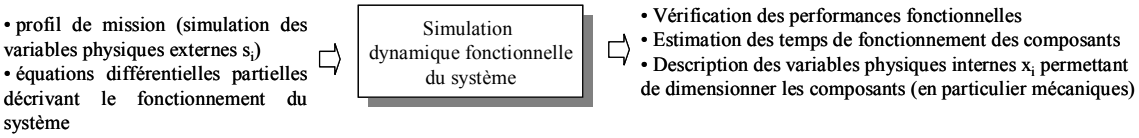

FIGURE 3.21 – Simulation dynamique fonctionnelle du système

Reprenons l'exemple de la figure 3.6 où la variable x_1 représente une variable interne du système. Le problème qui se pose à nous est : Comment obtenir ces variables physiques internes ?

L'analyse qualitative précédemment effectuée permet d'illustrer l'ensemble du fonctionnement d'un système qui peut être décrit par des équations différentielles partielles (EDP) associées à ce même système. Les variables internes d'un système x_i (efforts internes, temps de fonctionnement des différents composants, etc.) dépendent des variables externes s_i auxquelles il est soumis (niveau de sollicitation, conditions limites, profil d'usage, etc.). En d'autre termes, les variables internes du systèmes sont obtenues grâce

à la résolution des équations différentielles en effectuant des simulations dynamiques du modèle Simulink associé (voir l'exemple de la figure 3.18).

L'étape de la modélisation fonctionnelle et dysfonctionnelle de l'analyse qualitative précédemment effectuée, nous a permis de construire le réseau de Petri (voir l'exemple de la figure 3.22).

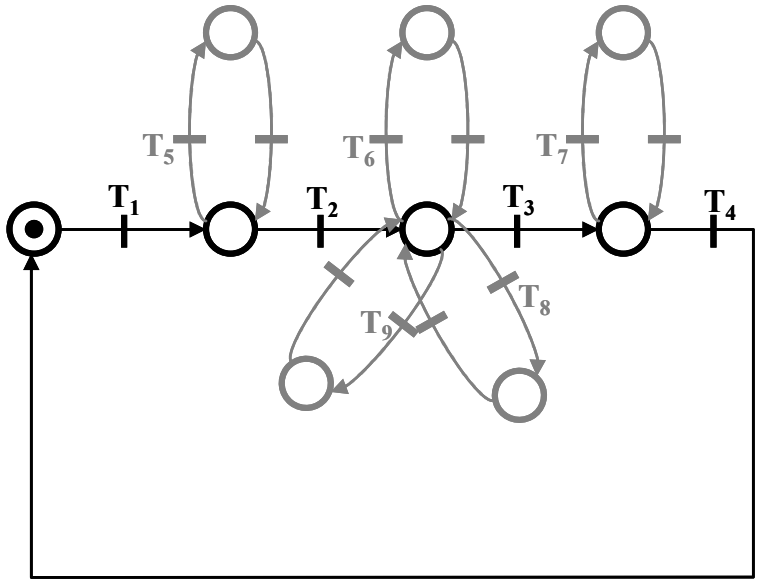

FIGURE 3.22 – Transitions associées au réseau de Petri fonctionnel et dysfonctionnel

Sur les réseau de Petri de la figure 3.22 nous remarquons deux types de transitions : les transitions fonctionnelles qui sont T_1, T_2, T_3 et T_4 seront pour la plupart décrites par des équations différentielles (équation 3.6) :

$$T_F = \frac{dx}{dt} \tag{3.6}$$

Et les transitions dysfonctionnelles qui sont T_5, T_6, T_7, T_8 et T_9 sont définies comme suit (équation 3.7) :

$$T_D = F^{-1}(VA, \theta) \tag{3.7}$$

VA représente une valeur aléatoire et θ les paramètres des lois de fiabilité.

Cette étape de la simulation dynamique fonctionnelle nous permet de déterminer, d'une part, les variables physiques internes et, d'autre part, les temps de fonctionnement des différents composants du système.

Ces temps de fonctionnement sont obtenus grâce à la résolution des équations différentielles partielles et sont associés aux transitions fonctionnelles T_1, T_2, T_3 et T_4 du réseau

de Petri de la figure 3.22.

Les variables physiques internes, que nous obtenons aussi à l'aide de Simulink, seront utilisées comme données pour effectuer l'étape présentée ci-dessous.

3.3.3.3 Détermination des lois de fiabilité

En ce qui concerne les transitions dysfonctionnelles T_{Di}, il est nécessaire d'associer des lois de probabilité à ces différentes transitions. Dans le cas de composants électroniques et logiciels nous utilisons des lois de probabilité qui caractérisent leurs défaillances. Pour les composants électroniques, la loi exponentielle (équation 2.15) est tout à fait adaptée pour représenter les défaillances de ces composants, quant aux composants logiciels le modèle de Musa (équation 2.33), présenté dans la chapitre 2, est choisi.

Dans le cas des composants mécaniques standards, on peut utiliser les recueils de données (NPRD95, AVCO, etc.), mais dès lors que l'on utilise un composant spécifique, il est nécessaire de déterminer la loi de fiabilité et ses paramètres. Pour ce faire, nous proposons d'utiliser la méthode PHI2 (définie dans le chapitre 2) proposée par [59, 2, 3, 5, 92, 91, 90, 89] pour estimer la probabilité de défaillance $P_f(t)$ du composant mécanique. Cette loi de fiabilité est nécessaire pour le déroulement de l'étape suivante.

Pour construire ces lois de fiabilité nous avons besoin de connaître certaines variables physique internes qui sont obtenues lors de l'étape de la simulation dynamique fonctionnelle et par résolution des équations différentielles partielles.

Les systèmes et les composants mécaniques assurent des fonctions en vue d'actions plus ou moins compliquées. Ces actions sont effectuées et pilotées par un ou plusieurs utilisateurs dans des conditions variées (profil de mission). La diversité des utilisateurs conduit ainsi à un grand nombre de situations de chargement. Le défi des concepteurs des systèmes et composants mécaniques est alors d'intégrer ces conditions réelles d'usage [54].

Pour se rapprocher de ces conditions réelles d'usage, nous construisons un modèle physique du système à étudier et résolvons les EDP associées pour obtenir les variables internes de ce système (figure 3.18). Ces variables internes (efforts internes) sont sous forme de processus aléatoire (voir annexe F), c'est pourquoi il est nécessaire d'effectuer une analyse statistique de ces variables internes caractéristiques des composants mécaniques.

Cette analyse statistique consiste à obtenir les informations nécessaires pour disposer d'un histogramme ou d'une loi de distribution, à partir du processus aléatoire de la variable interne au cours du temps. Cette loi de distribution n'est, en réalité, qu'une représentation approchée de ce processus (figure 3.23).

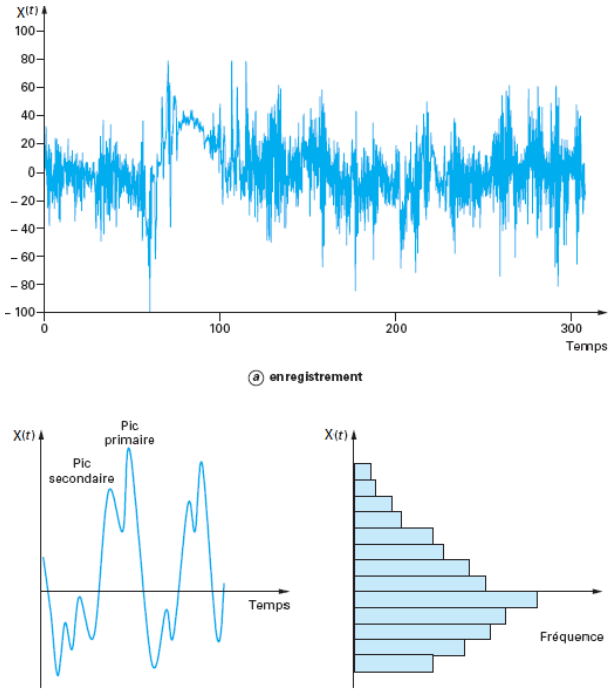

FIGURE 3.23 – Visualisation d'une sollicitation X(t) en conditions réelles d'usage [54]

La sollicitation *X(t)* est une variable interne du système qui est obtenue grâce aux simulations du modèle physique précédemment construit à l'aide des équations différentielles.

Hormis quelques cas particuliers de processus (trajectoire périodique sinusoïdale, processus stationnaire Gaussien à bande étroite), il est, en général, difficile d'associer une étendue de variation de contraintes à un cycle (figure 3.23).

Il existe des méthodes de comptage permettant d'extraire les informations nécessaires à partir d'une trajectoire donnée, comme montré sur la figure 3.24.

On peut citer trois grandes familles de comptage qui sont : les méthodes globales de comptage, les méthodes locales de comptage et enfin les méthodes matricielles de comptage.

Dans la famille des méthodes globales de comptage on trouve :

- Histogramme ou temps de maintien dans une classe d'amplitudes ;
- Comptage du nombre de dépassements d'un niveau donné.

La famille des méthodes matricielles de comptage regroupe :

- Comptage des étendues entre pics et creux ;
- Comptage des cycles moyens ;
- Méthode de la *goutte d'eau* ;
- Méthode du réservoir ;

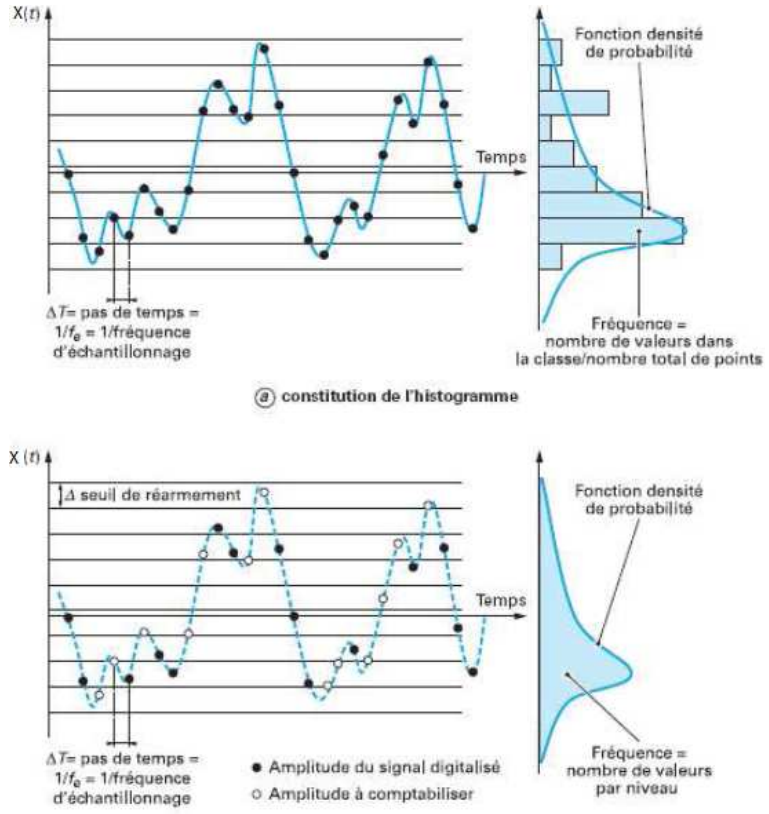

FIGURE 3.24 – Statistique descriptive d'une sollicitation [54]

– Méthode de la matrice de transition ou matrice de Markov.

Lorsque l'analyse statistique des variables internes des composants mécaniques du système est effectuée, il est possible, à présent, de déterminer les lois de fiabilité correspondant à ces composants mécaniques. La construction de ces lois de fiabilité se déroule comme illustré sur la figure 3.25.

Dans un premier temps, les variables internes $x_i(t)$ sont obtenues par la résolution des EDP représentant le système. Ces variables sont étudiées à l'aide d'une des méthodes de comptage citées précédemment dans le but de déterminer les distributions qui leur sont associées ($f(x_i)$).

Dans un deuxième temps, la construction de la surface de réponse est nécessaire, dans le cas général, pour construire la surface d'état limite $G(x)$ afin de pouvoir estimer la probabilité de défaillance des composants mécaniques. Cependant, nous pouvons utiliser une expression analytique pour $G(x)$.

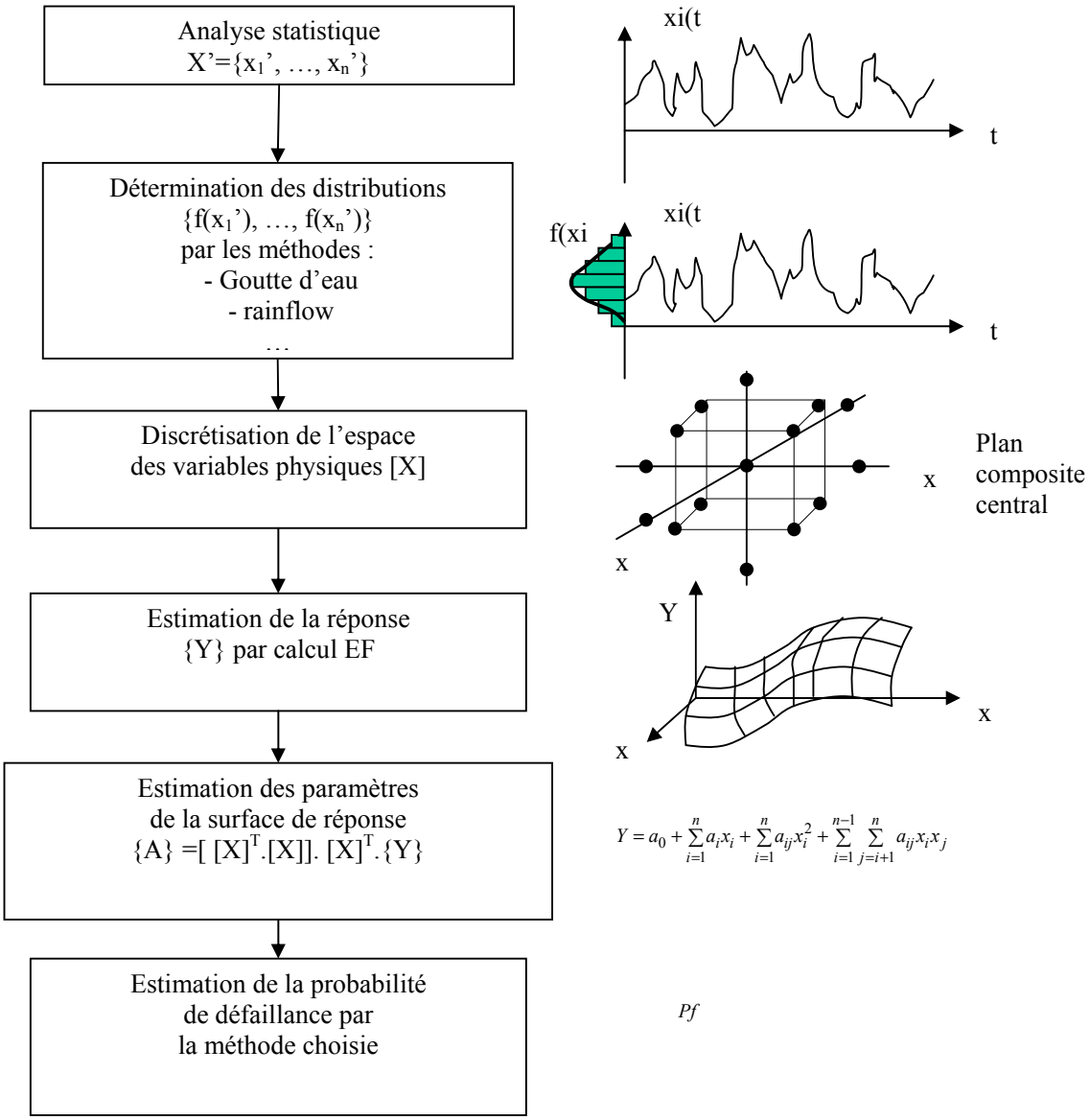

FIGURE 3.25 – Etapes de détermination des lois de fiabilité des composants mécaniques

Cette probabilité de défaillance est, ainsi, estimée pour un composant mécanique spécifique en utilisant la méthode PHI2 s'écrit comme suit (équation 3.8) :

$$P_{f,c}(t_1, t_2) \leq P_{f,i}(t_1) + \int_{t_1}^{t_2} \nu(t)\, dt \tag{3.8}$$

sachant que le taux de franchissement ν(t) s'écrit comme sur le montre l'équation 3.9 :

$$\nu^{+}_{PHI2}(t) = \frac{\|\alpha(t+\Delta t) - \alpha(t)\|}{\Delta t} \phi(\beta(t))\, \Psi\left(\frac{\beta(t+\Delta t) - \beta(t)}{\|\alpha(t+\Delta t) - \alpha(t)\|}\right) \tag{3.9}$$

La loi de fiabilité obtenue est nécessaire pour le déroulement de l'étape suivante.

3.3.4 Simulation

Dans la phase consacrée à la simulation du modèle fonctionnel et dysfonctionnel obtenu, deux étapes sont importantes. La première consiste à déterminer les états atteints par les réseaux de Petri et ainsi calculer les temps de défaillance des différents composants. La seconde étape consiste à analyser les résultats obtenus et ainsi estimer la fiabilité système, composants et fonctions.

3.3.4.1 Détermination des états atteints par les réseaux de Petri

La modélisation fonctionnelle et dysfonctionnelle d'un système mécatronique sera traitée grâce aux réseaux de Petri qui sont une méthode bien adaptée pour la modélisation de systèmes complexes. Ces réseaux sont utilisés pour décrire les processus de commande séquentielle dynamique d'un système. Ils permettent de décrire le comportement des systèmes dans les conditions de fonctionnement normal ainsi que dans le cas de défaillance de leurs composants. L'évolution d'un système dynamique décrit par un réseau de Petri est représentée par l'évolution des marquages (nombre de jetons dans les places), comme nous l'avons déjà présenté dans le chapitre 2.

Cette modélisation dynamique permet de quantifier la fiabilité en assignant des valeurs numériques aux paramètres du modèle. Ces valeurs attribuées aux paramètres du réseau sont obtenues grâce aux étapes décrites dans les paragraphes précédents (figure 3.26).

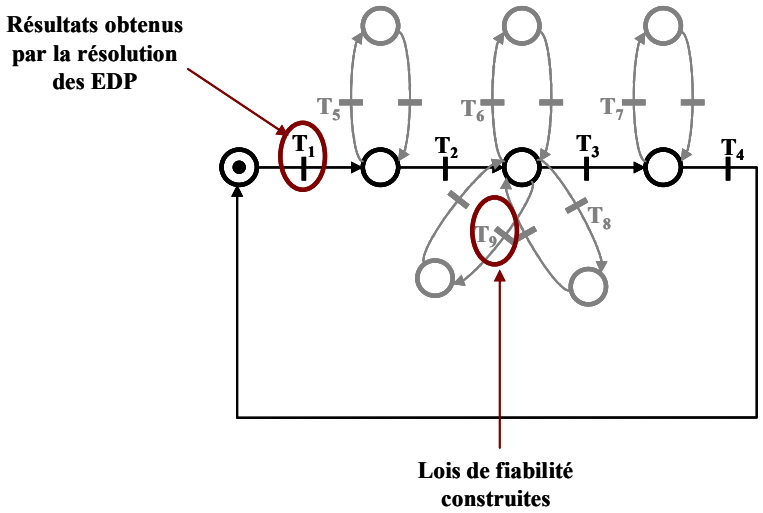

FIGURE 3.26 – Association des résultats obtenus au réseau de Petri

Sur cet exemple, Les transitions T_1, T_2, T_3 et T_4 représentent des transitions fonc-

tionnelles (T_F), et les transitions T_5, T_6, T_7, T_8 et T_9 des transitions dysfonctionnelles (T_D).

Il est impératif, une fois le réseau de Petri construit, de déterminer les états atteints par ce réseau : états fonctionnels (F), états fonctionnels avec présence de fautes (S) ou états défaillants (D) (figure 3.5).

Ces états atteints sont obtenus grâce aux simulations du réseau de Petri de la figure 3.26. L'évolution du réseau de Petri est obtenu par des franchissements (tirs) des transitions. Si un jeton se trouve dans la place P_i, le passage de ce jeton de la place P_i à la place P_{i+1} illustre le passage du système d'un état à un autre.

Pour effectuer ces simulations, nous avons besoin d'informations qui seront associées aux transitions du réseau. Ces informations sont obtenues, comme le montre la figure 3.27, par la résolution des équations différentielles après avoir déterminé les variables externes (profil de mission).

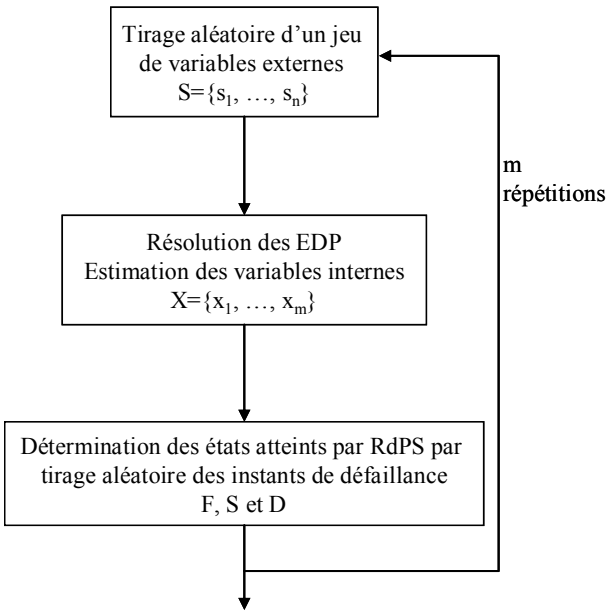

FIGURE 3.27 – Etapes de la détermination des états atteints par le réseau de Petri stochastique

La résolution des équations différentielles nous permet d'avoir les temps de fonctionnement des différents composants du système. Ces temps de fonctionnement sont attribués aux transitions fonctionnelles T_{Fi} du réseau (figure 3.26), quant aux transitions dysfonctionnelles T_{Di} du même réseau, différentes lois de probabilité sont associées à ces transitions selon le type du composant : le modèle de Musa pour la défaillance du composant logiciel, la loi exponentielle pour la défaillance du composant électronique. Enfin dans le cas de la défaillance du composant mécanique, une loi de fiabilité est déterminée dans

l'étape précédente.

La simulation du réseau de Petri (figure 3.26) est à présent possible et les états atteints par ce réseau sont déterminés. Ces états sont : F qui représente le fonctionnement normal du système, S son fonctionnement dégradé (en présence de fautes) et D la défaillance du système. Les états S et D sont atteint lorsque :

$$\sum T_{F_i} \geq T_{D_i} \tag{3.10}$$

3.3.4.2 Analyse statistique des résultats de simulation

Cette dernière étape de la partie analyse quantitative consiste à faire une analyse statistique des résultats des simulations de l'étape précédente. L'analyse statistique se fait en trois parties comme montré sur la figure 3.28.

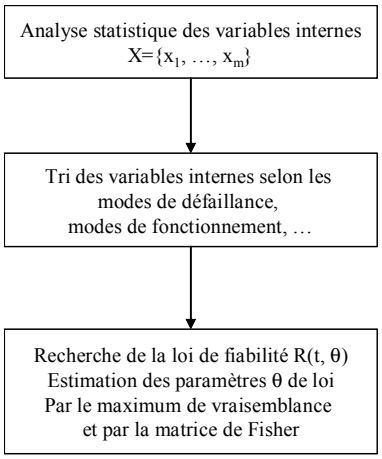

FIGURE 3.28 – Analyse statistique des résultats de simulation

La première partie est l'analyse statistique des variables internes x_i du système. Nous rappelons que ces variables internes sont obtenues après résolution des équations différentielles partielles à l'aide de Simulink.

La deuxième partie consiste à trier les variables internes selon le mode de défaillance, la fonction, le composant, etc. La figure 3.29 illustre cette deuxième partie :

La dernière partie de cette analyse statistique des résultats de simulation consiste à rechercher la loi de fiabilité pour les différents modes de défaillance.

A l'aide de la méthode du maximum de vraisemblance, nous déduisons les paramètres de distributions de la fiabilité.

La méthode du maximum de vraisemblance consiste, dans un premier temps, à évaluer la vraisemblance $L(t, \theta)$ des observations, c'est-à-dire la probabilité d'avoir obtenu

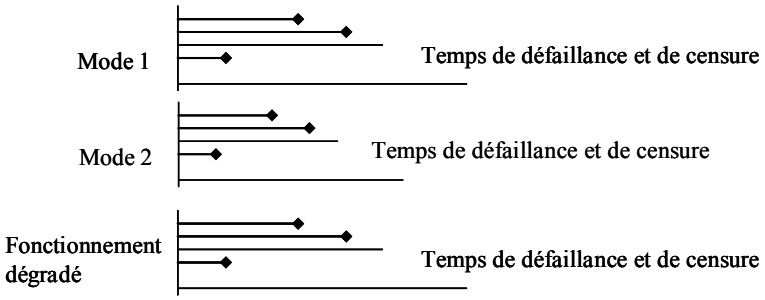

FIGURE 3.29 – Tri des variables internes selon le mode de défaillance

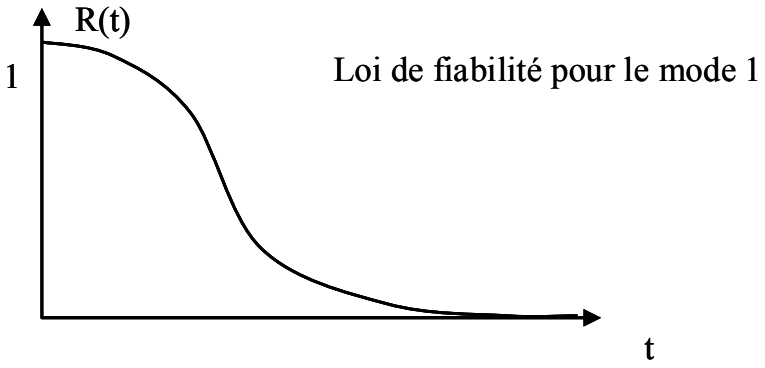

FIGURE 3.30 – Loi de fiabilité pour un mode donné

un certain nombre de défaillances et de censures à des instants ou à des intervalles de temps donnés pour un échantillon x.

La vraisemblance $L(t, \theta)$ s'écrit de la manière suivante :

$$L(t,\theta) = \left(\prod_{i=1}^{k} f(t_i,\theta)\right) \cdot \left(\prod_{i=k+1}^{n} R(t_i,\theta)\right) \tag{3.11}$$

La probabilité d'avoir observé une défaillance à un instant compris entre t et $(t+dt)$ est égale à $f(t)dt$ où $f(t)$ est la fonction densité de défaillance. Alors que la probabilité d'avoir observé une censure à droite à l'instant t est égale à la probabilité pour un système d'avoir bien fonctionné jusqu'à t ce qui est égale à $R(t)$, où $R(t)$ est la fonction fiabilité.

Ainsi la probabilité d'avoir observé k défaillances aux instants $(t_1, t_2,..., t_i,...,t_k)$ et $(n\text{-}k)$ censures à droite aux instants $(t_{k+1}, t_{k+2},..., t_j,...,t_n)$ est proportionnelle au produit des probabilités élémentaires comme illustré sur l'équation 3.11

Si $L(t, \theta)$ est dérivable et si le maximum de vraisemblance $\hat{\theta} = (\hat{\theta}_1,...,\hat{\theta}_r)$ existe, alors il satisfait l'équation suivante :

$$\left.\frac{\partial L(t,\theta)}{\partial \theta}\right|_{\theta=\hat{\theta}} = 0 \tag{3.12}$$

ou

$$\left.\frac{\partial ln\left(L\left(t,\theta\right)\right)}{\partial\theta}\right|_{\theta=\hat{\theta}}=0 \tag{3.13}$$

L'information de Fisher est définie comme la matrice des dérivées d'ordre deux de la fonction de vraisemblance (équation 3.14) :

$$\hat{I}=\begin{bmatrix} -\frac{\partial^2 L}{\partial\theta_1^2} & -\frac{\partial^2 L}{\partial\theta_1\partial\theta_2} & \cdots & -\frac{\partial^2 L}{\partial\theta_1\partial\theta_r} \\ -\frac{\partial^2 L}{\partial\theta_2\partial\theta_1} & -\frac{\partial^2 L}{\partial\theta_2^2} & \cdots & -\frac{\partial^2 L}{\partial\theta_2\partial\theta_r} \\ \cdots & \cdots & \cdots & \cdots \\ -\frac{\partial^2 L}{\partial\theta_r\partial\theta_1} & -\frac{\partial^2 L}{\partial\theta_r\partial\theta_2} & \cdots & -\frac{\partial^2 L}{\partial\theta_r^2} \end{bmatrix} \tag{3.14}$$

La matrice inverse $\hat{I}^{-1}$ de Fisher représente la matrice estimée de variance-covariance notée $\hat{\Sigma}$ (équation 3.15) :

$$\hat{\Sigma}=\begin{bmatrix} \hat{Var}\left(\hat{\theta}_1\right) & \hat{Cov}\left(\hat{\theta}_1,\hat{\theta}_2\right) & \cdots & \hat{Cov}\left(\hat{\theta}_1,\hat{\theta}_r\right) \\ \hat{Cov}\left(\hat{\theta}_2,\hat{\theta}_1\right) & \hat{Var}\left(\hat{\theta}_2\right) & \cdots & \hat{Cov}\left(\hat{\theta}_2,\hat{\theta}_r\right) \\ \cdots & \cdots & \cdots & \cdots \\ \hat{Cov}\left(\hat{\theta}_r,\hat{\theta}_1\right) & \hat{Cov}\left(\hat{\theta}_r,\hat{\theta}_2\right) & \cdots & \hat{Var}\left(\hat{\theta}_r\right) \end{bmatrix} \tag{3.15}$$

Cette matrice sera utilisée pour estimer l'intervalle de confiance.

Intervalles de confiance : Bien souvent, le fiabiliste ne se satisfait pas d'associer uniquement une loi de probabilité aux données mesurées, il cherche également à établir l'ensemble des lois susceptibles de correspondre aux valeurs obtenues. Dans ce but, il détermine un intervalle de confiance associé aux paramètres estimés afin d'enrichir son estimation.

Pour un certain niveau de confiance α on a les limites inférieure et supérieure qui sont présentées sur l'équation 3.16 :

$$\hat{\theta}-u_{1-\frac{\alpha}{2}}\sqrt{Var\left(\hat{\theta}\right)}<\theta<\hat{\theta}+u_{1-\frac{\alpha}{2}}\sqrt{Var\left(\hat{\theta}\right)} \tag{3.16}$$

Les limites de confiance pour le cas où θ doit être positif s'écrivent (équation 3.17) :

$$\hat{\theta}e^{-\frac{u_{1-\frac{\alpha}{2}}\sqrt{Var(\hat{\theta})}}{\hat{\theta}}}<\theta<\hat{\theta}e^{\frac{u_{1-\frac{\alpha}{2}}\sqrt{Var(\hat{\theta})}}{\hat{\theta}}} \tag{3.17}$$

Une étude de sensibilité est importante dans le but de concevoir des systèmes stables. Cette étude permet de mettre en évidence l'influence de chaque composant sur la fiabilité globale du système ainsi que le composant le plus fiable ou le moins fiable. Grâce à cette

analyse de sensibilité, nous pouvons faire face aux faiblesses du système en modifiant son architecture et construire ainsi une architecture tolérante aux fautes.

A présent que la méthodologie est présentée, nous vous présentons son application à un système ABS.

3.4 Application

Afin d'illustrer la méthodologie présentée, nous avons choisi un exemple simple qui sera traité en détail.

3.4.1 Système 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 en Europe de l'ouest sont équipés de l'ABS qui n'est donc plus une option. Il est destiné à éviter qu'une roue ne se bloque au freinage par la suite d'un appui trop important sur la pédale de frein, ou, le plus souvent, par suite d'une adhérence trop faible de la chaussée. 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 [95, 71].

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.

Le blocage d'une roue est détecté par un capteur de rotation. Le calculateur compare les données avec les courbes de freinage dont il dispose en mémoire et détecte ainsi les

anomalies de freinage.

Physiquement, le maître-cylindre de frein est remplacé par des électrovannes qui libèrent la pression pour freiner la roue dont le système a détecté le blocage. L'huile évacuée lors du relâchement de la pression est remise dans le circuit par une pompe commune à l'ensemble du système.

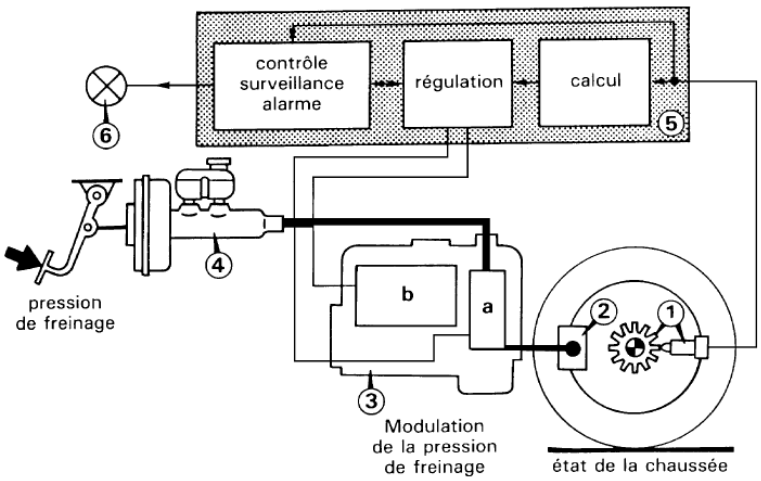

FIGURE 3.31 – Système ABS

La figure 3.31 représente le système ABS. Il est composé de :

1. un capteur de vitesse et sa cible ;
2. un étrier et un disque de frein ;
3. un groupe hydraulique ;
4. un maître cylindre ;
5. un calculateur ;
6. un voyant témoin.

3.4.2 Investigation systémique

Comme nous l'avons déjà cité dans le chapitre 2, l'analyse qualitative a pour objectif d'identifier toutes les causes de défaillance pouvant affecter le bon fonctionnement d'un système. Cette analyse qualitative est commencée par une analyse fonctionnelle.

3.4.2.1 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 : Les fonctions de base du système ABS sont déduites après une étude des milieux extérieurs [28, 27, 31, 29, 30].

La figure 3.32 représente la matérialisation du besoin pour le système ABS. On constate, sur cette figure, que le système ABS rend service au conducteur (réponse à la première question à qui ?), il agit sur la roue et plus généralement sur le véhicule (réponse à la deuxième question sur quoi ?) et il permet de freiner les roues du véhicule sans les bloquer (réponse à la dernière question pourquoi ?).

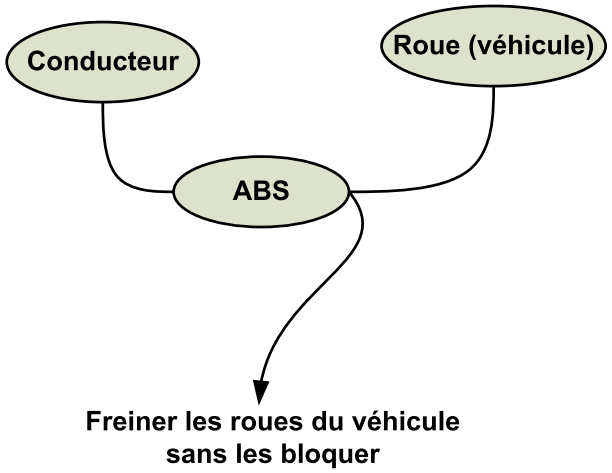

FIGURE 3.32 – Formalisation du besoin du système ABS

Après la formalisation du besoin, il est important d'établir les relations entre le système et les éléments de son milieu extérieur.

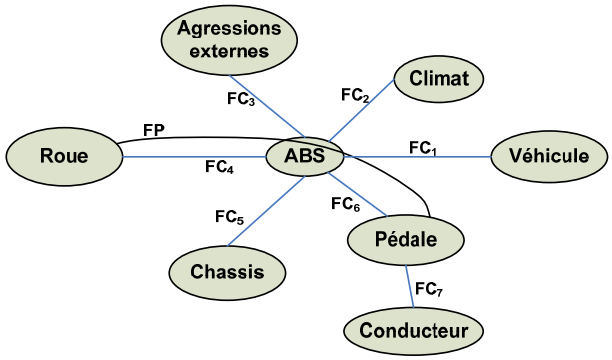

FIGURE 3.33 – Schéma de la pieuvre pour le système ABS

Pour cela on utilise le schéma de la *Pieuvre* comme montré sur la figure 3.33 qui nous permet de mettre en évidence la fonction principale de l'ABS qui consiste en le freinage des roues sans blocage ainsi que les fonctions de contrainte que subit ce système.

Ces fonctions sont résumées dans le tableau 3.2 :

Fonctions	**Désignations**
FP	Permet au conducteur de freiner le véhicule en évitant le blocage des roues
FC$_1$	Les caractéristiques du véhicule agissent sur le système
FC$_2$	Les conditions climatiques et la qualité du revêtement de la route agissent sur le freinage
FC$_3$	Situations nécessitant un freinage d'urgence
FC$_4$	Le système ABS doit être relié à la roue
FC$_5$	Le système doit avoir un support (châssis)
FC$_6$	La pédale sous action du conducteur déclenche le freinage
FC$_7$	Le conducteur doit appuyer sur la pédale de frein

TABLE 3.2 – Fonctions principales et de contraintes du système ABS

Dans le tableau 3.2, FP représente la fonction principale qui met en relation le conducteur avec le système ABS et la roue, les fonctions FC représentent les fonctions de contraintes qui sont soit imposées par le milieu extérieur ou soit une exigence de l'utilisateur.

L'Analyse Fonctionnelle Externe effectuée ci-dessus et qui consiste en la formalisation du besoin et le schéma de la Pieuvre, illustre les relations entre le système ABS et son milieu extérieur. Cependant, les fonctions internes de ce système ne sont pas connues. Voilà pourquoi nous effectuons une Analyse Fonctionnelle Interne.

Analyse Fonctionnelle Interne : Cette analyse permet de décrire les modes de fonctionnement du système et de connaître ses fonctions internes que nous n'avons pas pu obtenir après l'Analyse Fonctionnelle Externe.

Pour effectuer l'Analyse Fonctionnelle Interne du système ABS, nous avons choisi d'utiliser la méthode SADT définie dans le chapitre 2. Cette méthode a été choisie car elle s'applique aussi bien à la mécanique et à l'électronique qu'au logiciel. Elle nous permet de faire une décomposition hiérarchique du système ABS en éléments. Le premier diagramme représenté sur la figure 3.34 est le niveau A-0 de la méthode SADT.

Ce premier diagramme met en évidence la fonction principale du système ABS et qui consiste à freiner les roues du véhicule sans les bloquer. Cette fonction principale a été déduite à partir de la modélisation du besoin (figure 3.32). Ce premier diagramme montre également les relations de ce système ABS avec son milieu extérieur.

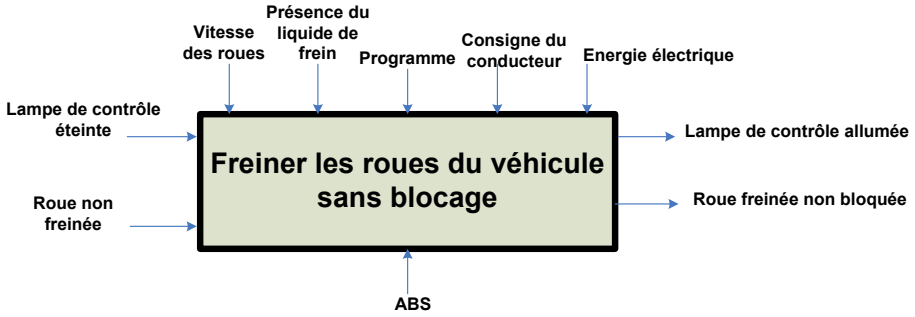

FIGURE 3.34 – Niveau A-0

Le deuxième diagramme qui est le niveau A_0 illustré sur la figure 3.35 est une décomposition du niveau A-0 précédent et il contient cinq boîtes :

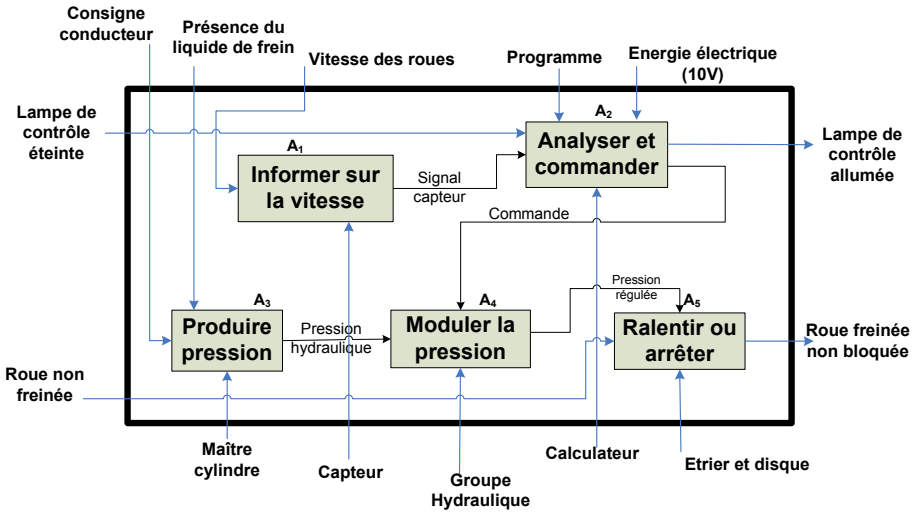

FIGURE 3.35 – Niveau A_0

- La boîte A_1 consiste à informer sur la vitesse de la roue grâce au capteur de vitesse et à envoyer cette information au calculateur dans le but de calculer le glissement en fonction de cette vitesse de roue ;
- La boîte A_2 consiste à analyser, grâce au calculateur, le bon déroulement des différentes opérations du freinage et à commander le groupe ;
- La boîte A_3 représente la production de la pression hydraulique dans le maître cylindre avant d'être envoyé dans le groupe hydraulique ;
- La boîte A_4 consiste à moduler la pression qui s'exerce dans l'étrier et cela grâce au groupe hydraulique ;
- Enfin la dernière boîte A_5 représente le freinage de la roue grâce à l'étrier et au disque de frein.

Le diagramme présenté sur la figure 3.36 est le niveau A_1 et est une décomposition de

la boîte *informer sur la vitesse*. Ce diagramme contient 2 boîtes :

- la boîte A_{11} consiste à détecter la vitesse de la cible et transmettre une forme géométrique
- la boîte A_{12} permet de transformer la forme géométrique reçue en un signal électrique

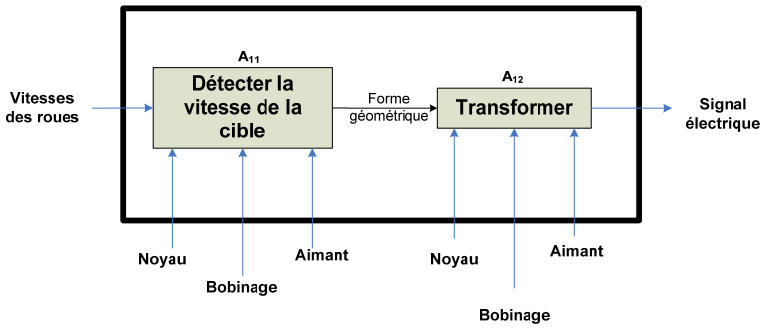

FIGURE 3.36 – Niveau A_1

Vient ensuite le niveau A_2 qui est une décomposition de la boîte A_2 du niveau A_0. Ce niveau décompose la boîte A_2 *Analyser et commander* et contient quatre boîtes :

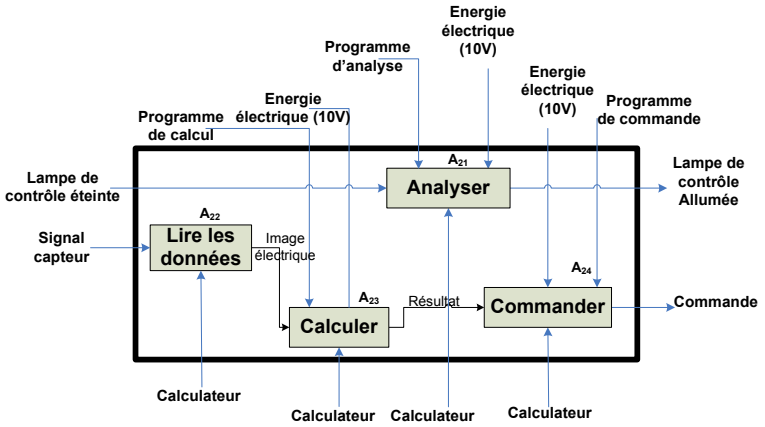

FIGURE 3.37 – Niveau A_2

- La boîte A_{21} consiste à analyser le bon déroulement des différentes opérations du freinage et d'allumer la lampe de contrôle en cas de détection de problème ;
- La boîte A_{22} reçoit les informations du capteur et les transmet à la partie calcul ;
- La boîte A_{23} permet de calculer le glissement à partir de la vitesse de la roue et de celle du véhicule ;
- La boîte A_{24} consiste à commander le groupe hydraulique à partir des résultats obtenus.

Le dernier niveau de décomposition pour notre étude de cas est le niveau A_4 qui est une décomposition de la boîte A_4 *Moduler*. Le groupe hydraulique permet de transmettre,

réduire ainsi que de maintenir la pression de freinage.

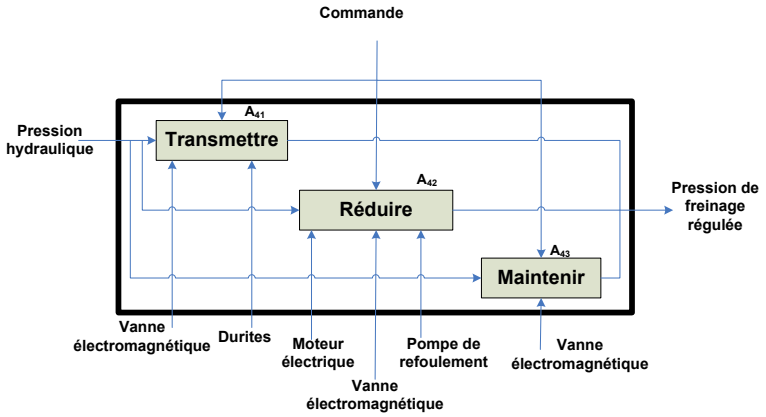

FIGURE 3.38 – Niveau A_4

Ce niveau A_4 comporte trois boîtes :

- La boîte A_{41} consiste à transmettre, sous ordre du calculateur, le fluide sans modifier la pression de freinage.
- La boîte A_{42} permet de réduire la pression du liquide de frein dans le but d'éviter le blocage des roues.
- La boîte A_{43} consiste à maintenir la pression qui s'exerce dans l'étrier.

L'aspect dynamique du système ABS est traité grâce à une extension de SADT qui est la méthode SA-RT. Elle nous permet d'approfondir notre connaissance du système à étudier.

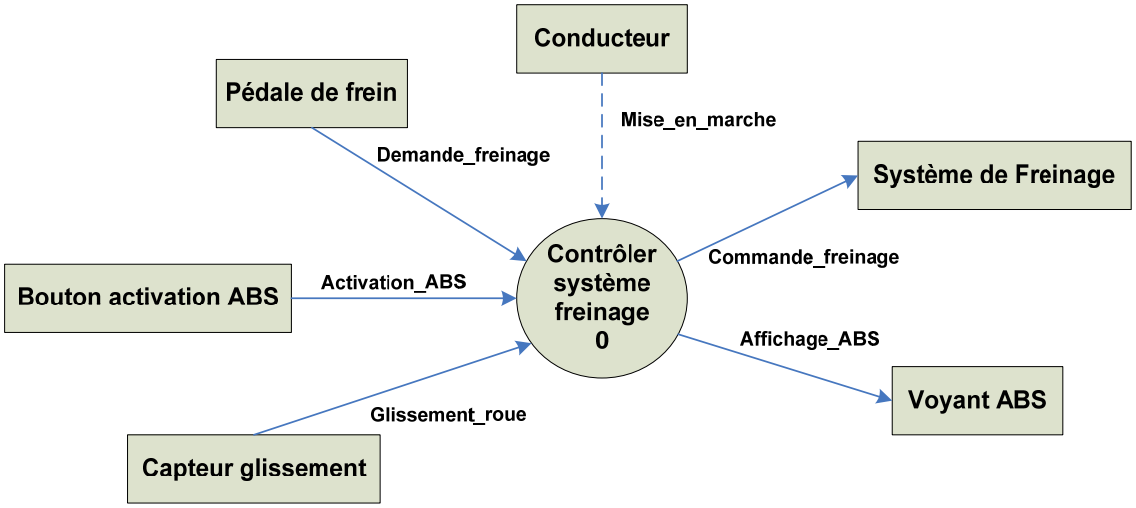

FIGURE 3.39 – Diagramme de contexte pour le système ABS

Le diagramme de contexte est une première étape extrêmement importante puisqu'elle va définir le contexte et l'environnement extérieur du système piloté.

La figure 3.39 représente le diagramme de contexte du système ABS. On constate sur cette figure que ce diagramme est constitué du processus fonctionnel *Contrôler système freinage 0* et de cinq bords de modèles (terminaisons) qui sont :

- *Pédale de frein* fournissant la donnée *Demande-freinage* ;
- *Bouton de l'activation de l'ABS* fournissant la donnée *Activation-ABS* ;
- *Capteur de glissement* fournissant la donnée *Glissement-roue* ;
- *Système de freinage* consommant la donnée *Commande-freinage* ;
- *Voyant ABS* consommant la donnée *Affichage-ABS*.

Ce diagramme de contexte définit parfaitement l'interface entre le concepteur et le client, c'est-à-dire les données à fournir ou à générer. La suite du travail d'analyse se situera dans l'expression du processus fonctionnel à réaliser : *Contrôler système freinage 0*.

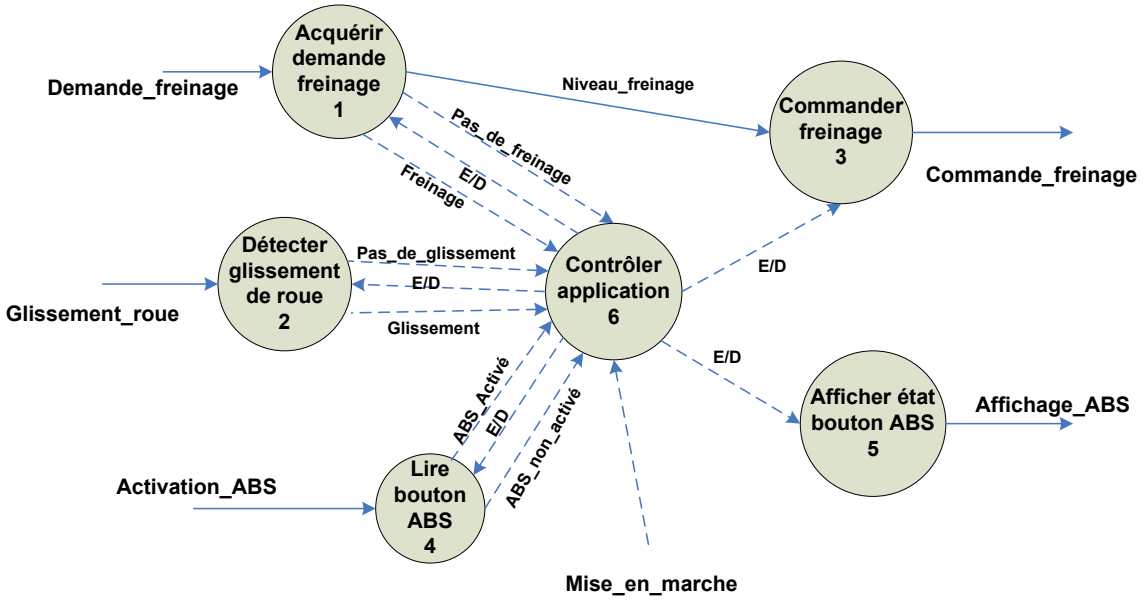

FIGURE 3.40 – Diagramme préliminaire pour le système ABS

Ce diagramme préliminaire (figure 3.40) est la première décomposition du processus à réaliser présenté dans le diagramme de contexte de la figure 3.39. A ce niveau, le diagramme représente la liste des processus fonctionnels nécessaires à l'application.

Cette analyse fait apparaître cinq processus fonctionnels de base (1,2,3,4,5) et un processus de contrôle (6) permettant de séquencer l'ensemble. Les événements E/D représentés sur ce diagramme sont utilisés pour piloter les processus fonctionnels de type *boucle sans fin*

La dernière étape de la méthode SA-RT consiste à construire un diagramme état/transition qui explique le fonctionnement du processus de contrôle.

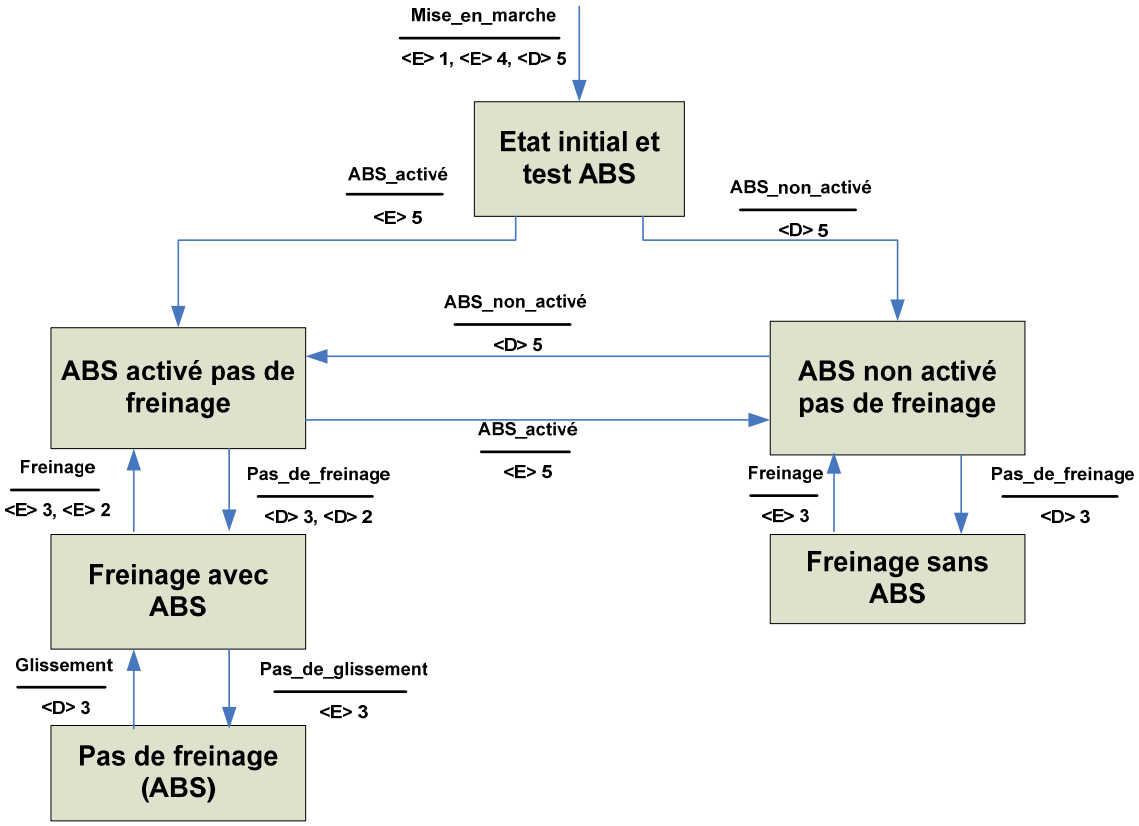

FIGURE 3.41 – Diagramme état/transition pour le système ABS

Ce diagramme état/transition représenté sur la figure 3.41, montre clairement les deux fonctionnements du système en cas de freinage avec le système ABS activé ou sans le système ABS. Cette information nous sera très utile dans la construction du réseau de Petri où on retrouvera ces deux modes de freinage.

L'analyse fonctionnelle que nous avons effectuée nous permet de prendre connaissance du fonctionnement du système ABS et ainsi nous pouvons construire le modèle fonctionnel du système ABS. Dans le cas de la modélisation dysfonctionnelle nous devons passer, tout d'abord, par l'analyse dysfonctionnelle pour identifier les différents modes de défaillance de ce système.

3.4.2.2 Analyse dysfonctionnelle

L'analyse fonctionnelle précédemment effectuée n'apporte aucune information sur les défaillances potentielles que peut rencontrer le système ABS que nous avons choisi d'étudier. 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.

La figure 3.42 représente le tableau AMDE et AEEL pour le système ABS regroupé

Fonction principale	**Composant**	**Fonction du composant**	**Mode de défaillance**	**Causes**	**Effets**
Eviter le blocage des roues, améliorer la stabilité du véhicule et raccourcir la distance de freinage	Disque	Lier la roue au système de freinage	Ne ralenti pas la roue	Absence de disque	Pas de freinage
				Disque très usé	
				Disque usé	Mauvais freinage
				Disque voilé	
				Disque fissuré	
				Présence de matière grasse sur le disque	
	Etrier	Exercer une pression sur le disque pour le ralentir	Ne ralenti pas la roue	Circuit hydraulique défaillant	Pas de freinage
				Absence de plaquettes	
			Freinage non performant	Mauvaise pression hydraulique	Mauvais freinage
				Plaquettes usées ou fissurées	
	Maître cylindre	Transformer une action mécanique en pression hydraulique	Absence de la pression	Piston cassé	Pas de freinage
				Circuit colmaté	
				Niveau d'huile bas	
			Mauvaise pression	Fuite dans le circuit	Mauvais freinage
				Absence d'huile dans le circuit	
				Circuit colmaté	
	Groupe hydraulique	Moduler la pression de freinage dans le système	Pas de pression	Vannes défaillantes	Pas de freinage
				Pompe de refoulement défaillante	
				Moteur électrique de pompe défaillant	
				Durites débranchées	
				Durites bouchées	
				Connecteurs électriques défaillant	
			Surpression	Vannes défaillantes	Risque de blocage des roues et de dérapage du véhicule
				Pompe de refoulement défaillante	
				Moteur électrique de pompe défaillant	
				Relais défaillant	
				Connecteurs électriques défaillant	
			Perte de pression	Vannes défaillantes	Mauvais freinage
				Pompe de refoulement défaillante	
				Moteur électrique de pompe défaillant	
				Durites débranchées	
				Durites bouchées	
				Connecteurs électriques défaillant	
	Capteur de vitesse	Transmet une information relative à la vitesse de la roue	Non détection de la vitesse de la roue	Aimant cassé	Pas d'assistance ABS : Risque de blocage des roues
				Aimant oxydé	
				Rupture bobinage	
				Court-circuit dans le bobinage	
				Noyau cassé	
	Calculateur	Analyse les informations reçues afin de piloter le groupe hydraulique et le voyant de contrôle	Non transmission d'informations au groupe hydraulique	Court-circuit	Pas d'assistance ABS : risque de blocage des roues
				Coupure	
				Tension inférieur à 10 V	
				Erreur dans le programme de calcul	
				Erreur dans le programme de commande	
				Pas de lecture du signal capteur	
			Non transmission d'informations au voyant	Erreur dans le programme d'analyse	Pas d'informations sur le fonctionnement de l'ABS
			Transmission d'informations erronées au groupe hydraulique	Défauts internes	Mauvaise commande du groupe hydraulique
				Erreur dans le programme de calcul	
				Erreur dans le programme de commande	
				Erreur dans la lecture du signal capteur	
			Transmission d'informations erronées au voyant	Erreur dans le programme d'analyse	Informations erronées pour l'utilisateur
	Voyant de contrôle	Informer le conducteur	Fonctionnement intempestif	Problème de bruit	Informations erronées pour l'utilisateur
				Faut contact	
			Fonctionnement intermittent	Court-circuit	Informations erronées pour l'utilisateur
				Coupure	
			Pas de fonctionnement	Coupure	Utilisateur non informé du fonctionnement de l'ABS
				Tension trop faible	
				Mauvais contact	

FIGURE 3.42 – AMDE/AEEL du système ABS

dans un même tableau. Il nous permet d'identifier toutes les défaillances que peut subir le système ABS.

Dans un premier temps, nous avons décomposé le système ABS en éléments qui sont : disque, étrier, maître cylindre, groupe hydraulique, capteur de vitesse, calculateur et enfin le voyant de contrôle. Dans un deuxième temps nous avons imaginé toutes les défaillances possibles pour chaque élément.

L'analyse qualitative que nous venons d'effectuer illustre le fonctionnement et le dysfonctionnement du système ABS et nous pouvons ainsi construire le modèle fonctionnel et dysfonctionnel. Cependant, cette analyse ne fournie pas d'information sur les probabilités de défaillance. C'est pourquoi il est indispensable de faire une analyse quantitative pour estimer la probabilité de défaillance du système.

3.4.3 Modélisation qualitative

La étape consiste à modéliser, grâce au réseau de Petri décrit en chapitre 2, le fonctionnement du système ABS. L'analyse fonctionnelle effectuée précédemment nous permet de faire une modélisation fonctionnelle du système ABS. Cette modélisation est illustrée sur la figure 3.43.

On retrouve sur cette figure 3.43 les différents éléments qui constituent le système ABS qui nous intéressent (capteur, calculateur, étrier, groupe hydraulique) ainsi que les deux étapes du freinage (avec ou sans ABS) identifié grâce au diagramme état/transition de la méthode SA-RT présenté sur la figure 3.41.

La deuxième étape de la modélisation consiste à rajouter la partie dysfonctionnelle du système ABS, obtenue dans la partie 3.4.2.2 à partir du tableau AMDE/AEEL de la figure 3.42 qui consiste à lister tous les modes de défaillance que peut rencontrer le système.

La figure 3.44 représente la modélisation fonctionnelle et dysfonctionnelle du système ABS basée sur les deux études effectuées précédemment qui sont l'analyse fonctionnelle et l'analyse dysfonctionnelle. Dans ce réseau de Petri, nous avons pris en compte uniquement les modes de défaillance qui ont pour effets l'absence de freinage et l'absence d'assistance ABS (voir tableau 3.42)

Le jeton se trouvant dans la place nommée *initial* représente le marquage initial du réseau de Petri et par la même occasion l'état initial du système de freinage. Lorsque le conducteur appuie sur la pédale de frein, le système de freinage est mis en marche. Le jeton franchira la transition *Normal* (qui représente le freinage normal ou sans ABS) ou la transition *ABS* (qui représente le freinage en utilisant le système ABS) en fonction de la cause du freinage (force appliquée sur la pédale) et à la vitesse à laquelle le conducteur

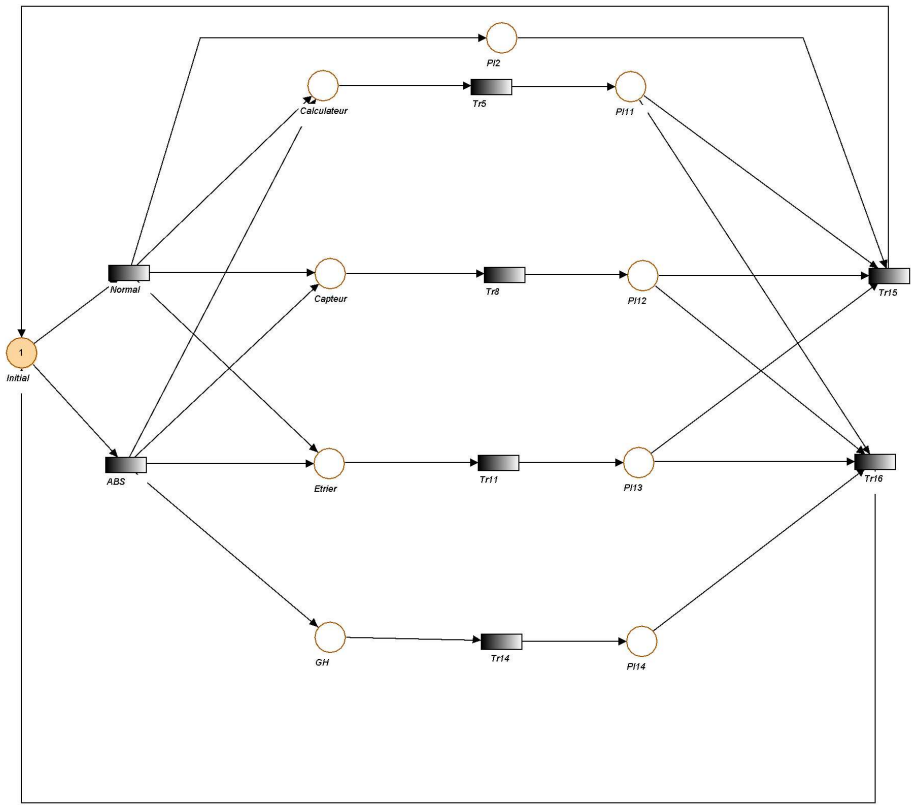

FIGURE 3.43 – Modélisation fonctionnelle du système ABS

roulait.

Si on considère le cas d'un freinage sans ABS, le jeton franchit la transition *Normal* et il se retrouve ainsi dans trois places qui sont : *Calculateur*, *Capteur* et *Etrier*. Ceci signifie que ces trois composants (le calculateur, le capteur et l'étrier) sont en fonctionnement.

Le jeton se trouvant dans la place *Calculateur*, par exemple, peut franchir deux transitions : *Def-Calculateur* et *tr5* ce qui correspond à deux états différents. S'il franchit la transition *tr5* cela signifie que le calculateur a fonctionné normalement et que le jeton peut revenir à la place *Initial*. Dans le cas contraire, le jeton se trouvera dans la place *Calculateur-HS* et illustrera une défaillance de ce composant.

Les transitions $T_{Def-Cal}$, $T_{Def-Cap}$, $T_{Def-Etr}$ et T_{Def-GH} représentent, respectivement, les probabilités de défaillance du calculateur, du capteur, de l'étrier et enfin du groupe hydraulique. Nous n'avons considéré qu'un seul mode de défaillance par composant afin de faciliter les calculs.

Le réseau de Petri que nous avons modélisé nous aidera à estimer la fiabilité du système ABS. Pour cela il est nécessaire d'attribuer des temps de fonctionnement aux transitions fonctionnelles ainsi que des lois de probabilité pour les transitions dysfonctionnelles associées à chaque composant du système ABS.

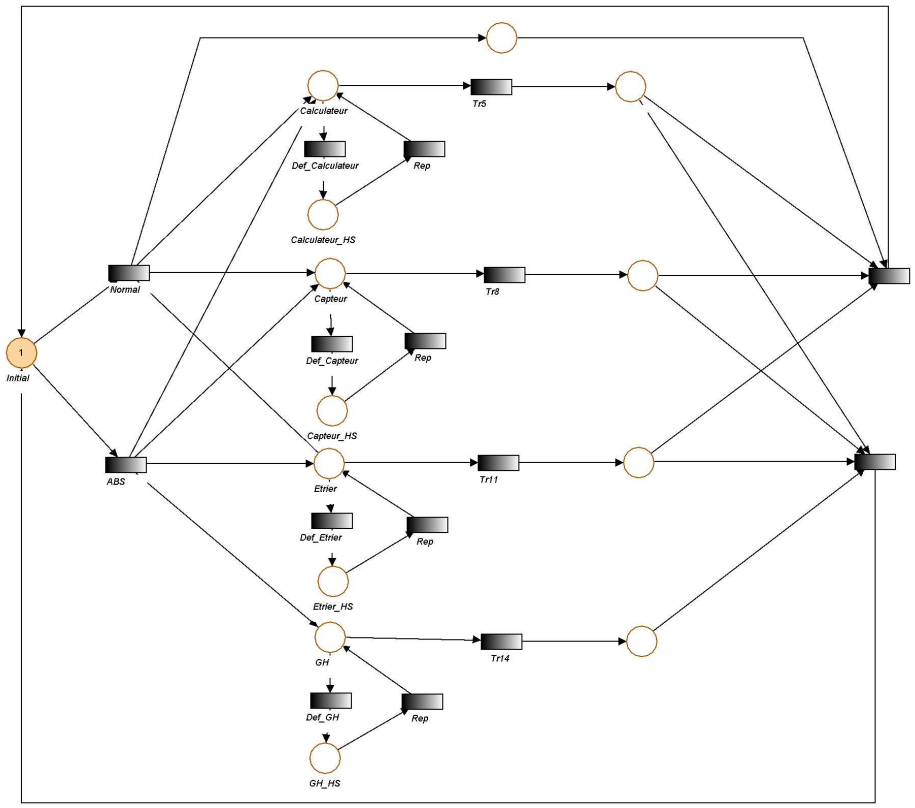

FIGURE 3.44 – Modélisation fonctionnelle et dysfonctionnelle du système ABS

Les temps associés aux transitions fonctionnelles (T_{ABS} et T_{Normal} dans la figure 3.44) représentent le temps du freinage avec ou sans ABS. Pour obtenir ces temps, il est nécessaire de construire un modèle physique grâce aux équations différentielles obtenues à partir de ce système.

3.4.4 Modélisation dynamique

La phase de la modélisation dynamique consiste à déterminer, à partir du profil de mission, les variables internes x_i.

La dynamique du système ABS est décrite par des équations différentielles qui permettent, également, de construire un modèle physique de ce système ABS.

3.4.4.1 Détermination des équations différentielles

Pour obtenir ces équations différentielles représentant, tout d'abord, une roue freinée du véhicule avec tous les efforts qui s'appliquent sur cette dernière (figure 3.45) [51, 88, 56, 98, 13, 62, 6, 7].

ω représente la vitesse angulaire, T_t est le moment de frottement, T_b le moment de

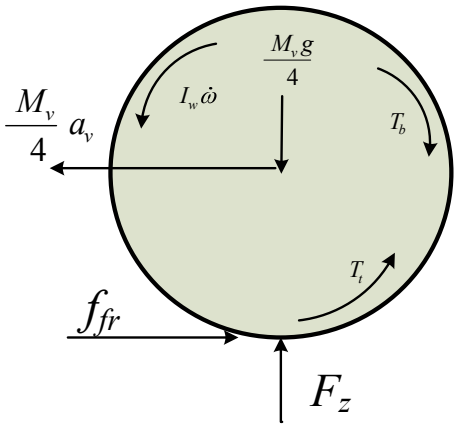

FIGURE 3.45 – Efforts agissant sur une roue freinée

freinage, I le moment d'inertie, a_v représente l'accélération du véhicule, f_{fr} est la force de frottement, M_v la masse du véhicule, μ le coefficient de frottement, F_z est l'effort normal agissant sur la roue, V_v représente la vitesse du véhicule et enfin R représente le rayon de la roue.

A partir des efforts appliqués sur une des quatre roues du véhicule comme le montre la figure 3.45 nous pouvons donc écrire les équations suivantes :

La somme des forces suivant l'axe y nous donne l'expression (équation 3.18) :

$$F_z = \frac{M_v}{4} \cdot g \tag{3.18}$$

La somme des forces suivant l'axe x nous permet d'avoir l'expression de la force de frottement (équation 3.19) :

$$-F_{fr} = \frac{M}{4} \cdot a_v \tag{3.19}$$

L'expression de la vitesse s'écrira alors comme suit (équation 3.20) :

$$V_v = \int a_v \cdot dt + V_{v0} = \int -\frac{4F_{fr}}{M_v} \cdot dt + V_{v0} \tag{3.20}$$

La force de frottement est égale à :

$$F_{fr} = \mu \cdot F_z \tag{3.21}$$

En remplaçant 3.18 dans 3.21, on obtient l'expression suivante :

$$F_{fr} = \mu \cdot \frac{M_v}{4} g \tag{3.22}$$

La somme des moments agissant sur la roue s'écrivent de la manière suivante (équation 3.23) :

$$T_t - T_b = I\dot{\omega} \tag{3.23}$$

Le moment généré par la force de frottement s'écrit comme montré sur l'équation 3.24 :

$$T_t = F_{fr} \cdot R = \mu \frac{M_v g}{4} R \tag{3.24}$$

En remplaçant 3.24 dans 3.23 on obtient l'équation 3.25 :

$$\mu \frac{M_v g}{4} R - T_b = I\dot{\omega} \tag{3.25}$$

L'expression de la vitesse angulaire ω s'écrit de la manière suivante (équation 3.26) :

$$\omega = \int \dot{\omega} \cdot dt + \omega_0 = \int \frac{1}{I} \left(\mu \frac{M_v g}{4} R - T_b \right) \cdot dt + \omega_0 \tag{3.26}$$

Le taux de glissement est défini comme suit (équation 3.27) :

$$S = \frac{V_v - R\omega}{V_v} \tag{3.27}$$

Afin de calculer la force de frottement F_{fr} présentée dans l'équation 3.21, il est nécessaire de connaître le coefficient de frottement μ. Pour cela nous utilisons la courbe présentée sur la figure 3.46.

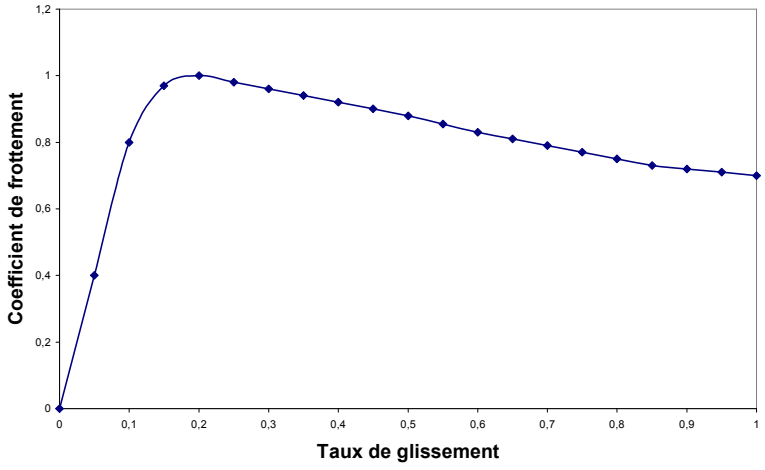

FIGURE 3.46 – Coefficient de frottement en fonction du glissement

Cette figure représente le graphe du coefficient de frottement en fonction du glissement.

Cette courbe a été tracée grâce à la formule *magique* de Pacejka (Pacejka magic formula) de l'équation 3.28 [104, 36, 80, 63].

$$F_{fr} = D \sin\left(C \arctan\left(B\phi\right)\right) + S_v \tag{3.28}$$

sachant que :

$$\phi = (1 - E)\left(S + S_h\right) + \frac{E}{B} \arctan\left(B\left(S + S_h\right)\right) \tag{3.29}$$

Coefficients	B	C	D	E	S_h	S_v
Valeurs	8	1,65	3444	-2,9	0	0

TABLE 3.3 – Valeurs des coefficients de la formule magique de Pacejka (équation 3.28)

3.4.4.2 Modélisation physique du système ABS

Après la détermination des équations différentielles propres au système ABS, nous construisons le modèle physique de ce système en utilisant Simulink.

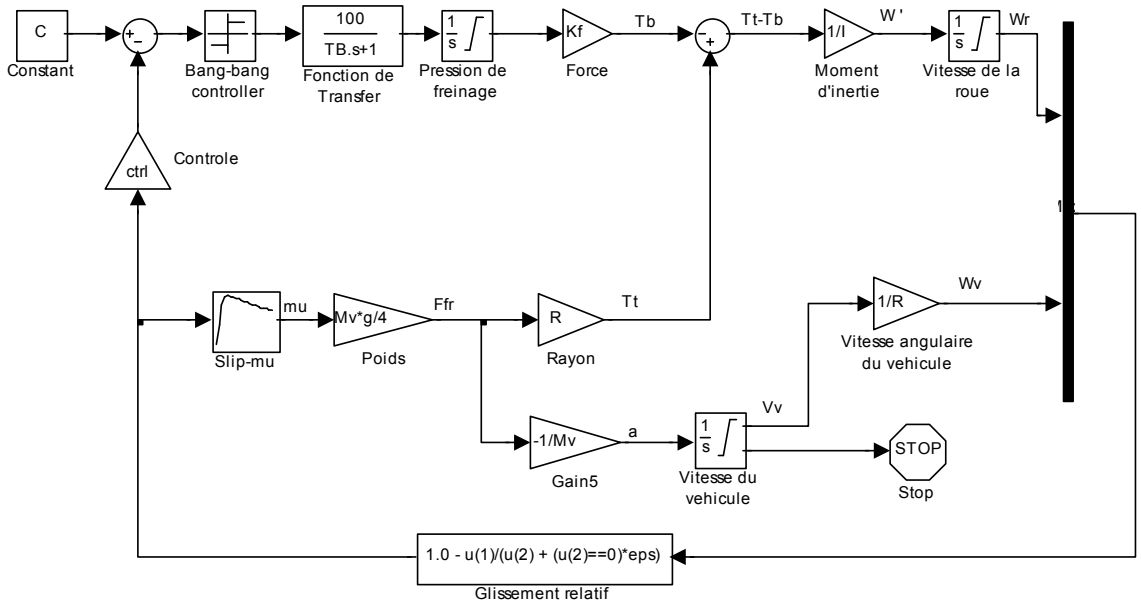

FIGURE 3.47 – Modélisation physique du système ABS dans Simulink

La figure 3.47 regroupe toutes les équations différentielles propres au système ABS. Cette figure nous permet de calculer les variables internes x_i dont nous avons besoin qui sont : le temps de fonctionnement des différents composants de l'ABS, le temps de freinage avec ou sans ABS, le nombre de cycles du groupe hydraulique, le glissement de la roue

ainsi que la pression du liquide de frein dans l'étrier. Les données de ces simulations sont regroupées dans le tableau 3.4 :

Paramètres	C	g (m/s^2)	R (m)	M_v (kg)	I ($kg.m^2$)
Valeurs	0.2	9.81	0.387	1200	5

TABLE 3.4 – Valeurs des paramètres utilisés dans le modèle physique

Le système subit des sollicitations externes qui jouent un rôle important dans le profil de mission de ce système. En effet, ces sollicitations externes peuvent influencer le passage du système d'un état à un autre ou de modifier les temps de fonctionnement des différents composants de ce système. En ce qui concerne le système de freinage, la vitesse initiale V_0 au moment du freinage, la force avec laquelle le conducteur appuie sur la pédale de frein, la charge du véhicule (nombre de personnes à bord, coffre vide ou plein, etc.) sont des facteurs influant sur le profil de mission de ce système de freinage. Nous nous sommes intéressés, dans cette application, uniquement à la vitesse initiale V_0. Nous effectuons les simulations pour quatre vitesses initiales différentes et les résultats obtenus sont illustrés sur la figure 3.48.

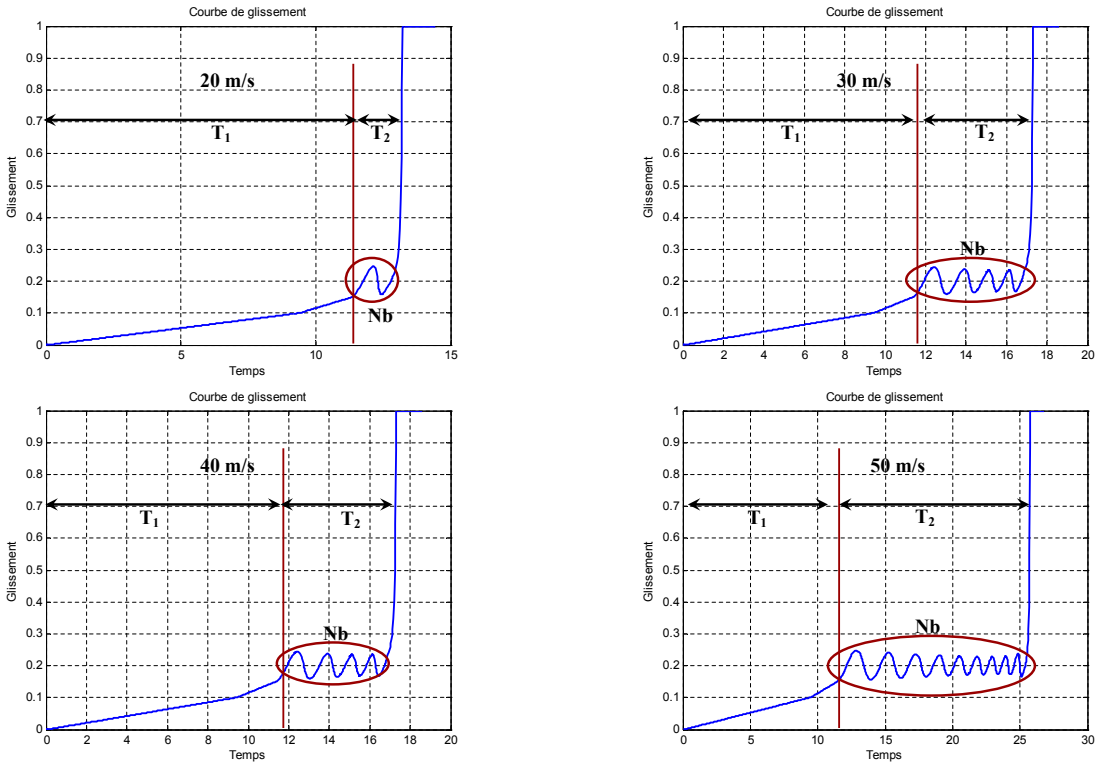

FIGURE 3.48 – Courbes de glissement

Les courbes illustrées sur la figure 3.48 représentent la valeur du glissement en fonction du temps pour différentes vitesses initiales. A partir de ces courbes nous pouvons en

déduire le temps de freinage avec ou sans ABS, le nombre de cycles du groupe hydraulique ainsi que le temps de fonctionnement des différents composants du système. Ces résultats sont récapitulés dans le tableau :

	20 m/s (30 %)	**30 m/s** (15 %)	**40 m/s** (10 %)	**50 m/s** (5 %)
$\mathbf{T_1}$	11,7627	11,9138	12,032	12,1324
$\mathbf{T_2}$	2,6684	6,6864	10,6098	14,6766
Nb	2	8	14	18
T	14,4311	18,6002	22,6418	26,809

TABLE 3.5 – Résultats des simulations du modèle physique du système ABS

T_1 représente le temps de freinage sans ABS, T_2 le temps de freinage avec ABS, Nb le nombre de cycles du groupe hydraulique et T le temps de freinage total.

On peut déduire de ce tableau que plus la vitesse initiale est grande plus le temps de fonctionnement des différent composants est important.

Lors de l'utilisation du véhicule, la vitesse initiale (début du freinage) varie aléatoirement en fonction des différents paramètres. Par exemple ; le conducteur ne roule pas à la même vitesse s'il est sur une autoroute ou sur une nationale ce qui peut engendrer une différence dans la vitesse initiale au moment du début de freinage. Cette vitesse initiale aléatoire est représentée sur la figure 3.49.

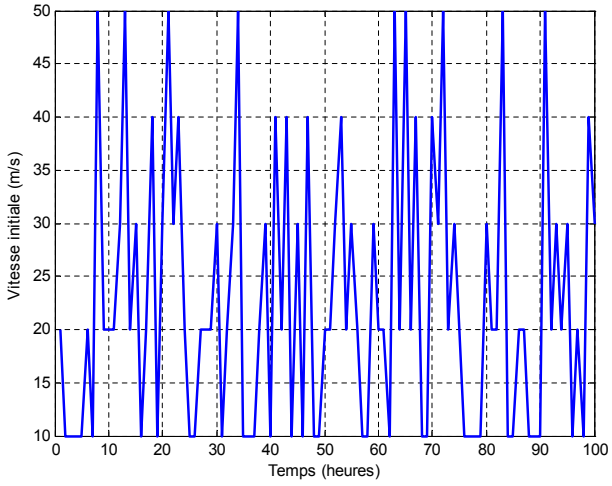

FIGURE 3.49 – Vitesse initiale (m/s)

A partir de cette vitesse initiale aléatoire, nous pouvons déduire les temps de freinage sans l'utilisation du système ABS par simulation du modèle Simulink ce qui nous donne les résultats de la figure 3.50.

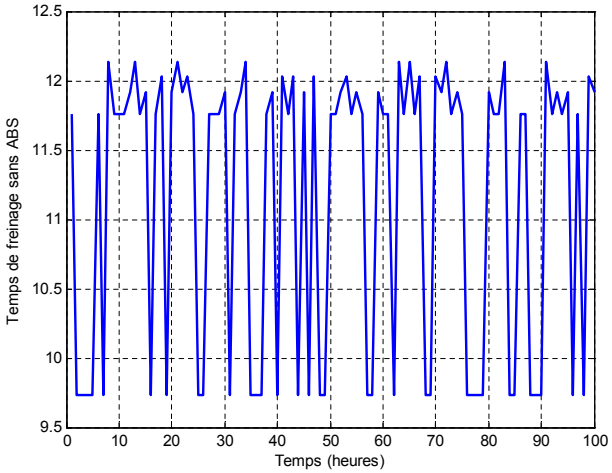

FIGURE 3.50 – Temps de freinage sans ABS (s)

De la même façon, nous pouvons, également, calculer les temps de freinage en utilisant l'ABS associés à cette vitesse initiale. Les résultats sont illustrés sur la figure 3.51.

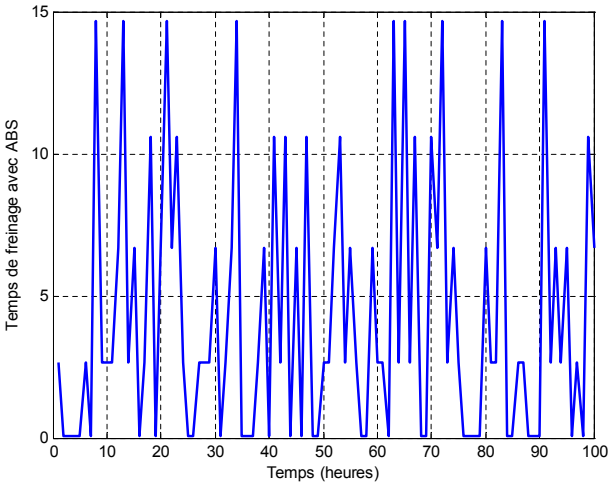

FIGURE 3.51 – Temps de freinage avec ABS (s)

Une autre information peut être obtenue grâce aux simulations du modèle physique de Simulink : c'est la variable interne que subit le système. Dans notre cas d'étude cette variable interne est la pression exercée sur l'étrier et elle est représentée sur la figure 3.52.

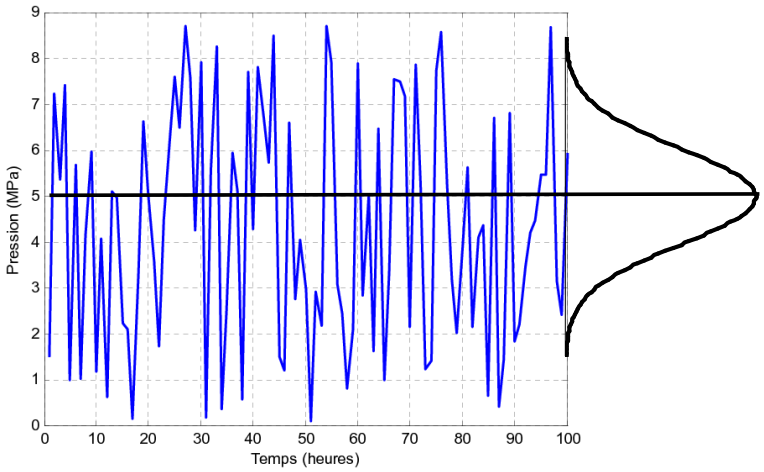

FIGURE 3.52 – Pression appliquée sur l'étrier

La pression que subit l'étrier est un processus stochastique aléatoire pour lequel nous avons associé une loi de distribution afin d'obtenir une représentation approchée de celui-ci. A ces résultats de la figure 3.52, nous associons une loi normale qui a pour moyenne $\mu_P = 5$ MPa et un écart-type $\sigma_P = 0.5$ MPa.

3.4.4.3 Fiabilité du composant mécanique (étrier)

Pour estimer la fiabilité de l'étrier, nous avons choisi d'utiliser la méthode PHI2 qui consiste à utiliser une approche qui permet de calculer le taux de franchissement comme on l'a déjà vu dans le chapitre 2.

La démarche de la méthode PHI2 est la suivante :

- Faire un premier calcul FORM pour estimer l'indice de fiabilité β(t) associé à $G(t,X(t,\omega))\leq 0$
- Faire un deuxième calcul FORM pour estimer l'indice de fiabilité β(t+Δt) associé à $G(t+\Delta t,X(t+\Delta t,\omega))\leq 0$
- Calculer le taux de franchissement (donné par [90]) qui s'écrit :

$$\nu^{+}_{PHI2}(t) = \frac{\|\alpha(t+\Delta t)-\alpha(t)\|}{\Delta t}\phi(\beta(t))\,\Psi\left(\frac{\beta(t+\Delta t)-\beta(t)}{\|\alpha(t+\Delta t)-\alpha(t)\|}\right) \tag{3.30}$$

Pour les deux calculs FORM on considère le cas instationnaire défini par [3, 90] où $G(t,X(t,\omega))$ est égal à :

$$G(t, X(t,\omega)) = R(\omega) - d\cdot t - S(t,\omega) \tag{3.31}$$

La contrainte S est obtenue, à partir de la pression, grâce à un calcul élément fini sur

l'étrier. Les variables sont données sur le tableau 3.6 :

Variables	μ_R	σ_R	μ_S	σ_S	d
Valeurs	227,6	22,76	161,2	11	2,5

TABLE 3.6 – Données numériques relatives à l'étrier

L'écart-type de la contrainte S est calculé par l'expression suivante (équation 3.32) :

$$\sigma_S = \sqrt{\left(\frac{d\sigma_{\max}(P)}{dP}\right)^2 \times \sigma_P^2} \tag{3.32}$$

avec :

$$\frac{d\sigma_{\max}(P)}{dP} \approx \frac{\sigma_{\max}(P+dP) - \sigma_{\max}(P)}{dP} \tag{3.33}$$

m_R représente la moyenne de la résistance, σ_R l'écart type de la résistance, m_S est la moyenne de la sollicitation, σ_S l'écart type de la sollicitation et d un coefficient de dégradation.

La résistance est représentée par la limite d'endurance σ_D qui est donnée par :

$$N = A \cdot \sigma_D^{-k} \tag{3.34}$$

N est le nombre de cycles ($N = 10^7$) est A et K représente les paramètres du modèle de Basquin avec A= $5{,}81.10^{51}$ et k = 18.99 [43].

Le taux de franchissement de l'équation 3.30 peut être calculé est le résultat est présenté sur la figure 3.53

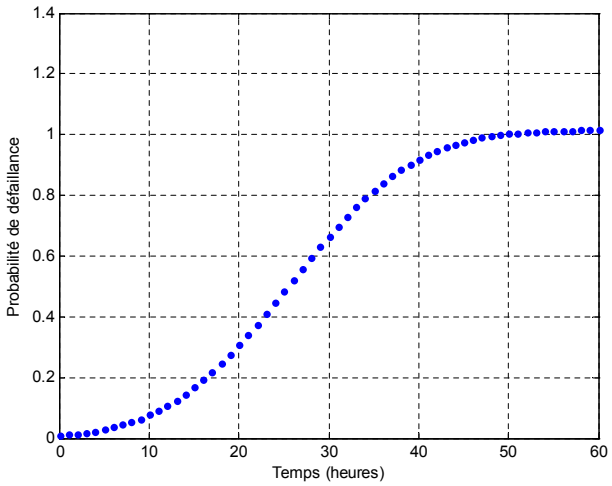

FIGURE 3.53 – Taux de franchissement en fonction du temps

La probabilité de défaillance est, ainsi égale à :

$$P_{f,c}\left(t_1, t_2\right) \leq P_{f,i}\left(t_1\right) + \int_{t_1}^{t_2} \nu\left(t\right) dt \tag{3.35}$$

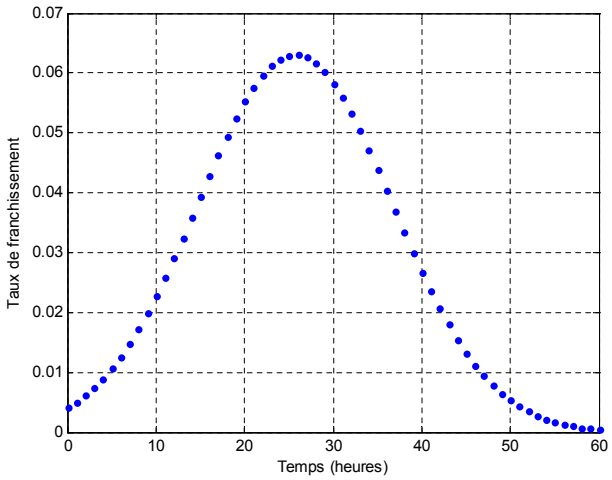

FIGURE 3.54 – Probabilité de défaillance de l'étrier en fonction du temps

La fiabilité du composant mécanique est désormais connue, nous pouvons donc estimer la fiabilité du système ABS.

3.4.5 Simulation

La dernière étape de notre méthodologie consiste à effectuer des simulations du réseau de Petri de la figure 3.44 en considérant les lois de distribution du tableau 3.7 avec les paramètres qui leur sont associés. Nous tenons compte également des temps de fonctionnement que nous avons obtenus à partir des simulations du modèle physique de la figure 3.47.

Composants	**lois**	**Paramètres**
Capteur	Exponentielle	$\lambda = 3.10^{-4}$ (h^{-1})
Calculateur	Exponentielle	$\lambda = 50\mathrm{x}3.10^{-6}$ (h^{-1})
Etrier	Weibull	$\beta = 2{,}69$, $\eta = 4000$ (h)
Pompe	Weibull	$\beta = 1{,}5$ $\eta = 1000$ (cycles)

TABLE 3.7 – Valeurs des paramètres utilisés pour les simulations fonctionnelle et dysfonctionnelle

Après simulation nous obtenons les résultats présentés sur la figure 3.55

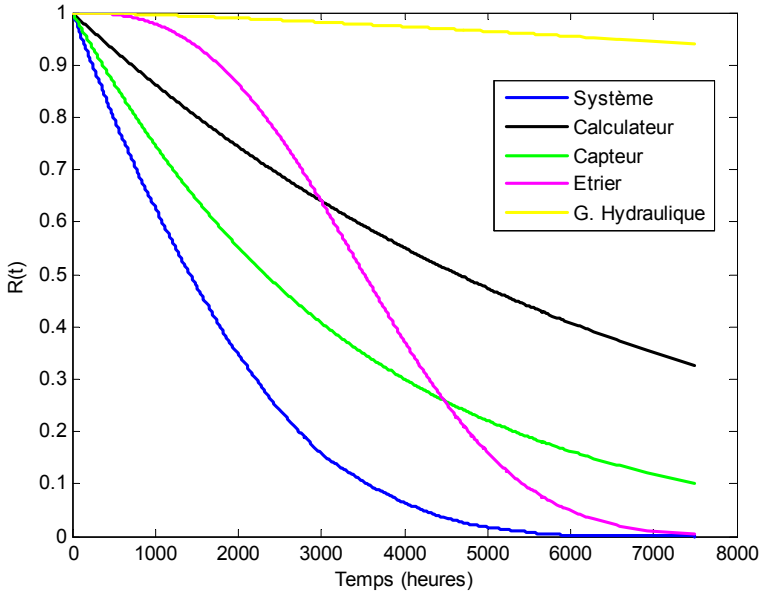

FIGURE 3.55 – Fiabilité du système ABS et de ses différents composants

Sur cette figure 3.55, nous avons tracé la fiabilité du système ABS ainsi que celle des différents composants : calculateur, capteur, étrier et groupe hydraulique. Nous constatons sur ce graphe que la fiabilité du groupe hydraulique est la plus importante ceci peut s'expliquer par son utilisation occasionnelle (1%) du temps total.

Composants	**Lois**	**Paramètres estimés**	**Borne inférieure**	**Borne supérieure**
Calculateur	Exponentielle	$\hat{\lambda} = 1.61\ 10^{-4}$	$\hat{\lambda}_{inf} = 1.49\ 10^{-4}$	$\hat{\lambda}_{sup} = 1.72\ 10^{-4}$
Capteur	Exponentielle	$\hat{\lambda} = 3.034\ 10^{-4}$	$\hat{\lambda}_{inf} = 2.91\ 10^{-4}$	$\hat{\lambda}_{sup} = 3.16\ 10^{-4}$
Etrier	Weibull	$\hat{\eta} = 3968.52$ $\hat{\beta} = 2.79$	$\hat{\eta}_{inf} = 3883.86$ $\hat{\beta}_{inf}$ 2.61	$\hat{\eta}_{sup} = 4045.53$ $\hat{\beta}_{sup}$ 2.82
Pompe	Weibull	$\hat{\eta} = 93482.32$ $\hat{\beta} = 1.18$	$\hat{\eta}_{inf} = 37716.91$ $\hat{\beta}_{inf} = 0.93$	$\hat{\eta}_{sup} = 231698.31$ $\hat{\beta}_{sup} = 1.5$

TABLE 3.8 – Valeurs des paramètres estimés

Une autre remarque peut être faite : la fiabilité composants est plus élevée que la fiabilité système. Cela est dû à l'interaction entre les composants qui fait en sorte que le système est moins fiable que les composants qui le constituent.

Pour compléter cette étude nous estimons la fiabilité par fonctions du système. Le système ABS possède deux fonctions différentes : freinage avec ABS ou freinage sans ABS.

La figure 3.56 nous montre la fiabilité de ces deux fonctions et nous constatons que

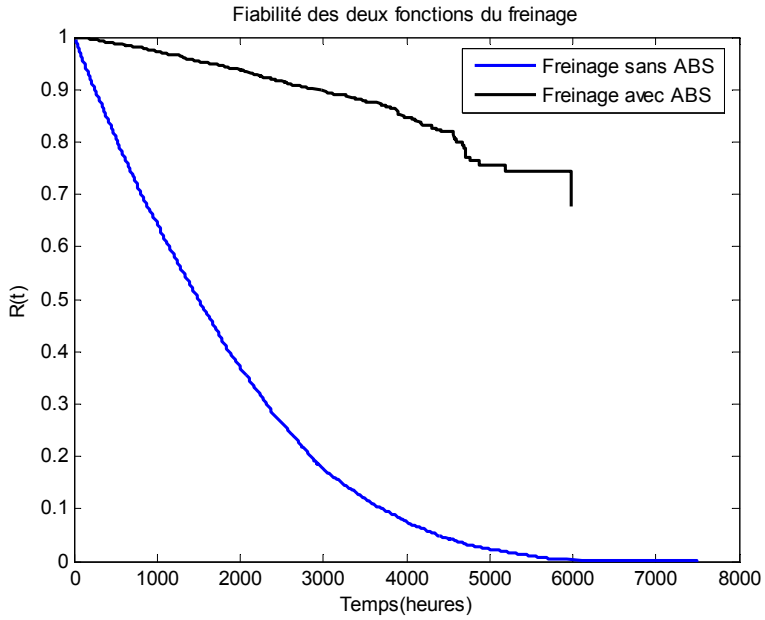

FIGURE 3.56 – Fiabilité des deux fonctions du freinage

la fiabilité de la première fonction qui est le freinage avec ABS est plus élevée que la deuxième fonction (freinage sans ABS) du fait de son utilisation réduite (1% du temps de freinage).

Pour compléter cette étude nous pouvons également estimer la fiabilité des différents composants qui constituent le système mécatronique.

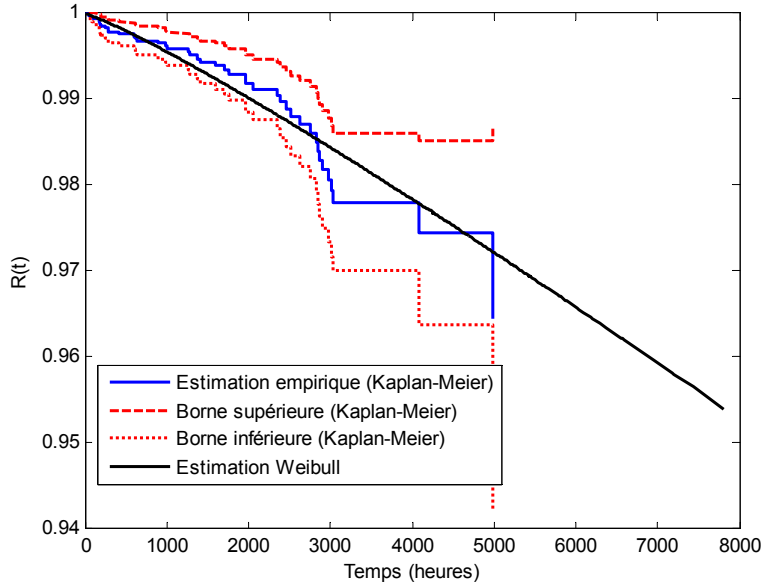

FIGURE 3.57 – Fiabilité de la pompe en fonction du temps

La figure 3.57 représente la fiabilité de la pompe avec les intervalles de confiance à

95% en fonction du temps.

La fiabilité de ce composant peut être estimée en fonction du nombre de cycles comme montré sur la figure 3.58

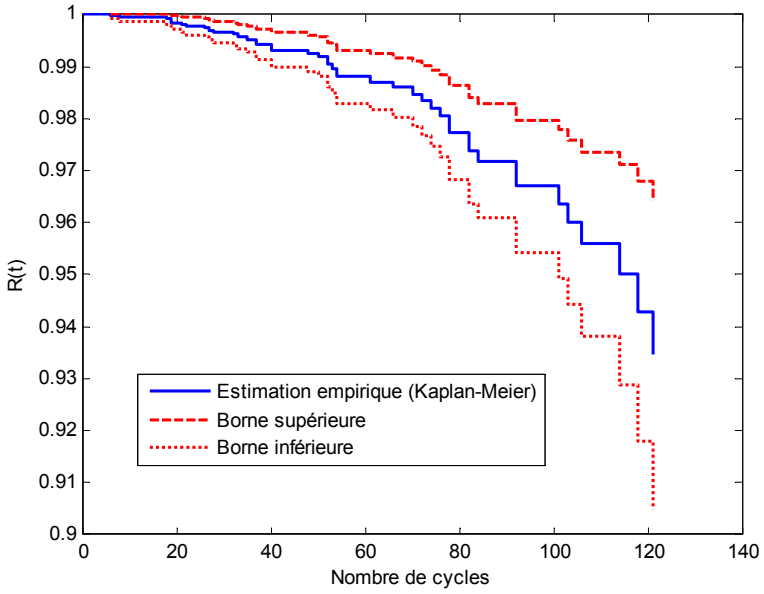

FIGURE 3.58 – Fiabilité de la pompe en fonction du nombre de cycles

Cette étude permet de statuer sur le niveau de fiabilité atteint par la conception étudiée. Afin d'améliorer cette fiabilité, une étude des facteurs de sensibilité est nécessaire pour déterminer l'influence de chaque composant du système sur la fiabilité de ce dernier. Grâce à cette analyse de sensibilité, nous pouvons faire face aux faiblesses du système en modifiant son architecture et construire ainsi une architecture tolérante aux fautes.

3.5 Conclusion

Dans ce chapitre, nous avons exposé la problématique des systèmes mécatroniques et nous avons proposé une méthodologie dans le but de faire face à ces problèmes engendrés par ces systèmes.

Pour estimer la fiabilité d'un système complexe, il est important, dans un premier temps, de le modéliser. C'est pourquoi, la première partie de la méthodologie que nous proposons est l'analyse qualitative qui nous fournira toutes les informations nécessaires sur le fonctionnement et le dysfonctionnement d'un système mécatronique.

Afin d'obtenir ces informations, nous devons effectuer deux types d'analyses : une analyse fonctionnelle et une analyse dysfonctionnelle.

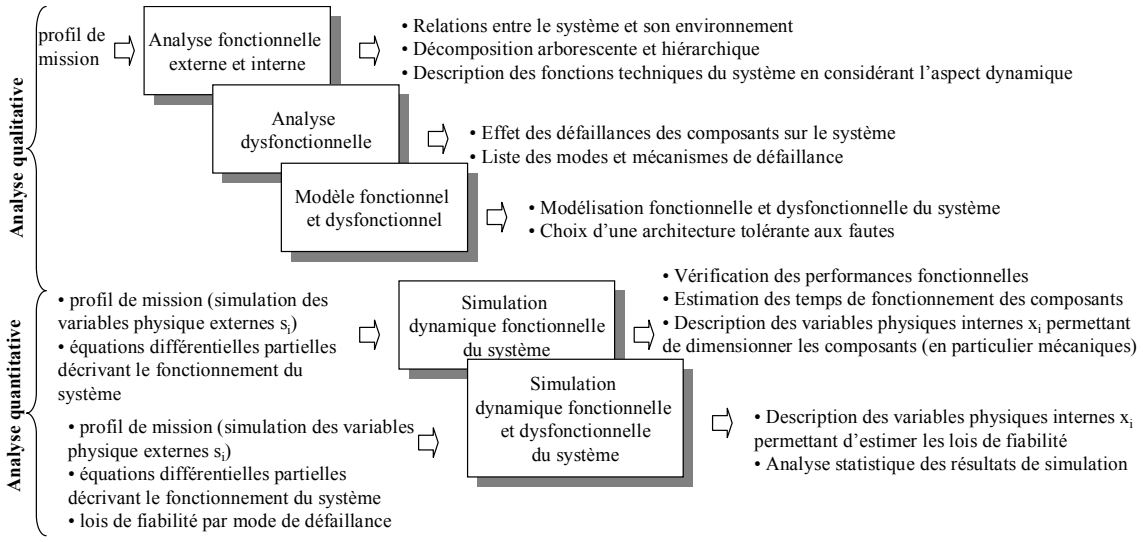

FIGURE 3.59 – Démarche globale pour l'évaluation, la modélisation et l'estimation de la fiabilité d'un système mécatronique

Pour commencer l'analyse fonctionnelle, une Analyse Fonctionnelle Externe (AFE) est appliquée au système mécatronique à traiter. Cette analyse fonctionnelle externe, que nous avons détaillée dans le chapitre 2, permet d'illustrer les relations entre un système et son milieu extérieur. Néanmoins, aucune information sur les fonctions internes du système n'est obtenue.

Il est donc nécessaire d'effectuer une Analyse Fonctionnelle Interne (AFI) qui comble ce manque d'information. Cette analyse permet de décrire les modes de fonctionnement d'un système ainsi que ses fonctions internes.

Ces deux analyses fonctionnelles interne et externe (AFE et AFI) fournissent uniquement des indications concernant le fonctionnement d'un système. Il est important d'avoir des informations sur les différents modes de défaillance de ce système. C'est pour cette raison que nous effectuons une analyse dysfonctionnelle afin de déterminer les principales causes de défaillance ainsi que les différents états d'un système.

Les analyses fonctionnelle et dysfonctionnelle constituent l'analyse qualitative qui illustre le fonctionnement et le dysfonctionnement d'un système. Grâce à cette analyse qualitative, nous pouvons modéliser le système afin d'effectuer la deuxième phase de notre méthode qui concerne l'analyse quantitative qui permettant d'estimer la fiabilité d'un système mécatronique.

Par la suite, nous avons appliqué cette méthodologie pour traiter un système mécatronique simple et bien connu dans le monde automobile : le système ABS. Les différentes étapes que nous avons citées précédemment dans ce chapitre sont utilisées pour l'estima-

tion de la fiabilité de ce système ABS.

Conclusion générale

L'apparition des systèmes mécatroniques est une révolution pour le monde industriel, il affecte de plus en plus le monde du transport et en particulier le secteur automobile. L'utilisation de ces systèmes se généralise rapidement et à tous les secteurs de l'industrie.

Durant cette thèse, nous avons développé une méthodologie globale permettant d'estimer la fiabilité des systèmes complexes.

Les systèmes mécatroniques étant des systèmes dynamiques (relations changeantes au court de la mission), hybrides (phénomènes continus et événements discrets), reconfigurables (architectures tolérantes aux fautes) et multitechnologies (mécanique, électronique, logiciel, hydraulique, etc.), notre méthodologie se doit de tenir compte de tous ces aspects. C'est pourquoi nous nous somme basé sur la démarche systémique afin d'élaborer cette méthodologie.

Aussi, la conception des systèmes mécatroniques, comportant une intégration élevée de composants de technologies différentes et relevant de plusieurs disciplines, nécessite dès le début de l'étude un travail collaboratif entre les différents acteurs du développement, afin de réaliser un produit industriel compétitif et de qualité. Il est, donc, nécessaire de disposer d'une démarche unique qui permet de construire la fiabilité. La méthodologie proposée aborde les points suivants :

- les fonctions à remplir ;
- les profils de mission (utilisation et environnement) ;
- effets des défaillances des composants sur le système ;
- les mécanismes de tolérance aux fautes (architecture matériel et logiciel) ;
- l'hétérogénéité technologique des composants (mécanique, électronique, logiciel, etc.) ;
- la dynamique de fonctionnement (description physique du fonctionnement) ;
- la défaillance des composants (lois de fiabilité pour chaque composant) ;
- le modèle fonctionnel et dysfonctionnel (modèle unifié) ;
- l'estimation de la fiabilité aux niveaux système, fonction et composant.

Deux parties sont indispensables pour répondre à ces différents points : une partie analyse qualitative et une autre quantitative.

1. **L'analyse qualitative :** L'objectif de l'analyse qualitative est d'identifier toutes les fonctions d'un système ainsi que toutes les causes de défaillance pouvant affecter son bon fonctionnement. Cette analyse qualitative est généralement composée de deux grandes étapes qui sont l'analyse fonctionnelle et l'analyse dysfonctionnelle.
   - *L'analyse fonctionnelle* permet la description synthétique des modes de fonctionnement d'un système et la connaissance des fonctions à garantir. En d'autres termes, elle consiste à rechercher et à caractériser les fonctions offertes par un système pour satisfaire les besoins de son utilisateur.

     L'analyse fonctionnelle externe permet d'illustrer les relations entre un système et son milieu extérieur. Cependant, nous n'avons aucune information concernant ces fonctions internes d'où la nécessité de faire une analyse fonctionnelle interne. L'analyse fonctionnelle interne permet de réaliser une décomposition arborescente et hiérarchique du système en éléments. Elle décrit également les fonctions techniques du système. Nous avons choisi d'utiliser la méthode SADT car elle s'applique à tout le système mécatronique, c'est à dire qu'elle s'adapte aussi bien aux composants mécaniques et électroniques qu'au logiciel. Nous nous somme intéressé, aussi, à la méthode SA-RT dans le but de prendre en compte l'aspect dynamique, qui manque à la méthode SADT. De plus, à partir de la méthode SA-RT nous construisons une correspondance avec les réseaux de Petri.

     Cette analyse fonctionnelle ne prend pas en compte les défaillances que peut rencontrer le système. C'est pourquoi nous l'avons complétée avec une analyse dysfonctionnelle.
   - *L'analyse dysfonctionnelle* permet de mettre en évidence les défaillances potentielles que peut rencontrer un système mécatronique.

     Ces étapes (analyse fonctionnelle et dysfonctionnelle) nous permettent de construire un modèle fonctionnel et dysfonctionnel grâce aux réseaux de Petri. Notre choix s'est porté sur les réseaux de Petri car ils permettent :
     - la modélisation d'un système mécatronique intégrant différents technologies ;
     - l'utilisation dans chaque étape du cycle de développement ;
     - l'analyse du comportement fonctionnel et dysfonctionnel ;
     - la prise en compte de l'aspect dynamique du système.
2. **L'analyse qualitative** fournie des informations sur le fonctionnement et le dysfonctionnement d'un système mécatronique, mais ne donne aucune information sur les quantités telle que la probabilité de défaillance. Afin de la compléter, on se doit de faire une analyse quantitative.

   La première étape de cette analyse quantitative consiste à effectuer des simulations

dynamiques fonctionnelles du système en tenant compte du profil de mission (simulations des variables physiques externes) et en utilisant les équations différentielles partielles décrivant le fonctionnement du système. Ces simulations dynamiques fonctionnelles nous permettent de connaître le temps de fonctionnement de chaque composant ainsi que la description des variables internes. Ces temps de fonctionnements sont associés aux transitions fonctionnelles du réseau de Petri précédemment modélisé.

En ce qui concerne les transitions dysfonctionnelles, nous avons attribué une loi exponentielle pour le composant électronique et le modèle de Musa pour le composants logiciel. Cependant, d'autres lois de probabilité peuvent être attribuées aux différents composants du système mécatronique. Dans le cas du composant mécanique, nous avons construit la loi de fiabilité associée en utilisant les variables physiques internes obtenues par la résolution des EDP et la méthode PHI2 qui permet d'estimer la fiabilité d'un composant mécanique en fonction du temps.

La simulation dynamique fonctionnelle et dysfonctionnelle nous permet d'estimer la fiabilité au niveau système, fonctions et composants.

Pour faciliter l'utilisation future de notre méthodologie dans un contexte industriel, il est nécessaire de concevoir un outil informatique automatisant les calculs. Cela pourrait être, par exemple, par l'implémentation de bibliothèques permettant la résolution des équations différentielles.

Dans le cas de l'analyse fonctionnelle nous utilisons les méthodes SADT et SA-RT. Depuis quelques temps, plusieurs améliorations sont apportées aux langages UML et SysML ce qui permet peut être de traiter des systèmes complexes en tenant compte, d'une part des aspects dynamique, hybride et reconfigurable et, d'autre part, des différents composants qui constituent le système mécatronique. Il serait donc intéressant d'étudier plus en détail ces deux langages.

La méthodologie que nous avons développée traite uniquement la fiabilité prévisionnelle et la compléter par une étude de fiabilité opérationnelle et expérimentale est intéressante.

Il est très important, également, de prendre en compte le facteur humain qui joue un rôle important dans la conception du système. Les erreurs engendrées par le facteur humain peuvent être très variées et peuvent survenir à tout moment de la conception du système.

Une autre perspective de notre travail consiste à effectuer des essais de robustesse et d'estimation de la fiabilité grâce, entre autres, à la méthode de l'injection de fautes.

Annexe A

Méthodes d'analyse fonctionnelle

A.1 Cahier des Charges Fonctionnel (CdCF)

Traditionnellement, la définition préliminaire d'un produit ou d'un système est consignée sur un cahier des charges général. Ce CdCF met en évidence le service attendu du système par l'utilisateur. Il n'impose aucune solution et représente simplement l'expression du besoin en terme de résultat sans faire allusion à des solutions [10, 93, 107, 17]. Selon la norme NF X50-151, le CdCF est défini comme étant un document par lequel le demandeur exprime son besoin en terme de fonctions de service et de contraintes.

Le CdCF qui résulte d'une analyse fonctionnelle externe, est le document qui exprime le besoin en termes de fonctions détaillées et caractérisées. Peu importe le choix des solutions, le CdCF ne change pas pour autant mais la seule raison qui peut le faire évoluer est la modification du besoin par un complément de l'étude de marché ou par de nouvelles directives de l'utilisateur. Néanmoins il peut s'enrichir progressivement au cours de la création du système.

L'élaboration d'un CdCF doit permettre une juste perception du besoin et peut être décomposé de la manière suivante :

- définir le sujet traité ;
- situer le projet dans son contexte général ;
- former un groupe qui sera chargé d'effectuer les premières recherches de l'information ;
- valider le besoin et faire une analyse fonctionnelle externe ;
- rédiger et valider le CdCF.

Considérons l'exemple d'un CdCF d'une tondeuse à gazon électrique pour la quelle les informations suivantes sont disponibles [93] :

- tondeuse à gazon pour petites et moyennes surfaces ;

- électrique 220V ;
- permettant le taillage des touffes ;
- coupe à hauteur réglable ;
- avec récupération d'herbe coupée ;
- milieu de gamme.

N_0	**Désignation**	**K**	**Critère**	**Niveau**	**Tolérance**	**F**
1	Couper le gazon	5	Hauteur	20mm sans	+ 11mm	2
			Netteté de coupe	arrachement	- 8mm	
2	Tailler les touffes	2	Aspect	Test	-	3
3	Récupérer l'herbe coupée	2	Volume	$1/8m^3$	± 10%	2
4	Être puissante	3	Puissance	500W	± 10%	0
5	Être fiable	4	MTBF	500h	± 50h	1
6	Permettre le vidage	1	Accès	-	-	3
			Temps	2min	±10%	2
			Facilité	Test	-	3
7	Être ergonomique	3	Position des commandes	Test	-	3
8	Être maniable	2	Efforts	3dn	± 10%	1
			Poids	15kg	+0, -10%	1
9	Avoir une bonne vitesse de taille	3	Vitesse	20m/min	± 5%	2
10	Avoir une largeur de coupe adaptée	1	Largeur	0.40m	± 5%	2

TABLE A.1 – CdCF pour les fonctions de service d'une tondeuse à gazon

Le tableau A.1 représente le CdCF des fonctions de service d'une tondeuse à gazon. Il est nécessaire, dans cet exemple, d'effectuer d'autres CdCF pour les fonctions de service d'autre cas d'utilisation ainsi que pour les contraintes.
La désignations des coefficients K et F sont :
K : 1.utile - 2.nécessaire - 3.important - 4.très important - 5.vital.
F : 0.impératif - 1.peu négociable - 2.négociable - 3.très négociable.

A.2 Bloc diagramme Fonctionnel (BdF)

Le Bloc diagramme Fonctionnel est une représentation mettant en évidence les relations entre les composants et leurs milieux extérieurs, les interactions entre les composants du système ainsi que la circulation des flux à travers et à l'intérieur du système. Ce diagramme est utilisé dans le cas de systèmes mécaniques, électriques ou électroniques [82, 107].

Le BdF nous permet d'identifier les flux d'énergie. Certains de ces flux supportent les fonction de services du système qui sont reliés aux milieux extérieurs. Les flux bouclés internes sont le support des fonctions techniques ou des contraintes.

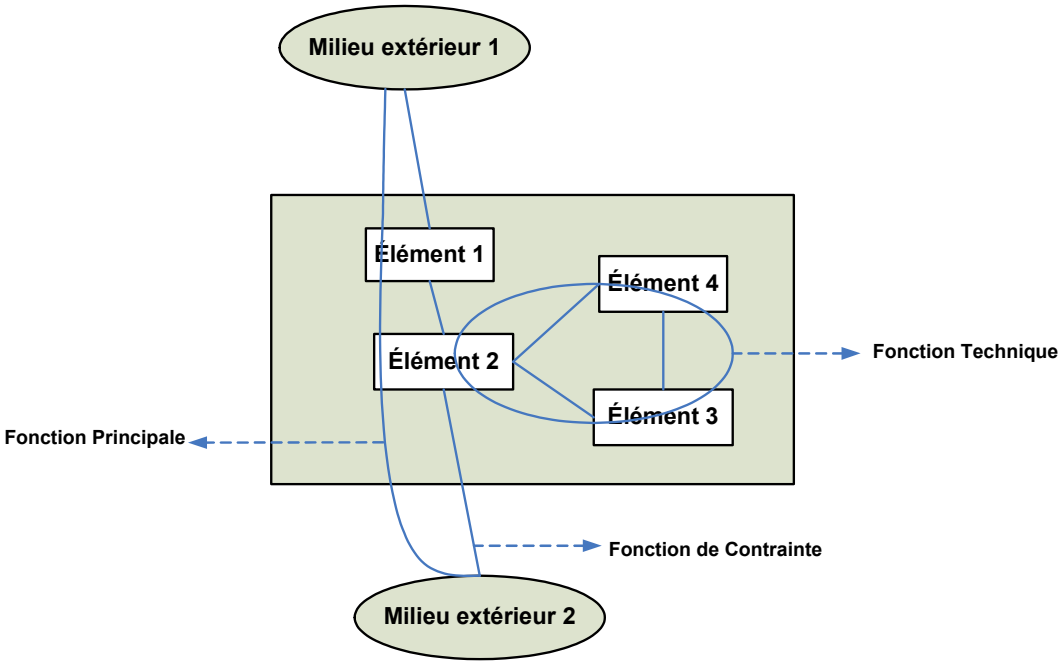

FIGURE A.1 – Description des relations entre les composants d'un système

La figure A.1 représente un système comportant quatre éléments et deux milieux extérieurs. A partir de celle-ci nous constatons qu'il existe, dans ce cas, une fonction principale qui met en relation l'élément 1 et l'élément 2, une fonction technique qui regroupe les éléments 2, 3 et 4 et enfin des fonctions de contraintes qui relient les éléments 1 et 2 ainsi que les deux milieux extérieurs.

Le BdF est généralement complété par un Tableau d'Analyse Fonctionnelle (TAF) résumé dans le paragraphe suivant.

A.3 Tableau d'Analyse Fonctionnelle (TAF)

Pour un système donné, nous constituons une liste des fonctions principales, techniques et de contraintes lues sur le BdF dans le but d'obtenir un tableau qui représentera le Tableau d'Analyse Fonctionnelle (TAF).

Le tableau A.2 représente un TAF et met en relation les fonctions élémentaires de tous les composants d'un système avec ses fonctions de service (principales et contraintes) et ses fonctions techniques.

	Fonctions élémentaires	**Fonctions de base**		**Fonctions techniques**
		principales	contraintes	
Elément 1				
Elément 2				
Elément 3				

TABLE A.2 – Tableau d'Analyse Fonctionnelle

A.4 Arbre Fonctionnel RELIASEP

La méthodologie de l'arbre fonctionnel a été développée par la Société Européenne de Propulsion (SEP). L'objectif de cette méthode est de faciliter les études de sûreté de fonctionnement durant les différentes phases de vie d'un système en déterminant avec précision le besoin à satisfaire [107, 93].

Le plan de travail de cette méthode peut se décomposer de la manière suivante :

- faire une analyse fonctionnelle externe en respectant le cadre de mission ;
- construire l'arbre fonctionnel qui prend en compte les données d'entrée et de sortie ;
- établir l'architecture du système ;
- faire une analyse fonctionnelle interne ;
- lister les modes de défaillance du système par une analyse AMDEC.

Cette méthode permet, dans un premier temps, de faire une modélisation fonctionnelle du système et de clarifier ses besoins c'est-à-dire déterminer les fonctions principales liées à ce système. Elle permet, ensuite, de faire une analyse des défaillances afin d'apporter les améliorations nécessaires à la modélisation initiale.

A.5 Functional Analysis System Technique (FAST)

La méthode FAST, introduite par l'américain Charles W. Bithenay, complète la boîte à outils d'analyse fonctionnelle. C'est une méthode qui permet de relier les diverses solutions techniques qui pourraient convenir pour répondre aux besoins. Elle présente l'avantage d'ordonner les fonctions suivant un ordre logique, de contribuer à la clarification de l'état fonctionnel d'un système et de rédiger un CdCF plus détaillé [107, 17, 93].

A partir des fonctions précédemment définies, nous pouvons identifier les fonctions qui s'appliquent à l'ensemble du produit et ainsi les répertorier en marge du diagramme. Les fonctions dites générales peuvent ne pas figurer sur ce diagramme afin d'éviter de l'encombrer.

Les fonctions sont notées chacune sur des cartes indépendantes. Ces cartes seront disposées les unes à côté des des autres dans un ordre qui sera déterminé par les réponses

aux trois questions :

1. Pourquoi ?
2. Comment ?
3. Quand ?

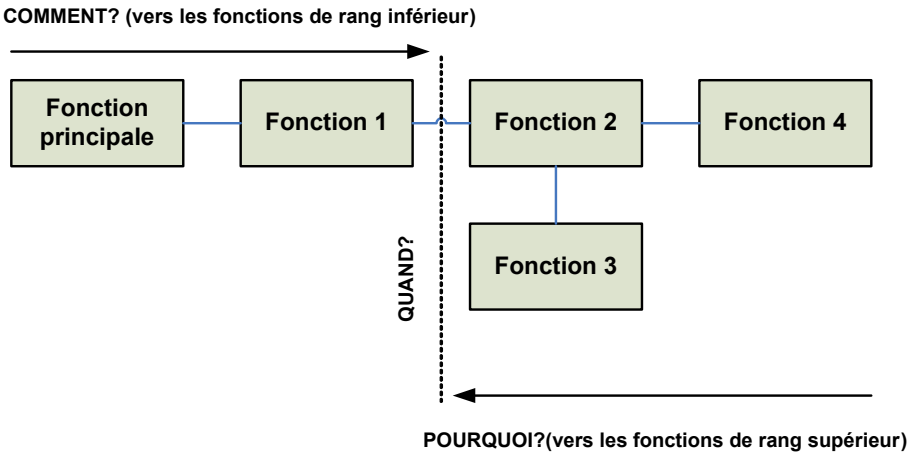

FIGURE A.2 – Principe de la méthode FAST

Le diagramme FAST est tracé de gauche à droite selon deux axes de questionnement : l'axe orienté de la gauche vers la droite du *Comment ?* et l'axe inverse du *Pourquoi ?* On place à gauche la fonction principale qui est la réponse à la question *Comment ?* permettant de déduire les fonctions qui la réalisent.

Les fonctions justifiant une réponse à la question *Pourquoi ?* sont dites de rang supérieur. La chaîne du *Comment ?*, qui relie les fonctions de rang inférieur, montre le *chemin critique*. La réponse à la question *Quand ?* détermine les fonctions qui doivent être satisfaites simultanément (figure A.2).

Le diagramme de la figure A.3 comporte à gauche et à droite deux droites verticales. Ces deux lignes marquent la limite de certitude. En d'autre termes, cela représente la zone où sont comprises les fonctions propres du système.

La fonction principale de ce système consiste à améliorer l'aspect de la pelouse. Cette fonction dépend de la façon dont la tondeuse est utilisée. C'est l'utilisateur qui choisit les endroits et les réglages de coupe, non la tondeuse.

l'utilisateur et la source de courant représentent les éléments extérieurs. La tondeuse conserve sa capacité mais la présence de ces deux éléments extérieurs est nécessaire pour tondre le gazon.

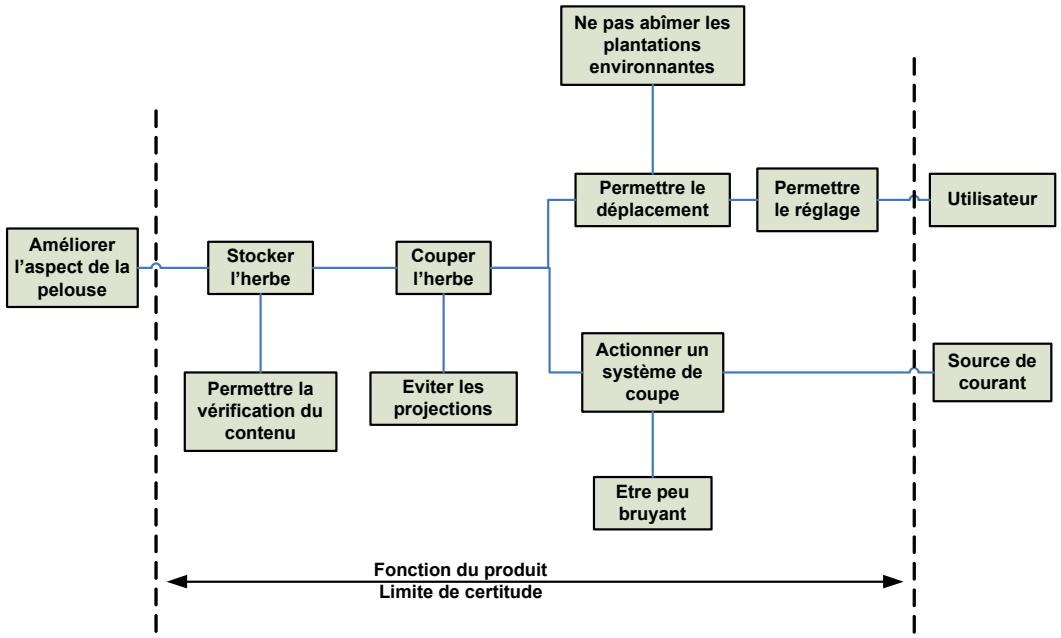

FIGURE A.3 – FAST pour une tondeuse à gazon électrique

A.6 Unified Modeling Language (UML) et System Modeling Language (SysML)

UML est définie comme un langage de modélisation graphique et textuelle destiné à la conception de systèmes logiciels. La version 1.0 d'UML est publiée et adoptée par l'OMG (l'Object Management Group) en novembre 1997 [45, 26, 66]. Son application exige l'adoption d'une méthodologie claire et l'utilisation d'un bon outil logiciel mettant en oeuvre ce langage. Malgré cette volonté d'unification, UML n'est pas une solution totale pour la conception système, car elle n'établit pas la façon dont les diagrammes doivent être employés et moins encore un principe d'intégration ou d'interopérabilité entre eux. L'utilisation de ce langage perd beaucoup d'efficacité sans une méthodologie et sans le support d'un outil.

Ce langage est composé de diagrammes qui sont des représentations graphiques permettant à l'utilisateur de visualiser et de manipuler des éléments de modélisation. Il définit quatre diagrammes structurels et cinq comportementaux pour représenter, respectivement, des vues statiques et dynamiques d'un système [78]. L'UML s'articule autour de 13 diagrammes différents dont 4 nouveaux diagrammes induits par UML 2.0 qui est une nouvelle version introduite en 2005. Cette nouvelle version propose des modifications afin d'améliorer l'organisation générale du langage, de simplifier la syntaxe et de fournir des éléments plus adaptés pour la modélisation comportementale des systèmes.

Hormis l'approche objet, l'avantage majeur du langage UML est la multiplicité de diagrammes qu'il offre. Il permet au concepteur de créer différentes représentations du fonctionnement du système. Néanmoins, il pêche par sa complexité sémantique et son manque d'interopérabilité entre les diagrammes.

La conception orientée objet intéresse de plus en plus les ingénieurs système en particulier le langage UML grâce à la place qu'il a conquise dans le monde du logiciel. SysML a ainsi vu le jour en tant qu'extension du langage UML pour couvrir toutes les étapes de conception de systèmes complexes. Elle a été conçue de manière à être abordable contrairement à UML pour ne pas constituer un frein à son adoption dans le monde d'ingénierie système [45, 99]. Ce langage SysML rajoute des diagrammes à UML et en modifie d'autres.

Annexe B

Méthodes d'analyse dysfonctionnelle

B.1 Analyse Préliminaire des Dangers/Risques

L'APD a été utilisée au début des années 60 aux États Unis pour l'analyse de sécurité de missiles. Elle est utilisée dans les premières phases de conception d'un système et constitue un premier outil d'identification des risques potentiels. Elle est mise en oeuvre avant une étude de sûreté de fonctionnement plus fine, telle qu'une Analyse des Modes de Défaillance et de leurs Effets [107, 102, 82]. Le principe de cette analyse consiste à rechercher les entités et les situations dangereuses ainsi que les accidents potentiels à partir de la connaissance et de l'expérience des spécialistes. Il est recommandé d'utiliser cette analyse dès les premières phases de la conception. Les résultats obtenus par cette analyse sont présentés dans le tableau B.1.

système	phase	entités dangereuses	événement la causant	situation dangereuse	événement le causant	accident potentiel	effet	gravité	mesures préventives	application des mesures

Table B.1 – Tableau de l'Analyse Préliminaire des Dangers

Par extension, l'APR complète l'APD par une estimation de la probabilité d'occurrence des situations dangereuses et des accidents potentiels ainsi que leurs effets et conséquences. Le but premier de cette analyse est de déterminer les moyens et les actions correctives permettant d'éliminer ou du moins de maîtriser les situations dangereuses et accidents potentiels mis en évidence.

Ces deux analyses sont souvent utilisées pour la phase d'identification des risques et sont orientées vers la sécurité.

B.2 Arbre de Défaillance(AdD)

La méthode des Arbres de Défaillance a été développée dans le début des années 60 au sein de la société Bell Telephone. Elle constitue une technique d'analyse de fiabilité déductive et est une représentation statique du système. Le point de départ de cette représentation est la considération de défaillances potentielles appelées événements sommets ou *Top Events*. Le but consiste à descendre progressivement des causes finales initiatrices d'un événement sommet jusqu'aux causes élémentaires. Chaque niveau d'événements est relié en cascade à l'aide de symboles correspondant à des opérateurs logiques (et, ou, si...) [102, 107, 82, 86].

A la base, ces arbres de défaillance ne renferment que des informations qualitatives. Cependant, ils peuvent être utilisés pour quantifier les probabilités des événements sommets en propageant les probabilités d'occurrence des événements de base vers le sommet des arbres [47].

Pour construire un Arbre de Défaillance, trois étapes sont nécessaires :

- recherche des causes immédiates, nécessaires et suffisantes de l'évènement sommet ;
- classement et analyse des évènements intermédiaires ;
- recherche des causes immédiates, nécessaires et suffisantes des évènements ; intermédiaires jusqu'à obtention de l'évènement de base.

L'objectif qualitatif consiste à construire une synthèse de tout ce qui peut conduire à un événement redouté et à évaluer l'effet d'une modification du système, de comparer les conséquences des mesures qui peuvent être envisagées pour réduire l'occurrence de l'événement redouté étudié [76]. Cependant, l'emploi de cette méthode se révèle difficile, voir impossible pour l'étude des systèmes fortement dépendants du temps.

B.3 Table de Vérité (TV)

Basée sur l'algèbre booléenne, la méthode de la Table de Vérité permet d'identifier tous les états (fonctionnements et pannes) du système à partir de comportements binaires.

Le principe de cette méthode consiste à décomposer le système et à recenser les modes de défaillances des différents composants, ainsi que leurs états de panne. Chaque composant est caractérisé par un état de fonctionnement (1) ou par un état de panne (0). Établir la Table de Vérité d'un système consiste à analyser les effets de tous les vecteurs des états des composants et à déterminer tous les mauvais fonctionnements du système. A partir de cette table, il est facile de déduire les combinaisons de défaillance et les pannes conduisant à un événement indésirable [102].

Cette méthode est limitée à des systèmes simples avec un nombre faible de composants. Néanmoins, on peut utiliser cette méthode après décomposition du système à un niveau où le nombre de combinaisons de défaillance reste acceptable.

B.4 Méthode des Combinaisons de Pannes Résumées (MCPR)

La méthodes des Combinaisons de Pannes Résumées a été créée pour l'analyse de sécurité des avions Concorde et Airbus [107]. Elle permet de mettre en évidence les combinaisons de défaillance conduisant à des événements indésirables ainsi que de regrouper les pannes ayant les mêmes effets et de tenir compte des systèmes élémentaires.

Cette méthode se divise en quatre principales étapes :

1. décomposition du système global en sous-système ;
2. élaboration des pannes résumées internes ;
3. élaboration des pannes résumées externes ;
4. élaboration des pannes résumées globales.

La méthode MCPR complète une analyse AMDE et regroupe les pannes ayant les mêmes effets et tient compte des interactions entre les différents sous-systèmes. A partir de cette méthode, il est facile de construire un Arbre des Causes dans le but d'aborder l'aspect quantitatif manquant à cette méthode [107].

B.5 Méthode du Diagramme Causes-Conséquences (MDCC)

La méthode MDCC a été développée par le laboratoire Riso au Danemark dans les années 70. Comme son nom l'indique, cette méthode comporte deux grandes parties : une partie *Cause* et une partie *Conséquence* [102, 107].
La partie *Cause* consiste à utiliser les principes de la Méthode de l'Arbre des Causes (MAC) et permet de représenter les causes d'un événement sommet conduisant à des conséquences indésirables.

La partie *conséquence* basée sur les principes de la Méthode des Arbres de Conséquences (MACQ) permet de déterminer les conséquences que peut subir un système lorsque les événements sommets se réalisent.

La méthode MDCC suit, simultanément, les principes de la méthode MAC et de la méthode MACQ.

La Méthode de l'Arbre des Causes (MAC), développée dans les années 60, est une représentation statique du système et consiste à considérer une défaillance donnée du système et à construire l'ensemble des combinaisons de défaillances des composants.

L'événement indésirable est placé au sommet de l'arbre et l'analyse a pour but de déterminer toutes les causes liées à cet événement.

Cette méthode à pour objectifs la détermination des différentes combinaisons possibles entraînant l'événement redouté ainsi que la représentation graphique arborescente de ces combinaisons.

La Méthode de l'Arbre des Conséquences (MACQ), utilisée dans les années 70 aux États-Unis, est une méthode inductive permettant d'élaborer et d'évaluer des séquences d'événements [102]. Elle est généralement employée en liaison avec la méthode MAC décrite précédemment.

B.6 Diagramme de Succès (MDS)

Historiquement, la méthode MDS est la plus ancienne qui a été utilisée pour analyser des systèmes et permettre des calculs de fiabilité. Cette méthode est proche de la structure physique du système et consiste à construire un diagramme composé de blocs. Chacun d'eux représentant une entité (composant, sous-système...) reliés par des lignes orientés indiquant les dépendances des entités entre elles. Ce diagramme conduit à une modélisation du fonctionnement du système et nous permet de calculer la fiabilité ou la disponibilité du système supposé irréparable [102, 107].

Annexe C

Méthodes de modélisation

C.1 Réseaux Bayésiens

Les réseaux Bayésiens possèdent un fort potentiel puisqu'ils sont capables de combiner l'aspect statistique, probabiliste, avec des aspects décisionnels, et des aspects de gestion de connaissances.

Le formalisme des réseaux Bayésiens a débuté il y a 20 ans environ grâce notamment aux travaux de Pearl.

Un réseau bayésien peut se définir comme un modèle graphique probabiliste. Il porte également d'autres appellations comme réseaux probabilistes ou réseaux de croyances. C'est un outil complet permettant la visualisation de variables et de leurs dépendances (ou indépendances). Il permet également de décrire quantitativement le fonctionnement d'un système grâce aux différents calculs de probabilité concernant les variables du système. Généralement, on modélise les variables aléatoires comme étant des nœuds. On peut alors dresser un arc entre certaines variables du système. Les arcs tracés peuvent rendre compte d'un phénomène de causalité entre les variables reliées (réseaux causaux), mais ce n'est pas obligatoirement le cas [100].

Le fait d'indiquer un arc entre deux variables implique une dépendance directe entre ces deux variables : l'une est le parent, et l'autre l'enfant. Il faut fournir le comportement de la variable enfant au vu du comportement de son ou ses parents. Pour cela, chaque nœud du réseau possède une table de probabilités conditionnelles. Une table de probabilités conditionnelles associée à un nœud permet de quantifier l'effet du ou des nœuds parents sur ce nœud : elle décrit les probabilités associées aux nœuds enfants suivant les différentes valeurs des nœuds parents. Pour les nœuds racines (sans parents), la table de probabilité n'est plus conditionnelle et fixe alors des probabilités a priori concernant les valeurs de la variable.

Les réseaux bayésiens interdisent les dépendances enfants vers les parents. Ainsi, l'ensemble de variables et des arcs vont former un graphe dirigé et acyclique.

Un réseau bayésien est défini par [79] :

- Un graphe acyclique orienté G, $G = (V, E)$, où V est l'ensemble des nœuds de G, et E l'ensemble des arcs de G,
- un espace probabilisé fini (Ω, Z, p), avec Ω un ensemble fini non-vide, Z un ensemble de sous-espace de Ω, et p une mesure de probabilité sur Z avec $p(\Omega) = 1$,
- un ensemble de variables aléatoires associées aux nœuds du graphe et définies sur (Ω, Z, p), tel que :

$$p\left(V_1, V_2, ..., \mathrm{V_n}\right) = \prod_{i=1}^{n} p\left(V_i | C\left(V_i\right)\right) \tag{C.1}$$

où $C(V_i)$ est l'ensemble des parents (causes) de V_i dans le graphe G.

C.2 Réseaux de Neurones

Les premiers travaux sur les Réseaux de Neurones artificiels ont commencé au début des années 40 et ont été mené par McCulloch et Pitts. Dix années plus tard, le premier modèle réel d'un réseau de neurones a été constitué.

Le Neurone biologique est une cellule vivante spécialisée dans le traitement de signaux électriques. Les neurones sont reliés entre eux par des liaisons appelées axones [83]. Un réseau de neurones est un automate mathématique qui réalise une interpolation non linéaire dans un espace à plusieurs dimensions. Les neurones font une sommation des signaux reçus en entrée et en fonction du résultat obtenu vont fournir un courant de sortie.

Un schéma d'un neurone est représenté sur la figure C.1. Cette représentation est le reflet de l'inspiration biologique qui a été à l'origine de la première vague d'intérêt pour les neurones formels, dans les années 1940 à 1970 [34].

Le neurone artificiel est un processus élémentaire. Il reçoit un nombre variable d'entrée en provenance de neurones situés en amont. A chacune de ses entrées $(x_1, x_2, x_3 ... x_n)$ est associé des poids $(w_1, w_2, w_3 ... w_n)$ représentatif de la force de connexion. Chaque processus élémentaire (neurone) est doté d'une sortie unique.

Un neurone reçoit une information de la part de n entrées $(x_1, x_2, x_3 ... x_n)$. Chaque entrée est pondérée par un poids propre w_i que l'on nomme poids synaptique (en référence aux synapses des neurones naturel) [100]. Conformément à l'usage (également inspiré par la biologie), cette combinaison linéaire sera appelée *Potentiel*. Le potentiel v le plus

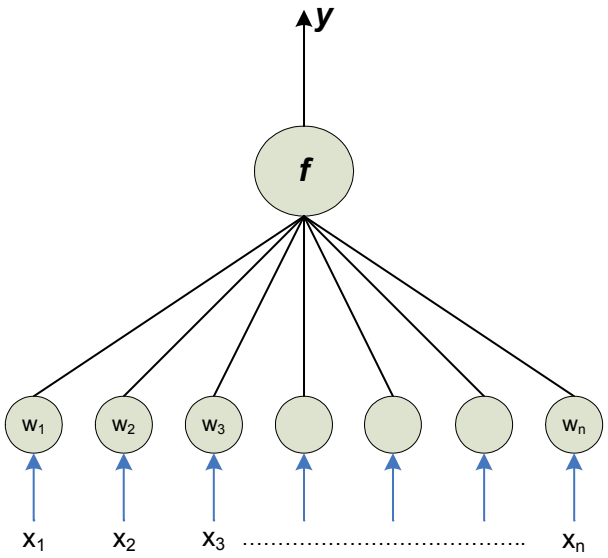

FIGURE C.1 – Un neurone artificiel réalise une fonction non linéaire f

fréquemment utilisé est la somme pondérée, à laquelle s'ajoute un terme constant :

$$v = w_0 + \sum_{i=1}^{n-1} w_i x_i \tag{C.2}$$

La sortie d'un neurone peut s'écrire de la manière suivante :

$$y = f\left[w_0 + \sum_{i=1}^{n-1} w_i x_i\right] \tag{C.3}$$

Un neurone permet de modéliser une quantité considérable de comportements suivant les poids synaptiques w_i qu'il possède mais également suivant la fonction d'activation f qu'il renferme. Différentes fonctions d'activation peuvent être utilisées mais les principales sont représentées sur la figure C.2.

Il est recommandé d'utiliser une fonction d'activation sigmoïde (c'est-à-dire une fonction en forme de S) symétrique par rapport à l'origine telle que la tangente hyperbolique ou la fonction arctangente.

Le premier réseau de neurone est le Perceptron. Ce réseau est un discriminateur linéaire. Cette linéarité a freiné considérablement le développement des réseaux de neurones pendant de nombreuses années [100].

Un des réseaux le plus utilisé est le Perceptron MultiCouches (PMC). Un perceptron multicouche est un réseau subdivisé en couche de neurones : la sortie d'un neurone d'une couche n'est liée qu'aux neurones de la couche suivante. Il n'y a donc aucune liaison entre

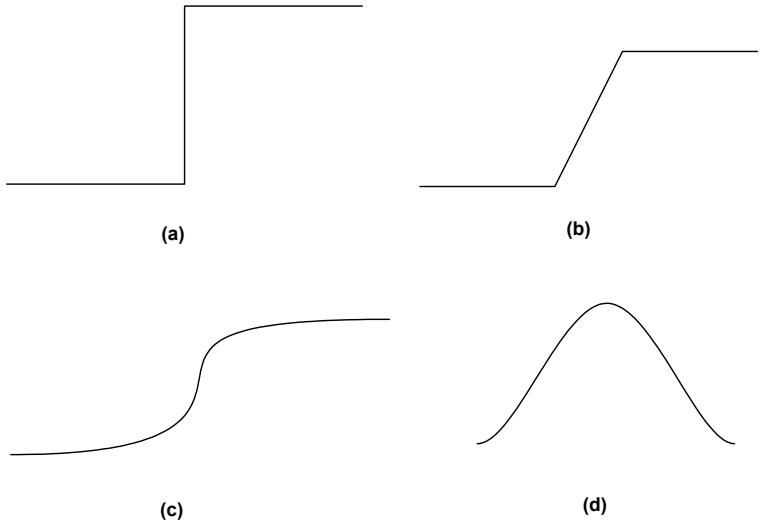

FIGURE C.2 – Les différentes fonctions d'activation f : (a) fonction à seuil, (b) fonction linéaire, (c) fonction sigmoïde, (d) fonction gaussienne

les neurones d'une même couche [100, 34].

La première couche est généralement appelée couche d'entrée et la dernière couche, couche de sortie. Entre ces deux couches se situe alors une ou plusieurs couches de neurones nommées couches cachées.

Un exemple de perceptron multicouche à quatre entrées, une sortie et une couche cachée est présenté sur la figure C.3.

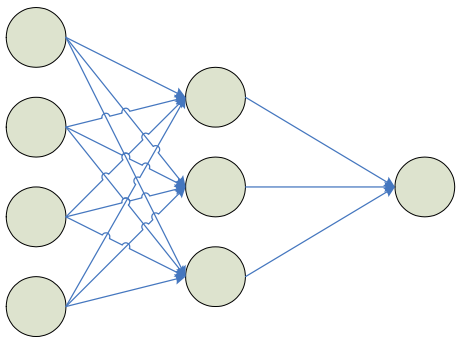

FIGURE C.3 – Perceptron multicouches classique

Bien que le nombre de neurones de la couche d'entrée soit imposé par le nombre d'entrées du système et le nombre de neurones de la couche de sortie par la codification des différentes classes, aucune règle mathématique au sens strict ne permet de déterminer, pour un problème donné, le nombre de couches cachées ainsi que le nombre de neurones de chacune de ces couches.

Annexe D

Autres lois de probabilité

D.1 Loi Gamma

Elle représente la loi de probabilité d'occurrence de a événements dans un processus poissonien. Par exemple si t_i est le temps entre les défaillances successives d'un système, et que t_i suit une distribution exponentielle, le temps cumulé d'apparition de a défaillances suit une loi Gamma :

La densité de probabilité

$$f(t) = \frac{t^{a-1}e^{-\frac{t}{b}}}{b^a \Gamma(a)} \tag{D.1}$$

Le taux de défaillance

$$\lambda(t) = \frac{t^{a-1}e^{-\frac{t}{b}}}{b^a \int_t^\infty \Gamma(a) f(u)\, du} \tag{D.2}$$

D.2 Loi Bêta

Cette loi représente, en particulier, la probabilité pour qu'un matériel survive jusqu'à un instant t, quand on essaie n matériels. D'où son intérêt dans l'évaluation de la durée des essais de fiabilité. La loi Bêta a deux paramètres a et b :

La densité de probabilité

$$f(t) = \frac{\Gamma(a+b)}{\Gamma(a) \cdot \Gamma(b)} t^{a-1} (1-t)^{b-1} \tag{D.3}$$

D.3 Loi uniforme

La loi uniforme est souvent utilisée en fiabilité pour les essais bayésiens en l'absence de connaissances pour construire l'information a priori. Cette loi peut prendre toute valeur dans un intervalle *(a,b)* avec une densité de probabilité constante.

La fonction de répartition

$$F(t) = \frac{t-a}{b-a} \tag{D.4}$$

La densité de probabilité

$$f(t) = \frac{1}{b-a} \tag{D.5}$$

Annexe E

Autres méthodes d'évaluation de la fiabilité dynamique

E.1 Méthodes analytiques et semi - analytiques

Dans le cas des méthodes analytiques, la généralisation des équations de Chapman - Kolmogorov conduit à un système mathématique de très grande taille puisque la densité de probabilité dépend, dans chaque état, d'un grand nombre de variables (les variables physiques et le temps). La résolution analytique de ce système n'est possible qu'au niveau de cas-tests. En ce qui concerne les méthodes semi-analytiques, le but est de résoudre le système d'équation de Chapman - Kolmogorov à l'aide d'une technique numérique classique, mais comme pour les méthodes analytiques, on sera confronté à un problème de taille.

E.2 Arbres dynamiques discrets

La discrétisation du temps d'un arbre d'événements continus pour obtenir un arbre d'événements dynamique discret a été l'outil le plus développé pour faire face aux problèmes de fiabilité dynamique. Il s'agit d'une méthode de simulation qui modélise explicitement l'évolution des variables physiques tout en tenant compte des éventuelles modifications de l'état du hardware et du comportement humain si nécessaire. Dans l'évolution du système, tous les branchements possibles qui suivent un événement initiateur sont pris en compte. La restriction de base des arbres d'événements dynamiques discrets par rapport aux arbres d'évènements continus est la suivante : les branchements peuvent seulement avoir lieu à des intervalles de temps discrets. Cependant, en cet instant, tous les change-

ments possibles de comportement sont pris en compte pour générer de nouvelles branches. Tout d'abord cet intervalle de temps était directement déterminé par l'utilisateur. Ensuite un critère probabiliste a été introduit : dès que la probabilité conditionnelle de rester sur la branche courante depuis le dernier point de branchement descend sous un seuil donné, un nouveau point de branchement est défini. Cette approche a été la plus largement utilisée pour le traitement d'applications réalistes. Cependant, comme son nom générique le suggère, elle se prête plus spécifiquement aux études probabilistes de sûreté.

Annexe F

Processus stochastique scalaire

Un processus stochastique, ou processus aléatoire, est un modèle mathématique d'évolution dont la dépendance envers le temps et/ou l'espace est gouvernée par des lois de probabilités. Dans toute la suite, seule la dépendance envers le temps t est considérée. La notation retenue ici pour un processus stochastique scalaire est :

$$S\left(t,\omega\right),t\in T,\omega\in\Omega \tag{F.1}$$

- Pour t fixé, *S(t=t1,ω)* est une fonction sur l'espace de probabilité Ω et, est ainsi, une variable aléatoire que nous notons $\mathrm{S}_{t1}(\omega)$;
- Pour ω fixé, *S(t,ω=ω1)* définit une fonction de t et est une réalisation, une fonction d'échantillonnage ou encore une trajectoire du processus stochastique que nous notons *S(t)*.

On note $m_s(t) = E[S(t,\omega)]$ la moyenne du processus *S(t,ω)* et $\sigma_s(t)$ son écart-type. Soit $R_{ss}(t_1,t_2)$, la fonction d'autocorrélation du processus *S(t,ω)*. Elle est définie par :

$$R_{ss}\left(t_1,t_2\right)=E\left[S\left(t_1,\omega\right)S\left(t_2,\omega\right)\right] \tag{F.2}$$

L'opérateur E[.] désigne l'opération d'espérance mathématique.

La fonction de covariance normalisée, également appelée coefficient de corrélation $\rho_{ss}(\mathrm{t}_1,\mathrm{t}_2)$ du processus *S(t,ω)*, de moyenne $m_s(t)$ et d'écart-type $\sigma_s(t)$, est définie par :

$$\rho_{ss}\left(t_1,t_2\right)=\frac{R_{ss}\left(t_1,t_2\right)-m_s\left(t_1\right)m_s\left(t_2\right)}{\sigma_S\left(t_1\right)\sigma_S\left(t_2\right)} \tag{F.3}$$

Annexe G

Formule de Rice

La première expression permettant le calcul du taux de franchissements a été proposée par Rice en 1944. Elle est basée sur l'hypothèse selon laquelle le processus *S(t,ω)* est scalaire, différentiable et que les trajectoires sont continument différentiables. Elle a été généralisée aux processus vectoriels par Belayev [3].

La relation donnée par Rice est basée sur le dépassement d'un seuil par le processus considéré. Soit :

- *z(t)* une fonction de niveau, déterministe ;
- $f_{S\dot{S}}(u,v)$ la distribution de probabilité conjointe des valeurs des processus $S(t,\omega)$ et $\dot{S}(t,\omega)$

Dans le cas scalaire, le taux de franchissement ν^+ peut être déterminé grâce à la formule de Rice :

$$\nu^+(t) = \int_{\dot{z}(t)}^{\infty} (\dot{s} - \dot{z}(t))\, f_{S\dot{S}}(z(t), \dot{s})\, d\dot{s} \tag{G.1}$$

Dans le cas vectoriel, le calcul se fait avec la formule de Belayev qui est une généralisation de celle de Rice

$$\nu^+(t) = \int_{\partial D_f} E\left[n^t(s)\, \dot{S}(t,\omega)\, |S(t,\omega) = s\right] f_{S(t,\omega)}(S)\, dS \tag{G.2}$$

Bibliographie

[1] AFIS. Ingénierie système. pourquoi ? comment ? 2005.

[2] C. Andrieu, A. Rachad, J-C. Mitteau, and M. Lemaire. Evaluation de la fiabilité d'une structure au cours de sa dégradation dans le temps. *Fiabilité : conception, maintenance*, pages 469–477, 2002.

[3] C. Andrieu-Renaud. *Fiabilité mécanique des structures soumises à des phénomènes physiques dépendant du temps*. PhD thesis, Université Blaise Pascal, 2002.

[4] C. Andrieu-Renaud, M. Lemaire, and B. Sudret. La méthode phi2 ou comment prendre en compte la dépendance du temps dans une analyse en fiabilité mécanique. *Colloque National en Calcul des structures*, 2003.

[5] C. Andrieu-Renaud, B. Sudret, and M. Lemaire. The phi2 method : a way to compute time-variant reliability. *Reliability Engineering and System Safety*, 84 :75–86, 2004.

[6] S. Anwar and B. Ashrafi. A predictive control algorithm for an anti-lock braking system. *SAE International*, 2002.

[7] Doug Bays and Vikrant Shah. Effectiveness of anti-lock braking system in automobiles. 2003.

[8] A. Benoit, B. Plaateau, and W.J. Stewart. Réseaux d'automates stochastiques à temps discret. *RSTI-TSI*, 24 :229–248, 2005.

[9] J. Beretta. *Electronique, électricité et mécatronique automobile*. Lavoisier, 2008.

[10] B. Bretesche. *La méthode APTE, Analyse de la Valeur, Analyse Fonctionnelle*. Petrelle edition, 2000.

[11] L. Burgazzi. About time-variant reliability analysis reference to passive systems assessement. *Reliability Engineering and System Safety*, 93 :1682–1688, 2008.

[12] A. Cabarbaye and R. Laulheret. Evaluation de la sûreté de fonctionnement des systèmes dynamiques par modélisation récursive. *QUALITA*, 2005.

[13] J.J. Carré. Technologie du freinage : Freins à disque. *Techniques de l'ingénieur*, 1993.

[14] G. A. Perez Castaneda, J. F. Aubry, and N. Brinzei. Etat de l'art en fiabilité dynamique. *JDMACS*, 2007.

[15] G.A. Perez Castaneda, J.F. Aubry, and N. Brinzei. Automate stochastique appliqué à l'évaluation de la fiabilité dynamique. *MOSIM'08*, 2008.

[16] G.A Perez Castaneda, J.F. Aubry, and N. Brinzei. Simulation de monte carlo par automate stochastique hybride, application à un cas test pour la fiabilité dynamique. *QUALITA*, 2009.

[17] C. Cazaubon, G. Gramacia, and G. Massard. *Management de projet technique - Méthodes et outils.* ellipses, 1997.

[18] M. Cazuguel, M. Mejri, and J.Y. Cognard. Une approche fiabiliste fonction du temps appliquée au vieillissement des structures navales à comportement non-linéaire. *Journées Fiabilité des Matériaux et des Structures*, 2008.

[19] J.L. Chabot. *Approche probabiliste relative à l'étude des scénarios d'incendie.* PhD thesis, Université de Poitiers - ENSMA, 1998.

[20] L.W. Chan and T.P. Leung. Spiral design model for consumer mechatronic products. *Mechatronics*, 6 :35–51, 1996.

[21] P. Charpenel, R. Digout, M. Giraudeau, M. Glade, JP. Guerveno, N. Guillet, A. Lauriac, S. Male, D. Manteigas, R. Meister, E. Moreau, D. Perie, F. Relmy-Madinska, and P. Retailleau. Fides, la nouvelle méthodologie pour la prévision de fiabilité des systèmes électroniques. *Lambda Mu*, 14 :332–337, 2004.

[22] H. Christofol. *Modélisation systémique du processus de conception de la coloration d'un produit.* PhD thesis, ENSAM Paris, 1995.

[23] C. Cocozza-Thivent and R. Eymard. Algorithme de fiabilité dynamique. *Lambda Mu*, 16, 2006.

[24] F. Cottet and E. Grolleau. *Système Temps Réel de Contrôle-Commande. Conception et implémentation.* Dunod, 2005.

[25] R. David and H. Alla. *Du Grafcet aux réseaux de Petri.* Hermes, 1997.

[26] L. Debrauwer and F. Van-Der-Heyde. *UML2 Initiation, exemples et exercices corrigés.* ENI, eni edition, Janvier 2005.

[27] A. Demri, A. Charki, F. Guérin, M. Barreau, and H. Christofol. Fiabilisation d'un système mécatronique dès la phase de conception. *CFM*, 2007.

[28] A. Demri, A. Charki, F. Guérin, and H. Christofol. Analyses fonctionnelle et dysfonctionnelle d'un système mécatronique. *Qualita*, mars 2007.

[29] A. Demri, A. Charki, F. Guérin, and H. Christofol. Functional and dysfunctional analysis of a mechatronic system. *RAMS*, 2008.

[30] A. Demri, A. Charki, F. Guérin, and H. Christofol. Modélisation d'un système complexe grâce aux réseau de petri et à l'intégration de la méthode phi2. *CFM*, 2009.

[31] A. Demri, A. Charki, F. Guérin, P. Khan, and H. Christofol. Analyse qualitative et quantitative d'un système mécatronique. *CPI*, 2007.

[32] A. Desroches. *Concepts et méthodes probabilistes de base de la sécurité.* Lavoisier, tec&doc edition, mai 1995.

[33] G. Donnnadieu, D. Durand, D. Neel, E. Nunez, and L. Saint-Paul. L'approche systémique : de quoi s'agit-il ? 2003.

[34] G. Dreyfus, J-M. Martinez, M. Samuelides, M. B. Gordon, S. Thiria, and L. Hérault. *Réseaux de neurones : Méthodologie et applications.* Eyrolles, 2002.

[35] F. Dufour and Y. Dutuit. Dynamic reliability : A new model, fiabilité dynamique : Un nouveau modèle. *Lambda Mu*, 13 :350–353, 2002.

[36] B. Ewers, J. Bordeneuve-Guibé, and C. Langlois. A symbolic sensor for an antilock braking system of a commercial aircraft. In *Proceeding of the 5th IEEE Mediterranean Conference on Control and Systems*, Août 1997.

[37] FIDES. *Méthodologie de fiabilité pour les systèmes électroniques.* 2004.

[38] J-P. Fournier. *Fiabilité du logiciel. Concepts, modélisaions, perspectives.* Hermes, 1993.

[39] H. Garin. *AMDEC, AMDE, AEEL L'essentiel de la méthode.* 1994.

[40] R. Gautier. *Qualité en conception de produits nouveaux "Proposition d'une méthode de fiabilisation du processus de management de l'information".* PhD thesis, Ecole Nationale Supérieure d'Arts et Métiers, Paris, 1995.

[41] C. Girault and R. Valk. *Petri Nets for Systems Engineering. A guide to modelling verification and application.* Springer, springer edition, 2003.

[42] F. Guérin, M. Barreau, A. Charki, and A. Todoskoff. Bayesian estimation of failure probability in mechanical systems using monte carlo simulation. *Quality Technology & Quantitative Management QTQM*, 4 :51–70, 2007.

[43] F. Guérin, B. Dumon, and R. Hambli. correspondeance between the weibull distribution and the failure modes. *ICCOSAR*, 2001.

[44] K. Hamidi. *Contribution à un modèle d'évaluation quantitative des performances fiabilistes de fonctions électroniques et programmables dédiées à la sécurité.* PhD thesis, Institut National Polytechnique de Lorraine, 2005.

[45] J-C. Hamon. *Méthodes et outils de la conception amont pour les systèmes et les microsystèmes.* PhD thesis, Institut National Polytechnique de Toulouse, 2005.

[46] M. Haoues, K.N. Mouss, and L.H. Mouss. L'utilisation conjointe des réseaux de petri stochastiques et des processus de markov pour l'évaluation des performances d'une ligne d'emboutissage. *CPI*, 2007.

[47] A. Hähnel, M. Lemaire, and F. Rieuneau. Une approche pour l'étude physique et probabiliste de la défaillance de systèmes mécaniques. *CFM*, 2005.

[48] R. Isermann. Mechatronic systems - innovative products with embedded control. *Control Engineering Practice*, 16 :14–29, 2008.

[49] P. Jaulent. *Génie logiciel les méthodes SADT, SA, E-A, SA-RT, SYS-P-O, OOD, HOOD...* Armand Colin, 1992.

[50] O. Kaynak. Recent advances in mechatronics. *Robotics and Autonomous Systems*, 19 :113–116, 1996.

[51] R. Keshmiri and A. M. Shahri. Intelligent abs fuzzy controller for diverse road surfaces. *Waset*, 23 :292–297, 2007.

[52] S. Khalfaoui. *Méthode de recherche des scénarios redoutés pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile.* PhD thesis, Institut National Polytechnique, Toulouse, 2003.

[53] S. Khalfaoui, E. Guilhem, H. Demmou, and R. Valette. Une méthodologie pour obtenir des scénarios critiques dans les systèmes mécatroniques. *Lambda Mu*, 13, 2002.

[54] R. Kouta and D. Play. Durée de vie d'un système mécanique. analyse de chargements aléatoires. *Technique de l'ingénieur*, BM5030, 2007.

[55] K. Labadi, H. Chen, and L. Amodeo. Nouvelles propriétés comportementales pour les réseaux de petri lots déterministes et stochastiques. *MejecStic*, 2 :13–15, 2004.

[56] J. Lacombe. Tire model for simulations of vehicle motion on high and low friction road surfaces. *Winter Simulation Conference*, pages 1025–1034, 2000.

[57] P. Ladet. Réseaux de pétri. *Techniques de l'ingénieur*, page 17, avril 1989. R 7252.

[58] J.C. Lapris, J. Arlat, J-P. Blanquart, A. Costes ans Y. Crouzet, Y. Deswarte, J-C. Fabre, H. Guillermain, M. Kaâniche, K. Kanoun, C. Mazet, D. Powell, and C. Rabéjac ans P. Thévenod. *Guide de la sûreté de fonctionnement.* 1995.

[59] M. Lemaire, A. Chateauneuf, and J.C. Mitteau. *Fiabilité des structures. Couplage mécano-fiabiliste statique.* Hermes, 2005.

[60] C.T. Leondes. *Mechatronic Systems Techniques and Application : Diagnostic, Reliability and Control System Techniques*, volume 5. Gordon and Breach Science, 2000.

[61] C.T. Leondes. *Mechatronic Systems Techniques and Application. Transportation and Vehicular Systems*, volume 2. Gordon and Breach Science, 2000.

[62] E. Ligan. "variable mass braking system" un nouveau système de freinage de véhicule automobile. *Mechanics Research Communications*, 31 :75–80, 2004.

[63] C.Y. Lu and M.C Shih. Application of the pacejka magic formula tyre model on a study of a hydraulic anti-lock braking system for a light motorcycle. *Vehicle System Dynamics*, 41 :431–448, 2004.

[64] R. Lupan, A. Kobi, C. Roblédo, A. Delamarre, and H. Christofol. Modélisation et évaluation de la performance en conception. *6ème Conférence Francophone de MOdélisation et SIMulation - MOSOM'06*, 2006.

[65] P. Lyonnet. *Ingénierie de la fiabilité.* Lavoisier, tec&doc edition, mars 2006.

[66] R. Maurice. *Contribution à la méthodologie de conception système : Application à la réalisation d'un microsystème multicapteurs communicant pour le génie civil.* PhD thesis, Institut National Polytechniques de Toulouse, 2005.

[67] M. Medjoudj. *Contribution à l'analyse des systèmes pilotés par calculateurs : Extraction de scénarios redoutés et vérification de contraintes temporelles.* PhD thesis, Université Paul Sabatier de Toulouse, 2006.

[68] R.E. Melchers. *Structural Reliability Analysis and Prediction.* Wiley, 1999.

[69] A. Mihalache. *Modélisation et évaluation de la fiabilité des systèmes mécatroniques : Application sur systèmes embarqué.* PhD thesis, ISTIA - Université d'Angers, 2007.

[70] MIL-HDBK-338B. *MIL-HDBK-338B. Military handbook electronic reliability design handbook.* 1998.

[71] H. Mèmeteau. *Technologie fonctionnelle de l'automobile. Transmission, train roulant et équipement électrique.* Dunod, 2006.

[72] S. Moammadkhani-Shali. *Contribution de l'étude de redondance dans les ponts : analyses des mecanismes de défaillance par surfaces de réponse.* PhD thesis, Ecole nationale des ponts et chaussées, 2007.

[73] G. Moncelet. *Application des Réseaux de Pétri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile.* Automatique et informatique industriels, Université Paul Sabatier de Toulouse, octobre 1998.

[74] G. Moncelet, S. Chirstensen, H. Demmou, M. Paludetto, and J. Porras. Analysing a mechatronic system with coloured petri nets. 1998.

[75] Y. Mortureux. La sûreté de fonctionnement : méthodes pour maîtriser les risques. *Techniques de l'ingénieur*, octobre 2001.

[76] Y. Mortureux. Arbres de défaillance, des causes et d'événement. *Techniques de l'Ingénieur*, 2002.

[77] Y. Mortureux. Amde(c). *Techniques de l'Ingénieur*, 2005.

[78] P.A. Muller and N. Gaertner. *Modélisation objet avec UML.* Eyrolles, 2000.

[79] P. Naïm, P.H. Wuillemin, P. Leray, O. Pourret, and A. Becker. *Réseaux Bayésiens.* 7090. Eyrolles edition, mai 2004.

[80] H.B. Pacejcka and E. Bakker. The magic formula tyre model. *Colloquium on Tire Models for Vehicle Dynamics Analysis*, 1991.

[81] F. Parrennes. *Analyse de la sûreté du logiciel par interprétation abstraite et contraintes.* PhD thesis, Université de Paris VI, 2002.

[82] L. Peyras. *Diagnostic et analyse de risque liés au vieillissement des barrages, développement de méthodes d'aide à l'expertise.* PhD thesis, Blaise Pascal, Cleremont-Ferrand, 2002.

[83] S. Piechowiak. Intelligence artificielle et diagnostic. *Technique de l'ingénieur*, page 20, decembre 2003.

[84] H. Procaccia and P. Morilhat. *Fiabilité des structures des installations industrielles. Théorie et Applications de la mécaniques probabiliste.* Eyrolles, 1996.

[85] N. Sadou. *Aide à la conception des systèmes embarqués sûrs de fonctionnement.* PhD thesis, Université Toulouse III - Paul Sabatier, 2007.

[86] I. Barragan Santiago. *Elaboration de propriétés formelles de contrôleurs logiques à partir d'analyse prévisionnelle par Arbre des Défaillances.* PhD thesis, Ecole Normale Supérieure de Cachan, 2007.

[87] R. Schoenig. *Définition d'une méthodologie de conception des systèmes mécatroniques sûrs de fonctionnement.* Automatique, Institut National Polytechnique de Lorraine, Lorraine, 2004.

[88] J. Song. Performance evaluation of a hybrid electric brake system with sliding mode controller. *Mechatronics*, 15 :339–358, 2005.

[89] B. Sudret. Analytical derivation of the outcrossing rate in time-variant reliability problems. *Structures and Infrastructures Engineering*, 2007.

[90] B. Sudret. *Uncertainty propagation and sensitivity analysis in mechanical models. Contribution to structural reliability and stochastic spectral methods*. PhD thesis, Ecole Nationale des Ponts et Chausées, 2007.

[91] B. Sudret, G. Defaux, and M. Pendola. Time-invariant finite element reliability analysis application to the durability of cooling towers. *Structural Safety*, 27 :93–112, 2005.

[92] B. Sudret and A. Der Kiureghian. Comparaison of finit element reliability methods. *Probabilistic Engineering Machanics*, 17 :337–348, 2002.

[93] R. Tassinari. *Pratique de l'Analyse fonctionnelle*. Dunod, 2003.

[94] A.P. Tchangani and D. Noyes. Attempt to modeling dynamic reliability using dynamic bayesian networks. *Qualita*, 2005.

[95] Centre technique des industries mécaniques CETIM. *Etat de l'art et perspectives de la mécatronique dans l'industrie automobile en Europe et en France*. Cetim, 2006.

[96] Thesame. La mécatronique à l'épreuve du marché. *Jitec*, 2003.

[97] M. Tollenaere. *Conception de produits mécaniques - méthodes, modèles et outils.* Hermes, 1998.

[98] O. Tur, O. Ustun, and R.N. Tuncay. Application note on regenerative braking of electric vehicle as anti-lock braking system. In *Ansoft, LLC*, 2006.

[99] S. Turki and T. Soriano. Un profile bond graphs blocks pour sysml. *CPI*, 2007.

[100] S. Verron. *Diagnostic et surveillance des processus complexes par réseaux bayésiens*. PhD thesis, ISTIA - Université d'Angers, 2007.

[101] G. Vidal-Naquet and A. Choquet-Geniet. *Réseaux de Petri et Systèmes Parallèles*. Armand Colin, armand colin edition, 1992.

[102] A. Villemeur. *Sûreté de fonctionnement des systèmes industriels*. 1988.

[103] S. Vivier. *Stratégies d'optimisation par la méthode des plans d'experiences et application aux dispositifs électrotechnique modélisés par élements finis*. Génie electrique, Ecole Centrale de Lille et Université des Sciences et Technologie de Lille, Lille, 2002.

[104] M.C. Wu and M.C. Shih. Simulated and experimental study of hydraulic anti-lock braking system using sliding-mode pwm control. *Mechatronics*, 13 :331–351, 2003.

[105] K.O. Yusuf and N.J. Smith. Modelling business processes in steel fabrication. *International Journal of Project Management*, 14 :367–371, 1996.

[106] G. Zwingelstein. *Diagnostic des défaillances - Théorie et pratique pour les systèmes industriels.* Hermes, 1995.

[107] G. Zwingelstein. *La maintenance basée sur la fiabilité - Guide pratique d'application de la RCM.* Hermes, Paris, 1996.

Résumé

Cette thèse porte sur l'étude des systèmes complexes tels que les systèmes mécatroniques, en tenant compte de leur aspect dynamique, hybride, reconfigurable et multitechnologies. Le premier chapitre est consacré au contexte actuel des systèmes mécatroniques et la nécessité qu'ils soient conçus et développés de manière collaborative afin d'obtenir des systèmes sûrs de fonctionnement. La démarche systémique aide à l'étude de ces systèmes complexes. Le second chapitre expose les différentes méthodes utilisées dans l'analyse qualitative ainsi que dans l'analyse quantitative. Le choix se porte alors sur les méthodes SADT et SA-RT pour l'analyse fonctionnelle, l'AMDE et l'AEEL pour l'analyse dysfonctionnelle et sur les réseaux de Petri pour l'analyse quantitative. Le dernier chapitre expose la méthodologie proposée pour l'estimation de la fiabilité des systèmes mécatroniques ainsi que l'application de cette méthodologie sur un système ABS. Finalement, les conclusions et les perspectives de l'approche proposée sont émises.

Mots-clés: Mécatronique, modélisation fonctionnelle et dysfonctionnelle, réseaux de Petri, analyse qualitative, analyse quantitative, fiabilité.

Abstract

This thesis focuses on the study of complex systems such as mechatronic systems, taking into account their dynamic, hybrid, reconfigurable and multitechnologies aspect. The first chapter concerns the current context of mechatronic systems. These systems must be designed and developed in a collaborative manner in order to obtain reliable systems. The systemic approach helps to study these complex systems. The second chapter describes different methods used in qualitative and in quantitative analysis. The choice was on SADT and SA-RT methods for the functional analysis, FMEA and SEEA methods for the dysfunctional one and Petri nets for the quantitative analysis. The last chapter presents the methodology proposed for estimating the reliability of mechatronic systems and an application of this methodology on an ABS system. Finally, conclusions and outlooks of the proposed approach are given.

Keywords: Mechatronic, functionnal and dysfunctionnal modelling, Petri nets, qualitative analysis, quantitative analysis, reliability.