**Université des Sciences et des Technologies de Lille**

Numéro d'ordre : 4344

# THÈSE

pour l'obtention du

## Doctorat de l'université des Sciences et des Technologies de Lille

*Discipline : Automatique, Génie informatique, Traitement du signal et Images*

# Prise en compte des séquences de défaillances pour la conception de systèmes d'automatisation

## Application au ferroutage

présentée par

**Joffrey CLARHAUT**

**Soutenue publiquement le 23 mars 2009 devant le jury composé de :**

| | | |
|---|---|---|
| M. Jean-François AUBRY | Professeur, ENSEM-CRAN | Rapporteur |
| M. Christophe BERENGUER | Professeur, UTT-LM2S | Rapporteur |
| M. El Miloudi EL KOURSI | Directeur de recherche, INRETS-ESTAS | Président |
| M. Jean-Marc THIRIET | Professeur, UJF-GIPSA-Lab | Examinateur |
| M. Marc BOUISSOU | Ingénieur HDR, EDF R&D | Examinateur |
| M. Saïd HAYAT | Chargé de recherche HDR, INRETS-ESTAS | Directeur |
| M. Vincent COCQUEMPOT | Professeur, USTL-LAGIS | Co-directeur |
| M. Blaise CONRARD | Maître de conférences, USTL-LAGIS | Co-encadrant |

Thèse préparée aux laboratoires ESTAS de l'Institut National de Recherche sur les Transports et leur Sécurité (INRETS) et LAGIS de l'Université des Sciences et des Technologies de Lille (USTL)

*Je dédie ce mémoire à Aurore qui par son amour et son soutien permanent m'a permis de faire aboutir ce travail.*

*Je dédie également ce mémoire à Jacques, mon grand-père.*

# Avant-propos

Les travaux présentés dans ce mémoire ont été menés à l'Institut National de Recherche sur les Transports et leur Sécurité (INRETS) de Villeneuve d'Ascq, au sein de l'équipe Évaluation des Systèmes de Transport Automatisés et de leur Sécurité (ESTAS) dirigée par Monsieur El-Miloudi El Koursi. Ces travaux ont été réalisés en collaboration avec l'équipe Sûreté de Fonctionnement des Systèmes Dynamiques (SFSD) dirigée par le Professeur Mireille Bayart du Laboratoire d'Automatique, Génie Informatique et Signal - LAGIS UMR CNRS 8146 de l'Université de Lille 1 (USTL).
Tout d'abord, je remercie l'INRETS et le Conseil Régional du Nord-Pas de Calais de m'avoir octroyé une bourse de recherche pour mener à bien les travaux présentés dans ce mémoire.

Je tiens très sincèrement à témoigner toute ma reconnaissance à mes directeurs de thèse, Messieurs Saïd Hayat, Chargé de recherche HDR à l'Institut National de Recherche sur les Transports et leur Sécurité (INRETS), Blaise Conrard, Maître de conférences à l'Université de Lille 1, et Vincent Cocquempot, Professeur à l'Université de Lille 1, qui ont accepté de diriger cette thèse. Leurs nombreux conseils, leurs remarques, leur confiance et les longues discussions que nous avons eues, m'ont guidé tout au long de ce travail.

J'exprime également ma profonde gratitude à Messieurs Jean-François Aubry, Professeur à l'Ecole Nationale Supérieure d'Electricité et de Mécanique (ENSEM) et Christophe Bérenguer, Professeur à l'Université de Technologie de Troyes (UTT) qui m'ont fait l'honneur d'être rapporteurs de ce mémoire.

Je remercie Monsieur El Miloudi EL Koursi, Directeur de recherche et directeur de l'unité ESTAS, pour m'avoir fait l'honneur de présider mon jury.

Je remercie particulièrement Messieurs Jean-Marc Thiriet, Professeur à l'Université Joseph Fourier et Marc Bouissou, Ingénieur HDR à EDF R&D pour l'intérêt qu'ils portent à mes recherches et pour l'honneur qu'ils me font en acceptant de prendre part à mon jury de thèse.

J'ai aussi pu bénéficier de l'aide et de l'expérience de Mme Emilie Martin-Balzac, Ingénieur SNCF à l'Etablissement Industriel de Maintenance du Matériel (EIMM) de Lille, et de Monsieur Serge Bossut, formateur du SUAIO de Lille. Qu'ils en soient ici remerciés.

J'adresse également tous mes remerciements à toutes les personnes que j'ai côtoyées durant ces trois années au sein de l'INRETS et du LAGIS. Je pense plus particulièrement à ceux ayant travaillé avec moi au sein des deux unités de recherche. Je tiens notamment à saluer Sonia, Fred, Nathalie, Greg, Neda, Meriem, François, Jérôme, Georges, Philippe, Vincent, Julie, Sana, Seb, Denis, Rim, Touria et Arnaud pour leur aide et leur bonne humeur. Chacun à sa manière, ils ont contribué à la réalisation de ce mémoire.

Je remercie chaleureusement mes parents, qui ont toujours cru en moi, ainsi que ma famille et mes amis pour la patience qu'ils ont eue à mon égard et les moments de joie et de détente qu'ils ont su m'apporter.

Enfin, *Last but not least*, je tiens à remercier Aurore, mon petit bout de femme, pour son soutien sans faille et qui a su, pendant cette période, me supporter avec tendresse et m'attendre.

# Table des matières

# Table des figures

# Liste des tableaux

# Table des définitions et des notations

## Liste des définitions



## Liste des notations

# Introduction générale

L'amélioration de la qualité, de l'intermodalité et des performances a toujours été une préoccupation constante dans les transports guidés afin de proposer à ses voyageurs ou aux transporteurs de marchandises un système de transport toujours plus sûr. Tous ces progrès ont été possibles grâce à l'introduction de systèmes d'automatisation embarqués qui interviennent sur tous les fronts du domaine ferroviaire : en matière de sécurité (systèmes de protection incendie et d'anti-déraillement), d'environnement (réduction du bruit de roulement pour les voyageurs et pour les riverains) et de performances du matériel roulant (amélioration de la "grande vitesse") mais aussi dans les domaines des communications (GSM-R pour la téléphonie dans les trains), de l'intermodalité (introduction du système européen ERTMS) et dans un futur proche du multimédia (Internet embarqué). Pour les voyageurs, le train ne se limite plus à un rôle purement fonctionnel de transport d'un endroit à un autre mais il contribue également à leur bien être et cela en toute sécurité. Pour le transport de marchandises, et plus particulièrement pour le ferroutage, l'objectif est de proposer aux transporteurs une offre alternative au "tout routier" offrant des performances similaires et une souplesse de transport homogène au niveau européen tout en assurant un niveau de sécurité maximum.

L'introduction des systèmes d'automatisation embarqués n'est pas sans conséquences sur le développement des méthodes de conception. La complexité croissante de ces systèmes impose d'adapter les méthodes et outils existants par rapport à leurs caractéristiques et au respect des exigences toujours plus fortes en matière de sûreté de fonctionnement. Cependant, dans le cadre particulier du ferroutage, son caractère relativement innovant et le transport d'un véhicule routier non conçu au départ pour être transporté sur un train ajoute des contraintes supplémentaires pour garantir un niveau de sécurité optimal. Pour mettre en oeuvre une méthodologie de conception tenant compte des contraintes innovantes du ferroutage, il est impératif de se doter d'outils permettant d'évaluer un niveau de sûreté de fonctionnement dès les toutes premières phases de la conception. En outre, ces outils doivent aussi faciliter l'étude précise de chaque variante d'architecture pour aider le concepteur à en évaluer l'intérêt et choisir le système correspondant le plus à ses besoins en termes de coût et de niveau de sûreté de fonctionnement. L'évaluation du niveau de sûreté des systèmes d'automatisation embarqués permet ainsi de concevoir un système de ferroutage sûr répondant

aux besoins actuels sans surdimensionner les investissements et en utilisant au mieux l'existant.

Ce dernier point s'avère crucial dans le contexte actuel. En effet, la demande, en termes de transport ferroviaire de camions, est appelée à évoluer (congestion des axes de transport occasionnant des retards de livraisons, augmentation des coûts de transport liés à la consommation de carburants, accidents routiers importants) et à croître fortement (besoins accrus en termes de souplesse et de rapidité, alternative écologique souhaitée à la route, ...) dans les prochaines années. Dans ce cadre, cette évolution de la demande se révèle particulièrement importante dans une région comme le Nord-Pas-de-Calais, celle-ci étant placée en position de carrefour ferroviaire au niveau européen. Les travaux de cette thèse contribuent à répondre à cette demande croissante en proposant un système de ferroutage sûr et performant centré autour d'un wagon dit "intelligent" par le fait qu'il est doté de fonctions supplémentaires.
Ces travaux, issus de la collaboration entre l'INRETS[1] (unité de recherche ESTAS[2]) et l'USTL-LAGIS[3] (équipe SFSD[4]) cofinancés par la région Nord-Pas-de-Calais, s'inscrivent dans l'une des thématiques principales de ces deux laboratoires : la conception des systèmes de transport sûrs de fonctionnement. Plus précisément, le problème traité ici relève du domaine de la conception de systèmes de sécurité rendant attractif le ferroutage.

Le champ de domaines soulevés lors d'une étude de conception est vaste. Il inclut notamment la détermination des fonctions supplémentaires de sécurité du wagon intelligent. Cependant, d'autres points se posent également.
Nous cherchons tout d'abord à définir un formalisme de modélisation fonctionnelle et comportementale, support de la méthodologie. De plus, les multiples possibilités de conception doivent pouvoir être représentées.

Ensuite, nous apportons une importance centrale à la sûreté de fonctionnement. A ce titre, une place considérable est accordée à la définition d'une méthode de représentation et d'analyse dysfonctionnelle. Il paraissait primordial de disposer d'un formalisme de description graphique, similaire aux arbres de défaillances, afin de faciliter la représentation du comportement de systèmes d'automatisation complexes. Le comportement dysfonctionnel d'un système dépend non seulement des fonctions du système qui sont affectées par des composants défaillants mais ce comportement dépend également de séquences de modes de défaillances ordonnés dans le temps (ou **scénarios**). Cependant, les méthodes d'évaluation classiques de la sûreté de fonctionnement ne sont pas bien appropriées pour prendre en compte ces scénarios. De même, les méthodes de simulation basées sur les graphes de Markov

[1]Institut National de REcherche sur les Transports et leur Sécurité
[2]Évaluation des Systèmes de Transport Automatisés et de leur Sécurité
[3]Laboratoire d'Automatique, Génie Informatique et Signal, UMR CNRS 8146
[4]Sûreté de Fonctionnement des Systèmes Dynamiques

présentent des limites : long temps de simulation, explosion combinatoire du nombre d'états à considérer. Par ailleurs, ces méthodes sont développées dans le but d'analyser un système fini et non pour le concevoir. Nous nous sommes donc intéressés à une approche quantitative d'évaluation d'un grand nombre d'architectures matérielles basée sur les scénarios et sur une description graphique afin de contourner ces limites.

**Le premier objectif de ce travail est de proposer une méthodologie de conception de systèmes d'automatisation sûrs de fonctionnement basée sur un modèle fonctionnel permettant de représenter toutes les possibilités d'agencements et sur un modèle comportemental utilisant les scénarios. Le second objectif est de l'appliquer dans le domaine du ferroutage afin de déterminer les possibilités de réalisation de quelques fonctions d'un wagon intelligent**.

Dans la suite, ce mémoire est décomposé en deux parties. La première partie (Chap. 1 et 2) est consacrée aux développements méthodologiques, la seconde partie (Chap. 3 et 4) à l'application.

Le **chapitre 1** introduit les systèmes d'automatisation et leurs évolutions vers les systèmes à intelligence distribuée. Les aspects liés à la complexité de ces systèmes d'automatisation et la problématique de conception qui en découle sont ensuite détaillés. Une présentation des notions liées à la sûreté de fonctionnement permet d'expliquer la problématique d'évaluation du niveau de sûreté de fonctionnement des systèmes d'automatisation. Issus de ces deux problématiques, nos besoins en une méthodologie de conception et d'évaluation de systèmes intégrant les scénarios sont développés. Les inadéquations entre nos besoins et les méthodes d'évaluation actuelles, décrites plus en détails dans ce chapitre, permettent de justifier nos travaux.

Dans le **chapitre 2**, nous développons les différents éléments de la méthodologie que nous proposons. Cette méthodologie couvre notamment les problèmes de modélisation des différentes possibilités d'agencement des composants, d'utilisation des scénarios dans un modèle dysfonctionnel et de définition de paramètres quantitatifs d'évaluation du niveau de sûreté de fonctionnement. Un exemple illustratif de cette méthodologie pour la conception d'un système d'asservissement d'une cuve est détaillé tout au long de ce chapitre. Ce chapitre se termine par une présentation de l'atelier logiciel ALoCSyS que nous avons réalisé.

L'application que nous avons étudiée est décrite dans le **chapitre 3**. Sa position dans le domaine des transports guidés, les risques et les besoins sécuritaires de ce système y sont

soulignés. Le modèle fonctionnel du wagon intelligent et son découpage en plusieurs phases de fonctionnement sont aussi présentés.

Enfin, le **chapitre 4** illustre la méthodologie sur deux fonctions du wagon intelligent pour le ferroutage : un système de protection contre l'incendie et un système de protection contre le désarrimage du véhicule routier. Notre approche d'évaluation est comparée à la méthode d'évaluation plus classique basée sur les arbres de défaillances. Cette comparaison permet de mettre clairement en évidence les apports de notre méthode. En outre, la conception de ces deux systèmes par regroupement de leurs ressources communes montrera les limitations actuelles de notre approche.

Ce mémoire se termine par une conclusion générale qui rappelle les principaux points développés dans ce travail et envisage plusieurs perspectives de recherche.

# Première partie :

# Conception de systèmes sûrs

# Chapitre 1

# Conception de systèmes sûrs de fonctionnement

## 1.1 Introduction

L'évolution des systèmes d'automatisation rend difficile leur conception et leur évaluation du point de vue de la sûreté de fonctionnement. En effet, le nombre de plus en plus important de fonctions à remplir avec un niveau de performances attendu et l'introduction des instruments intelligents possédant de nouvelles fonctionnalités rendent délicate l'étude du comportement fonctionnel et dysfonctionnel de tels systèmes ainsi que la quantification de paramètres de sûreté de fonctionnement permettant de choisir le système optimal, c'est-à-dire le système correspondant le mieux aux besoins du concepteur. Cette difficulté de modélisation, d'analyse et de quantification de ces systèmes, qualifiés alors de *complexes*, génère un développement important de méthodologies de conception et d'outils d'évaluation du niveau de sûreté de fonctionnement.
Dans ce contexte de besoins forts en méthodologies de conception et de maîtrise du fonctionnement des systèmes complexes, les méthodes d'analyse basées sur les cycles de développement permettent de définir les différentes architectures du système à concevoir et de les optimiser. Par ailleurs, concernant l'évaluation du niveau de sûreté de fonctionnement des systèmes d'automatisation, plusieurs approches permettent de caractériser le comportement en présence de dysfonctionnements et de fournir des critères permettant d'aider le concepteur au choix de ses équipements et de ses systèmes.

La première partie de ce chapitre présente les systèmes d'automatisation et les instruments intelligents. Prenant appui sur ces définitions, la démarche générale de conception d'un système est ensuite expliquée ainsi qu'une présentation des différentes sources de complexité d'un système d'automatisation. La deuxième partie de ce chapitre présente la sûreté

de fonctionnement ainsi que les différentes démarches de conception d'un système sûr. Cette partie présente également les différents moyens matériels pour rendre le système plus sûr. La problématique liée à l'évaluation de systèmes complexes sûrs de fonctionnement est ensuite abordée dans la troisième partie de ce chapitre. Un état de l'art sur les principales méthodes liées à l'évaluation du niveau de sûreté de fonctionnement d'un système complexe est d'abord présenté. L'explication des limites de ces méthodes d'évaluation justifiera le cadre de nos travaux de recherche.

## 1.2 Les systèmes d'automatisation intelligents

### 1.2.1 Présentation

#### 1.2.1.1 Les systèmes d'automatisation

Un système d'automatisation est composé d'un ensemble d'équipements qui sont organisés dans l'objectif d'accomplir un ensemble de missions au sein d'un processus industriel (ou processus physique) conformément à des objectifs économiques et techniques. Ces équipements sont de différents types :

- des capteurs traduisant l'état du processus industriel et des équipements,
- des actionneurs agissant sur le processus industriel,
- des unités de traitement (des régulateurs, des automates, des calculateurs, etc ...) élaborant les commandes à destination des actionneurs, à partir des informations générées par les capteurs,
- des moyens de communication reliant les différents composants du système d'automatisation.

Ces systèmes sont qualifiés de réactifs, c'est-à-dire qu'ils réagissent de façon permanente aux sollicitations de leur environnement ou du processus industriel. Le système réactif contrôle le comportement de l'environnement en observant son évolution dans le temps par les capteurs et en le pilotant au moyen d'actionneurs comme illustré sur la figure 1.1.

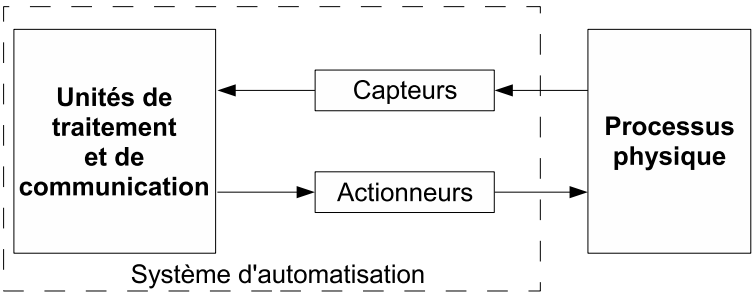


FIG. 1.1 – Interactions système d'automatisation / Processus industriel

Les systèmes d'automatisation présentent habituellement une architecture dite *centralisée* présentée figure 1.2, comprenant un ensemble de capteurs et d'actionneurs raccordés par des liaisons directes via des cartes d'entrées/sorties numériques ou analogiques à une unité de traitement [BCCR05] qui effectue les traitements complexes. Cette architecture permet l'échange point à point d'une seule information entre les équipements et l'unité centrale :

- un capteur fournit une mesure,
- un actionneur reçoit une commande.

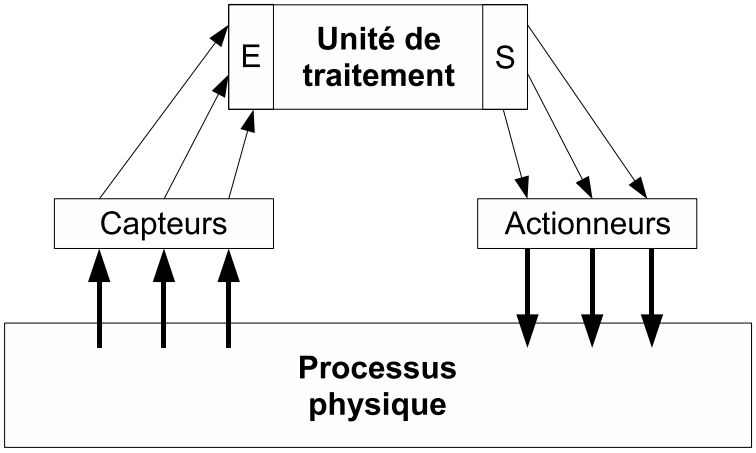


FIG. 1.2 – Système d'automatisation centralisé

#### 1.2.1.2 Evolution vers les systèmes d'automatisation à intelligence distribuée

Les systèmes d'automatisation à intelligence distribuée (SAID) ont été introduits dans les années 80. Ils sont issus des systèmes d'automatisation précédents et ont été développés dans le but de répondre aux besoins de plus en plus importants en informations à traiter au sein des processus industriels. En effet, l'évolution des processus automatisés qui prennent en compte, en plus du contrôle commande, la maintenance, la sécurité et la gestion technique a conduit à une augmentation croissante des traitements d'informations en nombre et en complexité.

Afin de répondre à ces besoins, les systèmes d'automatisation ont subi deux évolutions [BCCR05] :

- Une première évolution est apparue avec l'introduction des bus de terrain (ou réseaux locaux industriels) [Tho04]. Ces bus ont permis de déporter les entrées/sorties digitales et analogiques. Cependant, ils ont également conservé l'architecture centralisée et ses inconvénients (long temps de réponse, gestion simultanée de nombreuses variables, ...). La figure 1.3 présente cette architecture centralisée dont les entrées/sorties sont déportées.

– Une seconde évolution a été de répartir l'unité centrale et de rapprocher les traitements au plus près des équipements ce qui a abouti au SAID présenté figure 1.4.

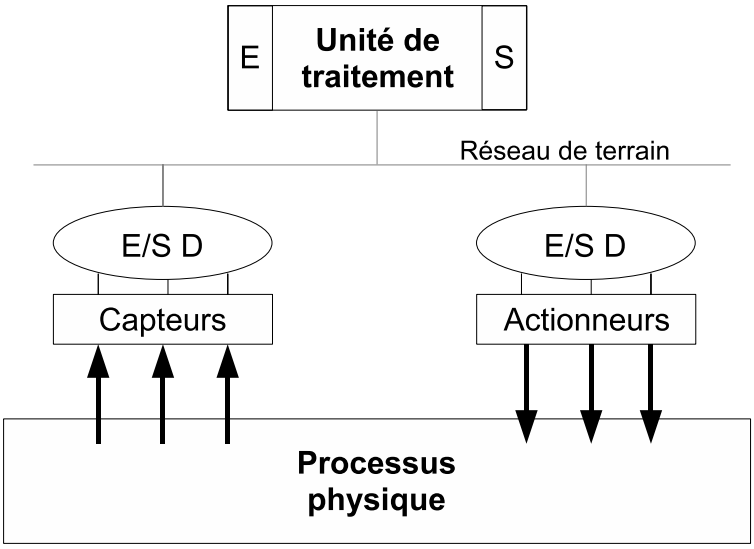


FIG. 1.3 – Système d'automatisation centralisé et E/S déportées

Les SAID sont composés de capteurs et d'actionneurs dits *intelligents* capables de traiter localement l'information et de la communiquer aux autres composants. Les SAID peuvent également être composés de petites unités de traitements (microautomate) gérant un sous-ensemble de capteurs et d'actionneurs comme présenté figure 1.4. Ces systèmes permettent une grande flexibilité en termes de commande, de sécurité et de fiabilité [MTA06].

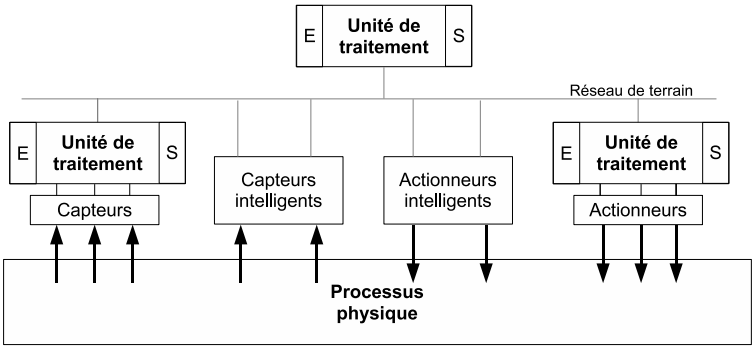


FIG. 1.4 – Système d'automatisation à intelligence distribuée

#### 1.2.1.3 Les instruments intelligents

La notion d'instrument intelligent est apparue à la fin des années 80. En effet, à cette époque, les possibilités offertes par la technologie des microprocesseurs permettent de conce-

voir et d'utiliser des constituants dits *intelligents* jusque dans les capteurs et les actionneurs. Un instrument intelligent (qu'il soit capteur ou actionneur) est un équipement qui intègre des fonctionnalités supplémentaires ou évoluées aptes à améliorer ce pourquoi il a été conçu [BCCR05], [CIA09].
Ainsi, en plus de sa fonction élémentaire d'acquisition d'une grandeur physique dans le cas du capteur ou d'action sur un processus dans le cas de l'actionneur, on attend d'un instrument intelligent qu'il offre des fonctions de compensation, de validation, d'autodiagnostic, d'autoconfiguration, associées à des moyens de communication adaptés.
C'est à travers ces nouveaux services qu'un instrument intelligent se distingue d'un composant standard. De ce fait, il existe différents types d'instruments :

- l'instrument *analogique* dont le rôle est de convertir. Pour un capteur, il s'agit de transformer une grandeur physique en un signal électrique utilisable par une unité de traitement. Pour un actionneur, il s'agit de transformer un signal en une action sur le processus industriel. Le lecteur intéressé peut se référer à [Gro02] et [DIA90] pour de plus amples détails.
- l'instrument *numérique* dont le rôle est également de convertir mais à travers une chaîne de traitements dans laquelle figure une ou plusieurs opérations numériques susceptibles d'améliorer cette conversion.
- l'instrument *intelligent* qui possède des fonctionnalités qui améliorent ses performances, par des fonctions embarquées de mémorisation et de traitement des données et qui possède une capacité à crédibiliser sa fonction associée à une implication dans les fonctions du système auquel il appartient. Cette crédibilisation fait référence à la capacité à valider la mesure produite pour le capteur ou à rendre compte de la réalisation effective de l'action pour l'actionneur. L'implication de l'instrument intelligent dans le système concerne, entre autre, sa participation à la sécurité du système en offrant des possibilités d'alarme, à la commande du système en intégrant des fonctions de régulation, ...

Un instrument est souvent considéré comme intelligent dès qu'il intègre au moins un traitement numérique (complexe ou non) et ce quel que soit son apport en termes de services [BCCR05], [CIA09]. Dans la suite de ce mémoire, on adoptera cette définition dans laquelle un instrument ou un système n'est considéré comme intelligent que par les fonctions supplémentaires qu'il est susceptible de rendre par rapport à un instrument ou un système standard et ce tout au long de son cycle de vie.

D'un point de vue matériel, un instrument ou un système intelligent se compose alors de trois sous ensembles présenté sur la figure 1.5 :

- Une unité de traitement numérique : elle inclut un organe de calcul (microcontrôleur, microprocesseur, DSP, ...), les périphériques associés (mémoires) et une alimentation.

– Une interface de communication permettant un dialogue bidirectionnel numérique avec le système d'automatisation.
– Une chaîne principale d'interface avec le processus : cette chaîne d'acquisition (capteur) ou d'action (actionneur) est composée d'un ou plusieurs équipements associés à des conditionneurs.

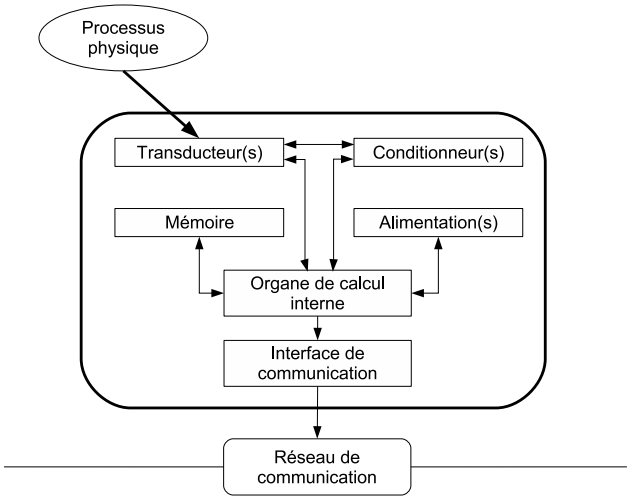


FIG. 1.5 – Architecture matérielle d'un instrument intelligent

## 1.2.2 Conception de systèmes d'automatisation

### 1.2.2.1 Démarche et modèle de conception

Le cycle de vie d'un système est composé de trois étapes, une étape de conception, une étape d'exploitation-maintenance et une étape de démantèlement. Dans le cadre de ce mémoire, nous nous intéresserons à l'étape de conception du système. Cette étape est importante pour le système puisqu'elle permet, à partir de l'expression d'un besoin initial, de définir les caractéristiques d'un système opérationnel permettant de le satisfaire. Ainsi, sont déterminés, entre autres, le coût des équipements utilisés, les spécifications (technologie employée) et les performances du système conçu.
L'activité de conception d'un système peut être modélisée sous la forme d'un cycle de développement composé d'activités élémentaires. Ce cycle a fait l'objet de plusieurs modèles comme le modèle de [PB96] qui propose une approche algorithmique et une procédure systématique à suivre ou encore comme les modèles développés en génie informatique : le cycle en cascade [Roy70], le cycle en X [Hod91], le cycle en V [AFN96] ou encore le cycle en spirale [Boe88]. Mais quel que soit le modèle utilisé, un cycle de développement est considéré comme un enchaînement d'activités nécessaires pour créer une ou plusieurs représentations

du système différenciées les unes des autres par le niveau d'abstraction de la représentation du système. Par exemple, les principales activités du cycle en V [AFN96], présenté figure 1.6, sont la définition des besoins (dans le cahier des charges), la spécification du système et de ses performances, la conception, puis la réalisation, le choix des constituants et l'intégration et enfin, le test et la validation-certification. Ce cycle montre deux phases dans l'activité de conception : une phase de spécification-conception qui est globalement descendante (ou top-down) et une phase de réalisation-test qui est globalement ascendante (ou bottom-up). En outre, ce cycle montre aussi qu'il existe deux parties possibles pour l'activité de conception : une conception préliminaire où l'on fait une première ébauche du système et de ses fonctions puis une conception détaillée.

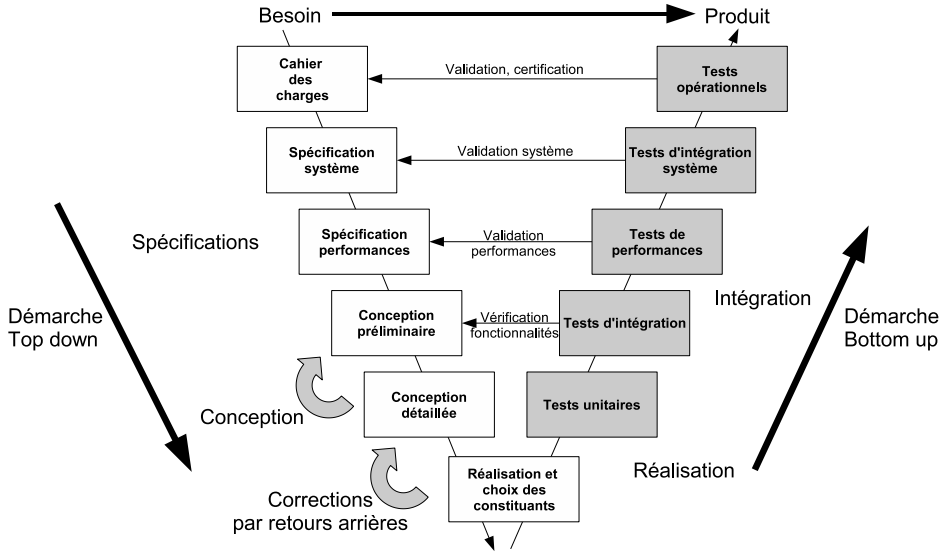


FIG. 1.6 – Cycle de développement en V d'un système

Ces modèles ont été étendus pour prendre en compte les particularités des systèmes d'automatisation [Cal90], [PRZ92]. En effet, ces systèmes sont caractérisés par l'utilisation de matériels spécialisés (instruments intelligents) ayant des fonctions spécifiques et par l'utilisation de matériels programmables (automates, calculateurs) intégrant de nombreux traitements logiciels. De ce fait, la conception de ces systèmes implique une activité de définition et de répartition du logiciel sur le matériel mais également une activité de définition et de dimensionnement de ce matériel support.
La conception d'un système d'automatisation (à intelligence distribuée ou non) passe par la définition et la validation de trois architectures distinctes : l'architecture fonctionnelle, l'architecture matérielle et l'architecture opérationnelle [SLTBS95].

– L'architecture fonctionnelle, résultat de l'activité de spécification, est une description

des solutions envisagées pour répondre aux besoins. Elle exprime l'ensemble des activités du système.
- L'architecture matérielle est l'arrangement d'équipements et de moyens de communication qui définissent une solution. C'est le résultat d'un choix d'équipements et de leur dimensionnement compte tenu des besoins initiaux. La caractérisation (coûts, performances, ...) des équipements d'une architecture matérielle est indispensable pour vérifier les propriétés de l'architecture opérationnelle et ainsi la valider.
- L'architecture opérationnelle est le résultat de la projection de l'architecture fonctionnelle sur l'architecture matérielle à l'aide de critères précis (exigences de sûreté de fonctionnement, coût financier minimum, ...). Cette projection est effectuée de manière à ce que chaque fonction (ou groupe de fonctions) de l'architecture fonctionnelle soit implantée sur un équipement de l'architecture matérielle.

Le résultat de l'activité de conception est l'architecture opérationnelle optimale. Il s'agit de l'architecture opérationnelle qui optimise un ou plusieurs critères parmi les architectures opérationnelles admissibles, c'est-à-dire respectant les contraintes énoncées avec les besoins initiaux.

#### 1.2.2.2 L'architecture fonctionnelle

La première architecture à définir lors de la conception d'un système est l'architecture fonctionnelle. [MES94] et [Aka96] parlent de l'architecture fonctionnelle comme étant le modèle abstrait et formalisé de la structure du système, le lecteur intéressé pourra se reporter à [Amo99b] où un état de l'art des modélisations fonctionnelles est dressé.
L'activité de conception fonctionnelle consiste à décomposer les fonctions que doit rendre le système en fonctions plus simples, elles-mêmes décomposables en sous-fonctions encore plus simples jusqu'à aboutir à des fonctions ou des composants élémentaires. L'organisation et le comportement des fonctions décrivent les activités du système d'automatisation tout au long de son cycle de vie. De nombreux ouvrages comme [Cal90] et [Bre00] recensent les méthodes de décomposition de systèmes (ou méthodes d'analyse fonctionnelle) les plus utilisées dont le principe est d'analyser, comprendre et spécifier le système de façon hiérarchique. Ces méthodes sont classifiables en trois catégories [Lut97] :
- une catégorie *orientée fonctions* qui identifie les fonctions et leurs interactions. Parmi les méthodes de cette catégorie se trouve la méthode SADT (Structured Analysis and Design Technique) [IGL89], la méthode APTE [Bre00], le diagramme des interacteurs [PZB03] ou encore la méthode FAST (Functional Analysis System Technique) [Byt79].
- une catégorie *orientée données* qui modélise les informations utilisées par le système étudié. On fait alors appel à des méthodes comme SART (Structured Analysis for Real Time) [HP87], MERISE [TRC83] ou les graphes de fluence [Rob61].
- une catégorie *orientée objets* qui étudie simultanément les fonctions et les données du

système. Dans ce cas, on utilisera les approches orientées objets [Rum95], [OMG07]. Le tableau 1.1, issu de [SB96a], présente la description et le domaine d'utilisation de quelques-unes de ces méthodes ainsi que l'étape d'application dans le cycle de vie du système. Par ailleurs, dans [Pet07] est présenté un ensemble de méthodes et modèles utilisés dans le domaine spécifique des systèmes d'automatisation.

| Méthode | Etape | Objectifs | Système |
|---|---|---|---|
| Graphe de fluence | Conception Exploitation | Identification des variables, de leurs rôles et de leurs interactions | Processus continus ou discontinus |
| SADT | Conception Exploitation | Identification de toutes les fonctions du système et de leurs supports | Systèmes d'organisation ou informatiques |
| Arbre Fonctionnel | Conception | Traduction d'un besoin en termes de fonctions. Optimisation des moyens associés aux fonctions | Systèmes électromécaniques ou mécaniques |
| MERISE | Conception Exploitation | Description formelle d'un système d'information | Systèmes d'information ou d'organisation |
| APTE | Conception Exploitation | Identification des fonctions et procédures à assurer | Systèmes d'organisation |
| FAST | Conception | Aide à la révision de la conception | Systèmes mécaniques ou d'organisation |
| Diagramme des interacteurs | Conception Exploitation | Identification de toutes les fonctions du système et de leurs interactions avec l'environnement | Systèmes mécaniques, électroniques ou d'organisation |

TAB. 1.1 – Principales méthodes d'analyse fonctionnelle

Nous avons utilisé la méthode du diagramme des interacteurs pour déterminer nos fonctions et concevoir nos architectures fonctionnelles. En effet, cette méthode présente plusieurs avantages :

- Elle est utilisée pour concevoir tous types de systèmes : mécaniques, électroniques, hydrauliques, d'automatisation ou d'organisation.
- Elle permet de lister l'ensemble des fonctions d'un système sans que le concepteur soit influencé *a priori* par des structures prédéfinies ou par des solutions matérielles existantes.
- Elle représente le système et ses interactions vis-à-vis de son environnement.

La figure 1.7 présente un exemple de diagramme des interacteurs. Ce diagramme est une représentation très schématique du système dans laquelle [PZB03] :

- le système central représente le système à concevoir, par exemple un système d'automatisation,
- les systèmes périphériques représentent l'environnement extérieur du système, on peut citer par exemple les opérateurs du système et le milieu environnant.
- le trait *droit*, noté F1 sur la figure 1.7, relie directement le système central avec un milieu extérieur et explicite une interaction (représentée par une fonction) entre le système et un seul environnement extérieur. La fonction de transmission des informations entre le système d'automatisation et les opérateurs du système en est un exemple,
- le trait *à main levée*, noté F2 sur la figure 1.7, explicite une relation (représentée également par une fonction) entre plusieurs environnements extérieurs par l'intermédiaire du système central. La fonction de mesure de la température extérieure permettant de contrôler et de maintenir la température d'une marchandise transportée est un exemple de ce type de relation.

Les traits sont obtenus par des questionnements successifs du concepteur sur les missions que doit remplir le futur système [PZB03]. Ce diagramme permet d'expliciter les premières interactions entre le système et son environnement extérieur proche et de lister exhaustivement tous les besoins du concepteur sous forme de fonctions avant de les décomposer en sous-fonctions plus simples au sein d'un arbre fonctionnel.

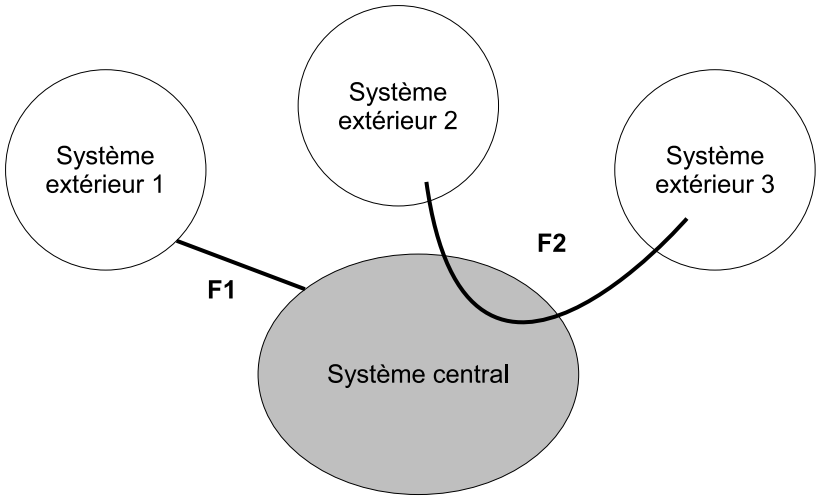


FIG. 1.7 – Diagramme des interacteurs

L'analyse fonctionnelle du système constitue la principale donnée d'entrée pour la construction d'une architecture opérationnelle. Elle peut être décrite sous la forme d'un ensemble d'éléments structurés par des liens de contrôle et de données. Cette description s'applique à toute architecture fonctionnelle, qu'elle soit relative à un instrument isolé (capteur, actionneur) ou à l'ensemble d'un système d'automatisation.

#### 1.2.2.3 L'architecture matérielle

La réalisation des fonctions de l'architecture fonctionnelle nécessite un choix d'équipements adaptés matériels et logiciels (sous-systèmes, capteurs, actionneurs, systèmes de traitement et de communication, ...) et dont l'agencement, les uns par rapport aux autres, constitue l'architecture matérielle [Bou97]. Un exemple d'architecture matérielle utilisant des instruments intelligents et standards est donnée figure 1.8.

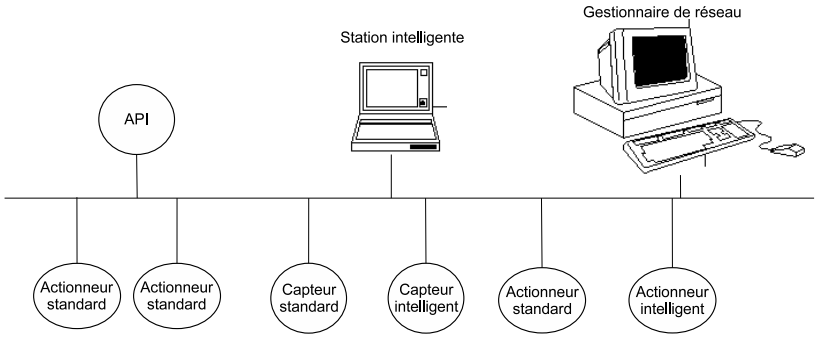


FIG. 1.8 – Exemple d'architecture matérielle

Ainsi, une architecture matérielle est constituée :
- d'un ensemble organisé d'équipements munis, pour certains, de traitements logiciels,
- d'un ensemble de moyens de communication connectant les équipements entre eux et vers d'autres systèmes ou opérateurs humains.

L'architecture matérielle spécifie également pour chaque équipement l'ensemble de ses caractéristiques globales parmi lesquelles on trouvera : le fournisseur, l'encombrement, le poids, le prix, les conditions d'utilisation, la consommation électrique, ... Au niveau des unités de traitement, les caractéristiques sont par exemple : un ou plusieurs processeurs, la taille mémoire maximale, les entrées/sorties disponibles, ... A noter également que les instruments intelligents sont également des équipements élémentaires du système d'automatisation ayant des caractéristiques globales utilisées au niveau de l'architecture matérielle comme celles relatives à leur interfaçage avec le reste du système (entrées/sorties, communication, alimentation embarquée ou non) et celles relatives à leurs capacités de traitement.

#### 1.2.2.4 L'architecture opérationnelle

L'architecture opérationnelle est définie par [SB94] et [Aka96] comme la projection de l'architecture fonctionnelle sur une architecture matérielle conduisant à affecter des fonctions à un équipement. Cette projection fait appel à des fonctions coûts pour évaluer les différentes solutions, et fait appel à des outils d'évaluation tels que ceux utilisés pour évaluer un niveau de sûreté de fonctionnement ou un niveau de performance. Les fonctions coûts peuvent

prendre en compte soit le coût financier de la solution, soit un coût d'exécution et/ou de communication. Dans ce mémoire, la fonction coût est prise en compte afin d'évaluer le coût financier des solutions possibles et les outils d'évaluation sont ceux utilisés pour évaluer un niveau de sûreté de fonctionnement.

## 1.3 Problématique liée à la conception des systèmes d'automatisation

Nous avons vu dans la section précédente que l'évolution des processus automatisés a conduit à une augmentation croissante des traitements d'informations en nombre et en complexité et au développement des SAID. Par ailleurs, la prise en compte, en plus du contrôle commande, de la maintenance, de la sécurité et de la gestion technique étend de plus en plus les applications des SAID qui sont alors qualifiés de complexes. La complexité d'un SAID met en évidence des difficultés à le modéliser à l'aide des trois architectures puis à l'analyser. Nous allons d'abord voir quelles sont les différentes sources de cette complexité et quelles sont les difficultés liées à la conception de ces systèmes, c'est-à-dire concernant la détermination des trois architectures.

### 1.3.1 Les SAID : des systèmes complexes

#### 1.3.1.1 Complexité liée au nombre de composants

La réalisation de systèmes d'automatisation remplissant de nombreuses missions nécessite l'utilisation possible d'un grand nombre de composants de différents types. En général, les composants sont choisis de manière à réduire globalement le coût de l'architecture matérielle, mais en respectant certaines contraintes technologiques (par exemple, des contraintes de fiabilité ou de disponibilité). A noter que dans la majorité des cas, les composants matériels ne sont pas développés spécifiquement pour le système d'automatisation à concevoir. [QL03] parle de "composants sur l'étagère" (ou off-the-shelf component) dont un inconvénient repose sur une documentation succincte.
Il est évident que le nombre d'éléments du système d'automatisation a une influence directe sur la modélisation du système. Plus celui-ci est élevé, plus le modèle du système est important et plus celui-ci est complexe.

#### 1.3.1.2 Complexité technologique

L'augmentation du nombre de composants s'accompagne généralement de l'emploi de technologies innovantes et différentes. Dans le cadre des SAID, la complexité technologique est liée à l'emploi d'instruments intelligents qui apportent de nouvelles possibilités mais qui

introduisent également de nouvelles contraintes sur certains objectifs à atteindre (performances, sûreté de fonctionnement [CD95], ...). Par ailleurs, ces technologies peuvent être sources de défaillances difficilement prévisibles.

#### 1.3.1.3 Complexité d'états

Le nombre d'états dans lesquels un système d'automatisation peut se trouver est fonction du nombre de composants qui le constituent et du nombre d'états dans lesquels ces composants peuvent eux-mêmes se trouver.
L'exemple de l'avion à 4 réacteurs introduit par [Vil88] illustre bien la notion de vecteur d'états (16 états au total). Le pilotage de l'avion est totalement différent en fonction de la localisation et du nombre de réacteurs défaillants. A chaque vecteur d'état correspond un nouveau système à piloter dont les caractéristiques sont différentes.
Les modes ou états, qu'un système peut atteindre, sont classés par [Gru99] en trois catégories :

- les modes de fonctionnement nominal : ensemble de tous les états de fonctionnement normal du système.
- les modes d'arrêt : ensemble de tous les modes conduisant à un arrêt du système pour des raisons extérieures.
- les modes de défaillance : ensemble de toutes les défaillances conduisant à la perte du service.

#### 1.3.1.4 Complexité fonctionnelle

La fonction d'un système est définie dans [Cal90] comme une "entité assurant une activité spécifique du système". Une fonction peut être élémentaire ou complexe. Par décompositions successives, une fonction complexe se décompose sous la forme d'une structure composée de fonctions élémentaires. Les fonctions sont définies dans le cahier des charges lors de la définition des besoins, indépendamment des aspects technologiques.
Comme pour le nombre de composants ou le nombre d'états, le nombre de fonctions à remplir par un système d'automatisation a également une influence sur la modélisation du système. Plus le nombre de fonctions est élevé, plus sa complexité augmente.

#### 1.3.1.5 Complexité structurelle

L'architecture opérationnelle du système d'automatisation forme une structure composite (composants, sous-systèmes, systèmes, ...) structurée en plusieurs niveaux et où il existe de nombreuses dépendances/interactions entre les différentes fonctions pour un même niveau et entre les différents niveaux [MES94].
Le tableau 1.2 et la figure 1.9 résument les structures classiques utilisées pour représenter la logique de fonctionnement de la plupart des systèmes industriels d'automatisation.

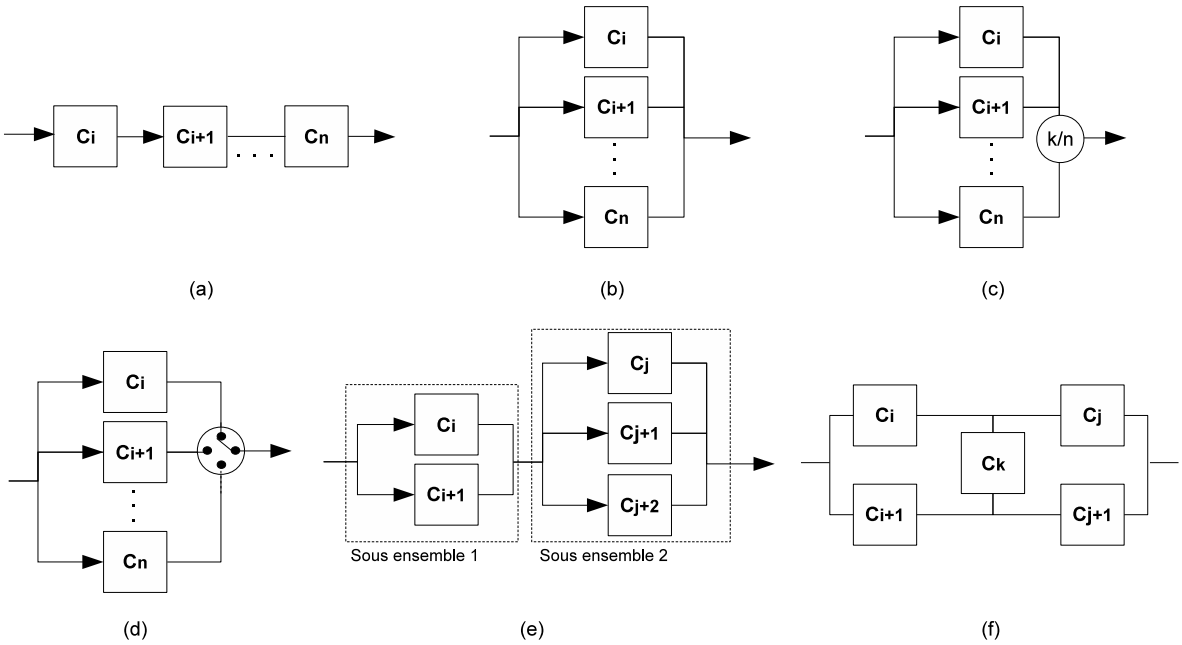


FIG. 1.9 – Représentation des différentes structures par blocs

| Type | Représentation | Comportement |
|---|---|---|
| Série | (a) | Les n éléments du système fonctionnent simultanément |
| Parallèle en redondance active | (b) | Tous les éléments du système fonctionnent simultanément |
| Parallèle en redondance active partielle | (c) | k éléments sur les n du système fonctionnent simultanément |
| Parallèle en redondance passive | (d) | Parmi les n éléments du système, un élément est en fonctionnement tandis que les autres sont en état d'attente. Un dispositif de commutation assure le remplacement d'un élément par l'un des (n-1) éléments en attente |
| Mixte | (e) | Les éléments du système sont disposés dans des sous-ensembles soit en série soit en parallèle et possèdent les propriétés de ces structures |
| En pont | (f) | Dans les systèmes dits "en pont", la structure du système n'est pas toujours évidente. Il est toutefois possible de ramener cette structure en pont à des représentations séries/parallèles/mixtes en employant le théorème des probabilités totales |

TAB. 1.2 – Comportement des structures de la figure 1.9

Comme pour les autres aspects de la complexité, l'utilisation et la combinaison de ces structures au sein d'une architecture matérielle a également une influence sur la modélisation du système. Plus le nombre de ces structures est élevé, plus le système et son comportement sont complexes.

### 1.3.2 Difficultés liées à l'obtention des architectures

Du fait que les SAID sont complexes (compte tenu du nombre de composants et de structures utilisables, de l'hétérogénéité technologique de ces composants ainsi que des fonctions et des états qu'ils introduisent), la première difficulté vient dans le choix de l'architecture matérielle.

En effet, l'activité de conception consiste à choisir les composants du SAID sur un ensemble fourni par les catalogues fournisseur, puis à les dimensionner en définissant les paramètres tels que le coût financier, les performances, le nombre d'entrées/sorties, ... En relation avec ces choix de composants, il convient également de définir le système de communication dont le dimensionnement est fonction de l'architecture fonctionnelle qui détermine les flux de données. L'architecture matérielle résulte donc de nombreux choix (type de composant, dimensionnement, ...) effectués en vue de pouvoir supporter l'architecture fonctionnelle établie préalablement.
L'architecture fonctionnelle influence donc l'étape du choix, mais son impact n'est pas simple à modéliser et, actuellement, le choix de l'architecture matérielle ne suit pas une méthode formalisée, ni même une méthode déductive, ce choix repose sur le savoir faire technique et l'expérience du concepteur [Cho00].

Une autre difficulté apparaît pour la définition de l'architecture opérationnelle et concerne le partitionnement des fonctions de l'architecture fonctionnelle et leur affectation sur les éléments de l'architecture matérielle. Si certaines adéquations sont évidentes compte tenu de l'adéquation entre les fonctions souhaitées et celles offertes par l'architecture matérielle (par exemple la fonction de mesure accomplie au moyen de capteurs), d'autres nécessitent un découpage plus complexe et doivent tenir compte d'éléments supplémentaires (flux de données, contrainte de temps, ...). Pour chaque sous-système identifié issu des fonctions complexes, il est donc impératif de préciser les liens entre les données.

Une difficulté supplémentaire concerne la validation de l'architecture opérationnelle. Il s'agit de déterminer l'architecture opérationnelle qui optimise un ou plusieurs objectifs (coût financier, performances, niveau minimum de sûreté de fonctionnement, ...) parmi l'ensemble des architectures opérationnelles admissibles. La validation peut être définie suivant deux approches qui peuvent être complémentaires :

– La première approche dite *a priori* consiste à établir un modèle (choix de l'équipement, choix des critères de projection) et à prouver que la solution possédera les propriétés exigées (conformité aux normes, contraintes de consommation électrique, poids, ...). La

difficulté apparaît dans le choix du modèle et de sa précision permettant de justifier le respect des propriétés souhaitées.
- La seconde approche dite *a posteriori* consiste à réaliser une partie ou l'ensemble de la solution obtenue de manière à la tester. La qualité de cette approche dépend de l'exhaustivité des tests. Dans certains cas, il n'est pas possible de tester tous les scénarios et il est fait appel à des approches statistiques.

Quelle que soit l'approche utilisée, si la validation n'est possible sur aucune des solutions, l'architecture fonctionnelle devra être remise en cause ou les contraintes opérationnelles devront être modifiées.

Enfin, la dernière difficulté concerne l'analyse et l'évaluation de la sûreté de fonctionnement des systèmes d'automatisation. En effet, un système (d'automatisation ou non) est sujet à des défaillances internes au cours de son cycle de vie. Les multiples sources de complexité et les multiples possibilités d'équipement pour concevoir un système d'automatisation rendent difficile l'analyse du comportement final du système face à ces défaillances. Ces défaillances étant susceptibles de le faire se comporter de telle sorte qu'il ne puisse pas remplir les fonctions pour lesquelles il a été conçu, il est impératif de pouvoir rendre le système tolérant à ces défaillances. La sûreté de fonctionnement a pour objectif d'analyser ce comportement non désiré par différents outils. Par ailleurs, il existe des techniques matérielles pouvant être utilisées afin de rendre un système plus sûr correspondant aux besoins définis initialement. Nous allons présenter dans la section suivante les concepts liés à la sûreté de fonctionnement ainsi que les techniques permettant de rendre un système plus sûr.

## 1.4 Sûreté de fonctionnement et activité de conception

### 1.4.1 Historique et terminologie

#### 1.4.1.1 La sûreté de fonctionnement

Les premières études de sûreté de fonctionnement sont apparues à partir des années 1950 dans des domaines à hauts risques tels l'aéronautique, l'aérospatiale ou le nucléaire. Les études statistiques sur les fréquences de pannes et accidents qui étaient alors menées, avaient pour objectif de renforcer la sécurité des systèmes par l'amélioration de la fiabilité des pièces jugées critiques ou en ayant recours à la redondance matérielle [Tit92]. Les résultats de ces études statistiques ont montré que l'amélioration de la sécurité d'un système ne passe pas uniquement par la prise en compte des pièces les plus faibles mais par la prise en compte de l'ensemble des composants en interaction du système [Vil88]. Ainsi, c'est à partir des années 1960 que sont apparues de nouvelles méthodes et techniques de sûreté telles que l'Analyse des Modes de défaillances et de leurs Effets (AMDE), la méthode du Diagramme de Succès (MDS) ou la méthode de l'arbre de défaillances (AdD). Dès lors, la sûreté de fonctionnement

joue un rôle important dans la conception de nouveaux systèmes ainsi que dans la maintenance de ces systèmes en phase d'exploitation. Le souci de rentabiliser les investissements engagés pour produire des biens et des services a conduit à formaliser les notions de disponibilité, de maintenabilité et les concepts associés : testabilité, survivabilité, diagnostic, soutien logistique intégré [Zwi99]. Les années 80 et 90 ont été marquées par la prise en compte dans les études de sûreté de fonctionnement de la pénétration de l'informatique industrielle et des facteurs humains, avec l'apparition d'outils tels que les chaînes de Markov, les réseaux de Petri et les simulateurs d'accidents. Ces nouveaux aspects soulignent les efforts menés pour concevoir des systèmes toujours plus sûrs.

Les études de sûreté de fonctionnement visent à évaluer le comportement du système tout au long de son cycle de vie [Väl01]. Dès la phase de conception et de réalisation, la sûreté de fonctionnement spécifie les objectifs à atteindre en termes de durée de vie et de performances pour le système. Pendant la phase d'exploitation, et jusqu'à son démantèlement, la maintenance (préventive et corrective) permet d'obtenir, par retours d'expérience, les données de défaillances et de réparations des composants du système [Lyo00]. Ces données permettent d'améliorer et de concevoir des systèmes plus sûrs.

#### 1.4.1.2 Les paramètres de la sûreté de fonctionnement

[LAB+95] présente la sûreté de fonctionnement comme un arbre dont les feuilles sont les différents éléments qui la constituent. Cet arbre est illustré par la Figure 1.10.

La fiabilité, la maintenabilité, la disponibilité et la sécurité sont les quatre paramètres fondamentaux de la sûreté de fonctionnement. Ces paramètres permettent de définir les objectifs attendus d'un système et/ou d'évaluer la qualité du service délivré par le système afin de cibler les points critiques à améliorer. Ils se définissent de la manière suivante [Vil88], [Zwi99].

- La fiabilité (Reliability), notée R(t), est l'aptitude d'un système à accomplir une fonction requise dans des conditions d'utilisation données sur l'intervalle [0, t[. La probabilité R(t) se définit de la manière suivante :

$$R(t) = P\{Système\ non\ défaillant\ sur\ [0,t[\} \tag{1.1}$$

- La disponibilité (Availability), notée A(t), est l'aptitude d'un système à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné, en supposant que la fourniture des moyens extérieurs nécessaires de maintenance soit assurée :

$$A(t) = P\{Système\ non\ défaillant\ à\ l'instant\ t\} \tag{1.2}$$

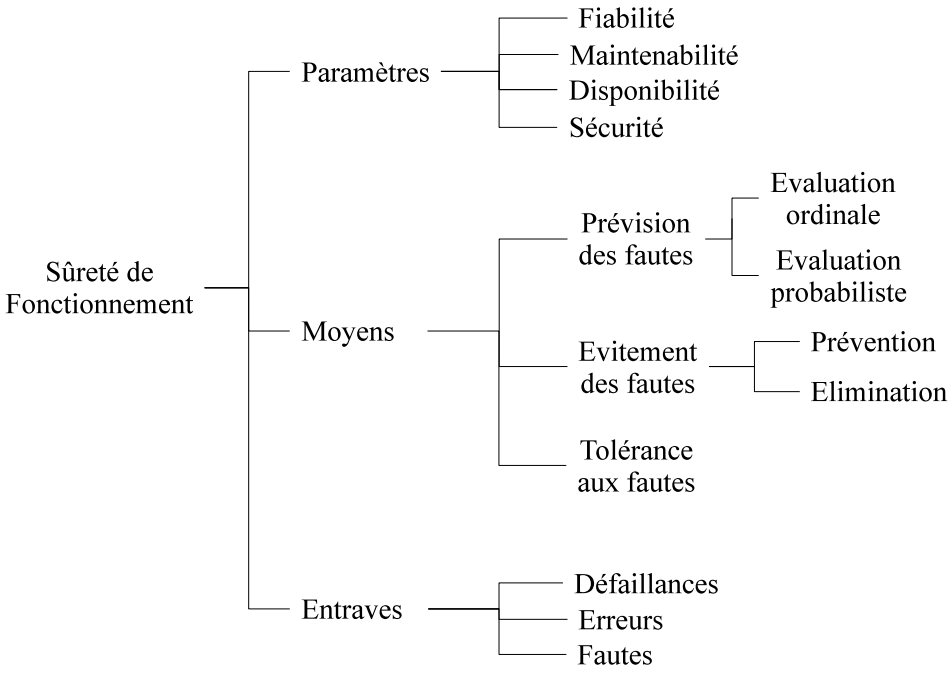


FIG. 1.10 – Arbre détaillé de la sûreté de fonctionnement.

– La maintenabilité (Maintainability), notée M(t), est l'aptitude d'un système à être maintenu dans un état dans lequel il peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits :

$$M(t) = P\{Système\ réparé\ au\ temps\ t\} \tag{1.3}$$

– La sécurité (Safety), notée S(t), est l'aptitude d'un système à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

$$S(t) = P\{Système\ sans\ défaillance\ catastrophique\ sur\ [0,t[\} \tag{1.4}$$

Ces quatre paramètres présentés précédemment sont dépendants les uns des autres comme le montre la figure 1.11 [CCCB04], [SB96a].

Ces dépendances sont les suivantes [CCCB04] :

– Diminuer la fiabilité du système entraîne une faible disponibilité (à cause de la présence de nombreuses défaillances) et a un impact sur le niveau de sécurité du système (une défaillance pouvant amener le système dans un état dangereux).
– Une maintenabilité inadéquate (dans le cas de systèmes réparables) peut compromettre la disponibilité du système (à cause de l'augmentation du nombre de défaillances di-

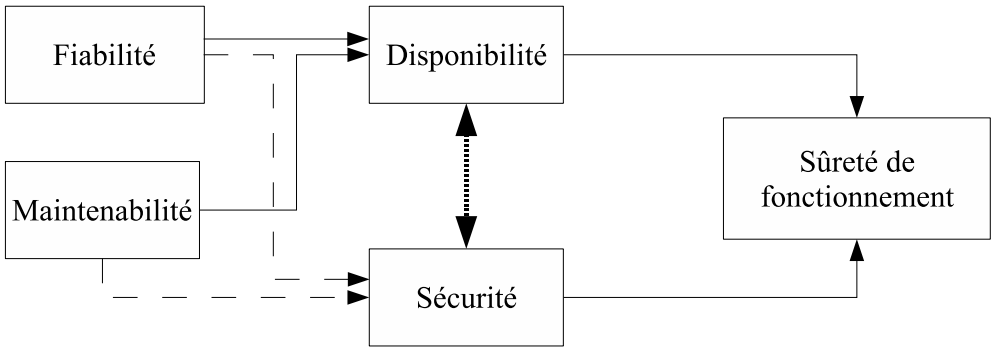


FIG. 1.11 – Interdépendance des paramètres fondamentaux de la sûreté de fonctionnement.

verses) et la sécurité du système (à cause de l'augmentation du risque d'accident).
- Augmenter le niveau de sécurité du système (par l'ajout de multiples éléments de sécurité) réduit sa disponibilité (le système stoppe intempestivement dès la première défaillance) tandis que l'augmentation du niveau de disponibilité est obtenue au détriment du niveau de sécurité [Hol99], [Cab99].

#### 1.4.1.3 Les moyens de la sûreté de fonctionnement

Les techniques et méthodes actuelles, permettant le développement d'un système sûr de fonctionnement constituent différents *moyens* appliqués à chaque phase du cycle de vie du système : des spécifications et à la conception, en passant par la réalisation et l'exploitation, jusqu'à la mise hors service et le démantèlement du système. Ces moyens agissent sur les *fautes*, les *erreurs* et les *défaillances*. Ces dernières rendent inacceptable le service d'un système et sont qualifiées d'*entraves* à la sûreté de fonctionnement.
D'après la figure 1.10, les moyens de la sûreté de fonctionnement sont classés en trois catégories [LAB+95] :

- La **prévision des fautes**. Elle permet d'estimer l'occurrence et les conséquences des fautes par des évaluations ordinales (identification et classement des fautes) ou probabilistes.
- L' **évitement des fautes** par la prévention et l'élimination des fautes. La prévention permet d'éviter l'occurrence ou l'introduction de fautes en phase de spécification et de conception. L'élimination permet la correction des fautes par des techniques de vérification, par des techniques de test, ou par des techniques de diagnostic.
- La **tolérance aux fautes**. Elle permet au système de fournir un service malgré les fautes, le mode de fonctionnement du système est alors qualifié de *mode dégradé*. Elle utilise des techniques de recouvrement d'erreur de trois types :
  - Par reprise. Le système est ramené à un point de fonctionnement avant l'erreur.

- Par poursuite. Le système est amené dans un nouvel état à partir duquel il peut continuer son fonctionnement.
- Par compensation. Le système fournit son service malgré les fautes grâce à l'utilisation de redondances matérielles et/ou logicielles.

#### 1.4.1.4 Terminologie relative à la sûreté de fonctionnement

#### 1.4.1.5 Notions de défaillance, erreur et faute

La sûreté de fonctionnement possède de nombreux concepts puisqu'elle inclut la connaissance, l'évaluation, la prévision et la maîtrise des défaillances. Selon [LAB+95], la sûreté de fonctionnement a pour objectif de spécifier, concevoir, réaliser et exploiter des systèmes où la faute est naturelle, prévue et tolérable.
Une **faute** est la cause première d'une erreur. Lorsqu'elle se manifeste, elle est susceptible de générer de nouvelles erreurs [Lor05].
Un système ou un sous-système est déclaré en **erreur** s'il ne répond plus au besoin qui lui est associé [Lor05] et si cette erreur est susceptible d'entraîner une défaillance [Beu06].
Un système qui ne fournit plus la fonction pour laquelle il a été conçu est déclaré comme **défaillant**. Selon la définition de la Commission Electrotechnique Internationale, la défaillance est la *fin de l'aptitude d'un dispositif à accomplir sa fonction requise.*
Un composant peut devenir défaillant suite à la succession d'événements observables ou non classés parmi les fautes et les erreurs. Ces événements ne conduisent pas nécessairement à un comportement défaillant car cela dépend de la composition du système (existence de redondance, capacité du système à compenser ces fautes ou erreurs).

#### 1.4.1.6 Notion d'événement redouté

Nous allons appeler Evénement Redouté (ER), les conséquences de l'occurrence d'une seule défaillance ou d'une séquence de défaillances amenant le système dans une situation de blocage en l'absence de réparation (cas du système non réparable) [Sch04].

Ce terme restera volontairement assez général et pourra désigner une des situations suivantes :

- *événement indésirable* : c'est un événement ne devant pas se produire ou devant se produire avec une probabilité moins élevée au regard d'objectifs de sûreté de fonctionnement. Par exemple nous pouvons citer le cas de l'alarme intempestive.
- *événement critique* : c'est un événement qui entraîne la perte d'une ou de plusieurs fonctions du système ce qui provoque des dommages importants au système ou à l'environnement mais ne présente qu'un risque négligeable de mort ou de blessure.
- *événement catastrophique* : c'est un événement qui occasionne la perte d'une ou de plusieurs fonctions essentielles du système en causant des dommages importants au

système ou à l'environnement et pouvant entraîner pour l'homme la mort ou des dommages corporels. Il est important de préciser que les événements qualifiés de catastrophiques sont surtout exploités dans l'aéronautique et dans le ferroviaire.

Ainsi, l'événement redouté permet de considérer les paramètres FMDS de la sûreté de fonctionnement de façon plus qualitative et plus compréhensible [CCB07]. Par exemple, les événements redoutés "impossibilité d'achever la mission", "arrêt inattendu" ou "comportement dangereux" sont relatifs respectivement aux paramètres de disponibilité, fiabilité et sécurité.

#### 1.4.1.7 Notion de système sûr

Nous allons utiliser la définition de [CB06b] du système sûr : "un système sûr est un système qui accomplit ce pourquoi il a été conçu, sans incident réduisant sa disponibilité et sans accident réduisant sa sécurité". Comme les paramètres disponibilité et sécurité sont dépendants des paramètres de maintenabilité et de fiabilité d'après la figure 1.12 [SB96a], la conception d'un système sûr nécessite de trouver le meilleur compromis disponibilité-sécurité et donc intrinsèquement fiabilité-maintenabilité.

### 1.4.2 Vers une architecture matérielle plus sûre

#### 1.4.2.1 Généralités

Toute architecture matérielle contient des fautes qui se manifesteront potentiellement par l'apparition de défaillances au cours de la vie opérationnelle du système. Il est donc important d'évaluer les conséquences de ces défaillances grâce à des méthodes adaptées et de déterminer l'architecture optimale (c'est-à-dire le meilleur agencement de composants) correspondant aux exigences de sécurité et de disponibilité. Le concepteur dispose de moyens permettant a priori d'éviter les fautes mais engendrant des coûts prohibitifs : choix de composants de qualité ayant une solidité intrinsèque supérieure aux composants standards (technique également appelée *durcissement d'un composant*), utilisation de composants autotestables, utilisation de méthodes formelles ... [Aub87], [Sch04].

Le concepteur peut également introduire des mécanismes de tolérance aux fautes afin d'éviter que des erreurs ou des fautes entraînent une défaillance du système. Ces techniques sont basées sur le principe de la redondance, ce dispositif est constitué de manière générale par :

- un élément primaire dont on peut tolérer les erreurs,
- un élément redondant pouvant réaliser tout ou une partie des fonctions de l'élément primaire,
- un élément de détection,
- un dispositif de réaction à cette erreur.

L'erreur peut alors être confinée, corrigée, ou bien l'élément défaillant peut être remplacé par un élément redondant suite à la reconfiguration du système. Dans [LAB+95] est détaillé un certain nombre de stratégies de reconfiguration pouvant être mises en oeuvre suite à la détection d'une erreur.

Il existe deux types de redondances [Aub87] :

- La redondance active : le nombre d'éléments redondés peut être important et chacun d'entre eux participe à la réalisation de la fonction. Il s'agit, entre autres, de dispositifs de vote majoritaire, pour lesquels le résultat final issu du vote résulte de la comparaison entre les différentes sorties des éléments redondés.
- La redondance passive : l'élément redondant ne participe à la fonction qu'après détection et réaction à l'erreur.

Il est à noter ici qu'il existe également les défaillances liées au logiciel qui constituent une problématique importante mais qui ne seront pas traitées dans le cadre de ces travaux. Le lecteur intéressé pourra se reporter à [Arl95] qui présente les conditions de vérification et d'élimination de fautes logicielles ou encore à [SL02] qui présente une technique de vérification formelle du comportement des portes d'un métro.
Nous allons présenter les défaillances matérielles que l'on peut rencontrer au sein d'un système d'automatisation ainsi que les principales stratégies de reconfiguration associées.

#### 1.4.2.2 Les défaillances liées au matériel et les stratégies de reconfiguration

Les équipements d'un système sont soumis à un stress important de la part de l'environnement qui constitue la principale cause de défaillance : humidité, vibration, température, champ électromagnétique ...

Nous allons passer en revue les principales sources de défaillances au sein d'un système d'automatisation [Zie96] :

1. *Les capteurs.* Les principaux modes de défaillance habituellement considérés sont la défaillance en valeur (les données sont erronées), la défaillance temporelle (l'information capteur n'est pas envoyée à temps) et la défaillance par arrêt (le capteur n'envoie plus de données, ou reste figé à une valeur constante).
   Les méthodes de tolérance permettant d'assurer une continuité du fonctionnement en présence de ces modes sont :
   - La réplication du capteur : elle permet de tolérer des fautes intermittentes et permanentes qui sont dues à des défaillances en valeur ou par arrêt. Cette réplication peut être matérielle ou logicielle (observateurs, estimateurs).
   - La relecture du capteur : elle permet surtout de tolérer des fautes transitoires dues à des défaillances en valeur ou temporelles.

2. *Les actionneurs*. Les modes de défaillance considérés sont : la défaillance en valeur (l'actionneur agit de façon trop forte ou trop faible), la défaillance temporelle (il agit avec un décalage temporel) et la défaillance par arrêt (l'actionneur ne fait plus aucune action, ou une action constante). La technique de tolérance la plus courante consiste à introduire une des deux structures suivantes :
   - Deux actionneurs sont mis en série : par exemple deux actionneurs sont nécessaires pour effectuer l'action souhaitée ; cette technique permet de réduire la probabilité de déclenchement intempestif de l'action si l'un des actionneurs est défaillant.
   - Deux actionneurs sont mis en parallèle : un seul actionneur est nécessaire pour effectuer l'action souhaitée ; cette technique permet de tolérer une défaillance par arrêt de l'un des actionneurs.
3. *Les unités de traitement* : ces composants sont en général plus fiables que les capteurs et les actionneurs. Néanmoins, leur complexité rend difficile la connaissance des nombreux modes de défaillances possibles. De nombreuses techniques de traitement d'erreur sont alors utilisées. Les unités de traitement permettent également de diagnostiquer la présence d'erreurs dans leur propre système par des contrôles d'erreur ou encore par la duplication et la comparaison d'informations. Le lecteur intéressé pourra se référer à [LAB+95] pour des compléments d'informations.

Du fait de sa complexité et bien qu'il existe des techniques matérielles permettant de rendre un système plus sûr, nous allons voir dans le paragraphe suivant que l'évaluation de la sûreté de fonctionnement du système d'automatisation est problématique et fait l'objet de nombreux travaux de recherche. De ce constat, nous présenterons nos besoins en une méthodologie de conception de systèmes d'automatisation sûrs de fonctionnement.

### 1.4.3 Nécessité d'une méthodologie de conception de systèmes d'automatisation sûrs de fonctionnement

#### 1.4.3.1 Besoins premiers

Avant l'ère des systèmes mécatroniques (constitués d'éléments électriques, mécaniques, pneumatiques), un système était conçu de façon à remplir une mission bien définie afin de répondre à des besoins nouveaux de productivité, et/ou à plus faible coût. Chaque fonction pouvait être étudiée et développée indépendamment des autres et l'implication de la sûreté de fonctionnement se résumait à la réutilisation des modèles initiaux complétés des données issues du retour d'expérience afin de répondre aux normes de sécurité.
Cependant, cette approche ne permettait pas de prendre en compte les risques inhérents à un nouveau système exploitant des technologies différentes et de complexité accrue dès les premières phases de conception. En effet, le choix d'une architecture fonctionnelle et

matérielle se limitait uniquement à la bonne tenue de performances locales (rendement, coût ...) et les objectifs de sûreté de fonctionnement n'étaient appliqués qu'en fin de cycle de conception lorsque les choix technologiques étaient effectués et de ce fait difficilement réversibles.
Le choix d'une architecture matérielle en phase de conception doit tenir compte des performances à accomplir mais doit être également lié à des objectifs globaux intégrant la sûreté de fonctionnement. Les performances de sûreté de fonctionnement doivent être formulées au niveau le plus haut, c'est-à-dire au niveau du système complet puis déclinées à des niveaux inférieurs (sous-systèmes, composants) suivant la structure du dit système.
Par conséquent, la démarche de sûreté de fonctionnement au niveau global du système se résume dans la démarche suivante :

- Analyse des risques visant à identifier les événements redoutés critiques pour la sécurité et la disponibilité.
- Etude de la sûreté de fonctionnement par des méthodes et outils adaptés.
- Choix des actions correctives à implanter suivant les objectifs de sûreté exprimés dans le cahier des charges.

La définition d'une méthodologie orientée sûreté de fonctionnement permet d'identifier au plus tôt les risques potentiels, de les classer et d'envisager des actions correctives avant que les choix de conception ne soient figés. Une telle démarche permet également de justifier au plus tôt, à l'aide de l'évaluation d'un niveau de sûreté de fonctionnement, le choix d'une architecture matérielle répondant aux critères de sûreté avant que la complexité du modèle, encombré par un niveau de détails trop fin, ne nuise à la compréhension globale du système. L'évaluation de la sûreté de fonctionnement effectuée dès la phase de conception permet ainsi d'éviter, ou tout du moins de réduire le nombre de modifications tardives et donc coûteuses lors de la réalisation finale du système. Bien qu'il existe des techniques permettant de rendre un système plus sûr, l'évaluation du niveau de sûreté de fonctionnement des SAID permettant de garantir un niveau minimal n'est pas aisée compte tenu de leur complexité et de leur multiples possibilités de conception.

Issus de ce constat, de nombreux travaux tentent de proposer des solutions permettant de concevoir des systèmes d'automatisation sûrs de fonctionnement. Les travaux de [ECAY03] et de [KPTH01] concernent les systèmes ayant une architecture prédéfinie ou des systèmes spécifiques (parallèle-série, série-parallèle, ...). Peu de travaux concernent la conception de l'architecture matérielle [MBCC06]. Dans [CB06a], l'architecture opérationnelle est déterminée à partir de l'architecture fonctionnelle et d'une architecture matérielle surdimensionnée en évaluant la disponibilité et la fiabilité puis en sélectionnant la solution qui maximise ces paramètres tout en minimisant le coût de la solution. L'approche de [CCCB04] présentée figure 1.12 propose une démarche d'obtention de l'architecture opérationnelle

intégrant dès la phase de conception les contraintes liées aux paramètres de la sûreté de fonctionnement.

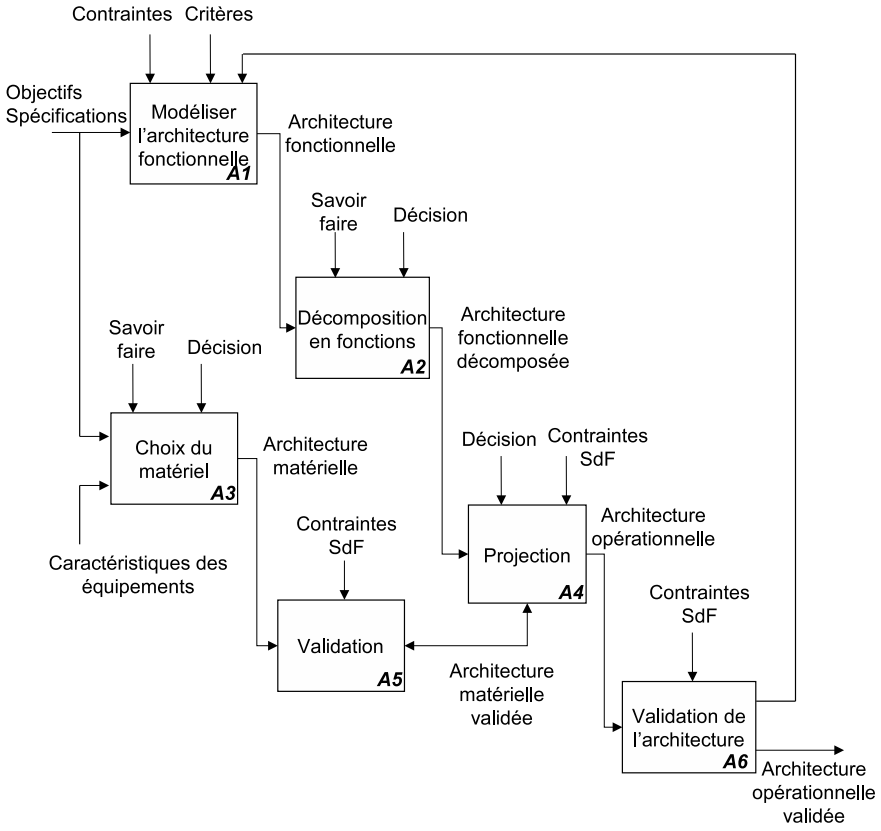


FIG. 1.12 – Démarche d'obtention d'une architecture opérationnelle

Selon la figure 1.12, les objectifs de sûreté de fonctionnement, les contraintes et les spécifications fonctionnelles du système à concevoir sont définis dans le cahier des charges et permettent de modéliser son architecture fonctionnelle (Figure A1). Les fonctions du système sont décomposées en sous-fonctions et fonctions élémentaires nécessaires à la réalisation de ces fonctions (Figure A2). L'architecture matérielle est le résultat de choix effectués sur des ressources matérielles à incorporer au système (Figure A3). Les choix de cette architecture peuvent être également améliorés par l'application de contraintes (de sûreté de fonctionnement par exemple mais d'autres également, Figure A5). La projection de l'architecture fonctionnelle sur l'architecture matérielle permet par agrégations successives de déduire une architecture opérationnelle du système (Figure A4). Cette architecture opérationnelle est ensuite validée par rapport aux objectifs fixés dans le cahier des charges (Figure A6). Les objectifs de sûreté de fonctionnement peuvent servir à valider cette architecture. Selon les résultats obtenus, l'architecture opérationnelle proposée est soit validée soit modifiée afin d'atteindre les performances exigées dans le cahier des charges. Cette modification peut se

faire de plusieurs façons :

- Soit en introduisant de nouvelles exigences aux différentes fonctions de l'architecture fonctionnelle.
- Soit en introduisant des éléments ayant des performances améliorées (taux de fiabilité par exemple ...).
- Soit en redondant les différents éléments matériels existants.

Cependant, cette méthode nécessite des données de fiabilité validées pour les critères de comparaison puis de choix du système optimal. Dans notre recherche, ces critères sont le coût financier et le niveau de sûreté de fonctionnement du système à concevoir. Si le premier critère relatif au coût financier peut être approximé par la somme des coûts individuels des composants, le critère sûreté de fonctionnement est de par sa nature plus délicat à quantifier. En effet, il doit rendre compte des différents aspects que sont la fiabilité, la disponibilité, la maintenabilité et la sécurité. Chacun de ces paramètres peut être quantifié comme nous l'avons vu dans le paragraphe 1.4.1.2 (R(t), A(t), M(t), probabilité d'occurrence d'accident, taux de défaillance, ...). Cependant l'utilisation des nouvelles technologies innovantes et des composants programmables aux multiples modes de défaillance parfois mal connus, rend difficile l'accès aux données de fiabilité pour le concepteur et leur validation. Par ailleurs, l'environnement (vibrations, CEM, poussière, température) et le choix de la politique de maintenance (souvent déterminé tard dans la démarche de conception) ont une forte influence sur la fiabilité ou la disponibilité des composants employés (taux de défaillance non constant, ...).

#### 1.4.3.2 Intérêt d'intégrer des scénarios pour l'évaluation de la sûreté de fonctionnement

Nous proposons d'évaluer, à l'aide de paramètres que nous allons définir, les scénarios d'un système afin de quantifier son niveau de sûreté de fonctionnement. Un scénario sous-entend un début, une fin et une histoire qui décrit l'évolution d'un système. Dans le contexte de la sûreté de fonctionnement, un scénario mène à un état catastrophique ou dangereux : c'est l'état final (ou *événement redouté*). L'état initial est un état de bon fonctionnement du système. Le scénario décrit comment le système quitte le bon fonctionnement pour évoluer vers un fonctionnement défini comme dangereux. Le scénario doit décrire cette évolution de manière précise pour la compréhension et de manière concise. Un scénario est ainsi vu comme une description du système sous la forme d'un changement d'état (état initial vers état final) et d'une suite d'événements qui mènent à l'événement redouté. Le scénario est une explication claire des raisons pour lesquelles le système s'est trouvé ou risque de se trouver dans un état final donné. C'est une séquence de différents événements comportant un ordre d'apparition précis. Le scénario se différencie ainsi de la *coupe*. Une coupe est définie dans [Mor01] comme "une combinaison sans lien de causalité d'événements et de conditions

suffisantes pour provoquer l'état final étudié" et dans [HLA+07] à l'aide d'une fonction de structure (fonction qui représente la relation entre la défaillance du système et la défaillance de ses composants et qui peut prendre plusieurs formes, des formes analytiques et des formes graphiques) :
Soit S un système à état binaire, il fonctionne (état de marche) ou ne fonctionne pas (état de panne). Supposons que S est composé de r composants $e_i$ (à état binaire également) et que son état ne dépende que de l'état de ces r composants. Ces états sont représentés avec la notation suivante [KGC75] :

- $e_i$ : les composants et e = $\{e_1,e_2,...,e_r\}$ l'ensemble des r composants.
- $x_i$ : la variable d'état du composant $e_i$ : $x_i = 1$ si $e_i$ fonctionne ; $x_i = 0$ si $e_i$ est défaillant.
- x = $\{x_1,x_2,...,x_r\}$ est le r-uple état de l'ensemble des composants ($x \in \{0,1\}^r$) qui peut prendre $2^r$ valeurs différentes.
- y : la variable d'état du système S de fonction de structure $y = \varphi(x)$ tel que : y = 1 si le système fonctionne ; y = 0 s'il est en panne.

Une *coupe* est un sous-ensemble de composants a $\in$ e dont la défaillance entraîne la défaillance du système (y = 0), les autres composants étant en état de fonctionnement.

L'intérêt d'utiliser des scénarios plutôt que des coupes vient du fait que les scénarios permettent d'améliorer la modélisation du comportement dysfonctionnel d'un système complexe et d'évaluer le niveau de sûreté de fonctionnement de ce système de manière beaucoup plus précise. En effet, un scénario (ou une séquence d'événements) peut conduire à un événement redouté alors que les mêmes événements se produisant dans un ordre différents n'y conduisent pas. Cela est notamment dû à l'agencement des composants dans l'architecture [CHCC07a] et au comportement du système.
L'exemple du système de régulation du niveau d'une cuve permet d'illustrer cette limite.

La figure 1.13 présente une architecture possible dont le niveau de sûreté de fonctionnement doit être évalué. L'architecture utilise deux détecteurs standards de niveau d'eau C1 et C2 mesurant le niveau d'eau de la cuve, cette cuve est reliée à un processus qui nécessite d'avoir un niveau d'eau minimal détecté par C1 pour fonctionner. C1 actionne une pompe de remplissage si le niveau d'eau est insuffisant. Le détecteur C2, quant à lui, est en redondance passive avec C1, c'est-à-dire que C2 ne participe à la fonction de mesure qu'après détection de la défaillance de C1. La commutation d'un détecteur à un autre est supposée immédiate. On considère maintenant l'événement redouté *Débordement de la cuve* qui caractérise le niveau de sécurité du système de régulation. Les détecteurs ont pour mode de défaillance une détection continuellement passive notée *CP*, c'est-à-dire que le détecteur ne détecte pas de niveau d'eau en présence d'un niveau.

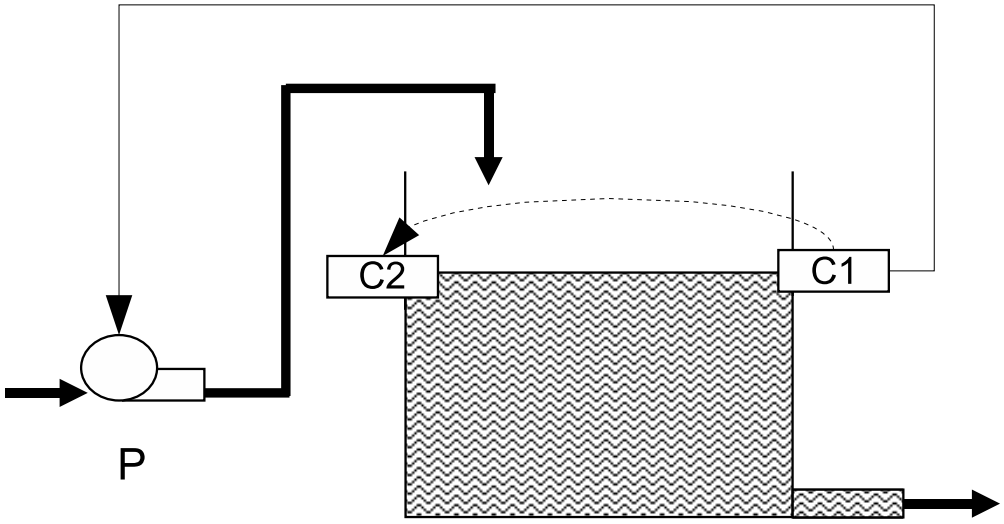


FIG. 1.13 – Systèmes de régulation d'une cuve

| Liste des coupes | Liste des scénarios |
|---|---|
| $\{C1_{CP}, C2_{CP}\}$ | $[C1_{CP}, C2_{CP}]$,$[C2_{CP}, C1_{CP}]$ |

TAB. 1.3 – Liste des coupes et des scénarios de la figure 1.13 amenant au débordement de la cuve

Les coupes et les scénarios amenant au débordement de la cuve sont déterminés et regroupés dans le tableau 1.3.

D'après ce tableau, l'évaluation de l'architecture détermine une coupe d'ordre 2. Cette coupe permet d'en déduire deux scénarios menant à un débordement de la cuve. Or, lorsque l'on détaille ces scénarios, on constate que le scénario $[C2_{CP}, C1_{CP}]$ est impossible du fait de la redondance passive entre C2 et C1. Une évaluation utilisant directement des scénarios et non des coupes aurait abouti à la détermination d'un seul scénario pour ce système. Par ailleurs, la probabilité d'occurrence de cet événement redouté en utilisant les coupes aurait été deux fois plus forte par rapport à une évaluation utilisant directement les scénarios. De ce fait, l'évaluation du niveau de sûreté de fonctionnement basée sur les coupes amène à une mauvaise quantification. Cette mauvaise quantification peut conduire à une erreur de conception par le choix d'un système moins robuste que prévu.

En résumé, un scénario permet de décrire l'évolution de certains composants du système à partir d'un état de bon fonctionnement jusqu'à l'occurrence de l'événement redouté tout en tenant compte du comportement du système d'automatisation. L'évaluation directe des scénarios constitue un moyen supplémentaire et efficace d'accroître la précision d'évaluation du niveau de sûreté de fonctionnement d'un système en éliminant les séquences impossibles.

#### 1.4.3.3 Les besoins liés au développement d'une méthodologie de conception de systèmes sûrs

Comme nous l'avons vu dans les sections précédentes, le développement d'une méthodologie de conception de systèmes d'automatisation sûrs de fonctionnement impose le besoin d'utiliser les scénarios afin d'évaluer au mieux le système. Cette méthodologie doit, de ce fait, intégrer :

- des outils de modélisation et d'évaluation rapides utilisant les scénarios redoutés. Ces outils permettront de :
  - Construire graphiquement un modèle fonctionnel basé sur une décomposition fonctionnelle hiérarchique.
  - Prendre en compte, à partir de ce modèle, les nombreuses possibilités de conception de l'architecture matérielle ainsi que les différentes technologies utilisées.
  - Construire un modèle dysfonctionnel basé sur les arbres de défaillances.
- des algorithmes d'optimisation adaptés à l'utilisation des scénarios pour la recherche d'architectures optimales et permettant de déterminer un ensemble de solutions optimales.
- des critères pour l'évaluation et l'optimisation des architectures matérielles possibles. Ces critères sont de deux types :
  - le coût financier des architectures proposées.
  - le niveau de sûreté de fonctionnement de ces mêmes architectures évalué à l'aide des scénarios.

Nous allons voir dans la section suivante l'inadéquation des méthodes d'évaluation de la sûreté de fonctionnement avec ces besoins.

## 1.5 Problématique sur l'évaluation de la sûreté de fonctionnement

Lors de la conception du système d'automatisation, l'évaluation (c'est-à-dire la quantification de paramètres) du niveau de sûreté de fonctionnement de ce système peut-être réalisée à l'aide de nombreux outils et méthodes analytiques. De nombreux travaux de recherche [KH96], [RH04] et la norme internationale dédiée à la sûreté de fonctionnement [IEC03] décrivent la plupart de ces méthodes. La simulation et la méthode d'analyse par arbres de défaillances sont les plus répandues dans les études de sûreté de fonctionnement.

L'évaluation du niveau de sûreté de fonctionnement d'un système d'automatisation est réalisée selon des besoins fixés lors de la première étape d'un cycle de développement. Lors de l'évaluation de ce niveau pendant l'activité de conception, le concepteur étudie une ou

plusieurs architectures opérationnelles par rapport à la capacité de celles-ci à gérer et à tolérer un certain nombre de défaillances de composants. Une telle évaluation doit aider le concepteur à trouver le meilleur compromis entre une solution robuste (tolérante à un nombre précis de défaillances, reconfigurable ...) et le coût engendré par ces solutions.
Parmi les nombreuses méthodes d'évaluation probabilistes existantes, deux catégories de méthodes sont à distinguer : les méthodes basées sur une approche analytique et les méthodes basées sur une approche expérimentale [LAB+95]. Ces deux approches exploitent des modèles ayant un niveau d'abstraction du système plus ou moins grand. Les méthodes analytiques comme les graphes de Markov et les arbres de défaillances reposent sur la construction d'un modèle graphique qui, après traitement, fournit l'ensemble des grandeurs recherchées. Les méthodes expérimentales s'appuient sur l'observation du comportement du système en cours de fonctionnement. Le modèle utilisé est soit empirique (un modèle de simulation), soit physique (étude d'un prototype ou d'un système réel). Le niveau de détail de ces modèles est donc plus grand et reflète plus fidèlement le fonctionnement réel du système. Les techniques d'injection de fautes ou de simulation (par exemple la simulation de Monte-Carlo) entrent dans cette catégorie. Les niveaux de sûreté de fonctionnement sont estimés à partir d'un traitement statistique des résultats.
Nous allons présenter quelques exemples de techniques issues de ces deux catégories de méthode et expliquer leurs limites par rapport à nos besoins de conception et d'évaluation par scénarios.

### 1.5.1 Les méthodes basées sur une approche expérimentale

La simulation permet, en principe, d'étudier des modèles d'un système avec n'importe quel niveau de détail. Cependant, en pratique, il n'est pas toujours possible d'étudier un modèle très détaillé à cause de limitations dues au matériel employé. En effet, les simulations sont souvent gourmandes en ressources (mémoire vive de l'ordinateur par exemple) et en temps de calcul lorsque les modèles utilisés sont très réalistes ou bien si l'on souhaite obtenir des résultats avec une précision élevée.

**Simulation de Monte Carlo** Les simulations de Monte Carlo englobent toutes les méthodes qui utilisent des variables aléatoires ou pseudo-aléatoires pour modéliser les systèmes. Le système lui-même peut être déterministe ou stochastique [ID01].
C'est une méthode numérique basée sur le tirage de nombres aléatoires. La quantité que l'on désire estimer correspond à l'espérance mathématique d'une variable aléatoire. Le principe consiste à étudier l'évolution d'un système en simulant un modèle représentant le comportement du système au cours de ce que l'on appelle un scénario ou une histoire.
La quantification de la grandeur recherchée, (par exemple la fiabilité ou la probabilité d'ap-

parition d'un événement redouté) est alors basée sur l'étude d'un certain nombre de scénarios différents, permettant d'en extraire des résultats statistiques (estimateurs).
Pour effectuer une estimation de la probabilité d'apparition d'un événement redouté, on peut associer un estimateur de type binaire à cette probabilité et incrémenter un compteur d'une unité pour chaque histoire dans laquelle l'événement redouté se produit. L'estimation de la probabilité est alors obtenue en faisant le rapport entre le nombre d'histoires ayant connu un événement redouté et le nombre total d'histoires [LK02].

L'avantage de ce type d'approche est la possibilité de simuler des systèmes complexes et/ou de grande taille bien que la modélisation de ces systèmes reste un problème.
Cependant, dans le cadre de la sûreté de fonctionnement, le modèle simulé est régi par des événements très rares (les défaillances) et des événements très fréquents (événements internes de la partie contrôle commande et du processus physique), et ce simultanément. La simulation est alors cadencée par de nombreuses occurrences d'événements fréquents qui ne reflètent pas le comportement du système en présence de défaillances. C'est le problème de simulation des événements rares. Un nombre important d'histoires est nécessaire pour voir apparaître un événement redouté, impliquant des temps de calcul importants. Ces temps deviennent faramineux si, en plus, on souhaite obtenir un intervalle de confiance acceptable.

De nombreuses techniques d'accélération de la simulation permettent de réduire ces temps. Elles sont basées soit sur une diminution de la complexité du modèle, soit sur la réduction du nombre de scénarios à simuler, par exemple en favorisant l'apparition des événements rares [Gar98]. Cependant, ces méthodes ne sont pas toujours faciles à mettre en oeuvre et/ou ne fournissent pas forcément des estimations de qualité [Sch04].

### 1.5.2 Les méthodes basées sur une approche analytique

Les méthodes analytiques sont décomposables en deux classes : les approches statiques basées sur les diagrammes de fiabilité et les arbres de défaillances classiques et les approches dynamiques basées sur les arbres de défaillances dynamiques et les graphes de Markov. Les évaluations quantitatives ont pour but de caractériser formellement la nature aléatoire des phénomènes engendrant les défaillances. Ainsi les changements d'états, les dates d'occurrence des défaillances ou d'autres événements non déterministes sont formalisés mathématiquement et étudiés à l'aide de processus stochastiques.

#### 1.5.2.1 Les approches statiques

**Diagramme de fiabilité** La méthode d'analyse par des diagrammes de fiabilité, également appelée diagrammes de succès, est une des plus anciennes méthodes pour estimer la

fiabilité des systèmes non-réparables où il y a une faible interaction entre les composants. Le diagramme de fiabilité est une représentation graphique du comportement fonctionnel d'un système [Vil88].
Ce graphe se compose d'un ensemble de blocs représentatifs de la réalisation d'une fonction par un composant. Leurs interconnexions décrivent les liens fonctionnels entre les composants permettant le succès quant à la réalisation de la mission du système. Plus explicitement, le système est en état d'accomplir sa mission, s'il existe un chemin, menant de l'entrée à la sortie, sachant que la panne d'un composant interdit de traverser le bloc auquel il est associé. La figure 1.14 présente un exemple de diagramme de fiabilité d'un système utilisant 5 composants. La combinaison des pannes (c'est-à-dire la coupe) des composants E1 et E2 entraîne la panne de ce système puisqu'il n'existe pas de chemin menant de l'entrée à la sortie.

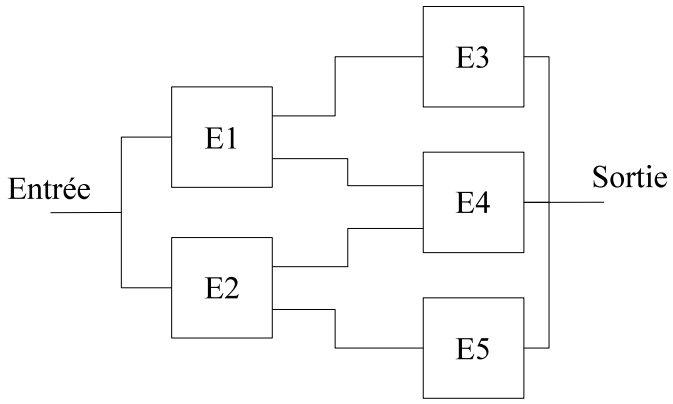


FIG. 1.14 – Exemple de diagramme de fiabilité d'un système utilisant 5 composants

L'approche par les diagrammes de fiabilité a l'avantage d'être facilement compréhensible. Mais la simplicité des modèles construits limite leur analyse à l'étude de combinaisons de pannes (coupe) sans tenir compte de leur ordre d'apparition. De plus, il est impossible ou très difficile de considérer différents modes de défaillance des composants.

**Arbre de défaillances classiques** La méthode d'analyse par arbre de défaillances (ou AdD), également appelée arbre des causes, permet de représenter graphiquement les combinaisons d'événements qui conduisent à la réalisation d'un événement redouté, aussi appelé événement non souhaité (ENS). Il se construit de manière déductive par la constitution d'événements générés à partir des événements de niveau inférieur par l'intermédiaire de portes logiques. Ce processus déductif est poursuivi jusqu'à l'obtention des événements indépendants et élémentaires. Ces événements élémentaires peuvent être des pannes, des erreurs humaines, des perturbations, ...
Le but de cette construction est d'en extraire une formule booléenne (une fonction de structure), permettant d'expliciter l'ensemble des combinaisons minimales d'événements qui

mènent au sommet de l'arbre (des coupes minimales) et ainsi d'identifier les composants ou les parties du système qui sont sensibles ou susceptibles de causer la perte du système. L'AdD permet ainsi de calculer les valeurs statistiques classiques de la sûreté de fonctionnement comme la disponibilité, la fiabilité et tous les temps moyens caractéristiques du modèle (Mean Time Between Failures, ...). Les calculs peuvent se faire par l'évaluation des coupes minimales puis par l'application d'une technique de disjonction de ces coupes ou bien en une seule étape si l'on traduit la formule booléenne de l'arbre de défaillances sous forme de diagrammes de décision binaire (ou BDD). Les BDD sont des structures de données qui permettent un codage optimal de fonctions booléennes et peuvent se construire à partir de la décomposition de Shannon. On distingue deux types d'AdD : les arbres classiques statiques [Vil88] dont la figure 1.15 présente un exemple et les arbres dynamiques [CM02], [MDCS98] présentés dans le paragraphe des approches dynamiques.

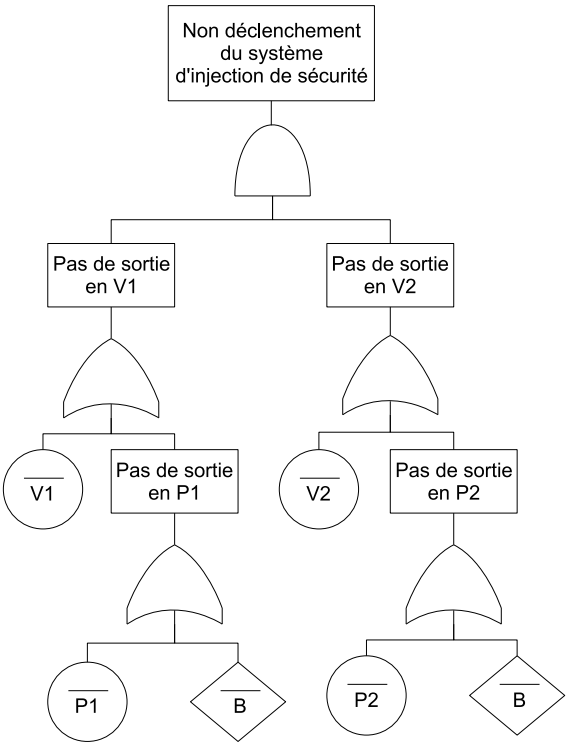


FIG. 1.15 – Arbre des défaillances du système d'injection de sécurité d'une centrale nucléaire selon [Vil88]

Comme nous venons de le voir, l'AdD sous sa forme classique est une représentation statique d'un système. Plusieurs variantes existent comme les arbres dits cohérents ou avec restriction. L'arbre est constitué d'événements de base, d'événements dits *maison* qui ne sont pas des événements dysfonctionnels et qui permettent de représenter différentes configurations du système étudié, et de portes logiques. Ces portes logiques permettent de modéliser, entre autre, des conjonctions ou des disjonctions d'événements, des votes k/n mais également

des délais ou des portes matricielles. L'ensemble de ces constituants sont des blocs de formes normalisées.
Comme pour le diagramme de fiabilité, l'approche par AdD a l'avantage d'être facilement compréhensible par des personnes autres que le créateur même de l'arbre mais de par sa construction, l'arbre classique possède un certain nombre de limites trop fortes dans le cadre des analyses que nous souhaitons mener. L'arbre est la représentation d'une formule booléenne sous forme de graphe et ne tient donc pas compte de l'ordre d'apparition des événements et des dépendances fonctionnelles, caractéristiques pourtant très importantes dans les systèmes physiques [SS99], [KS03]. Afin de combler ces lacunes, de nouvelles méthodes intégrant les scénarios ont été étudiées au sein des approches dynamiques.

#### 1.5.2.2 Les approches dynamiques

**L'approche Markovienne** Les processus de Markov sont couramment utilisés pour l'étude des systèmes de production (définition d'une politique de maintenance par exemple dans [Amo99a]) et dans le domaine de la sûreté de fonctionnement. En effet, l'approche markovienne reste séduisante de par sa simplicité conceptuelle, par la possibilité de représentation graphique simple sous la forme d'un graphe d'états et par l'étude des propriétés géométriques et analytiques. Dès lors que les hypothèses markoviennes sont vérifiées, la mise en équation du problème permet une résolution analytique exacte et rigoureuse par opposition à une évaluation statistique qui ne fournit qu'une estimation de la solution recherchée. De plus, les processus de Markov permettent de modéliser fidèlement un grand nombre de systèmes lorsque ces derniers possèdent un nombre d'états pas trop important.
L'approche markovienne permet de pallier les insuffisances des méthodes dites classiques (arbres de défaillances, diagramme de fiabilité ...) grâce à la possibilité d'intégrer des dépendances fonctionnelles entre plusieurs fonctions, de modéliser des scénarios, ou encore de modéliser des composants ayant des défaillances de mode commun grâce à l'ajout d'arcs et de transitions supplémentaires entre des états. Enfin, un avantage réside dans la possibilité d'introduire implicitement le temps. Le temps intervient à la fois dans l'analyse quantitative de la fiabilité, par exemple, lorsque la durée de sollicitation d'un composant ou d'un équipement influe sur sa durée de vie ou sur son taux de défaillance mais aussi dans l'analyse qualitative lorsqu'un système de commande inclut un grand nombre de modes de fonctionnement assurant une continuité du service en cas de défaillances. Par exemple, pour un ensemble donné de défaillances, une séquence particulière peut faire passer le système d'un état nominal à un état dégradé (E1) mais toujours fonctionnel alors que la même séquence ordonnée différemment a potentiellement des conséquences différentes : l'état d'arrivée est soit redouté (ER), soit dégradé (E2) mais différent de (E1).
Néanmoins, on reproche habituellement à cette technique d'être difficilement applicable pour des systèmes complexes, en raison du nombre d'états générés (risque d'explosion combina-

toire) [Mon98] [JAG01] et des hypothèses assez fortes (emploi exclusif de taux de transition constants utilisant des lois exponentielles) [SACH06]. Des études visant à diminuer le nombre de ces états par des méthodes de simplification ou d'agrégation ont été réalisées dans le domaine informatique ou des systèmes industriels [Amo99a],[Buc99]. L'inconvénient des techniques proposées est la nécessité de disposer dans un premier temps d'un graphe exhaustif initial puis d'appliquer les principes de simplification développés. Ces approches sont donc moins applicables au niveau industriel de par le flot d'équations nécessaire et des principes théoriques devant être mis en oeuvre.

**Les arbres de défaillances dynamiques** L'approche par arbre de défaillances dynamiques permet de prendre en compte au sein d'un modèle les scénarios des systèmes étudiés [CM02], [MDCS98], [BB03].

**Arbres de Dugan** Dugan [Dug01] propose de résoudre ce problème en décomposant l'arbre classique initial en une partie statique et une partie dynamique. La partie statique de l'arbre est alors traitée et encodée de manière statique à l'aide de structures de données efficaces sous forme de BDD, la partie dynamique étant, quant à elle, traitée à l'aide d'une approche markovienne. Cette approche consiste à décomposer l'aspect dynamique de l'AdD en contraintes logiques, i.e. des contraintes qui traduisent comment les événements se combinent en utilisant les opérateurs ET et OU, et des contraintes temporelles traduisant l'ordre d'occurrence des événements. Elle obtient l'algorithme de génération de séquences suivant :

- Etape 1 : Remplacement des portes dynamiques par les portes statiques qui correspondent à leurs contraintes logiques.
- Etape 2 : Génération des coupes minimales sur l'AdD statique obtenu.
- Etape 3 : Raffinement des coupes minimales en prenant en compte les contraintes temporelles (on peut se contenter de raffiner le sous-ensemble des coupes initialement issues de portes dynamiques).

**Arbres de Cepin et Mavko** Cepin et Mavko [CM02] ont proposé une approche d'arbres dynamiques basée sur le principe de la composition de sous arbres correspondant à chacune des configurations du système comme ceci est décrit sur la figure 1.16.

L'évolution de manière discrète dans le temps des événements maison est encodée dans une matrice. Cette matrice permet, lors du traitement de l'arbre, d'activer ou de désactiver certaines branches de l'arbre et donc de se placer dans une configuration précise à un instant $t$ donné.

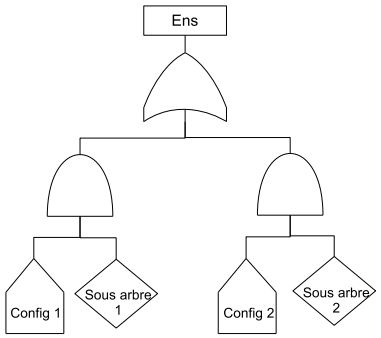


FIG. 1.16 – Arbre des défaillances dynamiques selon [CM02]

**BDMP** Bouissou [BB03], [BD04] a développé un nouveau type de modélisation pour les études fiabilistes de systèmes complexes : les BDMP (ou Boolean Logic Driven Markov Processes). Les BDMP sont le résultat d'une hybridation entre les arbres de défaillances et les processus markoviens. Ce formalisme a fait l'objet d'une définition mathématique rigoureuse, ce qui a permis de démontrer qu'il possédait la capacité de réduire la combinatoire des états et transitions à prendre en compte dans un processus de Markov modélisant un système avec de fortes interactions entre composants. Les BDMP permettent de gagner au moins une décade dans la taille en nombre de composants des problèmes que l'on peut traiter par modélisation markovienne.

Comme nous venons de le préciser, les BDMP sont associés à une représentation graphique proche des arbres de défaillances afin de faciliter leur construction. Un BDMP est issu d'un arbre de défaillances de la manière suivante :

- Les modèles simples de feuilles d'un arbre de défaillances sont remplacés par des Processus de Markov quelconques. Les états de ces processus sont classés en deux catégories. Suivant la catégorie à laquelle appartient l'état d'une feuille à un instant donné, *l'événement* correspondant à cette feuille est considéré comme VRAI ou FAUX.
- L'indépendance des feuilles d'un arbre de défaillances est remplacée par des dépendances simples. Chaque feuille a deux modes *sollicité* et *non sollicité*, correspondant à deux processus de Markov différents. Le choix du mode dans lequel une feuille se trouve à un instant donné est déterminé par la valeur (VRAI ou FAUX) d'un ensemble de feuilles. Les transitions entre ces deux modes définissent éventuellement des états instantanés dans lesquels on peut déclencher des transitions instantanées probabilisées (pour modéliser par exemple des refus de démarrage).

La structure globale d'un BDMP est donnée par une fonction logique utilisée dans les arbres de défaillances. Un BDMP comme celui présenté figure 1.17 est constitué des éléments suivants :

- un arbre de défaillances F,

– un événement principal r,
– un ensemble de *gâchettes* T,
– un ensemble de *processus de Markov pilotés* Pi associés aux événements de base de l'arbre F,
– la définition de deux catégories d'états (marche et panne) pour les processus Pi.

L'événement principal (r) du BDMP est censé représenter l'ensemble des états de panne du processus markovien global.

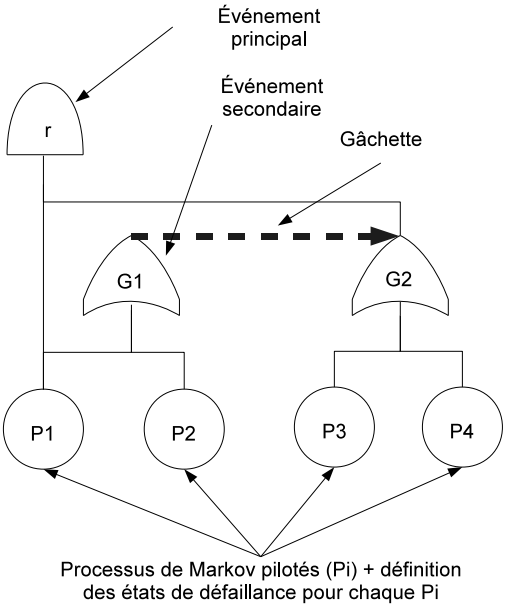


FIG. 1.17 – Exemple de BDMP selon [BB03]

Si on considère le BDMP de la figure 1.17, on a donc la structure logique d'un arbre de défaillances avec en plus une gâchette, ayant pour origine la porte G1 et pour cible la porte G2, et des définitions pour chaque processus Pi. La gâchette entre les deux portes G1 et G2 joue un rôle d'activation des modes de défaillances des processus P3 et P4. Une gâchette permet ainsi de limiter les défaillances des composants aux seuls éléments pertinents initialements sollicités et de les faire intervenir ultérieurement dans le processus.
Dans un BDMP, les portes sans parent (telles que G1 et r dans l'exemple de la figure 1.17) sont sollicitées par défaut. Ces sollicitations se propagent de *père* en *fils* tout au long des branches du BDMP jusqu'à ce qu'elles rencontrent l'arrivée d'une gâchette. La présence d'une telle arrivée conditionne le passage du signal de sollicitation ; ainsi la porte cible transmet la sollicitation à ses descendants seulement si l'événement qui est à l'origine de la gâchette est VRAI (ou FAUX dans le cadre de l'utilisation d'une gâchette dite *inversée*). Si c'est le cas, la sollicitation est ensuite transmise aux portes et feuilles en dessous suivant le même principe.

L'utilisation des gâchettes permet de modéliser simplement toutes sortes de dépendances entre les composants d'un système (une redondance passive par exemple), en permettant de préciser dans quels contextes les défaillances à la sollicitation ou en fonctionnement des composants doivent être envisagées.

**Limites des approches dynamiques** Ces approches qui permettent de prendre en compte les scénarios du modèle sont développées dans le but d'analyser une architecture complexe d'un système déjà existant afin de rechercher ses points vulnérables. Ces approches ne semblent pas adaptées dans le cadre d'une conception d'un système. En effet, comme il a été dit précédemment, concevoir un système revient à trouver le meilleur agencement de composants et de fonctions parmi un ensemble composé de nombreuses possibilités d'architectures matérielles.
Par ailleurs, ces approches débouchent sur des analyses utilisant des approches markoviennes. Comme il a été dit précédemment, les graphes de Markov sont lourds à gérer du fait du risque d'explosion combinatoire. De plus, ces approches nécessitent des données exactes pour évaluer un niveau de sûreté de fonctionnement or notre besoin est d'évaluer un ensemble d'architectures à l'aide de critères semi-quantitatifs.

## 1.6 Conclusion

Ce chapitre a souligné les difficultés liées à la conception et à l'évaluation du niveau de sûreté de fonctionnement des systèmes d'automatisation. Ces difficultés sont liées à la complexité grandissante des systèmes d'automatisation et aux limites des méthodes de modélisation et d'évaluation actuelles face à cette évolution de la complexité. La complexité du système mène ce dernier, en cas de multiples défaillances, d'un état normal vers un état redouté prévisible mais dont le comportement est lui imprévisible. Ces comportements, comme atteindre des états redoutés, doivent être évités ou maîtrisés afin de rendre les systèmes d'automatisation plus sûrs. Dans ce but, l'utilisation, dès les premières phases de conception, des scénarios de défaillances permettant de caractériser le comportement dysfonctionnel du système est l'approche d'évaluation envisagée dans ces travaux.

Le premier point abordé dans ce chapitre concerne les notions de système d'automatisation et d'instruments intelligents. La définition d'un système d'automatisation à intelligence distribuée ainsi que la démarche et les problèmes de conception pour ces types de systèmes ont ensuite été abordés. Le second point abordé a présenté la sûreté de fonctionnement, ses concepts et ses techniques. Les travaux de recherche sur les méthodes de conception

intégrant la sûreté de fonctionnement ont également été présentés afin de montrer l'importance du développement de telles méthodes pour les systèmes d'automatisation.

Enfin, la problématique liée à l'évaluation de la sûreté de fonctionnement d'un système d'automatisation a été présentée. Plus précisément le besoin d'intégrer les scénarios de défaillances associé aux limites des méthodes d'évaluation actuelles permettent d'exposer les besoins d'une méthodologie de conception de systèmes intégrant au plus tôt la sûreté de fonctionnement et une évaluation basée sur les scénarios.

En conclusion, la modélisation des comportements fonctionnels et dysfonctionnels des systèmes d'automatisation intégrant les scénarios, est à privilégier dès les toutes premières phases de conception de ces systèmes. Cette approche doit intégrer l'ensemble des interactions qui existent entre fonctions et composants dans un système. Ces caractéristiques sont à considérer pour l'étude et l'évaluation de la sécurité et de la disponibilité d'un système d'automatisation, objet de nos travaux de recherche. Le deuxième chapitre propose une méthodologie de conception de systèmes d'automatisation tout en intégrant les scénarios répondant à la problématique d'évaluation présentée dans ce chapitre. Dans ce deuxième chapitre, les formalisations, les notations et les différentes étapes de cette méthodologie sont expliquées. A titre d'illustration, la conception d'un système hydraulique régulé est également détaillée dans ce chapitre.

# Chapitre 2

# Méthodologie de conception de systèmes sûrs

## 2.1 Introduction

Dès qu'un système est un tant soit peu complexe, le concepteur chargé de l'étude de sûreté de fonctionnement doit construire un modèle représentatif du comportement du système en fonctionnement normal et en présence de défaillances. Ce modèle représentatif doit être suffisamment abstrait pour ne contenir que des éléments pertinents et essentiels à l'évaluation des performances recherchées. Ce modèle doit également être concis afin d'être facilement interprétable par d'autres acteurs participant à la conception et à la construction du système. Ainsi, les méthodes à base d'un modèle statique telles que les arbres de défaillances ont eu et ont toujours un succès dans le milieu industriel car elles offrent une représentation facilitant la lecture, l'interprétation, la communications entre acteurs. En outre l'analyse de ces modèles permet de déterminer assez facilement leur combinaison ou leur séquence de défaillances conduisant à l'occurrence d'un événement redouté précis. Comme il a été remarqué dans le chapitre 1, la plupart de ces méthodes n'offrent qu'une vision statique des combinaisons de défaillances, et de ce fait ne sont pas adaptées pour tenir compte des séquences ordonnées dans le temps d'apparition de ces défaillances.
Les méthodes à base de changement d'état basées sur les graphes de Markov permettent de tenir compte des séquences de défaillances et offrent à l'instar des arbres de défaillance classiques, un support visuel donnant le comportement du système en présence de défaillances. Cependant, ces méthodes nécessitent, pour évaluer le niveau de sûreté de fonctionnement, des données exactes qui sont parfois difficiles d'accès avec l'utilisation de nouvelles technologies innovantes. Les graphes de Markov souffrent également de l'explosion combinatoire du nombre d'états à étudier.
Le modèle représentatif doit, de plus, permettre d'estimer des grandeurs quantifiant des

mesures quantitatives de sûreté de fonctionnement. Ces estimations dépendent des probabilités d'occurrence des pannes de composants élémentaires mais également de l'architecture du système. Intuitivement, l'architecture (c'est-à-dire l'agencement des composants) du système a une influence sur les conséquences possibles d'une séquence de défaillances. Il s'agit donc de représenter le plus précisément ces influences et ces conséquences par la différenciation entre les séquences possibles et celles impossibles suivant l'architecture du système. L'étude exhaustive des séquences permet donc de quantifier le niveau de sûreté de fonctionnement d'un système de façon précise par rapport à l'étude des coupes.

La construction d'un modèle graphique décrivant la structure fonctionnelle du système d'automatisation permettant de caractériser précisément son comportement dysfonctionnel par l'utilisation des séquences ordonnées de modes de défaillances est le **premier objectif** de la méthodologie proposée.

L'idée de combiner les méthodes à base d'un modèle statique et les méthodes à base de changement d'état afin de modéliser de façon précise le comportement dysfonctionnel du système a fait l'objet de nombreux travaux de recherche [Dug01], [CM02]. Cependant, même si ces méthodes permettent de modéliser un système, elles semblent mal adaptées en phase de conception pour modéliser au sein d'un même modèle les différentes possibilités d'agencement de composants et pour évaluer cet ensemble d'architectures afin de pouvoir les comparer entre elles. En effet, la conception d'un système impose la modélisation, l'évaluation et la comparaison de différentes architectures matérielles parmi un grand ensemble d'architectures possibles en vue d'en déterminer la meilleure.

Ainsi la modélisation des différentes possibilités d'agencement de composants au sein d'un même modèle et l'évaluation relative du niveau de sûreté de fonctionnement entre architectures matérielles constituent le **second objectif** de la méthodologie proposée.

Dans le cadre de l'optimisation du système, le concepteur se doit de disposer des critères permettant l'évaluation puis la comparaison des architectures possibles. Dans notre cas, ces critères sont le coût et le niveau de sûreté de fonctionnement. Si le premier critère relatif au coût est approximable, le critère sûreté de fonctionnement est de par sa nature plus délicat à quantifier. En effet, il doit rendre compte des différents aspects fiabilité, disponibilité, maintenabilité et sécurité souvent antagonistes ou difficilement conciliables. Par ailleurs, l'utilisation des nouvelles technologies et des composants programmables aux multiples modes de défaillance parfois mal connus, rend difficile l'accès aux données de fiabilité pour le concepteur. Ainsi, l'environnement (vibrations, CEM, température), le choix de la politique de maintenance (déterminée tard dans la démarche de conception) ont une forte

influence sur la fiabilité ou la disponibilité des composants employés. Ce manque de données précises rend nécessaire la définition de nouveaux paramètres facilement quantifiables. L'objectif global est de faciliter le travail du concepteur en le dispensant du recueil d'une grande quantité de données, tout en lui permettant d'obtenir des résultats suffisamment pertinents pour effectuer le choix des composants et de l'architecture du système à concevoir.

L'obtention d'un ensemble d'architectures optimisées, dont chaque solution est caractérisée par un coût et par un niveau de sûreté de fonctionnement utilisant des critères de quantification est le **troisième objectif** de la méthodologie proposée.

La méthodologie proposée est décomposable en deux étapes : une première étape de modélisation fonctionnelle et dysfonctionnelle du système et une seconde étape d'optimisation de l'ensemble des architectures possibles obtenues à partir de cette modélisation. La première partie de ce chapitre introduit le formalisme utilisé dans ces deux étapes. Nous détaillons quelques définitions et propriétés utiles pour la compréhension des mécanismes d'évaluation et de comparaison intégrés dans chacune des deux étapes. La deuxième partie de ce chapitre explique l'étape de modélisation de la méthodologie de conception. Les phases de construction des différents modèles sont détaillées et illustrées sur un exemple de système hydraulique régulé. La troisième partie de ce chapitre détaille l'étape d'optimisation de la méthodologie, l'approche utilisée pour l'analyse des modèles construits et la détermination de l'ensemble des architectures optimales. Les différents résultats obtenus sont illustrés sur le même exemple de système hydraulique. Afin de clore ce chapitre, les fonctionnalités de la plate-forme de conception nommée ALoCSyS issue de ces travaux sont présentées.

## 2.2 Formalisation du problème de conception

Dans cette partie, nous définissons les concepts et les notions qui sont utilisés dans la méthodologie proposée. Nous posons les définitions d'un scénario et de ses paramètres. Nous présentons ensuite les opérateurs et les propriétés nécessaires à la modélisation du comportement dysfonctionnel du système à concevoir. Enfin, les critères nécessaires à la comparaison et à l'optimisation du système d'automatisation que sont le coût et le niveau de sûreté de fonctionnement sont également définis dans cette partie.

### 2.2.1 Défaillance, scénario, longueur et ensemble de scénarios

Basée sur la définition de la défaillance donnée au chapitre 1 comme étant la fin de l'aptitude d'un dispositif à accomplir sa fonction requise, une défaillance est caractérisée par un événement non désiré. Cet événement est généralement lié à la transition d'un état

normal à un état non désiré d'un composant ou d'un ensemble de composants. Dans cet état non désiré, il est supposé que le composant ne peut accomplir correctement sa mission.

Dans tout le reste de ce mémoire, le système est supposé comme étant non réparable au moins pendant l'exercice de sa mission, c'est-à-dire qu'un composant ne peut revenir à son état initial. Par ailleurs, une défaillance du système correspond à un événement redouté et une défaillance de composant correspond à un mode de défaillance.

**Définition 2.1 (Scénario)**
*Un scénario correspond à une séquence de défaillances de composant qui entraîne l'événement redouté D. Un scénario est un ensemble, ordonné dans le temps, de défaillances noté $\psi_D$ tel que :*

$$\psi_D = [F_i^1, ..., F_j^n] \tag{2.1}$$

*où $F_\alpha^\beta$ est la défaillance $F_\alpha$ qui apparaît à la position $\beta$ dans le scénario $\psi_D$ .*

**Notation 2.1 (Ensemble de scénarios)**
*Soit $\Phi_D$ l'ensemble de tous les scénarios amenant le système vers un événement redouté D. Soit $\psi_D^i$ un élément de $\Phi_D$.*

$$\Phi_D = \{\psi_D^1, ..., \psi_D^m\} \tag{2.2}$$

*où $\psi_D^i$ est le $i^{ème}$ élément de $\Phi_D$.*

**Notation 2.2 (Longueur d'un scénario)**
*Soit $\psi_D^i$ un scénario de l'ensemble $\Phi_D$. La longueur de ce scénario, notée $L(\psi_D^i)$, est le cardinal de $\psi_D^i$.*

$$L(\psi_D^i) = card(\psi_D^i) \tag{2.3}$$

**Notation 2.3 (Longueur minimale d'un ensemble de scénarios)**
*$L_{min}^D$ est la longueur minimale de tous les scénarios contenus dans l'ensemble $\Phi_D$.*

$$L_{min}^D = \min_{1 \leq i \leq card(\Phi_D)} L(\psi_D^i) \tag{2.4}$$

*Concernant un événement redouté particulier, le paramètre $L_{min}^D$ exprime le nombre minimum de modes de défaillances qui entraînent l'occurrence de cet événement redouté.*

**Notation 2.4 (Ensemble de scénarios minimaux d'un ensemble de scénarios)**
*L'ensemble des scénarios minimaux de $\Phi_D$, noté $\Delta_D$, est un sous-ensemble de $\Phi_D$ contenant tous les scénarios dont la longueur est $L_{min}^D$.*

$$\Delta_D = \{\psi_D^i \in \Phi_D / L(\psi_D^i) = L_{min}^D\} \tag{2.5}$$

**Remarque :** Dans la littérature [RH04], [BD04], un scénario qui amène le système vers un événement redouté est considéré comme minimal s'il n'est pas inclus dans un autre scénario qui amène vers le même événement redouté. L'ensemble des scénarios ayant une longueur minimale, comme défini dans la définition 2.4, est un sous ensemble de l'ensemble des scénarios minimaux où seules les séquences ayant la longueur minimale sont considérées.

**Notation 2.5 (Nombre de scénarios d'un ensemble de scénarios minimaux)**
*Le nombre de scénarios contenus dans l'ensemble $\Delta_D$ est noté $N^D_{min}$. Ce paramètre, associé au $L^D_{min}$, correspond à la probabilité d'occurrence de l'événement redouté D. Ce point est développé dans le paragraphe 2.2.3.*

$$N^D_{min} = card(\Delta_D) \tag{2.6}$$

### 2.2.2 Opérateurs caractérisant les relations entre défaillances

Les arbres de défaillance classiques représentent graphiquement les relations entre les différents modes de défaillances. Classiquement, les opérateurs **AND** (ET) et **OR** (OU) sont utilisés. Dans le but de prendre en compte les séquences d'apparition ordonnées de défaillances, il est nécessaire d'ajouter deux nouveaux opérateurs notés **PAND** (ET prioritaire) et **SEQ** (Séquentiel) [DBB92], [CSD00]. Pendant la phase de modélisation, ces opérateurs caractérisent les relations entre les différents modes de défaillances des fonctions, sous-fonctions et fonctions élémentaires du système physique étudié. Ces opérateurs ont également des propriétés mathématiques (ou lois de composition) qui sont appliquées pendant la phase d'optimisation lors du traitement de l'arbre. Ces propriétés sont énoncées ci-après. Les preuves de ces propriétés sont données en annexe A.

Considérons A, B et C, trois événements redoutés, tels que C est le résultat de l'association de A et de B avec l'un des opérateurs. $\Delta_A$, $\Delta_B$ et $\Delta_C$ sont les ensembles de scénarios minimaux associés à A, B et C. Nous prenons pour hypothèse que les événements redoutés A et B sont indépendants, c'est-à-dire qu'une défaillance ne peut pas apparaître simultanément dans A et B et que les scénarios conduisant à A et B ne partagent pas de défaillances.

#### 2.2.2.1 Opérateur AND

L'opérateur **AND** représente le cas où l'occurrence de C se produit suite à l'occurrence de A et de B.

**Propriété 2.1**
*Avec $C = A$ **AND** $B$, les paramètres de $\Delta_C$ peuvent être évalués à l'aide des relations suivantes :*

$$L^C_{min} = L^A_{min} + L^B_{min} \tag{2.7}$$

$$N_{min}^{C} = \frac{(L_{min}^{A} + L_{min}^{B})!}{L_{min}^{A}! \times L_{min}^{B}!} \times N_{min}^{A} \times N_{min}^{B} \tag{2.8}$$

#### 2.2.2.2 Opérateur OR

L'opérateur **OR** représente le cas où l'occurrence de C se produit suite à l'occurrence de A ou de B.

**Propriété 2.2**
*Avec $C = A$ **OR** $B$, les paramètres de $\Delta_C$ peuvent être évalués à l'aide des relations suivantes :*

$$Si\ L_{min}^{A} < L_{min}^{B}\ ;\ \begin{cases} L_{min}^{C} = L_{min}^{A} \\ N_{min}^{C} = N_{min}^{A} \end{cases} \tag{2.9}$$

$$Si\ L_{min}^{A} = L_{min}^{B}\ ;\ \begin{cases} L_{min}^{C} = L_{min}^{A} \\ N_{min}^{C} = N_{min}^{A} + N_{min}^{B} \end{cases} \tag{2.10}$$

$$Si\ L_{min}^{A} > L_{min}^{B}\ ;\ \begin{cases} L_{min}^{C} = L_{min}^{B} \\ N_{min}^{C} = N_{min}^{B} \end{cases} \tag{2.11}$$

#### 2.2.2.3 Opérateur PAND

**Définition 2.2 (Opérateur PAND)**
*L'opérateur **PAND** est un opérateur temporel qui représente le cas où l'occurrence de C se produit suite aux occurrences **successives** de A puis de B. Cet opérateur est utile lorsque les effets de deux événements sont différents selon leur ordre d'occurrence.*

**Propriété 2.3**
*Avec $C = A$ **PAND** $B$, les paramètres de $\Delta_C$ peuvent être évalués à l'aide des relations suivantes :*

$$L_{min}^{C} = L_{min}^{A} + L_{min}^{B} \tag{2.12}$$

$$N_{min}^{C} = \frac{((L_{min}^{A} - 1) + L_{min}^{B})!}{(L_{min}^{A} - 1)! \times L_{min}^{B}!} \times N_{min}^{A} \times N_{min}^{B} \tag{2.13}$$

#### 2.2.2.4 Opérateur SEQ

**Définition 2.3 (Opérateur SEQ)**
*L'opérateur **SEQ**, comme l'opérateur **PAND**, représente le cas où l'occurrence de C se produit suite aux occurrences **successives** de A puis de B. Cependant, l'opérateur **SEQ** impose qu'aucune défaillance de composant amenant le système vers l'événement B ne peut se produire avant l'occurrence de l'ensemble des défaillances amenant à l'événement redouté A.*

Cet opérateur est utile dans la modélisation des redondances passives. En effet, la fonction redondée démarre seulement quand la fonction principale est défaillante. De ce fait, l'occurrence de défaillance liée à la fonction redondée ne peut se produire qu'après l'occurrence de la défaillance de la fonction principale.

**Propriété 2.4**
*Avec $C = A$ **SEQ** $B$, les paramètres de $\Delta_C$ peuvent être évalués à l'aide des relations suivantes :*

$$L^C_{min} = L^A_{min} + L^B_{min} \tag{2.14}$$

$$N^C_{min} = N^A_{min} \times N^B_{min} \tag{2.15}$$

### 2.2.3 Comparaison entre niveaux de sûreté de fonctionnement et entre systèmes

Dans cette section, nous décrivons et définissons les paramètres permettant de comparer des systèmes équivalents entre eux. Nous présentons ensuite les mécanismes de comparaison et la notion de système optimal.
La première notion définie est celle de systèmes équivalents. Cette notion permet de définir les critères permettant de comparer sur des bases identiques, deux systèmes entre eux.

**Définition 2.4 (Systèmes équivalents)**
*Deux systèmes (ou composants) sont équivalents s'ils peuvent accomplir les mêmes fonctions et si les mêmes événements redoutés peuvent être définis pour ces deux systèmes.*

Nous définissons ensuite le niveau de sûreté de fonctionnement d'un événement redouté précis. Cette définition permet de relier les paramètres $L_{min}$ et $N_{min}$ définis dans le paragraphe 2.2.1 à la caractérisation d'un niveau de sûreté de fonctionnement.

**Notation 2.6 (Niveau de sûreté de fonctionnement pour un événement redouté)**
*Pour un système $S$ et pour un événement redouté $D$, le niveau de sûreté de fonctionnement est formé par le couple de paramètres $(L^{D,S}_{min}\ N^{D,S}_{min})$. Ce couple est noté $DL^S_D$.*

Pour un système particulier, ce couple caractérise la probabilité d'occurrence de l'événement redouté D. Ainsi, ce couple peut être utilisé pour comparer plusieurs systèmes entre eux du point de vue de la sûreté de fonctionnement.

**Propriété 2.5 (Comparaison entre niveaux de sûreté de fonctionnement)**
*Pour deux systèmes équivalents $S_1$ et $S_2$ et pour le même événement redouté $D$, le niveau de sûreté de fonctionnement de $S_1$ est meilleur que celui de $S_2$, si l'une des deux relations suivantes est vérifiée :*

$$L^{D,S_1}_{min} > L^{D,S_2}_{min} \tag{2.16}$$

$$ou \left\{ \begin{array}{l} L_{min}^{D,S_1} = L_{min}^{D,S_2} \\ N_{min}^{D,S_1} < N_{min}^{D,S_2} \end{array} \right. \tag{2.17}$$

*On notera alors* $DL_D^{S_1} > DL_D^{S_2}$.

Les relations 2.16 et 2.17 signifient que le niveau de sûreté de fonctionnement de $S_1$ est meilleur que celui de $S_2$ si :

- La longueur minimale de l'ensemble des scénarios de $S_1$ est supérieure à la longueur minimale de l'ensemble des scénarios de $S_2$,
- Ou si pour une même longueur, le nombre de scénarios de l'ensemble des scénarios de $S_1$ est inférieur au nombre de scénarios de l'ensemble des scénarios de $S_2$.

**Propriété 2.6**

*Par extension de la propriété 2.5, le niveau de sûreté de fonctionnement entre deux systèmes est dit identique, c'est-à-dire* $DL_D^{S_1} = DL_D^{S_2}$, *si* $L_{min}^{D,S_1} = L_{min}^{D,S_2}$ *et si* $N_{min}^{D,S_1} = N_{min}^{D,S_2}$.

**Notation 2.7 (Niveau de sûreté d'un système)**

*Pour un système (ou un composant) associé à n événements redoutés* $D_i$ $(i = 1...n)$, *le niveau de sûreté de fonctionnement est donné par l'ensemble* $DL^S$ *de tous les* $DL_{D_i}^S$.

$$DL^S = \{DL_{D_1}^S, ..., DL_{D_n}^S\} \tag{2.18}$$

*Cet ensemble caractérise la fiabilité du système considéré pour différents événements redoutés.*

**Propriété 2.7 (Comparaison entre systèmes équivalents du niveau de SdF)**

*Soit deux systèmes équivalents* $S_1$ *et* $S_2$ *et un ensemble d'événements redoutés, le niveau de sûreté de fonctionnement* $DL^{S1}$ *est supérieur à* $DL^{S2}$ *si la relation suivante est vérifiée :*

$$\forall i \; DL_{D_i}^{S1} \geq DL_{D_i}^{S2} \; et \; \exists j \; DL_{D_j}^{S1} > DL_{D_j}^{S2} \tag{2.19}$$

*On notera* $DL^{S1} > DL^{S2}$ *ce qui signifie que le système* $S_1$ *est plus robuste aux modes de défaillances que le système* $S_2$.

**Notation 2.8 (Coût d'un système)**

*A chaque composant est associée une valeur représentant son coût. Pour un système S, son coût équivaut à la somme des coûts individuels de ses q composants.*

$$\widehat{Co\hat{u}t}_S = \sum_{i=1}^{q} \widehat{Co\hat{u}t}_{composant_i} \tag{2.20}$$

**Notation 2.9 (Caractérisation d'un système)**
*Un système $S$ est caractérisé par le couple $C_S$ formé du coût et du niveau de sûreté de fonctionnement.*

$$C_S = \{\widehat{Coût}_S, DL^S\} \tag{2.21}$$

**Propriété 2.8 (Comparaison de systèmes)**
*Le système $S_1$ est meilleur que le système $S_2$, c'est-à-dire $C_{S1} > C_{S2}$, si la relation suivante est vérifiée :*

$$\begin{cases} \widehat{Coût}_{S1} = \widehat{Coût}_{S2} \\ DL^{S1} > DL^{S2} \end{cases} \tag{2.22}$$

$$ou \begin{cases} \widehat{Coût}_{S1} < \widehat{Coût}_{S2} \\ DL^{S1} \geq DL^{S2} \end{cases} \tag{2.23}$$

**Définition 2.5 (Systèmes optimaux)**
*Pour un ensemble de systèmes équivalents $\Omega$, l'ensemble des systèmes optimaux $\Omega_{optimal}$ est défini par la relation suivante :*

$$\Omega_{optimal} = \{S \in \Omega,\ tel\ qu'il\ n'existe\ pas\ S_i \in \Omega\ avec\ C_{Si} > C_S\} \tag{2.24}$$

**Remarque :** Il est à noter que si S1 n'est pas meilleur que S2, ceci n'implique pas que S2 est meilleur que S1. Les deux systèmes sont alors considérés comme non comparables entre eux (ou solutions non-dominées au sens de Pareto [Par96], [Die04]). Dans ce cas, c'est au concepteur de choisir le système correspondant le mieux à ses besoins.

### 2.2.4 Prise en compte des composants de sécurité et intelligents

#### 2.2.4.1 Définition du coefficient de fiabilité relatif (RRC)

L'utilisation précédente de scénarios et de leur comparaison sur la base de leur longueur implique que les modes de défaillances considérés sont équiprobables ou tout au moins ont une probabilité d'occurrence du même ordre de grandeur. Cependant certains composants peuvent avoir des fiabilités très dissemblables. C'est ainsi le cas des composants de sécurité qui présentent une grande fiabilité vis-à-vis du risque d'atteindre une situation dangereuse ou critique.
Afin de pouvoir comparer des composants aux fiabilités variées, la caractérisation des niveaux de sûreté de fonctionnement peut être enrichie en substituant les longueurs $L^D_{min}$ par un coefficient équivalent rendant mieux compte des probabilités d'occurrence des séquences considérées et pour lequel les relations précédentes restent valides. Noté RRC (Relative Reliability Coefficient), ce coefficient rend compte de la probabilité qu'un événement ou qu'une séquence d'événements apparaisse.

**Définition 2.6 (Coefficient de fiabilité relatif)**
*Le coefficient de fiabilité relatif, noté $RRC^{F_i}$ [CB06b], caractérise le nombre de composants de référence montés en redondance permettant d'obtenir la même probabilité de défaillance $F_i$ que le composant considéré au cours de la durée d'exécution d'une mission.*

*La relation entre la défiabilité d'un composant standard et la défiabilité d'un composant de sécurité pour un mode de défaillance $F_i$ pendant la durée d'exécution de la mission est définie par la relation 2.25.*

$$\overline{R}(t) = (\overline{R}_{ref}(t))^{RRC^{F_i}} \tag{2.25}$$

*où $\overline{R}_{ref}(t)$ est la défiabilité d'un composant standard.*

Le concept du RRC peut être étendu à un scénario et correspond à sa probabilité d'occurrence. Pour un scénario, cette valeur est évaluée par la somme des RRC des événements qui le composent.

$$RRC^{\psi_D} = \sum_{F_i \in \psi_D} RRC^{F_i} \; avec \; \psi_D = \{F_i^1, ..., F_j^n\} \tag{2.26}$$

#### 2.2.4.2 Exemple

D'un point de vue pratique, si le concepteur veut distinguer certains composants ayant une fiabilité supérieure à d'autres, il leur affecte un RRC supérieur à 1, tandis que les composants standards ont un RRC à 1, valeur servant de référence. Ainsi un RRC d'une valeur de 2 appliquée à un mode de défaillance particulier d'un composant indique que sa probabilité de défaillance est *équivalente* à la défaillance de deux composants standards.
Pour illustrer ceci, considérons que la défiabilité $\overline{R}_F(t)$ d'un composant standard (pour lequel on pose $RRC^F = 1$) durant une mission est de l'ordre de $10^{-3}$. Le $RRC^{F_r}$ d'un composant robuste pour une défaillance $F_r$ avec la défiabilité de l'ordre de $\overline{R}_{F_r}(t) = 10^{-5}$ est évalué à 1,66 par la relation suivante, déduite de la relation 2.25 dont la condition d'application est démontrée en annexe B.

$$RRC^{F_r} = \frac{ln(\overline{R}_{F_r}(t))}{ln(\overline{R}_F(t))} \tag{2.27}$$

Nous pouvons, de ce fait, donner la relation suivante entre les deux types de composants :

$$RRC^{F_{Composant\ sécuritaire}} = 1,66 \times RRC^{F_{Composant\ standard}} \tag{2.28}$$

## 2.3 Etape de modélisation

Dans cette section et dans la suivante, la méthodologie de conception de systèmes d'automatisation est expliquée. Cette méthodologie est décomposable en une étape de modélisation

et une étape d'optimisation suivant le schéma présenté figure 2.1. L'étape de modélisation se décompose en deux phases : dans la première phase, le système est décrit à l'aide d'une architecture fonctionnelle et matérielle puis dans la seconde phase, les relations entre événements redoutés sont ajoutées à cette architecture fonctionnelle afin d'obtenir l'architecture comportementale sous la forme d'un modèle graphique similaire à un arbre de défaillance, l'arbre de défaillances multiples amélioré. L'étape d'optimisation permet d'analyser ce modèle graphique et de déterminer les architectures optimales par l'algorithme du type branch and bound.

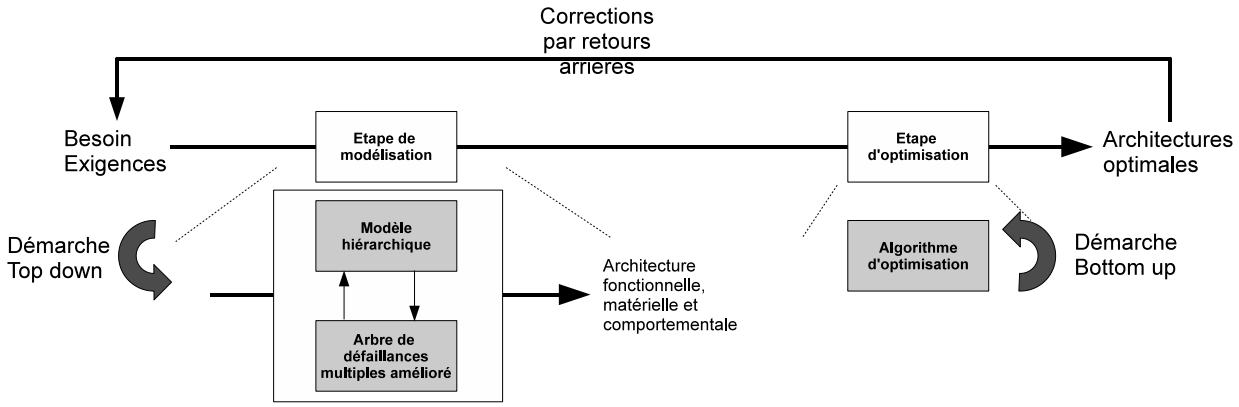


FIG. 2.1 – Démarche de conception proposée

A titre d'illustration de notre méthodologie, la conception du système d'automatisation pour la régulation du niveau d'eau d'une cuve est détaillée étape par étape. L'objectif, pour ce chapitre, est de déterminer les systèmes d'automatisation offrant les meilleurs compromis entre coût et niveau de sûreté de fonctionnement.

## 2.3.1 Modèle hiérarchique fonctionnel

L'analyse hiérarchique est une forme assez naturelle pour modéliser des systèmes de contrôle commande [CB06b], [CCCB04]. Elle permet de représenter les fonctions, les sous-fonctions et les fonctions élémentaires nécessaires à la réalisation des missions définies par le concepteur. Les résultats de cette analyse sont mis sous une forme de décomposition arborescente facile à comprendre comme celle qui sera proposée au chapitre 3 pour le wagon intelligent.

### 2.3.1.1 Définition des missions principales et du modèle fonctionnel

La première phase de cette étape est de construire le modèle hiérarchique selon une démarche déductive, c'est-à-dire en partant de la (des) mission(s) considérée(s) et en décom-

posant en fonctions et sous-fonctions jusqu'à atteindre des fonctions élémentaires physiquement réalisable par un unique composant. Cependant, le formalisme de cette architecture fonctionnelle tel qu'il est défini dans la norme AFNOR NF X50-151 [AFN04] ne permet pas de représenter les différentes possibilités de conception. Dans ce but, nous avons défini trois types de noeuds : le noeud associatif, le noeud alternatif et le noeud élémentaire.

- Le **noeud associatif** modélise une fonction nécessitant, pour sa réalisation, un ensemble de sous-fonctions. Par exemple, sur la figure 2.2 (a), une fonction de contrôle par bouclage nécessite une fonction de mesure, une fonction de régulation et une fonction d'action.
- Le **noeud alternatif** est utilisé pour modéliser différentes possibilités d'implantation d'une fonction. Par exemple, sur la figure 2.2 (b), pour une fonction de mesure, le concepteur peut choisir d'utiliser soit un unique capteur, soit une fonction d'estimation ou soit un ensemble de capteurs redondés.
- Le **noeud élémentaire** représenté sur la figure 2.2 (c) est utilisé pour modéliser une fonction associée à un composant physique.

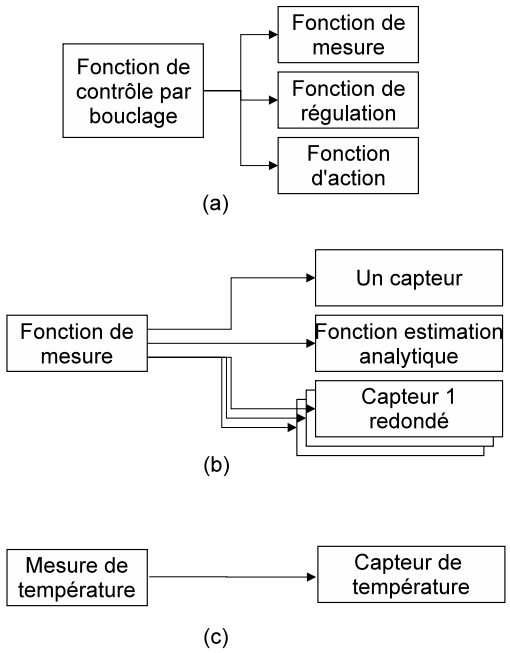


FIG. 2.2 – Exemples de noeud associatif (a), noeud alternatif (b) et noeud élémentaire (c)

**Remarque :** La figure 2.3 (a) présente le cas où deux fonctions (notées Fonction 1 et Fonction 2) nécessitent, pour leur réalisation, l'association des trois mêmes sous-fonctions (notées Fonctions A, B et C) ainsi que l'équivalence graphique (b) de ce cas de figure.

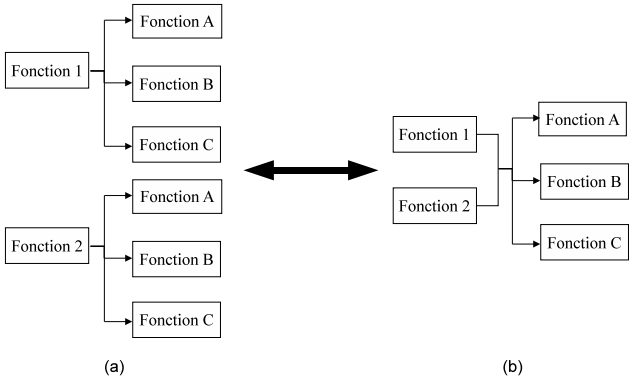


FIG. 2.3 – Exemple d'équivalence graphique de deux fonctions utilisant la même association de trois sous-fonctions

**Illustration avec le système hydraulique** Dans le cadre du système hydraulique, on dispose d'une cuve et d'une pompe alimentant la cuve en eau. Par ailleurs, afin d'être constamment alimenté en eau, un processus industriel est relié à cette cuve. L'objectif du concepteur est de déterminer un système d'automatisation offrant le meilleur compromis coût-niveau de sûreté de fonctionnement et qui permet d'alimenter le processus en eau tout en assurant une hauteur d'eau constante dans la cuve. Ce système d'automatisation doit également éviter les débordements et les vidanges intempestives de cette cuve.
La première étape de cette conception est de déterminer la mission du système. Cette mission est *asservir le niveau d'eau* de la cuve afin qu'elle contienne une hauteur d'eau précise. Elle est assurée par une fonction de commande du système composée de trois sous-fonctions : *Mesurer le niveau d'eau de la cuve*, *Pomper* et *Réguler ce niveau* en fonction de la hauteur d'eau mesurée.
Le système doit assurer l'ensemble des trois sous-fonctions. Afin de modéliser cette possibilité de conception, un noeud associatif est placé entre la fonction *Commander le système* et ses trois sous-fonctions. La figure 2.4 présente le modèle obtenu.

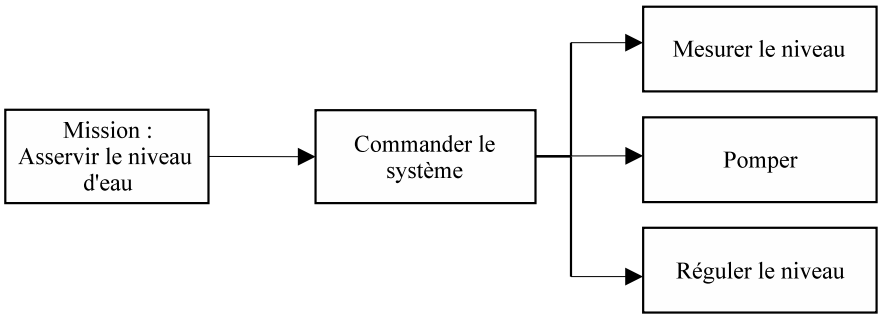


FIG. 2.4 – Modèle hiérarchique de la mission du système hydraulique

#### 2.3.1.2 Enrichissement avec les fonctions de sécurité et de surveillance

Après définition de la mission et des sous-fonctions du système, le précédent modèle doit être enrichi avec les fonctions de sécurité et de surveillance que le système de commande doit accomplir. Ces fonctions sont déterminées selon le même principe de construction déductif que pour la mission du système.

**Illustration avec le système hydraulique** Pour la conception du système hydraulique, deux fonctions sont ajoutées à celle de la commande du système : *Surveiller les niveaux d'eau haut et bas de la cuve* et *Mettre le système en repli* lors d'un risque de débordement de la cuve.
La mission de régulation du système est accomplie par un système de contrôle qui commande le système. A cette fonction de commande, les deux fonctions de surveillance et de sécurité sont ajoutées. Afin de modéliser cette possibilité de conception, un noeud associatif est placé entre la mission et les trois fonctions. De la même façon, un noeud associatif est placé entre la fonction *Surveiller les niveaux* et ses sous-fonctions *Surveiller le niveau haut* et *Surveiller le niveau bas*. La figure 2.5 présente le modèle enrichi issu de celui de la figure 2.4.

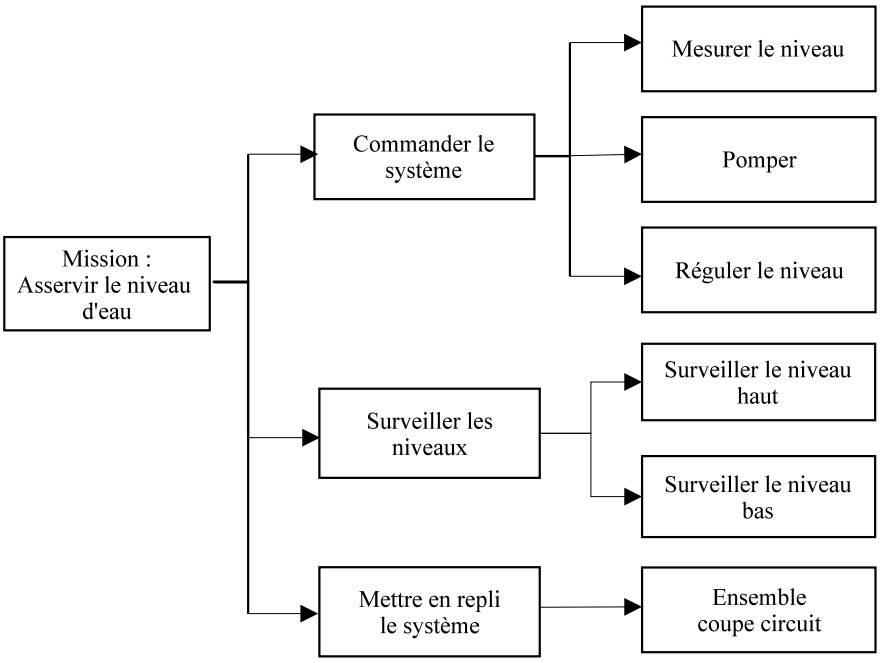


FIG. 2.5 – Modèle hiérarchique enrichi du système hydraulique

#### 2.3.1.3 Ajout des équipements au modèle fonctionnel

**Définition des composants et de leurs agencements** La phase suivante est d'ajouter au modèle fonctionnel les différents composants utilisés par les fonctions. Il s'agit également d'ajouter, pour chaque fonction, différentes stratégies d'agencement de ces composants : redondance active ou passive, structure série ou parallèle. Pour rappel, les structures série ou parallèle font référence à l'organisation matérielle des composants tandis que dans le cadre d'une redondance active, les composants remplissent leur mission au même moment et dans le cadre d'une redondance passive, le composant en redondance débute sa mission après la défaillance du premier composant. Ces stratégies d'agencement visent soit à une meilleure disponibilité en tentant de poursuivre la mission malgré la perte de composant(s), soit à une meilleure sécurité en mettant le système en repli à la moindre défaillance détectée.

**Illustration avec le système hydraulique** Le modèle du système hydraulique est composé d'une mission *Asservir le niveau d'eau* et de cinq fonctions de base : *Mesurer le niveau*, *Pomper*, *Réguler le niveau*, *Surveiller le niveau haut/bas* et *Mettre le système en repli*. Plusieurs composants sont utilisés pour ces fonctions de base : des capteurs de niveau qui mesurent la hauteur d'eau dans la cuve, des pompes, des détecteurs de niveau qui détectent une hauteur d'eau précise, des API qui effectuent des traitements en fonction des données reçues et qui déclenchent les pompes, des coupe-circuits qui arrêtent les pompes. De la même façon, la mission du système peut être accomplie par un ou deux systèmes de commande.
La correspondance entre ces composants et les fonctions est résumée dans le tableau 2.1.

#### 2.3.1.4 Définition des alternatives de composants

La dernière phase de construction du modèle est d'ajouter les alternatives des composants utilisés. Ces alternatives correspondent à différents types de composants que l'on souhaite utiliser comme les composants standards et sécuritaires. Nous verrons par ailleurs dans le paragraphe 2.3.2.2 que ces alternatives possèdent des coûts et des niveaux de tolérance aux fautes différents comme défini dans le paragraphe 2.2.4.1.

**Illustration avec le système hydraulique** Dans le cadre de la conception du système hydraulique, les composants de base et leurs alternatives sont décrits dans le tableau 2.2. Les composants de type *Sûr type 1* et *Sûr type 2* d'une même famille de composants correspondent à des composants sécuritaires ayant des coûts et/ou des niveaux de tolérance aux fautes différents qui seront définis dans le paragraphe 2.3.2.2.

Ainsi, le modèle hiérarchique complet du système d'asservissement est présenté figure 2.6.

| Fonctions | Composants associés | Possibilités d'organisation |
|---|---|---|
| Asservir le niveau | Système de commande | - Un seul système<br>- Deux systèmes en redondance passive |
| Pomper | Pompe | - Une seule pompe<br>- Deux pompes en redondance active<br>- Deux pompes en redondance passive |
| Réguler le niveau | API | - Un seul automate<br>- Deux automates en redondance active |
| Mesurer le niveau | Capteur niveau | - Un seul capteur<br>- Deux capteurs en parallèle |
| Surveiller le niveau | Détecteur niveau | - Un seul détecteur<br>- Deux détecteurs en série<br>- Deux détecteurs en parallèle |
| Mettre le système en repli | Coupe-circuit | - Un seul C-C<br>- Deux C-C en série<br>- Deux C-C en parallèle |

TAB. 2.1 – Fonctions, composants utilisés et possibilités d'organisation pour le système hydraulique

| Composants | Types de composants |
|---|---|
| Pompe | - Standard<br>- Sûr |
| API | - Standard<br>- Sûr |
| Capteur niveau | - Standard<br>- Sûr |
| Détecteur | - Standard<br>- Sûr type 1<br>- Sûr type 2 |
| Coupe-circuit | - Standard<br>- Sûr type 1<br>- Sûr type 2 |

TAB. 2.2 – Composants et alternatives pour le système d'asservissement d'une cuve

### 2.3.2 Modèle dysfonctionnel : l'arbre de défaillances multiples

Le modèle hiérarchique défini dans le paragraphe 2.3.1 donne la structure initiale du modèle comportemental. Dans l'objectif de déterminer le comportement du système lors de l'occurrence d'une défaillance, le modèle hiérarchique précédent doit être complété par une description des modes de défaillances possibles et de la propagation de leurs effets dans le système sous forme de relations entre modes de défaillances. La construction du modèle com-

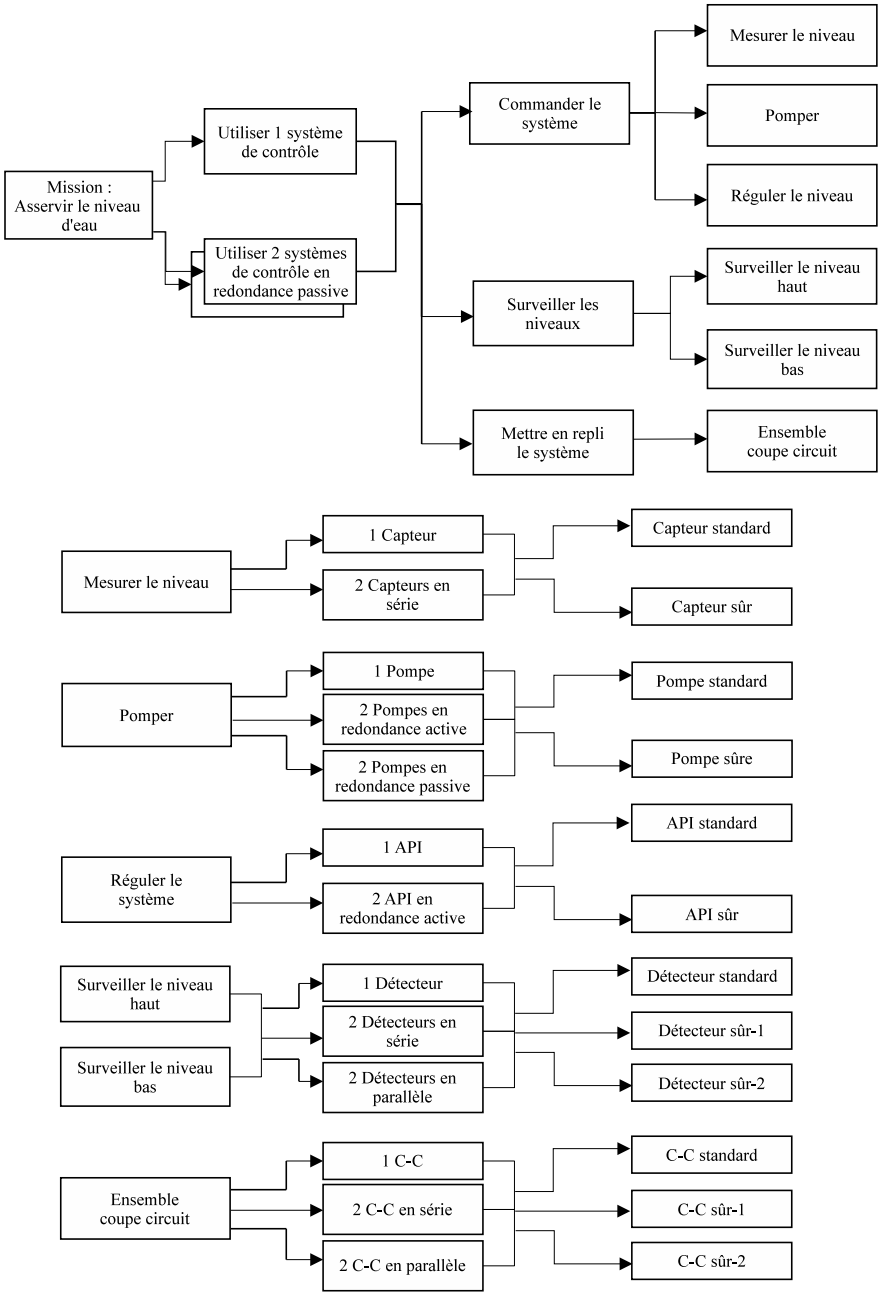


FIG. 2.6 – Modèle hiérarchique du système hydraulique

portemental appelé arbre de défaillances multiples est similaire à la construction d'un arbre de défaillances classique et reprend donc les règles de construction définies dans [VGRH81]. Nous allons présenter l'hypothèse de départ que nous avons considérée pour les modes de défaillances ainsi que l'ajout du comportement du système à l'aide de relations entre modes de défaillances.

#### 2.3.2.1 Hypothèse liée aux systèmes considérés

Dans le chapitre 1, nous avons parlé d'occurrence de modes de défaillances. Une défaillance, suivant la nature du système, peut être réparable ou non réparable. Si elle est non réparable, ses effets la font exister continuellement et ne permet pas au système de revenir dans un état normal de fonctionnement. Dans le cadre de la construction de l'arbre de défaillances multiples puis de son analyse et de son optimisation, nous considérons que tous les systèmes utilisés sont non réparables durant l'exécution d'une mission le temps de leur utilisation.

#### 2.3.2.2 Relations entre modes de défaillances

Lors de la construction de l'arbre de défaillances amélioré, il s'agit tout d'abord de lier les événements redoutés de la mission du système à concevoir aux modes de défaillances des composants. Il s'agit ensuite d'associer à chaque noeud de l'arbre (indirectement par les fonctions intermédiaires) un ensemble de relations entre modes de défaillances qui affectent l'accomplissement de la fonction correspondante.
Pour des fonctions complexes, des relations liant les modes de défaillances de la fonction complexe et les modes de défaillances de ses sous-fonctions doivent être ajoutées. Les opérateurs **AND**, **OR**, **PAND** et **SEQ**, définis dans le paragraphe 2.2.4.1, sont utilisés dans ce but. Par exemple, les deux relations entre modes de défaillances correspondant à la figure 2.7 peuvent être les suivantes :

$$\begin{gathered}(mode\ de\ défaillance\ 2A\ \textbf{PAND}\ mode\ de\ défaillance\ 3A) \\ \Rightarrow mode\ de\ défaillance\ 1A \\ (mode\ de\ défaillance\ 2B\ \textbf{AND}\ mode\ de\ défaillance\ 3B) \\ \Rightarrow mode\ de\ défaillance\ 1B\end{gathered} \tag{2.29}$$

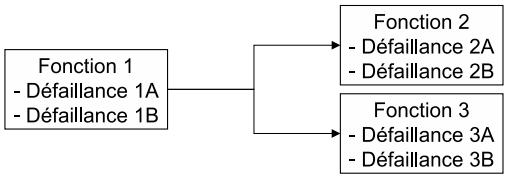


FIG. 2.7 – Exemples de modes de défaillances associés aux fonctions

Pour les noeuds alternatifs, l'ensemble des modes de défaillances n'est pas nécessairement le même que celui issu de l'ensemble des modes de défaillances des alternatives proposées. En fait, suivant la technologie utilisée et pour certaines alternatives, des modes de défaillances peuvent ne pas apparaître. Afin de prendre en compte ce cas spécifique, le RRC associé à ces

modes de défaillances qui ne doivent pas apparaître prendra une très grande valeur qui sera considérée comme infinie. De même, pour les noeuds élémentaires, le RRC associé à chaque mode de défaillance définit la fiabilité et la robustesse du composant proposé et permet de distinguer les composants standards ou sécuritaires. Enfin, pour les noeuds associatifs, l'ensemble des modes de défaillances est issu de l'ensemble des modes de défaillances du niveau hiérarchique inférieur.
Ainsi, pour chaque noeud de l'arbre, les relations entre modes de défaillances sont associées avec le même principe depuis les composants jusqu'à atteindre le sommet de l'arbre. Grâce à cette association de relations noeud par noeud, la propagation des défaillances depuis les composants à la base de l'arbre jusqu'à la mission à son sommet est ainsi facilement caractérisable et formalisable.
L'arbre de défaillances multiples ainsi obtenu modélise les réalisations technologiques possibles du système et caractérise le comportement dysfonctionnel à l'aide de relations entre défaillances pour chaque niveau de la décomposition.

**Illustration avec le système hydraulique** Si nous illustrons cette étape pour la conception du système hydraulique, nous obtenons l'arbre de défaillances multiples présenté figure 2.8 et dans les tables 2.4 et 2.5. Cet arbre caractérise le comportement du système en présence de défaillances. Pour la clarté de l'exposé, seuls deux événements redoutés sont considérés dans cet arbre mais la méthodologie s'applique aussi bien à un nombre plus important. Les événements redoutés sont au niveau système :

- La vidange inattendue de la cuve (mode de défaillance noté $ER_1$) : cet événement est causé par la mise en sécurité de l'installation suite à la détection d'une défaillance jugée dangereuse ou à des défaillances dans le système et entraîne l'arrêt du remplissage de la cuve. Cet événement rend indirectement compte de la disponibilité du système.
- Le débordement de la cuve (mode de défaillance noté $ER_2$) : suite à des défaillances, le système a un comportement dangereux pouvant entraîner le débordement de la cuve. Cet événement peut être associé à la sécurité du système.

Le tableau 2.3 donne les modes de défaillances pour les composants de base définis dans la première étape de la phase de modélisation ainsi que le coût financier et le RRC associé à chaque mode de défaillance permettant de définir les différentes robustesses de ces composants. Par exemple, il existe trois types de coupe-circuits : le standard, le sûr type 1 et le sûr type 2. Le sûr type 1 et le sûr type 2 se différencient du type standard par le fait que les modes de défaillance respectifs *bloqué ouvert* et *bloqué fermé* sont moins probables et équivalents à la probabilité d'avoir deux défaillances (RRC = 2).

Pour les relations entre modes de défaillances, nous allons utiliser les notations suivantes :

- Dans le cas d'une fonction ou d'un seul composant : $X(M)$ où X correspond à la

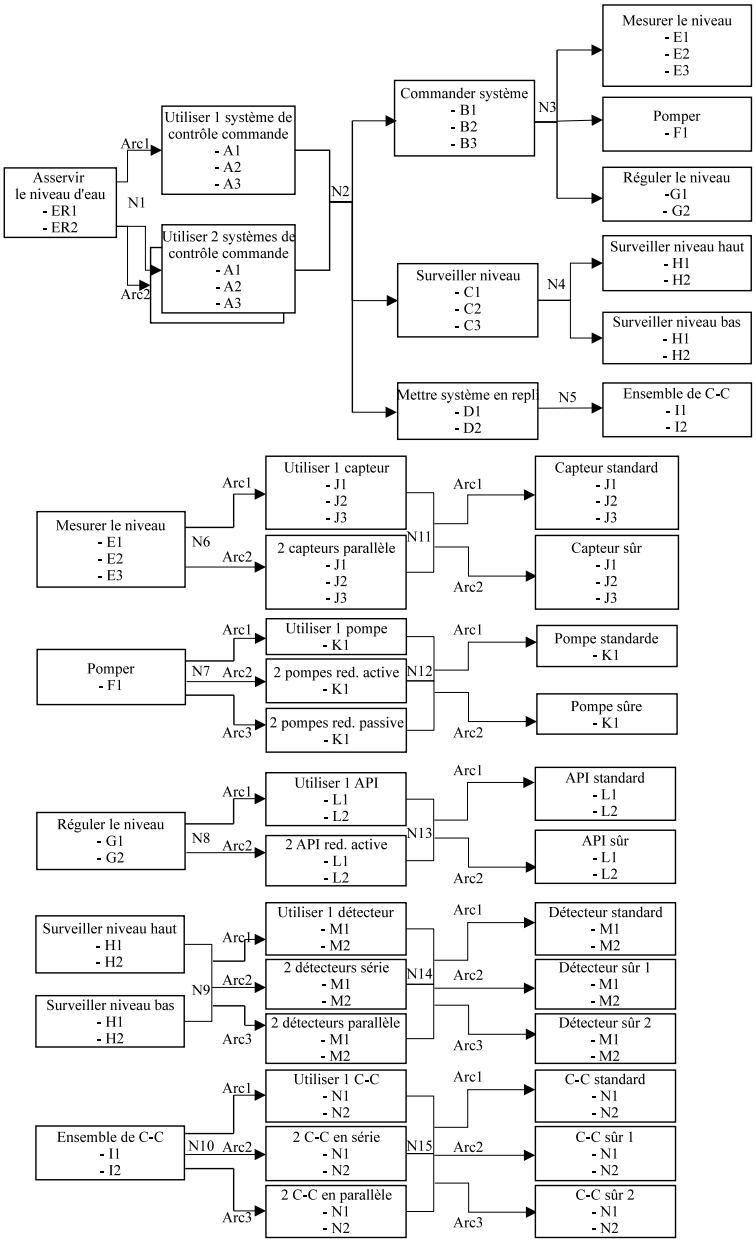


FIG. 2.8 – Arbre de défaillances multiples amélioré du système hydraulique

dénomination de la fonction (ou du composant) dans l'arbre et M au numéro du mode de défaillance correspondant à cette fonction (ce composant) dans les tableaux de correspondances.

– Dans le cas de plusieurs composants : $X_y(M)$ où X correspond à la dénomination du composant dans l'arbre de défaillances, y correspond au numéro de ce composant et M au numéro du mode de défaillance correspondant à ce composant dans les tableaux de correspondances.

| Composants | Mode de défaillance | Types de composants (Coût, {RRC}) |
|---|---|---|
| Pompe | - Arrêt inattendu | - Standard (5, {1})<br>- Sûr (10, {2}) |
| API | - Arrêt inattendu<br>- Comportement aberrant | - Standard (3, {1, 1})<br>- Sûr (8, {1, 2}) |
| Capteur niveau | - Mesure trop basse<br>- Mesure trop haute<br>- Pas de mesure | - Standard (2, {1, 1, 100[1]})<br>- Sûr (4, {2, 2, 1}) |
| Détecteur | - Continuellement actif<br>- Continuellement passif | - Standard (1, {1, 1})<br>- Sûr 1 (2, {2, 1})<br>- Sûr 2 (2, {1, 2}) |
| Coupe-circuit | - Bloqué ouvert<br>- Bloqué fermé | - Standard (1, {1, 1})<br>- Sûr 1 (2, {2, 1})<br>- Sûr 2 (2, {1, 2}) |

TAB. 2.3 – Types de composants de base et modes de défaillances du système hydraulique

Dans le but d'illustrer ces notations et d'expliquer comment les relations entre modes de défaillances sont obtenues dans cet arbre, considérons le système d'automatisation qui utilise un seul système de commande. Les deux relations entre modes de défaillances représentées par l'arc *Arc1* du noeud N1 sur la figure 2.8 sont expliquées ci dessous :

- Vidange inattendue de la cuve (noté $ER_1$ dans la table 2.4) si :
  - Le système de commande (noté *Syst.com.*) a un arrêt inattendu avec mise en route d'une alarme (mode de défaillance noté $A_1$)

  **OR**
  - La cuve se vidange sans que le système de commande ne le détecte (mode de défaillance noté $A_2$)

L'équation 2.30 formalise cette relation entre modes de défaillances.

$$Syst.com.(A_1) \textbf{ OR } Syst.com.(A_2) \Rightarrow ER_1 \tag{2.30}$$

- Débordement de la cuve (noté $ER_2$) si :
  - Le système de commande (noté *Syst.com.*) provoque un remplissage continu de la cuve (mode de défaillance noté $A_3$)

De la même façon, nous formalisons cette relation avec l'équation 2.31.

$$Syst.com.(A_3) \Rightarrow ER_2 \tag{2.31}$$

[1]Comme ce mode de défaillance ne doit pas apparaître, son RRC prend une très grande valeur qui est considérée comme infinie (cf. paragraphe 2.3.2.2).

Relations entre modes de défaillances de la figure 2.8 :

$$\text{(N1)} \begin{cases} Arc1 \begin{cases} Syst.com.(A_1)\ \textbf{OR}\ Syst.com.(A_2)\ \Rightarrow ER_1 \\ Syst.com.(A_3) \Rightarrow ER_2 \end{cases} \\ Arc2 \begin{cases} Syst.com._1(A_2)\ \textbf{OR}\ (Syst.com._1(A_1)\ \textbf{SEQ}\ Syst.com._2(A_1)) \\ \textbf{OR}\ (Syst.com._1(A_1)\ \textbf{SEQ}\ Syst.com._2(A_2)) \Rightarrow ER_1 \\ Syst.com._1(A_3)\ \textbf{OR}\ (Syst.com._1(A_1)\ \textbf{SEQ}\ (Syst.com._2(A_3)) \Rightarrow ER_2 \end{cases} \end{cases}$$

$$\text{(N2)} \begin{cases} Com.syst.(B_1)\ \textbf{OR}\ Surv.niveau(C_3) \Rightarrow A_1 \\ (Com.syst.(B_3)\ \textbf{AND}\ Surv.niveau(C_2))\ \textbf{OR} \\ (Syst.repli(D_2)\ \textbf{AND}\ Surv.niveau(C_2)) \Rightarrow A_2 \\ (Com.syst.(B_2)\ \textbf{AND}\ Surv.niveau(C_1))\ \textbf{OR} \\ (Com.systeme(B_2)\ \textbf{AND}\ Syst.repli(D_1)) \Rightarrow A_3 \end{cases}$$

$$\text{(N3)} \begin{cases} Mes.niveau(E_1)\ \textbf{OR}\ Pomper(F_1)\ \textbf{OR}\ Reg.niveau(G_1) \Rightarrow B_1 \\ Mes.niveau(E_2)\ \textbf{OR}\ Reg.niveau(G_2) \Rightarrow B_2 \\ Mes.niveau(E_3)\ \textbf{OR}\ Reg.niveau(G_2)\ \textbf{OR}\ Pomper(F_1) \Rightarrow B_3 \end{cases}$$

$$\text{(N4)} \begin{cases} Ens.Detect.Haut(H_2) \Rightarrow C_1 \\ Ens.Detect.Bas(H_1) \Rightarrow C_2 \\ Ens.Detect.Haut(H_1)\ \textbf{OR}\ Ens.Detect.Bas(H_2) \Rightarrow C_3 \end{cases}$$

$$\text{(N5)} \begin{cases} Ens.C-C(I_2) \Rightarrow D_1 \\ Ens.C-C(I_1) \Rightarrow D_2 \end{cases}$$

$$\text{(N6)} \begin{cases} Arc1 \begin{cases} Capt.niveau(J_1) \Rightarrow E_1 \\ Capt.niveau(J_2) \Rightarrow E_2 \\ Capt.niveau(J_3) \Rightarrow E_3 \end{cases} \\ Arc2 \begin{cases} (Capt.niveau_1(J_3)\ \textbf{AND}\ Capt.niveau_2(J_2))\ \textbf{OR} \\ (Capt.niveau_1(J_2)\ \textbf{AND}\ Capt.niveau_2(J_3)) \Rightarrow E_1 \\ (Capt.niveau_1(J_1)\ \textbf{SEQ}\ Capt.niveau_2(J_2))\ \textbf{OR} \\ (Capt.niveau_2(J_1)\ \textbf{SEQ}\ Capt.niveau_1(J_2)) \Rightarrow E_2 \\ (Capt.niveau_1(J_1)\ \textbf{SEQ}\ Capt.niveau_2(J_3))\ \textbf{OR} \\ (Capt.niveau_2(J_1)\ \textbf{SEQ}\ Capt.niveau_1(J_3)) \Rightarrow E_3 \end{cases} \end{cases}$$

$$\text{(N7)} \begin{cases} Arc1 \begin{cases} Pompe(K_1) \Rightarrow F_1 \end{cases} \\ Arc2 \begin{cases} Pompe_1(K_1)\ \textbf{AND}\ Pompe_2(K_1) \Rightarrow F_1 \end{cases} \\ Arc3 \begin{cases} Pompe_1(K_1)\ \textbf{SEQ}\ Pompe_2(K_1) \Rightarrow F_1 \end{cases} \end{cases}$$

$$\text{(N8)} \begin{cases} Arc1 \begin{cases} API(L_1) \Rightarrow G_1 \\ API(L_2) \Rightarrow G_2 \end{cases} \\ Arc2 \begin{cases} (API_1(L_1)\ \textbf{AND}\ API_2(L_1))\ \textbf{OR}\ (API_1(L_2)\ \textbf{OR}\ API_2(L_2)) \Rightarrow G_1 \\ (API_1(L_1)\ \textbf{SEQ}\ API_2(L_2))\ \textbf{OR}\ (API_2(L_1)\ \textbf{SEQ}\ API_1(L_2)) \Rightarrow G_2 \end{cases} \end{cases}$$

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Mission : Réguler le niveau d'eau | Noeud alternatif N1 | - ER1 : Vidange<br>- ER2 : Débordement |
| Utiliser 1 système de contrôle commande | Noeud associatif N2 | - A1 : Arrêt avec alarme<br>- A2 : Vidange non détectée<br>- A3 : Remplissage continu |
| Utiliser 2 systèmes de contrôle commande | Noeud associatif N2 | - A1 : Arrêt avec alarme<br>- A2 : Vidange non détectée<br>- A3 : Remplissage continu |
| Commander le système | Noeud associatif N3 | - B1 : Arrêt avec alarme<br>- B2 : Remplissage continu<br>- B3 : Absence de remplissage |
| Surveiller le niveau | Noeud associatif N4 | - C1 : Inactif sur niveau haut<br>- C2 : Inactif sur niveau bas<br>- C3 : Fausse alarme |
| Mettre en repli le système | Noeud élémentaire N5 | - D1 : Inactif<br>- D2 : Arrêt intempestif |
| Mesurer le niveau | Noeud alternatif N6 | - E1 : Absence de mesure<br>- E2 : Mesure trop basse<br>- E3 : Mesure trop haute |
| Pomper | Noeud alternatif N7 | - F1 : pas de pompage |
| Réguler le niveau | Noeud alternatif N8 | - G1 : Arrêt inattendu<br>- G2 : Fonctionnement aberrant |
| Surveiller le niveau haut | Noeud alternatif N9 | - H1 : Continuellement actif<br>- H2 : Continuellement passif |
| Surveiller le niveau bas | Noeud alternatif N9 | - H1 : Continuellement actif<br>- H2 : Continuellement passif |
| Ensemble de C-C | Noeud alternatif N10 | - I1 : Bloqué ouvert<br>- I2 : Bloqué fermé |
| Utiliser 1 capteur | Noeud alternatif N11 | - J1 : Absence de mesure<br>- J2 : Mesure trop basse<br>- J3 : Mesure trop haute |
| Utiliser 2 capteurs en parrallèle | Noeud alternatif N11 | - J1 : Absence de mesure<br>- J2 : Mesure trop basse<br>- J3 : Mesure trop haute |
| Utiliser 1 pompe | Noeud alternatif N12 | - K1 : Arrêt inattendu |
| Utiliser 2 pompes en redondance active | Noeud alternatif N12 | - K1 : Arrêt inattendu |
| Utiliser 2 pompes en redondance passive | Noeud alternatif N12 | - K1 : Arrêt inattendu |

TAB. 2.4 – A : Correspondance entre fonctions et modes de défaillances de la figure 2.8

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Utiliser 1 API | Noeud alternatif N13 | - L1 : Arrêt inattendu<br>- L2 : Comportement aberrant |
| Utiliser 2 API en redondance active | Noeud alternatif N13 | - L1 : Arrêt inattendu<br>- L2 : Comportement aberrant |
| Utiliser 1 détecteur | Noeud alternatif N14 | - M1 : Continuellement actif<br>- M2 : Continuellement passif |
| Utiliser 2 détecteurs en série | Noeud alternatif N14 | - M1 : Continuellement actif<br>- M2 : Continuellement passif |
| Utiliser 2 détecteurs en parallèle | Noeud alternatif N14 | - M1 : Continuellement actif<br>- M2 : Continuellement passif |
| Utiliser 1 C-C | Noeud alternatif N15 | - N1 : Bloqué fermé<br>- N2 : Bloqué ouvert |
| Utiliser 2 C-C en série | Noeud alternatif N15 | - N1 : Bloqué fermé<br>- N2 : Bloqué ouvert |
| Utiliser 2 C-C en parallèle | Noeud alternatif N15 | - N1 : Bloqué fermé<br>- N2 : Bloqué ouvert |
| Capteur standard | Pas de noeud (Composant) | - O1 : Absence de mesure<br>- O2 : Mesure trop basse<br>- O3 : Mesure trop haute |
| Capteur sûr | Pas de noeud (Composant) | - O1 : Absence de mesure<br>- O2 : Mesure trop basse<br>- O3 : Mesure trop haute |
| Pompe standard | Pas de noeud | - P1 : Arrêt inattendu |
| Pompe sûre | Pas de noeud | - P1 : Arrêt inattendu |
| API standard | Pas de noeud (Composant) | - Q1 : Arrêt inattendu<br>- Q2 : comportement aberrant |
| API sûr | Pas de noeud (Composant) | - Q1 : Arrêt inattendu<br>- Q2 : comportement aberrant |
| Détecteur standard | Pas de noeud (Composant) | - R1 : Continuellement actif<br>- R2 : Continuellement passif |
| Détecteur sûr 1 | Pas de noeud (Composant) | - R1 : Continuellement actif<br>- R2 : Continuellement passif |
| Détecteur sûr 2 | Pas de noeud (Composant) | - R1 : Continuellement actif<br>- R2 : Continuellement passif |
| C-C standard | Pas de noeud (Composant) | - S1 : Bloqué fermé<br>- S2 : Bloqué ouvert |
| C-C sûr 1 | Pas de noeud (Composant) | - S1 : Bloqué fermé<br>- S2 : Bloqué ouvert |
| C-C sûr 2 | Pas de noeud (Composant) | - S1 : Bloqué fermé<br>- S2 : Bloqué ouvert |

TAB. 2.5 – B : Correspondance entre fonctions et modes de défaillances de la figure 2.8

$$
\text{(N9)}\begin{cases}
Arc1\begin{cases} Detect.niveau(M_1) \Rightarrow H_1 \\ Detect.niveau(M_2) \Rightarrow H_2 \end{cases} \\
Arc2\begin{cases} Detect.niveau_1(M_1)\ \textbf{AND}\ Detect.niveau_2(M_1) \Rightarrow H_1 \\ Detect.niveau_1(M_2)\ \textbf{OR}\ Detect.niveau_2(M_2) \Rightarrow H_2 \end{cases} \\
Arc3\begin{cases} Detect.niveau_1(M_1)\ \textbf{OR}\ Detect.niveau_2(M_1) \Rightarrow H_1 \\ Detect.niveau_1(M_2)\ \textbf{AND}\ Detect.niveau_2(M_2) \Rightarrow H_2 \end{cases}
\end{cases}
$$

$$
\text{(N10)}\begin{cases}
Arc1\begin{cases} C - C(N_2) \Rightarrow I_1 \\ C - C(N_1) \Rightarrow I_2 \end{cases} \\
Arc2\begin{cases} C - C_1(N_1)\ \textbf{AND}\ C - C_2(N_1) \Rightarrow I_1 \\ C - C_1(N_2)\ \textbf{OR}\ C - C_2(N_2) \Rightarrow I_2 \end{cases} \\
Arc3\begin{cases} C - C_1(N_1)\ \textbf{OR}\ C - C_2(N_1) \Rightarrow I_1 \\ C - C_1(N_2)\ \textbf{AND}\ C - C_2(N_2) \Rightarrow I_2 \end{cases}
\end{cases}
$$

$$
\text{(N11)}\begin{cases}
Arc1\begin{cases} Capt.niveau - Standard(O_1) \Rightarrow J_1 \\ Capt.niveau - Standard(O_2) \Rightarrow J_2 \\ Capt.niveau - Standard(O_3) \Rightarrow J_3 \end{cases} \\
Arc2\begin{cases} Capt.niveau - Sur(O_1) \Rightarrow J_1 \\ Capt.niveau - Sur(O_2) \Rightarrow J_2 \\ Capt.niveau - Sur(O_3) \Rightarrow J_3 \end{cases}
\end{cases}
$$

Les noeuds N12 à N15 ne sont pas détaillés car ils reprennent la même structure que le noeud N11 à la différence que leurs modes de défaillances correspondent à ceux de la figure 2.8 et que le composant est remplacé par le composant correspondant (Detect.niveau-Sûr1, Pompe-Standard, ...).

## 2.4 Etape d'optimisation

L'objectif de l'étape d'optimisation est de déterminer l'ensemble des architectures optimales (au sens Pareto-optimal [Par96], [Die04]) du système d'automatisation parmi toutes les architectures potentielles décrites dans l'arbre de défaillances multiples. Une approche dite « bottom-up » est proposée et est comparable à un algorithme du type branch and bound. Nous allons décrire dans les sections suivantes le mécanisme d'optimisation que nous utilisons afin de déterminer l'ensemble des solutions optimales puis montrer qu'il est comparable à un algorithme du type branch and bound.

### 2.4.1 Algorithme d'optimisation

Le principe général de l'optimisation est de déterminer l'ensemble des solutions optimales ou *systèmes optimaux*. Cet algorithme est décomposable en deux étapes :

- La première étape est de subdiviser le problème d'optimisation en sous-problèmes selon une démarche ascendante de scrutation des noeuds de l'arbre. Ainsi, chaque noeud de l'arbre est considéré comme un sous-problème d'optimisation sur lequel nous allons ensuite déterminer les solutions optimales pour la réalisation de chaque fonction de ce noeud. Cette démarche de décomposition en sous-problèmes n'est valide que sous la contrainte d'indépendance des fonctions.
- La seconde étape est de traiter chaque sous-problème d'optimisation en deux temps :
  - La génération des solutions admissibles pour la réalisation d'une fonction.
  - La sélection des solutions optimales par comparaison des solutions deux à deux.

La figure 2.9 présente le principe général de l'algorithme d'optimisation

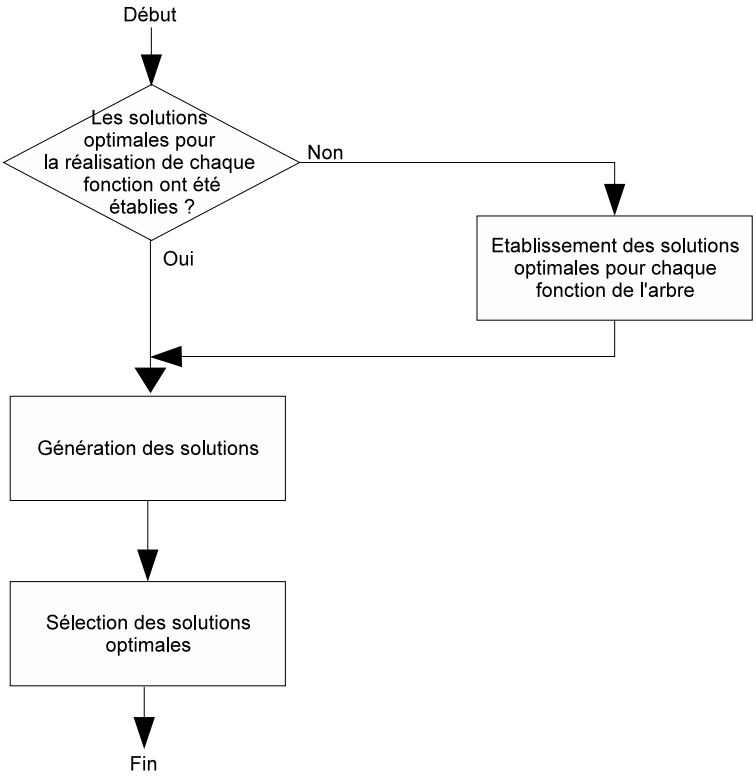


FIG. 2.9 – Principe général du mécanisme d'optimisation

#### 2.4.1.1 Génération des solutions

La génération des solutions admissibles (solutions réalisables mais pas forcément optimales) dépend du type de noeud considéré et n'est valable que grâce à l'hypothèse d'indépendance des fonctions de l'arbre :

- Pour le noeud alternatif, l'ensemble des solutions admissibles est déterminé par l'union des différentes solutions admissibles de chaque fonction.

- Pour le noeud associatif, l'ensemble des solutions admissibles est déterminé par scrutation de toutes les combinaisons de solutions admissibles de chaque fonction requise. Pour chaque combinaison de solutions, une solution est établie par l'évaluation :
  - du coût par addition des coûts individuels des solutions de la combinaison étudiée.
  - du niveau de sûreté de fonctionnement en utilisant, pour chaque mode de défaillance, les lois de composition correspondantes aux opérateurs de la relation associée à ce mode de défaillance.
- Pour le noeud élémentaire utilisé à la base de l'arbre, l'ensemble des solutions admissibles est composé d'une seule solution caractérisée par le coût de son composant et par un niveau de sûreté de fonctionnement composé des couples :
  - La valeur du RCC permettant de caractériser sa robustesse (standard, sécuritaire, durci, ...) pour le mode de défaillance considéré.
  - Le nombre de scénarios amenant au mode de défaillance considéré ($N_{min}$) égal à 1.

La figure 2.10 présente ce mécanisme d'établissement tenant compte des trois types de noeuds.

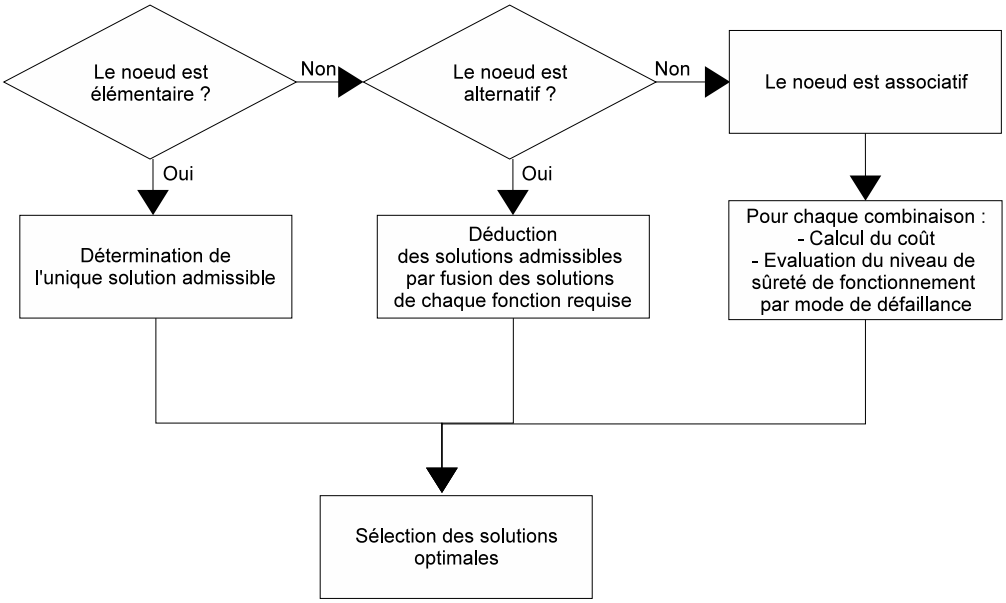


FIG. 2.10 – Schéma du mécanisme d'établissement des solutions suivant le type de noeud pris en considération

### 2.4.1.2 Sélection des solutions optimales

Les solutions de l'ensemble des solutions admissibles sont comparées entre elles deux à deux. Cette comparaison ayant pour objectif de déterminer la meilleure des deux solutions est effectuée au sens de la définition 2.5 du paragraphe 2.2.3. Les solutions moins bonnes et

donc non-optimales sont ensuite éliminées de l'ensemble.
A la fin de l'étape d'optimisation, la méthodologie fournit l'ensemble Pareto-optimal, c'est à dire qu'il n'existe pas de solutions qui fassent diminuer un critère sans augmenter dans le même temps au moins un autre critère. La figure 2.11 représente le principe de comparaison puis d'élimination des solutions non-optimales.

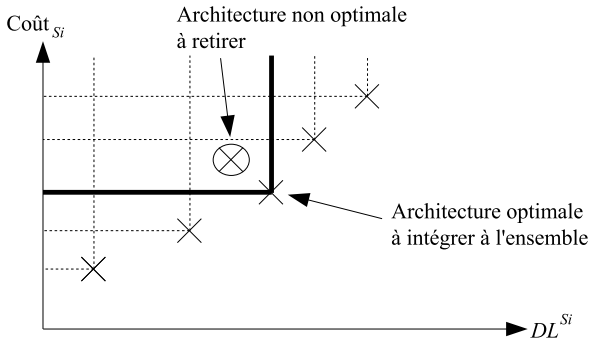


FIG. 2.11 – Constitution d'un ensemble de solution d'après [CB06a]

#### 2.4.1.3 Aspect pratique

D'un point de vue plus pratique, la construction de l'ensemble des solutions optimales se fait selon une démarche progressive :

- L'ensemble des solutions optimales est initialement vide.
- Cet ensemble est d'abord construit avec les solutions optimales de chaque fonction en commencant par les plus basses dans l'arbre de défaillances, c'est-à-dire en générant les solutions admissibles et en sélectionnant les premières solutions optimales.
- Cet ensemble est ensuite progressivement construit au fur et à mesure que l'on remonte l'arbre jusqu'à son sommet. Pour cela, à chaque noeud, on génère et on sélectionne les nouvelles solutions optimales en comparant chaque nouvelle solution admissible avec celles précédemment trouvées. Plus précisément, une nouvelle solution admissible est ajoutée à l'ensemble optimal seulement s'il n'existe pas de meilleure solution dans cet ensemble. C'est-à-dire si son coût est inférieur à celui d'une solution de l'ensemble optimal ou si son niveau de sûreté de fonctionnement est supérieur comme défini dans la propriété 2.8 du paragraphe 2.2.3. Basé sur le même principe, quand une nouvelle solution est ajoutée, si d'autres solutions sont moins bonnes que la nouvelle, elles sont retirées de l'ensemble optimal.

La figure 2.12 présente ce mécanisme de construction des solutions.

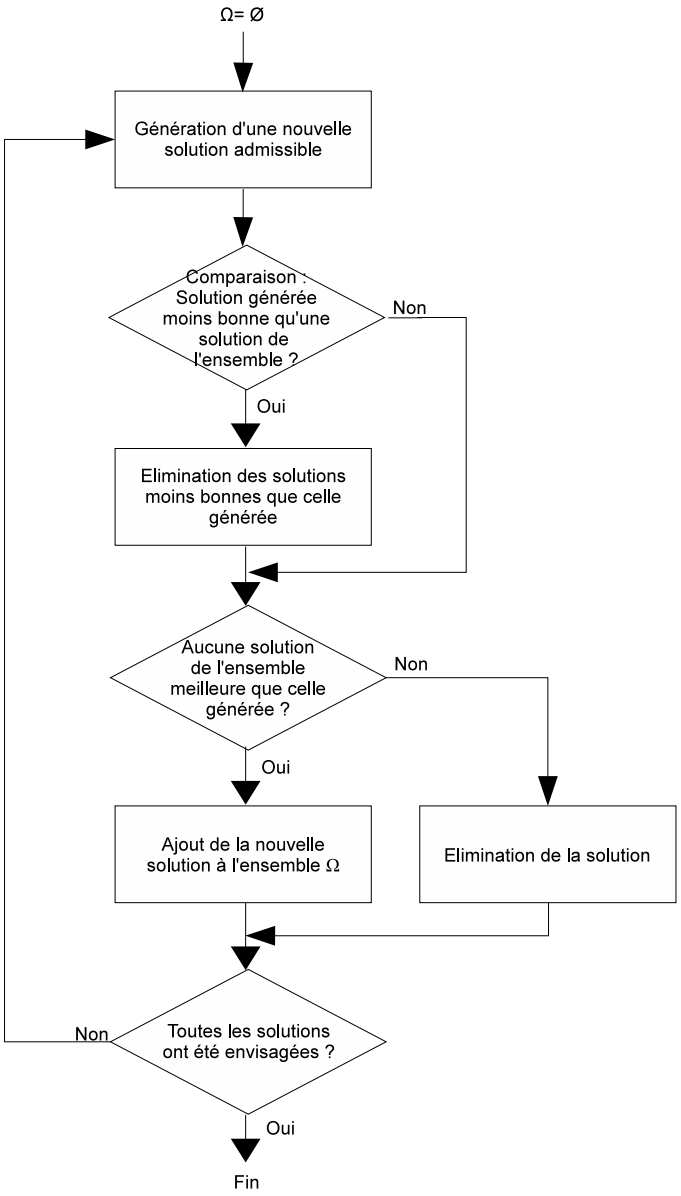


FIG. 2.12 – Schéma du mécanisme de construction des solutions

### 2.4.2 Comparaison avec la méthode d'optimisation du type branch and bound

Dans ce paragraphe, nous allons voir que l'algorithme d'optimisation que nous avons utilisé est comparable à celui du branch and bound.

L'algorithme du type branch and bound (procédure par séparation progressive *branch* et évaluation *bound*) consiste à énumérer une partie des architectures admissibles et à

déterminer celles qui sont intéressantes en utilisant certaines propriétés du problème d'optimisation afin d'éliminer les architectures partielles qui ne mènent pas à l'architecture que l'on recherche [DPP06].
L'algorithme commence par considérer le problème d'optimisation avec son ensemble de solutions. Une propriété définie par le concepteur (la détermination d'une borne) est appliquée sur les premières solutions de cet ensemble pour soit les exclure soit les maintenir comme des solutions potentielles. L'ensemble des solutions est ensuite subdivisée en deux sous-problèmes suivant une démarche également définie par le concepteur. La méthode est ensuite appliquée récursivement à ces sous problèmes. Si une solution optimale est trouvée pour un sous-problème, elle est potentiellement admissible, mais pas nécessairement optimale pour le problème de départ. Cependant, comme elle est admissible, elle peut être utilisée pour éliminer toute sa descendance : si la borne de la solution admissible dépasse la valeur d'une solution optimale déjà connue, alors on peut affirmer que la solution optimale ne peut être contenue dans ce sous ensemble de solutions. On élimine ainsi des groupes de solutions non-optimales. La recherche continue jusqu'à ce que tous les sous-problèmes soient optimisés.

L'algorithme du branch and bound est comparable avec celui que nous utilisons et cela pour deux raisons :

- Nous utilisons le même principe de subdivision du problème initial en sous-problèmes à optimiser à l'aide des noeuds de notre arbre de défaillances.
- Nous utilisons le même principe d'élimination de groupes de solutions non-optimales que cet algorithme. En effet, par l'élimination des solutions non-optimales d'une fonction, on restreint la recherche aux solutions potentiellement optimales.

**Optimisation de grands systèmes** Pour l'optimisation de très grands systèmes, cette méthode d'optimisation peut être utilisée mais en imposant des contraintes permettant de réduire l'espace des solutions :

- soit en imposant une contrainte sur le coût maximal des solutions à obtenir. Cette limite permet de ne pas considérer au sein de notre méthode des solutions plus chères que ce coût.
- soit en imposant une limite sur les niveaux de sûreté de fonctionnement. Les solutions ayant une séquence amenant à un événement redouté de longueur supérieure à une certaine longueur ne sont pas considérées.

**Optimisation avec des fonctions partagées** L'approche proposée d'optimisation ne s'applique que sous l'hypothèse d'indépendance des fonctions de l'arbre. Or, dans certaines situations, une fonction se comporte comme une ressource commune à plusieurs autres fonctions. C'est notamment le cas d'unités de traitement qui effectuent des opérations afin de rem-

plir plusieurs fonctions. Ces situations correspondent à des fonctions dites *partagées* ou *ressource commune*. Bien que notre approche de modélisation permette de représenter ces fonctions partagées, notre approche d'optimisation ne permet pas d'optimiser immédiatement de tels systèmes. Ainsi, suivant le nombre de ces fonctions partagées, deux approches peuvent être envisagées :

- Si les fonctions partagées sont peu nombreuses et/ou distinctes (non dépendantes d'autres fonctions partagées), la transposition du modèle fonctionnel en un modèle fonctionnel sans fonctions partagées est effectuée. Un exemple illustré de transposition est présenté figure 2.13. Sur cette figure, le modèle (a) comporte une fonction partagée notée B utilisée par les fonctions F1 et F2. Ce modèle peut être modifié en modèle (b) afin de retirer cette fonction partagée. Les deux modes de défaillances ($FM^1_{FTop}$ et $FM^2_{FTop}$) de la fonction sommet ($F_{Top}$) sont les mêmes pour les deux modèles quelle que soit la combinaison de composants défaillants (A, B et C) considérée. Ainsi, les deux modèles peuvent être considérés comme *équivalents* et la méthode d'optimisation peut être utilisée.
- Si les fonctions partagées sont nombreuses et/ou interdépendantes entre elles, l'utilisation d'un autre algorithme d'optimisation avec une évaluation de la longueur et du nombre de combinaisons des scénarios du système peut être une solution. Des recherches en ce sens, sont en cours.

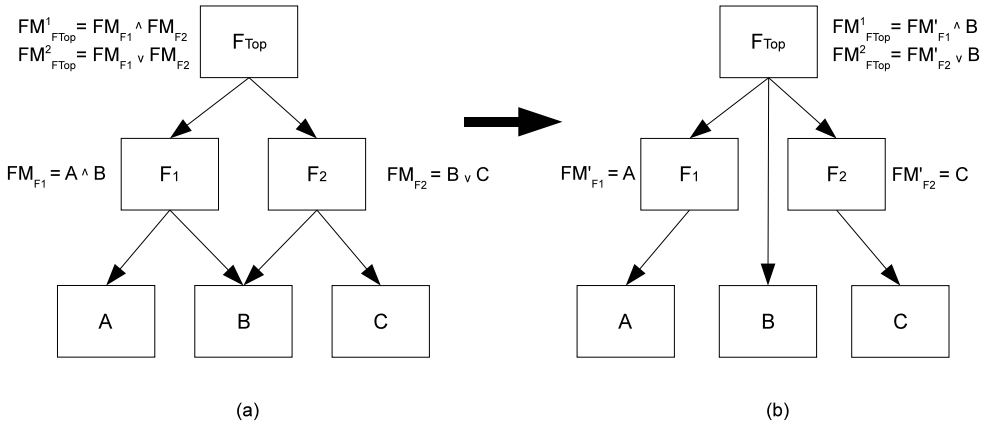


FIG. 2.13 – Exemple de transposition d'un modèle fonctionnel (a) en un modèle fonctionnel sans ressources partagées (b)

### 2.4.3 Obtention des architectures matérielles optimales

Lors de l'évaluation et de l'optimisation de l'arbre de défaillances et pour chaque solution optimale déterminée, notre méthodologie donne les composants de base utilisés et leur orga-

| Nombre de solutions et coûts | | $L_{min}$ des scénarios pour $ER_1$ 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $L_{min}$ des scénarios pour $ER_2$ | 2 | 1 système C : 13 | 2 systèmes C : 26, 27 | 2 systèmes C : 47, 48 | Pas de système |
| | 3 | 1 système C : 15 | 4 systèmes C : 28 à 31 | Pas de système | Pas de système |
| | 4 | 1 système C : 17 | 5 systèmes C : 32 à 35 | 8 systèmes C : 49 à 54 | 19 systèmes C : 71 à 76 |

TAB. 2.6 – Synthèse des systèmes d'automatisation optimaux trouvés

nisation dans l'architecture. Ainsi, le type de redondance, le nombre et le type de composants sont précisément définis pour chaque solution optimale trouvée.

**Illustration avec le système hydraulique** L'évaluation de l'arbre de défaillances multiples amélioré par la méthode d'optimisation donne 43 solutions optimales pour le système d'automatisation. La table 2.6 synthétise ces solutions par rapport aux deux événements redoutés $ER_1$ et $ER_2$. Le nombre de solutions ainsi que les coûts minimum et maximum sont donnés pour chaque niveau de sûreté de fonctionnement.

| Solutions ayant une longueur minimale de 4 pour $ER_1$ et $ER_2$ | | | | | | |
|---|---|---|---|---|---|---|
| Coût du système | 71 | 72 | 73 | 74 | 75 | 76 |
| $N_{min}$ pour $ER_1$ : Vidange inattendue | 156 | 132 | 120 | 108 | 100 | 124 |
| $N_{min}$ pour $ER_2$ : Débordement | 64 | 64 | 64 | 72 | 76 | 60 |

TAB. 2.7 – Détails de systèmes issus de la table 2.6

La table 2.7 montre quelques solutions issues de la table 2.6 dont la longueur minimale des scénarios redoutés ($L_{min}$) est égale à 4 pour chaque événement redouté. On constate dans cette table que si des composants sont ajoutés, le coût global du système augmente et le nombre de combinaisons de ces scénarios ($N_{min}$) diminue pour les deux événements redoutés jusqu'à un niveau précis. Par exemple, la solution ayant un coût de 74 unités montre que le nombre de combinaisons de ces scénarios ($N_{min}$) augmente pour l'événement redouté $ER_2$. Cela est dû à un nombre très important de composants dans cette architecture. En effet, plus il y a de composants dans une architecture, plus importante est la probabilité d'un composant d'être défaillant. Il est donc important de choisir une bonne architecture représentant un bon compromis entre le coût et le niveau de sûreté de fonctionnement. C'est pourquoi, afin de permettre au concepteur de pouvoir décider quel système correspond le mieux à son cahier des charges, nous lui proposons un ensemble d'architectures optimales possibles ayant des caractéristiques clairement identifiées.

Par exemple, une solution optimale obtenue avec notre approche est présentée figure 2.14. Cette solution a un coût de 71 unités et la longueur minimale des scénarios redoutés est de

4 pour les deux événements redoutés. C'est-à-dire que cette architecture est tolérante à 3 modes de défaillances. Elle utilise deux systèmes de commande en redondance passive. Le premier système de commande utilise :

- un système de mesure du niveau d'eau composé de deux capteurs standards,
- un système de pompage composé de deux pompes standards en redondance passive,
- un système de régulation composé de deux automates sûrs en redondance active,
- un système de surveillance des niveaux composé d'un détecteur sûr type 1 pour le niveau haut et de deux détecteurs sûr de type 1 en parallèle pour le niveau bas,
- et un système de mise en repli composé d'un seul coupe-circuit sûr de type 1.

Le second système de commande utilise quant à lui :

- un système de mesure du niveau d'eau composé d'un capteur standard,
- un système de pompage composé de deux pompes standards en redondance passive,
- un système de régulation composé de deux automates sûrs,
- un système de surveillance composé d'un détecteur sûr type 1 pour le niveau haut et d'un détecteur sûr de type 2 pour le niveau bas,
- un système de mise en repli composé d'un seul coupe-circuit standard.

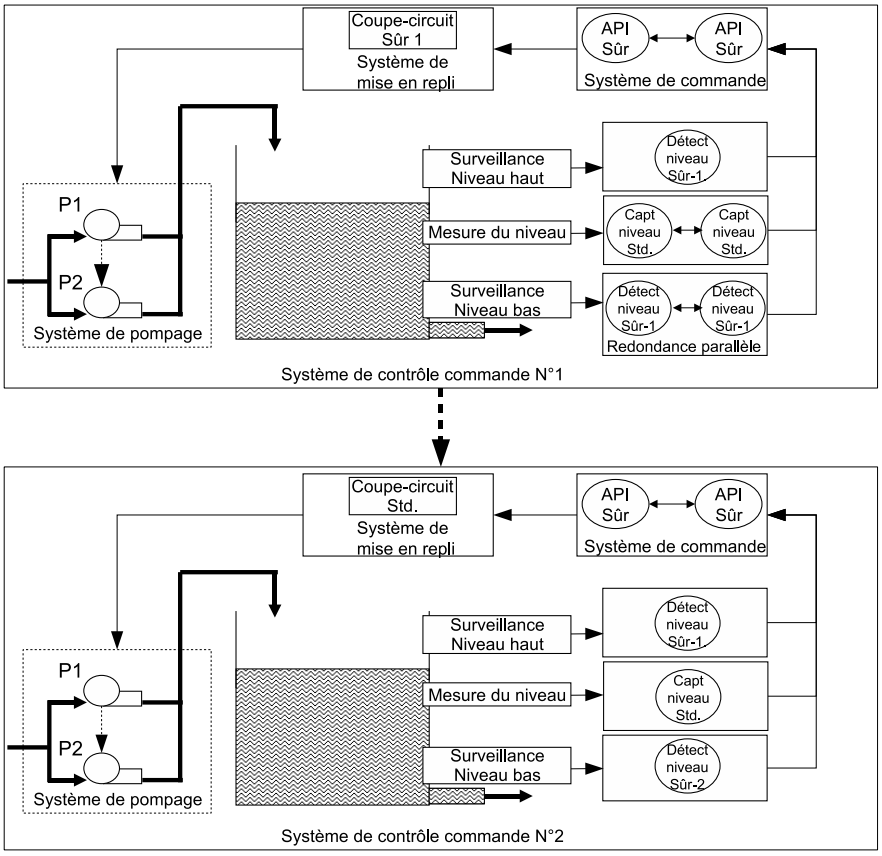


FIG. 2.14 – Architecture opérationnelle optimale pour le système hydraulique d'automatisation

## 2.5 Présentation de la plate forme ALoCSyS

Durant ces travaux de recherche une plateforme de conception nommée ALoCSyS (pour Atelier Logiciel de Conception de Systèmes Sûrs) a été développée.
ALoCSyS désigne l'outil automatisant l'ensemble des opérations nécessaires pour passer du modèle comportemental décrivant l'arbre de défaillances multiples au calcul des paramètres de sûreté de fonctionnement et à la détermination des architectures opérationnelles offrant le meilleur compromis entre coût et niveau de sûreté de fonctionnement.

Parmi les applications possibles d'ALoCSyS, en plus des applications pour le domaine des transports guidés, on peut citer :

- la conception de systèmes d'automatisation de procédés industriels à risques, tels que le nucléaire, la chimie ou la pétrochimie,
- la révision de la conception de ces mêmes systèmes dans l'objectif d'améliorer leurs caractéristiques,
- l'évaluation du niveau de sûreté de fonctionnement des systèmes de haute technologie (systèmes embarqués, médical).

### 2.5.1 Description de la plateforme actuelle

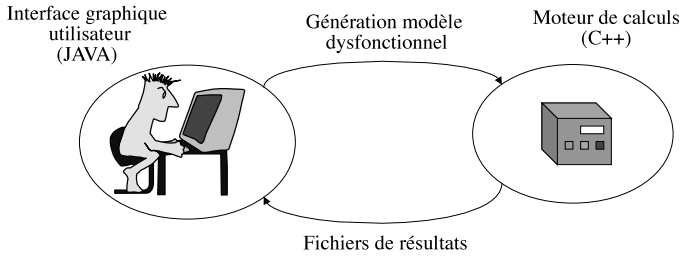


FIG. 2.15 – Architecture actuelle de la plateforme ALoCSyS

Comme présentée figure 2.15, ALoCSyS se compose actuellement de deux éléments :

- Une interface graphique, écrite en langage JAVA, permet d'orienter le concepteur dans l'introduction des données de son modèle dysfonctionnel (composants, fonctions, sous-fonctions, noeuds et relations entre modes de défaillances) puis d'afficher les résultats obtenus. Une vue de la fenêtre de saisie des données de cette interface est présentée figure 2.16. De plus, les autres fenêtres de cette interface (fenêtre principale, fenêtre de saisie, fenêtre d'affichage du modèle et fenêtre de résultats) sont présentées en annexe C.1.

– Un moteur de calculs, écrit en langage C++, qui intègre l'algorithme d'optimisation du type branch and bound. Ce moteur utilise le modèle saisi par le concepteur et génère des fichiers de résultats. Les codes C++ d'un noeud élémentaire, alternatif et associatif sont présentés en annexe C.2.

La raison de l'utilisation de deux langages de programmation est liée à la volonté de profiter des avantages de chacun d'eux : le langage C++ avec sa puissance de calcul et le langage JAVA avec sa facilité de création d'une interface graphique. Par ailleurs, l'avantage de l'utilisation de ces deux langages de programmation est de permettre une portabilité de la plateforme sur différents systèmes d'exploitation.

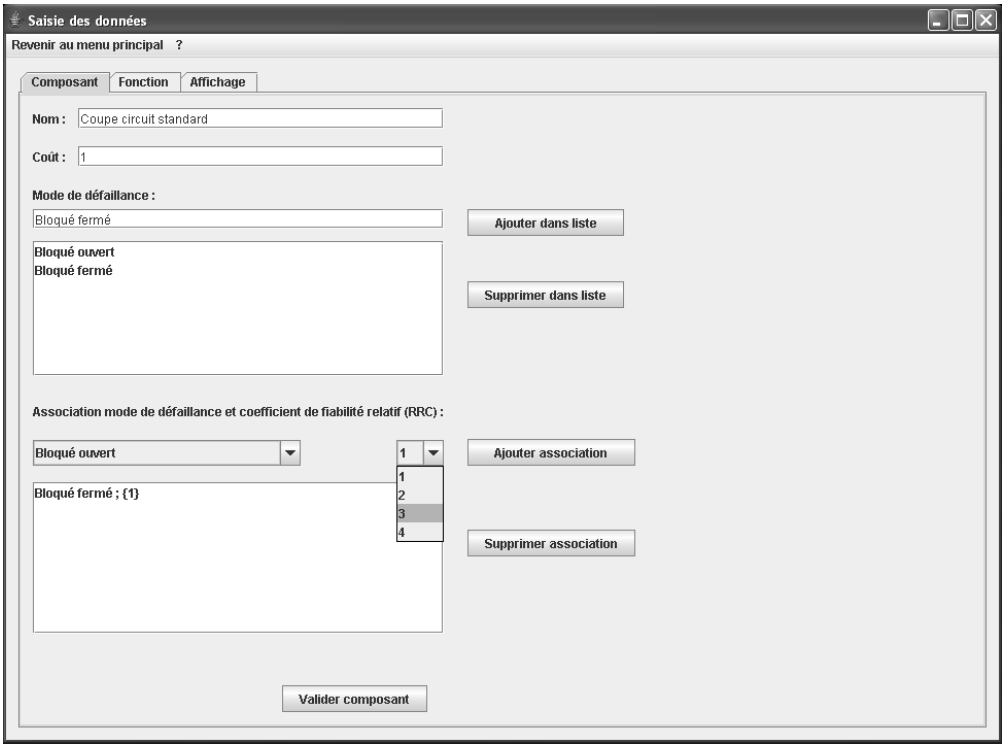


FIG. 2.16 – Vue d'écran de l'interface graphique d'ALoCSyS

Avec ALoCSyS, l'analyse de l'arbre de défaillances multiples produit les résultats dans deux fichiers séparés :

– Un fichier *listing.txt* comprenant la liste des architectures optimales trouvées classées en ordre décroissant selon leur coût financier et leur niveau de sûreté de fonctionnement (longueur minimale des scénarios critiques et nombre de scénarios minimaux). Une liste d'architectures optimales générée par ALoCSyS pour le système hydraulique est présentée en annexe C.3.

– Un fichier *structures.txt* comprenant le détail des architectures optimales trouvées : nombre et types des composants utilisés, type de redondance employée et organisation

générale du système. L'architecture optimale détaillée de la figure 2.14 issue de ce fichier est présentée en annexe C.4.

### 2.5.2 Améliorations envisagées

Nous envisageons des améliorations à la plateforme actuelle [Har08], présentées figure 2.17, et qui ont les objectifs suivants :

- Améliorer l'interface graphique afin de la rendre plus conviviale pour l'utilisateur, c'est-à-dire le guider dans la saisie de ses données et dans la recherche des erreurs de saisie.
- Aider le concepteur à construire rapidement le modèle hiérarchique fonctionnel et l'arbre de défaillances multiples amélioré en lui fournissant un certain nombre d'objets dont les comportements fonctionnels et dysfonctionnels sont prédéfinis et regroupés dans une base de données. Cette base de données pourra être enrichie par l'utilisateur au fur et à mesure de ses expérimentations.
- Générer une documentation complète imprimable du modèle avec les résultats obtenus.
- Transférer les résultats vers les tableurs du commerce afin de présenter graphiquement ou dans différents tableaux les résultats des calculs.

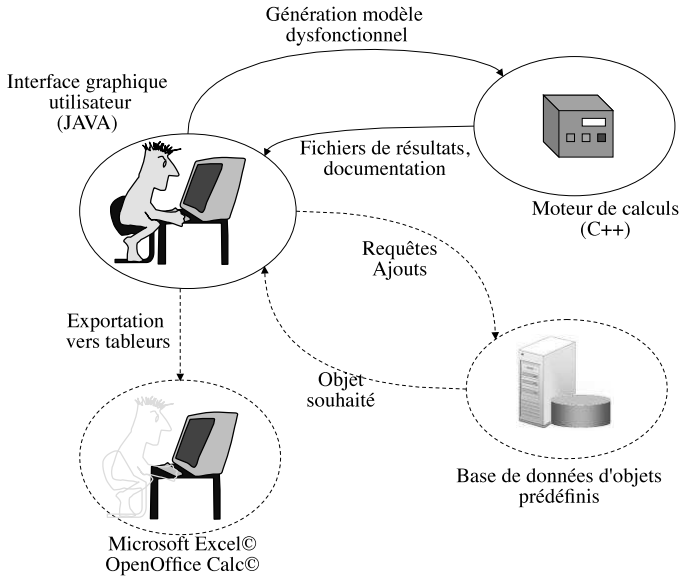


FIG. 2.17 – Architecture envisagée de la plateforme ALoCSyS

## 2.6 Conclusion

Dans ce deuxième chapitre, nous avons proposé une nouvelle approche méthodologique pour la conception de systèmes d'automatisation sûrs de fonctionnement. Cette approche a

pour objectif d'évaluer le niveau de sûreté de fonctionnement d'un ensemble d'architectures matérielles, composé de nombreuses possibilités, en s'appuyant sur les scénarios. L'utilisation des scénarios permet de tenir compte de particularités présentées au chapitre 1 liées à la complexité des systèmes d'automatisation. Le concepteur de ces systèmes d'automatisation pourra faire le choix de l'architecture optimale correspondant le mieux aux critères de son cahier des charges.
La première partie de ce chapitre s'est d'abord attachée à définir clairement les concepts, les formalisations et les notations utilisées pour cette nouvelle approche. Plus précisément, la caractérisation d'un système est effectuée par le paramètre du coût financier de ce système et par deux variables caractérisant le niveau de sûreté de fonctionnement que sont :

- la longueur minimale des scénarios de pannes et,
- le nombre de combinaisons de ces scénarios.

Par ailleurs, des noeuds fonctionnels et des opérateurs temporels ont été définis. Ils permettent, respectivement, de représenter les différentes possibilités de conception et d'établir le comportement dysfonctionnel du système à concevoir.
La deuxième partie de ce chapitre a exposé la première étape de la méthodologie proposée, c'est-à-dire l'étape de modélisation. Cette étape a pour objectif de représenter le système du point de vue fonctionnel et comportemental en déterminant un modèle basé sur les arbres de défaillances : "l'arbre de défaillances multiples amélioré". Cette modélisation cherche à surmonter le problème de l'intégration des scénarios au sein d'un modèle graphique.
La troisième partie de ce chapitre a illustré la seconde étape de la méthodologie, c'est-à-dire l'étape d'optimisation. Cette étape analyse l'arbre de défaillances suivant un algorithme comparable à celui du *branch and bound* et recherche les systèmes potentiellement optimaux. Ainsi, un ensemble de systèmes optimaux est déterminé et constitué.
Enfin, la dernière partie de ce chapitre a décrit les fonctionnalités de la plateforme informatique ALoCSyS issue de ces travaux de recherche. Les développements futurs de cette plateforme comme la génération de documentations et l'intégration d'une base de données d'objets prédéfinis ont notamment été présentés.

Dans un but purement illustratif de notre méthodologie, la conception d'un système de régulation du niveau d'eau d'une cuve a été présentée tout au long de ce chapitre. Cet exemple a permis de détailler la construction des différents modèles proposés et d'expliquer la signification des résultats obtenus, notamment l'influence du nombre de composants sur le nombre de combinaisons de scénarios. Dans le dernier chapitre de cette thèse, une comparaison entre notre méthodologie et une méthode plus classique d'évaluation du niveau de sûreté de fonctionnement montrera clairement les contributions de cette nouvelle approche.

La deuxième partie est consacrée à l'application de notre méthodologie dans le domaine du ferroutage. Le chapitre 3 présente le ferroutage et précise le concept du wagon intelligent

de ferroutage permettant de réduire les risques d'accidents. Le modèle fonctionnel de ce wagon est également détaillé. Le chapitre 4 applique notre méthodologie pour la conception de deux systèmes de protection du wagon intelligent puis compare les résultats obtenus avec ceux issus d'une méthode d'évaluation plus classique.

# Seconde partie :

# Application au ferroutage

# Chapitre 3

# Le wagon intelligent pour améliorer la sûreté de fonctionnement du ferroutage

## 3.1 Introduction

La sécurité des systèmes de transport guidé est assurée par l'utilisation de divers systèmes qui sont considérés comme garants du niveau de sécurité du système global. La conception de ces systèmes de sécurité fait l'objet de nombreuses normes qui prescrivent précisément les conditions de conception et de test afin d'attester de leur caractère sécuritaire et du niveau de sécurité obtenu [Sch02]. Cependant, dans le cadre du système de ferroutage, l'absence de normes spécifiques, tenant compte des particularités de ce système, ne permet pas de déterminer les conditions de conception et de test de ces systèmes sécuritaires. Cela est dû au caractère innovant du système de ferroutage. Ce caractère relativement innovant, l'intensification prévue du ferroutage afin de réduire la congestion routière et les accidents impliquant ces systèmes de ferroutage démontrent qu'il existe un besoin d'ajouter des systèmes de sécurité au système actuel. Prévu dans le but de réduire les risques d'accident du système de ferroutage, l'ajout de systèmes de sécurité au système de ferroutage est de ce fait de plus en plus nécessaire.

La première partie de ce chapitre présente le principe de fonctionnement du ferroutage et les besoins liés à son développement actuel. Les accidents impliquant les systèmes de ferroutage démontrent les besoins grandissants en un système de ferroutage sécurisé.

La seconde partie de ce chapitre porte sur la classification des risques pouvant exister lors de l'exploitation des systèmes de transport guidé, c'est-à-dire les différents types d'accidents

pouvant intervenir. Elle vise à identifier les différents événements redoutés du système de ferroutage.

La troisième partie de ce chapitre propose le concept du wagon intelligent, extension de la notion de composant intelligent, qui participe plus activement à la sûreté de fonctionnement du système global de ferroutage. La présentation de deux accidents ferroviaires des années 90 illustre l'intérêt de ce nouveau concept et les moyens de réduction des risques d'accidents. Se basant sur la démarche de conception de systèmes d'automatisation sûrs de fonctionnement présentée au chapitre 1, l'architecture fonctionnelle du wagon intelligent est proposée pour les trois phases de fonctionnement de ce système ferroviaire. Enfin, à titre d'illustration, la présentation de deux systèmes de protection qui pourraient être implantés sur le wagon est effectuée. Ces deux systèmes seront conçus à l'aide de notre méthodologie dans le dernier chapitre.

## 3.2 Présentation du ferroutage

Dans cette section, nous présentons la place du ferroutage dans le réseau de transport ferroviaire français, son principe de fonctionnement ainsi que ses atouts et les besoins liés à son développement. Nous verrons également le contexte normatif sécuritaire ferroviaire qui introduira les risques et besoins sécuritaires liés au ferroutage.

### 3.2.1 Ferroutage et réseaux de transport ferroviaires

En France, il existe différents réseaux de transport ferroviaires qui sont présentés ci-après :

- Le réseau à grande vitesse : Sur ce réseau circulent des trains de voyageurs comme le TGV (Train à Grande Vitesse - France), le Thalys (France-Belgique-Allemagne) et l'Eurostar (France-Angleterre-Belgique). La particularité de ce réseau est que les trains circulent à des vitesses commerciales pouvant dépasser les 300 km/h. Ces vitesses élevées posent des contraintes importantes d'anticipation des dangers extérieurs pour les conducteurs et lors de l'arrêt des trains qui demandent une distance de freinage importante. Ce réseau nécessite donc des infrastructures et des équipements adaptés. On peut citer l'absence d'interaction avec le trafic routier (pas de passage à niveau), les barrières de deux mètres de hauteur autour des voies afin d'empêcher l'intrusion d'un animal ou d'un humain en zone de circulation, des courbures de virage larges, une signalisation embarquée en cabine transmise par balises (ERTMS).
- Le réseau urbain et suburbain : Sur ce réseau circulent les RER (Réseau Express Régional) et les tramways métropolitains, qui englobent une grande part des transports en commun des grandes villes. La vitesse autorisée sur ces réseaux est faible (50km/h)

et les véhicules y circulant sont qualifiés de légers. Ils nécessitent des distances de freinage plus petites. Ce réseau fait transiter un flux de personnes très dense sur une surface moins étendue que pour les autres réseaux.

- Le réseau conventionnel : Sur ce réseau circulent des wagons de fret et/ou des voitures de passagers à des vitesses commerciales modérées, de l'ordre des vitesses observées dans le trafic routier (jusqu'à 120km/h). Les véhicules circulant sur ces réseaux sont qualifiés de lourds et nécessitent des grandes distances de freinage. Par ailleurs, ils interagissent avec le réseau routier au travers des passages à niveau. Parmi les wagons de fret se trouve une offre de transport combiné Rail-Route qui tend actuellement à se diversifier. Deux concepts plus ou moins concurrents s'affrontent :
  - Le transport de conteneurs également appelé transport combiné non accompagné. Les conteneurs sont des boîtes métalliques, qui ont été inventées pour le trafic maritime. Les plus répandus sont les 40 pieds (12,2 m de longueur), mais on utilise aussi des 20 et parfois des 30 pieds. Ils sont normalisés en largeur, mais pas en hauteur. On mesure le trafic en EVP (Equivalent Vingt Pieds). Le transport combiné utilise également des « caisses mobiles », moins lourdes que les conteneurs, mais inaptes au trafic maritime, car ils ne peuvent être gerbés.
  - Le transport par ferroutage également appelé transport combiné accompagné. Le ferroutage est un terme générique, désignant l'ensemble des techniques qui permettent de charger des camions complets sur un train : tracteur routier plus remorque plus chauffeur. Le lecteur intéressé pourra se référer à l'annexe D où un état de l'art complet des différents systèmes et projets de ferroutage est décrit ainsi qu'une classification de ces systèmes.

### 3.2.2 Principe de fonctionnement et atouts

Nous venons de voir que le ferroutage est basé sur la technique du transport de camions sur des trains spéciaux tout en respectant le gabarit GB1. Le GB1, détaillé en annexe E, est le plus petit gabarit dans lequel il est techniquement possible d'inscrire un camion standard Européen. Plus précisément, le ferroutage est fondé sur une Unité de Transport Intermodal (UTI), dans laquelle la marchandise est transportée de bout en bout par le mode de transport le plus approprié :

- le mode de transport routier seulement utilisé en desserte d'extrémité (trajet initial et terminal), avec un parcours le plus court possible.
- le mode de transport ferré pour le parcours principal.

Le rapport entre ces deux phases du transport fait que la distance de pertinence généralement admise pour le ferroutage est supérieure à 500 km. En effet, une telle distance permet *d'amortir* le coût induit par les chargements et déchargements liés aux changements de mode de transport, propre au transport multimodal. Ainsi, en France, l'importance des trafics de

longue distance, due à l'éloignement des principales régions urbaines entre elles, constitue un véritable atout pour le développement du ferroutage. Il doit permettre de délester le réseau routier du trafic longue distance.
En effet, en plus de son objectif de désengorger le trafic routier, le ferroutage possède de nombreux atouts :

- Environnementaux : le ferroutage contribue à la diminution de la pollution de l'air et à la réduction de la consommation de carburant.
- Sécuritaires : il contribue à la diminution des risques d'accidents impliquant des poids lourds à la réduction du nombre de matières dangereuses transportées par la route.

Le lecteur intéressé pourra se reporter à l'annexe F dans laquelle les atouts du ferroutage sont détaillés.

### 3.2.3 Premiers besoins liés au développement du ferroutage

Malgré ses atouts, le taux de pénétration du ferroutage reste faible (la part modale en tonnes-kilomètres comparativement à la route est de l'ordre de 7% en 2005). Afin de concurrencer le transport routier en termes de compétitivité, ce système doit se développer. Pour cela, de nombreux projets dits "d'Autoroute Ferroviaire" (terme désignant les projets Français de lignes ferroviaires par ferroutage détaillés en annexe G) sont en cours de réalisation et impliqueront une augmentation importante du trafic par ferroutage. Les systèmes de ferroutage utilisés actuellement ou ceux en projet nécessiteront d'avoir une disponibilité et un niveau de sécurité élevés afin de pouvoir répondre à cette augmentation de trafic tout en conciliant les besoins liés à la sécurité ferroviaire. Nous allons préciser ces exigences sécuritaires ferroviaires dans les paragraphes suivants puis détailler les risques liés au système ferroviaire en général et au ferroutage en particulier. Cette présentation des risques et des besoins en découlant permettra d'introduire le concept du wagon intelligent répondant à ces besoins.

### 3.2.4 Exigences sécuritaires ferroviaires européennes

Les exigences sécuritaires ferroviaires européennes sont structurées au sein d'une réglementation en trois niveaux qui sont ensuite traduites par chaque état membre en décrets, lois et arrêtés nationaux. Le premier niveau est la directive européenne, le second niveau est la STI (Spécification Technique d'Interopérabilité) et le troisième niveau est la norme européenne. Cette réglementation décrit tous les aspects liés au développement et à l'exploitation des réseaux de chemin de fer communautaires en grande vitesse et en rail conventionnel : performances, sécurité, qualité de service et coût. Cette réglementation concerne aussi bien les infrastructures ferroviaires que le matériel roulant. Dans le cadre de nos travaux de recherche, nous nous focalisons sur la réglementation sécuritaire des systèmes de transport guidé et plus

particulièrement sur le système du ferroutage.

#### 3.2.4.1 Contexte législatif sécuritaire des systèmes de transport guidé européens

La sécurité des systèmes de transports européens fait partie intégrante des directives européennes depuis 2004 avec les directives 49/CE [Dir04a] et 50/CE [Dir04b]. Ces directives ont valeur législative pour chaque état membre et préconisent l'interopérabilité du réseau ferroviaire européen. Cette interopérabilité signifie que les futurs systèmes de transport déployés seront capables de circuler sur l'ensemble des sections de réseau ferré appartenant aux divers états membres. Ainsi, un train de fret quittant le Royaume Uni à destination de la Pologne pourra traverser sans modification (changement de locomotive, basculement d'un réseau électrique à un autre par exemple) la France, la Belgique et l'Allemagne. Ces directives fixent donc les objectifs d'harmonisation nécessaires entre les différents partenaires en définissant les processus de certification, les procédures, les techniques et les méthodes d'analyse communes. Ces objectifs référent, notamment, l'usage de méthodes d'évaluation de la sécurité et la rédaction du dossier de sécurité. Ces dossiers de sécurité détaillent l'ensemble des méthodes de gestion des risques dans les transports guidés.
Pour permettre d'atteindre les objectifs d'harmonisation, les directives imposent aux états membres l'adoption des STI (Spécifications Techniques d'Interopérabilité). Ces STI fournissent des solutions techniques qui aident à la gestion de la complexité du système ferroviaire. Elles se présentent sous la forme de normes révisées régulièrement afin de tenir compte des dernières recommandations des directives. L'AEIF (Association Européenne pour l'Interopérabilité Ferroviaire qui regroupe des gestionnaires d'infrastructures et des industriels ferroviaires) jusqu'en juin 2005 puis l'ERA (European Railway Agency) s'occupent de la révision régulière des STI. Pour le domaine de la grande vitesse, il existe actuellement 5 STI (Infrastructure, Matériel Roulant, Contrôle commande, Energie et Exploitation). Pour le rail conventionnel, il existe également 5 STI :

- Wagons de fret [STI06e] : elle énonce les procédures d'évaluation de conformité et d'aptitude à l'emploi des wagons de fret actuels, améliorés ou rénovés. Elle décrit la structure des véhicules, l'équipement de freinage, les organes de roulement, la suspension, les portes et les systèmes de communication qui doivent être utilisés pour une exploitation sûre sur le réseau européen.
- Contrôle commande et signalisation [STI06b] : elle définit les exigences essentielles et leurs modalités d'application qui permettent le mouvement sûr des trains.
- Exploitation du train et gestion du trafic [STI06c] : elle énonce les règles d'exploitation et de maintenance spécifiques au rail conventionnel.
- Matériel roulant - bruit [STI06d] : elle décrit les normes et niveaux relatifs au bruit en stationnement, au démarrage et au passage du train ainsi que le bruit dans les cabines de conduite.

– Applications télématiques au service du fret [STI06a] : elle décrit les échanges d'informations pour la conduite sécuritaire des trains de fret.

A ces 5 STI du rail conventionnel doit s'ajouter prochainement la STI Infrastructure et la STI Energie.

Les STI sont applicables par le biais des normes européennes harmonisées (ou en cours d'harmonisation suivant les modifications des STI). Plus particulièrement, les normes EN 50126 [CEN00], EN 50128 [CEN01] et EN 50129 [CEN03] traitent à différents niveaux les aspects sécuritaires des systèmes ferroviaires.

Chaque état membre traduit les exigences européennes sous forme de décrets, d'arrêtés et de lois nationales. Pour la France, on peut citer par exemple l'arrêté du 1er juillet 2004 relatif aux exigences et caractéristiques techniques des matériels circulant sur le réseau ferré français [Arr04] transposant les exigences de la directive européenne 50/CE.

#### 3.2.4.2 Un constat : l'absence d'exigences sécuritaires européennes pour le ferroutage

Lorsque l'on regarde les exigences européennes sécuritaires pour les systèmes de ferroutage, on constate au point 2.1 page 19 de la STI rail conventionnel wagon de fret que les wagons de ferroutage sont considérés comme des wagons de fret classiques : *les wagons de fret incluent le matériel roulant destiné au transport des camions.*

Ainsi la marchandise transportée, que ce soit un camion ou un conteneur est appréhendé de la même façon et les particularités liées au transport d'un camion ne sont pas prises en compte (l'arrimage par exemple). Cela est d'autant plus flagrant que la STI wagon de fret décrit en annexe YY les solutions techniques de fixation par type de wagon pour le transport de conteneurs mais pas pour le transport de camions. Il n'y a donc pas d'exigences spécifiques sécuritaires européennes pour le ferroutage. De ce fait, en attendant une directive pour le ferroutage, les concepteurs de wagon doivent se référer aux textes législatifs et normatifs existants dans chaque état membre et faire valider leurs wagons pays par pays.

Cependant, les rencontres effectuées avec des responsables des établissements de sécurité européens et nationaux comme l'ERA et l'EPSF (Etablissement Public de Sécurité Ferroviaire) ou indépendants comme CERTIFER (Agence de Certification Ferroviaire) ont montré qu'une telle directive est nécessaire pour l'interopérabilité et la sécurité du ferroutage et qu'une codification relative aux wagons de ferroutage devra être mise en place. Afin de fournir une approche générique d'analyse et d'évaluation des exigences sécuritaires pour cette directive, l'utilisation de la démarche d'analyse par les SIL (*Safety Integrity Level*, niveaux d'intégrité de sécurité) issue de la norme EN 61508 [IEC00] relatif au domaine des systèmes électriques, électroniques et électroniques programmables (E/E/PE) peut être envisageable [Beu06].

L'absence d'exigences sécuritaires européennes pour le ferroutage est d'autant plus génante que ce système particulier comprend les risques généraux à tout système ferroviaire (mais

dont les moyens de réduction de ces risques sont codifiés dans les directives) ainsi que les risques liés au matériel transporté (mais dont les moyens de réduction de ces risques sont codifiés état par état et ce de façon non uniforme ni interopérable). Dans l'objectif d'un développement considérable du ferroutage ayant pour but de résoudre les problèmes de congestion routière européennes, ces risques doivent être réduits et maîtrisés. Nous allons voir dans la section suivante quels sont les risques liés au système de ferroutage, les besoins sécuritaires qui en découlent ainsi que le concept proposé dans le cadre de ces travaux de recherche pour y répondre.

## 3.3 Les risques liés aux systèmes de transport guidé

Cette section présente les risques généraux existant au sein d'un système de transport guidé ainsi que les risques particuliers liés au système de ferroutage. Une présentation des besoins de sûreté de fonctionnement permettra d'introduire le concept du wagon intelligent de ferroutage.

### 3.3.1 Les risques généraux

Une classification des risques généraux existant dans les systèmes de transport guidé a été proposée dans [HMSBC98]. Cette classification distingue quatre catégories d'accidents : les accidents utilisateur, les accidents système, les accidents utilisateur/système et les accidents environnement/système.

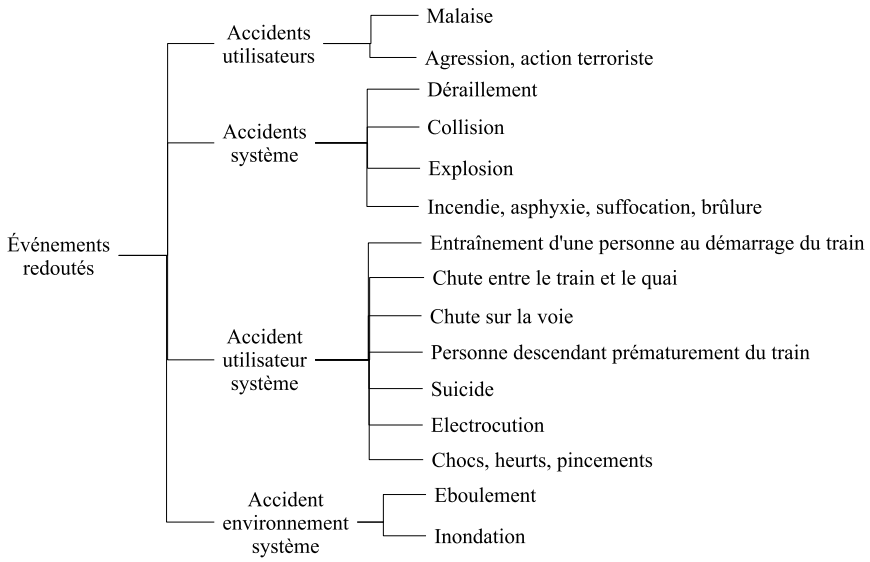


FIG. 3.1 – Classification des événements redoutés existants dans le domaine des transports guidés issue de [HMSBC98]

La figure 3.1 présente ces quatre catégories et détaille les risques associés comme suit :

- Les *accidents utilisateur* sont associés aux dommages causés à un ou plusieurs utilisateurs (usagers et/ou opérateurs) du système alors qu'aucun problème de fonctionnement du système ne soit survenu, et qu'aucune action de cet ou ces utilisateurs n'ait été constatée.
- Les *accidents système* sont associés aux dommages causés au système et aux utilisateurs lors d'un accident initié par le système lui-même. Dans cette catégorie se trouvent les déraillements, les collisions, les explosions et les incendies. Ces défaillances sont issues soit de défaillances liées au matériel (défaillance d'un composant), soit de défaillances liées au système logiciel (absence d'information, mauvaises informations transférées, ...), soit d'erreurs commises par les utilisateurs intervenant dans les différentes phases du système (lors de l'exploitation, lors de la maintenance, ...).
- Les *accidents utilisateur/système* sont associés aux dommages causés à un ou plusieurs utilisateurs du système, lors d'une action effectuée par ce ou ces utilisateurs durant le fonctionnement normal du système. Cette action peut être soit volontaire (un suicide par exemple), soit involontaire (une chute d'une personne par exemple).
- Les *accidents environnement/système* sont associés aux dommages causés au système et aux utilisateurs lors de conditions environnementales particulières (catastrophes naturelles par exemple).

Les risques généraux dépendent également du type de transport guidé considéré (transport de voyageurs ou de marchandises). Pour le transport de voyageurs, la plupart de ces risques sont liés au facteur humain. Pour le transport de marchandises, ce sont principalement des risques matériels qui engendrent des risques humains (par exemple dans le cas d'un déraillement d'un transport de marchandises dangereuses pouvant affecter la population proche du lieu de l'accident).

Dans la suite de nos travaux de recherche, nous nous focaliserons sur les risques de la catégorie *accident système* sur un réseau conventionnel et plus particulièrement sur les risques liés au matériel et à la circulation des trains. Dans le cadre du ferroutage, ces risques matériels peuvent être liés soit au matériel de transport (le wagon) soit au matériel transporté (le camion). Pour nos travaux, nous nous concentrerons sur les risques liés à ces matériels pouvant entraîner des incendies et des désarrimages du véhicule transporté. Nous allons voir dans la section suivante comment les risques matériels, eux-mêmes liés à la circulation des trains peuvent entraîner ces deux événements redoutés.

### 3.3.2 Les risques liés au matériel et à la circulation des trains

**Risques liés à la circulation des trains** Pour les systèmes de transport guidé, les risques liés à la circulation des trains entraînent principalement deux événements redoutés :

des déraillements et des collisions.

- Les déraillements sont principalement liés à une survitesse, à un rail cassé, à une surchauffe au niveau des essieux ou à un obstacle sur la voie. Cependant, dans le cadre du ferroutage, aux causes de déraillement s'ajoute celles lié à un basculement sur le wagon du camion transporté à cause d'un problème matériel.
- Il existe plusieurs types de collisions en raison des différentes situations du train : les collisions par mauvais sens de marche (deux trains sur une même voie dont l'un se dirige vers l'autre suite à une erreur d'itinéraire), les collisions par rattrapage (rattrapage d'un train par un autre), les collisions par prise en écharpe ou latérale (lors d'une intersection de voies), les collisions par dérive (un train normalement immobilisé sur une voie inclinée qui se déplace vers un autre train suite à un problème de freins) ou encore les collisions avec des obstacles. Dans le cadre du ferroutage, ce sont les risques liés à la collision avec des obstacles qui nous intéressent plus particulièrement car ces risques sont renforcés par le transport du camion. En effet, suite à un problème matériel, une remorque peut se mettre en porte-à-faux sur le wagon et entraîner une collision avec un obstacle permanent (contre un pont, un tunnel par exemple) ou non permanent (contre un autre train stationné sur une voie parallèle, un autre train arrivant dans l'autre sens, un élément de l'infrastructure positionné de sorte qu'il se trouve dans le gabarit des trains par exemple).

**Risques liés au matériel roulant et transporté** Comme nous venons de le voir, les risques liés à la circulation des trains pour les systèmes de transport guidé classiques ou par ferroutage sont liés aux risques du matériel roulant et du matériel transporté.

Les risques liés au matériel roulant sont relatifs à [Beu06] :

- l'état du matériel roulant et de l'infrastructure. Ces risques concernent les défaillances et détériorations du matériel survenant en exploitation selon le vieillissement des équipements (défaillance du système de freinage, défaillance d'un circuit de commande, défaillance d'un chevalet d'arrimage ...) et, selon le vieillissement et la robustesse des structures mécaniques (rupture d'essieu, rupture de bandage de roue, cassure d'un rail, déformation de la voie ...).
- certains problèmes dans la conception des composants et des équipements, des sous-systèmes ..., susceptibles d'être à l'origine de défaillances peuvent entraîner la défaillance du système de sécurité embarqué et générer des risques supplémentaires pour le système de transport guidé. Les analyses de sûreté de fonctionnement faites en conception et durant tout le cycle de vie du système s'efforcent de gérer ces problèmes pour créer un système tolérant aux fautes et répondant aux fonctionnalités attendues.

Ces risques matériels peuvent entraîner, par la circulation du train, un déraillement ou une

collision mais également un incendie (surchauffe au niveau des essieux, d'une roue de bogie par exemple).

Dans le cadre du ferroutage, à ces risques matériels liés au matériel roulant s'ajoute une classe de risques liée au matériel transporté. En effet le camion, non conçu initialement pour être transporté par un train, possède des caractéristiques physiques propres (Pneus, réservoir, moteur, amortisseurs, produit transporté entre autres) très différents d'une charge classique (un conteneur par exemple). Ainsi, le camion peut être mal fixé au wagon, son produit transporté peut avoir été mal réparti (entraînant des vibrations du camion), s'échapper de son conteneur (fuite), le tracteur routier peut présenter des fuites au niveau de son réservoir de carburant, du moteur (fuite d'huile), de ses pneus (dégonflement), avoir un problème sur son système de freinage ou sur ses amortisseurs. Tous ces risques liés au matériel transporté peuvent entraîner un incendie ou un désarrimage du camion et/ou de sa remorque.
Ces particularités entraînent des besoins en systèmes de sécurité supplémentaires pour le système de ferroutage permettant de détecter ces événements redoutés (déraillement, collision, incendie, désarrimage). A ces besoins sécuritaires s'ajoutent les besoins en terme de disponibilité afin de rendre attractif le ferroutage.

### 3.3.3 Les besoins liés au système de ferroutage

Comme nous l'avons vu dans la première partie de ce chapitre, le ferroutage est envisagé comme une solution complémentaire à la route. Cependant, les besoins en terme de disponibilité qu'il doit rendre sont nombreux s'il veut être envisagé comme un mode de transport complémentaire à la route. Ces besoins sont liés à sa complexité et à la qualité de service qu'il doit rendre. Nous allons les passer en revue.

#### 3.3.3.1 Les besoins liés à la qualité de service rendue

Les normes de qualité exigées par les clients du ferroutage ont été déterminées en fonction de celles offertes par le transport routier afin de le rendre attractif et équivalent au transport routier. Ces besoins concernent principalement la disponibilité, la rapidité, la souplesse et la fiabilité. La réponse à ces différents besoins relève des critères suivants :

- Une bonne fréquence d'acheminement des véhicules routiers (fiabilité et rapidité).
- Des temps de transport adaptés à la distance et respectés (disponibilité et rapidité).
- Des plages horaires de départ respectées (fiabilité).
- Des informations sur les envois et leur suivi (souplesse).
- L'organisation des dessertes routières (souplesse).
- Le stockage des Unités de Transport Intermodal (UTI) en gare (souplesse).

Ces critères conditionnent la qualité de service offerte par le ferroutage. Or, actuellement le ferroutage en France ne répond pas de manière satisfaisante à l'ensemble de ces critères alors qu'il est encore relativement innovant et peu développé en France. Cependant, la réalisation de nouvelles lignes d'autoroutes ferroviaires présentées en annexe G impliquera une augmentation du trafic par ferroutage (augmentation de la fréquence des navettes, amélioration de la rapidité du chargement/déchargement par exemple) et rendra ses besoins indispensables.

#### 3.3.3.2 Les besoins liés à la nature complexe et distribuée du ferroutage

Le système de ferroutage faisant partie des systèmes de transport ferroviaire s'appréhende, dans sa structure générale, comme un système complexe et cela pour plusieurs raisons [CHCC06a] :

- Par l'hétérogénéité des différents acteurs en présence. Nous avons en interaction des véhicules routiers non conçus pour le transport ferroviaire, des trains et une infrastructure plus ou moins spécialisée pour le transport de ces véhicules routiers.
- Par l'hétérogénéité des matières transportées principalement liée à ses caractéristiques physiques (matières dangereuses ou périssables, variation du poids entre deux véhicules par exemple).
- Par l'existence de plusieurs phases de fonctionnement (chargement du camion, convoi par exemple).
- Par la variabilité dynamique de son environnement (traversée de tunnels, de ponts et de villes).

Ces raisons impliquent les besoins sécuritaires suivants :

- Pour le système de ferroutage : garantir la sécurité du train et du wagon.
- Pour le chargement : protéger la marchandise transportée et le tracteur routier.
- Pour l'environnement immédiat : réduire les conséquences d'accidents de ferroutage sur les infrastructures environnantes.

De plus, la gestion de ce système est distribuée et cela également pour plusieurs raisons :

- Par la présence de plusieurs terminaux sur une même ligne afin de garantir une bonne rapidité de chargement et de déchargement et une souplesse équivalente au système routier.
- Par la méthode de chargement - déchargement des véhicules. En effet, quelle que soit la méthode de chargement (série ou parallèle), le fait que seule une partie du chargement du train change à chaque terminal impose des contraintes de gestion de la marchandise transportée.

Pour l'ensemble de ces raisons (système complexe et distribué, augmentation future du trafic, qualité de service à rendre), les systèmes utilisés actuellement nécessiteront de répondre à des exigences et des besoins de sûreté de fonctionnement spécifiques et cela, dans

toutes les phases de fonctionnement du ferroutage, c'est-à-dire :

- accroître la disponibilité et la fiabilité du système,
- protéger les marchandises en zone de stock contre les différentes agressions, à la fois humaines et environnementales,
- aider à la maintenance et à la gestion,
- surveiller les risques potentiels liés à la charge et au wagon lors des opérations de chargement et de transport (équilibre de la charge, fixation de la remorque, fuite de carburant, incendie, sur-échauffement des freins).

L'existence de ces besoins spécifiques impose la définition et la conception d'un système d'automatisation adapté au ferroutage [CHCC06b]. Ce système d'automatisation sera le résultat de la modélisation et de l'analyse d'une partie du système de ferroutage (le wagon) tenant compte d'exigences spécifiques au ferroutage et intégrant la sûreté de fonctionnement lors de son optimisation.
Ce système d'automatisation sûr est défini, dans nos travaux, par le concept du wagon intelligent de ferroutage [CHCC06b], [CHCC07b]. Nous allons présenter et définir ce concept dans la section suivante.

## 3.4 Le concept du wagon intelligent

#### 3.4.0.3 Pourquoi un wagon intelligent ?

Le système de ferroutage actuel comprend plusieurs acteurs multi-fonctionnels (véhicules routiers, wagons et infrastructure). Dans les systèmes actuels de ferroutage ainsi que dans les projets en développement, le wagon de fret joue un rôle passif du point de vue de la sûreté de fonctionnement. En effet, ce wagon ne possède ni énergie embarquée, ni capteurs, ni actionneurs permettant d'analyser et de déterminer un éventuel risque lié à ce système. Les constructeurs ferroviaires justifient l'absence d'équipements afin de limiter au maximum la tare du wagon (poids à vide) et augmenter le ratio de productivité (R) pour les transporteurs routiers. Ce ratio est le rapport en tonnes entre le poids transporté (PTrans) et le poids total du système (PTotal) selon la formule suivante :

$$R = \frac{PTrans}{Ptotal} \tag{3.1}$$

Prenons par exemple, pour un wagon Modalohr qui pèse 40 tonnes et qui permet de charger deux remorques ayant une charge transportée de 17 tonnes et un poids à vide de 6 tonnes. Le poids transporté est donc de 46 tonnes (les deux remorques) pour un poids total de 86 tonnes. Le ratio de productivité est donc de 0,53. Par la route, avec un tracteur routier de 9 tonnes, ce ratio est également de 0,53 ce qui permet de dire que le ferroutage est un moyen complémentaire comparable à la route si le tracteur routier n'est pas transporté avec

la remorque.
Cependant, cette conclusion est obtenue en allégeant au maximum le wagon de tout système embarqué permettant de justifier d'un niveau de sûreté de fonctionnement maximal. L'ajout d'intelligence au wagon à l'aide de fonctions supplémentaires embarquées permettrait de contribuer activement à l'amélioration du niveau de sûreté de fonctionnement global de l'ensemble du système de ferroutage dans toutes ses phases de fonctionnement mais en diminuant obligatoirement le ratio de productivité.
En effet, le wagon est le seul acteur du système de ferroutage présent dans toutes les phases de fonctionnement du système complexe. Par ailleurs, le wagon permet de faire le lien entre les deux autres acteurs du système c'est-à-dire avec les véhicules routiers et avec l'infrastructure ferroviaire. Afin d'étayer ces propos, nous allons présenter l'intérêt du concept du wagon intelligent en analysant deux accidents de ferroutage.

#### 3.4.0.4 Analyse de deux accidents de ferroutage

**L'accident de la navette Eurotunnel 7539 (France-Angleterre)** Le 18 novembre 1996, le train navette poids-lourds 7539 à destination de la Grande Bretagne s'est immobilisé dans le tunnel ferroviaire avec un incendie à bord. Celui-ci dégageait d'importantes fumées qui ont rapidement enveloppé la voiture salon et la locomotive de tête compliquant l'évacuation. L'incendie a été maîtrisé avec difficultés du fait de l'environnement confiné dans le tunnel [Eur97]. Le tunnel et le train ont subi des dégâts considérables et il a fallu reconstruire l'ensemble des infrastructures sur plus de 1 km. L'exploitation de ce tronçon de tunnel a été suspendue pendant 2 mois. Aucune marchandise dangereuse n'a été mise en cause et personne n'a été tué, 34 personnes ont été plus ou moins intoxiquées par les fumées. Cet incendie a montré des défaillances dans les systèmes de détection d'incendie du tunnel et de confirmation d'incendie. De plus, le système de communication et de confinement des fumées dans un seul tunnel ont présenté quelques défaillances.
L'origine exacte de l'incendie n'a pas pu être déterminée. On ignore s'il provenait du chargement ou s'il provenait des systèmes du wagon. Cependant, le feu se serait déclenché avant l'entrée du train dans le tunnel mais n'a pas pu être détecté avant son entrée effective dans le tunnel.

**Intérêt du concept du wagon intelligent** L'intérêt du concept du wagon intelligent s'expose aisément avec cet accident. L'ajout de fonctions, telles que la détection de température dans le wagon, sur ses organes principaux (Boîte d'essieu, roues de boggie, freins, ...) mais également sur la marchandise transportée ainsi que la surveillance d'autres paramètres importants comme la fuite de liquide provenant de la charge auraient permis de faire de la maintenance préventive sur le wagon, de refuser éventuellement le chargement du

camion et lors de l'exploitation en convoi de détecter avant l'entrée dans le tunnel le risque d'incendie et/ou l'incendie en lui-même.

**L'accident du Iron Highway 121 (Canada)** Le 13 août 1997, une remorque routière transportée à bord du train 121 s'est désarrimée et s'est mise en porte-à-faux sur la plate-forme qui la portait, excédant la largeur du wagon. Pendant que le train roulait sous un passage supérieur aménagé pour une route, cette remorque a heurté les colonnes d'appui du pont. La remorque a subi des dommages considérables, et il a fallu fermer le passage supérieur pendant plusieurs jours car plusieurs colonnes du pont ont été endommagées. Cependant, aucune marchandise dangereuse n'a été mise en cause et personne n'a été blessé [BST99].
La remorque s'est désarrimée à cause d'un chevalet d'arrimage de la remorque défectueux rendant le mécanisme de verrouillage inopérant et ne pouvant être détectée visuellement par les opérateurs lors du chargement.

**Intérêt du concept du wagon intelligent** L'intérêt du concept du wagon intelligent s'expose également facilement dans le cadre de cet accident. En effet, l'ajout d'un système permettant de surveiller l'arrimage de la charge aurait permis de détecter plusieurs paramètres utiles relatifs aux mouvements de la charge (sa position par rapport au wagon et l'accélération transversale de la remorque par exemple). Même si l'on ne pouvait détecter l'inaction du chevalet d'arrimage, la surveillance de ces deux paramètres aurait aidé à détecter la mise en porte-à-faux de la remorque sur le wagon et aurait pu permettre de prévenir les opérateurs afin d'éviter l'accident et les dommages en résultant.

#### 3.4.0.5 La réduction des risques par le wagon intelligent

Les accidents par ferroutage sont heureusement rares, cependant, du fait des matières transportées et de l'environnement traversé (tunnels, villes ...), une défaillance peut entraîner d'importantes conséquences sur le système ferroviaire et sur son environnement. C'est pourquoi le système de ferroutage doit intégrer de nouvelles fonctions permettant de répondre aux exigences de sécurité, de fiabilité et de disponibilité.
L'ajout de telles fonctions implique la définition d'un système d'automatisation sûr de fonctionnement pour le wagon de ferroutage.

### 3.4.1 Présentation générale du concept

Comme nous venons de le voir, l'ajout de fonctions au wagon de ferroutage permettrait de contribuer plus activement à la sûreté de fonctionnement du ferroutage. L'ajout de ces fonctions implique l'introduction des équipements suivants sur le wagon :

- Des fonctions logicielles permettant de remplir des missions de surveillance, commande, communication, ... [AHS01]
- Une instrumentation adaptée composée de capteurs matériels et d'instruments intelligents afin de récupérer les variables physiques nécessaires aux fonctions logicielles précédentes [SB96b].
- Des redondances matérielles et logicielles afin de rendre le système tolérant aux défaillances [CTR05].

Ces équipements supplémentaires vont constituer le système d'automatisation du wagon de ferroutage et doivent pouvoir répondre aux besoins de sûreté de fonctionnement du système de ferroutage. La figure 3.2 présente le modèle du wagon intelligent calqué sur celui des instruments intelligents.

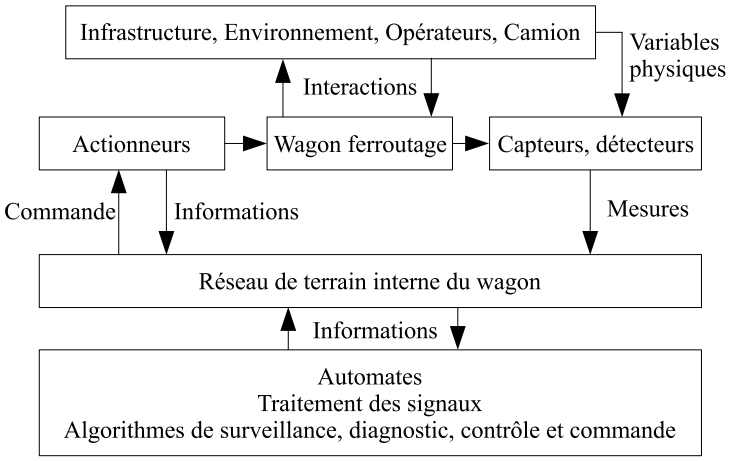


FIG. 3.2 – Modèle du wagon intelligent

D'après cette figure, le wagon de ferroutage intelligent est équipé d'unités de traitement (automates, régulateurs, calculateurs) accomplissant des traitements logiciels afin d'effectuer ses missions (surveillance, diagnostic, contrôle et commande). Le wagon intelligent est également équipé d'un réseau de terrain reliant les unités de traitement aux capteurs et aux actionneurs placés sur sa structure. Ce réseau permet de transmettre des commandes à destination des actionneurs et de récupérer les informations issues des actionneurs (accomplissement d'une commande par exemple) ainsi que les mesures générées par les capteurs. Ces mesures sont obtenues à partir de variables physiques issues de l'environnement proche du wagon (infrastructure ferroviaire, opérateurs, camions).

Afin de concevoir ce système d'automatisation, il est d'abord nécessaire de déterminer l'ensemble des fonctions qu'il doit rendre et cela dans toutes ses phases de fonctionnement. Cette identification passe par une analyse fonctionnelle dont les résultats sont présentés dans la section suivante. Après avoir défini l'ensemble de ces fonctions, il s'agit ensuite de pouvoir déterminer les architectures optimales offrant, pour le concepteur, le meilleur compromis entre niveau de sûreté de fonctionnement et coût financier de ces ajouts.
Par ailleurs, le lecteur intéressé pourra se référer à la norme EN 61508 [IEC00] qui définit une démarche similaire de conception et d'analyse pour le domaine des systèmes électriques et électroniques. En effet, cette norme fournit une méthode de développement pour réaliser la sécurité fonctionnelle des systèmes relatifs à la sécurité, elle définit les niveaux d'intégrité de sécurité (SIL) des systèmes E/E/PE relatifs à la sécurité et elle décrit une approche basée sur l'analyse de risque pour déterminer les niveaux d'intégrité de sécurité à atteindre pour un risque donné.

## 3.4.2 Décomposition fonctionnelle

### 3.4.2.1 Définition des hypothèses et des phases de fonctionnement

L'analyse fonctionnelle est un outil souvent utilisé pour modéliser des systèmes d'automatisation [BCR05], [CB06b]. Le modèle obtenu est décrit sous forme d'une décomposition fonctionnelle hiérarchique comme définie par la norme AFNOR NF X50-151 [AFN04]. Avant de modéliser les fonctions de notre système d'automatisation, il est nécessaire de définir ses limites, ses phases de fonctionnement, les différents acteurs qui le composent ainsi que les éléments extérieurs ayant une incidence sur son fonctionnement à l'aide du diagramme des interacteurs présenté au chapitre 1.
Le système central de l'analyse est évidemment le système d'automatisation du wagon de ferroutage, c'est-à-dire les fonctions et les équipements supplémentaires. Les systèmes autres que ceux contribuant à la sûreté de fonctionnement mais faisant partie du wagon (bogie, freins, coque) et de l'infrastructure (rails, tunnels, système de signalisation, ...) sont considérés comme extérieurs au système central et sont dénommées respectivement par partie mécatronique wagon et partie mécatronique infrastructure. Les autres éléments extérieurs du système central sont les suivants :

- Les opérateurs humains : ces opérateurs n'ont pas les mêmes fonctions suivant les phases de fonctionnement du système. Ils peuvent être des opérateurs de l'infrastructure, conducteurs de trains ou de véhicules routiers.
- Les véhicules routiers : ces véhicules peuvent être équipés d'instruments intelligents ou non. L'hypothèse que nous avons prise est d'avoir des véhicules passifs. Dans le cas contraire, les capteurs de ces véhicules viendront s'ajouter à ceux du système.
- L'énergie utilisée : elle n'est pas produite par le système mais celui-ci doit pouvoir se

connecter à différentes sources (électrique, pneumatique, mécanique).
- Le milieu environnant : il regroupe l'ensemble des autres milieux extérieurs non référencés précédemment. Les conditions atmosphériques font parties de ce milieu par exemple.

De la même façon, nous définissons les phases de fonctionnement du système :
- Phase de chargement-déchargement : cette phase décrit le comportement de l'ensemble du système depuis l'arrêt d'un train en gare jusqu'à son ordre de départ. Cette phase comprend les étapes : de mise en place du train et du système de chargement, du gerbage des véhicules et du blocage de la charge sur le wagon.
- Phase de convoi : cette phase de fonctionnement du système est définie temporellement depuis l'ordre de départ du train jusqu'à son arrivée dans la gare suivante.
- Phase de parking-maintenance : cette phase décompose le comportement du système en dehors de son utilisation dite "normale", c'est-à-dire lors des opérations de maintenance d'un acteur du système ou lors de son immobilisation sur une voie ferrée.

Nous appliquons maintenant la démarche de construction du diagramme des interacteurs et des arbres fonctionnels afin de déterminer les fonctions supplémentaires du wagon. Nous avons représenté ces fonctions pour chaque phase de fonctionnement du système. Ces résultats sont présentés dans les paragraphes suivants.

#### 3.4.2.2 Diagrammes obtenus et fonctions supplémentaires à implanter

La première phase considérée est la phase de chargement-déchargement du véhicule routier sur le train.

**Phase de chargement-déchargement** Cette phase décrit le comportement de l'ensemble du système depuis l'arrêt d'un train en gare jusqu'à son ordre de départ. Cette phase comprend les étapes : de mise en place du train et du système de chargement, du gerbage des véhicules et du blocage de la charge sur le wagon. Le diagramme de cette phase est présenté figure 3.3.

**Fonctions supplémentaires obtenues**
- F1 : Surveiller la mise en place du véhicule sur le wagon : cette fonction permet de vérifier l'installation correcte du véhicule sur le wagon, c'est-à-dire sa mise en place dans la poche du wagon ainsi que son arrimage pour la phase de convoi. Le système reçoit des informations provenant des capteurs présents sur l'infrastructure (fonction F5) et sur le wagon avec lequel il est en relation.
- F2 : Surveiller l'intégrité physique de la charge : cette fonction permet au système intelligent de vérifier les informations importantes de la charge afin d'autoriser ou

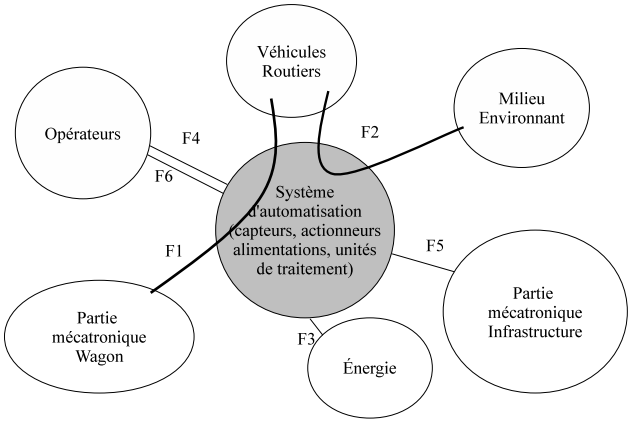


FIG. 3.3 – Diagramme de la phase de chargement déchargement

non sa mise en place pendant et après sa mise en place sur le wagon. Ces informations regroupent l'état de la marchandise transportée (température, poids ...) mais également l'état de la remorque routière et/ou de son tracteur (système pneumatique, pression des pneus ...).

- F3 : Alimenter le système intelligent en énergie : comme pour les phases de chargement et de convoi, cette fonction permet au système d'être alimenté sur le wagon et de détecter une anomalie dans son système de distribution d'énergie. Ces énergies étant pneumatiques, hydrauliques et électriques.
- F4 : Transmettre des informations : cette fonction fait appel à l'ensemble des matériels d'émission et de logiciels de communication pour émettre des messages vers les opérateurs ou les automatismes. Certains messages sont directement émissibles (signaux visuels, sonores ...) alors que d'autres nécessitent un système d'interprétation, de codage et de vérification. Ces messages sont informatifs (fin de mouvement d'un actionneur, disponibilité du wagon, début du blocage de la charge, ...) tandis que d'autres ont pour objet de prévenir d'une défaillance (fuite détectée, température anormale, changement de position, ...).
- F5 : Recevoir des informations de l'infrastructure : cette fonction permet au système de recevoir des informations des automatismes et de les comprendre. Ces informations peuvent être des requêtes (demande de passage dans un autre mode d'utilisation ...) et / ou des données (paramètres de configuration, images provenant de capteurs d'autres systèmes ...).
- F6 : Recevoir des informations des opérateurs : cette fonction est similaire à la précédente puisqu'elle permet de recevoir des informations des opérateurs et de les comprendre. Ces informations peuvent également être des requêtes (Date de la dernière opération de maintenance, valeur de la température des freins du wagon numéro i, durée de station-

nement ...) et / ou des données pour le transport (type et dangerosité des marchandises installées, ville d'arrivée, ville de départ, ...).

**Phase de convoi** Cette phase de fonctionnement du système est définie temporellement depuis l'ordre de départ du train jusqu'à son arrivée dans la gare suivante. Le diagramme de cette phase est présenté figure 3.4.

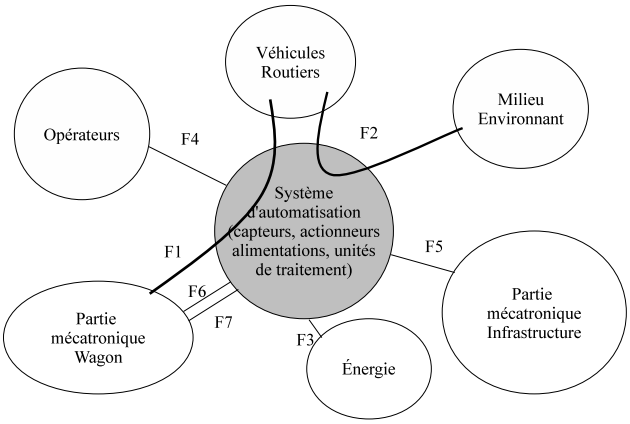


FIG. 3.4 – Diagramme de la phase de convoi

**Fonctions supplémentaires obtenues**

- F1 : Détecter un défaut d'arrimage de la charge sur le wagon : cette fonction vérifie l'adéquation entre le wagon et la charge. Elle surveille l'état du système d'arrimage et les mouvements de la charge (modification du centre de gravité, basculement sur un côté, mise en porte-à-faux ...).
- F2 : Surveiller l'intégrité physique de la charge : cette fonction permet au système intelligent de vérifier les informations importantes de la charge. Ces informations regroupent l'état de la matière transportée (température, poids par exemple) mais également l'état de la remorque routière et de son tracteur (système pneumatique, pression des pneus ...).
- F3 : Alimenter le système intelligent en énergie : comme pour les phases de chargement et de convoi, cette fonction permet au système d'être alimenté sur le wagon et de détecter une anomalie dans son système de distribution d'énergie. Ces énergies étant pneumatiques, hydrauliques et électriques.
- F4 : Transmettre des informations : comme pour la phase de chargement-déchargement, cette fonction fait appel à l'ensemble des matériels d'émission et de logiciels de communication pour émettre des messages vers les opérateurs ou les automatismes. Certains messages sont directement émissibles (signaux visuels, sonores ...) alors que d'autres

nécessitent un système d'interprétation, de codage et de vérification. Ces messages sont informatifs (fin de mouvement d'un actionneur, disponibilité du wagon, début du blocage de la charge ...) tandis que d'autres ont pour objet de prévenir d'une défaillance (fuite détectée, température anormale ...).

- F5 : Recevoir des informations de l'infrastructure : cette fonction permet au système de recevoir des informations des automatismes extérieurs et de les comprendre. Ces informations peuvent être des requêtes (demande de passage dans un autre mode d'utilisation ...) et / ou des données (température des tunnels, images provenant de capteurs en avant du convoi ou sur le convoi, ...).
- F6 : Surveiller les paramètres physiques du wagon : cette fonction vérifie les données importantes du wagon pendant la phase de convoi (température des freins, des roues de bogie et de la boite d'essieu, accélération horizontale ...).
- F7 : Recevoir les alarmes d'autres wagons : cette fonction permet au système de recevoir des informations des autres wagons du convoi et de les relayer vers les opérateurs. Ces informations sont principalement des données (température de la charge, défaillance détectée sur le wagon numéro j par exemple).

**Phase de parking maintenance** Cette phase décompose les fonctions supplémentaires du système en dehors de son utilisation dite "normale", c'est-à-dire lors des opérations de maintenance du wagon ou lors de son immobilisation sur une voie ferrée. Le diagramme de cette phase est présenté figure 3.5.

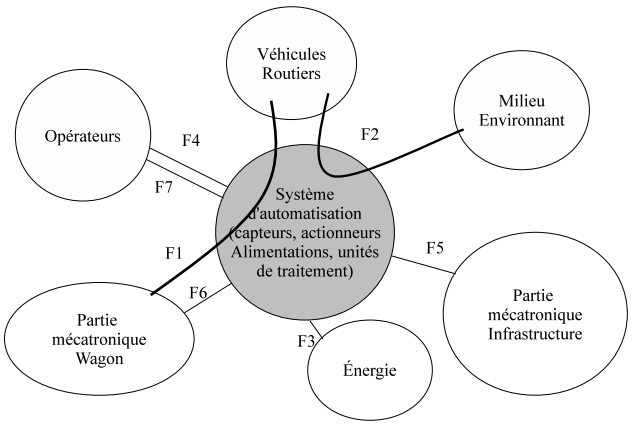


FIG. 3.5 – Diagramme de la phase de parking maintenance

**Fonctions supplémentaires obtenues**

- F1 : Vérifier la présence d'une charge sur le wagon : cette fonction fait appel à un système de détection d'une charge sur le wagon (variation du poids du système, images

...) et de réception des informations provenant des opérateurs pour confirmation de cette présence (type de marchandise, durée de stationnement ...).

- F2 : Surveiller l'intégrité physique de la charge : comme pour la phase de convoi, cette fonction permet au système intelligent de vérifier les informations importantes du système quelles que soient les conditions extérieures. Ces informations regroupent l'état de la matière transportée (température, poids ...), mais aussi l'état de la remorque routière et de son tracteur routier (système pneumatique, pression des pneus ...). Le but de cette fonction est d'éviter les agressions sur le système provenant de l'environnement et les agressions humaines (dégradations ...).
- F3 : Alimenter le système intelligent en énergie : comme pour les phases de chargement et de convoi, cette fonction permet au système d'être alimenté sur le wagon et de détecter une anomalie dans son système de distribution d'énergie. Ces énergies étant pneumatiques, hydrauliques et électriques.
- F4 : Transmettre des informations : comme pour les phases de chargement et de convoi, cette fonction fait appel à l'ensemble des matériels d'émission et de logiciels de communication pour émettre des messages vers les opérateurs ou les automatismes. Certains messages sont directement émissibles (signaux visuels, sonores ...) alors que d'autres nécessitent un système d'interprétation, de codage et de vérification. Ces messages sont informatifs (fin de mouvement d'un actionneur, disponibilité du wagon, origine de la charge, durée de stationnement ...) tandis que d'autres ont pour objet de prévenir d'une défaillance (fuite détectée, température anormale ...).
- F5 : Recevoir des informations de l'infrastructure : comme pour les phases de chargement-déchargement et de convoi, cette fonction permet au système de recevoir des informations des automatismes extérieurs et de les comprendre. Ces informations peuvent être des requêtes (demande de passage dans un autre mode d'utilisation ...) et / ou des données (images provenant de capteurs entourant le wagon ...).
- F6 : Surveiller les paramètres physiques du wagon : comme pour la phase de convoi, cette fonction vérifie les données importantes du wagon pendant la phase de parking (blocage des freins et de l'arrimage de la charge, fonctionnement des systèmes ...).
- F7 : Recevoir des informations des opérateurs : comme pour la phase de chargement-déchargement, cette fonction permet de recevoir des informations des opérateurs et de les comprendre. Ces informations peuvent également être des requêtes (date de la dernière opération de maintenance, durée de stationnement ...) et / ou des données (type et dangerosité des marchandises installées, ville d'arrivée, ville de départ ...).

#### 3.4.2.3 Arbres fonctionnels hiérarchiques du wagon intelligent

Ces arbres fonctionnels permettent de structurer les fonctions obtenues sous forme de modèle hiérarchique.

**Phase de chargement-déchargement** Sur cette phase, on constate que parmi les fonctions obtenues précédemment, les fonctions F1, F2 et F3 peuvent se regrouper autour d'une mission commune : surveiller le chargement transporté. Ces fonctions constitueront une même branche de l'arbre hiérarchique autour de cette mission globale du ferroutage. Les fonctions F5 et F6 peuvent se regrouper autour de la mission : recevoir des informations. Un dernier regroupement peut s'effectuer entre la fonction F4 et le groupe F5-F6 autour de la mission : communiquer son état.
On obtient donc l'arbre présenté sur la figure 3.6.

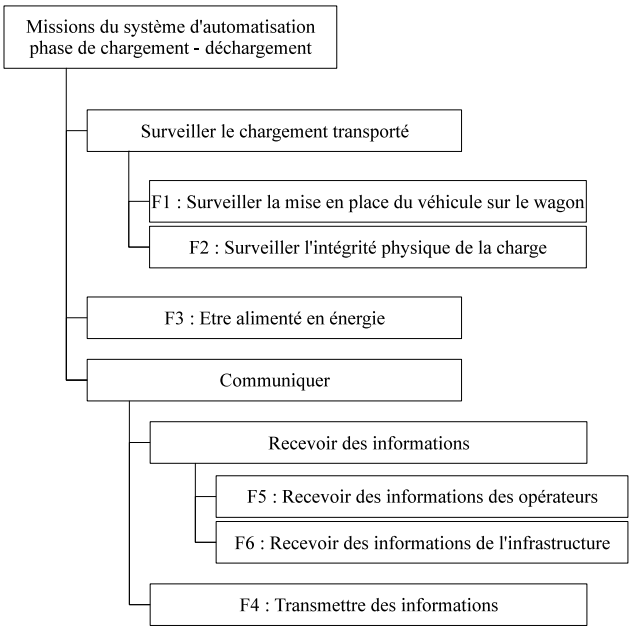


FIG. 3.6 – Arbre fonctionnel de la phase de chargement déchargement

**Phase de convoi** De la même façon que pour la phase de chargement - déchargement, on regroupe les fonctions obtenues. On constate que les fonctions F1 et F2 peuvent se regrouper autour d'une mission commune : surveiller la charge et le système d'arrimage du wagon. De même, F3, F6 et le regroupement F1-F2 peuvent se rassembler autour de la mission commune : surveiller la globalité du système de ferroutage. De la même façon, il est fait un regroupement similaire avec les fonctions F4 et le groupe F4-F7 autour de la mission : communiquer son état.
A partir de l'ensemble des regroupements effectués, nous déduisons l'arbre fonctionnel présenté sur la figure 3.7.

**Phase de parking maintenance** Pour la phase de parking - maintenance, on constate que les fonctions F1, F2, F3 et F6 peuvent se regrouper autour d'une mission commune :

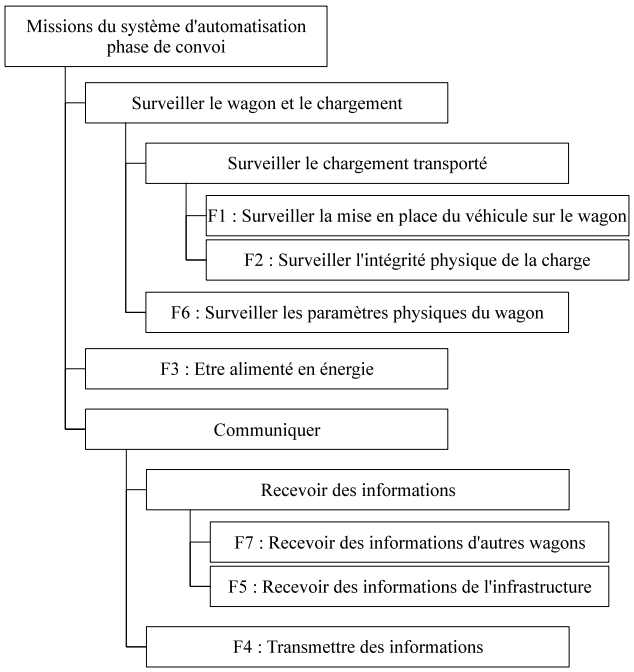


FIG. 3.7 – Arbre fonctionnel de la phase de convoi

surveiller l'ensemble du système complexe. De même, F5 et F7 se rassemblent autour de la mission commune : communiquer son état. De la même façon, il est fait un regroupement similaire avec les fonctions F4 et le groupe F5-F7 autour de la mission : communiquer son état.
A partir de l'ensemble des regroupements effectués, nous déduisons l'arbre hiérarchique présenté sur la figure 3.8.

### 3.4.3 Les sous-systèmes considérés pour la conception

Nous considérons dans la suite de nos travaux la conception des sous-systèmes liés à la protection contre les incendies, au bon arrimage du camion sur le wagon ainsi qu'au signalement aux opérateurs du système de ces deux événements redoutés et ceci pour la phase de convoi. L'objectif étant de réduire ces deux risques d'accidents liés au système de ferroutage. En effet, pour le cas de l'incendie, les risques liés au matériel transporté présentés au paragraphe 3.3.2 augmentent les probabilités de déclenchement d'un incendie, l'accident de l'Eurotunnel de 1996 en est un exemple concret, il est donc impératif de détecter au plus tôt un incendie.
Pour le cas de l'arrimage, de la même façon que pour la marchandise transportée par un camion, le camion et sa marchandise transportée par un wagon sont soumis à des sollicitations lors des changements d'allure ou de direction du train [Aum92], [AGG+06]. Pour être

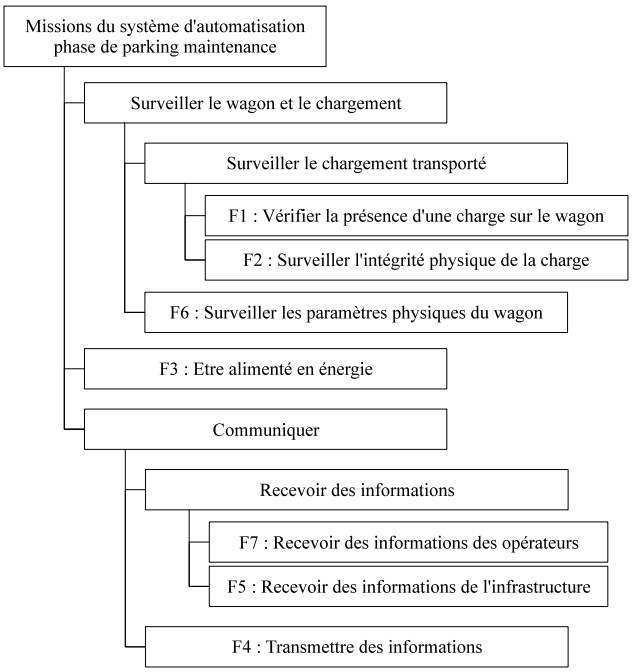


FIG. 3.8 – Arbre fonctionnel de la phase de parking maintenance

transporté en sécurité, le camion doit être correctement réparti sur le wagon de ferroutage et ne pas pouvoir bouger.
En effet, un camion mal calé ou mal arrimé sur un wagon de ferroutage risque de :

- glisser et défoncer le wagon devant lui en cas d'arrêt brutal du train,
- se mettre en porte-à-faux sur le wagon en cours de transport puis heurter un objet mobile (un train en sens contraire) ou une infrastructure,
- tomber sur un opérateur lors du déchargement,
- provoquer le déraillement du wagon et celui du train.

Il est donc impératif d'arrimer convenablement le camion. Pour cela, les concepteurs de wagon de ferroutage ont développé des moyens d'arrimage adaptés afin d'exclure tous moyens de fortune, nous pouvons citer par exemple les chevalets d'arrimage Trinity pour l'Iron Highway ou le palonnier d'arrimage pour le Modalohr. Cependant, malgré les procédures de maintenance préventive, ces systèmes d'arrimage peuvent être défaillants, l'accident de l'Iron Highway en 1997 en est un exemple. Il est donc nécessaire de détecter au plus tôt, c'est-à-dire dès la phase de convoi, un désarrimage.
La conception de ces deux systèmes correspondant aux deux accidents de ferroutage présentés dans ce chapitre permettra d'appuyer l'intérêt du concept du wagon intelligent.
La mission du système de protection contre les incendies est de détecter l'incendie sur le train et de prévenir les opérateurs de cet incendie. La mission du système de protection de l'arrimage est de détecter un désarrimage et de prévenir les opérateurs de ce désarrimage.

D'après la figure 3.7, ces missions correspondent aux fonctions F2, F3 et F4 du système.
Le diagramme 3.9 est obtenu à partir de la décomposition de la fonction F2 "Surveiller l'intégrité physique de la charge" issue de la phase de convoi. Ce diagramme détaille plus particulièrement les phénomènes physiques détectables et envisageables pour les sous-missions de détection du désarrimage et de détection des incendies.

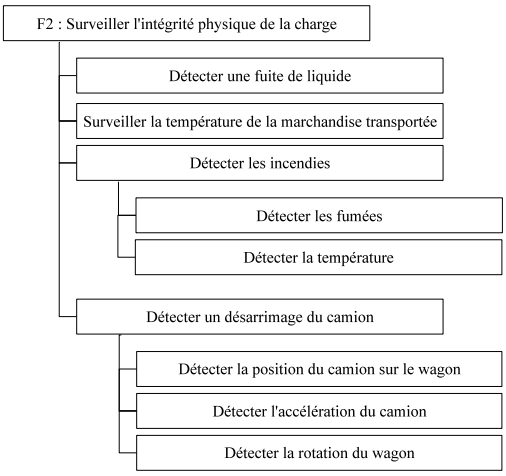


FIG. 3.9 – Décomposition hiérarchique de la fonction F2 "Surveiller l'intégrité physique de la charge"

Cependant, au sein de cette décomposition hiérarchique, nous ne pouvons ni modéliser les équipements potentiellement utilisables (capteurs, actionneurs, unités de traitement), leur type (standard, sécuritaire, intelligent, ...) et leurs possibilités d'organisation (redondance série ou passive par exemple). Par ailleurs, il n'est pas possible de caractériser le comportement en présence de pannes de cette architecture. Afin de prendre en compte ces critères en conception, la décomposition fonctionnelle précédente doit être enrichie à l'aide de l'approche définie dans le chapitre précédent.

## 3.5 Conclusion

Dans ce troisième chapitre, nous avons présenté les concepts généraux du ferroutage ainsi que le concept du wagon intelligent permettant d'améliorer la sûreté de fonctionnement globale du ferroutage.
La première partie de ce chapitre a présenté le ferroutage ainsi que les besoins particuliers pour le développement de ce système. L'absence de norme de sécurité ferroviaire européenne adaptée aux systèmes de ferroutage est problématique pour garantir que le niveau de sécurité du système actuel est suffisant pour répondre à l'intensification future du trafic.
La seconde partie a mis en évidence les différents risques existant dans les systèmes de transport guidés ainsi que les risques particuliers liés au ferroutage. Les besoins en systèmes

de sécurité pour le système de ferroutage découlant de ces risques ont ensuite été présentés. Enfin, la troisième partie a présenté le concept du wagon intelligent permettant de réduire l'ensemble des risques liés à la fois au matériel de transport ainsi que ceux liés au matériel transporté. Une architecture fonctionnelle pour ce wagon intelligent a été proposée suivant les étapes de modélisation présentées dans le premier chapitre. Au sein de cette architecture, les systèmes de protection incendie et de protection de l'arrimage ont été plus particulièrement détaillés. Ce sont les deux systèmes qui montrent l'intérêt du concept du wagon intelligent par rapport aux accidents ferroviaires de 1996 et 1997. Le chapitre suivant se propose d'appliquer notre méthodologie pour la conception de ces deux systèmes de protection. Dans ce chapitre, les deux systèmes de protection seront d'abord conçus indépendamment l'un de l'autre puis conçus globalement. Une comparaison avec une méthode classique d'évaluation de la sûreté de fonctionnement montrera clairement les contributions de notre approche tenant compte des scénarios.

# Chapitre 4

# Application de l'approche de conception au wagon intelligent

## 4.1 Introduction

Ce chapitre a pour objectif d'appliquer au wagon intelligent notre méthodologie de conception présentée au chapitre 2. Cette dernière permet en particulier d'évaluer les différentes architectures possibles d'un système de protection en se basant sur les scénarios. Pour cela, nous concevons deux systèmes de protection présentés au chapitre 3 et qui sont en rapport direct avec les accidents de ferroutage de 1996 et 1997. La conception de ces deux systèmes particuliers montrera l'intérêt du concept du wagon intelligent permettant de limiter ces risques d'accidents et rendant plus sûr le ferroutage. Le premier système ainsi conçu est un système de protection contre les incendies [CHCC08c], [CHCC09] tandis que le second système est un système de protection contre les désarrimages des camions transportés [CHCC08a], [CHCC08b]. Ces deux systèmes sont conçus indépendamment puis de façon globale au travers du logiciel ALoCSyS que nous avons développé et dont les fonctionnalités les plus importantes sont présentées au chapitre 2.
La première partie s'attache à concevoir les deux systèmes de protection indépendamment l'un de l'autre. Nous rappelons les missions de ces systèmes et définissons les composants utilisables ainsi que leurs possibilités d'agencements. Les modèles fonctionnels et dysfonctionnels sont déterminés ainsi que les résultats obtenus. Enfin, une comparaison de nos résultats avec ceux d'une méthode d'évaluation classique de la sûreté de fonctionnement nous permet de valider notre approche et d'en montrer ses avantages.
La deuxième partie présente la conception d'un système global regroupant les fonctions des deux systèmes de protection précédents. Un exemple d'architecture opérationnelle est donné avec les résultats. Nous comparons ensuite ces résultats avec ceux obtenus dans la première partie du chapitre pour montrer les avantages et les inconvénients de chaque démarche.

## 4.2 Etape de modélisation

### 4.2.1 Définition des missions principales et des modèles fonctionnels

La première phase de cette étape est de construire les modèles hiérarchiques en partant de leurs missions respectives. Les missions à remplir pour chaque système de protection ont été détaillées dans le chapitre 3. Nous allons définir deux modèles, un pour chaque système de protection.

**Système de protection de l'incendie** Le système de protection contre les incendies a une mission en phase de convoi : *Détecter les incendies*. Cette mission est assurée par une fonction de contrôle du système qui possède la sous-fonction : *Détecter un incendie*. Cette détection est assurée par deux sous-fonctions : *Détecter la température* et *Détecter la fumée*. Un incendie est détecté de trois façons différentes, on peut :

- soit détecter l'augmentation de la température **ou** le dégagement de fumées,
- soit détecter l'augmentation de la température **et** le dégagement de fumées en même temps,
- soit détecter le dégagement de fumées **puis** l'augmentation de la température.

La figure 4.1 présente le modèle hiérarchique obtenu.

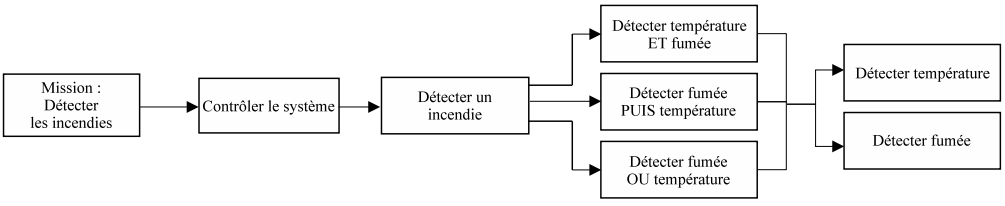


FIG. 4.1 – Modèle hiérarchique de la mission du système de protection contre les incendies

**Système de protection de l'arrimage** Le système de protection contre les désarrimages, quant à lui, a une mission en phase de convoi : *Détecter un désarrimage longitudinal et/ou transversal du camion transporté*. Cette mission est assurée par une fonction de contrôle du système qui possède une sous-fonction : *Détecter les mouvements du camion*. Cette détection est assurée par deux sous-fonctions : *Détecter un mouvement longitudinal* et *Détecter un mouvement transversal*.

La détection du mouvement longitudinal est assurée par deux sous-fonctions : *Détecter la position longitudinale du camion sur le wagon* et *Détecter l'accélération longitudinale du camion par rapport au wagon*. De plus, un mouvement longitudinal est détecté de trois façons différentes, on peut :

- soit détecter une accélération brutale **ou** une position inattendue du camion,
- soit détecter une accélération brutale **et** une position inattendue du camion,
- soit détecter une accélération brutale **puis** une position inattendue du camion.

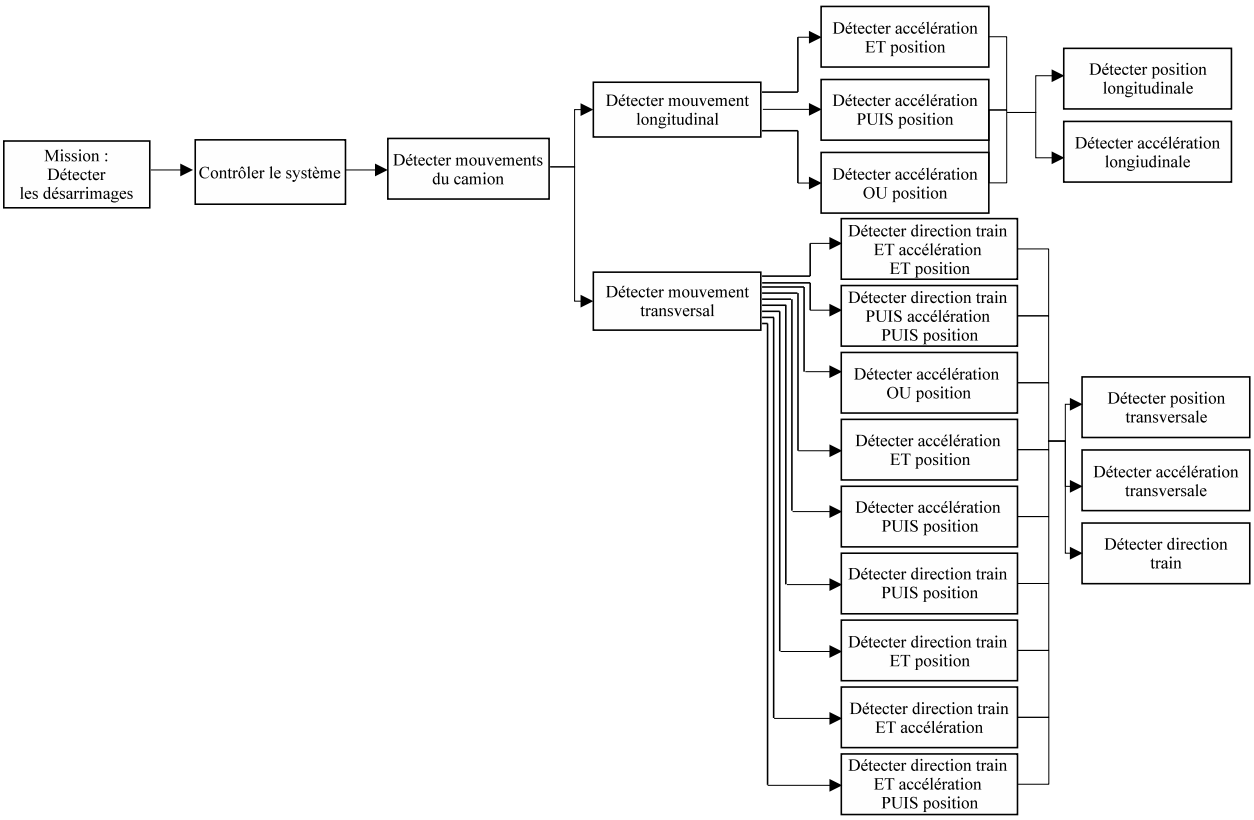


FIG. 4.2 – Modèle hiérarchique de la mission du système de protection contre le désarrimage

De la même façon, la détection du mouvement transversal est assurée par trois sous-fonctions : *Détecter la position transversale du camion*, *Détecter l'accélération transversale* et *Détecter la direction du train*. De plus, un mouvement transversal est détecté de neuf façons différentes (la seule détection d'un changement de direction du train n'est pas suffisante pour détecter un éventuel désarrimage du camion), on peut :

- soit détecter une accélération brutale **ou** une position inattendue du camion,
- soit détecter une accélération brutale **et** une position inattendue du camion,
- soit détecter une accélération brutale **puis** une position inattendue du camion,
- soit détecter un changement de direction du train **puis** une position inattendue du camion,

- soit détecter un changement de direction du train **et** une position inattendue du camion,
- soit détecter un changement de direction du train **puis** une accélération brutale,
- soit détecter un changement de direction du train **et** une accélération brutale **et** une position inattendue du camion,
- soit détecter un changement de direction du train **et** une accélération brutale **puis** une position inattendue du camion,
- soit détecter un changement de direction du train **puis** une accélération brutale **puis** une position inattendue du camion.

La figure 4.2 présente le modèle hiérarchique obtenu.

### 4.2.2 Enrichissement du modèle avec des fonctions de sécurité

La deuxième phase consiste à enrichir le précédent modèle avec des fonctions de sécurité. Pour les deux systèmes de protection, cette fonction consiste à *alerter les opérateurs du système* (conducteur du train et/ou opérateur d'un poste de contrôle commande par exemple). Cette fonction est assurée par l'association de deux sous-fonctions : *Envoyer un signal depuis le système de traitement embarqué* et *Alimenter en énergie le système de traitement embarqué*. Les figures 4.3 et 4.4 présentent les modèles hiérarchiques enrichis pour les deux systèmes de protection.

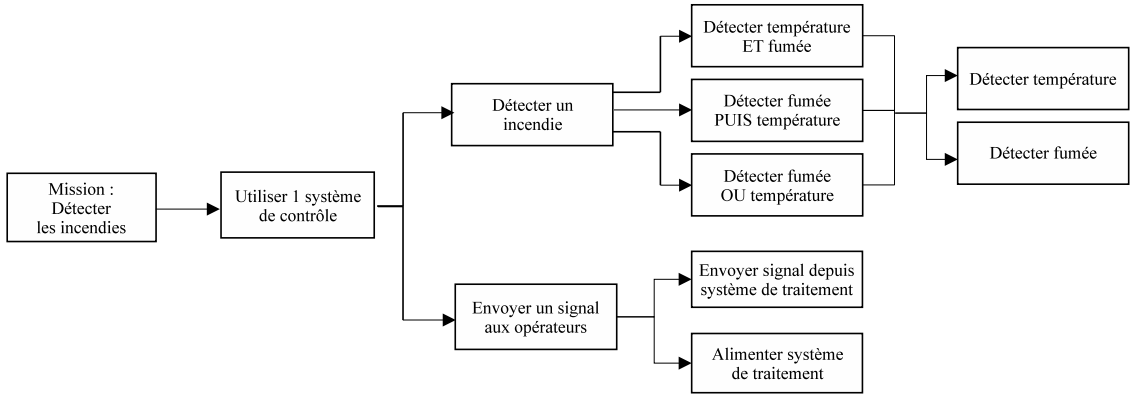


FIG. 4.3 – Modèle hiérarchique enrichi du système de protection contre les incendies

### 4.2.3 Ajout des équipements au modèle fonctionnel

La phase suivante consiste à ajouter les stratégies d'agencement et les composants utilisés par les fonctions du modèle fonctionnel précédent. Pour nos deux systèmes de protection, deux types de redondances peuvent être choisies : active ou passive et deux types de structures : série ou parallèle.

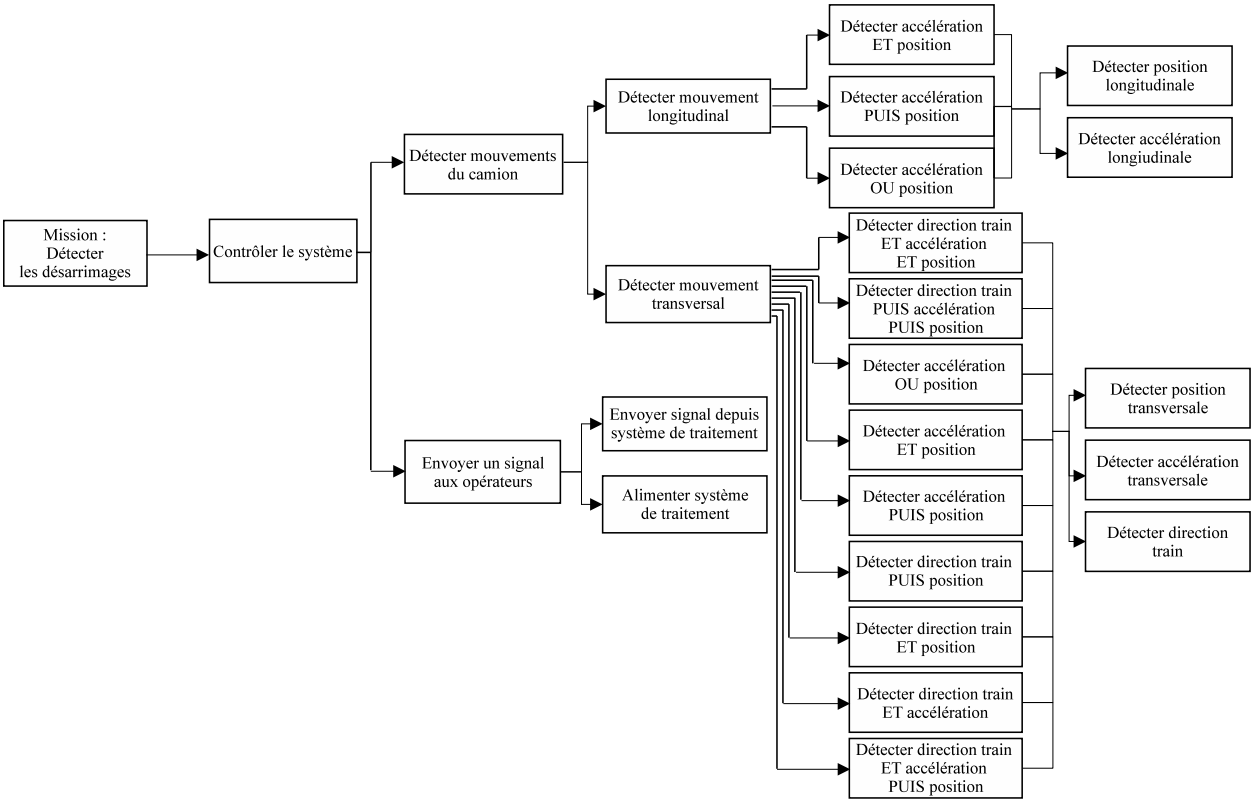


FIG. 4.4 – Modèle hiérarchique enrichi du système de protection contre les désarrimages

**Système de protection de l'incendie** Le modèle du système de protection contre les incendies est composé d'une mission et de quatre fonctions de base : *Détecter température*, *Détecter fumée*, *Envoyer un signal depuis le système de traitement* et *Alimenter le système de traitement*. Plusieurs composants peuvent être utilisés : des détecteurs de température et de fumées, des automates programmables (API) qui effectuent des traitements en fonction des données reçues et qui envoient des alarmes aux opérateurs et des blocs d'alimentation qui alimentent les API sur le train. Par ailleurs, la mission de ce système peut être accomplie par un ou deux systèmes de contrôle.
Il est bon de noter également que les API sont agencés avec ou sans alarme prioritaire. Ces possibilités font référence à deux automates organisés en redondance active qui produisent ou non une alarme lorsqu'ils sortent de leur mode de fonctionnement normal.
La correspondance entre ces composants et les fonctions de base est résumée dans le tableau 4.1.

**Système de protection de l'arrimage** Le modèle du système de protection de l'arrimage est composé d'une mission et de sept fonctions de base auxquelles il faut ajouter des composants : *Détecter la position longitudinale*, *Détecter l'accélération longitudinale*, *Détecter*

| Fonctions | Composants associés | Possibilités d'organisation |
|---|---|---|
| Détecter les incendies | Système de contrôle | - Un seul système<br>- Deux systèmes en redondance passive |
| Alimenter le système | Bloc d'alimentation | - Une seule alimentation<br>- Deux alimentations en redondance active<br>- Deux alimentations en redondance passive |
| Envoyer un signal | API | - Un seul automate<br>- Deux automates avec alarme prioritaire<br>- Deux automates sans alarme prioritaire |
| Détecter température | Détecteur température | - Un seul détecteur<br>- Deux détecteurs en série<br>Deux détecteurs en parallèle |
| Détecter fumée | Détecteur fumée | - Un seul détecteur<br>- Deux détecteurs en série<br>Deux détecteurs en parallèle |

TAB. 4.1 – Fonctions, composants utilisés et possibilités d'agencement pour le système de protection incendie

| Fonctions | Composants associés | Possibilités d'organisation |
|---|---|---|
| Détecter les désarrimages | Système de contrôle | - Un seul système<br>- Deux systèmes en redondance passive |
| Alimenter le système | Bloc d'alimentation | - Une seule alimentation<br>- Deux alimentations en redondance active<br>- Deux alimentations en redondance passive |
| Envoyer un signal | API | - Un seul automate<br>- Deux automates avec alarme prioritaire<br>- Deux automates sans alarme prioritaire |
| Détecter position | Détecteur position | - Un seul détecteur<br>- Deux détecteurs en série<br>Deux détecteurs en parallèle |
| Détecter accélération | Détecteur d'accélération | - Un seul détecteur<br>- Deux détecteurs en série<br>Deux détecteurs en parallèle |
| Détecter direction train | Gyroscope | - Un seul gyroscope<br>- Deux gyroscopes en redondance active<br>Deux gyroscopes en redondance passive |

TAB. 4.2 – Fonctions, composants utilisés et possibilités d'agencement pour le système de protection de l'arrimage

*la position transversale*, *Détecter l'accélération longitudinale*, *Détecter la direction du train*, *Envoyer un signal depuis le système de traitement* et *Alimenter en énergie le système de traitement*. Le mouvement longitudinal est détecté par le système de protection de l'arrimage à l'aide de détecteurs de position placés à l'avant et à l'arrière du wagon et de détecteurs d'accélération 1 axe placés sur le camion lors de la phase de chargement.
Le mouvement transversal est lui aussi détecté par des détecteurs de position sur la droite et sur la gauche du wagon, par des détecteurs d'accélération 1 axe sur le camion et par des gyroscopes placés sur le wagon permettant de déterminer un changement de direction du train.
Des automates programmables (API) et des blocs d'alimentation indépendants du système de protection incendie sont utilisés pour l'envoi de signaux d'alarme aux opérateurs. Par ailleurs, la mission de ce système peut être accomplie par un ou deux systèmes de contrôle. La correspondance entre ces composants et les fonctions est résumée dans le tableau 4.2.

### 4.2.4 Définition des alternatives de composants

La dernière phase de construction du modèle est d'ajouter les alternatives des composants utilisés. Pour les deux systèmes de protection ferroviaires deux types de composants (standards et sécuritaires) peuvent être utilisés et sont décrits dans le tableau 4.3

| Système Incendie | | Système Arrimage | |
|---|---|---|---|
| Composants | Types de composants | Composants | Types de composants |
| Bloc d'alimentation | - Standard<br>- Sûr | Bloc d'alimentation | - Standard<br>- Sûr |
| API | - Standard<br>- Sûr type 1<br>- Sûr type 2 | API | - Standard<br>- Sûr type 1<br>- Sûr type 2 |
| Détecteur température | - Standard<br>- Sûr type 1<br>- Sûr type 2 | Détecteur position | - Standard<br>- Sûr type 1<br>- Sûr type 2 |
| Détecteur fumée | - Standard<br>- Sûr type 1<br>- Sûr type 2 | Détecteur d'accélération | - Standard<br>- Sûr type 1<br>- Sûr type 2 |
| | | Gyroscope | - Standard<br>- Sûr type 1<br>- Sûr type 2 |

TAB. 4.3 – Composants et alternatives utilisés pour les systèmes de protection

Ainsi les deux modèles hiérarchiques sont présentés Figures 4.5 et 4.6.

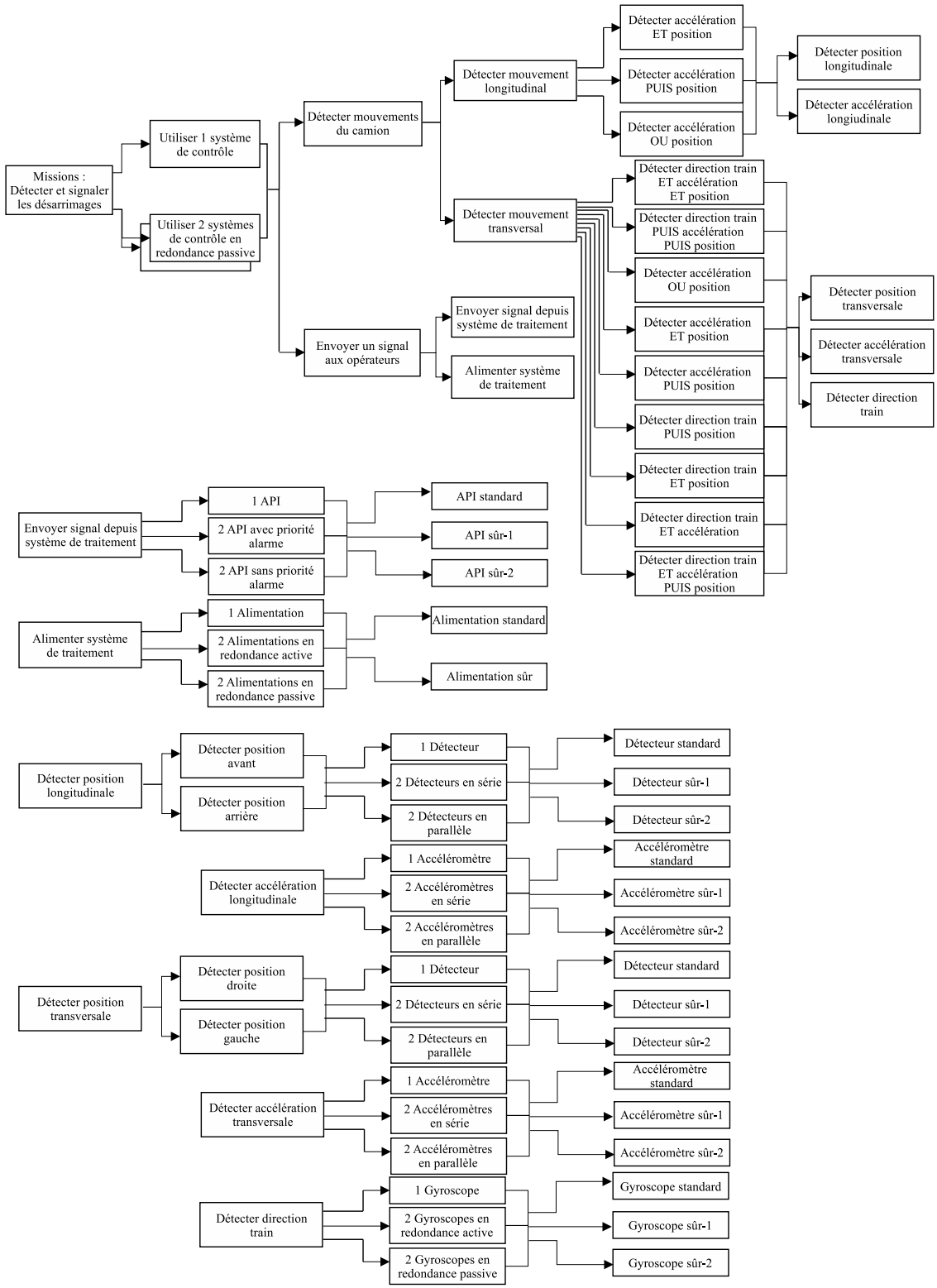


FIG. 4.5 – Modèle hiérarchique du système de protection contre les désarrimages

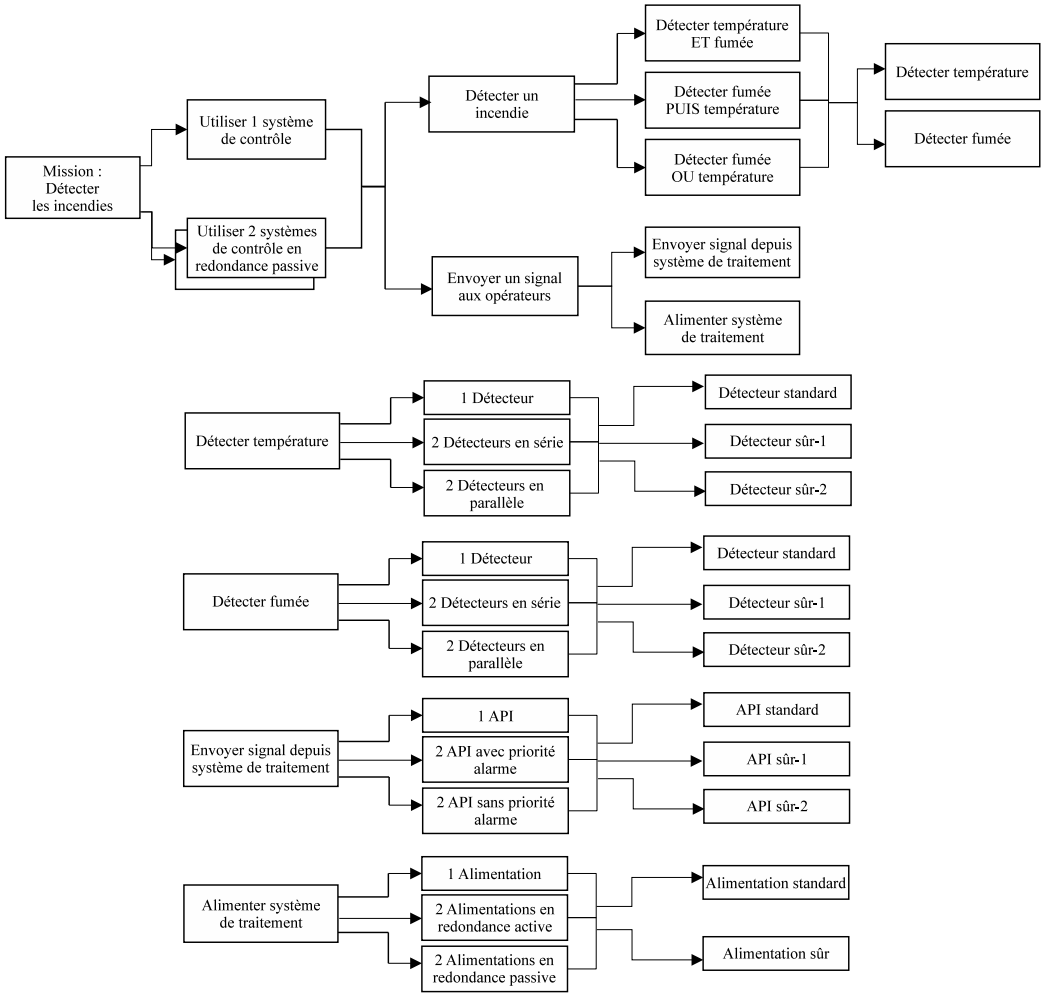


FIG. 4.6 – Modèle hiérarchique du système de protection contre les incendies

## 4.2.5 Construction du modèle comportemental

### 4.2.5.1 Définition des événements redoutés et des modes de défaillances

La première étape dans la construction de l'arbre est de définir les événements redoutés associés aux missions des systèmes. Ainsi, les événements redoutés suivants sont affectés pour le système de protection de l'incendie :

- Non détection de l'incendie provenant du système de traitement quand un incendie est présent (mode de défaillance noté $ER_1$). Cet événement est associé au niveau de sécurité du système.
- Fausse alarme (mode de défaillance noté $ER_2$) : suite à des défaillances, le système active de façon intempestive une alarme en l'absence d'incendie provoquant un arrêt temporaire du train sur la ligne. Cet événement peut être associé à la disponibilité du système.

| Composants | Mode de défaillance | Types de composants (Coût, {RRC}) |
|---|---|---|
| Bloc d'alimentation | - Arrêt inattendu | - Standard (5, {1})<br>- Sûr (10, {2}) |
| API | - Arrêt inattendu avec alarme<br>- Arrêt inattendu sans alarme | - Standard (3, {1, 1})<br>- Sûr type 1 (8, {2, 1})<br>- Sûr type 2 (8, {1, 2}) |
| Détecteur de température | - Continuellement actif<br>- Continuellement passif | - Standard (1, {1, 1})<br>- Sûr type 1 (2, {2, 1})<br>- Sûr type 2 (2, {1, 2}) |
| Détecteur de fumée | - Continuellement actif<br>- Continuellement passif | - Standard (1, {1, 1})<br>- Sûr type 1 (2, {2, 1})<br>- Sûr type 2 (2, {1, 2}) |

TAB. 4.4 – Composants, modes de défaillances et types pour le système de protection incendie du ferroutage

| Composants | Mode de défaillance | Types de composants (Coût, {RRC}) |
|---|---|---|
| Bloc d'alimentation | - Arrêt inattendu | - Standard (5, {1})<br>- Sûr (10, {2}) |
| API | - Arrêt inattendu avec alarme<br>- Arrêt inattendu sans alarme | - Standard (3, {1, 1})<br>- Sûr type 1 (8, {2, 1})<br>- Sûr type 2 (8, {1, 2}) |
| Détecteur de position | - Continuellement actif<br>- Continuellement passif | - Standard (1, {1, 1})<br>- Sûr type 1 (2, {2, 1})<br>- Sûr type 2 (2, {1, 2}) |
| Détecteur d'accélération | - Continuellement actif<br>- Continuellement passif | - Standard (2, {1, 1})<br>- Sûr type 1 (3, {2, 1})<br>- Sûr type 2 (3, {1, 2}) |
| Gyroscope | - Continuellement actif<br>- Continuellement passif | - Standard (3, {1, 1})<br>- Sûr type 1 (4, {2, 1})<br>- Sûr type 2 (4, {1, 2}) |

TAB. 4.5 – Composants, modes de défaillances et types pour le système de protection de l'arrimage

De la même façon, les événements redoutés suivants sont affectés pour le système de protection de l'arrimage :

- Non détection d'un désarrimage provenant du système de traitement quand un désarrimage est effectif (mode de défaillance noté $ER_3$). Cet événement est associé au niveau de sécurité du système.
- Fausse alarme (mode de défaillance noté $ER_4$) : suite à des défaillances, le système ac-

tive de façon intempestive une alarme en l'absence de désarrimage provoquant également un arrêt temporaire du train sur la ligne. Cet événement peut être associé à la disponibilité du système.

Les tableaux 4.4 et 4.5 donnent les modes de défaillances pour les composants utilisés dans le modèle hiérarchique ainsi que le coût et le RRC associé à chaque mode de défaillance permettant de définir les différentes robustesses de ces composants.

#### 4.2.5.2 Ajout des relations entre modes de défaillances

La seconde étape dans la construction de l'arbre est d'associer à chaque noeud de l'arbre hiérarchique l'ensemble des relations entre modes de défaillances décrivant le comportement dysfonctionnel de la fonction correspondante. Ainsi, ces arbres caractérisent le comportement des systèmes considérés en présence de défaillances.

**Cas du système incendie** L'arbre de défaillances multiples est présenté sur la figure 4.7. Sur cette figure, la fonction de détection des incendies peut être accomplie de trois façons différentes (noeud alternatif N3) : soit la fumée et la température sont détectées simultanément (arc *Arc1*), soit successivement (arc *Arc2*) ou soit uniquement la fumée ou soit uniquement la température (arc *Arc3*). Il est bon de noter qu'avec l'arbre de défaillance classique, la seconde possibilité, la détection successive, ne peut être modélisée.
Considérons la détection d'incendie qui considère la détection de fumées suivie de la détection de l'augmentation de température afin d'expliquer comment le comportement dysfonctionnel de cette détection est modélisé. Les deux relations entre modes de défaillances, représentées par l'arc *Arc2* du noeud N3 de la figure 4.7, sont expliquées ci-dessous :

- Non détection de l'incendie provenant du système de traitement quand un feu est détecté ($B_1$), si :
  - La fonction de détection de fumées est continuellement passive, c'est-à-dire que la fonction ne produira pas d'alarme ($E_1$).

  **AND**
  - La fonction de détection de température est continuellement passive, c'est-à-dire que la fonction ne produira pas d'alarme ($D_1$).

L'équation 4.1 formalise cette relation entre modes de défaillances.

$$Detec.Fumee(E_1) \textbf{ AND } Detec.Temp(D_1) \Rightarrow B_1 \tag{4.1}$$

- Fausse alarme provenant du système ($B_2$), si :
  - La fonction de détection de fumées est continuellement active, c'est-à-dire que la fonction produit une fausse alarme ($E_2$).

  **PAND**

– La fonction de détection de température est continuellement active, c'est-à-dire que la fonction produit une fausse alarme ($D_2$).

De la même façon, nous formalisons cette relation avec l'équation 4.2.

$$Detec.Fumee(E_2)\ \textbf{PAND}\ Detec.Temp(D_2)\ \Rightarrow B_2 \tag{4.2}$$

Puis, pour chaque noeud de cet arbre, les relations entre modes de défaillances sont associées avec le même principe de formalisation jusqu'à atteindre les composants et nous déterminons l'arbre de défaillances multiples présenté figure 4.7 et dans les tables 4.6 et 4.7.

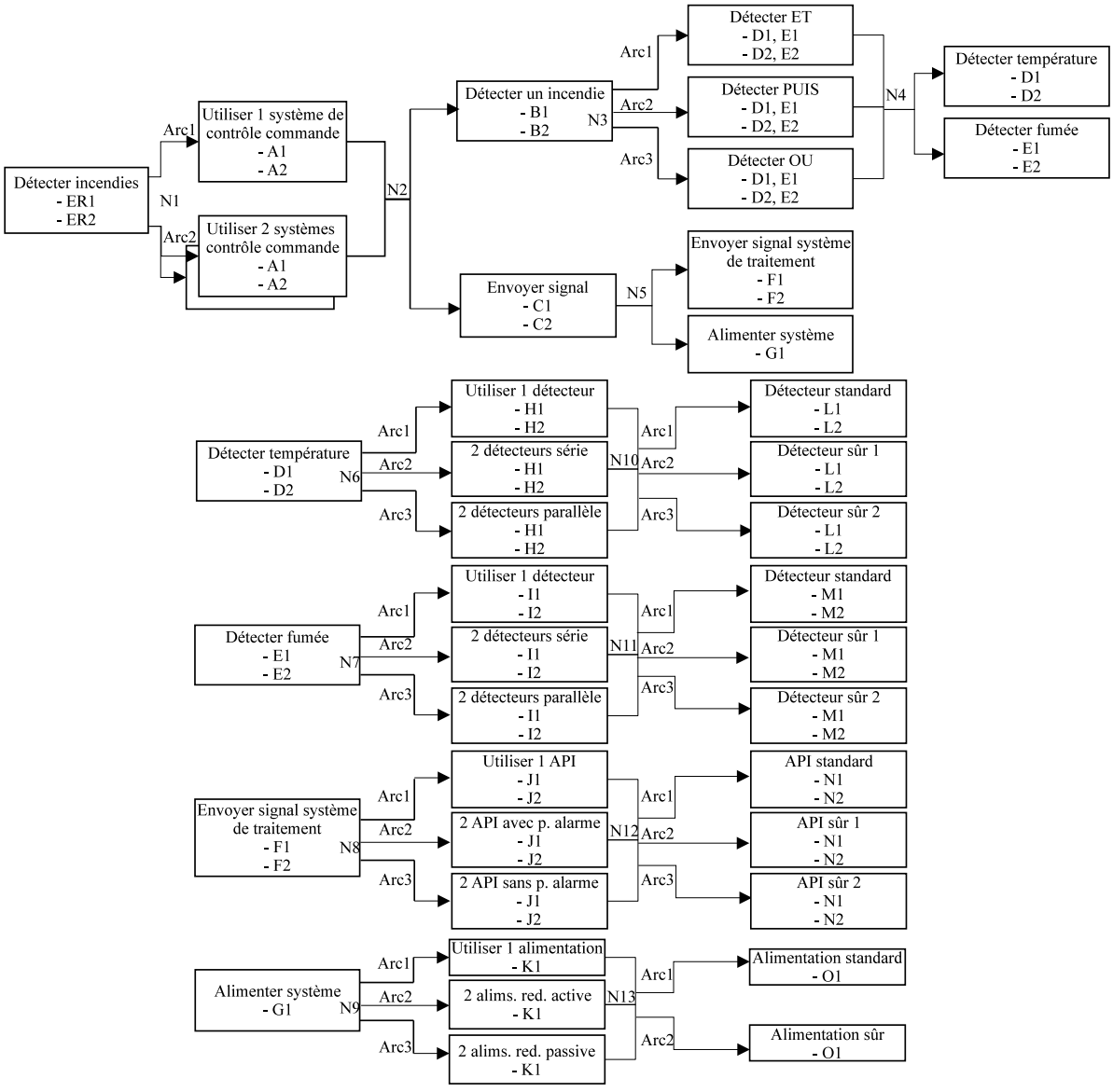


FIG. 4.7 – Arbre de défaillances multiples amélioré du système de protection de l'incendie

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Mission : Détecter et signaler incendies | Noeud alternatif N1 | - ER1 : Non détection<br>- ER2 : Fausse alarme |
| Utiliser 1 système de contrôle commande | Noeud associatif N2 | - A1 : Non détection<br>- A2 : Fausse alarme |
| Utiliser 2 systèmes de contrôle commande | Noeud associatif N2 | - A1 : Non détection<br>- A2 : Fausse alarme |
| Détecter un incendie | Noeud alternatif N3 | - B1 : Non détection<br>- B2 : Fausse alarme |
| Détecter Température ET Fumée | Noeud élémentaire N4 | - D1, E1 : Continuellement passif<br>- D2, E2 : Continuellement actif |
| Détecter Fumée PUIS température | Noeud élémentaire N4 | - D1, E1 : Continuellement passif<br>- D2, E2 : Continuellement actif |
| Détecter Fumée OU température | Noeud élémentaire N4 | - D1, E1 : Continuellement passif<br>- D2, E2 : Continuellement actif |
| Envoyer signal aux opérateurs | Noeud associatif N5 | - C1 : Non détection<br>- C2 : Fausse alarme |
| Détecter température | Noeud alternatif N6 | - D1 : Continuellement passif<br>- D2 : Continuellement actif |
| Détecter fumée | Noeud alternatif N7 | - E1 : Continuellement passif<br>- E2 : Continuellement actif |
| Envoyer signal depuis système de traitement | Noeud alternatif N8 | - F1 : Arrêt inattendu ac alarme<br>- F2 : Arrêt inattendu ss alarme |
| Alimenter système de traitement | Noeud alternatif N9 | - G1 : Arrêt inattendu |
| Utiliser 1 détecteur température | Noeud alternatif N10 | - H1 : Continuellement actif<br>- H2 : Continuellement passif |
| Utiliser 2 détecteurs en série | Noeud alternatif N10 | - H1 : Continuellement actif<br>- H2 : Continuellement passif |
| Utiliser 2 détecteurs en parrallèle | Noeud alternatif N10 | - H1 : Continuellement actif<br>- H2 : Continuellement passif |
| Utiliser 1 détecteur fumée | Noeud alternatif N11 | - I1 : Continuellement actif<br>- I2 : Continuellement passif |

TAB. 4.6 – A : Correspondance entre fonctions et modes de défaillances de la figure 4.7

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Utiliser 2 détecteurs en série | Noeud alternatif N11 | - I1 : Continuellement actif<br>- I2 : Continuellement passif |
| Utiliser 2 détecteurs en parallèle | Noeud alternatif N11 | - I1 : Continuellement actif<br>- I2 : Continuellement passif |
| Utiliser 1 API | Noeud alternatif N12 | - J1 : Arrêt avec alarme<br>- I2 : Arrêt sans alarme |
| Utiliser 2 API avec priorité alarme | Noeud alternatif N12 | - J1 : Arrêt avec alarme<br>- I2 : Arrêt sans alarme |
| Utiliser 2 API sans priorité alarme | Noeud alternatif N12 | - J1 : Arrêt avec alarme<br>- I2 : Arrêt sans alarme |
| Utiliser 1 Alimentation | Noeud alternatif N13 | - K1 : Arrêt inattendu |
| Utiliser 2 Alimentations en redondance active | Noeud alternatif N13 | - K1 : Arrêt inattendu |
| Utiliser 2 Alimentations en redondance passive | Noeud alternatif N13 | - K1 : Arrêt inattendu |
| Détecteur Température standard | Pas de noeud | - L1 : Continuellement passif<br>- L2 : Continuellement actif |
| Détecteur Température sûr type 1 | Pas de noeud | - L1 : Continuellement passif<br>- L2 : Continuellement actif |
| Détecteur Température sûr type 2 | Pas de noeud | - L1 : Continuellement passif<br>- L2 : Continuellement actif |
| Détecteur Fumée standard | Pas de noeud | - M1 : Continuellement passif<br>- M2 : Continuellement actif |
| Détecteur Fumée sûr type 1 | Pas de noeud | - M1 : Continuellement passif<br>- M2 : Continuellement actif |
| Détecteur Fumée sûr type 2 | Pas de noeud | - M1 : Continuellement passif<br>- M2 : Continuellement actif |
| API standard | Pas de noeud | - N1 : Arrêt inattendu avec alarme<br>- N2 : Arrêt inattendu sans alarme |
| API sûr type 1 | Pas de noeud | - N1 : Arrêt inattendu avec alarme<br>- N2 : Arrêt inattendu sans alarme |
| API sûr type 2 | Pas de noeud | - N1 : Arrêt inattendu avec alarme<br>- N2 : Arrêt inattendu sans alarme |
| Alimentation standard | Pas de noeud | - O1 : Arrêt inattendu |
| Alimentation sûr | Pas de noeud | - O1 : Arrêt inattendu |

TAB. 4.7 – B : Correspondance entre fonctions et modes de défaillances de la figure 4.7

Relations entre modes de défaillances de la figure 4.7 :

$$\text{(N1)} \begin{cases} Arc1 \begin{cases} Syst.commande(A_1) \Rightarrow ER_1 \\ Syst.commande(A_2) \Rightarrow ER_2 \end{cases} \\ Arc2 \begin{cases} Syst.commande_1(A_1) \textbf{ SEQ } Syst.commande_2(A_2) \Rightarrow ER_1 \\ (Syst.commande_1(A_1) \textbf{ SEQ } Syst.commande_2(A_2)) \\ \textbf{OR } (Syst.commande_1(A_2) \textbf{ SEQ } Syst.commande_2(A_2)) \Rightarrow ER_2 \end{cases} \end{cases}$$

$$\text{(N2)} \begin{cases} Detec.incendie(B_1) \textbf{ OR } Envoi.signal(C_1) \Rightarrow A_1 \\ Detec.incendie(B_2) \textbf{ OR } Envoi.signal(C_2) \Rightarrow A_2 \end{cases}$$

$$\text{(N3)} \begin{cases} Arc1 \begin{cases} Detec.Temp(D_1) \textbf{ OR } Detec.Fumee(E_1) \Rightarrow B_1 \\ Detec.Temp(D_2) \textbf{ AND } Detec.Fumee(E_2) \Rightarrow B_2 \end{cases} \\ Arc2 \begin{cases} Detec.Temp(D_1) \textbf{ AND } Detec.Fumee(E_1) \Rightarrow B_1 \\ Detec.Fumee(E_2) \textbf{ PAND } Detec.Temp(D_2) \Rightarrow B_2 \end{cases} \\ Arc3 \begin{cases} Detec.Temp(D_1) \textbf{ AND } Detec.Fumee(E_1) \Rightarrow B_1 \\ Detec.Temp(D_2) \textbf{ OR } Detec.Fumee(E_2) \Rightarrow B_2 \end{cases} \end{cases}$$

$$\text{(N4)} \begin{cases} D_1 \Rightarrow D_1 \\ D_2 \Rightarrow D_2 \\ E_1 \Rightarrow E_1 \\ E_2 \Rightarrow E_2 \end{cases}$$

$$\text{(N5)} \begin{cases} Syst.traitement(F_2) \textbf{ OR } Alim.systeme(G_1) \Rightarrow C_1 \\ Syst.traitement(F_1) \Rightarrow C_2 \end{cases}$$

$$\text{(N6)} \begin{cases} Arc1 \begin{cases} Detec.Temp(H_2) \Rightarrow D_1 \\ Detec.Temp(H_1) \Rightarrow D_2 \end{cases} \\ Arc2 \begin{cases} (Detec.Temp_1(H_2) \textbf{ OR } Detec.Temp_2(H_2)) \Rightarrow D_1 \\ (Detect.Temp_1(H_1) \textbf{ AND } Detec.Temp_2(H_1)) \Rightarrow D_2 \end{cases} \\ Arc3 \begin{cases} (Detec.Temp_1(H_2) \textbf{ AND } Detec.Temp_2(H_2)) \Rightarrow D_1 \\ (Detec.Temp_1(H_1) \textbf{ OR } Detec.Temp_2(H_1)) \Rightarrow D_2 \end{cases} \end{cases}$$

$$\text{(N7)} \begin{cases} Arc1 \begin{cases} Detec.Fumee(I_2) \Rightarrow E_1 \\ Detec.Fumee(I_1) \Rightarrow E_2 \end{cases} \\ Arc2 \begin{cases} (Detec.Fumee_1(I_2) \textbf{ OR } Detec.Fumee_2(I_2)) \Rightarrow E_1 \\ (Detec.Fumee_1(I_1) \textbf{ AND } Detec.Fumee_2(I_1)) \Rightarrow E_2 \end{cases} \\ Arc3 \begin{cases} (Detec.Fumee_1(I_2) \textbf{ AND } Detec.Fumee_2(I_2)) \Rightarrow E_1 \\ (Detec.Fumee_1(I_1) \textbf{ OR } Detec.Fumee_2(I_1)) \Rightarrow E_2 \end{cases} \end{cases}$$

$$\text{(N8)} \begin{cases} Arc1 \begin{cases} API(J_1) \Rightarrow F_1 \\ API(J_2) \Rightarrow F_2 \end{cases} \\ Arc2 \begin{cases} (API_1(J_1)\ \textbf{OR}\ API_2(J_1)) \Rightarrow F_1 \\ (API_1(J_2)\ \textbf{AND}\ API_2(J_2)) \Rightarrow F_2 \end{cases} \\ Arc3 \begin{cases} (API_1(J_1)\ \textbf{AND}\ API_2(J_1)) \Rightarrow F_1 \\ (API_1(J_2)\ \textbf{OR}\ API_2(J_2)) \Rightarrow F_2 \end{cases} \end{cases}$$

$$\text{(N9)} \begin{cases} Arc1 \begin{cases} Alim.(K_1) \Rightarrow G_1 \end{cases} \\ Arc2 \begin{cases} Alim._1(K_1)\ \textbf{AND}\ Alim._2(K_1) \Rightarrow G_1 \end{cases} \\ Arc3 \begin{cases} Alim._1(K_1)\ \textbf{SEQ}\ Alim._2(K_1) \Rightarrow G_1 \end{cases} \end{cases}$$

$$\text{(N10)} \begin{cases} Arc1 \begin{cases} Detec.Temp - Standard(L_1) \Rightarrow H_1 \\ Detec.Temp - Standard(L_2) \Rightarrow H_2 \end{cases} \\ Arc2 \begin{cases} Detec.Temp - Sur1(L_1) \Rightarrow H_1 \\ Detec.Temp - Sur1(L_2) \Rightarrow H_2 \end{cases} \\ Arc3 \begin{cases} Detec.Temp - Sur2(L_1) \Rightarrow H_1 \\ Detec.Temp - Sur2(L_2) \Rightarrow H_2 \end{cases} \end{cases}$$

Les noeuds N11 à N13 ne sont pas détaillés car ils reprennent la même structure que le noeud N10 à la différence que leurs modes de défaillances correspondent à ceux de la figure 4.7 et que le terme *Detec.Temp-Standard* est remplacé par celui du composant correspondant (Detec.Fumee-Sur1, Alim.-Standard, ...).

**Cas du système d'arrimage** Pour le système de protection de l'arrimage, nous obtenons l'arbre de défaillances multiples présenté figure 4.8 et dans les tables 4.8 et 4.9. Sur cette figure, de la même façon que pour la fonction de détection des incendies, la fonction de détection du mouvement longitudinal peut être accomplie de trois façons différentes (noeud alternatif N'5, arcs *Arc1* à *Arc3*) et la fonction de détection du mouvement transversal de neuf façons différentes (noeud alternatif N'6, arcs *Arc1* à *Arc9*).

Relations entre modes de défaillances de la figure 4.8 :

$$\text{(N'1)} \begin{cases} Arc1 \begin{cases} Syst.commande(A_1) \Rightarrow ER_3 \\ Syst.commande(A_2) \Rightarrow ER_4 \end{cases} \\ Arc2 \begin{cases} Syst.commande_1(A_1)\ \textbf{SEQ}\ Syst.commande_2(A_2) \Rightarrow ER_3 \\ (Syst.commande_1(A_1)\ \textbf{SEQ}\ Syst.commande_2(A_2)) \\ \textbf{OR}\ (Syst.commande_1(A_2)\ \textbf{SEQ}\ Syst.commande_2(A_2)) \Rightarrow ER_4 \end{cases} \end{cases}$$

$$\text{(N'2)} \begin{cases} Detec.Mvt.(B_1)\ \textbf{OR}\ Envoi.signal(C_1) \Rightarrow A_1 \\ Detec.Mvt.(B_2)\ \textbf{OR}\ Envoi.signal(C_2) \Rightarrow A_2 \end{cases}$$

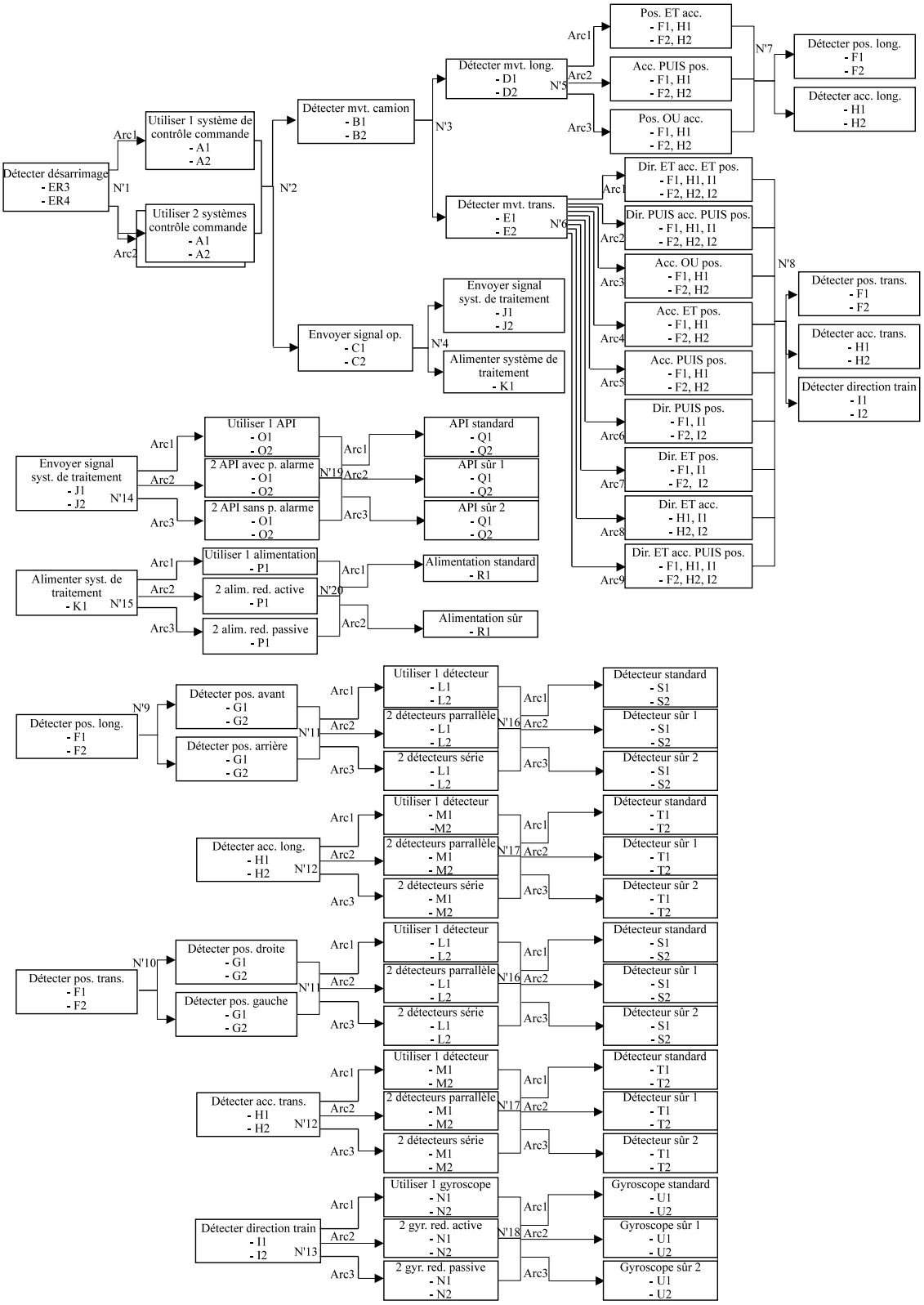


FIG. 4.8 – Arbre de défaillances multiples amélioré du système de l'arrimage

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Mission : Détecter et signaler désarrimage | Noeud alternatif N'1 | - ER3 : Non détection<br>- ER4 : Fausse alarme |
| Utiliser 1 système de contrôle commande | Noeud associatif N'2 | - A1 : Non détection<br>- A2 : Fausse alarme |
| Utiliser 2 systèmes de contrôle commande | Noeud associatif N'2 | - A1 : Non détection<br>- A2 : Fausse alarme |
| Détecter mouvements camion | Noeud associatif N'3 | - B1 : Non détection<br>- B2 : Fausse alarme |
| Envoyer signal aux opérateurs | Noeud associatif N'4 | - C1 : Non détection<br>- C2 : Fausse alarme |
| Détecter mvt long. | Noeud alternatif N'5 | - D1 : Non détection<br>- D2 : Fausse alarme |
| Détecter Accélération ET position | Noeud élémentaire N'7 | - F1, H1 : Continuellement passif<br>- F2, H2 : Continuellement actif |
| Détecter Accélération PUIS position | Noeud élémentaire N'7 | - F1, H1 : Continuellement passif<br>- F2, H2 : Continuellement actif |
| Détecter Accélération OU position | Noeud élémentaire N'7 | - F1, H1 : Continuellement passif<br>- F2, H2 : Continuellement actif |
| Détecter mvt trans. | Noeud alternatif N'6 | - E1 : Non détection<br>- E2 : Fausse alarme |
| Détecter Direction train ET accélération ET position | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |
| Détecter Direction train PUIS accélération PUIS position | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |
| Détecter Accélération OU position | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |
| Détecter Accélération ET position | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |

TAB. 4.8 – A : Correspondance entre fonctions et modes de défaillances de la figure 4.8

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Détecter Accélération PUIS position | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |
| Détecter Direction train PUIS position | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |
| Détecter Direction train ET position | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |
| Détecter Direction train ET accélération | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |
| Détecter Direction train ET accélération PUIS position | Noeud élémentaire N'8 | - F1, H1, I1 : Continuellement passif<br>- F2, H2, I2 : Continuellement actif |
| Détecter Position longitudinale | Noeud associatif N'9 | - F1 : Continuellement passif<br>- F2 : Continuellement actif |
| Détecter Position transversale | Noeud associatif N'10 | - F1 : Continuellement passif<br>- F2 : Continuellement actif |
| Détecter Position avant | Noeud alternatif N'11 | - G1 : Continuellement passif<br>- G2 : Continuellement actif |
| Détecter Position arrière | Noeud alternatif N'11 | - G1 : Continuellement passif<br>- G2 : Continuellement actif |
| Détecter Position droite | Noeud alternatif N'11 | - G1 : Continuellement passif<br>- G2 : Continuellement actif |
| Détecter Position gauche | Noeud alternatif N'11 | - G1 : Continuellement passif<br>- G2 : Continuellement actif |
| Détecter Accélération longitudinale | Noeud alternatif N'12 | - H1 : Continuellement passif<br>- H2 : Continuellement actif |
| Détecter Accélération transversale | Noeud alternatif N'12 | - H1 : Continuellement passif<br>- H2 : Continuellement actif |

TAB. 4.9 – B : Correspondance entre fonctions et modes de défaillances de la figure 4.8

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Détecter Direction train | Noeud alternatif N'13 | - I1 : Continuellement passif<br>- I2 : Continuellement actif |
| Envoyer signal depuis système de traitement | Noeud alternatif N'14 | - J1 : Arrêt inattendu ac alarme<br>- J2 : Arrêt inattendu ss alarme |
| Alimenter système de traitement | Noeud alternatif N'15 | - K1 : Arrêt inattendu |
| Utiliser 1 détecteur position | Noeud alternatif N'16 | - L1 : Continuellement actif<br>- L2 : Continuellement passif |
| Utiliser 2 détecteurs en série | Noeud alternatif N'16 | - L1 : Continuellement actif<br>- L2 : Continuellement passif |
| Utiliser 2 détecteurs en parrallèle | Noeud alternatif N'16 | - L1 : Continuellement actif<br>- L2 : Continuellement passif |
| Utiliser 1 détecteur accélération | Noeud alternatif N'17 | - M1 : Continuellement actif<br>- M2 : Continuellement passif |
| Utiliser 2 détecteurs en série | Noeud alternatif N'17 | - M1 : Continuellement actif<br>- M2 : Continuellement passif |
| Utiliser 2 détecteurs en parrallèle | Noeud alternatif N'17 | - M1 : Continuellement actif<br>- M2 : Continuellement passif |
| Utiliser 1 gyroscope | Noeud alternatif N'18 | - N1 : Continuellement actif<br>- N2 : Continuellement passif |
| Utiliser 2 gyroscopes redondance active | Noeud alternatif N'18 | - N1 : Continuellement actif<br>- N2 : Continuellement passif |
| Utiliser 2 gyroscopes redondance passive | Noeud alternatif N'18 | - N1 : Continuellement actif<br>- N2 : Continuellement passif |
| Utiliser 1 API | Noeud alternatif N'19 | - O1 : Arrêt avec alarme<br>- O2 : Arrêt sans alarme |
| Utiliser 2 API avec priorité alarme | Noeud alternatif N'19 | - O1 : Arrêt avec alarme<br>- O2 : Arrêt sans alarme |
| Utiliser 2 API sans priorité alarme | Noeud alternatif N'19 | - O1 : Arrêt avec alarme<br>- O2 : Arrêt sans alarme |
| Utiliser 1 Alimentation | Noeud alternatif N'20 | - P1 : Arrêt inattendu |
| Utiliser 2 Alimentations en redondance active | Noeud alternatif N'20 | - P1 : Arrêt inattendu |
| Utiliser 2 Alimentations en redondance passive | Noeud alternatif N'19 | - P1 : Arrêt inattendu |

TAB. 4.10 – C : Correspondance entre fonctions et modes de défaillances de la figure 4.8

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Détecteur Position standard | Pas de noeud | - S1 : Continuellement passif<br>- S2 : Continuellement actif |
| Détecteur Position sûr type 1 | Pas de noeud | - S1 : Continuellement passif<br>- S2 : Continuellement actif |
| Détecteur Position sûr type 2 | Pas de noeud | - S1 : Continuellement passif<br>- S2 : Continuellement actif |
| Détecteur Accélération standard | Pas de noeud | - T1 : Continuellement passif<br>- T2 : Continuellement actif |
| Détecteur Accélération sûr type 1 | Pas de noeud | - T1 : Continuellement passif<br>- T2 : Continuellement actif |
| Détecteur Accélération sûr type 2 | Pas de noeud | - T1 : Continuellement passif<br>- T2 : Continuellement actif |
| Gyroscope standard | Pas de noeud | - U1 : Continuellement passif<br>- U2 : Continuellement actif |
| Gyroscope sûr type 1 | Pas de noeud | - U1 : Continuellement passif<br>- U2 : Continuellement actif |
| Gyroscope sûr type 2 | Pas de noeud | - U1 : Continuellement passif<br>- U2 : Continuellement actif |
| API standard | Pas de noeud | - Q1 : Arrêt inattendu avec alarme<br>- Q2 : Arrêt inattendu sans alarme |
| API sûr type 1 | Pas de noeud | - Q1 : Arrêt inattendu avec alarme<br>- Q2 : Arrêt inattendu sans alarme |
| API sûr type 2 | Pas de noeud | - Q1 : Arrêt inattendu avec alarme<br>- Q2 : Arrêt inattendu sans alarme |
| Alimentation standard | Pas de noeud | - R1 : Arrêt inattendu |
| Alimentation sûr | Pas de noeud | - R1 : Arrêt inattendu |

TAB. 4.11 – D : Correspondance entre fonctions et modes de défaillances de la figure 4.8

$$\text{(N'3)} \begin{cases} Detec.Mvt.long.(D_1)\ \textbf{AND}\ Detec.Mvt.trans.(E_1) \Rightarrow B_1 \\ Detec.Mvt.long.(D_2)\ \textbf{OR}\ Detec.Mvt.trans.(E_2) \Rightarrow B_2 \end{cases}$$

$$\text{(N'4)} \begin{cases} Signal.syst.(J_2)\ \textbf{OR}\ Alim.syst.(K_1) \Rightarrow C_1 \\ Signal.syst.(J_1) \Rightarrow C_2 \end{cases}$$

$$\text{(N'5)} \begin{cases} Arc1 \begin{cases} Detec.Pos.(F_1)\ \textbf{OR}\ Detec.Acc.(H_1) \Rightarrow D_1 \\ Detec.Pos.(F_2)\ \textbf{AND}\ Detec.Acc.(H_2) \Rightarrow D_2 \end{cases} \\ Arc2 \begin{cases} Detec.Pos.(F_1)\ \textbf{AND}\ Detec.Acc.(H_1) \Rightarrow D_1 \\ Detec.Acc.(H_2)\ \textbf{PAND}\ Detec.Pos.(F_2) \Rightarrow D_2 \end{cases} \\ Arc3 \begin{cases} Detec.Pos.(F_1)\ \textbf{AND}\ Detec.Acc.(H_1) \Rightarrow D_1 \\ Detec.Pos.(F_2)\ \textbf{OR}\ Detec.Acc.(H_2) \Rightarrow D_2 \end{cases} \end{cases}$$

$$
\text{(N'6)}\begin{cases}
Arc1\begin{cases} Detec.Pos.(F_1)\ \textbf{OR}\ Detec.Acc.(H_1)\ \textbf{OR}\ Detec.Dir.(I_1) \Rightarrow E_1 \\ Detec.Pos.(F_2)\ \textbf{AND}\ Detec.Acc.(H_2)\ \textbf{AND}\ Detec.Dir.(I_2) \Rightarrow E_2 \end{cases} \\
Arc2\begin{cases} Detec.Pos.(F_1)\ \textbf{AND}\ Detec.Acc.(H_1)\ \textbf{AND}\ Detec.Dir.(I_1) \Rightarrow E_1 \\ Detec.Dir.(I_2)\ \textbf{PAND}\ Detec.Acc.(H_2)\ \textbf{PAND}\ Detec.Pos.(F_2) \Rightarrow E_2 \end{cases} \\
Arc3\begin{cases} Detec.Pos.(F_1)\ \textbf{AND}\ Detec.Acc.(H_1) \Rightarrow E_1 \\ Detec.Pos.(F_2)\ \textbf{OR}\ Detec.Acc.(H_2) \Rightarrow E_2 \end{cases} \\
Arc4\begin{cases} Detec.Pos.(F_1)\ \textbf{OR}\ Detec.Acc.(H_1) \Rightarrow E_1 \\ Detec.Pos.(F_2)\ \textbf{AND}\ Detec.Acc.(H_2) \Rightarrow E_2 \end{cases} \\
Arc5\begin{cases} Detec.Pos.(F_1)\ \textbf{AND}\ Detec.Acc.(H_1) \Rightarrow E_1 \\ Detec.Acc.(H_2)\ \textbf{PAND}\ Detec.Pos.(F_2) \Rightarrow E_2 \end{cases} \\
Arc6\begin{cases} Detec.Pos.(F_1)\ \textbf{AND}\ Detec.Dir.(I_1) \Rightarrow E_1 \\ Detec.Dir.(I_2)\ \textbf{PAND}\ Detec.Pos.(F_2) \Rightarrow E_2 \end{cases} \\
Arc7\begin{cases} Detec.Pos.(F_1)\ \textbf{OR}\ Detec.Dir.(I_1) \Rightarrow E_1 \\ Detec.Pos.(F_2)\ \textbf{AND}\ Detec.Dir.(I_2) \Rightarrow E_2 \end{cases} \\
Arc8\begin{cases} Detec.Acc.(H_1)\ \textbf{OR}\ Detec.Dir.(I_1) \Rightarrow E_1 \\ Detec.Acc.(H_2)\ \textbf{AND}\ Detec.Dir.(I_2) \Rightarrow E_2 \end{cases} \\
Arc9\begin{cases} Detec.Pos.(F_1)\ \textbf{AND}\ Detec.Acc.(H_1)\ \textbf{AND}\ Detec.Dir.(I_1) \Rightarrow E_1 \\ Detec.Dir.(I_2)\ \textbf{AND}\ (Detec.Acc.(H_2)\ \textbf{PAND}\ Detec.Pos.(F_2)) \Rightarrow E_2 \end{cases}
\end{cases}
$$

$$
\text{(N'7)}\begin{cases} F_1 \Rightarrow F_1 \\ F_2 \Rightarrow F_2 \\ H_1 \Rightarrow H_1 \\ H_2 \Rightarrow H_2 \end{cases}
$$

$$
\text{(N'8)}\begin{cases} F_1 \Rightarrow F_1 \\ F_2 \Rightarrow F_2 \\ H_1 \Rightarrow H_1 \\ H_2 \Rightarrow H_2 \\ I_1 \Rightarrow I_1 \\ I_2 \Rightarrow I_2 \end{cases}
$$

$$
\text{(N'9)}\begin{cases} Pos.Avant(G_1)\ \textbf{AND}\ Pos.Arriere(G_1) \Rightarrow F_1 \\ Pos.Avant(G_2)\ \textbf{OR}\ Pos.Arriere(G_2) \Rightarrow F_2 \end{cases}
$$

$$
\text{(N'11)}\begin{cases}
Arc1\begin{cases} Detec.Pos.(L_2) \Rightarrow G_1 \\ Detec.Pos(L_1) \Rightarrow G_2 \end{cases} \\
Arc2\begin{cases} (Detec.Pos._1(L_2)\ \textbf{OR}\ Detec.Pos._2(L_2)) \Rightarrow G_1 \\ (Detec.Pos._1(L_1)\ \textbf{AND}\ Detec.Pos._2(L_1)) \Rightarrow G_2 \end{cases} \\
Arc3\begin{cases} (Detec.Pos._1(L_2)\ \textbf{AND}\ Detec.Pos._2(L_2)) \Rightarrow G_1 \\ (Detec.Pos._1(L_1)\ \textbf{OR}\ Detec.Pos._2(L_1)) \Rightarrow G_2 \end{cases}
\end{cases}
$$

$$\text{(N'10)} \begin{cases} Pos.Droite(G_1)\ \textbf{AND}\ Pos.Gauche(G_1) \Rightarrow F_1 \\ Pos.Droite(G_2)\ \textbf{OR}\ Pos.Gauche(G_2) \Rightarrow F_2 \end{cases}$$

$$\text{(N'12)} \begin{cases} Arc1 \begin{cases} Detec.Acc.(M_2) \Rightarrow H_1 \\ Detec.Acc.(M_1) \Rightarrow H_2 \end{cases} \\ Arc2 \begin{cases} (Detec.Acc._1(M_2)\ \textbf{OR}\ Detec.Acc._2(M_2)) \Rightarrow H_1 \\ (Detec.Acc._1(M_1)\ \textbf{AND}\ Detec.Acc._2(M_1)) \Rightarrow H_2 \end{cases} \\ Arc3 \begin{cases} (Detec.Acc._1(M_2)\ \textbf{AND}\ Detec.Acc._2(M_2)) \Rightarrow H_1 \\ (Detec.Acc._1(M_1)\ \textbf{OR}\ Detec.Acc._2(M_1)) \Rightarrow H_2 \end{cases} \end{cases}$$

$$\text{(N'13)} \begin{cases} Arc1 \begin{cases} Gyr.(N_2) \Rightarrow I_1 \\ Gyr.(N_1) \Rightarrow I_2 \end{cases} \\ Arc2 \begin{cases} (Gyr._1(N_2)\ \textbf{OR}\ Gyr._2(N_2)) \Rightarrow I_1 \\ (Gyr._1(N_1)\ \textbf{AND}\ Gyr._2(N_1)) \Rightarrow I_2 \end{cases} \\ Arc3 \begin{cases} (Gyr._1(N_2)\ \textbf{AND}\ Gyr._2(N_2)) \Rightarrow I_1 \\ (Gyr._1(N_1)\ \textbf{OR}\ Gyr._2(N_1)) \Rightarrow I_2 \end{cases} \end{cases}$$

$$\text{(N'14)} \begin{cases} Arc1 \begin{cases} API(O_2) \Rightarrow J_1 \\ API(O_1) \Rightarrow J_2 \end{cases} \\ Arc2 \begin{cases} (API_1(O_2)\ \textbf{OR}\ API_2(O_2)) \Rightarrow J_1 \\ (API_1(O_1)\ \textbf{AND}\ API_2(O_1)) \Rightarrow J_2 \end{cases} \\ Arc3 \begin{cases} (API_1(O_2)\ \textbf{AND}\ API_2(O_2)) \Rightarrow J_1 \\ (API_1(O_1)\ \textbf{OR}\ API_2(O_1)) \Rightarrow J_2 \end{cases} \end{cases}$$

$$\text{(N'15)} \begin{cases} Arc1 \begin{cases} Alim.(P_1) \Rightarrow K_1 \end{cases} \\ Arc2 \begin{cases} Alim._1(P_1)\ \textbf{AND}\ Alim._2(P_1) \Rightarrow K_1 \end{cases} \\ Arc3 \begin{cases} Alim._1(P_1)\ \textbf{SEQ}\ Alim._2(P_1) \Rightarrow K_1 \end{cases} \end{cases}$$

$$\text{(N'16)} \begin{cases} Arc1 \begin{cases} Detec.Pos.-Standard(S_1) \Rightarrow L_1 \\ Detec.Pos.-Standard(S_2) \Rightarrow L_2 \end{cases} \\ Arc2 \begin{cases} Detec.Pos.-Sur1(S_1) \Rightarrow L_1 \\ Detec.Pos.-Sur1(S_2) \Rightarrow L_2 \end{cases} \\ Arc3 \begin{cases} Detec.Pos.-Sur2(S_1) \Rightarrow L_1 \\ Detec.Pos.-Sur2(S_2) \Rightarrow L_2 \end{cases} \end{cases}$$

Les noeuds N'17 à N'20 ne sont pas détaillés car ils reprennent la même structure que le noeud N'16 à la différence que leurs modes de défaillances correspondent à ceux de la figure 4.8 et que le terme *Detec.Pos.-Standard* est remplacé par celui du composant correspondant (Detec.Acc.-Sur1, Alim.-Standard, ...).

| Nombre de systèmes et coûts | | Longueur minimale des scénarios pour $ER_1$ 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Longueur minimale des scénarios pour $ER_2$ | 1 | 1 système C : 10 | 2 systèmes C : 18, 19 | Pas de système | Pas de système |
| | 2 | 4 systèmes C : 13 à 16 | 1 systèmes C : 20 | 3 systèmes C : 28 à 30 | 8 systèmes C : 36 à 41 |
| | 3 | 2 systèmes C : 19, 20 | 4 systèmes C : 23 à 26 | 10 systèmes C : 31 à 36 | 7 systèmes C : 42 à 46 |
| | 4 | 2 systèmes C : 25, 26 | 3 systèmes C : 29 à 34 | 9 systèmes C : 37 à 42 | 5 systèmes C : 48 à 53 |

TAB. 4.12 – Synthèse des systèmes trouvés de protection de l'incendie

| Nombre de systèmes et coûts | | Longueur minimale des scénarios pour $ER_3$ 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Longueur minimale des scénarios pour $ER_4$ | 1 | 1 système C : 17 | 3 systèmes C : 26 à 31 | 2 systèmes C : 35, 39 | 1 système C : 44 |
| | 2 | 3 systèmes C : 21 à 23 | 4 systèmes C : 34 à 36 | 1 système C : 43 | 1 système C : 52 |
| | 3 | 4 systèmes C : 27 à 33 | 3 système C : 38 à 40 | 5 systèmes C : 47 à 52 | 7 systèmes C : 56 à 61 |
| | 4 | 6 systèmes C : 35 à 42 | 4 systèmes C : 44 à 50 | 7 systèmes C : 53 à 60 | 6 systèmes C : 62 à 68 |

TAB. 4.13 – Synthèse des systèmes trouvés de protection de l'arrimage

## 4.3 Etape d'optimisation

### 4.3.1 Ensembles optimaux obtenus

L'évaluation des arbres de défaillances multiples amélioré par la méthode d'optimisation donne 58 solutions optimales pour le système de protection de l'arrimage et 61 solutions optimales pour le système de protection de l'incendie. Les tables 4.12 et 4.13 synthétise ces solutions par rapport aux événements redoutés respectifs des deux systèmes. Le nombre de solutions ainsi que le coût minimum et maximum sont donnés pour chaque niveau de sûreté de fonctionnement.

Une solution optimale pour le système de protection de l'arrimage est présentée figure 4.9 (a). Cette solution a un coût de 60 unités et la longueur minimale des scénarios redoutés est de 4 pour les événements redoutés $ER_3$ et $ER_4$. C'est à dire que cette architecture est tolérante à 3 modes de défaillances pour chaque événement redouté. Elle utilise deux systèmes de commande en redondance passive. Les systèmes de détection des mouvements transversaux et horizontaux sont utilisés pour détecter l'accélération puis la position du camion sur le wagon. Le premier système de commande utilise :

- un système de mesure du mouvement longitudinal composé d'un détecteur d'accélération standard, d'un détecteur standard de position gauche et d'un détecteur standard de position droite,
- un système de mesure du mouvement transversal composé d'un détecteur d'accélération standard, d'un détecteur standard de position gauche et d'un détecteur standard de position droite,
- un système de traitement composé de deux automates (l'un standard et l'autre sûr type 2) en redondance active avec priorité d'alarme,
- et un système d'alimentation électrique composé d'un bloc standard et d'un bloc d'alimentation sécurisé en redondance passive.

Le second système de commande utilise quant à lui :

- un système de mesure du mouvement longitudinal composé d'un détecteur d'accélération sûr de type 1, d'un détecteur standard de position gauche et d'un détecteur standard de position droite,
- un système de mesure du mouvement transversal composé d'un détecteur d'accélération sûr de type 1, d'un détecteur standard de position gauche et d'un détecteur standard de position droite,
- un système de traitement composé de deux automates (l'un standard et l'autre sûr type 1) en redondance active sans priorité d'alarme,
- et un système d'alimentation électrique composé d'un bloc standard.

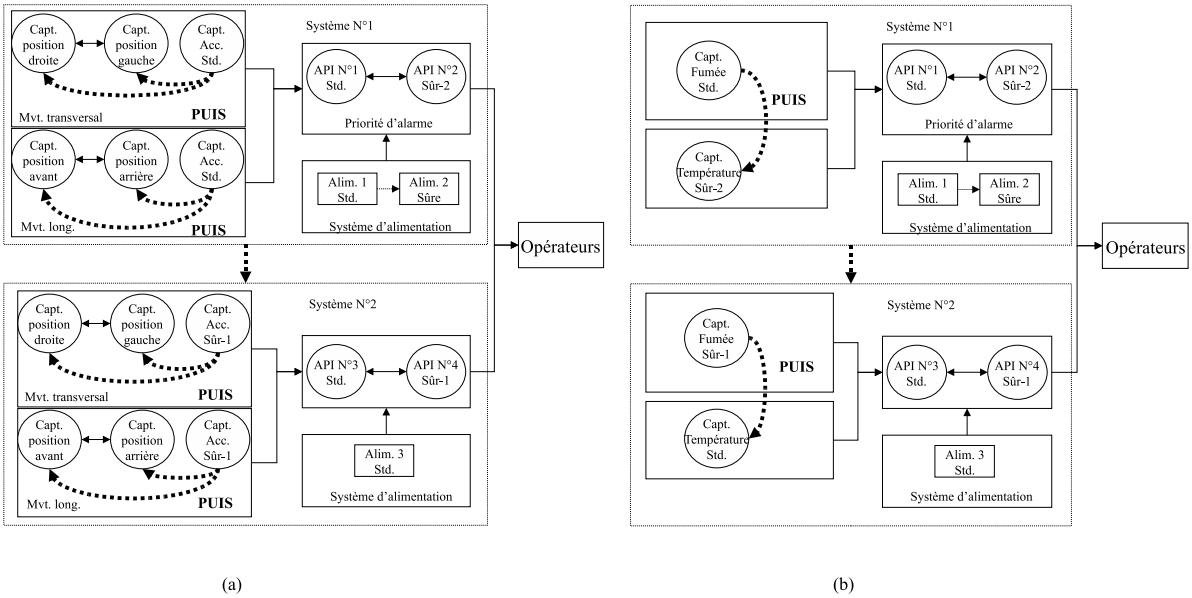


FIG. 4.9 – Architectures opérationnelles comprenant des fonctions temporelles et des composants sûrs

Par ailleurs, une solution optimale pour le système de protection de l'incendie est présentée

figure 4.9 (b). Cette solution a un coût de 48 unités et la longueur minimale des scénarios redoutés est également de 4 pour les événements redoutés $ER_1$ et $ER_2$. Les systèmes de détection de l'incendie sont utilisés pour détecter la fumée puis l'augmentation de température.

### 4.3.2 Comparaison avec une méthode d'évaluation classique de la sûreté de fonctionnement

#### 4.3.2.1 Ensembles optimaux obtenus

Dans cette section, notre méthodologie est comparée avec la méthode d'évaluation basée sur les arbres de défaillances statiques qui est présentée au paragraphe 1.5.2.1. Nous rappelons ici que dans les arbres de défaillances classiques, seuls les opérateurs **AND** et **OR** sont utilisés et que les aspects temporels ne sont pas considérés. L'évaluation des deux arbres de défaillances par la méthode d'optimisation donne 115 solutions optimales pour le système de protection de l'incendie et 103 solutions optimales pour le système de protection de l'arrimage.

#### 4.3.2.2 Différences observées

De ces résultats, nous constatons que les ensembles de solutions issus de l'arbre de défaillance amélioré est plus petit que l'ensemble issu de l'arbre de défaillance classique. En effet, l'intégration des fonctions temporelles permet de prendre en compte des possibilités supplémentaires d'architectures optimisées qui éliminent des possibilités non optimales issues de l'arbre de défaillance classique.
Par ailleurs, la quantification du niveau de sûreté de fonctionnement des solutions obtenues avec notre approche est plus précise en raison d'un nombre de scénarios plus faible pour chaque événement redouté par rapport au nombre de scénarios issus des coupes de l'arbre classique. La table 4.14 présente quelques systèmes issus de la table 4.13. En effet, les opérateurs temporels suppriment les scénarios impossibles du fait de l'architecture choisie contrairement aux coupes de l'arbre de défaillances classique.

| Systèmes ayant une longueur minimale de 4 pour $ER_3$ et $ER_4$ | | | | | |
|---|---|---|---|---|---|
| Coût du système | | 62 | 64 | 66 | 68 |
| Opérateurs temporels | $N_{min}$ pour $ER_3$ | 12 | 12 | 12 | 3 |
| | $N_{min}$ pour $ER_4$ | 18 | 10 | 6 | 10 |
| Opérateurs classiques | $N_{min}$ pour $ER_3$ | 18 | 18 | 18 | 9 |
| | $N_{min}$ pour $ER_4$ | 75 | 30 | 15 | 30 |

TAB. 4.14 – Comparaison entre approches sur des systèmes issus de la table 4.13

Une constatation similaire peut être faite avec les systèmes de protection de l'incendie de la table 4.12 présentés dans la table 4.15.

| Systèmes ayant une longueur minimale de 4 pour $ER_1$ et $ER_2$ | | | | | |
|---|---|---|---|---|---|
| Coût du système | | 48 | 49 | 50 | 53 |
| Opérateurs temporels | $N_{min}$ pour $ER_1$ | 84 | 48 | 48 | 84 |
| | $N_{min}$ pour $ER_2$ | 32 | 32 | 24 | 8 |
| Opérateurs classiques | $N_{min}$ pour $ER_1$ | 180 | 120 | 120 | 180 |
| | $N_{min}$ pour $ER_2$ | 96 | 96 | 48 | 24 |

TAB. 4.15 – Comparaison entre approches sur des systèmes issus de la table 4.12

Par exemple, une solution optimale obtenue avec notre approche présentée figure 4.9 (a) et qui correspond à la solution ayant un coût de 62 unités dans la table 4.14 possède 12 scénarios amenant à l'événement redouté $ER_3$ *Non détection d'un désarrimage* contre 18 scénarios avec l'approche classique. Il y a donc 4 scénarios impossibles pris en compte par les arbres de défaillances classiques. L'un de ces scénarios est représenté de la façon suivante :

$$[Alim_2(P_1),\ Alim_1(P_1),\ Alim_3(P_1)] \Rightarrow ER_3 \tag{4.3}$$

où $Alim_2(P_1)$ à un RRC = 2, $Alim_1(P_1)$ et $Alim_3(P_1)$ ont un RRC = 1.

Ce scénario est impossible car l'alimentation 1 et 2 sont en redondance passive et donc, du fait de cette structure, l'alimentation 2 ne peut avoir son mode de défaillance avant celui de l'alimentation 1. Notre approche, à la différence de l'approche classique permet de prendre en compte ces différences de comportement.

## 4.4 Conception d'un système global de protection

Comme il a été souligné dans le chapitre 2, et bien que notre modélisation permet de prendre en compte les fonctions partagées, l'algorithme d'optimisation ne le permet pas puisqu'il ne s'applique que sous l'hypothèse d'indépendance des fonctions du modèle. Or, si l'on veut regrouper les deux systèmes de protection précédents afin de concevoir un système global de protection, la fonction *Alerter les opérateurs* et ses sous-fonctions seront partagées par les deux sous-systèmes de détection. Comme présenté dans le paragraphe 2.4.2, le modèle fonctionnel présenté figures 4.10 et 4.11 a été conçu afin de retirer cette fonction partagée et permettre l'optimisation du système.
L'objectif est désormais de concevoir un système global de protection. Il s'agit également de voir l'influence de cette conception globale sur le coût et sur le niveau de sûreté de fonctionnement par rapport à une conception séparée des deux systèmes. Pour cela, une comparaison montrera les avantages et les inconvénients de chaque démarche et clôturera ce chapitre.

### 4.4.1 Modélisation du système

**Modèle hiérarchique** Les possibilités d'agencement, les modes de défaillances des composants et les missions du système sont toujours les mêmes par rapport à la démarche précédente. Le modèle hiérarchique est présenté figures 4.10 et 4.11.

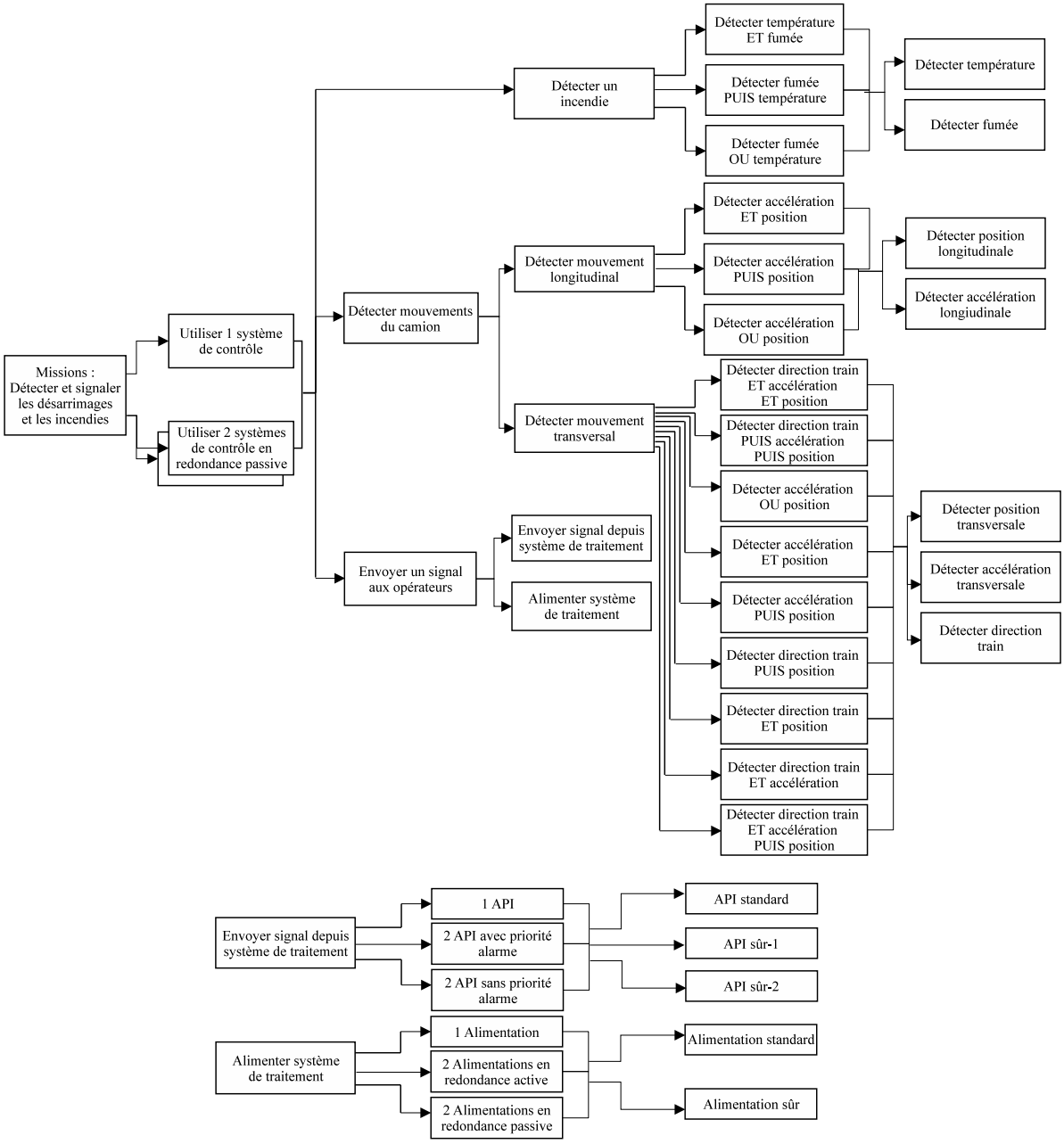


FIG. 4.10 – A. Modèle hiérarchique du système global de protection

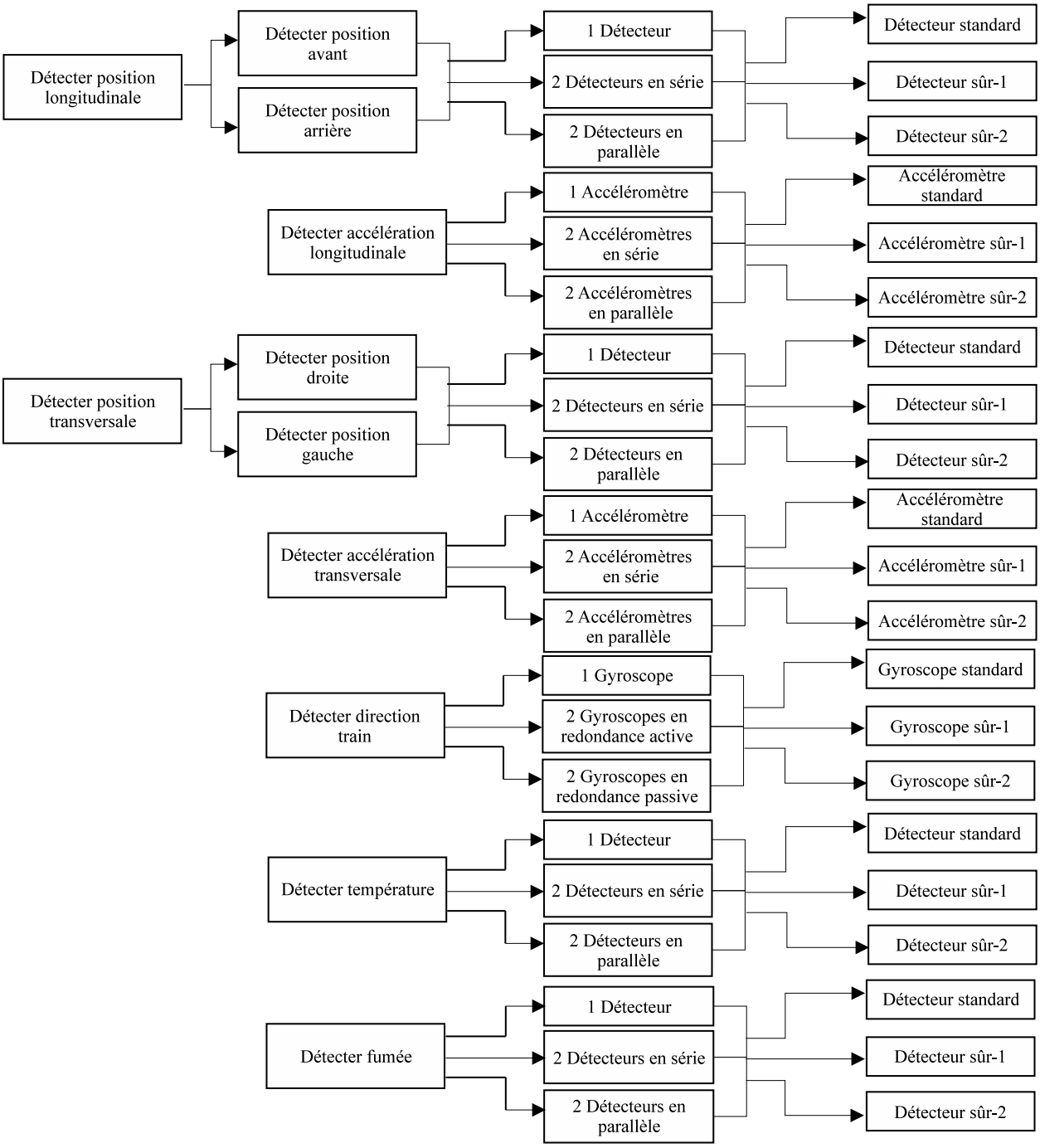


FIG. 4.11 – B. Modèle hiérarchique du système global de protection

**Modèle dysfonctionnel** De la même façon que pour le modèle hiérarchique, nous avons modélisé un unique arbre de défaillances dont la structure est présentée figures 4.12 et 4.13. Afin de conserver la lisibilité du mémoire, nous avons placé l'ensemble des données de cet arbre dans les tableaux H.1, H.2, H.3, H.4 et H.5 en annexe H.

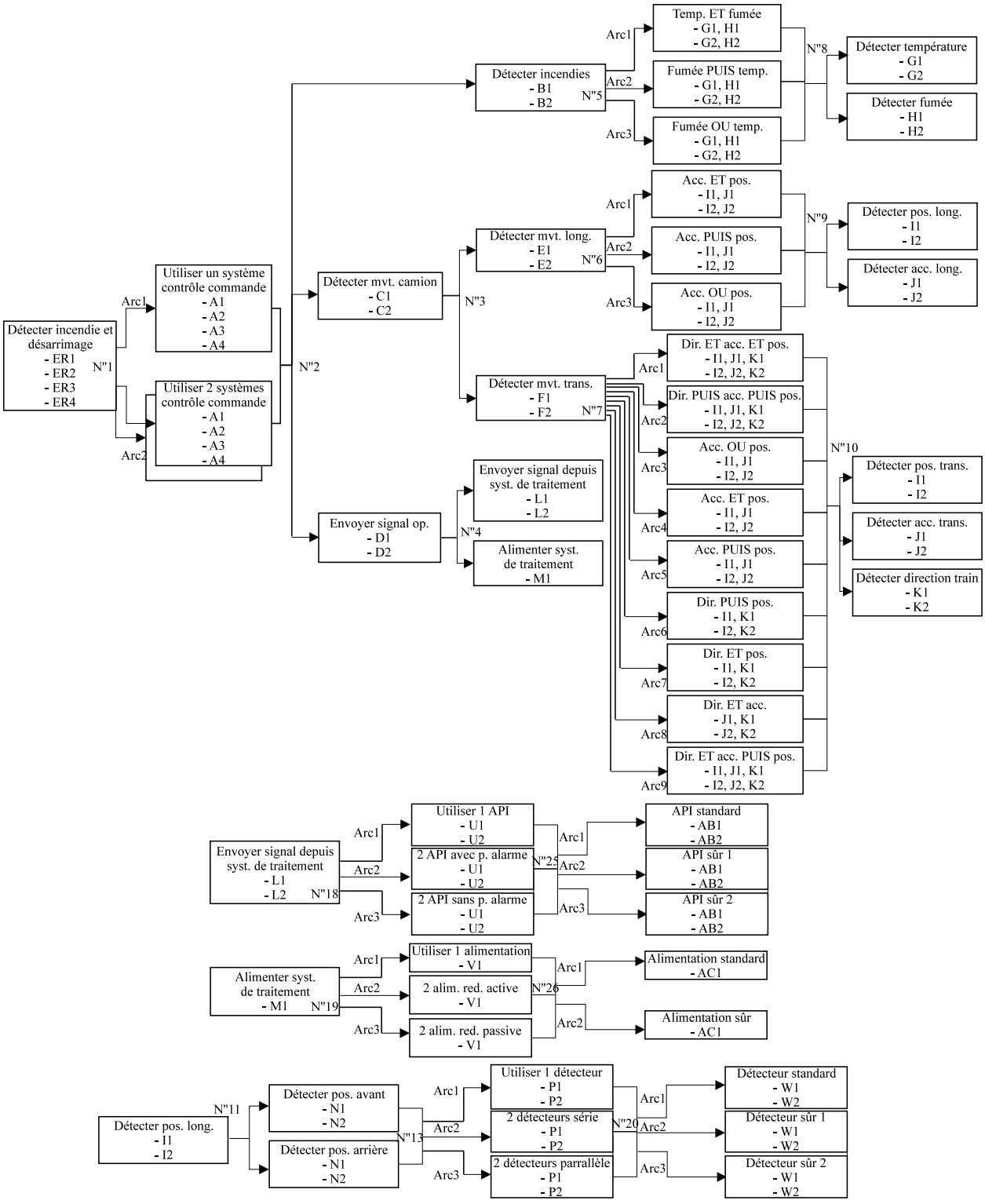


FIG. 4.12 – A. Arbre de défaillances multiples amélioré du système global de protection

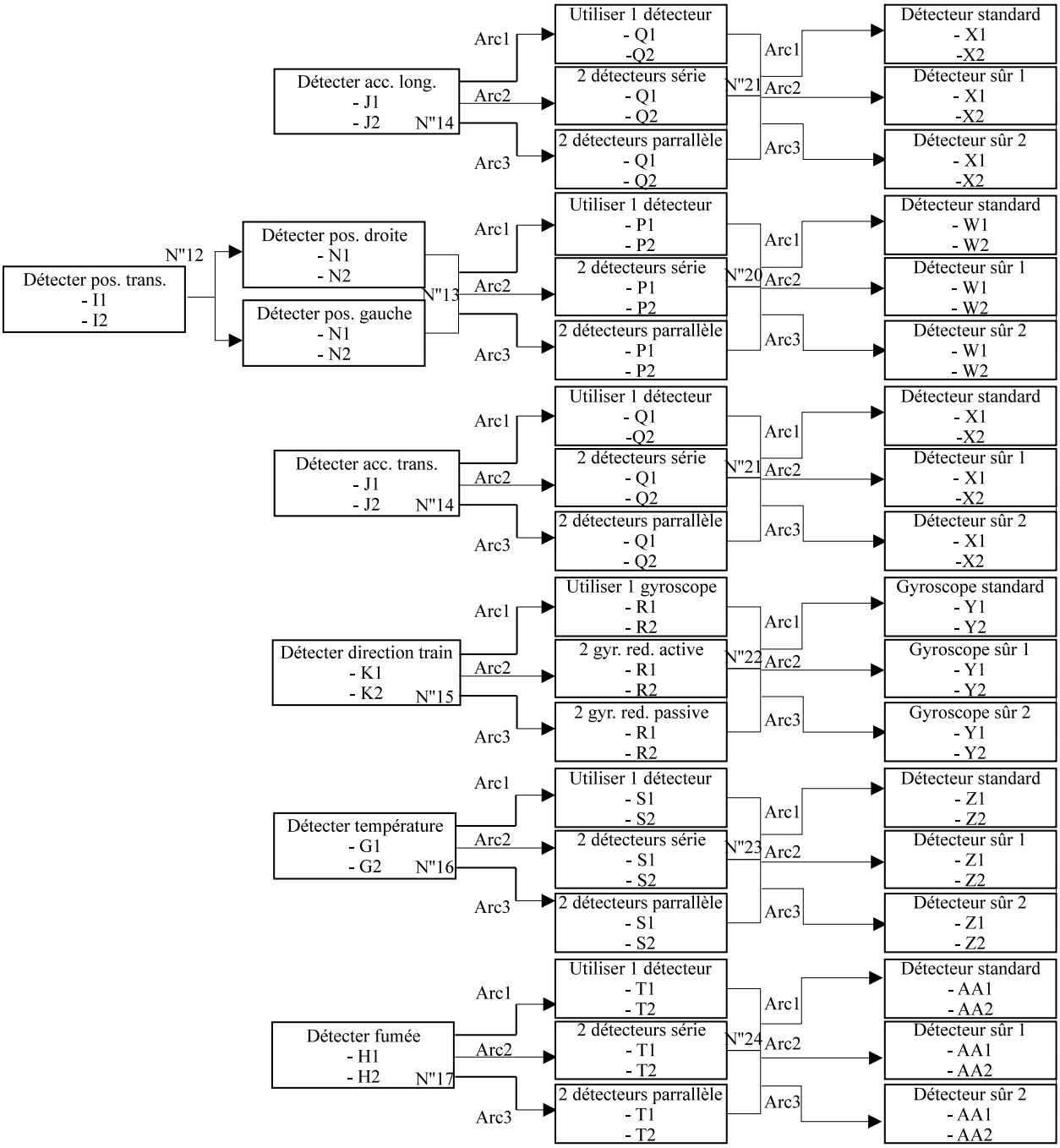


FIG. 4.13 – B. Arbre de défaillances multiples amélioré du système global de protection

## 4.4.2 Résultats de l'étape d'optimisation

L'évaluation de l'arbre de défaillances multiples amélioré par la méthode d'optimisation donne 196 solutions optimales pour le système global de protection incendie-arrimage. Pour rappel, nous avions trouvé 58 solutions optimales pour le système de protection de l'arri-

mage et 61 solutions optimales pour le système de protection de l'incendie soit 119 solutions optimales en tout pour les deux systèmes indépendants. Les solutions supplémentaires sont le résultat de l'augmentation du nombre de composants utilisables pour la conception du système global par rapport aux deux conceptions précédentes. Ainsi, cette augmentation implique un ensemble de combinaisons possibles plus important. La table 4.16 synthétise ces solutions par rapport aux quatre événements redoutés considérés. Le nombre de solutions ainsi que le coût minimum et maximum sont donnés pour chaque niveau de sûreté de fonctionnement.

Ainsi, pour chaque solution de cet ensemble optimal, nous retrouvons au sein de chaque solution, les caractéristiques des deux systèmes pris séparément. Par exemple, le système représenté 4.14 ayant une longueur minimale ($L_{min}$) égale à 4 pour les quatre événements redoutés est le rassemblement des solutions optimales présentées figure 4.9. Ces deux solutions indépendantes ont un coût total de 108 unités et l'utilisation des fonctions partagées permet d'obtenir *a priori* un système équivalent du point de vue de la sûreté de fonctionnement ayant un coût de 66 unités.

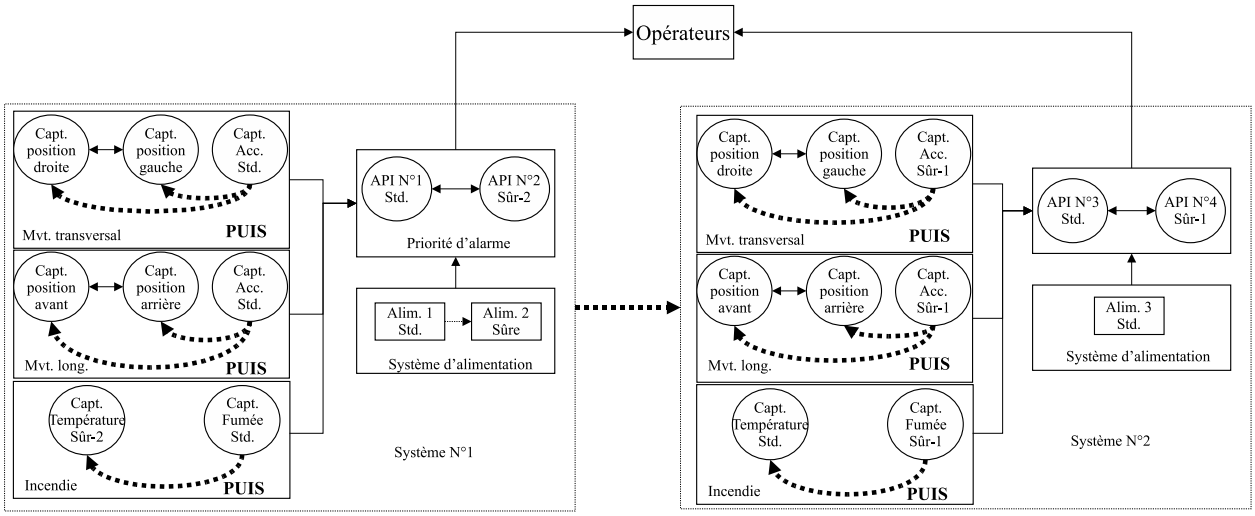


FIG. 4.14 – Exemple d'architecture obtenue pour le système global de protection

**Influence sur le coût financier du système** Nous déduisons immédiatement que la conception du système global permet de diminuer le coût financier du système. Ce gain financier correspondant aux coûts liés au retrait de 4 API et de 3 blocs d'alimentation dans notre exemple. Cependant, le regroupement des unités de traitement et d'alimentation a une influence sur le niveau de sûreté de fonctionnement global qui n'est pas discernable avec nos résultats actuels. Nous allons déterminer cette influence dans le paragraphe suivant.

| $L_{min}$ des scénarios pour | | | | Nombre de systèmes | Coût Max-Min |
|---|---|---|---|---|---|
| $ER_1$ | $ER_3$ | $ER_2$ | $ER_4$ | | |
| 1 | 1 | 1 | 1 | 1 | 18 |
| 1 | 1 | 2 | 2 | 12 | 21 à 26 |
| 1 | 1 | 2 | 3 | 3 | 27 à 28 |
| 1 | 1 | 2 | 4 | 3 | 33 à 34 |
| 1 | 1 | 3 | 2 | 1 | 28 |
| 1 | 1 | 3 | 3 | 7 | 29 à 34 |
| 1 | 1 | 3 | 4 | 4 | 35 à 38 |
| 1 | 1 | 4 | 2 | 1 | 37 |
| 1 | 1 | 4 | 3 | 1 | 38 |
| 1 | 1 | 4 | 4 | 11 | 39 à 46 |
| 2 | 2 | 1 | 1 | 8 | 26 à 34 |
| 2 | 2 | 2 | 2 | 9 | 36 à 38 |
| 2 | 2 | 3 | 3 | 12 | 39 à 44 |
| 2 | 2 | 3 | 4 | 3 | 45 à 46 |
| 2 | 2 | 4 | 3 | 1 | 46 |
| 2 | 2 | 4 | 4 | 7 | 47 à 52 |
| 3 | 2 | 1 | 1 | 1 | 36 |
| 3 | 3 | 1 | 1 | 4 | 37 à 43 |
| 3 | 3 | 2 | 2 | 3 | 44 à 46 |
| 3 | 3 | 3 | 3 | 27 | 47 à 52 |
| 3 | 3 | 3 | 4 | 4 | 53 à 54 |
| 3 | 3 | 4 | 3 | 1 | 54 |
| 3 | 3 | 4 | 4 | 13 | 55 à 60 |
| 4 | 2 | 1 | 1 | 1 | 46 |
| 4 | 3 | 1 | 1 | 1 | 47 |
| 4 | 3 | 3 | 3 | 1 | 57 |
| 4 | 3 | 3 | 4 | 1 | 63 |
| 4 | 3 | 4 | 3 | 1 | 64 |
| 4 | 3 | 4 | 4 | 1 | 65 |
| 4 | 4 | 1 | 1 | 2 | 48, 49 |
| 4 | 4 | 2 | 2 | 9 | 52 à 57 |
| 4 | 4 | 3 | 3 | 24 | 58 à 63 |
| 4 | 4 | 3 | 4 | 4 | 64 à 65 |
| 4 | 4 | 4 | 3 | 1 | 65 |
| 4 | 4 | 4 | 4 | 13 | 66 à 71 |

TAB. 4.16 – Synthèse des systèmes globaux de protection

**Influence sur le niveau de sûreté de fonctionnement** Afin de déterminer cette influence sur le niveau de sûreté de fonctionnement, nous examinons les solutions obtenues suivant les deux critères suivants qui tiennent compte des événements redoutés définis dans

le paragraphe 4.2.5.1 :

- C1 : Longueur minimale des scénarios entraînant un événement redouté pour chaque système de protection simultanément. Ce critère signifie que les deux systèmes de protection du système global sont défaillants au même instant. Ce critère rend compte directement d'une défaillance due à une ressource commune.
- C2 : Longueur minimale des scénarios entraînant un événement redouté pour chaque système de protection de manière successive. Ce critère informe que les deux systèmes sont défaillants mais selon le scénario suivant : le premier système de protection devient défaillant puis le second système l'est à son tour.

La table 4.17 synthétise ces solutions par rapport aux deux critères précédents. Pour chaque solution est indiqué le niveau de sûreté de fonctionnement obtenu ainsi que le sous-système mis en cause.

| Systèmes répondant au critère C1 | | Systèmes répondant au critère C2 | |
|---|---|---|---|
| $L_{min}$ des scénarios | Nombre de systèmes | $L_{min}$ des scénarios | Nombre de systèmes |
| 1 | 61 | 1 | 0 |
| 2 | 45 | 2 | 0 |
| 3 | 77 | 3 | 0 |
| 4 | 13 | 4 | 0 |

TAB. 4.17 – Synthèse des systèmes montrant l'influence de la conception globale sur le niveau de sûreté de fonctionnement

De cette table, nous constatons que l'ensemble des systèmes obtenus répondent au critère C1. La seule différence étant dans la tolérance aux fautes de ces systèmes à la défaillance due à la ressource commune.

Ainsi, le regroupement des sous-systèmes de traitement et d'alimentation entraîne une perte simultanée des deux systèmes de protection dès que le scénario minimal est atteint pour ce sous-système. Par exemple, la perte du système d'alimentation et/ou la perte du système de traitement du système global entraîne la perte simultanée des deux systèmes de protection de la figure 4.14, ce qui n'est pas le cas pour deux systèmes indépendants, le second système de protection pouvant continuer à remplir ses missions après la défaillance du système de traitement-alimentation du premier. Ainsi, la conception du système global de protection permet une diminution des coûts d'une architecture en regroupant les ressources mais entraîne également une diminution du niveau de sûreté de fonctionnement global par l'ajout de dépendances dysfonctionnelles entraînant des défaillances dues à une ressource commune.

## 4.5 Conclusion

Ce quatrième chapitre a permis de mettre en oeuvre, pour le wagon intelligent, notre approche méthodologique de conception tenant compte des scénarios.

La première partie s'est concentrée sur la modélisation et l'optimisation des deux systèmes de protection selon une approche indépendante. D'après les caractéristiques à accomplir par les deux systèmes de protection décrits dans le modèle hiérarchique (missions, fonctions, composants, agencements possibles) le comportement dysfonctionnel de ces systèmes basé sur l'arbre de défaillances multiples amélioré a été décrit. L'analyse des résultats issus de ces modèles a permis d'effectuer une comparaison avec les résultats issus d'un arbre de défaillance classique. Cette comparaison a montré clairement que les solutions optimales obtenues étaient mieux évaluées que les solutions obtenues par une analyse classique du fait de l'utilisation des scénarios à la place de coupes.

La dernière partie du chapitre a consisté à modéliser un système de protection selon une approche globale, c'est-à-dire par regroupement des ressources communes (tout en conservant l'indépendance des fonctions du modèle) entre les deux systèmes de protection. Les résultats obtenus ont permis de conclure sur les avantages et les inconvénients de l'approche globale par rapport à l'approche indépendante. En effet, bien que le coût financier des solutions obtenues a été diminué, le niveau de sûreté de fonctionnement global a également diminué du fait de l'introduction de défaillances de ressources communes. Nos résultats doivent être améliorés par l'intégration des défaillances de ressources communes dans notre modèle dysfonctionnel. Cette intégration nous permettra de distinguer ces défaillances particulières des autres défaillances. Ce dernier point fait partie des perspectives de nos recherches.

# Conclusion générale

Les dernières décennies ont vu apparaître de nouvelles méthodes théoriques et outils fonctionnels de modélisation et d'analyse de la sûreté de fonctionnement. La multiplication et l'introduction d'outils et de méthodes de conception ne peut être effectuée que si l'on se soucie de leur cohérence dans une démarche méthodologique définie et structurée.
Ainsi, le premier objectif des travaux présentés dans ce mémoire a consisté à identifier les éléments permettant de proposer une démarche cohérente méthodique de conception de systèmes au regard de ce constat : un formalisme de modélisation fonctionnelle, un modèle comportemental, une analyse algorithmique de ces modèles et une évaluation du niveau de sûreté de fonctionnement d'architectures matérielles.

Il s'agissait également de prendre en considération le domaine d'application de ces travaux de recherche : les transports guidés. La mission d'un système de transport guidé consiste à assurer le déplacement de passagers ou de marchandises d'un lieu donné à un autre, selon un temps de parcours établi et selon des conditions de sécurité optimales. Pour le ferroutage, cette mission s'inscrit dans le contexte actuel d'avoir des solutions alternatives au "tout routier" offrant des performances, une intermodalité et une souplesse de transport similaire tout en assurant un niveau de sécurité maximum. C'est dans cette optique que nous avons proposé le concept du wagon intelligent doté de fonctions additionnelles. Cependant, le caractère innovant de ce wagon et le principe de transport du véhicule routier non conçu au départ pour être transporté sur le train ajoute des contraintes et des besoins sécuritaires importants. Ainsi, les systèmes d'automatisation introduits sur le wagon, utilisant des technologies avancées et de nombreuses fonctions nouvelles, doivent être conçus et analysés pour garantir un système de ferroutage sûr et performant. Les travaux de recherche présentés dans ce mémoire de thèse ont pris pour défi de proposer une architecture fonctionnelle complète du wagon intelligent compte tenu des particularités techniques du ferroutage puis de concevoir deux de ses fonctions additionnelles : le système de protection contre les incendies et le système de protection contre le désarrimage du véhicule routier.

Le dernier point considéré dans ces travaux traite du domaine de la sûreté de fonctionnement. De nombreuses méthodes d'analyse existent et s'appliquent dans différents secteurs industriels. Bien que les principes fondamentaux de construction d'un modèle dysfonctionnel et d'analyse quantitative soient relativement simples, il n'en demeure pas moins que la complexité sans cesse accrue des systèmes d'automatisation rend de plus en plus délicate l'évaluation de la sûreté de fonctionnement de ces systèmes : nombre de composants et de fonctions importantes, interactions entre composants, dépendances fonctionnelles et temporelles entre défaillances, ... De même, cette complexité impose de modéliser le comportement dysfonctionnel du système de manière plus précise afin de connaître les événements redoutés les plus probables. Dans cet objectif, l'utilisation des scénarios de modes de défaillances permet d'évaluer ce comportement dysfonctionnel très précisément.
Les méthodes d'analyses classiques comme les arbres de défaillances pour lesquels un événement redouté est la conséquence d'une combinaison statique de défaillances sont limitées si l'on veut prendre en compte ces scénarios. Cependant, ces méthodes, basées sur la logique combinatoire offrent au concepteur un support graphique facilement compréhensible par tous.
Les méthodes de simulation basées sur les graphes de Markov répondent à ces besoins mais sont fortement contraintes par des hypothèses lourdes. Les problèmes d'explosion combinatoire constituent également un frein à son exploitation. Enfin, les méthodes comme les arbres de défaillances dynamiques combinent les avantages graphiques des méthodes classiques et ceux des méthodes de simulation. Cependant, ces méthodes débouchent sur des analyses utilisant des approches markoviennes et sont utilisées dans le but d'analyser de grands systèmes existants et non pour les concevoir, c'est-à-dire rechercher parmi un ensemble de solutions possibles, la solution présentant le meilleur compromis du cahier des charges du concepteur.

La méthodologie proposée tente d'exploiter les avantages de ces méthodes et d'en contourner leurs limites. Nous en rappelons les principaux concepts :

- La méthodologie est décomposée en **deux étapes** : une étape de modélisation du système et une étape d'optimisation et de recherche des systèmes optimaux.
- La méthodologie exploite deux **formalismes graphiques** : un modèle fonctionnel hiérarchique et un modèle dysfonctionnel basé sur les arbres de défaillances baptisé *arbre de défaillances multiples amélioré*.
- Les **possibilités d'agencements** des composants dans une architecture matérielle sont représentées à l'aide de plusieurs types de noeuds : un noeud associatif, un noeud alternatif et un noeud élémentaire.
- L'emploi de coefficients de fiabilité relatifs (RRC) associés à des modes de défaillances permet de définir **plusieurs types de composants** ayant des fiabilités différentes tels

que des composants standard ou sécuritaires.
- Les **événements redoutés** du système sont déterminés suivant une démarche déductive en associant à chaque noeud de l'arbre de défaillances des relations entre modes de défaillances composées d'opérateurs temporels : **AND**, **OR**, **PAND** et **SEQ**.
- L'arbre de défaillances multiples détermine le niveau de sûreté de fonctionnement de chaque système possible en **évaluant la longueur des scénarios** de cette possibilité et **le nombre de combinaisons possibles de ces scénarios**.
- La recherche des solutions optimales est faite à chaque niveau de l'arbre de défaillances par l'adaptation à notre formalisme de l'algorithme d'optimisation du type **Branch and Bound**.
- La méthodologie fournit un **ensemble de solutions optimales possibles** caractérisées par un coût financier et un niveau de sûreté de fonctionnement permettant au concepteur de choisir le système correspondant le mieux à ses besoins. Par ailleurs, l'architecture matérielle de chaque solution obtenue est décrite : composants, agencements et types utilisés.

Ainsi, la philosophie générale de notre méthodologie est basée sur l'utilisation des scénarios pour évaluer le niveau de sûreté de fonctionnement d'un ensemble d'architectures matérielles possibles décrits dans un modèle graphique. De plus l'utilisation des modes de défaillances et des opérateurs temporels au sein de cette modélisation permet de décrire précisément le comportement dysfonctionnel du système. La connaissance du système ne s'en trouve alors qu'améliorée. Par ailleurs, la comparaison avec une méthode d'évaluation classique a mis en évidence le gain de précision de notre approche dans l'évaluation du niveau de sûreté de fonctionnement des systèmes.

Soulignons néanmoins que le traitement des fonctions partagées et des dépendances associées n'est possible dans l'état actuel de développement de notre méthodologie que grâce à une modification du modèle. Une amélioration de la méthode d'optimisation dans ce sens ainsi que la modélisation des défaillances de ressources communes dans le modèle comportemental constituent les perspectives à court et moyen terme de ces travaux. Par ailleurs, la prise en compte de ces améliorations dans l'atelier logiciel ALoCSyS que nous avons réalisé constitue une pérennisation de cette méthodologie. Les perspectives s'orientent aussi sur la possibilité d'optimiser de grands systèmes sans imposer des contraintes permettant de réduire l'espace des solutions. Enfin, la conception de nouvelles fonctions du wagon intelligent comme la protection contre les décrochages, la détection de problèmes mécaniques au niveau du bogie ou encore les fonctions de communication (wagon-camion, wagon-locomotive, wagon-infrastructure) constituent des perspectives à long terme.

Pour terminer, le développement de systèmes de transport guidés de plus en plus com-

plexes et critiques vis-à-vis de la disponibilité et de la sécurité confortera incontestablement la nécessité de disposer d'une méthodologie de conception dans laquelle le domaine de la sûreté de fonctionnement à une place importante. A travers ce mémoire, nous avons contribué à ce développement.

# Glossaire

**AdD** Arbres de défaillances

**AEIF** Association Européenne pour l'Interopérabilité Ferroviaire

**AFNOR** Association France de Normalisation

**ALoCSyS** Atelier Logiciel de Conception de Systèmes Sûrs

**API** Automate Programmable Industriel

**BDD** Binary Decision Diagram

**BDMP** Boolean Logic Driven Markov Processes

**CEM** Compatibilité Electro Magnétique

**CERTIFER** Agence de Certification Ferroviaire

**Ferroutage** Technique consistant à mettre sur des wagons de chemin de fer spécialisés des camions complets et/ou des semi-remorques pour effectuer un voyage sur plusieurs centaines de kilomètres. Cette technique est également appelée transport combiné accompagné

**EPSF** Etablissement Public de Sécurité Ferroviaire

**ERA** European Railway Agency. Agence Ferroviaire Européenne (ex-AEIF)

**ERTMS** European Railway Traffic Management System

**FMDS** Fiabilité Maintenabilité Disponibilité Sécurité

**Gerbage** Terme désignant l'opération de chargement dans le milieu ferroviaire et maritime. Pour le ferroviaire, cette opération consiste à superposer des conteneurs sur des wagons construits à cet effet en vue de leur transport sur des lignes où le gabarit en hauteur est suffisamment dégagé. Dans le cadre du ferroutage, ce gabarit est le UIC GB1.

**GSM-R** Global System for Mobile communications - Railways. Système de téléphonie mobile pour les trains

**INRETS** Institut National de Recherche sur les Transports et leur Sécurité

**ISO** International Organization for Standardization. Fédération Mondiale d'organisations nationales de normalisations.

**LAGIS** Laboratoire d'Automatique, Génie Informatique et Signal

**RRC** Relative Reliability Coefficient. Coefficient de fiabilité relatif.

**STI** Spécifications Techniques d'Interopérabilité Européennes. Ces spécifications se présentent sous forme de normes et regroupent les solutions techniques permettant l'intéropérabilité du réseau ferroviaire européen. Les STI sont issues des directives européennes et se classent en deux familles : la grande vitesse et le rail conventionnel

**Transport combiné** Terme désignant soit un mode de transport bimodal (route et rail par exemple) ou un mode de transport multimodal (rail, route, mer par exemple). Le conditionnement des marchandises par ce mode de transport se fait en conteneurs maritimes ou en caisses mobiles pour la terre, on distingue le transport combiné accompagné du transport combiné non accompagné

**UIC** Union Internationale des Chemins de Fer

# Bibliographie


[AFN96] *AFNOR NF-Z 68-901, Génie automatique. Représentation des systèmes de contrôle et de commande des systèmes automatisés de production.* 1996.

[AFN04] AFNOR : *NF X50-151, Management par la valeur et ses outils, analyse fonctionnelle, analyse de la valeur, conception à objectif désigné.* Editions AFNOR, 2004.

[AGG+06] M. Aumas, B. Giraud, B. Gouillon, W. Héraud, H. Jacoby, G. Marie et J. P. Nail : *Transport routier de marchandises. Vigilant à l'arrêt comme au volant.* Institut National de Recherche et de Sécurité (INRS), Brochure ED826, 2006.

[AHS01] S. Attouche, S. Hayat et M. Staroswieki : An efficient algorithm for the design of fault tolerant multi-sensor systems. *In Proceedings of the 40th IEEE Conference on Decision and Control (CDC01)*, 2001.

[Aka96] J. Akaichi : *Systèmes automatisés de Production à Intelligence Distribuée, des stratégies de répartition basées sur une approche de classification.* Thèse de doctorat, Université des Sciences et Technologies de Lille (USTL), 1996.

[Amo99a] L. Amodeo : *Contribution à la simplification et à la commande des réseaux de Petri stochastiques. Application aux systèmes de production.* Thèse de doctorat, UFR des Sciences et Techniques de l'Université de Franche-Comté, 1999.

[Amo99b] G. A. Amoussou : *Modélisation fonctionnelle dans la conception et la reconception des systèmes industriels.* Thèse de doctorat, UTC, 1999.

[Arl95] J. Arlat : Informatique sûre de fonctionnement : défis et solutions. *In Sûreté des procédés industriels : journées CNRS-CRIN du 11 octobre*, 1995.

[Arr04] *Arrêté du 1er Juillet 2004 relatif aux exigences applicables aux matériels roulants circulant sur le réseau ferré national.* Journal Officiel de la République Française du 6 Aout 2004 n°181, 2004.

[Aub87] J. F. Aubry : *Conception des systèmes de commande numériques des convertisseurs électromécaniques : vers une méthodologie intégrant la sûreté de fonctionnement.* Thèse de doctorat, Institut National Polytechnique de Lorraine, 1987.

[Aum92] M. Aumas : *Arrimage des charges sur les véhicules routiers*. Institut National de Recherche et de Sécurité (INRS), Document ED 759, 1992.

[BB03] M. Bouissou et J. L. Bon : A new formalism that combines advantages of fault trees and markov models : Boolean logic driven markov processes. *Reliability Engineering and System Safety, Eselvier Editions*, N°82:Pages 149–163, 2003.

[BCCR05] M. Bayart, B. Conrard, A. Chovin et M. Robert : Capteurs et actionneurs intelligents. *Techniques de l'ingénieur*, S7-520, 2005.

[BCR05] V. Benard, L. Cauffriez et D. Renaux : The safe-sadt method for aiding designers to choose and improve dependable architectures for complex automated systems. *Reliability Engineering and System Safety, Elsevier Editions*, N°93-2:179–196, 2005.

[BD04] M. Bouissou et Y. Dutuit : Reliability analysis of a dynamic phased mission system. *In MMR2004 congress, Santa Fe*, 2004.

[Beu06] J. Beugin : *Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé*. Thèse de doctorat, Université de Valenciennes et du Hainaut-Cambresis (UVHC), 2006.

[Boe88] B. W. Boehm : A spiral model of software development and enhancement. *IEEE Computer*, N°21-5:Pages 61–72, 1988.

[Bou97] A. Bouras : *Contribution à la conception d'architectures réparties : modèles génériques et interopérabilité d'instruments intelligents*. Thèse de doctorat, Thèse de doctorat de l'université des sciences et technologies de Lille, 1997.

[Bre00] B. Bretesche : *La méthode APTE, analyse de la valeur, analyse fonctionnelle*. Pretrelle Ed., ISBN 2-84440-019-1, 2000.

[BST99] BST : Collision contre un passage supérieur routier survenue le 13 aout 1997 près de bedell (ontario), train numéro cp 121-13. Rapport technique, Rapport numéro R97H0008 du BST (Bureau Sécurité et Transport du Canada) "http ://www.tsb.gc.ca/fr/reports/rail/1997/r97h0008/r97h0008.asp", 1999.

[Buc99] P. Buchholz : An adaptative aggregation/disaggregation algorithm for hierarchical markovian models. *European Journal of Operational Research*, N°116: Pages 545–564, 1999.

[Byt79] C. W. Bytheway : The creative aspects of fast diagramming. *Safe Proceedings*, N°6:pages 301–312, 1979.

[Cab99] E. Cabeau : *Introduction à la conception de la sûreté*. Cahier technique Schneider Electric n°144, 1999.

[Cal90] J. P. Calvez : *Spécification et conception des systèmes : une méthodologie*. Editions Masson, ISBN 2-225-82107-0, 1990.

[Car02] *CargoSpeed veut concurrencer le Modalohr jusqu'au principe.* Transports & Technologies, N°34, 2002.

[Car04] *Cargo Speed demonstrated.* Railway Gazette International, 01 Sept. 04, 2004.

[CB06a] B. Conrard et M. Bayart : Conception d'architectures de commande distribuées par une évaluation semi-quantitative de la sûreté de fonctionnement. *In 15ème congrès de Maitrise des Risques et de Sûreté de fonctionnement, Lambda-Mu, Lille, 9-13 Octobre*, 2006.

[CB06b] B. Conrard et M. Bayart : Design of dependable control system thanks to a semi-quantitative optimisation. *Proceedings of Safety and Reliability for Managing Risk (ESREL 06)*, Estoril, 18-22 september:pages 1583–1589, 2006.

[CCB07] B. Conrard, V. Cocquempot et M. Bayart : Design of automation systems with criterion of cost and dependability. *In Qualita 2007 congress, Tanger, Maroc, 20-22 Mars*, 2007.

[CCCB04] L. Cauffriez, J. Ciccotelli, B. Conrard et M. Bayart : Design of intelligent distributed systems : a dependability point of view. *Reliability Engineering and System Safety, Eselvier Editions*, Vol. 84:Pages 19–32, 2004.

[CD95] L. Cauffriez et J. Defrenne : Viabilité de l'information et réseau à diffusion : deux atouts pour la prise de décision dans un système réparti de contrôle commande tolérant les fautes. *Revue européenne de sûreté de fonctionnement et de diagnostic, Editions Hermes*, N°5-2:Pages 219–247, 1995.

[CEN00] CENELEC : *NF EN 50126, Applications ferroviaires : spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS).* CENELEC, Comité Européen de Normalisation Electrotechnique. Fontenay aux roses, France, UTE, Union Technique de l'Electricité et de la communication, 2000.

[CEN01] CENELEC : *NF EN 50128, Applications ferroviaires : logiciels pour systèmes de commande et de protection ferroviaire.* CENELEC, Comité Européen de Normalisation Electrotechnique. Fontenay aux roses, France, UTE, Union Technique de l'Electricité et de la communication, 2001.

[CEN03] CENELEC : *NF EN 50129, Applications ferroviaires : systèmes électroniques de sécurité pour la signalisation.* CENELEC, Comité Européen de Normalisation Electrotechnique. Fontenay aux roses, France, UTE, Union Technique de l'Electricité et de la communication, 2003.

[CHCC06a] J. Clarhaut, S. Hayat, B. Conrard et V. Cocquempot : Conception de systèmes intelligents sûrs de fonctionnement : application au ferroutage. *In Communiquer, Naviguer, Surveiller. Innovations pour des transports plus sûrs,*

*plus eficaces et plus attractifs. Actes INRETS n°109, ISBN 978-2-85782-642-2, pages 153-164*, 2006.

[CHCC06b] J. Clarhaut, S. Hayat, B. Conrard et V. Cocquempot : Safety intelligent system conception for piggyback service. *IEEE ICIT International Conference on Industrial Technology, ISBN 1-4244-0726-5*, N°6:pages 1659–1664, 2006.

[CHCC07a] J. Clarhaut, S. Hayat, B. Conrard et V. Cocquempot : Contribution à la conception de systèmes sûrs de fonctionnement appliqués aux wagons de ferroutage. *In Communiquer, naviguer surveiller. Innovations pour des transports plus sûrs, plus efficaces et plus attractifs, Actes INRETS n°112, ISBN 978-2-85782-654-5, pages 55-68*, 2007.

[CHCC07b] J. Clarhaut, S. Hayat, B. Conrard et V. Cocquempot : Safety system conception by using a semi-quantitative reliability evaluation application. application to a railroad transportation system. *Proceedings of international conference on Industrial Engineering and Systems Management (IESM 2007), ISBN 978-7-302-15312-2, Tsinghua University Press, Pekin, Chine*, pages 330–331, 2007.

[CHCC08a] J. Clarhaut, S. Hayat, B. Conrard et V. Cocquempot : Méthodologie de conception d'architectures de systèmes sécuritaires pour le ferroutage basée sur des séquences de défaillances ordonnées dans le temps et des arbres e défaillances multiples. *In Actes du Workshop Surveillance, Sûreté et Sécurité des Grands Systèmes (3SGS), Université de Technologie de Troyes, 4-5 juin*, 2008.

[CHCC08b] J. Clarhaut, S. Hayat, B. Conrard et V. Cocquempot : Méthodologie de conception de systèmes sûrs et économiques utilisant les scénarios de défaillances. *In Actes du 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement (Lambda Mu 16), N°8B3, pages 1-8, ISBN 2-35147-008-7, 6-10 Octobre, Avignon, France*, 2008.

[CHCC08c] J. Clarhaut, S. Hayat, B. Conrard et V. Cocquempot : Optimal design of control systems using a dependability criteria and temporal sequences evaluation application to a railroad transportation system. *In Proceedings of ESREL 2008 and the 17th SRA-Europe Conference, Vol. 4, pages 3199-3208, ISBN 978-0-415-48513-5, 22-25 septembre, Valencia, Espagne*, 2008.

[CHCC09] J. Clarhaut, S. Hayat, B. Conrard et V. Cocquempot : Optimal design of dependable control system architectures using temporal sequences of failures. *Version révisée envoyée à IEEE Transactions on Reliability*, 2009.

[Cho00] C. Choukair : *Contribution à la conception d'architectures opérationnelles validées*. Thèse de doctorat, Thèse de doctorat de l'université de Lille 1, 2000.

[CIA09] *Les réseaux de terrain : Critères de sûreté de fonctionnement, sous la direction du CIAME.* Traité systèmes automatisés, IC2, Hermes, Paris, ISBN : 2-7462-1946-8, 2009.

[CM02] M. Cepin et B. Mavko : A dynamic fault tree. *Reliability Engineering and System Safety, Eselvier Editions*, N°75:Pages 83–91, 2002.

[CSD00] D. Coppit, K. J. Sullivan et J. B. Dugan : Formal semantics for computational engineering : A case study n dynamic fault trees. *In 11th International Symposium on Software Reliability Engineering (ISSRE'00)*, 2000.

[CTR05] B. Conrard, J. M. Thiriet et M. Robert : Distributed system design on dependability evaluation : a case study on a pilot thermal process. *Reliability Engineering and System Safety, Eselvier Editions*, N°88:Pages 109–119, 2005.

[DBB92] J. B. Dugan, S. J. Bavuso et M.A. Boyd : Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Transactions on Reliability*, Vol. 41-3:pages 363–377, 1992.

[Des03] J. P. Desmoulins : Aperçu du système intégré r-shift-r. *Colloque options techniques pour le transport des marchandises à travèrs l'Arc Alpin, Archamps, Haute Savoie, ISSN : 0151-0304*, N°1:Pages 42–44, 2003.

[DIA90] Distributed intelligent actuators and sensors, project information. Rapport technique, ESPRIT PROJECT 2172, 1990.

[Die04] A. D. Dietz : *Optimisation multicritères pour la conception d'ateliers discontinus multiproduits : aspects économique et environnemental.* Thèse de doctorat, Thèse de doctorat de l'Institut National Polytechnique de Toulouse, N°ordre 2177, 2004.

[Dir04a] *Directive 2004/49/CE sur la sécurité des chemins de fer communautaires.* Parlement et Conseil Européens, Journal Officiel de l'Union Européenne, 2004.

[Dir04b] *Directive 2004/50/CE modifiant la directive 96/48/CE du conseil relative à l'interopérabilité du système ferroviaire transeuropéen à grande vitesse et la directive 2001/16/CE du parlement du Conseil relative à l'interopérabilité du système ferroviaire transeuropéen conventionnel.* Parlement et Conseil Européens, Journal Officiel de l'Union Européenne, 2004.

[DM02] J. P. Desmoulins et A. Margery : R-shift-r, un nouveau système de ferroutage - présentation du système. Rapport technique, http ://www.r-shift-r.com, 2002.

[DPP06] A. D'Ariano, D. Pacciarelli et M. Pranzo : A branch and bound algorithm for scheduling trains in a railway network. *European Journal of Operational Research, Science Direct Ed.*, N°183-2:pages 643–657, 2006.

[Dug01] J. B. Dugan : Fault tree analysis of computer-based systems. *In Annual Reliability and Maintainability Symposium*, 2001.

[ECAY03] A. Elegbede, C. Chu, K. Adjallah et F. Yalaoui : Reliability allocation through cost minimization. *IEEE Transactions on reliability*, N°52-1:pages 106–111, 2003.

[Eur97] Eurotunnel : *Inquiry into the fire on Heavy Goods Vehicle shuttle 7539 on 18 November 1996*. Eurotunnel, The Stationery Office. ISBN 0-11-551931-9, 1997.

[Gar98] R. Garnier : *Une méthode efficace d'accélération de la simulation des réseaux de Petri stochastiques*. Thèse de doctorat, Université de Bordeaux 1, 1998.

[Gro02] M. Grout : *Instrumentation industrielle, spécification et installation des capteurs et des vannes de régulation*. Dunod, Paris, ISBN 2-10-005731-6, 2002.

[Gru99] L. Grudzien : *Contribution à l'intégration de la sûreté de fonctionnement au sein d'une démarche de conception multimétiers*. Thèse de doctorat, Université de Valenciennes et du Hainaut Cambrésis (UVHC), 1999.

[Har08] M. Harmim : Atelier logiciel de conception de systèmes sûrs de fonctionnement. Rapport technique, Rapport de stage de master 2 effectué à l'INRETS-Villeneuve d'Ascq, Université d'Evry Val d'Essonne, ISRN : INRETS/RE-08-729-FR, 2008.

[HLA+07] R. Husson, C. Lung, J. F. Aubry, J. Daafouz et D. Wolf : *Automatique : du cahier des charges à la réalisation de systèmes*. Sciences Sup., Dunod Ed., ISBN : 978-2-10-050397-1, 2007.

[HMSBC98] H. Hadj-Mabrouk, A. Stuparu et D. Bied-Charreton : *Exemple de typologie d'accidents dans le domaine des transports guidés*. Revue générale des chemins de fer, Numéro de Mars, pages 17-55, 1998.

[Hod91] R. Hodgson : The x-model : a process model for object-oriented softwar development. *In Proc. of Le génie logiciel et ses applications, Toulouse*, 1991.

[Hol99] E. Hollnagel : Accident and barriers. *In 7th European Conference on Cognitive Science Approaches to Process Control*, pages 175–180, Villeneuve d'Ascq, France, 1999.

[HP87] D. Hatley et I. Pirbhai : *Strategies for Real Time System specifications*. John Wiley & Sons, ISBN : 978-093263304, 1987.

[ID01] J. A. Incera Dieguez : *Contribution à la modélisation et à la simulation accélérée de réseaux de communication*. Thèse de doctorat, Université de Rennes 1, 2001.

[IEC00] *IEC 61508, Functionnal Safety of electrical/electroni/programmable electronic safety-related systems.* IEC 61508-1 to 7, Geneva, Switzerland, IEC, International Electrotechnical Commission, 2000.

[IEC03] IEC : *60300-3-1 Dependability management. Part 3-1 : Application guide, Analysis techniques for dependability - guide on methodology.* International Electrotechnical Commission, Switzerland, Geneva, ISBN 2-8318-6791-6, 2003.

[IGL89] *IGL Technology, SADT : un langage pour communiquer.* Eyrolles, Paris, ISBN 2212081855, 1989.

[JAG01] D. Jampi, J. F. Aubry et E. Guilhem : Conception et sûreté de fonctionnement : deux activités indissociables. *In Congrès Francophone MOSIM 2001, Troyes*, 2001.

[KGC75] A. Kaufmann, G. Grouchko et R. Cruon : *Modèles mathématiques pour l'étude de fiabilité des systèmes.* Editions Massion et Cie, Paris, ISBN 2225403155, 1975.

[KH96] H. Kumamoto et E. J. Henley : *Probabilistic risk assessment and management for engineers and scientists.* IEEE Press, New York, ISBN 0-780-31004-7, 1996.

[KPTH01] W. Kuo, V. Prassad, F. Tillman et C. Hwang : *Optimal reliability design, fundamentals and applications.* Cambridge University Press, ISBN : 978-0521031912, 2001.

[KS03] C. Kerhen et S. Seguin : Evaluation qualitative de systèmes physiques pour la sûreté de fonctionnement. *In Formalisation des activités concurrentes (FAC03), Toulouse, France*, 2003.

[LAB+95] J.C Laprie, J. Arlat, J.P. Blanquart, A. Costes, Y. Crouzet, Deswarte Y., J.C. Fabre, H. Guillermain, K. Kanoun, C. Mazet, D. Powell, C. Rabéja et P. Thévenod : *Guide de la sûreté de fonctionnement.* Laboratoire d'Ingénierie de la Sûreté de fonctionnement, Toulouse, France, Cépaduès-Editions, ISBN 2-85428-382-1, 1995.

[LK02] P. E. Labeau et C. Kermisch : Approche dynamique de la fiabilité des systèmes. Rapport technique, Rapport MNFD 2002-07, Service de Métrologie Nucléaire, Université Libre de Bruxelles, 2002.

[Lor05] L. Lorimier : *La caractérisation dynamique des défaillances. Une nouvelle approche pour la gestion active des défaillances au sein des systèmes physiques industriels complexes.* Thèse de doctorat, Université des Sciences et Technologies de Lille (USTL), 2005.

[Lut97] D. Luttenbacher : *Modélisation du concept capteur intelligent par une approche orientée objet : application à un capteur intelligent de température*. Thèse de doctorat, Doctorat de l'Université Henri Poincaré, Nancy 1, 1997.

[Lyo00] P. Lyonnet : *La maintenance : Mathématiques et Méthodes*. 4ème Edition, Tec&Doc Editions, ISBN : 2-7430-0419-3, 2000.

[MBCC06] S. Maza, M. Bayart, B. Conrard et V. Cocquempot : On the dependability design of complex systems. *In Proc. of the 30 EsreDa'06, Reliability of Safety Critical System, SINTEF, Trondheim, Norway*, 2006.

[MDCS98] R. Manian, J. B. Dugan, D. Coppit et K. J. Sullivan : Combining various techniques for dynamic fault tree analysis of computer systems. *In Proceedings of International Symposium on High Assurance System Engineering*, 1998.

[MES94] MESR : Impact de l'émergence des réseaux de terrain et de l'instrumentation intelligent dans la conception des systèmes d'automatisation de processus. Rapport technique, Rapport final du projet MESR 2033, Ministère de l'enseignement supérieur et de la recherche, chapitre sûreté de fonctionnement, pages 39-44 et 87-90, 1994.

[Mon98] G. Moncelet : *Dependability evaluation of mecatronic automative systems using Petri Nets*. Thèse de doctorat, Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS (LAAS), 1998.

[Mor01] Y. Mortureux : La sûreté de fonctionnement, méthodes pour maîtriser les risques. Rapport technique, Techniques de l'ingénieur, AG4670, 2001.

[MTA06] A. Mkhida, J. M. Thiriet et J. F. Aubry : Effet de la variation des données de fiabilité sur le niveau de sécurité d'une boucle de sécurité intelligente. *In 6ème conférence de Modélisation et Simulation - MOSIM06 - 3-5 Avril, Maroc*, 2006.

[OMG07] *OMG, Unified Modeling language Specification, Version 2.1.1*. http ://www.omg.org, 2007.

[Par96] V. Pareto : *Cours d'économie politique*. Rouge, Lausanne, Switzerland, 1896.

[PB96] G. Pahl et W. Beitz : *Engineering design - A systematic Approach*. Springer-Verlag, Londres, 2ème edition, ISBN :1-846-283-183, 1996.

[Pet07] J. F. Petin : *Méthodes et modèles pour un processus sûr d'automatisation*. Thèse de doctorat, Habilitation à Diriger des Recherches de l'Université Henry Poincaré, Nancy, 2007.

[PRZ92] *Norme expérimentale, PRZ 68-901, représentation des systèmes de contrôle et de commande des systèmes automatisés, Projet : génie automatique*. 1992.

[PZB03] G. Prudhomme, P. Zwolinski et D. Brissaud : Integrating into the design process the needs of those involved in the product life cycle. *Journal of Engineering design*, N°14-3:pages 333–343, 2003.

[QL03] L. Quintian et P. Lahire : Vers une meilleure intégration des composants sur l'étagère. *In OCM03*, 2003.

[RH04] M. Rausand et A. Hoyland : *System Reliability Theory : Models, Statistical Methods and Applications*. Wiley, 2nd Edition, ISBN : 978-0471471332, 2004.

[Rob61] L. Robichaud : *Graphes de fluence*. Editions Eyrolles, Presses de l'Université Laval, ISBN 110015243, 1961.

[Roy70] W. W. Royce : Managing the development of large software systems. *In Proc. Westcon, California, USA*, 1970.

[Rum95] J. Rumbaugh : *OMT : Modélisation et conception orientées objet*. Prentice Hall, ISBN : 978-2225846847, 1995.

[SACH06] R. Schoenig, J. F. Aubry, T. Cambois et T. Hutinet : An aggregation method of markov graps for the reliability analysis of hybrid system. *Reliability Engineering and System Safety, Elsevier Editions*, N°91:pages 137–148, 2006.

[Sai02] *Project SAIL 10277, Deliverable 7 : SAIL Final Report*. European Union, Issue : 1a/2002-07-25, Document : Sail-Deliv7-1a, 2002.

[SB94] M. Staroswieki et M. Bayart : *Actionneurs intelligents*. Hermes, ISBN : 2-86601-439-1, 1994.

[SB96a] C. Sourisse et L. Boudillon : *La sécurité des machines automatisées*. Collection Technique, Groupe Schneider France, ISBN 2-907314-29-7, 1996.

[SB96b] M. Staroswieki et M. Bayart : Models and languages for the interoperability of smart instruments. *Automatica*, N°32-6:Pages 859–873, 1996.

[SC02a] M. J. M. Sompayrac et R. Claraco : *Brevet Resorail de l'exploitation ferroviaire en boucles de desserte*. Institut National de la propriété industrielle, Paris, N°2-817-526, 2002.

[SC02b] M. J. M. Sompayrac et R. Claraco : *Brevet Resorail du wagon porte-camions*. Institut National de la Propriété industrielle, Paris, N°2-816-570, 2002.

[Sch02] H. Schabe : The safety philosophy behind the cenelec railway standards. *In ESREL 2002, European safety and reliability conference, Lyon*, 2002.

[Sch04] R. Schoenig : *Définition d'une méthodologie de conception de systèmes mécatroniques sûrs de fonctionnement*. Thèse de doctorat, Thèse de l'Institut Polytechnique de Lorraine, 2004.

[SL02] R. Schoenig et A. Leblond : Méthodologie outillée d'aide à la conception des systèmes embarqués sûrs de fonctionnement. *In Lambda Mu 13, Pages 1-9*, 2002.

[SLTBS95] F. Simonot-Lion, J. P. Thomesse, M. Bayart et M. Staroswieki : Dependable distributed computer control systems : analysis of the design step activities. *13th IFAC Workshop on Distributed Control Systems, Toulouse, Sharaoui AEK Ed.*, pages pages 119–124, 1995.

[SS99] S. Swaminathan et C. Smidts : The mathematical formulation for the event sequence diagram framework. *Reliability Engineering and System Safety, Elsevier Editions*, N°65:pages 103–118, 1999.

[STI06a] STI : *Spécification Technique d'Interopérabilité concernant le sous système Applications télématiques au service du fret du système ferroviaire transeuropéen conventionnel.* Journal Officiel de l'Union Européenne, L13, 2006.

[STI06b] STI : *Spécification Technique d'Interopérabilité concernant le sous système Contrôle Commande et Signalisation du système ferroviaire transeuropéen conventionnel.* Journal Officiel de l'Union Européenne, L284, 2006.

[STI06c] STI : *Spécification Technique d'Interopérabilité concernant le sous système Exploitation et Gestion du trafic du système ferroviaire transeuropéen conventionnel.* Journal Officiel de l'Union Européenne, L359, 2006.

[STI06d] STI : *Spécification Technique d'Interopérabilité concernant le sous système Matériel Roulant - Bruit du système ferroviaire transeuropéen conventionnel.* Journal Officiel de l'Union Européenne, L37, 2006.

[STI06e] STI : *Spécification Technique d'Interopérabilité concernant le sous système Matériel roulant - wagons pour le fret du système ferroviaire transeuropéen conventionnel.* Journal Officiel de l'Union Européenne, L344, 2006.

[Tho04] J. P. Thomesse : Réseaux locaux industriels - concepts, typologie, caractéristiques. Rapport technique, Techniques de l'ingénieur, S7574, 2004.

[Tit92] L. Tittel : *LZ 129 Hindenburg.* Schriften zur Geschichte der Zeppelin-Luftshiffahrt, 1992.

[TRC83] H. Tardieu, A. Rochfeld et R. Colleti : *La méthode MERISE - Tome 1 Principe et Outils.* Editions d'organisation, ISBN 2-7081-1106-X, 1983.

[VGRH81] W.E. Vesely, F.F. Goldberg, N.H. Roberts et D.F. Haasl : Fault tree handbook. Rapport technique, U.S. Nuclear Regulatory Commission, ISBN : 978-0160055829, Washington, USA, 1981.

[Vil88] A. Villemeur : *Sûreté de fonctionnement des systèmes industriels.* Collection de la Direction des Etudes et Recherches d'Electricité de France, Eyrolles Editions, ISBN 2-212-01615-8, 1988.

[Väl01] T. Välisalo : Dependability management in mobile work machines. *In Qualita 2001*, pages pages 200–201, 2001.

[Zie96] C. Ziegler : *Sûreté de fonctionnement d'architectures informatiques embarquées sur automobile*. Thèse de doctorat, Institut National Polytechnique de Toulouse, 1996.

[Zwi99] G. Zwingelstein : Sûreté de fonctionnement des systèmes industriels complexes. Rapport technique, Techniques de l'ingénieur, Traité Informatique Industriel, S-8250, 1999.

# Annexe A

# Démonstrations des lois de composition du paragraphe 2.2.2

Pour chaque démonstration, considérons A, B et C, trois événements redoutés, tels que C est le résultat de l'association de A et de B avec l'un des opérateurs (AND, PAND ou SEQ). $\Delta_A$, $\Delta_B$ et $\Delta_C$ sont les ensembles de scénarios minimaux associés à A, B et C. Nous prenons pour hypothèse que les événements redoutés A et B sont indépendants, c'est-à-dire qu'une défaillance ne peut pas apparaître simultanément dans A et B.

## A.1 Lois de composition de l'opérateur AND

L'opérateur AND représente le cas où l'occurrence de C se produit après l'occurrence de A et de B. Les paramètres correspondants $L^C_{min}$ et $N^C_{min}$ peuvent être déterminés grâce au nombre de permutations entre 2 séquences de longueurs respectives $L^A_{min}$ et $L^B_{min}$, noté $R^{L^A_{min},L^B_{min}}_{L^C_{min}}$, et grâce au nombre de combinaisons entre les scénarios des deux ensembles $\Delta_A$ et $\Delta_B$.
Ainsi, l'ensemble $\Delta_C$ peut être caractérisé par les relations suivantes :

$$L^C_{min} = L^A_{min} + L^B_{min} \tag{A.1}$$

$$N^C_{min} = R^{L^A_{min},L^B_{min}}_{L^C_{min}} \times N^A_{min} \times N^B_{min},\ avec\ R^{L^A_{min},L^B_{min}}_{L^C_{min}} = \frac{L^C_{min}!}{L^B_{min}! \times L^A_{min}!} \tag{A.2}$$

## A.2 Lois de composition de l'opérateur PAND

L'opérateur PAND est un opérateur temporel qui représente le cas où l'occurrence de C se produit après les occurrences successives de A puis de B. De la même façon que pour l'opérateur AND, $L^C_{min}$ et $N^C_{min}$ peuvent être déterminés grâce au nombre de permutations

entre 2 séquences de longueurs respectives $L^A_{min}$ et $L^B_{min}$, noté $R^{L^A_{min},L^B_{min}}_{L^C_{min}}$, et grâce au nombre de combinaisons entre les scénarios des deux ensembles $\Delta_A$ et $\Delta_B$. Cependant, afin de prendre en compte les occurrences successives de A puis de B, cet opérateur impose une contrainte sur le premier mode de défaillance de l'ensemble $\Delta_A$ telle que la permutation de ce mode de défaillance ne soit pas possible.
Ainsi $N^C_{min}$ peut être déterminé grâce au nombre de permutations possibles entre 2 séquences de longueurs respectives $L^A_{min} - 1$ et $L^B_{min}$ tout en conservant une longueur finale pour les scénarios de l'ensemble $\Delta_C$ égale à $L^C_{min} = L^A_{min} + L^B_{min}$. De ce fait, l'ensemble $\Delta_C$ peut être caractérisé par les relations suivantes :

$$L^C_{min} = L^A_{min} + L^B_{min} \tag{A.3}$$

$$N^C_{min} = R^{(L^A_{min}-1),L^B_{min}}_{(L^A_{min}-1)+L^B_{min}} \times N^A_{min} \times N^B_{min},\ avec\ R^{(L^A_{min}-1),L^B_{min}}_{(L^A_{min}-1)+L^B_{min}} = \frac{((L^A_{min}-1)+L^B_{min})!}{(L^A_{min}-1)! \times L^B_{min}!} \tag{A.4}$$

## A.3 Lois de composition de l'opérateur SEQ

L'opérateur SEQ, comme l'opérateur PAND, représente le cas où l'occurrence de C se produit après les occurrences successives de A puis de B. Cependant, l'opérateur SEQ impose qu'aucune défaillance amenant le système vers l'événement redouté B ne peut se produire avant l'occurrence de l'ensemble des défaillances amenant à l'événement redouté A. Dans la théorie des ensembles, cet opérateur correspond à un produit cartésien entre les ensembles $\Delta_A$ et $\Delta_B$ dont le résultat est l'ensemble $\Delta_C$.
Ainsi $L^C_{min}$ et $N^C_{min}$ peuvent être déterminés grâce au nombre de combinaisons entre les scénarios de longueurs respectives $L^A_{min}$ et $L^B_{min}$ des deux ensembles $\Delta_A$ et $\Delta_B$. De ce fait, l'ensemble $\Delta_C$ peut être caractérisé par les relations suivantes :

$$L^C_{min} = L^A_{min} + L^B_{min} \tag{A.5}$$

$$N^C_{min} = N^A_{min} \times N^B_{min} \tag{A.6}$$

# Annexe B

# Démonstration RRC-Probabilités

Dans cette annexe, nous montrons que l'inégalité $RRC^{\psi_1} < RRC^{\psi_2}$ implique que la probabilité d'occurrence de la séquence $\psi_1$ est supérieure à celle de $\psi_2$ sous certaines hypothèses peu restrictives.
Tout d'abord, pour un intervalle de temps donné, la probabilité d'occurrence d'une séquence $\psi$ est donnée par la relation B.2 pour laquelle on considère que chaque faute $F_i$ de cette séquence $\psi$ a la probabilité d'occurrence suivante :

$$P(F_i) = \overline{R}(t) = (\overline{R}_{ref}(t))^{RRC^{F_i}} \tag{B.1}$$

$$P(\psi) = \frac{\prod(\overline{R}_{ref}(t))^{RRC^{F_i}}}{card(\psi)!} \tag{B.2}$$

Par ailleurs, les valeurs des RRC affectées aux différents modes de défaillance sont des valeurs discrètes choisies par le concepteur. Ainsi, pour 2 valeurs distinctes de RCC, un pas minimum est employé, noté $\Delta_{RRC}$.
Ainsi :

$$RRC^{\psi_1} < RRC^{\psi_2} \Longleftrightarrow RRC^{\psi_2} - RRC^{\psi_1} \geq \Delta_{RRC} \tag{B.3}$$

d'où :

$$RRC^{\psi_1} < RRC^{\psi_2} \Longleftrightarrow (\overline{R}_{ref}(t))^{RRC^{\psi_2} - RRC^{\psi_1}} \leq (\overline{R}_{ref}(t))^{\Delta_{RRC}} \tag{B.4}$$

puisque $\overline{R}_{ref}(t) \in ]0, 1[$

Si la condition B.5 est satisfaite, on obtient de ceci la relation B.8. Cette hypothèse s'appuie sur le fait que $\overline{R}_{ref}(t)$ est petit et que les séquences de fautes étudiées sont d'une longueur maximale connue, notée lg (généralement de l'ordre de 2, 3 ou 4).

$$(\overline{R}_{ref}(t))^{\Delta_{RRC}} < \frac{1}{lg!} \tag{B.5}$$

or puisque :

$$1 \leq card(\psi_1) \leq lg \; et \; 1 \leq card(\psi_2) \leq lg \tag{B.6}$$

on obtient :

$$(\overline{R}_{ref}(t))^{\Delta_{RRC}} < \frac{1}{lg!} \leq \frac{card(\psi_2)!}{card(\psi_1)!} \tag{B.7}$$

ainsi :

$$(\overline{R}_{ref}(t))^{RRC^{\psi_2} - RRC^{\psi_1}} \leq (\overline{R}_{ref}(t))^{\Delta_{RRC}} \leq \frac{card(\psi_2)!}{card(\psi_1)!} \tag{B.8}$$

d'où :

$$\frac{(\overline{R}_{ref}(t))^{RRC^{\psi_2}}}{card(\psi_2)!} < \frac{(\overline{R}_{ref}(t))^{RRC^{\psi_1}}}{card(\psi_1)!} \tag{B.9}$$

soit, au final :

$$RRC^{\psi_2} > RRC^{\psi_1} \Longrightarrow P(\psi_2) < P(\psi_1) \tag{B.10}$$

# Annexe C

# Plate-forme informatique de conception ALoCSyS

## C.1 Interface graphique JAVA

La fenêtre d'accueil d'ALoCSyS présentée figure C.1 est également la fenêtre principale qui sert à lancer les autres sous-fenêtres du logiciel. Cette fenêtre principale est composée de 5 menus :

- Menu *Fichier* qui permet de créer un nouveau modèle, de sauvegarder ses données et de quitter ALoCSyS.
- Menu *Saisie* qui permet de saisir les données du modèle (composants, fonctions, sous-fonctions et modes de défaillances), les noeuds et les relations entre modes de défaillances.
- Menu *Visualiser* qui permet d'afficher l'arbre, le fichier C++ du moteur de calculs, la liste des résultats et les architectures optimales obtenues.
- Menu *Calculer* qui lance le moteur de calculs.
- Menu *?* qui est le menu d'aide.


FIG. C.1 – Vue d'écran de l'interface d'accueil d'ALoCSyS

La figure C.2 présente la fenêtre de saisie des données du modèle qui se décompose en trois onglets :

- Un onglet *composant* pour la saisie des paramètres des composants.
- Un onglet *Fonctions* pour la saisie des paramètres des fonctions.
- Un onglet *Affichage* qui liste les données précédemment saisies pour vérification.

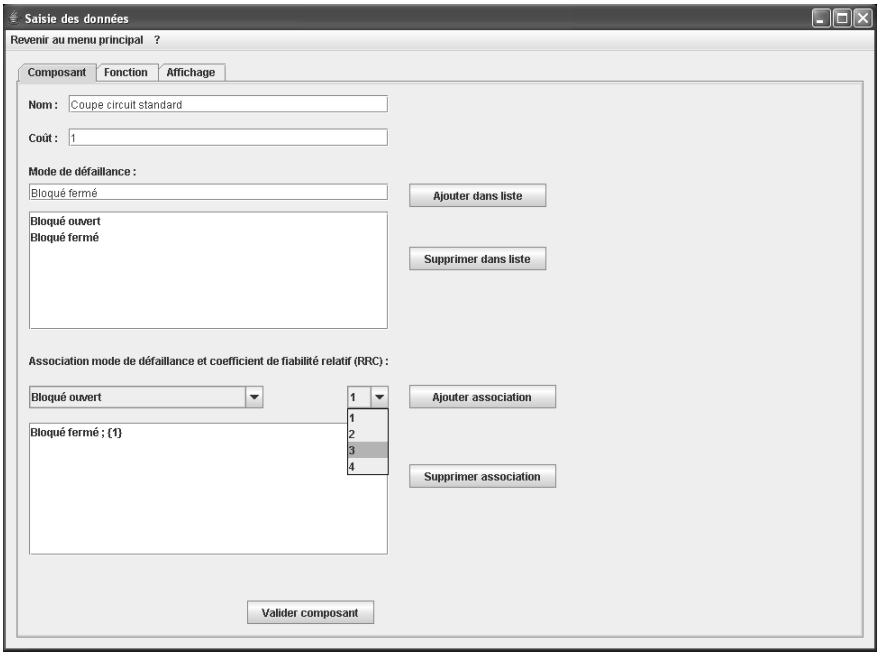


FIG. C.2 – Vue d'écran de l'interface de saisie des données

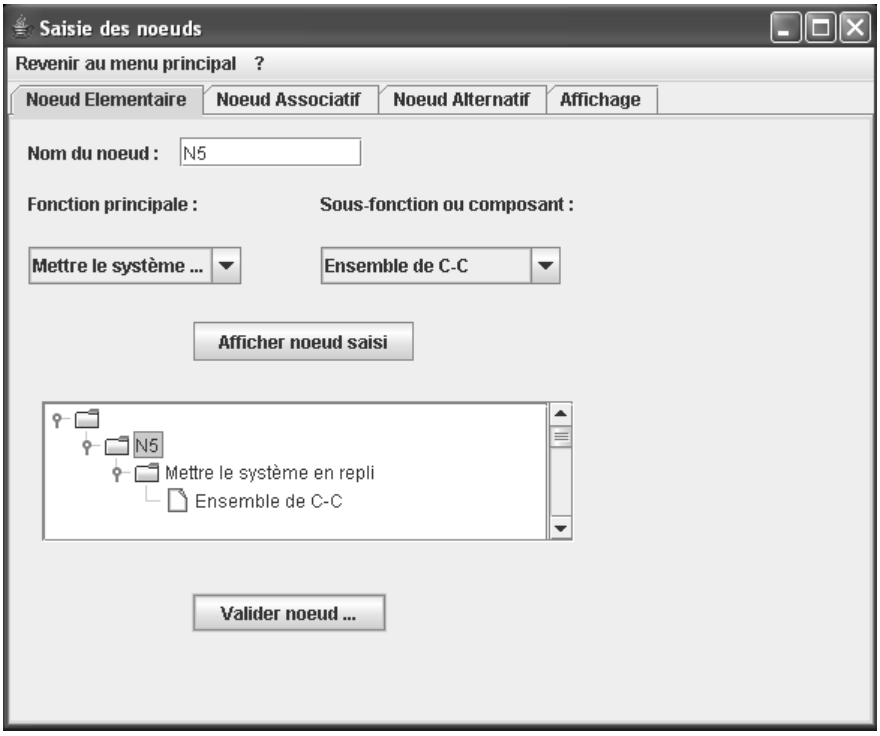


FIG. C.3 – Vue d'écran de l'interface de saisie des noeuds

La figure C.3 présente la fenêtre de saisie des noeuds du modèle qui se décompose en quatre onglets correspondant aux différents types de noeuds :

- Un onglet *noeud élémentaire*.
- Un onglet *noeud alternatif*.
- Un onglet *noeud associatif*.
- Un onglet *Affichage* qui liste les données précédemment saisies pour vérification.

La figure C.4 présente la fenêtre d'affichage du modèle du système hydraulique.

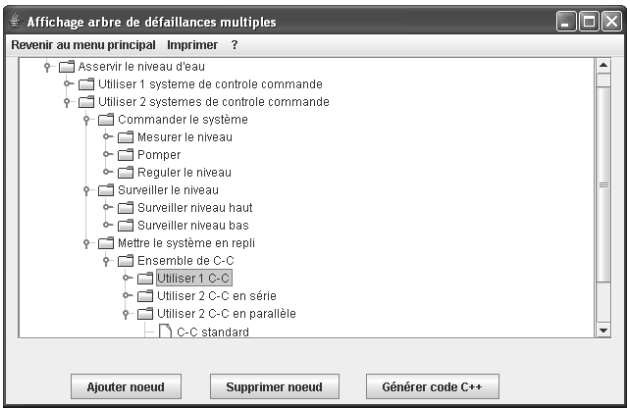


FIG. C.4 – Vue d'écran de l'interface d'affichage du modèle

La figure C.5 présente la fenêtre d'affichage du listing de résultats obtenus après calcul pour le système hydraulique.

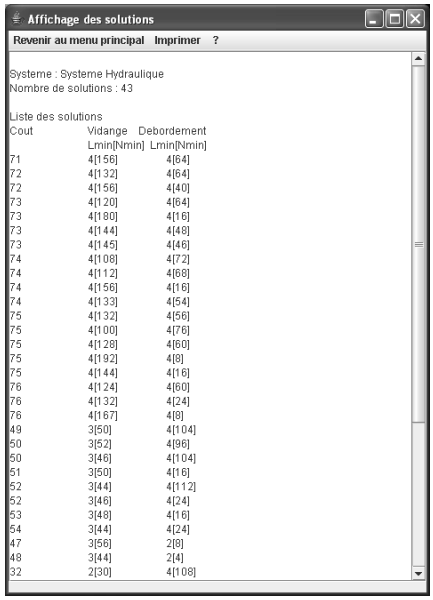


FIG. C.5 – Vue d'écran de l'interface d'affichage du listing de résultats

## C.2 Correspondance noeud / code C++

Cette annexe présente un exemple de code C++ pour les trois types de noeuds.

### Noeud Alternatif

Ce code décrit un noeud alternatif associé à la fonction "Utiliser 1 détecteur" et comprenant trois arcs :

- un détecteur standard,
- un détecteur sûr type 1,
- un détecteur sûr type 2.

```
NoeudAlternatif *N14 = new NoeudAlternatif("Utiliser 1 detecteur");
        N14->addAlternative(DetecteurStd);
        N14->addAlternative(DetecteurSur1);
        N14->addAlternative(DetecteurSur2);
```

### Noeud Associatif

Ce code décrit un noeud associatif ayant deux arcs. Il décrit également les relations entre modes de défaillances entre la fonction "Utiliser 2 Automates avec alarme prioritaire" et 2 API (notés API1 et API2).

```
NoeudAssociatif *N13 = new NoeudAssociatif("Utiliser 2 Automates avec alarme prioritaire");
N13->addMdD("arrêt sans alarme",
        new OpAND(
                new Element(API1,"arrêt sans alarme"),
                new Element(API2,"arrêt sans alarme")));
N13->addMdD("arrêt avec alarme",
        new OpOR(
                new Element(API1,"arrêt avec alarme"),
                new Element(API2,"arrêt avec alarme")));
N13->evalue();
```

### Noeud Elémentaire

Ce code décrit un noeud élémentaire entre une fonction "Detecter fumee" et son composant DetecteurStd.

```
NoeudElementaire *N12 = new NoeudElementaire("Detecter fumee", DetecteurStd);
```

## C.3 Liste de résultats obtenus pour le système hydraulique

Le tableau C.1 présente la liste des résultats pour le système hydraulique issue d'ALoC-SyS.

| Liste des solutions | | | | | |
|---|---|---|---|---|---|
| Coût | Vidange ($ER_1$) ($L_{min}[N_{min}]$) | Débordement ($ER_2$) ($L_{min}[N_{min}]$) | Coût | Vidange ($ER_1$) ($L_{min}[N_{min}]$) | Débordement ($ER_2$) ($L_{min}[N_{min}]$) |
| 71 | 4[156] | 4[64] | 51 | 3[50] | 4[16] |
| 72 | 4[132] | 4[64] | 52 | 3[44] | 4[112] |
| 72 | 4[156] | 4[40] | 52 | 3[46] | 4[24] |
| 73 | 4[120] | 4[64] | 53 | 3[48] | 4[16] |
| 73 | 4[180] | 4[16] | 54 | 3[44] | 4[24] |
| 73 | 4[144] | 4[48] | 47 | 3[56] | 2[8] |
| 73 | 4[145] | 4[46] | 48 | 3[44] | 2[4] |
| 74 | 4[108] | 4[72] | 32 | 2[30] | 4[108] |
| 74 | 4[112] | 4[68] | 33 | 2[20] | 4[108] |
| 74 | 4[156] | 4[16] | 34 | 2[35] | 4[48] |
| 74 | 4[133] | 4[54] | 34 | 2[30] | 4[60] |
| 75 | 4[132] | 4[56] | 35 | 2[13] | 4[16] |
| 75 | 4[100] | 4[76] | 28 | 2[24] | 3[44] |
| 75 | 4[128] | 4[60] | 29 | 2[16] | 3[44] |
| 75 | 4[192] | 4[8] | 30 | 2[24] | 3[12] |
| 75 | 4[144] | 4[16] | 31 | 2[16] | 3[12] |
| 76 | 4[124] | 4[60] | 26 | 2[24] | 2[8] |
| 76 | 4[132] | 4[24] | 27 | 2[16] | 2[8] |
| 76 | 4[167] | 4[8] | 17 | 1[5] | 4[48] |
| 49 | 3[50] | 4[104] | 15 | 1[4] | 3[12] |
| 50 | 3[52] | 4[96] | 13 | 1[4] | 2[8] |
| 50 | 3[46] | 4[104] | | | |

TAB. C.1 – Liste des systèmes optimaux trouvés pour le système hydraulique

## C.4 Exemple d'architecture matérielle

L'architecture matérielle ci-dessous correspond au système hydraulique de la figure 2.14 présentée au paragraphe 2.4.3 du chapitre 2.

- Syst. de comm. 1 (Redondance passive) : 38 2[12] 4[16] 4[24]
  - Ens. de commande : 30 2[9] 3[2] 2[1]

  - Ens. Commande API
    - Automate Sûr n°1 : 8 1[1] 2[1]
    - Automate Sûr n°2 : 8 1[1] 2[1]
  - Ens. pompage (Redondance passive)
    - Pompe Standard n°1 : 5 1[1]
    - Pompe Standard n°2 : 5 1[1]
  - Ens. Capt. Niveau
    - Capt. Standard n°1 : 2 1[1] 1[1] 100[1]
    - Capt. Standard n°2 : 2 1[1] 1[1] 100[1]
- Ens. de surveillance : 6 2[3] 1[1] 2[2]
  - Détecteur Haut
    - Détecteur Actif-sûr : 2 2[1] 1[1]
  - Détecteur Bas (2 Détecteurs parallèles)
    - Détecteur Actif-sûr n°1 : 2 2[1] 1[1]
    - Détecteur Actif-sûr n°2 : 2 2[1] 1[1]
- Ens. de mise en repli : 2 2[1] 1[1]
  - Ens. Coupe-circuit
    - Coupe-circuit Ouvert-sûr : 2 2[1] 1[1]
- Syst. de comm. 2 : 33 2[7] 2[4] 2[4]
  - Ens. de commande : 28 2[5] 1[1] 1[1]
    - Ens. Commande API
      - Automate Sûr n°1 : 8 1[1] 2[1]
      - Automate Sûr n°2 : 8 1[1] 2[1]
    - Ens. pompage (Redondance passive)
      - Pompe Standard n°1 : 5 1[1]
      - Pompe Standard n°2 : 5 1[1]
    - Ens. Capt. Niveau
      - Capt. Standard : 2 1[1] 1[1] 100[1]
  - Ens. de surveillance : 4 2[2] 1[1] 1[1]
    - Détecteur Haut
      - Détecteur Actif-sûr : 2 2[1] 1[1]
    - Détecteur Bas
      - Détecteur Inactif-sûr : 2 1[1] 2[1]
  - Ens. de mise en repli : 1 1[1] 1[1]
    - Ens. Coupe-circuit
      - Coupe-circuit Standard : 1 1[1] 1[1]

Nota : Les valeurs associées aux éléments sont le coût suivi de la longueur des séquences ($L_{min}$) et de leur nombre ([$N_{min}$]) pour chaque mode de défaillance.

# Annexe D

# Etat de l'art sur les systèmes de ferroutage

Il existe de nombreux systèmes de fret ferroviaire dans le monde. Les paragraphes suivants de cette annexe présentent une liste non exhaustive des principaux systèmes et projets ainsi qu'un classement suivant les différents types de chargement.

## D.1 Les systèmes existants en Amérique du Nord

### Le Road-Railer

Le principe technique du Road-Railer est le suivant : on utilise un bogie isolé et le châssis du semi-remorque se substitue à celui du wagon par un système de blocage au niveau des essieux comme le montre la figure D.1 On utilise des bogies et des roues de grande taille ce qui réduit les coûts liés à l'usure. On n'utilise que la remorque, il n'y a pas de moyens pour charger le tracteur routier séparément sur le train.
Ce système présente l'avantage d'une extrême simplicité mais impose l'utilisation de remorques routières spéciales dont la structure a été renforcée. Cette technique est répandue aux Etats Unis mais elle n'a pas percé commercialement en Europe car elle implique l'utilisation de camions spéciaux.

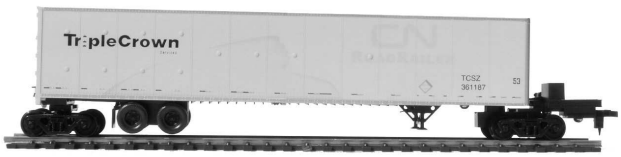


FIG. D.1 – Le système Road-Railer

### Le Iron Highway

Le Canada utilise deux systèmes de ferroutage : le Road-Railer et le « Iron Highway ». Ce système est composé d'une plateforme articulée continue de 366m de long sur bogies. Cette technologie fait appel à des rames de plateformes continues qui peuvent transporter 20 semi-remorques routières conventionnelles grandeur nature sans qu'il soit requis de les modifier ou de les renforcer.
Le système d'arrimage au terminal a été conçu pour faire en sorte que les semi-remorques n'aient pas à être renforcées. Aucune grue intermodale ni bogie d'attelage ne sont requis avec cette technologie. Elle permet aussi d'accommoder les semi-remorques de toutes les longueurs. Pour les phases de chargement et de déchargement, un petit tracteur s'occupe de monter ou descendre les remorques du train.

## D.2 Les systèmes existants en Europe

### Le système standard du wagon poche

Le wagon poche est un type de wagon ferroviaire conçu pour le transport de semi-remorques standard.
Un wagon poche pèse 16 tonnes. Il comporte entre les bogies une poche (d'où son nom) permettant de placer le train porteur (2 ou 3 essieux) de la semi-remorque et ainsi de respecter la hauteur du gabarit ferroviaire.
La semi-remorque doit être chargée à l'aide d'une grue ou d'un portique-grue.
Cette solution de transport combiné est en exploitation depuis les années 1970 dans toute l'Europe (France, Allemagne, Europe de l'Est, ...). Mais elle n'est pas comparable aux autres systèmes de ferroutage car elle nécessite une organisation logistique différente : manutention par grue, échange de tracteur routier au départ et à l'arrivée. De ce fait, les autres systèmes Européens et la route roulante Suisse prennent de plus en plus la prépondérance sur ce type de transport.

### Le système Français Modalohr

Ce système est utilisé depuis 2003 dans les Alpes et depuis 2007 sur la ligne Perpignan-Luxembourg. Il est basé sur un wagon surbaissé et articulé, à grandes roues.
Le principe de base du chargement, expliqué figure D.2, est la mise au point du concept de wagon à coque amovible (E) et pivotant pour le transport des semi-remorques. Cette coque est soulevée à la hauteur du quai par un système niché entre les rails. La coque pivote de

30° sur son axe jusqu'à reposer sur les deux quais (D et F) dans l'axe du poids lourd. Le chauffeur y fait alors monter son véhicule (C), positionne et cale sa remorque au centre avant de la détacher et de s'éloigner avec son tracteur. La coque pivote à nouveau et se bloque entre les deux bogies du wagon (B). Le tracteur routier peut également être chargé mais indépendamment de sa remorque et sur un autre wagon (A).

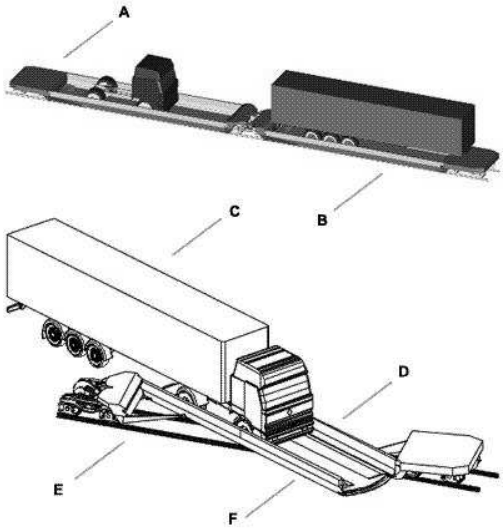


FIG. D.2 – Le système Français Modalohr

## Le système fret de l'Eurotunnel

Un train navette poids lourds de l'Eurotunnel est composé de deux rames encadré par deux locomotives. Chaque rame comprend 14 ou 15 wagons porteurs encadrées par deux wagons chargeurs / déchargeurs. Chaque wagon est équipé de vérins pour éviter le renversement pendant le chargement. De plus, chaque wagon chargeur est équipé de plats bords rabattables pour permettre le chargement des véhicules. Le chargement est longitudinal et ne nécessite ni de locotracteurs ni d'infrastructures spécialisées.

## Système existant en Suisse

La route roulante Suisse reprend le principe du système Iron Highway, c'est-à-dire le principe de la plate forme continue de transport. La différence est que ce système utilise des wagons à petites roues. Les petites roues servent à surbaisser le wagon afin qu'il passe les tunnels avec son chargement. L'embarquement des camions est longitudinal par une extrémité du train, sans l'aide de grues ou de locotracteurs. C'est une technologie utilisée depuis plus de 20 ans par la société Hupac.

## D.3 Les projets

### Le concept Cargo Speed

Ce concept est proche du système Modalohr décrit précédemment, c'est-à-dire qu'il reprend le principe du wagon pivotant [Car02]. Un premier prototype de ce wagon a d'ailleurs été dévoilé le 29 juillet 2004 en Angleterre [Car04]. La différence avec le système Modalohr est le système du pivot de la coque du wagon. Le système est prévu pour faire voyager trente remorques sur des parcours d'au moins 300kms et à une vitesse estimée de 120 km/h. Ce système ne peut prendre que les remorques seules sans possibilité de l'étendre au tracteur, contrairement à son système cousin Modalohr.

### Le système ResoRail

Ce concept français repose sur deux principes [SC02b], [SC02a] :

- Il utilise des wagons à bogies classiques et à grandes roues, dont le plancher est mobile. Dans les gares, l'infrastructure permet de monter le plancher en position haute, au niveau du quai, permettant au camion de monter ou de descendre sur le wagon. Hors des gares, le plancher se met en position basse pour pouvoir passer dans les tunnels. La mobilité de cette plate forme ne dépend que de la puissance de traction de la motrice.
- Il utilise le réseau actuel de gares en les structurant en boucles de desserte afin d'assurer une gestion en flux tendu. Les gares devant être disposées à 1h d'intervalle environ. De plus, ces gares ne nécessitent qu'une ou deux voies détachées des voies principales, donnant accès à un quai « haut ». Grâce au mécanisme passif de maintien du plateau du wagon, les camions se trouvent au niveau du quai lors du stationnement de la rame en gare. Ils n'ont qu'à manoeuvrer aussi simplement que sur un parking.

### Le concept R-Shift-R

Ce concept a été proposé par deux ingénieurs français [DM02], [Des03]. Il implique la création de gares, d'engins de manutention et de matériel roulants d'un type nouveau, mais il garantit également une rentabilité de l'investissement par la performance des services offerts aux clients (rapidité, fréquence).
Le matériel roulant se compose des éléments suivants : bogies, poutres de liaison entre les bogies, praticables, couverture de protection des charges, « automanipulateurs ", ... Les gares sont composées de 4 parties fonctionnelles : une zone centrale, une zone de chargement, une zone de circulation routière et un parc de stockage. La multiplication des postes d'embar-

quement et de débarquement permet de travailler en parallèle.

### Le projet SAIL

Le projet SAIL (Semitrailers in Advanced Intermodal Logistics) de l'université d'Aachen en Allemagne est sponsorisé par des opérateurs de combinés européens [Sai02]. Il permet le transbordement de semi-remorques ou de caisses mobiles sur des wagons. Ce projet est articulé autour de trois axes :

- Le premier axe est une réorganisation du système Ro-Ro (Roll on, Roll off). Ce système est complètement automatisé et adapté pour un grand nombre de modèles de semi-remorques.
- Le deuxième axe est basé sur un nouveau type de "Pocket Wagon" pour le transport de remorques au gabarit GB1, ce wagon universel est également capable de transporter des remorques de grand volume.
- Le troisième axe est conçu, non seulement pour le transport de tous les types de remorques, mais également pour transporter la nouvelle génération de « swap bodies » sans roues.

## D.4 Les deux types de chargement

Cet état de l'art des systèmes de ferroutage nous a permis de regrouper les techniques en deux familles distinctes suivant le type de chargement : chargement série ou chargement parallèle.

| Nom du système | Type de chargement | |
|---|---|---|
| | *Chargement série* | *Chargement parallèle* |
| RoadRailer (USA) | X | |
| Iron highway (Canada) | X | |
| Wagon poche (Europe) | X | |
| Eurotunnel Fret (France-Angleterre) | X | |
| Modalohr (France-Italie) | | X |
| Route roulante (Suisse) | X | |
| R-shift-R (Projet) | | X |
| Cargo speed (Projet) | | X |
| Resorail (Projet) | | X |
| Projet Sail (Allemagne) | X | |

TAB. D.1 – Systèmes de ferroutage en fonction de la technique de chargement du véhicule

Le tableau D.1 présente le classement des précédentes techniques suivant le principe de chargement du véhicule routier sur le train.

## Le chargement série

Techniquement, le chargement série autorise le chargement des camions longitudinalement, ce qui malheureusement ne permet de charger qu'un seul camion à la fois. Par contre, le chargement série ne nécessite qu'un seul quai de déchargement à l'extrémité de la rame, ce qui réduit considérablement les emprises routières de la plate-forme rail-route (Figure D.3). En contrepartie, l'utilisation de ces rames nécessite, généralement, un locotracteur de manoeuvre afin de refouler la rame sur le quai de déchargement.

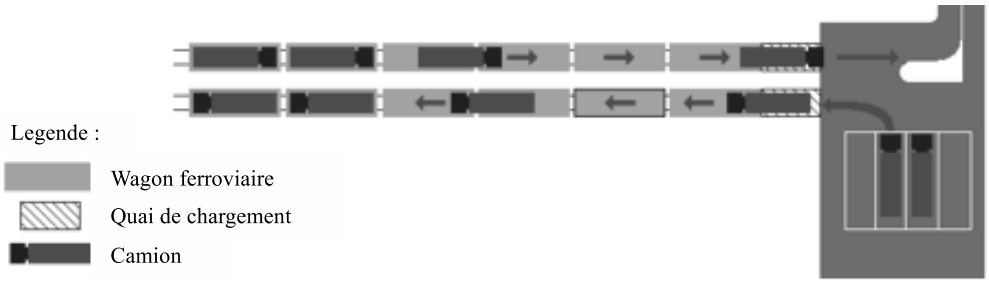


FIG. D.3 – Le principe du chargement série

## Le chargement parallèle

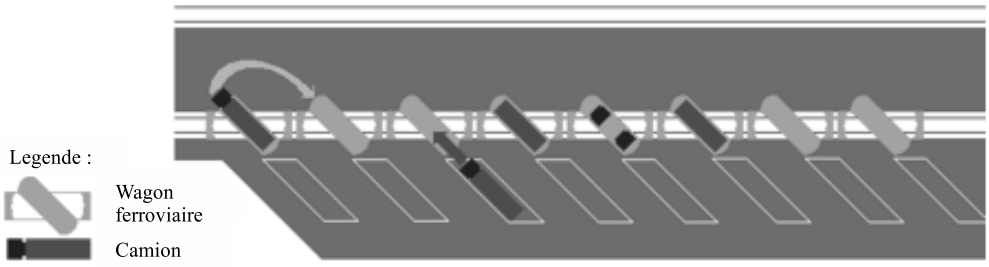


FIG. D.4 – Le principe du chargement parallèle

Le chargement parallèle permet de son côté de décharger l'ensemble des camions simultanément et perpendiculairement à l'axe de la rame, ce qui permet au système d'être beaucoup plus flexible que le précédent. Afin de permettre le chargement parallèle, le wagon comprend une partie amovible, contenant la remorque et / ou le tracteur, et qui pivote par rapport au centre du wagon (Figure D.4).

Mais, en contrepartie, en raison de l'encombrement des roues, à taille normale, le wagon n'autorise que le chargement d'une seule remorque et de son tracteur. Conséquence, malgré le chargement perpendiculaire à l'axe de la voie, le wagon impose une manoeuvre de désaccouplement et d'accouplement entre la remorque et le tracteur du semi-remorque.
De part la technique de chargement et de déchargement, perpendiculaire à l'axe de la voie, l'emprise routière de la plate-forme rail-route est donc beaucoup plus importante que dans le cas des wagons à petites roues. Cependant, la technique de chargement parallèle n'impose pas l'utilisation de locotracteurs pour manoeuvrer la rame.

# Annexe E

# Le gabarit GB1

Le gabarit de référence pour le transport ferroviaire de véhicules routiers détaillé figure E.1 est le gabarit UIC 506 GB1 appelé aussi en France "Gabarit B+". C'est le gabarit le plus petit dans lequel il est techniquement possible d'inscrire un camion standard Européen de 4m de haut et de 2.6m de large. Les principales lignes de transit ferroviaires en France offrent ce gabarit GB1 et la plupart des pays voisins de la France (Suisse, Allemagne, Italie par exemple) ont des lignes au gabarit plus généreux que le GB1.

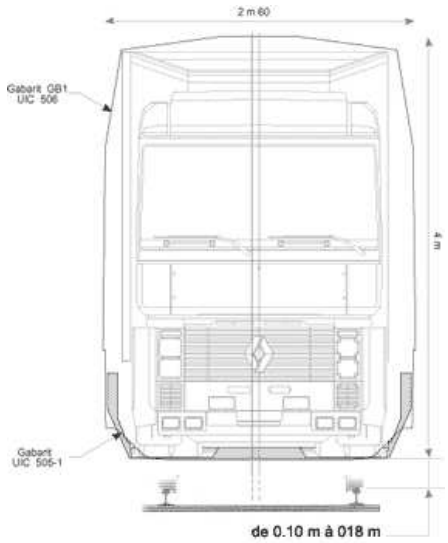


FIG. E.1 – Gabarit de référence GB1 pour le transport de véhicules routiers

En ce qui concerne les axes de transit Français inférieurs au gabarit GB1, ils nécessitent l'utilisation de wagons spéciaux à petites roues ayant des planchers surbaissés. L'utilisation de tels wagons à petites roues entraîne des contraintes d'usures supplémentaires par rapport à un wagon standard à roues normales (ou "grandes roues"). Pour une société de transport

ferroviaire, le wagon de transport de fret idéal serait un wagon à grandes roues et à plancher surbaissé et qui serait ainsi utilisable sur les lignes dont le gabarit est inférieur au GB1. Certains projets décrits dans l'annexe D tentent de résoudre cet inconvénient lié au gabarit des voies.

# Annexe F

# Présentation des atouts du ferroutage

## F.1 Une solution complémentaire au "tout-routier"

La généralisation de la gestion à flux tendus et le fractionnement des lots, qui correspondent aux deux grandes tendances d'évolution de la logistique, ont contribué à favoriser l'essor rapide du transport routier. De même, la concurrence accrue et l'émergence de tarifs toujours plus compétitifs qui en résulte, ont considérablement renforcé l'intérêt du mode de transport routier par rapport aux autres modes (ferroviaire, fluvial et aérien). Cependant, si la route réalise 90 % du tonnage transporté en France, elle éprouve de plus en plus de difficultés à maintenir un très haut niveau de qualité. En effet, la saturation progressive des itinéraires routiers et autoroutiers, associée à la difficulté d'accroître la capacité de ce réseau, amène les chargeurs à examiner la possibilité d'avoir recours à d'autres modes de transport. Par ailleurs, les coûts provoqués en termes d'environnement et de sécurité ont amené la collectivité à prendre conscience de la nécessité de limiter le développement du "tout routier". Les autres modes de transport, utilisés seuls, peuvent donc contribuer partiellement à absorber cette croissance des trafics et à lutter contre les méfaits de la route, mais il devient alors nécessaire que tous les sites expéditeurs et tous les sites destinataires soient équipés d'un embranchement ferroviaire ou fluvial, ce qui est assez difficile à faire.
Comme ce n'est pas le cas, le transport dit **multimodal** constitue alors la seule alternative. Dans l'absolu, toutes les combinaisons sont possibles entre les modes de transport (ferroviaire-fluvial, fluvial-routier, ...), mais en pratique, c'est essentiellement le **transport combiné accompagné rail-route** (ou **ferroutage**) qui progresse du fait de sa plus grande aptitude à s'inscrire dans une chaîne logistique multimodale.

Depuis une quinzaine d'années, en Europe et plus particulièrement en France, la volonté de recourir au ferroutage semble s'accentuer. Les raisons de cet engouement sont principalement de deux ordres. Elles se fondent sur la nécessité de lutter contre le développement

excessif du transport routier et sur les atouts propres au ferroutage.

## F.2 La lutte contre les conséquences négatives du tout routier

En France, le transport est déjà très largement dominé par la route (70% du tonnage-kilomètre), et de plus, un glissement s'est opéré dans les années 90 entre les voies fluviales et ferroviaires vers le mode routier. Ainsi, la part du transport routier en tonne/km est passée de 50 à 70% dans les quarante dernières années et continue de croître régulièrement.
Il est donc devenu nécessaire de prendre en considération les conséquences d'un excès du transport routier sur la saturation et la congestion des infrastructures, l'environnement et la sécurité. Le recours au ferroutage résout ces différents problèmes qui ont déjà atteint un seuil critique dans certaines régions françaises.

### Saturation et congestion des infrastructures

D'après les dernières prévisions, le trafic routier de marchandises devrait continuer de croître régulièrement dans les prochaines années. Ainsi, la commission européenne estime que le trafic routier intra-communautaire de marchandises pourrait poursuivre son évolution, avec une croissance supérieure à 90% d'ici 2010. En effet, de nombreux facteurs devraient alimenter cette croissance, et en particulier :

- la libéralisation du marché des transports,
- la généralisation de la gestion à flux tendus et la demande croissante des livraisons juste-à-temps, qui aggravent l'encombrement puisqu'elles conduisent à de plus fréquents trajets de retour à vide,
- l'importante concurrence à l'intérieur du secteur des transports routiers et la baisse des prix qu'elle entraîne,
- la libéralisation des échanges internationaux.

Ce développement des flux de marchandises est particulièrement important dans certaines zones et sur certains axes (le couloir du Rhône par exemple). Les bassins de forte production, de forte consommation et de forte densité démographique et urbaine sont donc menacés de saturation. Il existe un risque de congestion des principaux axes routiers entraînant des risques d'accidents routiers importants (le passage obligatoire par le Tunnel du Mont-Blanc occasionnant l'incendie du 24 mars 1999 par exemple). Des goulets d'étranglement aux abords des grandes villes et sur les grands axes routiers nationaux apparaissent de plus en plus fréquemment et menacent la qualité de service rendu (allongement des temps de transport, retard à la livraison, etc ...). Le recours au développement de nouvelles infrastructures routières et autoroutières pour résoudre ces problèmes atteint une certaine limite. En effet,

outre l'importance du coût de construction de telles infrastructures, les territoires sont déjà bien occupés.
En fait, c'est la répartition très inégale entre les modes de transport de marchandises qui est à l'origine de la saturation des axes routiers et autoroutiers. En 1997, sur le marché français, 90 % du transport de marchandises (en tonnage) était réalisé par route (contre 8% pour le fer et 2% pour le fluvial). Face à une telle répartition, les projets de rééquilibrage entre les modes de transport se multiplient, notamment en faveur du fer. Or la capacité par rail est limitée dans les zones de congestion de trafic et le développement de nouvelles infrastructures est coûteux et prend du temps. D'ailleurs le ferroviaire souffre d'un manque de fiabilité perçue par les clients. En effet, les trains de fret circulent à des plus faibles vitesses que les trains de voyageurs et ont tendance à être écartés pour les trains de voyageurs qui bénéficient d'une priorité de passage. De même le transport fluvial est limité puisqu'il dépend essentiellement de la position des fleuves et canaux.
Pour contrer la saturation et la congestion routière, le ferroutage est vu comme un moyen, sinon alternatif, du moins complémentaire au tout routier par le transfert d'une partie des trafics routiers. Ce transfert sera possible si les deux modes de transports se trouvent géographiquement disponibles à immédiate proximité des aires logistiques et si le ferroutage est rendu attractif par une offre régulière, sécurisée et cadencée pour les expéditeurs. Ainsi, en se substituant au *tout routier*, le ferroutage permettra de limiter la congestion routière mais il doit également limiter les nuisances pour l'environnement et les problèmes de sécurité liés à ce mode de transport.

## Environnement et sécurité

Au delà des coûts économiques, le développement du transport routier a un coût social élevé en termes d'environnement et de sécurité. En effet, l'accroissement du trafic routier risque de provoquer une augmentation de l'insécurité. Du fait de la nécessité d'avoir un faible coût de transport, ce mode de transport implique de longues distances et de nombreuses heures de conduite qui accroissent la fatigue des conducteurs routiers et augmentent ainsi le risque d'accident de la circulation (endormissement au volant par exemple).
Par ailleurs, la croissance du transport routier peut se révéler également dangereux pour l'environnement, en effet :

- la route augmente la pollution de l'air par le rejet dans l'atmosphère de gaz $CO_2$ favorisant l'effet de serre et les nuisances acoustiques,
- l'augmentation de nombre de camions entraîne l'augmentation du nombre de matières dangereuses transportées et du risque de pollution en cas d'accident (déversement, fumées toxiques, pollution de la nappe phréatique, ...),
- la croissance du transport routier augmente la consommation de carburant et la réduction des ressources d'origine fossile non renouvelables.

Le transport par ferroutage apparaît comme un moyen de concilier les besoins du marché des transports (rapidité et disponibilité) et les besoins de protection de l'environnement et de réduction de l'insécurité, en effet :

- les moteurs des camions transportés par ferroutage sont à l'arrêt, ils ne consomment donc pas de carburant et ne rejettent pas dans l'atmosphère de gaz à effet de serre,
- les chauffeurs routiers sont également transportés par le train et peuvent se reposer pendant le trajet. Les risques d'accidents routiers sont ainsi réduits.

## F.3 Qualités propres au ferroutage

Le ferroutage est une formule à la fois souple et fiable pour un client ayant des volumes à traiter ne relevant pas de la compétence du train complet et désirant une relation porte à porte. En effet, le client peut bénéficier des avantages fondamentaux des modes routiers et ferroviaires, puisqu'il allie la capacité de la route à desservir l'ensemble du territoire et l'aptitude du fer à effectuer des transports de longue distance de façon économique. Autrement dit, le transport combiné accompagné réunit la fiabilité du rail et la souplesse de la route. En effet, peu dépendant des impondérables comme les intempéries ou la circulation ralentie, l'acheminement peut être planifié avec précision. Ainsi le ferroutage, en plus de l'image écologique qu'il procure, par sa fiabilité et par sa souplesse permet d'atteindre une qualité de service satisfaisante pour les longs trajets. Une utilisation plus intensive de ce mode de transport permettrait une réduction importante du nombre de camions sur les routes. Afin de rendre le système de ferroutage plus attractif en France pour les transporteurs routiers, de nouvelles lignes de ferroutage sont développées. Celles-ci sont présentées dans l'annexe G.

# Annexe G

# Le ferroutage : un système en développement

## G.1 Les besoins

En France, le ferroutage est considéré comme une solution dans deux situations :

- Pour le franchissement d'un obstacle ponctuel qui entraîne des surcoûts par la voie routière, ou qui résulte de contraintes réglementaires. C'est pas exemple le cas de la traversée de la Manche (Système de l'Eurotunnel) ou celui d'une chaîne de montagne (Traversée des Alpes avec le système Modalohr).
- Pour des longs parcours, car dans ce cas, la contrainte vient de la réglementation routière, notamment des règles d'utilisation du personnel de conduite et des limitations de vitesse, voire des interdictions temporaires de circulation (week-ends, jours fériés) et qui rendent le ferroutage plus performant économiquement.

Concernant les longs parcours, il existe actuellement plusieurs projets visant à aménager des voies spécialement dédiées au ferroutage. Nous présentons ces projets dans cette annexe.

## G.2 Les Autoroutes Ferroviaires

### Le Lorry-Rail

Cet autoroute ferroviaire met en service des navettes entre les villes de Luxembourg et de Perpignan sur une distance de 1050 kms. La ligne a été ouverte au trafic commercial le 10 septembre 2007.

La traction est assurée par la SNCF et la commercialisation du service est effectuée par la société Lorry-Rail, dont les principaux actionnaires sont la société Autoroutes du Sud de la France (ASF, 40 %) et la caisse des dépôts et consignations (30 %). Le matériel est constitué

de wagons du système Modalhor.
Actuellement, le service consiste à faire circuler une paire de trains (un dans chaque sens) chaque nuit entre 18 h et 6 h du matin, même les dimanches et jours fériés quand les interdictions de circulation s'appliquent sur les autoroutes. Chaque train formé de vingt wagons offre une capacité de 40 véhicules. La charge maximale admise du véhicule est de 44 tonnes, permettant un gain de 17 % de charge utile par rapport aux masses maximales normalement admises. Par la suite, afin de proposer ce service à un plus grand nombre de transporteurs, la fréquence sera augmentée (davantage de trains dans chaque sens). Le trafic est estimé, pendant la phase actuelle de démarrage, à 30.000 camions par an.

## L'Eco-Fret

L'Eco-Fret est le nom du projet d'autoroute ferroviaire consistant à développer deux axes de transport par ferroutage. La figure G.1 présente une carte de 2007 avec les lignes de ferroutage réalisées, envisagées et à l'étude pour ce projet.

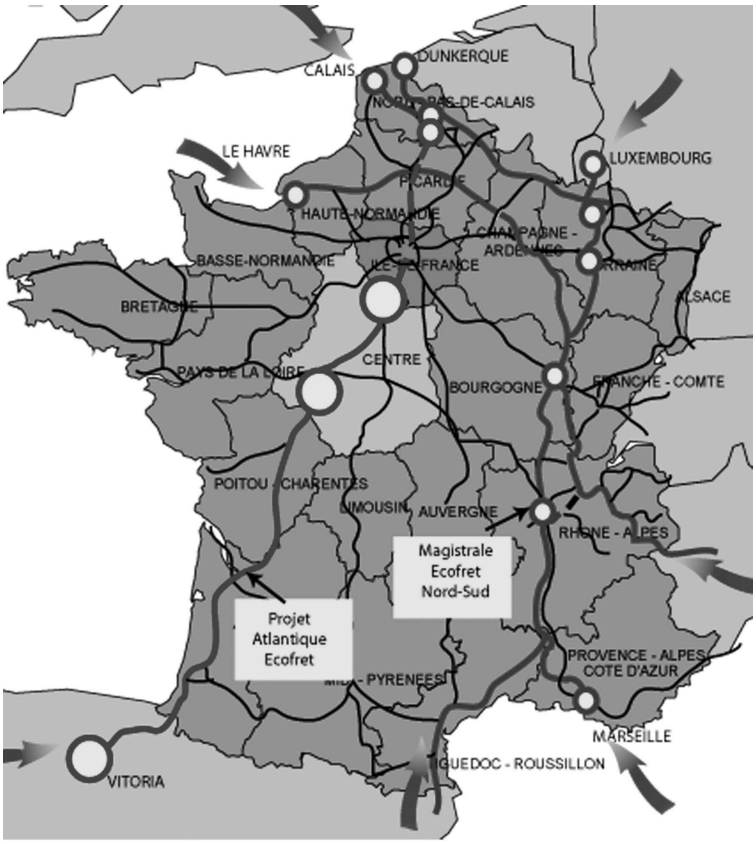


FIG. G.1 – Lignes de ferroutage du projet de l'Eco-Fret

Le premier axe est dénommé "Atlantique Eco-Fret", il consiste à offrir au fret un lien direct entre le nord de l'Europe, la France et l'Espagne. Actuellement en phase d'études pour définir les itinéraires les plus pertinents, il consiste à créer un service entre Bayonne et Brétigny en Ile de France. Puis à prolonger cet axe vers le sud au-delà de la frontière espagnole, et vers le nord dans les environs de Lille. Les travaux sont inscrits dans les contrats de projets Etat-Régions 2007-2013 pour une mise en service progressive en 2015.

Le second axe est dénommé "Magistrale Eco-Fret", il consiste à mettre en service des navettes depuis Calais vers Metz, Perpignan et Modane afin de fluidifier le trafic routier européen sur l'axe nord-sud. Le point de départ est la réutilisation des deux systèmes de ferroutage actuels en France (Eurotunnel et Modalohr) et de l'autoroute ferroviaire Luxembourg-Perpignan puis leur développement sur l'ensemble du territoire Français. Le système Eurotunnel sera développé vers Metz et le système Modalhor entre Lyon et Chambéry, ce qui permettra de créer un axe de transport entre l'Angleterre, la France, le Benelux, l'Allemagne, l'Espagne et l'Italie. L'utilisation de wagons surbaissés est envisagée. Ce projet à été approuvé en 2001 par le gouvernement français pour une mise en service totale vers 2020.

# Annexe H

# Données du modèle du système global de protection

## H.1 Relations entre modes de défaillances

Relations entre modes de défaillances des figures 4.12 et 4.13 :

$$(\text{N}^\text{o}1)\begin{cases} Arc1\begin{cases} Syst.commande(A_1) \Rightarrow ER_1 \\ Syst.commande(A_2) \Rightarrow ER_2 \\ Syst.commande(A_3) \Rightarrow ER_3 \\ Syst.commande(A_4) \Rightarrow ER_4 \end{cases} \\ Arc2\begin{cases} Syst.commande_1(A_1)\ \textbf{SEQ}\ Syst.commande_2(A_1) \Rightarrow ER_1 \\ (Syst.commande_1(A_1)\ \textbf{SEQ}\ Syst.commande_2(A_2)) \\ \textbf{OR}\ (Syst.commande_1(A_2)\ \textbf{SEQ}\ Syst.commande_2(A_2)) \Rightarrow ER_2 \\ Syst.commande_1(A_3)\ \textbf{SEQ}\ Syst.commande_2(A_3) \Rightarrow ER_3 \\ (Syst.commande_1(A_3)\ \textbf{SEQ}\ Syst.commande_2(A_4)) \\ \textbf{OR}\ (Syst.commande_1(A_4)\ \textbf{SEQ}\ Syst.commande_2(A_4)) \Rightarrow ER_4 \end{cases} \end{cases}$$

$$(\text{N}^\text{o}2)\begin{cases} Detec.Mvt.(C_1)\ \textbf{OR}\ Envoi.signal(D_1) \Rightarrow A_1 \\ Detec.Mvt.(C_2)\ \textbf{OR}\ Envoi.signal(D_2) \Rightarrow A_2 \\ Detec.incendie(B_1)\ \textbf{OR}\ Envoi.signal(D_1) \Rightarrow A_3 \\ Detec.incendie(B_2)\ \textbf{OR}\ Envoi.signal(D_2) \Rightarrow A_4 \end{cases}$$

$$(\text{N}^\text{o}3)\begin{cases} Detec.Mvt.long.(E_1)\ \textbf{AND}\ Detec.Mvt.trans.(F_1) \Rightarrow C_1 \\ Detec.Mvt.long.(E_2)\ \textbf{OR}\ Detec.Mvt.trans.(F_2) \Rightarrow C_2 \end{cases}$$

$$(\text{N}^\text{o}4)\begin{cases} Signal.syst.(L_2)\ \textbf{OR}\ Alim.syst.(M_1) \Rightarrow D_1 \\ Signal.syst.(L_1) \Rightarrow D_2 \end{cases}$$

$$
(\text{N}^\circ 5)\begin{cases}
Arc1\begin{cases} Detec.Temp(G_1)\ \textbf{OR}\ Detec.Fumee(H_1) \Rightarrow B_1 \\ Detec.Temp(G_2)\ \textbf{AND}\ Detec.Fumee(H_2) \Rightarrow B_2 \end{cases} \\
Arc2\begin{cases} Detec.Fumee(H_1)\ \textbf{AND}\ Detec.Temp(G_1) \Rightarrow B_1 \\ Detec.Temp(G_2)\ \textbf{PAND}\ Detec.Fumee(H_2) \Rightarrow B_2 \end{cases} \\
Arc3\begin{cases} Detec.Temp(G_1)\ \textbf{AND}\ Detec.Fumee(H_1) \Rightarrow B_1 \\ Detec.Temp(G_2)\ \textbf{OR}\ Detec.Fumee(H_2) \Rightarrow B_2 \end{cases}
\end{cases}
$$

$$
(\text{N}^\circ 6)\begin{cases}
Arc1\begin{cases} Detec.Pos.(I_1)\ \textbf{OR}\ Detec.Acc.(J_1) \Rightarrow E_1 \\ Detec.Pos.(I_2)\ \textbf{AND}\ Detec.Acc.(J_2) \Rightarrow E_2 \end{cases} \\
Arc2\begin{cases} Detec.Pos.(I_1)\ \textbf{AND}\ Detec.Acc.(J_1) \Rightarrow E_1 \\ Detec.Acc.(J_2)\ \textbf{PAND}\ Detec.Pos.(I_2) \Rightarrow E_2 \end{cases} \\
Arc3\begin{cases} Detec.Pos.(I_1)\ \textbf{AND}\ Detec.Acc.(J_1) \Rightarrow E_1 \\ Detec.Pos.(I_2)\ \textbf{OR}\ Detec.Acc.(J_2) \Rightarrow E_2 \end{cases}
\end{cases}
$$

$$
(\text{N}^\circ 7)\begin{cases}
Arc1\begin{cases} Detec.Pos.(I_1)\ \textbf{OR}\ Detec.Acc.(J_1)\ \textbf{OR}\ Detec.Dir.(K_1) \Rightarrow F_1 \\ Detec.Pos.(I_2)\ \textbf{AND}\ Detec.Acc.(J_2)\ \textbf{AND}\ Detec.Dir.(K_2) \Rightarrow F_2 \end{cases} \\
Arc2\begin{cases} Detec.Pos.(I_1)\ \textbf{AND}\ Detec.Acc.(J_1)\ \textbf{AND}\ Detec.Dir.(K_1) \Rightarrow F_1 \\ Detec.Dir.(K_2)\ \textbf{PAND}\ Detec.Acc.(J_2)\ \textbf{PAND}\ Detec.Pos.(I_2) \Rightarrow F_2 \end{cases} \\
Arc3\begin{cases} Detec.Pos.(I_1)\ \textbf{AND}\ Detec.Acc.(J_1) \Rightarrow F_1 \\ Detec.Pos.(I_2)\ \textbf{OR}\ Detec.Acc.(J_2) \Rightarrow F_2 \end{cases} \\
Arc4\begin{cases} Detec.Pos.(I_1)\ \textbf{OR}\ Detec.Acc.(J_1) \Rightarrow F_1 \\ Detec.Pos.(I_2)\ \textbf{AND}\ Detec.Acc.(J_2) \Rightarrow F_2 \end{cases} \\
Arc5\begin{cases} Detec.Pos.(I_1)\ \textbf{AND}\ Detec.Acc.(J_1) \Rightarrow F_1 \\ Detec.Acc.(J_2)\ \textbf{PAND}\ Detec.Pos.(I_2) \Rightarrow F_2 \end{cases} \\
Arc6\begin{cases} Detec.Pos.(I_1)\ \textbf{AND}\ Detec.Dir.(K_1) \Rightarrow F_1 \\ Detec.Dir.(K_2)\ \textbf{PAND}\ Detec.Pos.(I_2) \Rightarrow F_2 \end{cases} \\
Arc7\begin{cases} Detec.Pos.(I_1)\ \textbf{OR}\ Detec.Dir.(K_1) \Rightarrow F_1 \\ Detec.Pos.(I_2)\ \textbf{AND}\ Detec.Dir.(K_2) \Rightarrow F_2 \end{cases} \\
Arc8\begin{cases} Detec.Acc.(J_1)\ \textbf{OR}\ Detec.Dir.(K_1) \Rightarrow F_1 \\ Detec.Acc.(J_2)\ \textbf{AND}\ Detec.Dir.(K_2) \Rightarrow F_2 \end{cases} \\
Arc9\begin{cases} Detec.Pos.(I_1)\ \textbf{AND}\ Detec.Acc.(J_1)\ \textbf{AND}\ Detec.Dir.(K_1) \Rightarrow F_1 \\ Detec.Dir.(K_2)\ \textbf{AND}\ (Detec.Acc.(J_2)\ \textbf{PAND}\ Detec.Pos.(I_2)) \Rightarrow F_2 \end{cases}
\end{cases}
$$

$$
(\text{N}^\circ 8)\begin{cases}
G_1 \Rightarrow G_1 \\
G_2 \Rightarrow G_2 \\
H_1 \Rightarrow H_1 \\
H_2 \Rightarrow H_2
\end{cases}
$$

$$\text{(N"9)} \begin{cases} I_1 \Rightarrow I_1 \\ I_2 \Rightarrow I_2 \\ J_1 \Rightarrow J_1 \\ J_2 \Rightarrow J_2 \end{cases}$$

$$\text{(N"10)} \begin{cases} I_1 \Rightarrow I_1 \\ I_2 \Rightarrow I_2 \\ J_1 \Rightarrow J_1 \\ J_2 \Rightarrow J_2 \\ K_1 \Rightarrow K_1 \\ K_2 \Rightarrow K_2 \end{cases}$$

$$\text{(N"11)} \begin{cases} Pos.Avant(N_1) \textbf{ AND } Pos.Arriere(N_1) \Rightarrow I_1 \\ Pos.Avant(N_2) \textbf{ OR } Pos.Arriere(N_2) \Rightarrow I_2 \end{cases}$$

$$\text{(N"12)} \begin{cases} Pos.Droite(N_1) \textbf{ AND } Pos.Gauche(N_1) \Rightarrow I_1 \\ Pos.Droite(N_2) \textbf{ OR } Pos.Gauche(N_2) \Rightarrow I_2 \end{cases}$$

$$\text{(N"13)} \begin{cases} Arc1 \begin{cases} Detec.Pos(P_2) \Rightarrow N_1 \\ Detec.Pos(P_1) \Rightarrow N_2 \end{cases} \\ Arc2 \begin{cases} (Detec.Pos_1(P_2) \textbf{ OR } Detec.Pos_2(P_2)) \Rightarrow N_1 \\ (Detec.Pos_1(P_1) \textbf{ AND } Detec.Pos_2(P_1)) \Rightarrow N_2 \end{cases} \\ Arc3 \begin{cases} (Detec.Pos_1(P_2) \textbf{ AND } Detec.Pos_2(P_2)) \Rightarrow N_1 \\ (Detec.Pos_1(P_1) \textbf{ OR } Detec.Pos_2(P_1)) \Rightarrow N_2 \end{cases} \end{cases}$$

$$\text{(N"14)} \begin{cases} Arc1 \begin{cases} Detec.Acc(Q_2) \Rightarrow J_1 \\ Detec.Acc(Q_1) \Rightarrow J_2 \end{cases} \\ Arc2 \begin{cases} (Detec.Acc_1(Q_2) \textbf{ OR } Detec.Acc_2(Q_2)) \Rightarrow J_1 \\ (Detec.Acc_1(Q_1) \textbf{ AND } Detec.Acc_2(Q_1)) \Rightarrow J_2 \end{cases} \\ Arc3 \begin{cases} (Detec.Acc_1(Q_2) \textbf{ AND } Detec.Acc_2(Q_2)) \Rightarrow J_1 \\ (Detec.Acc_1(Q_1) \textbf{ OR } Detec.Acc_2(Q_1)) \Rightarrow J_2 \end{cases} \end{cases}$$

$$\text{(N"15)} \begin{cases} Arc1 \begin{cases} Gyr.(R_2) \Rightarrow K_1 \\ Gyr.(R_1) \Rightarrow K_2 \end{cases} \\ Arc2 \begin{cases} (Gyr._1(R_2) \textbf{ OR } Gyr._2(R_2)) \Rightarrow K_1 \\ (Gyr._1(R_1) \textbf{ AND } Gyr._2(R_1)) \Rightarrow K_2 \end{cases} \\ Arc3 \begin{cases} (Gyr._1(R_2) \textbf{ AND } Gyr._2(R_2)) \Rightarrow K_1 \\ (Gyr._1(R_1) \textbf{ OR } Gyr._2(R_1)) \Rightarrow K_2 \end{cases} \end{cases}$$

$$
(\text{N}^\text{o}16)\begin{cases}
Arc1 \begin{cases} Detec.Temp(S_2) \Rightarrow G_1 \\ Detec.Temp((S_1) \Rightarrow G_2 \end{cases} \\
Arc2 \begin{cases} (Detec.Temp(_1(S_2) \ \textbf{OR} \ Detec.Temp(_2(S_2)) \Rightarrow G_1 \\ (Detec.Temp(_1(S_1) \ \textbf{AND} \ Detec.Temp(_2(S_1)) \Rightarrow G_2 \end{cases} \\
Arc3 \begin{cases} (Detec.Temp(_1(S_2) \ \textbf{AND} \ Detec.Temp(_2(S_2)) \Rightarrow G_1 \\ (Detec.Temp(_1(S_1) \ \textbf{OR} \ Detec.Temp(_2(S_1)) \Rightarrow G_2 \end{cases}
\end{cases}
$$

$$
(\text{N}^\text{o}17)\begin{cases}
Arc1 \begin{cases} Detec.Fumee((T_2) \Rightarrow H_1 \\ Detec.Fumee(T_1) \Rightarrow H_2 \end{cases} \\
Arc2 \begin{cases} (Detec.Fumee_1(T_2) \ \textbf{OR} \ Detec.Fumee_2(T_2)) \Rightarrow H_1 \\ (Detec.Fumee_1(T_1) \ \textbf{AND} \ Detec.Fumee_2(T_1)) \Rightarrow H_2 \end{cases} \\
Arc3 \begin{cases} (Detec.Fumee_1(T_2) \ \textbf{AND} \ Detec.Fumee_2(T_2)) \Rightarrow H_1 \\ (Detec.Fumee_1(T_1) \ \textbf{OR} \ Detec.Fumee_2(T_1)) \Rightarrow H_2 \end{cases}
\end{cases}
$$

$$
(\text{N}^\text{o}18)\begin{cases}
Arc1 \begin{cases} API(U_2) \Rightarrow L_1 \\ API(U_1) \Rightarrow L_2 \end{cases} \\
Arc2 \begin{cases} (API_1(U_2) \ \textbf{OR} \ API_2(U_2)) \Rightarrow L_1 \\ (API_1(U_1) \ \textbf{AND} \ API_2(U_1)) \Rightarrow L_2 \end{cases} \\
Arc3 \begin{cases} (API_1(U_2) \ \textbf{AND} \ API_2(U_2)) \Rightarrow L_1 \\ (API_1(U_1) \ \textbf{OR} \ API_2(U_1)) \Rightarrow L_2 \end{cases}
\end{cases}
$$

$$
(\text{N}^\text{o}19)\begin{cases}
Arc1 \begin{cases} Alim.(V_1) \Rightarrow M_1 \end{cases} \\
Arc2 \begin{cases} Alim._1(V_1) \ \textbf{AND} \ Alim._2(P_1) \Rightarrow M_1 \end{cases} \\
Arc3 \begin{cases} Alim._1(V_1) \ \textbf{SEQ} \ Alim._2(P_1) \Rightarrow M_1 \end{cases}
\end{cases}
$$

$$
(\text{N}^\text{o}20)\begin{cases}
Arc1 \begin{cases} Detec.Pos - Standard(W_1) \Rightarrow P_1 \\ Detec.Pos - Standard(W_2) \Rightarrow P_2 \end{cases} \\
Arc2 \begin{cases} Detec.Pos - Sur1(W_1) \Rightarrow P_1 \\ Detec.Pos - Sur1(W_2) \Rightarrow P_2 \end{cases} \\
Arc3 \begin{cases} Detec.Pos - Sur2(W_1) \Rightarrow P_1 \\ Detec.Pos - Sur2(W_2) \Rightarrow P_2 \end{cases}
\end{cases}
$$

$$
(\text{N}^\text{o}21)\begin{cases}
Arc1 \begin{cases} Detec.Acc - Standard(X_1) \Rightarrow Q_1 \\ Detec.Acc - Standard(X_2) \Rightarrow Q_2 \end{cases} \\
Arc2 \begin{cases} Detec.Acc - Sur1(X_1) \Rightarrow Q_1 \\ Detec.Acc - Sur1(X_2) \Rightarrow Q_2 \end{cases} \\
Arc3 \begin{cases} Detec.Acc - Sur2(X_1) \Rightarrow Q_1 \\ Detec.Acc - Sur2(X_2) \Rightarrow Q_2 \end{cases}
\end{cases}
$$

$$
\begin{array}{ll}
\text{(N°22)} & \left\{\begin{array}{ll} Arc1 & \left\{\begin{array}{l} Gyr.-Standard(Y_1) \Rightarrow R_1 \\ Gyr.-Standard(Y_2) \Rightarrow R_2 \end{array}\right. \\ Arc2 & \left\{\begin{array}{l} Gyr.-Sur1(Y_1) \Rightarrow R_1 \\ Gyr.-Sur1(Y_2) \Rightarrow R_2 \end{array}\right. \\ Arc3 & \left\{\begin{array}{l} Gyr.-Sur2(Y_1) \Rightarrow R_1 \\ Gyr.-Sur2(Y_2) \Rightarrow R_2 \end{array}\right. \end{array}\right. \\
\text{(N°23)} & \left\{\begin{array}{ll} Arc1 & \left\{\begin{array}{l} Detec.Temp-Standard(Z_1) \Rightarrow S_1 \\ Detec.Temp-Standard(Z_2) \Rightarrow S_2 \end{array}\right. \\ Arc2 & \left\{\begin{array}{l} Detec.Temp-Sur1(Z_1) \Rightarrow S_1 \\ Detec.Temp-Sur1(Z_2) \Rightarrow S_2 \end{array}\right. \\ Arc3 & \left\{\begin{array}{l} Detec.Temp-Sur2(Z_1) \Rightarrow S_1 \\ Detec.Temp-Sur2(Z_2) \Rightarrow S_2 \end{array}\right. \end{array}\right. \\
\text{(N°24)} & \left\{\begin{array}{ll} Arc1 & \left\{\begin{array}{l} Detec.Fumee-Standard(AA_1) \Rightarrow T_1 \\ Detec.Fumee-Standard(AA_2) \Rightarrow T_2 \end{array}\right. \\ Arc2 & \left\{\begin{array}{l} Detec.Fumee-Sur1(AA_1) \Rightarrow T_1 \\ Detec.Fumee-Sur1(AA_2) \Rightarrow T_2 \end{array}\right. \\ Arc3 & \left\{\begin{array}{l} Detec.Fumee-Sur2(AA_1) \Rightarrow T_1 \\ Detec.Fumee-Sur2(AA_2) \Rightarrow T_2 \end{array}\right. \end{array}\right. \\
\text{(N°25)} & \left\{\begin{array}{ll} Arc1 & \left\{\begin{array}{l} API-Standard(AB_1) \Rightarrow U_1 \\ API-Standard(AB_2) \Rightarrow U_2 \end{array}\right. \\ Arc2 & \left\{\begin{array}{l} API-Sur1(AB_1) \Rightarrow U_1 \\ API-Sur1(AB_2) \Rightarrow U_2 \end{array}\right. \\ Arc3 & \left\{\begin{array}{l} API-Sur2(AB_1) \Rightarrow U_1 \\ API-Sur2(AB_2) \Rightarrow U_2 \end{array}\right. \end{array}\right. \\
\text{(N°26)} & \left\{\begin{array}{ll} Arc1 & \left\{\begin{array}{l} Alim.-Standard(AC_1) \Rightarrow V_1 \end{array}\right. \\ Arc2 & \left\{\begin{array}{l} Alim.-Sur(AC_1) \Rightarrow V_1 \end{array}\right. \end{array}\right.
\end{array}
$$

## H.2 Tableaux de données

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Mission : Détecter et signaler désarrimage et incendies | Noeud alternatif N"1 | - ER1 : Non détection incendie<br>- ER2 : Fausse alarme<br>- ER3 : Non détection arrimage<br>- ER4 : Fausse alarme |
| Utiliser 1 système de contrôle commande | Noeud associatif N"2 | - A1 : Non détection<br>- A2 : Fausse alarme<br>- A3 : Non détection arrimage<br>- A4 : Fausse alarme |
| Utiliser 2 systèmes de contrôle commande | Noeud associatif N"2 | - A1 : Non détection<br>- A2 : Fausse alarme<br>- A3 : Non détection arrimage<br>- A4 : Fausse alarme |
| Détecter incendies | Noeud alternatif N"5 | - B1 : Non détection<br>- B2 : Fausse alarme |
| Détecter mouvements camion | Noeud associatif N"3 | - C1 : Non détection<br>- C2 : Fausse alarme |
| Envoyer signal aux opérateurs | Noeud associatif N"4 | - D1 : Non détection d'alarme<br>- D2 : Fausse alarme |
| Détecter Température ET fumée | Noeud élémentaire N"8 | - G1, H1 : Continuellement passif<br>- G2, H2 : Continuellement actif |
| Détecter Fumée PUIS température | Noeud élémentaire N"8 | - G1, H1 : Continuellement passif<br>- G2, H2 : Continuellement actif |
| Détecter Fumée OU température<br>Détecter mvt long. | Noeud élémentaire N"8<br>Noeud alternatif N"6 | - G1, H1 : Continuellement passif<br>- G2, H2 : Continuellement actif<br>- E1 : Non détection<br>- E2 : Fausse alarme |
| Détecter Accélération ET position | Noeud élémentaire N"9 | - I1, J1 : Continuellement passif<br>- I2, J2 : Continuellement actif |
| Détecter Accélération PUIS position | Noeud élémentaire N"9 | - I1, J1 : Continuellement passif<br>- I2, J2 : Continuellement actif |
| Détecter Accélération OU position | Noeud élémentaire N"9 | - I1, J1 : Continuellement passif<br>- I2, J2 : Continuellement actif |

TAB. H.1 – A : Correspondance entre fonctions et modes de défaillances de la figure 4.12

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Détecter mvt trans. | Noeud alternatif N"7 | - F1 : Non détection<br>- F2 : Fausse alarme |
| Détecter Direction train ET accélération ET position | Noeud élémentaire N"10 | - I1, J1, K1 : Continuellement passif<br>- I2, J2, K2 : Continuellement actif |
| Détecter Direction train PUIS accélération PUIS position | Noeud élémentaire N"10 | - I1, J1, K1 : Continuellement passif<br>- I2, J2, K2 : Continuellement actif |
| Détecter Accélération OU position | Noeud élémentaire N"10 | - I1, J1 : Continuellement passif<br>- I2, J2 : Continuellement actif |
| Détecter Accélération ET position | Noeud élémentaire N"10 | - I1, J1 : Continuellement passif<br>- I2, J2 : Continuellement actif |
| Détecter Accélération PUIS position | Noeud élémentaire N"10 | - I1, J1 : Continuellement passif<br>- I2, J2 : Continuellement actif |
| Détecter Direction train PUIS position | Noeud élémentaire N"10 | - I1, J1, K1 : Continuellement passif<br>- I2, J2, K2 : Continuellement actif |
| Détecter Direction train ET position | Noeud élémentaire N"10 | - I1, J1, K1 : Continuellement passif<br>- I2, J2, K2 : Continuellement actif |
| Détecter Direction train ET accélération | Noeud élémentaire N"10 | - I1, J1, K1 : Continuellement passif<br>- I2, J2, K2 : Continuellement actif |
| Détecter Direction train ET accélération PUIS position | Noeud élémentaire N"10 | - I1, J1, K1 : Continuellement passif<br>- I2, J2, K2 : Continuellement actif |
| Envoyer signal depuis système de traitement | Noeud alternatif N"18 | - L1 : Arrêt inattendu ac alarme<br>- L2 : Arrêt inattendu ss alarme |
| Alimenter système de traitement | Noeud alternatif N"19 | - M1 : Arrêt inattendu |
| Détecter Température | Noeud alternatif N"16 | - G1 : Continuellement passif<br>- G2 : Continuellement actif |

TAB. H.2 – B : Correspondance entre fonctions et modes de défaillances de la figure 4.12

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Détecter Fumée | Noeud alternatif N"17 | - H1 : Continuellement passif<br>- H2 : Continuellement actif |
| Détecter Position longitudinale | Noeud associatif N"11 | - I1 : Continuellement passif<br>- I2 : Continuellement actif |
| Détecter Accélération longitudinale | Noeud alternatif N"14 | - J1 : Continuellement passif<br>- J2 : Continuellement actif |
| Détecter Position transversale | Noeud associatif N"12 | - I1 : Continuellement passif<br>- I2 : Continuellement actif |
| Détecter Accélération transversale | Noeud alternatif N"14 | - J1 : Continuellement passif<br>- J2 : Continuellement actif |
| Détecter Direction train | Noeud alternatif N"15 | - K1 : Continuellement passif<br>- K2 : Continuellement actif |
| Détecter Position avant | Noeud alternatif N"13 | - N1 : Continuellement passif<br>- N2 : Continuellement actif |
| Détecter Position arrière | Noeud alternatif N"13 | - N1 : Continuellement passif<br>- N2 : Continuellement actif |
| Détecter Position droite | Noeud alternatif N"13 | - N1 : Continuellement passif<br>- N2 : Continuellement actif |
| Détecter Position gauche | Noeud alternatif N"13 | - N1 : Continuellement passif<br>- N2 : Continuellement actif |
| Utiliser 1 détecteur position | Noeud alternatif N"20 | - P1 : Continuellement actif<br>- P2 : Continuellement passif |
| Utiliser 2 détecteurs en série | Noeud alternatif N"20 | - P1 : Continuellement actif<br>- P2 : Continuellement passif |
| Utiliser 2 détecteurs en parrallèle | Noeud alternatif N"20 | - P1 : Continuellement actif<br>- P2 : Continuellement passif |
| Utiliser 1 détecteur accélération | Noeud alternatif N"21 | - Q1 : Continuellement actif<br>- Q2 : Continuellement passif |
| Utiliser 2 détecteurs en série | Noeud alternatif N"21 | - Q1 : Continuellement actif<br>- Q2 : Continuellement passif |

TAB. H.3 – C : Correspondance entre fonctions et modes de défaillances de la figure 4.12

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Utiliser 2 détecteurs en parrallèle | Noeud alternatif N"21 | - Q1 : Continuellement actif<br>- Q2 : Continuellement passif |
| Utiliser 1 gyroscope | Noeud alternatif N"22 | - R1 : Continuellement actif<br>- R2 : Continuellement passif |
| Utiliser 2 gyroscopes redondance active | Noeud alternatif N"22 | - R1 : Continuellement actif<br>- R2 : Continuellement passif |
| Utiliser 2 gyroscopes redondance passive | Noeud alternatif N"22 | - R1 : Continuellement actif<br>- R2 : Continuellement passif |
| Utiliser 1 détecteur température | Noeud alternatif N"23 | - S1 : Continuellement actif<br>- S2 : Continuellement passif |
| Utiliser 2 détecteurs en série | Noeud alternatif N"23 | - S1 : Continuellement actif<br>- S2 : Continuellement passif |
| Utiliser 2 détecteurs en parrallèle | Noeud alternatif N"23 | - S1 : Continuellement actif<br>- S2 : Continuellement passif |
| Utiliser 1 détecteur fumée | Noeud alternatif N"24 | - T1 : Continuellement actif<br>- T2 : Continuellement passif |
| Utiliser 2 détecteurs en série | Noeud alternatif N"24 | - T1 : Continuellement actif<br>- T2 : Continuellement passif |
| Utiliser 2 détecteurs en parrallèle | Noeud alternatif N"24 | - T1 : Continuellement actif<br>- T2 : Continuellement passif |
| Utiliser 1 API | Noeud alternatif N"25 | - U1 : Arrêt avec alarme<br>- U2 : Arrêt sans alarme |
| Utiliser 2 API avec priorité alarme | Noeud alternatif N"25 | - U1 : Arrêt avec alarme<br>- U2 : Arrêt sans alarme |
| Utiliser 2 API sans priorité alarme | Noeud alternatif N"25 | - U1 : Arrêt avec alarme<br>- U2 : Arrêt sans alarme |
| Utiliser 1 Alimentation | Noeud alternatif N"26 | - V1 : Arrêt inattendu |
| Utiliser 2 Alimentations en redondance active | Noeud alternatif N"26 | - V1 : Arrêt inattendu |
| Utiliser 2 Alimentations en redondance passive | Noeud alternatif N"26 | - V1 : Arrêt inattendu |
| Détecteur Position standard | Pas de noeud | - W1 : Continuellement passif<br>- W2 : Continuellement actif |
| Détecteur Position sûr type 1 | Pas de noeud | - W1 : Continuellement passif<br>- W2 : Continuellement actif |
| Détecteur Position sûr type 2 | Pas de noeud | - W1 : Continuellement passif<br>- W2 : Continuellement actif |

TAB. H.4 – D : Correspondance entre fonctions et modes de défaillances de la figure 4.12

| Dénomination de la fonction | Noeud correspondant | Modes de défaillances |
|---|---|---|
| Détecteur Accélération standard | Pas de noeud | - X1 : Continuellement passif<br>- X2 : Continuellement actif |
| Détecteur Accélération sûr type 1 | Pas de noeud | - X1 : Continuellement passif<br>- X2 : Continuellement actif |
| Détecteur Accélération sûr type 2 | Pas de noeud | - X1 : Continuellement passif<br>- X2 : Continuellement actif |
| Gyroscope standard | Pas de noeud | - Y1 : Continuellement passif<br>- Y2 : Continuellement actif |
| Gyroscope sûr type 1 | Pas de noeud | - Y1 : Continuellement passif<br>- Y2 : Continuellement actif |
| Gyroscope sûr type 2 | Pas de noeud | - Y1 : Continuellement passif<br>- Y2 : Continuellement actif |
| Détecteur Température standard | Pas de noeud | - Z1 : Continuellement passif<br>- Z2 : Continuellement actif |
| Détecteur Température sûr type 1 | Pas de noeud | - Z1 : Continuellement passif<br>- Z2 : Continuellement actif |
| Détecteur Température sûr type 2 | Pas de noeud | - Z1 : Continuellement passif<br>- Z2 : Continuellement actif |
| Détecteur Fumée standard | Pas de noeud | - AA1 : Continuellement passif<br>- AA2 : Continuellement actif |
| Détecteur Fumée sûr type 1 | Pas de noeud | - AA1 : Continuellement passif<br>- AA2 : Continuellement actif |
| Détecteur Fumée sûr type 2 | Pas de noeud | - AA1 : Continuellement passif<br>- AA2 : Continuellement actif |
| API standard | Pas de noeud | - AB1 : Arrêt inattendu avec alarme<br>- AB2 : Arrêt inattendu sans alarme |
| API sûr type 1 | Pas de noeud | - AB1 : Arrêt inattendu avec alarme<br>- AB2 : Arrêt inattendu sans alarme |
| API sûr type 2 | Pas de noeud | - AB1 : Arrêt inattendu avec alarme<br>- AB2 : Arrêt inattendu sans alarme |
| Alimentation standard | Pas de noeud | - AC1 : Arrêt inattendu |
| Alimentation sûr | Pas de noeud | - AC1 : Arrêt inattendu |

TAB. H.5 – E : Correspondance entre fonctions et modes de défaillances de la figure 4.12

**Résumé :** Cette thèse s'intéresse à la conception de systèmes complexes d'automatisation sûrs de fonctionnement dont l'évaluation est basée sur des scénarios. Pour déterminer un système optimal, il est important de disposer d'outils de modélisation et d'évaluation rapides ainsi que des algorithmes d'optimisation adaptés au sein d'une méthodologie globale de conception. Cette méthodologie doit également permettre d'étudier l'impact des défaillances sur le comportement final du système contrôlé. Dans ce cadre, la détermination d'un architecture matérielle, son optimisation vis-à-vis de critères comme la longueur minimale des scénarios et le nombre de combinaisons de scénarios sont considérés.

Nous proposons une modélisation fonctionnelle et dysfonctionnelle utilisant les scénarios de modes de défaillances. Le niveau de détail considéré est suffisamment fin pour décrire différentes possibilités d'agencements des composants utilisables ainsi que plusieurs types de composants. Si la modélisation fonctionnelle est facile à appréhender, la modélisation dysfonctionnelle tenant compte des scénarios est plus difficile. Afin de répondre à ce problème, nous proposons un modèle graphique baptisé "Arbre de défaillances multiples amélioré" permettant de modéliser, à l'aide d'opérateurs temporels et de relations entre modes de défaillances, ce comportement dysfonctionnel. L'application de cette méthodologie à un système de ferroutage est présentée. Les résultats obtenus pour les fonctionnalités liées au problème de l'incendie et du désarrimage sont comparés avec une méthode classique d'évaluation afin de montrer l'efficacité de l'approche proposée. L'intégration de ces travaux dans un logiciel dédié à la conception de systèmes d'automatisation (plate forme ALoCSyS : Atelier Logiciel de Conception de Systèmes Sûrs) est décrite.

---

**Title :** Design of dependable automated system architectures using temporal sequences of failures

---

**Abstract :** This thesis deals with a design problem of dependable automated systems using scenarios. In order to determine an optimal system, having fast tools for modelling and evaluating dependability is important. These tools allow the set of possible architectures to be evaluated, and the impact of failures to be studied. The main considered questions include the determination of an equipment architecture, its optimization according to such criteria as the minimal length of scenarios, and its number of combinations.

A new graphical model, called improved multi fault tree, which is enough accurate to model component organizations and scenarios, is proposed for this problem. This model uses temporal operators and failure relationships to model system's behaviour in presence of multiple failures. Application of this method to the railroad piggybacking transportation system is also presented. Results obtained for a fire detection and a stowing protection system are presented. A comparison between the proposed approach and the classical dependability approach shows the benefits of this new methodology. The integration of this research in a software for designing dependable automated systems (ALoCSyS) is described.

---

**Discipline :** Automatique, Génie Informatique, Traitement du signal et Images

---

**Mots clés :** Transport multimodal - Fiabilité, Tolérance aux fautes, Optimisation combinatoire, Conception technique, Automatisation, Disponibilité, Détection de défaut

---

**Laboratoires :** INRETS-ESTAS, 20 rue Élisée Reclus, F-59650, Villeneuve d'Ascq, France
LAGIS-UMR CNRS 8146, USTL, Cité Scientifique, F-59650, Villeneuve d'Ascq Cedex, France

---