Une approche harmonisée pour l'évaluation de la sécurité des systèmes ferroviaires : de la décomposition fonctionnelle au modèle comportemental

Meriem Rafrafi

N^o d'ordre : 132

ECOLE CENTRALE DE LILLE

THESE

présentée en vue d'obtenir le grade de

DOCTEUR

en

Spécialité : Automatique et Informatique Industrielle

par

Meriem Rafrafi

Doctorat délivré par l'Ecole Centrale de Lille

Titre de la thèse :

Une approche harmonisée pour l'évaluation de la sécurité des systèmes ferroviaires

De la décomposition fonctionnelle au modèle comportemental

Soutenue le 26 Novembre 2010 devant le jury d'examen :

Rapporteur	*M. Abdellah El Moudni, Professeur, Université de Technologie de Belfort-Montbéliard*
Rapporteur	*M. Stefano Ricci, Professeur, Université de Rome « La Sapienza »*
Membre	*Mme Nathalie Duquenne, Project Officer, Agence Ferroviaire Européenne*
Membre	*Mme Nada Matta, HDR, Université de Technologie de Troyes*
Directeur de thèse	*M. El Miloudi El Koursi, Directeur, Unité de Recherche ESTAS (INRETS)*
Co-Directeur de thèse	*M. Pascal Yim, Directeur, Open Technologies*
Encadrant	*M. Thomas Bourdeaud'Huy, Maître de conférences, Ecole Centrale de Lille*

Thèse préparée au sein des Laboratoires ESTAS de l'INRETS et LAGIS de l'Ecole Centrale de Lille

ESTAS, 20 Rue Elisée Reclus, INRETS

LAGIS, UMR 8146, Ecole Centrale de Lille

École Doctorale SPI 072

Remerciements

Un moment émouvant pour le doctorant est le jour où il entreprend d'écrire ses remerciements.

Tout d'abord, cela signifie que la fin est proche, ce qui est en soi une très bonne nouvelle. Par ailleurs, cela permet de remercier toutes les personnes qui ont supporté nos humeurs dépressives au cours des années de thèse. Je tiens à saluer ici les personnes qui, de près ou de loin, ont contribué à la concrétisation de ce travail de thèse de doctorat.

Je remercie par avance ceux dont le nom n'apparaît pas dans ces remerciements et qui m'ont aidée d'une manière ou d'une autre. Ils se reconnaîtront.

Tout d'abord, mes remerciements s'adressent à la personne qui m'a proposé le sujet de thèse : M. El Miloudi El Koursi, mon directeur de thèse. Je souhaite le remercier pour sa confiance sa disponinilité et surtout son soutien inconditionnel durant ces années de thèse. Il m'a en particulier aidée à comprendre que, dans le domaine de la recherche, il est également nécessaire de faire des compromis entre l'exercice libre de l'esprit critique, que j'imaginais propre au chercheur, et la nécessité d'agir pour atteindre l'objectif fixé, propre à l'ingénieur.

Je remercie également M. Pascal Yim, mon co-directeur de thèse, et M. Thomas Bourdeaud'Huy, mon encadrant. Au travers de nos discussions, ils m'ont apporté une compréhension plus approfondie des divers aspects du sujet. Je salue aussi la souplesse et l'ouverture d'esprit qu'ils ont montrées à mon égard, en me laissant une large marge de liberté pour mener à terme ce travail de recherche.

Je les remercie particulièrement tous les trois d'avoir cru en moi et à l'aboutissement de ce travail.

Je suis très reconnaissante à M. Abdellah El Moudni et M. Stefano Ricci d'avoir accepté le rôle de rapporteur. Le regard critique, juste et avisé qu'ils ont porté sur mes travaux ne peut que m'encourager à être encore plus perspicace et engagée dans mes recherches.

Un grand merci à Mme Nada Matta et Mme Nathalie Duquenne d'avoir accepté de faire partie de mon jury et d'évaluer ce travail.

Mes chaleureux remerciements à tous mes collègues de l'INRETS - Villeneuve d'Ascq pour l'accueil familial qu'ils m'ont réservé durant mon séjour à l'INRETS. A cet égard, je tiens à exprimer ma reconnaissance à M. Gérard Couvreur, pour son soutien ainsi que les efforts qu'il a réalisés afin que j'achève mon travail dans les meilleures conditions possibles, au sein de l'Unité de Recherche ESTAS. Je tiens à mentionner le plaisir que j'ai eu à travailler au sein d'ESTAS, et j'en remercie ici tous ses membres.

Je remercie particulièrement Sana, mon amie et, comme le diraient certains, « *ma jumelle* ». Pour nos belles années de doctorantes chez les ch'tis, pour sa présence et ses encouragements, merci.
Ma gratitude s'adresse aussi à mes collègues et amis : Olivier, pour son soutien logistique ; Nathalie, pour son soutien administratif ; aini qu'à ceux qui ont été tour à tour mes collègues de bureau : Sonia, Joffrey et François. Je n'oublie pas le soutien des deux Seb, « *qui valent mieux qu'un* » !
Merci également à Bernard et Daniel pour tous les coups de main qu'ils m'ont donnés.

Cela va de soi, je remercie évidemment ma famille pour son irremplaçable et inconditionnel soutien. Ils ont été présents pour écarter les doutes, soigner les blessures et partager les joies. Cette thèse est un peu la leur, aussi. Merci Papa, Maman, Sonia et Sarra.
Enfin, ces remerciements ne seraient pas complets sans mentionner Moez qui a su me supporter pendants ces derniers mois de la thèse. Merci d'être là tous les jours.

A mes parents, perles de mon coeur...

Table des matières

Introduction Générale

On assiste dans le monde à un changement très profond de l'activité transport. Le ferroviaire n'est pas à l'écart de ce mouvement. Des directives européennes recomposent complètement ce secteur d'activité. La séparation de l'exploitation et de la gestion de l'infrastructure a tendance à augmenter le nombre d'acteurs ferroviaires. Maintenant, la déréglementation, nouvelle mutation, veut l'aider à mieux se préparer à l'Europe et à lui faire gagner des parts de marché supplémentaires. Le terrain de compétence devient en effet européen. Chaque réseau national doit être en mesure de s'adapter à ce nouvel environnement où la concurrence intramodale et intermodale, qui peut être mondiale, devient la nouvelle donne.

Il s'agit à l'évidence non pas de construire un réseau de référence qui sera constitué par une sorte de moyenne des caractéristiques des réseaux existants, mais de définir dans chaque catégorie d'utilisation les paramètres nécessaires afin de permettre aux différentes composantes du réseau ferroviaire de jouer pleinement le rôle que la société européenne attend de lui. Ces caractéristiques doivent être celles d'un réseau ferroviaire conquérant pour le vingt et unième siècle, à la fois ambitieux et réaliste.

Notre société refusant la fatalité et se caractérisant par une exigence croissante de sécurité, la tendance générale est à l'extension de la couverture des risques.

Le terme « sécurité » est probablement celui qu'on a le plus entendu, ou lu, dans les médias occidentaux depuis près de dix ans. Un véritable engouement médiatique, politique et social, s'est forgé autour de cette notion, à tel point que l'on ne sache plus, aujourd'hui, le sens exact du terme. Le résultat est que ce mythe contemporain renvoie dans l'imaginaire

du grand public directement à la notion de tranquilité et de sûreté. Néanmoins, en réalité, son sens est tout autre.

Compte tenu de l'absence des règles communes et la présence des règles, approches et cultures différentes en matière de sécurité, il était devenu difficile pour les entreprises ferroviaires de surmonter les entraves techniques et mettre en place des services internationaux ferroviaires.

Les normes de sécurité peuvent varier considérablement d'un Etat membre à l'autre. Ce facteur, ajouté aux barrières bureaucratiques, peut freiner l'exercice efficace des droits d'accès par les entreprises ferroviaires. Pour surmonter ce problème, une harmonisation communautaire des normes de sécurité a été envisagée par les autorités communautaires.

La Commission Européenne est, à cet égard, le premier décideur à avoir développé, pour le secteur ferroviaire, des spécifications techniques propres dans le but de garantir le niveau de sécurité global qu'elle a défini dans des textes de loi.

D'une économie étatique, on passe à une économie complètement libéralisée. Tels sont les grands principes édictés par les diverses directives européennes.

En vue de la création du système ferroviaire européen unique, l'adoption de la directive sur la sécurité ferroviaire est une toute première tentative faite cherchant à introduire une législation globale au niveau européen en matière de sécurité ferroviaire, et ce, en vue de parachever le cadre réglementaire dans lequel s'inscrira un système ferroviaire européen intégré.

Il est également important d'augmenter la confiance entre les acteurs en lice sur le marché, de même qu'entre les Etats membres. A cet effet, la directive introduit un mécanisme visant à adopter des Objectifs de Sécurité Communs (OSC) que devraient atteindre tous les systèmes ferroviaires ainsi que leurs différentes composantes.

Ainsi, outre la recherche de systèmes ferroviaires attractifs, le respect de la composante sécurité constitue un élément décisif pour chaque décision. En règle générale, l'évaluation de

la sécurité ne présente pas de difficultés particulières. En revanche, la tâche se complique pour nombre de décideurs lorsqu'il s'agit d'évaluer le risque spécifique d'un produit donné, tel que le transport ferroviaire, dont l'offre est extrêmement large et diverse. De plus, un quantificateur commun, autre que le niveau de sécurité global, peut s'avérer être une solution intéressante pour répondre à ce problème.

Problématique

Les systèmes complexes ferroviaires étant de plus en plus contraints par des autorités de décision placées à un haut niveau d'abstraction, il devient problématique d'imposer des critères à une autre échelle que fonctionnelle. Ainsi, dès lors que l'on descend plus bas, on se heurte à des spécificités des systèmes nationaux qui font perdre la généralité du travail des décisionnaires européens.

Le problème est qu'à chaque niveau d'abstraction, - structurel, fonctionnel ou logique - , des méthodes d'évaluation du risque existent, mais ne permettent pas de couvrir l'ensemble des niveaux de description du système. En effet, dans une vision de complétude de la méthodologie, ni les méthodes qualitatives ni les méthodes quantitatives ne permettent l'appréhension du domaine ferroviaire.

Par ailleurs, la combinaison des couches et la vision fonctionnelle du système ne prennent pas en compte l'impact des fonctions les unes sur les autres, ni le lien entre le niveau global et les composants afin d'allouer des niveaux de sécurité.

Nous proposons donc une démarche harmonisée d'évaluation du risque, capable de répartir les contraintes définies au niveau fonctionnel abstrait sur les entités qui implémentent les systèmes avec leurs spécificités.

Contribution

Notre contribution est essentiellement méthodologique puisque l'objectif de cette thèse est de proposer une méthodologie pour l'évaluation du risque. Elle part d'un modèle fonctionnel du système ferroviaire constitué en couches. Le but est de représenter le système sous forme de fonctions dont les entrées/sorties sont bien identifiées.

Une étude et comparaison des methodes d'évaluation des risques a fait que notre choix s'est porté sur les réseaux de Petri. A chaque couche de la décomposition correspond une classe de réseau de Petri. Ainsi, à la couche structurelle, nous associons les réseaux de Petri temporels ; à la couche fonctionnelle les réseaux de Petri stochastiques et enfin à la couche logique les réseaux de Petri prédicats transitions.

La méthodologie modulaire est utilisée pour évaluer le niveau de sécurité global du système. Le réseau de Petri permet en effet d'être simulé, ce qui permet de tester des hypothèses de fonctionnement et de vérifier ainsi la validation des objectifs alloués aux fonctions du système.

Ainsi, cette méthodologie d'évaluation du risque permet, à travers son modèle en réseaux de Petri, de représenter chaque module par un coefficient, afin de regrouper les modules selon des critères divers dans une démarche d'allocation d'objectifs de sécurité. Notre approche consiste à développer cette méthodologie, en reprenant la décomposition ferroviaire, et combiner un modèle hiérarchique à trois couches et un modèle modulaire.

Plan de la thèse

Pour appréhender cette problématique, le présent travail est articulé autour de trois chapitres. Les deux premiers chapitres décrivent le contexte ferroviaire d'une part et l'état de l'art scientifique de nos travauxd'autre part. Le dernier chapitre décrit notre contribution méthodologique dans une démarche d'allocation des objectifs de sécurité.

Le premier chapitre soulève le contexte industriel de l'étude : le contexte ferroviaire. Les concepts d'interopérabilité et de sécurité permettant une bonne appréhension des contraintes du domaine ferroviaire y sont exposés. Enfin, nous introduisons les normes qui régissent le domaine industriel de notre étude.

Dans le second chapitre, nous présentons d'abord les notions clés d'une manière générale et poursuivons par la présentation des critères d'acceptation du risque. Ensuite, nous introduisons les méthodes qualitatives et quantitatives pour l'évaluation des risques. Un comparatif de ces méthodes est dressé avant de clore sur la nécessité de combiner plusieurs méthodes pour une meilleure complétude de notre méthodologie.

Le troisième chapitre détaille la méthodologie proposée pour l'évaluation de la sécurité des systèmes ferroviaires. Cette méthodologie part de la décomposition ferroviaire fonctionnelle en couches. Ce modèle fonctionnel est ensuite raffiné par une approche modulaire permettant l'utilisation d'un outil unificateur : les réseaux de Petri. A chaque couche étudiée correspond une classe de réseaux de Petri. Enfin, le système global est illustré par un exemple de métro automatique.

Chapitre 1

Le ferroviaire en Europe : les contraintes normatives

Sommaire

1.1 Introduction

Afin de poursuivre les efforts visant à créer un marché unique des services de transport ferroviaire, entrepris en premier lieu par la directive 91/440/CEE du Conseil du 29 juillet 1991 relative au développement des chemins de fer communautaires (dir, 1991), il est nécessaire

d'établir un cadre réglementaire commun pour la sécurité des chemins de fer. Jusqu'à présent, les Etats membres ont mis au point leurs règles et normes de sécurité, principalement au niveau national, sur la base de concepts techniques et opérationnels nationaux. En outre, en raison de différences entre les principes, les approches et les cultures, il était difficile de surmonter les entraves techniques et d'établir des services de transport internationaux.

La directive 91/440/CEE constitue la première étape de la réglementation du marché européen des transports ferroviaires en ouvrant le marché des services internationaux de transport ferroviaire de marchandises. Toutefois, les dispositions sur la sécurité se sont révélées insuffisantes et il reste, outre les exigences en matière de sécurité, des différences qui affectent le fonctionnement optimal des transports ferroviaires dans la Communauté. Il est devenu particulièrement important d'harmoniser le contenu des règles de sécurité, la certification en matière de sécurité des entreprises ferroviaires, les tâches et le rôle des autorités de sécurité et les enquêtes sur les accidents.

Dans ce chapitre, nous présentons d'abord le besoin européen d'évaluation commune de la sécurité dans un contexte d'interopérabilité. Ensuite, notre présentation se focalisera sur les contraintes normatives qui régissent l'industrie ferroviaire.

1.2 Interopérabilité et sécurité

Afin de construire un marché intégré de transport ferroviaire, il fallait une harmonisation technique en vue d'atteindre une interopérabilité des réseaux et des matériels disparates des Etats membres. Il fallait donc introduire la concurrence, en bouleversant le régime séculaire des chemins de fer, pour qu'elle stimule les entreprises ferroviaires. Il faut noter que les initiatives d'entreprises dans le domaine des chemins de fer s'inscrivent dans le mouvement général de la libéralisation des secteurs mené par la Communauté.

La Commission Européenne (CE) a émis une série de directives qui portent sur :

- La séparation des activités de gestion des infrastructures de celles d'exploitation des trains ;
- Les conditions d'accès aux infrastructures, obtention de licence, de certificat de sécurité et de sillons ;
- L'harmonisation technique et opérationnelle, dite *interopérabilité du réseau transeuropéen à grande vitesse* ;
- L'harmonisation technique et opérationnelle, dite *interopérabilité du réseau conventionnel* ;
- La sûreté de fonctionnement de ces réseaux.

La mise en œuvre des directives qui portent sur l'interopérabilité des réseaux à grande vitesse et conventionnel a nécessité la mise en place de deux organes : le Comité Article 21 des Etats membres qui valide les travaux et l'Agence Ferroviaire Européenne (ERA - *European Railway Agency*), qui propose à la Commission et au Comité les textes réglementaires dits Spécifications Techniques d'Interopérabilité (STI) portant sur l'harmonisation technique et opérationnelle du réseau ferroviaire européen.

La première pierre de la réforme ferroviaire au niveau communautaire a été posée en 1991, avec l'adoption de la directive 91/440/CEE (dir, 1991) afin de développer les chemins de fer communautaires. Cette directive a posé quelques grands principes qui devaient contribuer à la résolution de la crise ferroviaire, à faciliter l'adaptation des chemins de fer communautaires aux exigences du marché unique et à accroître leur fiabilité. Pour ce faire, des critères d'acceptation des risques ont été mis en place par les autorités des Etats membres.

Les principes adoptés pour réorganiser le secteur ferroviaire visent à développer l'interopérabilité des systèmes, renforcer la sécurité des passagers et de l'environnement et enfin, assurer la reconnaissance mutuelle des produits et services.

Le socle de cette restructuration est constitué de deux concepts entrelacés : interopérabilité et sécurité.

1.2.1 Interopérabilité ferroviaire

L'interopérabilité dans le domaine ferroviaire désigne la possibilité de faire circuler sans entrave des trains sur des réseaux ferroviaires différents, notamment des réseaux situés dans des États différents.

Du fait de l'évolution historique du système ferroviaire, notamment sur le plan technique, les frontières nationales sont souvent des obstacles infranchissables, particulièrement pour le matériel roulant, imposant par exemple des changements de locomotives dans les gares frontières. Le cas du Danemark illustre bien cette évolution. Alors que les pays voisins (Allemagne, Suède, Norvège) avaient choisi, dès le début du XX^{me} siècle, d'électrifier leurs réseaux en courant alternatif 15 kV, 16 2/3 Hz, le réseau danois continuait son exploitation en traction thermique (d'abord vapeur puis diesel). Passant à l'électrification plus tardivement, il choisit une solution plus moderne, le courant industriel 25 kV, 50 Hz. Cette situation ne s'est pas révélée trop gênante du fait de sa situation géographique en impasse, jusqu'au moment où fut ouverte la liaison avec la Suède par le Pont de l'Oresund.

Cette situation concerne particulièrement l'Europe, du fait du morcèlement politique de ce continent. L'Union européenne s'est souciée depuis de nombreuses années d'améliorer l'interopérabilité ferroviaire afin de faciliter la création d'un grand marché du transport ferroviaire dans lequel la concurrence peut s'exercer librement. Son action s'est portée d'abord sur les lignes à grande vitesse dans la mesure où il est plus facile d'harmoniser un réseau en construction. Pour le réseau classique, l'harmonisation est une œuvre de longue haleine car les investissements sont, dans certains cas, trop élevés pour être rentables. On peut citer l'exemple du gabarit réduit du réseau britannique qui interdit au matériel continental de pénétrer en Grande-Bretagne. Le reconstruction de l'ensemble du réseau n'étant pas envisageable, seule pour l'instant la nouvelle ligne reliant Londres au tunnel sous la Manche est au gabarit préconisé par l'Union Internationale des Chemins de fer (UIC (uic)).

La question de l'interopérabilité ferroviaire comporte de nombreux aspects, dont certains sont déjà pris en charge par des organisations internationales comme l'Union Internationale

des Chemins de fer et l'Organisation intergouvernementale pour les Transports Internationaux Ferroviaires (OTIF) qui prescrivent notamment des normes techniques uniformes.

Au sein de l'Union européenne, l'interopérabilité ferroviaire concerne la conception, la construction, la mise en service, le réaménagement, le renouvellement, l'exploitation et la maintenance des éléments des systèmes ferroviaires ainsi que les qualifications professionnelles et les conditions de santé et de sécurité du personnel qui contribue à son exploitation.

Dans la directive 2001/16/CE du Parlement européen et du Conseil du 19 mars 2001 relative à l'interopérabilité du système ferroviaire transeuropéen conventionnel, elle est définie comme « *l'aptitude du système ferroviaire transeuropéen conventionnel à permettre la circulation sûre et sans rupture de trains en accomplissant les performances requises pour ces lignes. Cette aptitude repose sur l'ensemble des conditions réglementaires, techniques et opérationnelles qui doivent être remplies pour satisfaire aux exigences essentielles* » (dir, 2001).

Ainsi, l'interopérabilité est un concept à facettes multiples, qui peut être distingué selon les dimensions, les niveaux et les échelles.

Les quatre **dimensions** de l'interopérabilité sont :

- *Interopérabilité technique* : en considérant différents systèmes de transport, des relations entre eux sont possibles grâce à la similarité et la compatibilité de leurs technologies.
- *Interopérabilité organisationnelle* : c'est l'aptitude des organisations à coopérer, malgré leurs différences, pour procurer des services de transport aux utilisateurs.
- *Interopérabilité juridique* : relative à l'harmonisation des lois/directives au sein des Etats membres ou à la suppression de toute différence.
- *Interopérabilité culturelle* : relative à la réduction de l'impact de la différence sociale et des barrières régionales ou nationales pouvant exister.

Selon les modes de transport, trois **niveaux** d'interopérabilité peuvent être utilisés pour catégoriser l'interopérabilité :

- *Interopérabilité horizontale* relative à l'interopérabilité des marchés de transport individuels (opérations, infrastructure...)
- *Interopérabilité verticale* relative à l'interopérabilité entre les différents marchés (infrastructure et opérations)
- *Interopérabilité multi-modale* relative à l'interopérabilité à travers les différents modes de transport.

Enfin, les trois principales **échelles** d'interopérabilité :

- *Échelle Européenne* qui comprend non seulement l'interopérabilité entre les entreprises de même mode de transport dans des pays différents mais aussi les entreprises utilisant différents modes au sein de l'Europe.
- *Échelle Secteur* qui inclut uniquement les entreprises utilisant le même mode de transport, dans le même pays ou à l'Échelle Européenne.
- *Échelle Entreprise* qui examine l'interopérabilité entre les expériences individuelles des entreprises.

Tout compte fait, les problèmes d'interopérabilité ferroviaire sont liés aux anciennes réglementations nationales. D'un point de vue technique, elles concernent l'écartement des rails, la signalisation, l'électrification (différentes tensions et fréquences, ou absence d'électrification), la longueur des trains et le gabarit ; d'un point de vue réglementaire, l'aptitude à la conduite des trains, le contrôle des produits transportés, les horaires.

1.2.1.1 Conditions d'interopérabilité technique

Ces dernières années ont vu la mise en service de nombreux nouveaux trains à grande vitesse sur des lignes internationales. Ces liaisons transfrontalières sont réalisées en toute sécurité avec un minimum de perturbation pour l'utilisateur. Néanmois, pour la quasi-totalité de ces nouveaux trains, l'interopérabilité transfrontalière ainsi réalisée repose sur des solutions *ad hoc*, spécifiques à chaque ligne. En d'autres termes, ces nouveaux trains utilisent un type d'interopérabilité pas totalement conforme à la directive `96/48/CE` et aux STI connexes. En général, les matériels roulants utilisés sur ces lignes internationales sont spécialement

équipés pour ces liaisons, par exemple avec plusieurs systèmes de contrôle leur permettant de basculer rapidement d'un système à l'autre quand il le faut. Ces solutions *ad hoc* peuvent être génératrices de surcoûts de production. En revanche, la directive 96/48/CE et les STI connexes visent à faciliter l'harmonisation technique ultime de tout le système ferroviaire transeuropéen à grande vitesse en vue d'améliorer sa compétitivité, par exemple par l'abaissement des coûts de production, d'acceptation, d'exploitation et de maintenance.

1.2.1.2 Constituants d'interopérabilité

Les constituants d'interopérabilité et leurs caractéristiques interopérables sont déterminés par les STI. L'un des objectifs de la directive 96/48/CE et des STI connexes est de créer un marché industriel européen pour les produits ferroviaires avec la définition de constituants d'interopérabilité. Afin d'éviter la répétition inutile de procédures d'évaluation et des frais associés, les composants ou les sous-ensembles d'un sous-système nécessaires à l'interopérabilité [1], ont été définis comme des constituants d'interopérabilité.

D'une façon générale, les constituants d'interopérabilité présentent les points communs suivants :

- les caractéristiques des constituants d'interopérabilité peuvent être évaluées en se référant à une norme européenne ou à un autre document approprié, indépendamment du sous-système dans lequel les constituants seront intégrés ;
- les constituants d'interopérabilité peuvent être utilisés de façon isolée, en tant que pièces détachées, et être mis sur le marché européen par le fabricant, avant leur intégration dans un sous-système ;
- les constituants d'interopérabilité sont des éléments dont la conception peut être développée individuellement.

La qualification en tant que constituant d'interopérabilité ne dépend pas de la question de l'intégration dans un sous-système. Néanmoins, en tout état de cause, il est nécessaire de

1. fabriqués selon une conception identique en tant que produits de série, pour être vendus plus tard en quantité et être incorporés dans des sous-systèmes

vérifier si les constituants d'interopérabilité sont utilisés dans leur domaine d'utilisation.

Bien que la dimension technique d'interopérabilité soit en marche, il reste beaucoup à faire pour les autres dimensions.

1.2.1.3 Spécifications Techniques d'Interopérabilité

Les STI définissent les moyens par lesquels les sous-systèmes doivent réaliser l'interopérabilité. Pour autant, dans le but de réaliser l'interopérabilité du système ferroviaire transeuropéen à grande vitesse, chaque STI (dir, 1996) :

1. indique son champ d'application ; par exemple, la partie du réseau ou des matériels roulants, le sous-système ou la partie du sous-système ;
2. précise les exigences essentielles pour le sous-système concerné ;
3. énumère les paramètres fondamentaux du sous-système nécessaires à la satisfaction des exigences essentielles, ainsi que ses interfaces avec les autres sous-systèmes. La STI précise également les spécifications fonctionnelles et techniques à respecter par le sous-système et ses interfaces afin de réaliser des performances spécifiées pour différentes catégories de ligne, à savoir :
   - les lignes spécialement construites pour la grande vitesse,
   - les lignes spécialement aménagées pour la grande vitesse,
   - les lignes spécialement aménagées pour la grande vitesse ayant des caractéristiques spécifiques en raison de contraintes topographiques, du relief ou de l'environnement urbain ;
4. détermine les constituants d'interopérabilité et leurs interfaces qui sont nécessaires pour réaliser l'interopérabilité du système ferroviaire transeuropéen à grande vitesse dans le respect des exigences essentielles de la directive 96/48/CE. Le cas échéant, les constituants d'interopérabilité seront couverts par des spécifications européennes (dont certaines sont déjà disponibles), y compris des normes européennes ;

5. décrit, dans chaque cas envisagé, les procédures pour évaluer la conformité ou l'aptitude à l'emploi des constituants d'interopérabilité ou pour réaliser la vérification du sous-système. Cela comprend en particulier les modules appropriés définis dans la décision 93/465/CEE ou, le cas échéant, des procédures spécifiques. « *La conformité d'un constituant d'interopérabilité aux exigences essentielles qui le concernent est établie par rapport aux spécifications européennes pertinentes lorsqu'elles existent* » (dir, 1996). « *La vérification de l'interopérabilité, dans le respect des exigences essentielles, d'un sous-système de nature structurelle constitutif du système ferroviaire transeuropéen à grande vitesse est établie par référence aux* STI » (dir, 1996) ;
6. établit les modalités d'application dans certains cas spécifiques ; en particulier, des recommandations sont faites concernant le calendrier pour le passage progressif de la situation existante à la situation finale, où la conformité totale aux STI sera la règle.

Concernant leur développement, les projets des STI grande vitesse ont été préparés par l'Association Européenne pour l'Interopérabilité Ferroviaire (AEIF) sur mandat de la Commission Européenne. La Commission était assistée par un comité de réglementation composé de représentants des États membres et présidé par un représentant de la Commission, conformément à l'Article 21 de la directive 96/48/CE. Au cours de leur développement, les versions successives des STI étaient présentées au comité de réglementation, en moyenne tous les trois mois, où elles faisaient l'objet d'une analyse approfondie. À la fin de ce processus, les versions finales ont été présentées selon les règles au comité de réglementation, qui a donné, à l'unanimité, des avis favorables sur les six STI en décembre 2001.

1.2.1.4 ERTMS (*European Rail Traffic Management System*)

Dit aussi *Système de gestion du trafic ferroviaire européen*, il s'agit d'un système de contrôle commande des trains, harmonisé au niveau européen, destiné à se substituer progressivement aux systèmes de signalisation existants dans les différents pays. Les fonctions d'ERTMS sont implantées pour partie au sol, pour partie à bord des trains ; et les moyens de

communication entre sol et trains sont normalisés : communications ponctuelles par Eurobalises, communications continues par GSM-R[2].

Les principes qui ont été mis en place pour réorganiser le secteur ferroviaire visent à développer l'interopérabilité des systèmes, renforcer la sécurité des passagers, de l'environnement et enfin, assurer la reconnaissance mutuelle des produits et services. Le socle de cette restructuration est constitué du concept de la sécurité.

1.2.2 Sécurité ferroviaire

La sécurité a toujours été la préoccupation moyenne des opérateurs ferroviaires. Elle a été de la responsabilité d'opérateurs prenant en charge l'exploitation des trains et la gestion de l'infrastructure. Aujourd'hui, la séparation de l'exploitation et de la gestion de l'infrastructure a engendré d'autres éléments qu'il faut prendre en considération. En effet, il est primordial de maîtriser les risques internes, mais il faut aussi intégrer les risques partagés avec d'autres acteurs - tels qu'une nouvelle Entreprise Ferroviaire (EF) utilisant le réseau - avec des cultures *sécurité* différentes. Il est donc devenu urgent d'harmoniser le développement de la sécurité et les mesures de performance. C'est un aspect que la directive `2004/49/CE` traite à travers trois concepts fondamentaux : Méthodes de Sécurité Communes (MSC), Objectifs de Sécurité Communs (OSC) et Indicateurs de Sécurité Communs (ISC).

1.2.2.1 Méthodes de Sécurité Communes

Dites MSC, les Méthodes de Sécurité Communes sont « *les méthodes élaborées pour décrire comment évaluer les niveaux de sécurité, la réalisation des objectifs de sécurité et la conformité à d'autres exigences en matière de sécurité* » (dir, 2004a).

La MSC relative à l'évaluation et à l'appréciation des risques a pour objet de maintenir

2. Nouveau système de radiocommunications basé sur la norme GSM et destiné à remplacer la Radio Sol Train (RST) et les réseaux Maintenance Incidents Travaux (MIT) (ert)

ou d'améliorer le niveau de sécurité des chemins de fer de la Communauté (dir, 2004a). La MSC facilite l'accès au marché des services de transport ferroviaire par l'harmonisation :

1. des processus de gestion des risques utilisés pour évaluer les niveaux de sécurité et la conformité avec les exigences de sécurité ;
2. de l'échange d'informations relatives à la sécurité entre les différents acteurs du secteur ferroviaire afin de gérer la sécurité entre les différentes interfaces qui existent dans ce secteur ;
3. des preuves résultant de l'application du processus de gestion des risques.

1.2.2.2 Objectifs de Sécurité Communs

Les Objectifs de Sécurité Communs (OSC) définissent les niveaux de sécurité que doivent au moins atteindre les différentes parties du système ferroviaire [3]) et le système dans son ensemble, exprimés sous forme de critères d'acceptation des risques (dir, 2004a).

OSC et MSC sont introduits progressivement pour veiller au maintien d'un niveau de sécurité élevé et, lorsque cela est nécessaire et raisonnablement réalisable, à l'amélioration de ce niveau. Ils fournissent des outils pour l'évaluation du niveau de sécurité et des performances des opérateurs au niveau communautaire ainsi que dans les États membres.

La première série d'objectifs de sécurité communs (OSC) établie par l'ERA est relative à l'établissement d'un indicateur des personnes grièvement blessées et des personnes tuées, en fonction du type d'accident. Ces objectifs sont chiffrés à partir des données EUROSTAT qui permettent de cartographier le niveau de sécurité associé dans chaque état membre de l'Union Européenne. Par ailleurs, les Valeurs de Référence Nationales (VRN) sont également définies pour chaque catégorie des OSC représentant l'état de performance de chaque Etat membre.

3. Par système ferroviaire, nous entendons le système ferroviaire conventionnel, le système ferroviaire à grande vitesse, les tunnels ferroviaires de grande longueur ou les lignes utilisées uniquementpour le transport de marchandises.

1.2.2.3 Indicateurs de Sécurité Communs

Afin de faciliter l'évaluation de la réalisation des OSC et de permettre de suivre l'évolution générale de la sécurité des chemins de fer, les États membres collectent des informations sur les indicateurs de sécurité communs à l'aide des rapports annuels publiés par les autorités de sécurité.

La directive 2004/49/CE distingue cinq types d'ISC :

- Indicateurs relatifs aux accidents ;
- Indicateurs relatifs aux incidents survenus et aux incidents évités de justesse ;
- Indicateurs relatifs aux conséquences des accidents ;
- Indicateurs relatifs à la sécurité technique de l'infrastructure et à sa mise en oeuvre ;
- Indicateurs relatifs à la gestion de la sécurité.

1.2.2.4 Système de Gestion de la Sécurité

Toute EF et tout GI doit mettre en œuvre et maintenir un système de gestion de la sécurité (SGS ou SMS - *Safety Management System*). Ce système doit être approuvé par les Autorités Nationales de Sécurité (ANS) et comporte au moins les composantes suivantes :

1. la politique de la compagnie de chemin de fer en matière de sécurité ainsi que ses objectifs annuels de rendement en matière de sécurité et les initiatives connexes liées à la sécurité pour les atteindre, approuvés par un dirigeant supérieur de la compagnie et communiqués aux employés ;
2. les responsabilités, pouvoirs et obligations de rendre compte en matière de sécurité, exprimés clairement, à tous les paliers de la compagnie de chemin de fer ;
3. un système visant la participation des employés et de leurs représentants dans l'élaboration et la mise en œuvre du système de gestion de la sécurité de la compagnie de chemin de fer ;
4. des mécanismes visant à déterminer :

- d'une part, les règlements, règles, normes et ordres applicables en matière de sécurité ferroviaire et les procédures pour en démontrer le respect,
- d'autre part, les exemptions qui sont applicables et les procédures pour démontrer le respect, le cas échéant, des conditions fixées dans l'avis d'exemption ;

5. un processus qui a pour objet :
   - d'une part, de déterminer les problèmes et préoccupations en matière de sécurité, y compris ceux qui sont associés aux facteurs humains, aux tiers et aux modifications d'importance apportées aux opérations ferroviaires,
   - d'autre part, d'évaluer et de classer les risques au moyen d'une évaluation du risque ;
6. des stratégies de contrôle du risque ;
7. des mécanismes visant la déclaration des accidents et incidents, les analyses et les enquêtes s'y rapportant, et les mesures correctives ;
8. des méthodes pour faire en sorte que les employés et toute autre personne, - à qui la compagnie de chemin de fer donne accès aux biens de celle-ci - , disposent des compétences et de la formation appropriées et d'une supervision suffisante afin qu'ils puissent respecter toutes les exigences de sécurité ;
9. des procédures visant la collecte et l'analyse de données aux fins d'évaluation du rendement de la compagnie de chemin de fer en matière de sécurité ;
10. des procédures visant les vérifications internes périodiques de la sécurité, les examens effectués par la gestion, la surveillance et les évaluations du système de gestion de la sécurité ;
11. des mécanismes de surveillance des mesures correctives approuvées par la gestion ;
12. de la documentation de synthèse qui décrit les systèmes pour chacune des composantes du système de gestion de la sécurité.

1.3 Cadre normatif de la sécurité des systèmes

Dans le contexte industriel, la norme internationale de sécurité IEC 61508 (CEI, 2000) est une des dernières normes dédiées à la sécurité fonctionnelle.

Elle est devenue une norme française en 1999. Les normes filles, que cette norme de base a générées, sont plus récentes et restent encore assez peu connues des acteurs de la sécurité dans certains secteurs industriels français. Cet ensemble normatif s'impose comme la référence pour le développement, la mise en œuvre et l'exploitation des systèmes relatifs aux applications de sécurité.

1.3.1 Norme IEC 61508

La norme IEC 61508 (CEI, 2000) est une norme internationale qui porte plus particulièrement sur la sécurité fonctionnelle des systèmes Electriques/Electroniques/Electroniques Programmables concernés par la sécurité (E/E/PE).

La norme propose une approche opérationnelle pour mettre en place un système de sécurité E/E/PE, en partant de l'étude des exigences de sécurité (avec une définition du périmètre couvert, une analyse et une évaluation du risque) et en prenant en compte toutes les étapes du cycle de vie du système E/E/PE (Redmill, 1998).

Un des intérêts de cette norme est d'être générique et donc d'être applicable dans tous les secteurs où la sécurité peut être traitée avec des systèmes E/E/PE : industries manufacturières, industries des processus continus, pharmaceutiques, nucléaires, ferroviaires, *etc.*

L'IEC 61508 a été approuvée par le CENELEC en tant que norme européenne (EU - *European Norm*). Ceci signifie qu'elle doit être publiée en tant que norme nationale par chaque organisation de normalisation nationale (Brown, 2000). C'est chose faite en France par l'AFNOR depuis 1999, date de création de la NF 61508. Cela signifie également que tous les textes nationaux incompatibles avec l'IEC 61508 doivent être abrogés. Cependant, il n'y

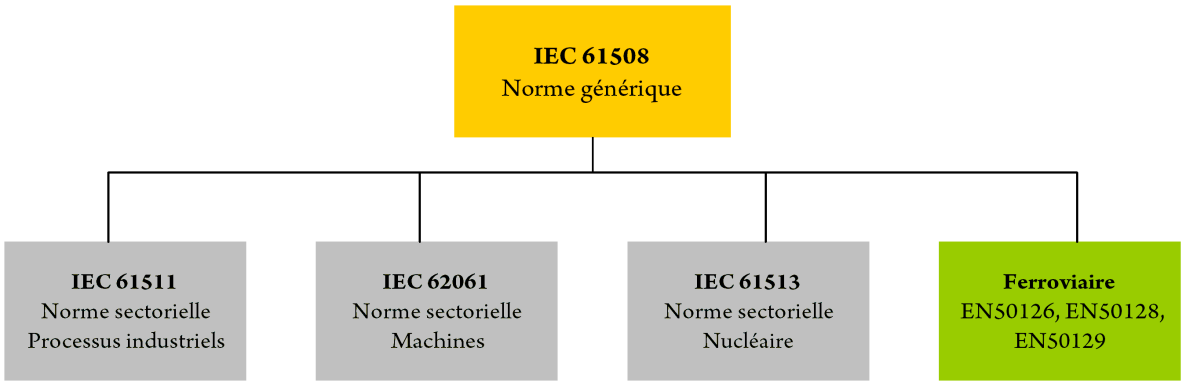

FIGURE 1.1: L'IEC 61508 et ses normes sectorielles

a pas d'obligation légale de se conformer aux normes européennes. Ceci signifie que le fait que la norme soit une norme européenne n'implique pas en soit qu'il existe une obligation légale de conformité à l'IEC 61508.

Il convient de noter que l'IEC 61508 n'a pas le statut de norme harmonisée européenne et que donc, aucune directive européenne de la commission n'y fait référence. Ceci est dû partiellement au fait que le périmètre de l'IEC 61508 inclut la totalité du cycle de vie et dépasse de loin le périmètre d'une norme associée à une directive produit [4]. Cependant, cela n'empêche pas d'utiliser la conformité à certaines parties de la norme pour supporter la déclaration de conformité avec une directive européenne produit si cela est approprié. Néanmoins, puisque l'IEC 61508 n'est pas une norme harmonisée, il n'y a pas de présomption de conformité avec quelque directive que ce soit. Il serait donc nécessaire d'expliquer dans le dossier technique d'un produit en quoi la conformité à l'IEC 61508 supporte la conformité avec des exigences essentielles d'une directive particulière.

La norme IEC 61508 est générique. Les normes sectorielles qui en sont issues sont totalement compatibles. Ceci signifie qu'il ne faut pas penser trouver une réduction du périmètre fonctionnel ou des entorses aux principes de bases de l'IEC 61508 dans ses normes filles. Les normes sectorielles (*cf.* Figure 1.1) ne font que préciser les modalités d'application.

4. Le concept de norme européenne *harmonisée* s'applique aux directives européennes pour des produits. Ceci signifie que la conformité à la norme vaut présomption de conformité aux *exigences essentielles* de la directive

1.3.1.1 Structure de la norme

L'IEC 61508 est constituée de 7 parties :

- IEC 61508-1, Exigences générales,
- IEC 61508-2, Exigences pour les systèmes E/E/PE concernés par la sécurité,
- IEC 61508-3, Exigences pour le logiciel,
- IEC 61508-4, Définitions et abréviations,
- IEC 61508-5, Exemples de méthodes pour la détermination des niveaux d'intégrité de sécurité (SIL),
- IEC 61508-6, Directives pour l'application de l'IEC 61508-2 et de l'IEC 61508-3,
- IEC 61508-7, Vue d'ensemble des mesures et des techniques.

1.3.1.2 Objectifs

Selon (CEI, 2000), la norme internationale IEC 61508, a pour but de :

- fournir le potentiel de technologie E/E/PE pour améliorer à la fois les performances économiques et en termes de sécurité,
- permettre des développements technologiques dans un cadre global de sécurité,
- fournir une approche système, techniquement saine, suffisamment flexible pour le futur,
- fournir une approche basée sur le risque pour déterminer les performances des systèmes concernés par la sécurité,
- fournir une norme générique pouvant être utilisée par l'industrie, mais qui peut également servir à développer des normes sectorielles ou des normes produit,
- fournir les moyens aux utilisateurs et aux autorités de réglementation d'acquérir la confiance dans les technologies basées sur l'informatique,
- fournir des exigences basées sur des principes communs pour faciliter :

  [label=•]une compétence améliorée de la chaîne d'approvisionnement des fournisseurs de soussystèmes et de composants à des secteurs variés, des améliorations de la communication et des exigences (c'est-à-dire de clarifier ce qui doit être spécifié),

le développement de techniques et de mesures pouvant être utilisées par tous les secteurs, augmentant de ce fait la disponibilité des ressources, le développement des services d'évaluation de la conformité si nécessaire.

Malgré ces objectifs, l'IEC 61508 ne couvre pas les précautions qui peuvent se révéler nécessaires pour empêcher des personnes sans autorisation d'endommager et/ou d'affecter la sécurité fonctionnelle réalisée par les systèmes E/E/EP concernés par la sécurité, notamment les intrusions dans les réseaux.

1.3.1.3 Evaluation des niveaux d'intégrité de sécurité

L'IEC 61508 spécifie 4 niveaux possibles de performance de la sécurité pour une fonction de sécurité. Ils sont appelés *niveaux d'intégrité de la sécurité* (SIL - Safety Integrity Level).

Le niveau d'intégrité de sécurité 1 (SIL1) est le plus bas niveau d'intégrité de la sécurité et le niveau d'intégrité de sécurité 4 (SIL4) est le niveau d'intégrité de la sécurité le plus élevé (Beugin, 2006). La norme détaille les exigences nécessaires pour atteindre chaque niveau d'intégrité de la sécurité. Ces exigences sont plus sévères aux niveaux d'intégrité de la sécurité les plus élevés de manière à garantir une probabilité de défaillance dangereuse plus basse.

Ainsi, la désignation SIL, apposée à un système, renvoie automatiquement sur des fonctions du système E/E/EP, pour être ensuite étendue, par conception, aux composants matériels et/ou logiciel qui participent aux fonctions.

L'expression et la signification du niveau d'intégrité de sécurité en termes de probabilité de défaillance sont différentes selon que le mode de demande du système de sécurité est :

- *faible :* la fréquence des demandes de fonctionnement sur le système de sécurité est inférieure à une par an et au plus égale à deux fois la fréquence des tests périodiques (*cf.* Tableau 1.1).
- *élevé ou en mode continu :* la fréquence des demandes de fonctionnement sur le système de sécurité est plus grande que une par an ou supérieure à deux fois la fréquence des tests périodiques (*cf.* Tableau 1.2).

SIL	**Probabilité de défaillance moyenne cible d'une sollicitation**
4	$[10^{-5}, 10^{-4}]$
3	$[10^{-4}, 10^{-3}]$
2	$[10^{-3}, 10^{-2}]$
1	$[10^{-2}, 10^{-1}]$

Tableau 1.1: Fonctionnement en mode sollicitation

SIL	**Probabilité cible des défaillances dangereuses pour exécuter la fonction instrumentée de sécurité (par heure)**
4	$[10^{-9}, 10^{-8}]$
3	$[10^{-8}, 10^{-7}]$
2	$[10^{-7}, 10^{-6}]$
1	$[10^{-6}, 10^{-5}]$

Tableau 1.2: Fonctionnement en mode continu

Ainsi, le niveau d'intégrité de sécurité renvoie automatiquement sur une fonction d'un système, qui elle-même renvoie automatiquement sur des matériels ou des logiciels, et ceci, bien évidement dans le cas de systèmes E/E/EP. On parlera donc d'intégrité de sécurité d'une fonction, d'intégrité de sécurité d'un matériel et d'intégrité de sécurité d'un logiciel, où :

- l'intégrité de sécurité du matériel revient à définir la partie de l'intégrité de sécurité du système liée aux défaillances aléatoires du matériel qui pourraient mener à un évènement dangereux.
- l'intégrité de sécurité du logiciel revient à définir la probabilité pour qu'un logiciel, dans un système électronique programmable, exécute ses fonctions de sécurité dans toutes les conditions spécifiées.

Dans le but de pouvoir mettre en œuvre les démarches décrites dans la norme IEC 61508, dans le domaine du ferroviaire, trois normes ont étés créées : la norme EN50126, EN 50128 et EN 50129.

1.3.2 Normes EN 50126/50128/50129

La mise en service d'un système dans le domaine du transport ferroviaire, urbain ou non, est liée à la mise en œuvre du référentiel CENELEC (EN50126, EN 50128 et EN 50129). Ce référentiel couvre les aspects système, matériel et logiciel. Les normes EN50129 et EN50128 bien qu'applicables au sous-système de signalisation, sont considérées comme applicables par les clients en l'absence d'autre référence.

1.3.2.1 La norme EN 50126 - « Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité »

Cette norme permet de mettre en œuvre une démarche cohérente de gestion de la *Fiabilité, Disponibilité, Maintenabilité et Sécurité* appelée FDMS (CENELEC, 2000). Elle peut être appliquée dans le ferroviaire tout au long du cycle de vie car elle intègre les exigences FDMS spécifiques à ce domaine.

1.3.2.2 La norme EN 50128 - « Systèmes de signalisation, de télécommunication et de traitement »

Cette norme traite en particulier des méthodes qu'il est nécessaire d'utiliser pour fournir des logiciels répondant aux exigences d'intégrité de la sécurité appliquées au domaine du ferroviaire. L'intégrité d'un logiciel est répartie sur quatre niveaux SIL, allant de SIL 1 à SIL 4. Ces niveaux SIL sont définis par association, dans la gestion du risque, de la fréquence et de la conséquence d'un événement dangereux. Afin de définir précisément le niveau de SIL d'un logiciel, des techniques et des mesures sont définies dans cette norme (CENELEC, 1998).

1.3.2.3 La norme EN 50129 - « Applications ferroviaires - Systèmes électroniques de sécurité pour la signalisation »

Cette norme aborde tous les points liés au processus d'approbation des systèmes individuels, qu'ils soient logiciels ou matériels, et qui peuvent exister dans le cadre d'un système global (CENELEC, 1999). Elle définit les preuves à fournir pour l'acceptation de chaque système individuel en fonction de son niveau d'intégrité SIL.

Les exigences définies dans ces normes constituent l'origine du concept d'évaluation et d'acceptation des risques.

1.4 Conclusion

Ce chapitre a présenté le contexte ferroviaire, avec un rappel de ses besoins naissants d'interopérabilité et de sécurité croissante.

Face au nouveau contexte ferroviaire d'harmonisation et dans une ère de plus en plus exigente au niveau des performances, tant les réglementations que les normes européennes insistent sur le besoin d'une évaluation commune. Cependant, les implémentations actuelles demeurent spécifiques à chaque Etat membre et la définition d'une démarche progressive pour l'harmonisation de l'évaluation d'un objectif de sécurité global est *a priori* la solution adoptée par les acteurs ferroviaires européens.

Dans le chapitre qui suit, nous nous intéressons à la notion d'acceptation des risques qui constitue la garantie de la sécurité, en application des directives, et le complément de la structure fonctionnelle du système ferroviaire.

Chapitre 2

Evaluation des risques

Sommaire

2.1 Introduction

L'évaluation des risques est un processus intégrant plusieurs activités essentielles pour la sécurité. Cependant, les notions de sécurité et de risque sont nuancées, et il se trouve que ces termes sont employés pour désigner la même chose. Nous avons donc jugé important de définir les notions de base pour l'évaluation des risques en s'inspirant essentiellement des normes de la sûreté de fonctionnement.

Dans ce chapitre, nous essayons de lever certaines ambigüités relatives aux notions de système complexe, danger, sécurité et risque, notions de base pour appréhender notre problématique. Ensuite, compte tenu de la complémentarité des différentes méthodes d'évaluation des risques réputées, il est nécessaire, avant de porter l'étude sur l'une d'entre elles, de présenter un panorama synthétique des différentes méthodes applicables. Enfin, nous établissons un comparatif de ces méthodes afin de définir les orientations choisies pour la suite de notre travail.

2.2 Notions de base

2.2.1 Système complexe

La notion de complexité tire son origine de travaux de recherche passés, remontant à près d'un demi-siècle, et en cours visant à établir des théories explicatives sur les systèmes issus des disciplines comme les sciences de la vie, les sciences de la nature, les sciences de l'ingénierie, les sciences sociales...

Un système qualifié de complexe se rapporte à l'incapacité de décrire et de déduire le comportement de ce système compte tenu du nombre d'éléments qui le constituent et de la nature

et de la variété des interactions entre ces éléments (rétroactions, régulations, contrôles...). Ainsi, pour Morin (Morin, 1994), la complexité se manifeste par les traits de l'inextricable, du désordre, de l'ambiguïté, de l'incertitude. Dès lors, toute tentative de décomposition d'un système complexe consisterait en une simplification de ce système.

Les systèmes compliqués, au contraire, sont susceptibles d'être décomposés analytiquement et réduits en plusieurs éléments simples permettant ainsi d'obtenir la connaissance totale des propriétés du système.

L'organisation des parties d'un système complexe marque de surcroît la différence entre systèmes complexes et systèmes compliqués, ces derniers s'organisant ou plutôt se structurant par niveaux hiérarchiques. Dans un système complexe, de la mise en relation des différentes parties du système, se dégagent de nouvelles propriétés que les parties n'ont pas à l'origine.

2.2.2 Notion de danger

2.2.2.1 Définitions

Selon la norme de sécurité IEC 61508 (CEI, 2000), le danger désigne « *une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes* ». En d'autres termes, les dangers peuvent avoir une incidence directe sur les personnes, par des blessures physiques ou des troubles de la santé, ou indirecte, au travers de dégâts subis par les biens ou l'environnement.

Le référentiel OHSAS 18001 (OHSAS, 1999), quant à lui, définit le danger comme une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments.

Soulignons que de nombreux termes sont employés, selon les normes ou les auteurs, autour de la notion de danger et la rendent ambiguë. De plus, les dictionnaires associent souvent le terme danger au terme risque, ce qui explique le fait qu'un grand nombre de personnes utilisent indifféremment ces termes.

Dans le cadre de ROSA (*Rail Optimisation Safety Analysis*), un projet réalisé dans le cadre de DEUFRAKO (coopération franco-allemande), l'objectif était de dresser une liste complète et générique de dangers couvrant l'exploitation normale d'un système ferroviaire. La finalité et la difficulté consistaient à définir ces dangers au niveau de détail le plus élevé possible sans refléter les spécificités des chemins de fer français et allemands. La liste (*cf.* Annexe **??**) a été créée à partir de listes de dangers existants en provenance des deux pays (SNCF et DB) et vérifiée en utilisant des listes de dangers en provenance d'autres pays. Malgré l'objectif déclaré d'être complète et générique, la liste n'est donnée ici qu'à titre d'exemple indicatif susceptible d'aider les acteurs chargés d'identifier les dangers d'un projet particulier. Il faut probablement s'attendre à ce que les dangers repris dans cette liste doivent être précisés ou complétés pour refléter les particularités de chaque projet.

Les dangers identifiés dans ROSA et présentés en Annexe D sont appelés « dangers de départ » (SPH - *Starting Point Hazards*), c'est-à-dire qu'il s'agit de dangers sur la base desquels des analyses des causes et des conséquences pourraient être réalisées afin de déterminer les mesures/barrières de sécurité et les exigences de sécurité pour maîtriser les dangers.

2.2.2.2 Situations dangereuses

Une situation dangereuse désigne une situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs phénomènes dangereux.

Dans (Desroches *et al.*, 2006), la situation dangereuse, notée SD, est définie comme une résultante de la conjonction d'un danger (D) et d'un événement contact (EC) qui met le système en présence ou au contact du danger. Cette configuration de l'état du système en présence de danger est modélisée par l'expression 2.1.

$$SD = D \cap EC \tag{2.1}$$

La situation à risque est définie par la nature, le potentiel de dangérosité et la vrai-

semblance de ce potentiel. De même, l'évènement redouté final ou accident (A) résulte de la conjonction de la situation dangereuse et d'un évènement amorce (EA) qui déclenche la dangérosité sur le ou les éléments vulnérables du système. Cette configuration accidentelle est modélisée par l'expression 2.2.

$$A = SD \cap EA = D \cap EC \cap EA \tag{2.2}$$

La gravité des conséquences directes et indirectes de l'accident, notée $G(A)$ correspond au montant des dommages en termes de perte ou préjudice mesurable.

2.2.2.3 Evènement redouté

Nous allons appeler évènement 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) (Schoenig et Aubry, 2004).

Un évènement redouté peut désigner une des situations suivantes :

- *évènement indésirable* : c'est un évènement 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.
- *évènement critique* : c'est un évènement 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.
- *évènement catastrophique* : c'est un évènement 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 évènements qualifiés de catastrophiques sont surtout exploités dans l'aéronautique et dans le ferroviaire.

Vue que la notion de danger est fortement liée à la notion de risque, il convient de définir cette notion complémentaire et indissociable du danger.

2.2.3 Notion de risque

Il serait bon d'expliquer la différence entre un danger et un risque parce que les deux termes tendent à être utilisés sans distinction et sans que leur sens précis ne soit bien compris – même certains dictionnaires définissent le terme danger comme un risque. Il y a, cependant, une importante différence sémantique entre ces deux mots.

En effet, contrairement au danger, qui est susceptible d'occasionner une blessure, un risque représente la probabilité que le danger occasionne une blessure dans les conditions régnantes. Le risque dépend donc de la façon dont les dangers sont traités ou contrôlés.

2.2.3.1 Définitions

Le risque est défini comme la « *probabilité que les effets dommageables surviennent réellement* ». Cette formulation met explicitement en avant le double aspect du risque, à savoir : le caractère aléatoire d'un événement assorti de la menace qu'il représente. De fait, il faut éviter de focaliser la notion de risque sur la seule gravité des accidents survenus : ce serait négliger la composante aléatoire des événements dont on peut dire d'emblée qu'elle est généralement - et heureusement - inversement proportionnelle aux dégâts causés.

Ceci conduit à considérer le risque sous un double aspect : *risque = aléa + vulnérabilité* :

- l'aléa correspond à la fréquence ou à la probabilité d'occurrence d'un évènement d'intensité donnée ;
- la vulnérabilité représente la gravité des conséquences de l'événement sur l'ensemble des entités exposées (vies humaines, richesses, environnement).

Le risque est donc la caractéristique d'un évènement, défini conjointement par sa vraisemblance d'occurence et la gravité de ses conséquences. C'est donc une variable à deux

dimensions : ce n'est ni une probabilité ni une gravité mais les deux à la fois. Cette caractéristique fait que la comparaison de deux risques n'est formellement possible que si chacune de ses deux dimensions, probabilité et gravité des conséquences, vérifie la même relation d'ordre.

En sécurité des systèmes, on définit un risque (g, p) comme la probabilité de survenance, p, d'un évènement redouté dont la gravité des conséquences dépasse un seuil de gravité, g, dans des conditions données.

Risque acceptable Un risque est acceptable s'il est conforme aux objectifs du référentiel d'acceptabilité. C'est la caractéristique d'un risque résultant d'une décision explicite établie de façon objective par comparaison avec des risques connus et admis, dans d'autres branches d'activité.

Risque résiduel C'est le risque subsistant après l'application des actions de réduction des risques. Ces dernières peuvent agir sur la gravité si c'est une action de protection et sur la probabilté du risque dans le cas d'une action de prévention.

Le risque résiduel dépend de :

- l'efficacité évaluée et consolidée des actions en réduction du risque par l'analyse de leur potentiel de défaillance,
- l'efficacité consolidée de leur application sur le terrain.

Action de protection Une action de protection a pour but de minimiser la *gravité des conséquences* de l'apparition d'un évènement redouté (Beugin, 2006). Elle constitue donc une barrière de sécurité visant à diminuer la gravité des dommages consécutifs à l'occurence de l'évènement redouté afin de rendre le risque résiduel acceptable.

Action de prévention Une action de prévention est une action prévisionnelle sur le système ou son exploitation et qui a pour but d'éliminer ou minimiser la *probabilité d'apparition* d'un évènement redouté (Beugin, 2006).

Autrement dit, une mesure de prévention est une barrière de sécurité visant à diminuer la probabilité d'occurence de l'évènement redouté afin de rendre le risque résiduel acceptable.

2.2.3.2 Classification des risques

Risque individuel C'est le risque pour une personne individuelle de subir un dommage dépendant du lieu. Egalement désigné en tant que risque lié à un lieu, il est exprimé en termes de probabilités.

Selon Desroches (Desroches *et al.*, 2006), le risque individuel est un évènement portant préjudice à un individu (ou un groupe restreint d'individus) indépendamment de toute autre considération liée à son appartenance à une collectivité. Chaque individu soumis à un risque le perçoit comme un risque individuel même si c'est la collectivité entière qui est exposée.

Un risque à impact rapide peut être considéré comme un risque individuel.

Risque collectif C'est le risque pour toutes les personnes impliquées, susceptibles de subir un dommage. Vis-à-vis d'un risque collectif, on ne considère pas séparément les personnes exposées mais leur ensemble en tant que communauté exposée. Le risque collectif est généralement associé, à tort, à une fréquence faible et une *gravité* élevée (Desroches *et al.*, 2006).

Risque environnemental Dans ce domaine, la directive 96/82 du 9 décembre 1996, dite SEVESO II, est souvent considérée comme référence. Ayant la particularité de s'appliquer dans une logique à deux niveaux en distinguant les établissements à risque faible et les établissements à risque élevé, elle introduit des évolutions substantielles. En effet, elle met l'accent sur la protection de l'environnement en introduisant, pour la première fois, dans son champ d'application les substances considérées comme dangereuses pour l'environnement, notamment les substances aquatoxiques. De nouvelles exigences portant notamment sur les systèmes de gestion de la sécurité, sur les plans d'urgence, sur l'aménagement du territoire

ou sur le renforcement des dispositions relatives aux inspections ou à l'information du public ont été incluses.

2.2.4 Notion de sécurité

La norme EN50126 (CENELEC, 2000) définit la sécurité comme étant « *l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à l'environnement, pendant le déroulement d'une activité* ».

Cependant, la notion de risque inacceptable est une notion très ambiguë. En effet, où se situe la limite de ce qui doit, ou non, être accepté ? A partir de quel moment une situation devient-elle inacceptable ? Afin de tenter de préciser la notion de risque inacceptable, on peut se référer à la Commission Européenne qui s'est appuyée sur le principe de précaution.

Le principe de précaution a vocation à couvrir toutes les hypothèses où les données scientifiques sont insuffisantes, peu concluantes et incertaines mais où il y a des motifs raisonnables de penser que les effets potentiellement dangereux sur la personne soient incompatibles avec le niveau de protection voulue.

Le périmètre de la notion de « *risque inacceptable* » reste flou, malgré les précisions de la Commission. La détermination d'un tel risque relève d'une application *in concreto*, appartenant aux autorités des Etats membres, à charge pour eux d'appliquer le principe de précaution.

2.2.4.1 Définitions

Fonction de sécurité La fonction de sécurité est une fonction devant être implémentée dans les systèmes Electriques/Electroniques/Electroniques Programmables (E/E/PE) concernés par la sécurité. Son principal objectif est d'atteindre ou de maintenir un état sûr pour les équipements contrôlés, dans le cadre d'un évènement dangereux particulier.

Sécurité des systèmes La sécurité des systèmes, quant à elle, est la caractéristique d'un système exprimée par l'aptitude ou la probabilité que le système accomplisse sa mission en l'absence de circonstances susceptibles d'occasionner des nuisances aux personnes, biens et environnement.

La sécurité du système est atteinte si l'état dans lequel le risque de dommages corporels ou matériels est limité à un niveau acceptable au regard d'objectifs préalablement établis.

2.2.4.2 Objectif de sécurité

Depuis dix à quinze ans, de nombreux objectifs quantifiés de sécurité ont été proposés et utilisés pour aider à des prises de décision tant pour la conception que pour l'exploitation.

Un objectif de sécurité est une limite d'acceptation que l'on souhaite atteindre vis-à-vis d'un risque.

Il comporte trois éléments :
- la définition de l'environnement de référence et des situations du système à considérer ;
- la définition précise de l'évènement redouté et du niveau du paramètre associé ;
- la définition de la borne supérieure de probabilité de survenance de ce niveau (probabilité acceptable).

Après la définition de ces trois éléments, un objectif de sécurité se définit comme l'expression qualitative ou quantitative de la probabilité acceptable d'occurence d'un évènement redouté, choisi en fonction de sa gravité pour un environnement de référence. Choisir un objectif de sécurité revient donc à accepter un risque résiduel.

Ceci implique que :
- chaque évènement redouté soit convenablement identifié ; sans oublier que chaque objectif doit être spécifié assez tôt dans le projet de développement du système afin d'orienter les travaux en conséquence ;
- chaque probabilité acceptable d'occurence soit établie en concertation entre l'utilisateur et/ou le réalisateur du système, en présence d'experts sécurité ;

– l'environnement de référence soit correctement spécifié afin d'éviter qu'il influence le niveau de sensibilité du système ainsi que le niveau de gravité des conséquences.

Le passage d'un objectif de sécurité de niveau donné en objectifs de niveaux inférieurs est réalisé en utilisant des méthodes d'allocation. Le problème qui se pose en décomposant un objectif en différents niveaux est alors une multiplication des sous-objectifs incompatibles avec les moyens financiers et techniques disponibles.

En outre, les objectifs de sécurité permettent de spécifier les attentes aussi bien à l'échelle sous-systémique qu'à l'échelle du système global. Ils se rapportent à des exigences qui sont soit qualitatives (exigences sur les effets environnementaux, par exemple), soit quantitatives (exigences de fréquences de défaillances des systèmes assurant la sécurité, par exemple). Dans ce dernier cas, ils peuvent être spécifiés par des critères de sûreté de fonctionnement ou être directement assimilés aux critères d'acceptation du risque tels que des mesures quantifiant les préjudices subis par des personnes impliquées dans un accident ou subis par l'environnement (Kumamoto *et al.*, 1996). Ces objectifs quantitatifs peuvent intégrer une part d'incertitude qui est susceptible d'affecter le processus de prise de décision concernant l'acceptation ou non du risque (Hoegberg, 1998).

Ces notions de danger, risque et sécurité ont depuis longtemps retenu l'attention des industriels. Cependant, en europe, pour chaque Etat Membre, ces trois concepts ont des poids et impacts différents dans l'acceptabilité des risques.

2.3 Acceptabilité des risques

Pour un individu, une technologie est acceptable si elle génère un équilibre acceptable entre coûts et bénéfices. Tous les jours, les gens adoptent des lignes de conduite dont les conséquences peuvent comporter des risques. Selon Fischhoff (Fischhoff et Fischoff, 2001), « *si les gens adoptent une ligne de conduite, et décident par exemple de prendre leur voiture*

pour se rendre quelque part, en connaissant les risques que cela suppose, on peut dire que ces risques sont acceptables, dans le contexte des autres conséquences de cette action ». Autrement dit, il souligne que ces individus peuvent choisir des lignes de conduite plus risquées, comme par exemple le fait de décider de doubler une voiture plus lente ; le risque peut donc être interprété comme une valeur relative dépendant de la recherche d'un équilibre entre les coûts et les bénéfices spécifiques à un contexte donné. Par conséquent, « *un degré de risque acceptable pour une activité peut sembler terriblement élevé ou exceptionnellement faible dans d'autres contextes* ».

Indépendamment de leur définition réelle, les critères d'acceptabilité des risques doivent remplir les exigences suivantes pour pouvoir apporter la preuve de la nécessité de mesures :

- application de critères d'acceptation quantitatifs ;
- harmonisation des critères d'acceptation avec d'autres domaines de l'évaluation des risques.

2.3.1 Diagramme d'acceptabilité des risques

Le diagramme d'acceptabilité des risques illustre les zones des risques acceptés, tolérables et inacceptables à partir des données relatives aux classes de gravité et probabilité. Ce diagramme peut prendre deux formes : soit un graphe soit un tableau.

Dans une représentation sous forme de graphe, il s'agit de la *courbe de Farmer*. Par contre, dans le cas d'une représentation en tableau, la *matrice des risques* est établie.

2.3.1.1 Courbe de Farmer

Dans le cas d'une représentation en graphe, le diagramme d'acceptabilité des risques ou *courbe de Farmer* montre la séparation entre les domaines des risques acceptables de ceux des risques inacceptables. Les gravités des conséquences des risques sont placées en abscisses

et sont regroupées par classe comme illustré dans la Figure 2.1 ; alors que les fréquences ou probabilités sont placées en ordonnées.

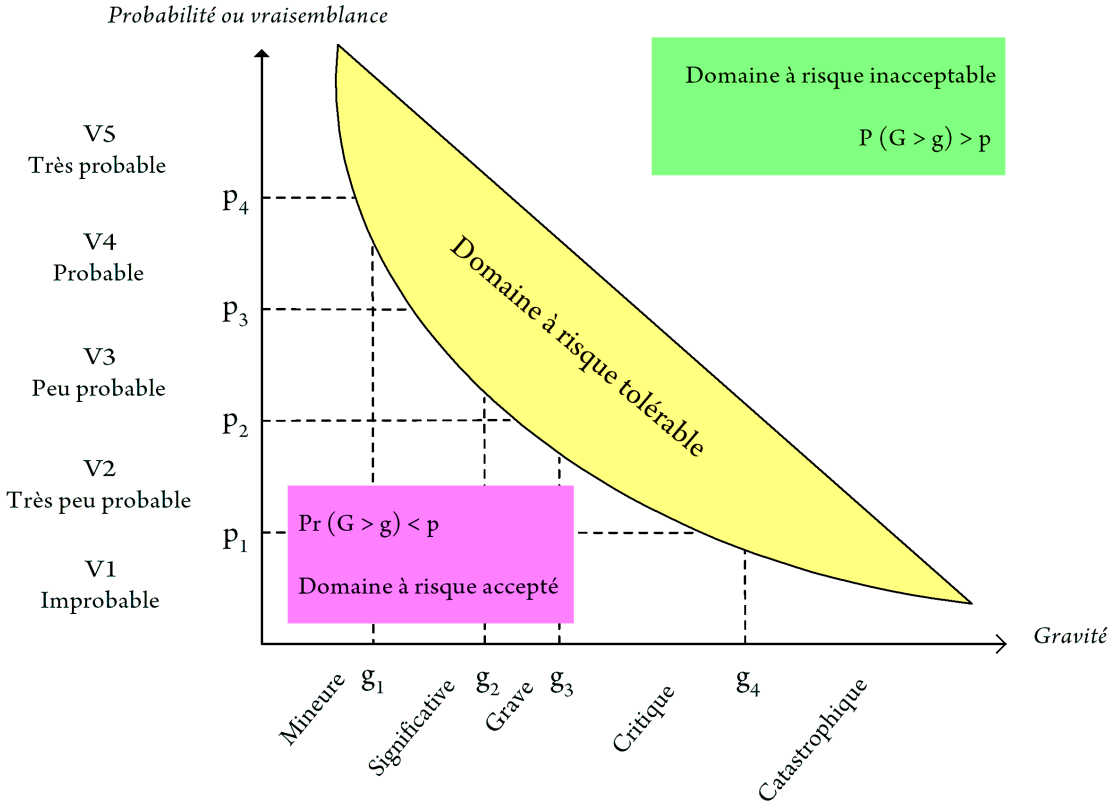

FIGURE 2.1: Diagramme de Farmer

Cette courbe est représentée par la relation 2.3.

$$P(G \geq g) = p \tag{2.3}$$

où g est un seuil maximum de gravité acceptable et p la fréquence ou probabilité associée.

La gravité G peut être définie de façon qualitative par la définition des évènements redoutés associés à chaque classe ou quantitativement par la valeur g du seuil de gravité.

La courbe d'acceptabilité des risques visualise l'ensemble des couples (g, p) respectant cette relation. Il en résulte qu'un risque est incacceptable si et seulement si $P(G \geq g) > p$. L'ensemble des couples respectant cette relation forme le *domaine à risque acceptable*. De

même, il en résulte qu'un risque est inacceptable si $P(G \geq g) < p$. L'ensemble des couples respectant cette relation forme le *domaine à risque acceptable*.

2.3.1.2 Matrice des risques

La matrice des risques est une méthode élargie de l'évaluation du risque. Elle convient aussi bien à la gestion des risques pour des organisations (entreprises, organisations à but non lucratif) que pour des systèmes (produits, prestations, processus, projets).

La méthode de la matrice des risques a pour objectif d'identifier les principaux scénarios de risques d'un système donné et de constituer un portefeuille de risques selon la catégorie de probabilité et de conséquences. A cet effet, un seuil de tolérance de risques est souvent indiqué dans le paysage des risques. On pourrait donc dire que les risques qui sont situés au-delà de ce seuil ne doivent pas être tolérés ; par contre, ceux qui sont situés sous ce seuil sont acceptables.

Contrairement à la méthode du diagramme de Farmer qui ne prend en compte qu'une fonction de sécurité, la matrice de gravité des risques intègre plusieurs fonctions de sécurité sous réserve de leur indépendance.

La méthode de la matrice des risques utilise une matrice des risques bidimensionnelle qui est couramment employée dans le domaine des transports guidés (Schäbe, 2001). En spécifiant une zone d'acceptation des risques dans un tableau de criticité (*cf.* Figure 2.2), cette matrice permet l'analyse d'un événement dangereux compte tenu de sa fréquence d'occurrence et de la gravité de ses conséquences.

2.3.2 Risque et enjeux

Dans le secteur des transports, les accidents engendrent de nombreuses conséquences négatives : des pertes de capacités productives, des coûts directs liés au traitement des

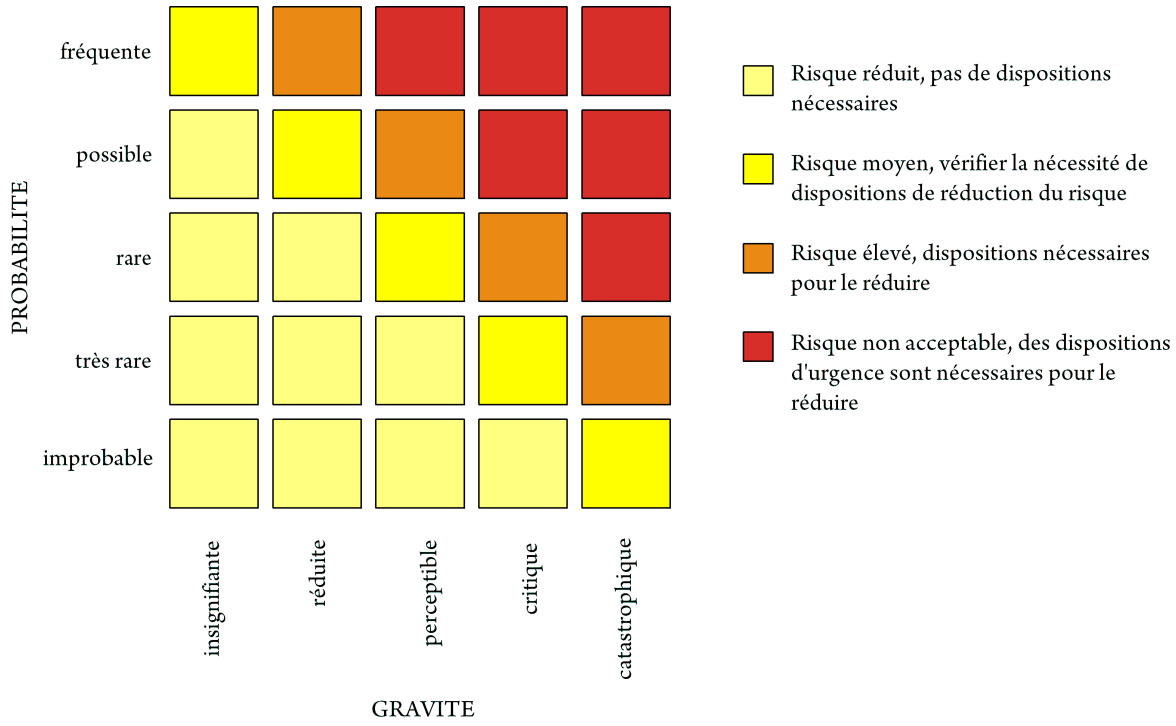

FIGURE 2.2: Matrice des risques

accidents et, ce qui est à la fois important et difficile à apprécier, des coûts très lourds en termes de souffrances physiques et morales pour les victimes et leurs proches.

L'évaluation de l'ensemble de ces coûts s'impose à plusieurs titres, ne serait-ce que pour établir l'étendue des conséquences monétaires ou monétarisables des accidents, et apprécier leurs poids relativement à d'autres coûts auxquels la société doit faire face. Il s'agit donc de disposer d'une valeur susceptible d'être utilisée dans le secteur des transports pour évaluer de façon cohérente diverses options d'investissement présentant des impacts différents sur la sécurité, et faire en sorte que l'utilisation des ressources disponibles soit la plus efficiente possible. Il s'agit moins à cette fin de déterminer la valeur en soi de la vie humaine, tâche bien délicate, que de fixer un montant tutélaire que la collectivité acceptera implicitement ou explicitement de prendre en compte pour une vie sauvée, ou perdue, dans le secteur des transports.

2.3.2.1 Analyse Coûts-Bénéfices

L'Analyse Coûts-Bénéfices (ACB) vise à réaliser toutes les décisions dont les *bénéfices* sont supérieurs aux *coûts* (Boardman *et al.*, 2006). S'agissant de la prévention, dans la partie bénéfices, on peut inclure les conséquences d'une baisse de la pollution, d'une baisse de l'incidence d'une maladie, ou d'une meilleure sécurité d'une usine. Dans la partie coûts, on peut inclure les coûts de dépollution, de changement de technologie, les coûts d'investissement dans la sécurité, et de recherche d'un substitut à un produit reconnu toxique (Mishan et Quah, 2007). Il faut noter immédiatement que la comparaison directe des coûts et des bénéfices impose une même unité de mesure. Les économistes adoptent traditionnellement la mesure monétaire (dollars, euros ...). Il n'est pas difficile de comprendre que, dans le domaine de la prévention, la mesure monétaire des bénéfices est en général, - et pas toujours - plus délicate à obtenir, et plus controversée, que la mesure des coûts.

L'ACB vise à améliorer la qualité d'une décision, au sens où cette décision est jugée de meilleure qualité si elle génère un surplus monétaire net plus important dans la société (Pearce, 1983). Cependant, il faut immédiatement ajouter un point fondamental. La qualité ne fait pas uniquement référence à un surplus monétaire, mais au bien-être que la décision génère pour les individus qui composent la société, c'est-à-dire au bien-être social.

Cette approche est appelée « *risque-bénéfice* » lorsque le risque est exprimé en fonction du bénéfice que l'individu ou la collectivité retire de l'activité considérée. Elle est appelée « *coût-bénéfice* » lorsque le coût d'une opération, dont le but est de réduire le risque, est exprimé en fonction du bénéfice attendu.

La mesure de l'impact des défaillances sur les coûts est donc le facteur le plus difficile à évaluer, et pose des problèmes quand il s'agit de sécurité : comment chiffrer la mort de vies humaines, comme il faudrait le faire quand on étudie les risques de déraillement d'un train par exemple ?

2.3.2.2 Valeur de la vie humaine

Il est important de mentionner que le consentement à payer concernant les risques de mortalité est souvent présenté en termes de *valeur statistique de la vie humaine* (VSL - *Value of Statistical Life*) [1].

En d'autres termes, si un projet a essentiellement pour but de *sauver* des vies humaines, et que la valeur de la vie est tirée d'une source exogène au modèle économique, par exemple une source se basant sur l'inférence statistique, l'équité ou la morale, la conclusion de l'étude n'a plus le support de la théorie économique [2] (Viscusi et Aldy, 2003).

La chose est particulièrement dérangeante dans le domaine des transports puisque, dans ce domaine, on ne peut pas éviter l'évaluation en vertu de l'efficacité car la justification des infrastructures de transport est justement l'efficacité (Persson *et al.*, 2001). De sorte que, dans le cas où la valeur de l'infrastructure vient principalement des vies *sauvées*, il faut, dans une analyse coûts-bénéfices, présenter à part l'estimation de la valeur de la vie en précisant qu'elle est exogène au modèle économique (De Blaeij *et al.*, 2003). À la limite, il est inutile de faire une analyse coûts-bénéfices, puisque dans ce cas, la solution est ailleurs.

Cette approche en termes de capital humain a suscité diverses critiques dans la communauté scientifique, et a conduit certains chercheurs à explorer d'autres voies. La méthode dite de la « *valeur des années de vie perdues* » proposée par H. Duval [3] postule, ce qui est classique en économie du bien-être, que ce sont les variations du bien-être de chacun des individus qui sont à l'origine de la valeur sociale de sauvegarde d'une vie humaine.

Ce changement de problématique, assez radical, conduit à retenir comme critère de mesure les satisfactions auxquelles un individu pouvait prétendre et dont l'accident le prive.

1. Le terme est mal choisi car on ne mesure pas ce qu'un individu est prêt à payer pour sauver sa propre vie, mais ce qu'il est prêt à payer pour augmenter, à la marge, ses chances de survie.

2. Il s'agit d'un cas semblable à celui du salaire minimum; on ne peut pas le justifier par la théorie économique de l'efficacité, mais certains gouvernements l'imposent.

3. La valeur publique de la sauvegarde d'une vie humaine est définie dans cette approche comme la somme actualisée des satisfactions que les personnes recueilleront dans le futur. On évalue à cette fin dix effets ayant trait aux variations de bien-être vécues tant par l'individu sauvé que par les autres individus de la communauté à laquelle il appartient.

Les méthodes de calcul proposées sont alors fondées sur les budgets-temps que les individus consacrent à différentes catégories d'activité sous plusieurs contraintes (espérance de vie, consommations obligées, ...). On s'efforce ainsi de déterminer, en plus de la valeur de la consommation et de l'épargne perdues, - correspondant à la valeur du temps de travail perdu - , un coût de la perte de temps libre et des autres préjudices moraux. L'intérêt de cette approche est d'offrir une analyse globale cohérente.

2.3.2.3 Coefficient d'aversion au risque

La *théorie sur la mesure du risque* fut à la base des théories économique et financière de l'aversion au risque (Bouyssou et Vansnick, 1990).

L'aversion au risque, concept né de Bernouilli, est une caractéristique de celui qui ne souhaite pas courir un risque et qui sera prêt à le transférer à un tiers moyennant une rémunération, ou qui refusera tout actif ou toute action lui faisant courir un risque qu'il perçoit comme excessif compte tenu de sa capacité à le supporter. Chaque acteur du système a donc une aversion au risque qui lui est propre.

Au vu de la variété de la nature du risque et de ses enjeux, il a fallu adopter des critères d'acceptation des risques.

2.3.3 Critères d'acceptation des risques

En Europe, les Etats membres ont recours à trois critères d'acceptation des risques.

2.3.3.1 ALARP

Le principe ALARP (*As Low As Reasonably Practicable*), appliqué au Royaume-Uni, définit un domaine pour un risque inacceptable nécessitant un traitement de risque lorsque des résultats de l'analyse des risques tombent dans ce domaine. Le domaine de tolérance limitrophe avec des valeurs inférieures entraîne des mesures conformément au principe ALARP,

alors que le domaine acceptable, avec un risque résiduel encore plus faible et insignifiant ne requiert pas de mesures de la part de l'autorité compétente.

Le principe ALARP utilise pour certains dangers, la relation entre le coût et le bénéfice d'une mesure de protection (Melchers, 2001). Pour les autres, c'est l'acceptabilité par le public qui est appliquée.

La signification et la valeur du triangle de la tolérabilité du risque (*cf.* Figure 2.3) ont été présentées par le *Health and Safety Executive* (HSE) de façon à être accessibles au grand public : le triangle représente les degrés de *risque* d'une activité donnée, plus importants lorsque l'on progresse vers le haut du *triangle*. Il peut être divisé en trois zones (Rafrafi, 2007).

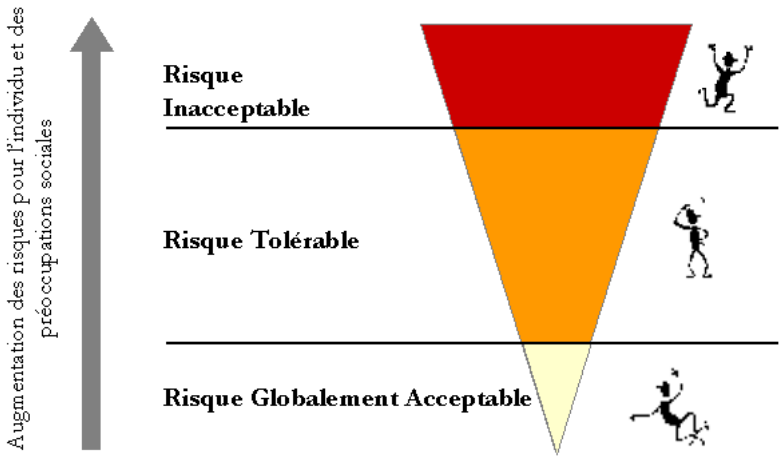

FIGURE 2.3: Modèle ALARP

1. **La zone supérieure** représente l'inacceptabilité. Pour des raisons pratiques, un risque placé dans cette zone est considéré inacceptable, quelsque soient les bénéfices associés à l'activité. Toute activité ou pratique générant des risques se classant dans la zone supérieure sera, par principe, rejetée ; à moins que l'activité ou la pratique ne soit modifiée pour que le degré de risque soit réduit et que l'activité descende dans l'une des zones inférieures ou qu'il n'existe des motifs exceptionnels pour le maintien de l'activité ou de la pratique.

2. **La zone inférieure** représente une acceptabilité globale. Les risques se classant dans cette zone sont en général considérés insignifiants et correctement contrôlés. Les organismes de réglementation n'exigent en général aucune action supplémentaire pour les réduire à moins que des mesures raisonnablement praticables ne soient possibles. Les risques placés dans cette zone sont comparables à ceux que les gens considèrent insignifiants ou triviaux dans leur vie quotidienne. Il s'agit en général de risques découlant d'activités qui ne sont pas en soi très dangereuses ou d'activités dangereuses qui peuvent être ou qui sont déjà contrôlées afin de ne générer que de très faibles risques. Le HSE estime néanmoins que les responsables doivent réduire ces risques lorsque cela est raisonnablement praticable ou lorsque la loi l'exige.
3. **La zone située entre les risques inacceptables et globalement acceptables** est destinée aux risques tolérables [4]. Les risques placés dans cette zone sont en général ceux qui découlent d'activités que les gens sont prêts à tolérer pour obtenir des avantages, dans l'espoir que :
   - la nature et le degré du risque ont été correctement évalués et que les résultats de ces évaluations ont été correctement utilisés pour déterminer les mesures de contrôle ;
   - le risque résiduel n'est pas excessivement élevé et est maintenu aussi bas que raisonnablement praticable ;
   - les risques sont régulièrement réévalués pour s'assurer qu'ils respectent toujours le critère ALARP.

Avantages La formulation de l'acceptabilité est valable aussi bien pour le transport que pour les industries dangereuses.

Le principe ALARP prend comme base les risques de tous les jours, sans se limiter aux faits technologiques, ce qui serait plus avantageux pour un manager de projet. De plus, il

4. Il est important de souligner, bien que certains universitaires aient parfois utilisé ces termes l'un pour l'autre, que dans le modèle de la tolérabilité du risque, la tolérabilité et l'acceptabilité sont des concepts différents. Contrairement à l'acceptabilité, qui est une notion absolue, la tolérabilité fait référence à une volonté de vivre avec un risque dans le but d'obtenir certains bénéfices, dans l'espoir que ce risque vaille la peine d'être pris et soit correctement contrôlé. Tolérer un risque signifie le garder sous contrôle et le réduire si possible et autant que possible.

a pour vocation d'expliciter l'intégration systématique des procédures et le comportement humain, ainsi que la relation étroite entre la fiabilité et la sécurité.

Inconvénients Les risques inacceptables ne supportent pas une appréciation numérique, ce qui enlève toute possibilité de démonstration par cette voie. Seuls les dangers pour lesquels aucun état de sécurité reconnu n'existe donnent lieu à une justification de la practicabilité.

Le nombre de victimes n'étant pas rapporté à la population bénéficiare du système, aucune argumentation sur l'effet de dilution des drames n'est recevable.

2.3.3.2 GAME

Le principe GAME (Globalement Au Moins Équivalent) utilise la relation potentielle entre acceptabilité par le public et les statistiques issues des systèmes en usage. Selon l'Article 3 du Décret 2000-286 relatif à la sécurité du réseau ferré national, « *la modification d'un système existant ainsi que la conception d'un nouveau système sont effectuées de telle sorte que le niveau global de sécurité en résultant soit au moins équivalent au niveau de sécurité existant ou à celui de systèmes existants assurant des services ou fonctions comparables* ».

Ce principe considère que l'évolution technologique d'un système ne doit pas induire de risque supérieur à ce qu'induisait la précédente génération. Ceci conduit à rechercher un risque moyen, au plus, égal à celui pris lors de l'exploitation de la précédente génération du système (Desroches *et al.*, 2006). En d'autres termes, le principe GAME admet que le niveau de sécurité du système existant est satisfaisant. Lorsque le système de référence n'existe pas, on considère alors un système équivalent en référence.

La comparaison peut se faire sur les bases suivantes (Le Trung, 2000) :

- *technologie :* niveau d'automatisation, degré d'intervention humaine dans l'exploitation, capacité du véhicule, vitesse, disponibilité ;
- *maturité :* degré atteint dans l'expérience de l'exploitant et dans la familiarité des usagers ;

– *dimension du système :* population desservie, nombre de sièges * kilomètres.

Avantages L'expression *au moins équivalent* est politiquement correcte, car personne ne trouvera d'objection à l'intention « *Nous avons su obtenir de bons résultats et nous allons faire mieux* ». L'acceptation selon GAME peut se prononcer au vu des moyens et méthodes mis en œuvre par le constructeur au regard des dangers couverts, non couverts et induits par le nouveau système.

Le terme *global* pourrait concerner les agents d'exploitation, même si ceux-ci dépendent de la législation sur le travail. En effet, un système très sûr à l'égard du public et peu sûr à l'égard des agents d'exploitation n'est certainement pas suffisant.

Inconvénients Il faut disposer de statistiques exploitables, si l'on veut pouvoir justifier le terme *global*. En particulier, le fait que les statistiques soient muettes sur les *presque-accidents* est un handicap, car on a besoin de savoir ce que ceux-ci deviendront dans le nouveau système. L'analyse coût-bénéfice n'étant pas explicite, la surenchère dans les objectifs de sécurité est telle qu'ils risquent de ne plus être démontrables.

2.3.3.3 MEM

Le principe MEM (*Minimum Endogenenous Mortality*) impose à la mortalité exogène d'être inférieure à la mortalité endogène minimale. Il prend pour référence le taux de mortalité naturelle de la population (excluant les décès par maladie, par infection ou par malformation congénitale) et à faire en sorte que le risque pris par un utilisateur du système n'augmente pas de façon significative le taux de mortalité.

Dans les pays développés, le taux de mortalité naturelle est de $2*10^{-4}$ décès par personne et par an.

Dans la pratique, il est admis d'utiliser les valeurs suivantes :

– $R1 < 10^{-5}$ décès par personne et par an ;

- $R2 < 10^{-4}$ blessures graves par personne et par an ;
- $R3 < 10^{-3}$ blessures légères par personne et par an.

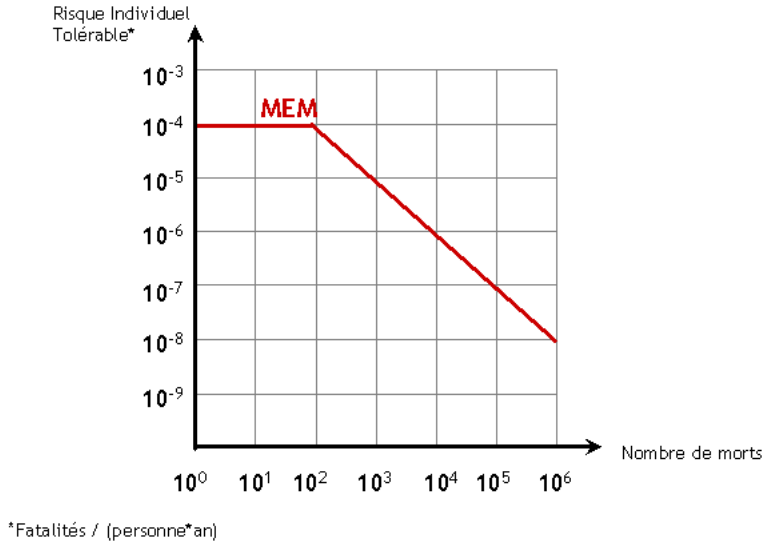

FIGURE 2.4: Critère MEM

Pour des systèmes pouvant entraîner un grand nombre de décès, il faut aussi prendre en compte un *coefficient d'aversion* (*cf.* section 2.3.2.3 page 44) qui réduit le risque acceptable.

Avantages La formulation par ce principe du risque acceptable est valable pour tout fait technologique, qu'il vienne d'une usine chimique ou d'un moyen de transport.

Les limites préconisées, respectivement relatives au taux de décès, de blessés graves et de blessés légers suggèrent la possibilité d'une équivalence dans la sévérité (Le Trung, 2000). C'est ainsi qu'un décès serait équivalent à dix blessés graves ou cent blessés légers. L'incidence d'un accident pourrait donc être globalement estimée selon l'équation 2.4.

$$Incidencedel'accident = Nombrededcs + 0.1Blesssgraves + 0.01Blessslgers \qquad (2.4)$$

Cette équivalence est utile, dans la mesure où la gravité d'un accident dépend en partie du niveau d'énergie mis en jeu dans le système : certains systèmes ont une propension à ne causer que des blessés, tandis que d'autres causeront uniquement des décès.

Inconvénients Le principe MEM ne fait pas de distinction entre risques responsables et risques non responsables.

Il n'est pas toujours possible d'évaluer l'acceptabilité des risques au niveau du système en utilisant un seul des trois principes d'acceptation des risques. L'acceptation des risques se basera souvent sur une combinaison de ces principes ainsi qu'une association à des méthodes qualitatives et quantitatives d'évaluation des risques.

2.4 Méthodes d'évaluation des risques

Cette section présente un état de l'art des méthodes d'évaluation des risques qui prennent en compte les données de fiabilité des composants pour l'évaluation des risques des systèmes.

Nous nous concentrons principalement sur les méthodes d'évaluation quantitatives et qualitatives. En effet, il n'y a pas de recherche de quantification sans analyse qualitative. Par contre, il peut y avoir analyse qualitative sans quantification. Nous qualifions de quantitatives les méthodes qui offrent une possibilité importante de quantification et de qualitatives les méthodes qui l'excluent ou dans lesquelles cet aspect est marginal.

Nous nous sommes fixés comme objectif de permettre, au travers de la présentation des principales méthodes d'analyse du risque, d'analyser leur utilisation pour l'évaluation des risques des systèmes.

2.4.1 Méthodes qualitatives

L'application des méthodes qualitatives d'analyse des risques fait systématiquement appel aux raisonnements par induction et par déduction. La plupart des méthodes revêtent un caractère inductif dans une optique de recherche allant des causes aux conséquences éventuelles.

Différentes méthodes qualitatives ont été répertoriées en matière d'évaluation des risques.

2.4.1.1 Analyse fonctionnelle

L'approche fonctionnelle d'un produit industriel a pour objet l'étude des fonctions de service et des fonctions techniques. Elle se construit en deux temps.

D'abord, l'expression fonctionnelle du besoin est conduite à partir du recensement et de la caractérisation des fonctions de service. Elle permet de décrire le besoin d'une manière nécessaire et suffisante.

Ensuite, vient la description fonctionnelle du produit qui est conduite à partir du recensement et de la caractérisation des fonctions techniques. Elle traduit les choix effectués par le concepteur pour satisfaire les fonctions de service.

FAST *(Function Analysis System Technique)* La technique FAST permet de décrire, sous la forme d'un diagramme, les fonctions de sécurité et les fonctions techniques dans un enchaînement logique. On peut adjoindre à la méthode FAST le descriptif des solutions constructives en vis-à-vis des fonctions techniques qu'elles réalisent.

A partir d'une fonction, la méthode FAST permet de répondre aux trois questions suivantes :

- Pourquoi cette fonction est-elle assurée ?
- Comment cette fonction est-elle assurée ?
- Quand cette fonction est-elle assurée ?

La réponse à chacune de ces questions n'est ni exclusive, ni unique. Aussi, il existe deux types d'embranchements entre les différentes colonnes, les embranchements de type « ET », et les embranchements de types « OU ». On représente les liaisons « OU » par deux flèches (ou plus) partant de la même origine, alors qu'une liaison « ET » se sépare après la case représentant la fonction origine. La Figue 2.5 illustre un exemple de représentation d'une fonction.

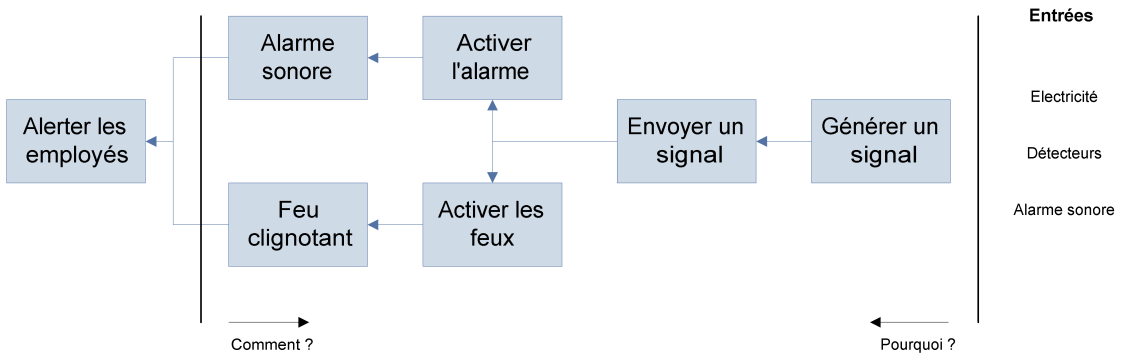

FIGURE 2.5: Exemple d'un diagramme FAST

SADT *(Structured Analysis and Design Technique)* Connue aussi sous le label IDEF0 (*Integration DEfinition for Function modeling*), SADT est une méthode d'origine américaine standardisée en 1993 de description graphique d'un système complexe par analyse fonctionnelle descendante, c'est-à-dire que l'analyse chemine du général (dit *niveau* A_0) vers le particulier (dit *niveaux* A_{ijk}). SADT est une démarche systémique de modélisation d'un système complexe ou d'un processus opératoire.

Méthode Une fonction est représentée par une *boîte* SADT comprenant :

- un rectangle contenant :
  - un verbe à l'infinitif définissant l'action et la valeur ajoutée de la fonction,
  - son label A_{ijk} d'identification, la lettre A du label signifiant *Activité*,
- des flèches d'entrée horizontales représentant la matière d'œuvre (souvent à caractère informationnel et immatériel),
- des flèches d'entrée verticales descentantes représentant la matière de contrôle (souvent à caractère informationnel et immatériel),
- des flèches d'entrée verticales ascendantes représentant les contraintes (souvent à caractère physique et matériel),
- des flèches de sortie horizontales représentant la valeur ajoutée de la fonction (souvent à caractère informationnel et immatériel).

La fonction courante A_{ijk} peut ensuite être décomposée au niveau inférieur, noté A^+_{ijk}, pour faire apparaître les sous-fonctions constituantes.

Soit la fonction ferroviaire A_8 « *Contrôle/Commande* ». Cette activité A_8^+ comprend deux sous-fonctions : A_{802} : *Assurer l'autorisation d'itinéraire*, A_{803} : *Assigner l'itinéraire au train.*

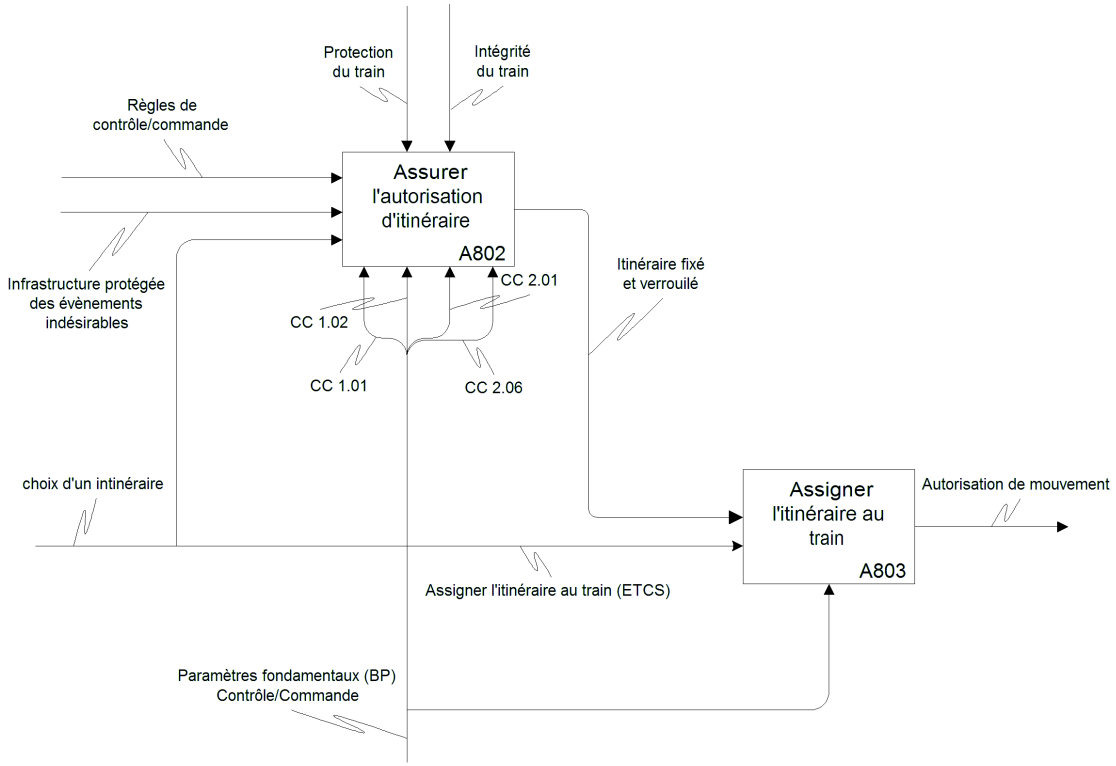

FIGURE 2.6: Exemple d'un actigramme SADT

Cet outil a l'avantage de permettre une clarification et une décompostion analytique de la complexité d'un système grâce à une structure hiérarchisée par niveau. Cependant, les diagrammes intemporels SADT ne permettent pas une représentation séquentielle à cause de l'absence de logique booléenne (ET, OU, *etc.*) ; ce qui nous prive d'une vue globale.

2.4.1.2 Analyse fonctionnelle des dangers

L'analyse fonctionnelle des dangers (FHA - *Functional Hazards Analysis*) est une technique inductive d'analyse de danger. Le raisonnement inductif part d'observations spécifiques pour engendrer des généralisations plus larges et des théories. D'une façon informelle, cette approche est aussi appelée une *approche ascendante*. Dans le raisonnement inductif, nous

commençons par des observations spécifiques et des mesures, détectons des modèles et des régularités. Ensuite, nous formulons quelques hypothèses expérimentales que nous pouvons explorer et finir finalement de développer quelques conclusions générales ou théories.

Dans l'analyse de sécurité, une analyse de danger inductive peut s'avérer plus concluante qu'une analyse de données (Ericson, 2005) dans un contexte d'identification de danger et non de cause première. De plus, une analyse fonctionnelle des dangers est une approche qualitative qui, au vu de grands systèmes avec beaucoup de dangers, est plus intéressante qu'une analyse quantitative de risque .

Dans la sécurité des systèmes, il a été prouvé que des techniques qualitatives sont très efficaces et fournissent généralement la capacité de prise de décisions comparable avec l'analyse quantitative.

Le processus de FHA implique l'exécution d'une analyse détaillée des fonctions du système. Un élément clé pour cette méthodologie consiste en l'identification et la compréhension de toutes les fonctions de système. Une liste de fonctions doit être créée et on recommande l'utilisation d'organigrammes fonctionnels pour leur capacité de fournir une aide à l'analyse. Chacune de ces fonctions devrait être évaluée par rapport à l'effet de l'état d'échec sur le système (Ericson, 2005).

Le processus d'une analyse fonctionnelle des dangers consiste en 10 étapes principales :

1. définir l'opération,
2. acquérir des données,
3. lister les fonctions,
4. conduire une analyse,
5. évaluer le risque système,
6. identifier les fonctions critiques de sécurité,
7. recommander l'action corrective,
8. contrôler l'action corrective,

9. tracer les dangers,
10. documenter la FHA.

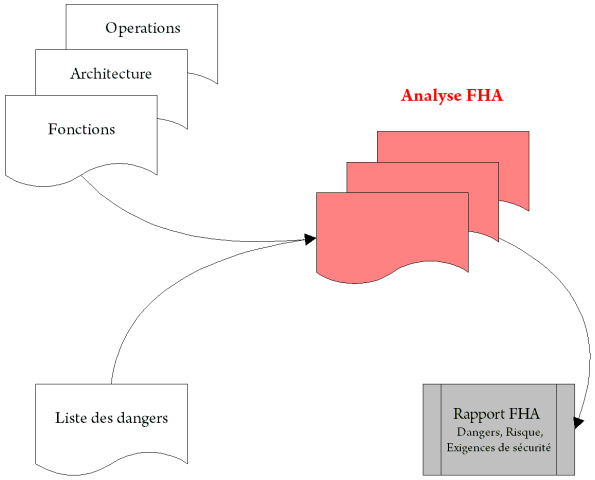

FIGURE 2.7: Processus d'une analyse fonctionnelle des dangers

Il est recommandé de procéder à une FHA en utilisant des tableaux, ce qui rend l'analyse plus structurée et rigoureuse. Typiquement, les feuilles de calcul à colonnes sont utilisées (Ericson, 2005).

Sous-système		FHA			
Fonction	Danger	Effet	Cause	IMRI	Action Recommandée
1	2	3	4	5	6

Tableau 2.1: Document de base d'une FHA

Les informations exigées sous chaque colonne dans cette feuille de travail traitent :

1. **Fonction.** Cette colonne inscrit et décrit chacune des fonctions de système.
2. **Danger (H)**. Cette colonne identifie le danger spécifique évalué pour l'échec fonctionnel.
3. **Effet (E)**. Cette colonne identifie l'effet et les conséquences du danger ; le plus mauvais résultat est exposé.
4. **Causes (C)**. Les facteurs causant tant l'échec fonctionnel que l'effet final.
5. **IMRI**. Cela signifie l'Indice de Risque Initial. Cette colonne fournit une mesure qualitative du risque, où le risque est une combinaison de gravité et probabilité d'occurence.

6. **Action Recommandée (AR)**. Elle est rapprochée de mesures préventives pour contrôler des dangers identifiés.

2.4.1.3 Noeud Papillon

Le « *Noeud Papillon* » est une approche arborescente développée par SHELL. Il permet de considérer une approche probabiliste dans la gestion des risques.

C'est aussi une connexion d'un arbre de défaillances et d'un arbre d'évènements, généralement établis lorsqu'il s'agit d'étudier des évènements hautement critiques.

Le point central du noeud papillon est l'*Evénement Redouté Central*. Généralement, ce dernier désigne une perte de confinement ou une perte d'intégrité physique (décomposition). La partie gauche sert à identifier les causes de cette perte de confinement, tandis que la partie droite du noeud s'attache à déterminer les conséquences de cet événement redouté central (INERIS-DRA, 2003; Direction des Risques Accidentels, 2004). Chaque scénario d'accident est relatif à un évènement redouté central et est représenté à travers un chemin possible allant des évènements indésirables ou courants jusqu'à l'apparition des effets majeurs.

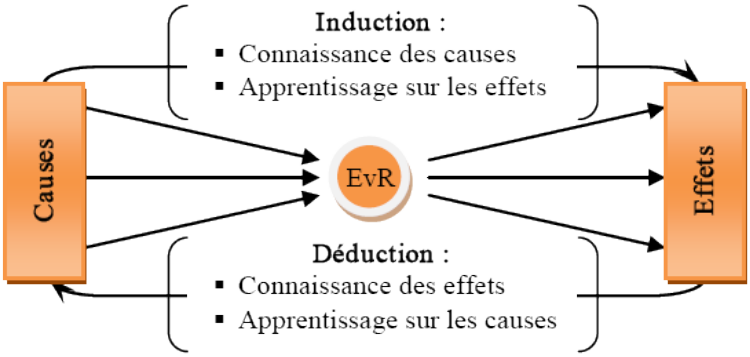

FIGURE 2.8: Raisonnement du modèle SHELL (Mazouni, 2008)

Un noeud papillon est généralement précédé par une analyse des risques plus générique de type Analyse Préliminaire des Risques (APR).

2.4.2 Méthodes quantitatives

Les analyses quantitatives sont supportées par des outils mathématiques ayant pour but d'évaluer la sûreté de fonctionnement, et entre autres, la sécurité. Cette évaluation peut se faire par des calculs de probabilités, par exemple lors de l'estimation quantitative de la probabilité d'occurrence d'un événement redouté, ou bien par recours aux modèles différentiels probabilistes tels que les réseaux de Petri.

2.4.2.1 AMDEC

L'armée américaine à développé l'AMDEC. La référence militaire MIL-P-1629, intitulée « *Procédures pour l'Analyse des Modes de Défaillance, de leurs Effets et leurs Criticités* » (AMDEC), est datée du 9 Novembre 1949. Cette méthode était employée comme une technique d'évaluation des défaillances afin de déterminer la fiabilité d'un équipement et d'un système Villemeur *et al.* (1988). Les défaillances étaient classées selon leurs impacts sur le personnel et la réussite des missions pour la sécurité de l'équipement.

Objectifs L'objectif d'une AMDEC est de permettre l'identification de toutes les possibilités de défaillances catastrophiques et critiques de sorte qu'elles puissent être minimisées ou éliminées le plus tôt possible par des interventions préventives pertinentes.

L'AMDEC a pour but d'évaluer l'impact, ou la criticité, des modes de défaillances des composants d'un système sur la fiabilité, la maintenabilité, la disponibilité et la sécurité de ce système.

Méthode Une analyse AMDEC sur les équipements critiques identifiés est réalisée en huit étapes :

1. Définir le système qui sera analysé ;
2. Construire des diagrammes en blocs fonctionnels et de fiabilité ;

3. Identifier tous les modes de défaillance potentiels et définir leurs effets sur la fonction immédiate ou sur l'actif, sur le système et sur la mission qui doit être réalisée ;
4. Évaluer l'importance des différentes conséquences des modes de défaillance potentiels et assigner une côte de criticité à chacun des modes de défaillance ;
5. Identifier les méthodes de détection possibles et les mesures compensatoires pour chacun des modes de défaillance ;
6. Identifier les modifications de conception ou les actions correctives nécessaires pour minimiser le risque ou éliminer complètement la défaillance ;
7. Identifier les effets des actions correctives ou les autres attributs du système comme les exigences pour le support logistique ;
8. Documenter les analyses et résumer les problématiques qui ne peuvent pas être corrigées par une modification de conception et identifier les contrôles spécifiques qui devront être effectués dans le but de réduire le risque de défaillance.

Cependant, le propre de la méthode AMDEC est de pouvoir également quantifier l'importance du risque lié à chaque effet. Trois critères sont ainsi définis :

- La *fréquence d'apparition de l'incident* (f) : on peut ainsi estimer qu'un certain genre d'incident risque d'arriver une fois par an. Une variante de la fréquence temporelle est de dire, par exemple, qu'une pièce ayant tel défaut sera produite toutes les 10000 pièces. C'est le premier critère auquel on pense, le plus intuitif en matière de sécurité, de maintenance et de disponibilité.
- La *gravité* (G) : elle est calibrée selon les critères de satisfaction du client, au sens large, c'est-à-dire le client de l'entreprise, l'utilisateur, l'entreprise elle-même ou l'ensemble de la population quand il s'agit de sécurité publique. De manière générale, on fait apparaître dans l'échelle de la gravité, en parallèle, la notion de danger associé à la défaillance. Toute atteinte à la sécurité de l'utilisateur ou du public est ainsi déclinée par un niveau élevé de la gravité.
- La *détection* (D) : c'est un facteur auquel on pense de façon beaucoup moins immé-

diate. Elle est calibrée en fonction des moyens de mesure de l'apparition des causes de dysfonctionnement mis en œuvre.

Ces trois indicateurs sont ensuite synthétisés par un indicateur appelé *criticité*, défini comme le produit des trois critères précédents.

Atouts Les aspects originaux de la méthode sont les suivants :

- Appliquée en groupe de travail pluridisciplinaire, elle est recommandée pour la résolution de problèmes mineurs dont on veut identifier les causes et les effets.
- En phase de conception, l'AMDEC est associée à l'analyse fonctionnelle pour la recherche des modes de défaillances spécifiques à chaque fonction ou contrainte des composants. Elle peut intervenir à titre correctif pour l'amélioration de systèmes existants.
- Cette méthode est qualifiée d'*inductive* au sens où elle s'appuie, pour l'analyse des défaillances, sur une logique de décomposition d'un système en sous-ensembles successifs pour parvenir au niveau des composants élémentaires. On s'intéresse alors aux défaillances liées au mauvais fonctionnement de ces composants et à leurs répercussions sur les niveaux supérieurs du système.

De plus, l'AMDEC fournit une autre vision du système par le biais des supports de réflexion, de décision et d'amélioration et surtout des informations à gérer au niveau des études de sûreté de fonctionnement et des actions à entreprendre.

Limites Bien que simple, la méthode s'accompagne d'une lourdeur certaine et la réalisation exige un travail souvent important et fastidieux. Ainsi, une des difficultés réside dans l'optimisation de l'effort entre le coût de l'analyse AMDEC, dépendant de la profondeur de l'analyse, et le coût de l'amélioration à apporter.

La solution pour surmonter le volume des entités à étudier est de conduire des AMDEC *fonctionnelles*. Cette approche permet de détecter les fonctions les plus critiques et de limiter ensuite l'AMDEC *physique* aux composants qui réalisent tout ou partie de ces fonctions.

La cohérence entre, d'une part, la gestion des AMDEC et des améliorations préconisées

et, d'autre part, les différentes versions du système est l'une des autres principales difficultés à résoudre.

Aussi, la méthode n'est pas bien adaptée aux projets en temps réel car elle ne permet pas de bien appréhender l'aspect temporel des scénarios.

En outre, les conséquences des erreurs humaines ne sont pas habituellement étudiées au cours d'une AMDEC. L'examen des interactions homme-machine se fait selon des méthodes particulières.

Bien qu'ayant subi de nombreuses critiques dûes au coût et à la lourdeur de son application, elle reste néanmoins l'une des méthodes les plus répandues et l'une des plus efficaces. En effet, elle est de plus en plus utilisée en sécurité, maintenance et disponibilité non seulement sur le matériel, mais aussi sur le système, le fonctionnel et le logiciel.

De plus, elle est maintenant largement recommandée au niveau international et systématiquement utilisée dans toutes les industries à risque, comme le nucléaire, le spatial et la chimie, dans le but de faire des analyses préventives de la sûreté de fonctionnement.

Dans le ferroviaire, la méthode a été expérimentée sur le logiciel critique dans le cadre des projets SACEM de la RATP en région parisienne et MAGGALY de SEMALY à Lyon. Une adaptation de cette méthode a donné naissance à la méthode AEEL (Analyse des Effets des Erreurs du Logiciel) qui ressemble beaucoup à l'AMDEC.

2.4.2.2 Arbre d'évènements

Appelé aussi ETA (*Event Tree Analysis*), l'analyse par arbre d'évènements est une représentation visuelle de tous les événements qui peuvent se produire dans un système.

L'analyse par arbre d'évènements fournit une approche déductive à l'évaluation de fiabilité pendant qu'ils sont construits en utilisant la logique vers l'avant.

Des arbres d'évènements peuvent être employés pour analyser les systèmes dans lesquels tous les composants sont à fonctionnement continu, ou pour les systèmes dans lesquels certains ou tous les composants sont en mode *attente* - ceux qui impliquent la logique opérationnelle séquentielle. Le point de départ perturbe l'exploitation du système normal. Ainsi, l'arbre d'évènements montre les séquences d'opérations comportant le succès et/ou l'échec des composants de système.

Le but d'un arbre d'évènements est de déterminer la probabilité d'un évènement basé sur les résultats de chaque évènement dans la séquence d'opérations chronologiques amenant à lui. En analysant tous les résultats possibles, on peut déterminer le pourcentage des résultats qui mènent au résultat désiré.

2.4.2.3 Arbre de défaillances

Cette méthode est née dans en 1961 (Villemeur *et al.*, 1988), dans les bureaux de la Bell Lab et a été ensuite développée et formalisée essentiellement par la société Boeing. Depuis 1965, elle est fréquemment employée dans de nombreux domaines industriels (aéronautique, nucléaire, chimie, *etc.*). L'appellation anglaise est *Fault Tree Analysis (*FTA*)*.

Principes Cette analyse déductive a pour but de rechercher toutes les combinaisons de pannes qui conduisent à l'évènement redouté. Elle s'appuie sur une technique graphique représentant les combinaisons de pannes conduisant à un ER. Un arbre de défaillances représente les diverses combinaisons possibles d'évènements qui peuvent induire la réalisation d'évènements indésirables.

L'arbre de défaillances est une représentation graphique de type *arbre généalogique*. Il représente une démarche d'analyse d'évènements. L'arbre de défaillances est construit en recherchant l'ensemble des évènements élémentaires, ou les combinaisons d'évènements, qui conduisent à un ER. L'objectif est de suivre une logique déductive en partant d'un ER pour déterminer de manière exhaustive l'ensemble de ses causes jusqu'aux plus élémentaires.

Méthode La construction de l'arbre de défaillances repose sur l'étude des évènements entraînant un ER. Les deux étapes suivantes sont réalisées successivement en partant de l'ER et en allant vers les évènements élémentaires.

1. Dans un premier temps, définir l'évènement redouté analysé en spécifiant précisément ce qu'il représente et dans quel contexte il peut apparaître.
2. Dans un deuxième temps, représenter graphiquement les relations de cause à effet par des portes logiques (ET, OU) qui permettent de spécifier le type de combinaison entre les évènements intermédiaires qui conduisent à l'évènement analysé.

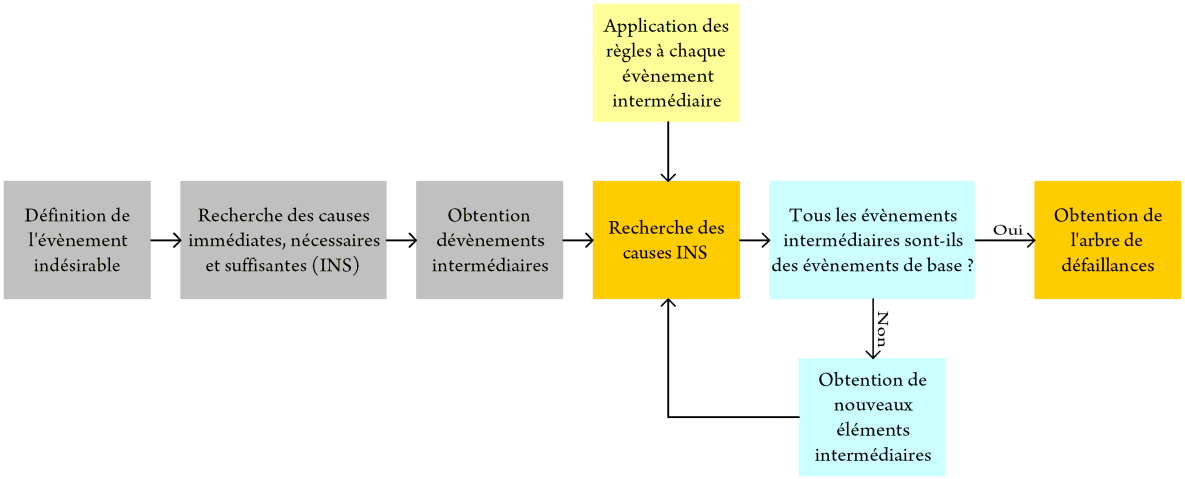

FIGURE 2.9: Processus d'élaboration d'un arbre de défaillances

2.4.2.4 Analyse probabiliste des risques

L'analyse probabiliste des risques a été constamment améliorée par les experts du domaine et a gagné de la crédibilité pendant les deux dernières décennies non seulement dans l'industrie nucléaire, mais également dans d'autres industries comme la pétrochimique, les plates-formes pétrolières et la défense (Bedford et Cooke, 2001; Stamatelatos *et al.*, 2002).

En raison de son approche logique, systématique et compréhensive, l'analyse probabiliste des risques a prouvé à plusieurs reprises qu'elle était capable de découvrir des faiblesses de conception, qui avaient échappé aux experts. Cette méthodologie a aussi prouvé qu'il était

très important d'examiner l'ensemble des scénarii ayant une faible probabilité d'occurrence, mais avec une forte conséquence sur le système concerné.

Après l'accident de la navette spatiale *Challenger*, le 28 janvier 1986, la NASA a décidé que l'analyse probabiliste des risques devait être appliquée à tout le programme spatial, mais a aussi déclaré que les techniques d'analyse devaient être systématiquement améliorées par des données précises et un historique complet.

Méthode L'analyse probabiliste des risques suit une méthodologie constituée des étapes suivantes :

- Définition des objectifs : Les objectifs de l'évaluation des risques doivent être bien définis et les conséquences indésirables identifiées.
- La connaissance du système : La connaissance du système concerné est primordiale. Elle couvre les aspects de conception jusqu'aux procédures de fonctionnement du système.
- Identification des évènements initiaux : L'ensemble des évènements initiaux déclenchant des scénarii d'accidents doit être identifié. Les évènements initiaux indépendants qui mènent à des scénarii semblables doivent être groupés ainsi que leurs fréquences, afin d'évaluer les fréquences initiales.
- Modélisation des scénarii : Chaque scénario d'accident doit être modélisé avec des arbres d'évènements.
- Modélisation des échecs : Chaque échec d'un évènement pivot dans un scénario d'accidents doit être modélisé avec des arbres de défaillances.
- Collecte de données et analyse : Divers types de données doivent être rassemblées et traitées. Les données rassemblées fournissent des informations sur les taux d'échec, les temps de réparation, les probabilités de défaillance de structure, les probabilités d'erreurs humaines, les probabilités de processus d'échec.
- Quantification : La fréquence de l'occurrence de chaque état d'extrémité est le produit de la fréquence d'EI et des probabilités conditionnelles des événements pivots le long du chemin liant l'EI à l'état d'extrémité. Les scénarii sont groupés selon l'état d'extrémité du scénario définissant une conséquence donnée. Tous les états d'extrémité doivent

être alors groupés, et leurs fréquences se résument alors à la fréquence d'un seul état représentatif d'extrémité.

- Analyse d'incertitude : Des analyses d'incertitude doivent être réalisées pour évaluer le degré de confiance que l'on peut porter sur les calculs numériques du risque. Des méthodes de simulation de type Monte-Carlo sont généralement employées pour réaliser une analyse d'incertitude.
- Analyse de sensibilité : Des analyses de sensibilité sont également fréquemment réalisées pour indiquer si des changements sur des valeurs d'entrée peuvent causer des changements importants des calculs numériques partiels ou finaux du risque.

2.4.2.5 Réseaux de Petri

Les Réseaux de Petri (RdP) ont été introduits par C.A. Petri, en 1962, dans (Petri, 1962), afin de modéliser la composition et la communication entre automates. Les réseaux de Petri sont des outils mathématiques et graphiques qui s'appliquent à un grand nombre d'applications où les notions d'évènements et d'évolutions simultanées sont importantes.

Plus précisément, il s'agit d'un outil théorique, s'appuyant sur les graphes, particulièrement adapté pour la modélisation et l'analyse des systèmes dynamiques à événements discrets. Les réseaux de Petri permettent de prendre en compte les notions de parallélisme, de synchronisation et de ressources, et sont utilisés, par exemple, dans l'étude des réseaux de communication, des systèmes de transport ou de production manufacturière.

La présentation qui suit s'inspire largement des définitions et propriétés énoncées par Murata dans (Murata, 1989) et par Diaz et *al.* dans (Diaz et al., 2001, 2003).

Les réseaux de Petri sont un formalisme graphique et mathématique qui permet de décrire des systèmes dans lesquels les notions de concurrence et parallélisme sont présentes. Il s'agit d'un quadruplet : $R =< P, T, Pre, Post >$ dans lequel P est un ensemble fini de places, T est un ensemble fini de transitions, Pre est l'application places précédentes et $Post$ est

l'application places suivantes. Les places des réseaux de Petri peuvent être marquées par des jetons, l'ensemble de jetons dans les places du réseau indiquant le marquage du réseau.

Outre le fait que les réseaux de Petri soient des automates à état fini, c'est leur possibilité de représentation graphique qui en fait tout l'intérêt.

Représentation graphique Un réseau de Petri peut se représenter graphiquement sous la forme d'un graphe orienté, pondéré biparti. Les places sont représentées sous forme de cercles et les transitions sous forme de rectangles. On associe à chaque place p du réseau un nombre de jetons équivalent à son marquage $m(p)$. Les jetons sont représentés par des disques pleins à l'intérieur des places, ou plus simplement par un entier étiquetant la place.

Les RdP de base, tels que les a décrits Petri, sont organisés en deux structures complémentaires :

- un dessin statique qui ne change pas au cours du temps ;
- des éléments dynamiques qui indiquent l'état du système à un instant donné.

La Figure 2.10 représente les éléments de base de la structure statique d'un RdP :

- les places représentées par des cercles et placées en amont ou/et en aval des transitions ;
- les transitions représentées par des rectangles aplatis. Chaque transition représente un événement susceptible de se produire dans le RdP ;
- les arcs amont ou aval reliant les places aux transitions ou les transitions aux places.

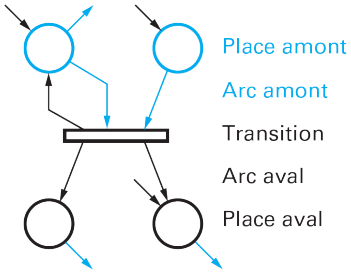

FIGURE 2.10: Structure statique

C'est sur cette structure statique et figée que viennent se superposer les éléments dynamiques permettant de décrire le comportement du système modélisé (*cf.* Figure 2.11).

Dans les RdP de base, ces éléments dynamiques sont constitués de simples jetons dont la disposition sur les places définit l'état du système à un moment donné. Chaque configuration de jetons est appelée *marquage du réseau* et correspond à un état spécifique. Une même structure statique peut ainsi supporter de nombreux marquages représentant autant d'états différents. Par comparaison avec les graphes de Markov pour lesquels la taille des modèles augmente exponentiellement en fonction du nombre des composants à modéliser, la taille des RdP n'augmente que linéairement. L'explosion combinatoire du nombre des états est donc jugulée et le traitement de systèmes de taille industrielle peut être envisagé sereinement.

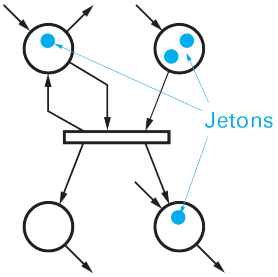

FIGURE 2.11: Eléments dynamiques

Arcs inhibiteurs Le modèle des réseaux de Petri ne permet pas de tester si une place est vide. Mais il est souvent possible de recourir à l'utilisation de deux places $p1$ et $p2$ telles que $m(p1) + m(p2) = K$, où K est une constante. Ainsi, si $m(p1) = K$, alors $m(p2) = 0$, et par conséquent, en testant si la place $p1$ possède K jetons, on teste du même coup si $p2$ n'a pas de jetons. On dit que $p1$ et $p2$ sont des places complémentaires. Ce mécanisme impose la connaissance d'une borne K, condition qu'il n'est pas toujours possible de satisfaire.

Les arcs inhibiteurs, introduits dans (Agerwala et Flynn, 1973), permettent d'accomplir ce test sans recourir à des places complémentaires et donc sans obligation de connaître une borne sur les jetons de la place que l'on souhaite tester à zéro. Cette extension permet aux réseaux de Petri de simuler une machine de Turing (Agerwala, 1975). L'accessibilité des états est donc indécidable. Outre le fait qu'ils permettent une expressivité plus grande, ils permettent aussi d'avoir un modèle plus réduit, dans le cas où les places complémentaires sont possibles.

Des variables peuvent être introduites au réseau de Petri. Elles peuvent être soit temporelles soit des prédicats.

RdP Temporels Les RdP temporels ont été introduits par Merlin (Merlin, 1974).

Un réseau de Petri temporel est une paire $< R, I >$ où :

- R est un réseau de Petri $< P, T, Pre, Post >$ auquel est associé un marquage initial M_0,
- I est la fonction d'intervalle initial qui associe à chaque transition un intervalle fermé rationnel $I(t) = [a, b]$ qui décrit une durée de sensibilisation de la transition t.

Nous avons présenté les réseaux de Petri temporels mais il est possible de simplifier encore plus la modélisation en RdP en utilisant des assertions.

RdP Prédicats Transitions Un prédicat est une grandeur dont on peut dire si elle est vraie ou fausse (booléenne), en étant associée aux transitions (Sadou, 2007).

Les plus simples des prédicats sont les messages élémentaires que les transitions échangent entre elles. Cet échange prend la forme « *condition/action* » suivante : $?Mr/!Me$. Le point d'interrogation indique un message reçu et le point d'exclamation un message émis une fois la condition vraie, par la transition au moment du tir.

Dans les réseaux de Petri prédicats transitions, les variables associées aux jetons ne peuvent être modifiées que par un franchissement de transition (Sadou, 2007). En d'autres termes, ces variables ne peuvent avoir une évolution continue.

Des lois de probabilité des délais peuvent être associées aux transitions pour définir quand vont-elles être tirées. On parle alors de réseau de Petri stochastique.

RdP Stochastiques Après avoir vu comment modéliser l'évolution du système grâce au tir des transitions, il reste à déterminer quand ces évolutions se produisent effectivement.

Les réseaux de Petri stochastiques (Molloy, 1982; Natkin, 1980; Chiola *et al.*, 1993) sont obtenus à partir des réseaux de Petri classiques en associant des durées de franchissement aléatoires aux transitions. Ils permettent de prendre en compte, de manière plus structurée que les graphes de Markov, l'occurrence des défaillances et leur influence sur le comportement du système. En effet, le parallélisme étant pris en compte, ils permettent d'expliciter l'architecture du système en décrivant indépendamment les états des divers objets composant le système et leurs interactions.

Ils sont bien adaptés pour la construction de modèles d'évaluation de la sûreté de fonctionnement de systèmes en tenant compte des dépendances stochastiques qui peuvent résulter des communications entre les composants, de l'architecture (répartition des composants logiciels sur les composants du matériel), des procédures de tolérance aux fautes et de maintenance, *etc.* (Malhotra et Trivedi, 1994; Reibman et Veeraraghavan, 1991).

Les réseaux de Petri stochastiques généralisés (*GSPN - Generalized Stochastic Petri Nets*) sont une extension des réseaux de Petri stochastiques.

Réseaux de Petri Stochastiques Généralisés *(GSPN)* Un réseau de Petri stochastique généralisé est un 4-uplet tel que défini par l'expression 2.5.

$$GSPN = (PN, T_1, T_2, W) \tag{2.5}$$

où

- $PN = (P, T, I^-, I^+, M_0)$ est le réseau Place-Transition
- $T_1 \subseteq T$ est l'ensemble des transitions temporisées
- $T_2 \subset T$ représente l'ensemble des transitions immédiates, $T_1 \cap T_2 = \emptyset, T = T_1 \cup T_2$
- $W = (w_1, \ldots, w_{|T|})$ est un tableau ayant pour entrées $w_i \in \mathbb{R}$
  - w_i est un taux de distribution exponentielle négative des délais de tir lorsque t_i est une transition temporisée.
  - w_i est un poids de tir lorsque t_i est une transition immédiate.

Les GSPN (Ajmone Marsan *et al.*, 1984) permettent de prendre en compte, en plus de transitions avec des lois exponentielles, d'autres transitions dites *immédiates* tirées sans délai et qui sont prioritaires par rapport aux transitions à délai aléatoire (Medjoudj, 2006).

Les fonctions stochastiques sont de deux types : des fonctions stochastiques temporisées ou immédiates.

Les **fonctions stochastiques temporisées** sont décrites par le couple $< I, D >$ où I est l'ensemble des intervalles de tirs associés aux transitions stochastiques temporisées et D est l'ensemble des densités de probabilités associées à ces mêmes transitions.

A une transition stochastique temporisée t_k nous associons la fonction densité de probabilité $D(t_k) = d_k(x)$ définie sur un intervalle de tir statique $I(t_k) = [a, b]$ (intervalle de réels). Il n'y a pas d'effet mémoire, c'est-à-dire que chaque fois que t_k est sensibilisée par un nouveau $n - uplet$ de jetons, un nouvel intervalle $I(t_k)$ est associé au franchissement de t_k par ce $n - uplet$. Cet intervalle est effacé si t_k cesse d'être sensibilisée par ce $n - uplet$, par exemple si l'un des jetons de ce dernier est consommé par un franchissement de transition.

En ce qui concerne les **fonctions stochastiques immédiates**, elles sont telles qu'une probabilité fixe est associée à chaque transition concernée. Ces transitions sont utiles pour la prise en compte des défaillances à la sollicitation et sont immédiates. En général, un composant qui peut être défaillant à la sollicitation est représenté par une place représentant l'état *attente* du composant possédant deux transitions en sortie. A ces deux transitions, sont associées des probabilités p_1 (probabilité de panne à la sollicitation) et p_2 (probabilité de bon fonctionnement après sollicitation) et telles que $p_1 + p_2 = 1$.

Les GSPN ont l'avantage de permettre la génération automatique d'une chaîne de Markov à partir d'une description du comportement du système et des interactions entre ses composants, et offrent des moyens d'analyse et de vérification structurelle des modèles. Il existe plusieurs outils pour construire des modèles basés sur des RdPS et leurs extensions. A titre d'exemple, nous citons TimeNet, GreatSPN (Chiola *et al.*, 1995), SPNP (Ciardo et Trivedi, 1989).

Un aspect délicat dans la modélisation par GSPN concerne la maîtrise de la construction et du traitement de modèles complexes. La complexité résulte généralement du niveau de détail de la modélisation, du nombre de composants à modéliser explicitement et de leurs interactions.

Différentes méthodes ont été proposées pour maîtriser la complexité des modèles (Balbo, 1995), dont la plupart est basée sur le principe de décomposition et d'agrégation qui consiste à ne pas générer le modèle global, mais à construire des sous-modèles et à combiner les mesures obtenues par le traitement des sous-modèles afin de calculer les mesures du système global. On peut citer par exemple, les travaux basés sur les modélisations hiérarchiques et hybrides combinant des réseaux de Petri et d'autres formalismes tels que files d'attente (Balbo *et al.*, 1988), arbres de fautes et diagrammes de fiabilité (Balakrishnan et Trivedi, 1995), des méthodes exploitant des propriétés structurelles du modèle (Chiola *et al.*, 1993; Ziegler et Szczerbicka, 1995), *etc.* De façon générale, ces travaux imposent des restrictions sur les interactions entre sous-modèles qui ne sont pas toujours satisfaites quand on construit des modèles de sûreté de fonctionnement de systèmes réels induisant de fortes dépendances. Dans ce contexte, il est nécessaire de construire le modèle global et d'évaluer les mesures de sûreté de fonctionnement à partir de ce modèle.

Les analyses quantitatives ont de nombreux avantages car elles permettent :

- d'évaluer la probabilité des composantes de la sûreté de fonctionnement ;
- de fixer des objectifs de sécurité ;
- de juger de l'acceptabilité des risques en intégrant les notions de périodicité des contrôles, la durée des situations dangereuses, la nature d'exposition, *etc.* ;
- d'apporter une aide précieuse pour mieux juger du besoin d'améliorer la sécurité ;
- de hiérarchiser les risques ;
- de comparer et ensuite ordonner les actions à entreprendre en engageant d'abord celles permettant de réduire significativement les risques ;
- de chercher de meilleures coordination et concertation en matière de sécurité entre différents opérateurs ou équipes.

Bien que l'utilité des méthodes quantitatives soit indiscutable, ces dernières présentent tout de même un certain investissement en temps, en efforts et également en moyens logiciels, matériels et financiers. Par ailleurs, il peut s'avérer que cet investissement soit disproportionné par rapport à l'utilité des résultats attendus, le cas échéant l'analyse quantitative est court-circuitée pour laisser la place aux approximations qualitatives telles les retours d'expérience et jugements d'experts.

Un point très important mérite d'être clarifié, c'est que les résultats de l'analyse quantitative ne sont pas des mesures absolues, mais plutôt des moyens indispensables d'aide au choix des actions pour la maîtrise des risques. Nous citons par exemple l'évaluation par des techniques floues/possibilistes de la subjectivité des experts humains, ou la priorisation de certaines actions de maîtrise par rapport à d'autres par une analyse de type coût/bénéfices.

2.4.3 Méthodes de résolution

2.4.3.1 Problèmes de satisfaction de contraintes

Les problèmes de satisfaction de contraintes (CSP - *Constraint Satisfaction Problems*) permettent de modéliser de la connaissance et de raisonner sur celle-ci afin de trouver l'ensemble des solutions compatibles avec un problème courant. Les premiers problèmes de satisfaction de contraintes ont été définis par Montanari (Montanari, 1974) il y a une trentaine d'années.

Définition 1 : Problèmes de satisfaction de contraintes Les problèmes de satisfaction de contraintes sont définis comme un triplet $(V; D; C)$ où :

- $V = v_1; v_2; \ldots; v_k$ est un ensemble fini de variables,
- $D = d_1; d_2; \ldots; d_k$ est un ensemble fini de domaines de définition des variables,
- $C = c_1; c_2; \ldots; c_k$ est un ensemble fini de contraintes portant sur les variables.

Trouver les solutions d'un problème donné revient à résoudre le problème de satisfaction de contraintes, c'est-à-dire à traduire les fragments de connaissances élémentaires soit sous forme d'élément unique de C, soit sous forme de plusieurs éléments répartis sur le triplet $(V; D; C)$ (Vernat, 2004). C'est le niveau d'abstraction du fragment qui va déterminer si celui-ci est directement utilisable sous la forme d'une contrainte, ou s'il doit être décomposé.

Définition 2 : Solution d'un CSP Une solution d'un problème de satisfaction de contraintes est une instanciation de toutes les variables respectant toutes les contraintes.

Propagation des contraintes Propager cette contrainte se fait alors simplement par arc-consistance locale sur chacune des contraintes. La contrainte est modélisée sous la forme d'un graphe biparti, où sont représentées d'un côté les variables, de l'autre l'union des domaines des variables. Une arête entre une variable et une valeur indique que cette valeur fait partie du domaine de la variable. La contrainte est évidemment consistante si et seulement si le couplage maximum du graphe est de cardinalité n.

L'intégration de tels algorithmes permet de bénéficier de l'efficacité de techniques de recherche opérationnelle dans le cadre très souple de la programmation par contraintes. En d'autres termes, nous disposons d'une part d'algorithmes très efficaces de recherche opérationnelle mais dont le spectre d'utilisation est parfois réduit, et d'autre part de techniques plus générales de propagation de contraintes dont le spectre est beaucoup plus large mais dont l'efficacité reste souvent à démontrer.

Résolution des problèmes de satisfaction des contraintes Les méthodes *complètes* de résolution de CSP explorent de manière systématique l'espace de recherche et sont capables de fournir toutes les solutions d'un problème. L'algorithme de recherche de base le plus souvent utilisé est l'algorithme de retour arrière ou *Backtrack* (Golomb et Baumert, 1965). Cet algorithme met en place une stratégie de profondeur avec un mécanisme de retour arrière sur la situation précédente lorsqu'il détecte que l'affectation partielle courante [5]

5. Une affectation est partielle lorsque seul un sous-ensemble des variables est instancié.

n'est pas cohérente. Il est souvent amélioré par des heuristiques déterminant, par exemple, l'ordre des variables à instancier et l'ordre des valeurs à tester pour minimiser le nombre de branches à explorer.

Les méthodes de résolution dites *incomplètes* n'explorent pas de façon systématique l'espace de recherche. Elles sont basées sur une exploration opportuniste de l'ensemble des affectations complètes [6] et ne fournissent qu'un sous-ensemble de solutions. Elles nécessitent une fonction d'évaluation et de comparaison d'affectations. Nous pouvons citer la méthode de recherche tabou (Glover et Laguna, 1993) ou le recuit simulé (Kirkpatrick *et al.*, 1983). Ces méthodes incomplètes sont généralement utilisées pour résoudre des problèmes de taille élevée.

Les méthodes de résolution utilisées fournissent un ensemble de solutions. Il faut alors choisir la solution la mieux adaptée au problème de départ. Comme pour les raisonnements à base de cas, ce choix final requiert un effort de réflexion et d'analyse supplémentaire.

Cependant, nous menons cette recherche dans un contexte où intervient le phénomène de l'explosion combinatoire, puisque la taille du problème peut évoluer exponentiellement avec la dimension du réseau étudié.

2.4.3.2 Simulation de Monte Carlo

La simulation de Monte Carlo est une méthode numérique basée sur le tirage de nombres aléatoires (Kermisch et Labeau, 2002). Elle permet d'estimer l'espérance mathématique d'une variable aléatoire qui est une fonction de plusieurs paramètres. Elle permet également d'estimer toute quantité, déterministe ou stochastique, dont la valeur a pu être associée à l'espérance mathématique d'une variable aléatoire qui n'est pas directement liée à la physique du problème étudié.

La simulation de Monte Carlo (Batut, 1986; Desieno et Stine, 1964; Dubi, 2000) est une technique utilisée pour estimer la probabilité des résultats en répétant un grand nombre

6. Une affectation est complète lorsque l'ensemble de toutes les variables est instancié.

de fois une expérience à l'aide de la simulation et en utilisant des nombres aléatoires. La simulation est une méthode qui a pour but d'imiter un système réel. La simulation de Monte Carlo est utilisée lorsque d'autres analyses sont mathématiquement trop complexes ou trop difficiles à reproduire.

L'utilisation de la simulation Monte Carlo dans l'étude de sûreté de fonctionnement permet de lever l'hypothèse markovienne et permet de traiter des systèmes industriels. Depuis les années 80, différentes méthodes ont été développées, comme les méthodes de transitions forcées qui permettent de réduire le nombre d'histoires à simuler. D'autres techniques se sont basées sur la réduction de temps d'une histoire. Des méthodes pour accélérer la simulation ont été développées dans (Champagnat, 1998).

En général, la simulation de Monte Carlo est associée à une autre méthode, cette dernière modélise le comportement d'un système. La simulation de Monte Carlo permet de réaliser un grand nombre d'histoires du système modélisé. Un traitement statistique permet ensuite d'obtenir les résultats recherchés.

Un des avantages de la simulation de Monte Carlo est sa faible sensibilité à la complexité et à la taille des systèmes. Cependant, dans le cadre de la sûreté de fonctionnement, le modèle simulé est régi par des évènements très rares, les défaillances, et des évènements très fréquents, fonctionnement normal du système, et ce, simultanément. La simulation est alors cadencée par de nombreuses occurrences d'évènements fréquents qui ne reflètent pas le comportement du système en présence de défaillances. C'est le problème de simulation des évènements rares. Un nombre important d'histoires est nécessaire pour voir apparaître un évènement redouté, ce qui implique des temps de calcul importants. De nombreuses techniques d'accélération de la simulation permettent de réduire ces temps (Garnier, 1998). Elles sont basées soit sur une diminution de la complexité du modèle, soit sur la réduction du nombre de scénarios à simuler, en favorisant l'apparition des évènements rares. Toutefois, ces méthodes ne sont pas toujours faciles à mettre en œuvre, car elles impliquent des hypothèses assez fortes et/ou ne fournissent pas forcément des estimateurs de qualité.

L'inconvénient de la simulation de Monte Carlo, par rapport à d'autres méthodes analytiques, est la durée du temps de calcul nécessaire. Ceci est directement lié à la précision. Par exemple, la précision d'un paramètre évalué à partir de N tirages aléatoires est définie par la quantité $K(N, \alpha)$ de la fonction de Kolmogorov pour un seuil de risque α donné.

$$K(N, \alpha) = \sqrt{\frac{ln(\frac{2}{\alpha})}{2(N+1)}} \tag{2.6}$$

Par ailleurs, pour les systèmes complexes, les ingénieurs se limitent le plus souvent à exécuter des simulations Monte Carlo car celles-ci sont basées sur l'utilisation de générateurs de nombres aléatoires. Cette méthode est mal adaptée, en particulier dans l'étude des évènements qui se produisent avec une faible probabilité. Les simulations Monte Carlo doivent alors être répétées un si grand nombre de fois que le temps de calcul en devient rédhibitoire.

Avec l'augmentation de la puissance de calcul des machines, cette critique devient moins fondée et il convient de remarquer que les méthodes de Monte Carlo permettent toujours d'estimer l'intervalle de confiance des résultats obtenus, ce qui est généralement impossible pour les méthodes analytiques nécessitant de nombreuses approximations dans leur mise en œuvre.

Cette section a porté sur les méthodes d'évaluation du risque. Nous avons d'abord présenté les méthodes qualitatives incluant les méthodes basées sur l'analyse fonctionnelle et la matrice des risques, devenues un standard dans le monde industriel. Ensuite, nous avons discuté les méthodes quantitatives utilisées pour évaluer le risque des systèmes complexes comme les systèmes relatifs aux applications de sécurité. Autant de méthodes pour un seul objectif : évaluer. Un comparatif des méthodes étudiées s'impose.

2.5 Comparaison des méthodes d'analyse des risques étudiées

Les méthodes d'analyse des risques ont de nombreuses caractéristiques communes :

- Décomposition hiérarchique du système étudié en plusieurs éléments importants pour la sécurité ; un élément peut être un sous-système, un composant, une fonction ou un humain.
- Elaboration d'un lien entre les causes et les effets.
- Définition de la couverture des risques par la proposition et le suivi des mesures de protection ou de prévention.

L'AMDEC est une approche descendante qui tient compte des modes de défaillances de chaque composant pris séparément. Cette méthode permet une certaine forme de redondance avant que son exécution ne devienne fastidieuse. De même, les résultats peuvent être difficilement vérifiés par une personne connaissant mal le système.

Les principaux inconvénients de l'AMDEC sont la difficulté de traiter la redondance et l'intégration des actions de remise en état, ainsi l'accent est mis sur des défaillances de composant unique. Une autre difficulté spécifique aux AMDEC concerne le calcul de la fréquence d'occurrence d'une défaillance d'un composant isolé fonctionnant dans un système complexe dans lequel les défaillances induites sont fréquentes.

En ce qui concerne l'analyse par arbre d'évènements, elle peut être qualitative ou quantitative et elle est utilisée pour identifier les conséquences possibles, et si nécessaire, leurs fréquences du fait de l'apparition d'un évènement initiateur. Cette méthode est fréquemment utilisée dans des installations munies de dispositifs intégrés de réduction de risque. La technique inductive de l'analyse consiste à répondre à la question fondamentale « *qu'arrive-t-il si* ... ? ». La difficulté majeure de cette technique est le fait qu'elle ne peut être exhaustive

dans la phase d'identification des événements initiateurs. En outre, les arbres d'évènements traitent uniquement des états de succès et d'échec d'un système et il est difficile d'y intégrer des évènements de succès ou de récupération différés ; ce qui est indispensable s'agissant de systèmes non-cohérents(*cf.* section 2.5.1.4 page 2.5.1.4).

2.5.1 Lacunes des méthodes d'analyse des risques

2.5.1.1 Non prise en compte des facteurs externes au système

Les facteurs externes au système étudié (conditions climatiques, environnement, facteurs humains) sont rarement pris en compte ou alors pas suffisamment.

2.5.1.2 Subjectivité dans l'estimation des risques

Il est plus raisonnable de considérer que cette phase vise simplement à donner des indications sur les risques les plus significatifs en vue d'envisager des mesures de prévention et de protection. L'estimation des probabilités d'occurrence d'un événement redouté est souvent subjective. L'approche par intervalle, qui consiste à répartir les gravités et les occurrences sur une matrice de criticité avant d'attribuer les niveaux de risque à chaque zone de criticité (Gravité, Occurrence), semble être une technique discriminatoire étant donné qu'il n'existe aucune règle permettant de définir les limites de ces zones précitées. A ceci, s'ajoute aussi la subjectivité de l'analyste dans la désignation d'une zone plutôt qu'une autre.

Cependant, il existe des approches d'évaluation de la subjectivité dans l'estimation des risques, telles que les approches par les théories des sous-ensembles flous et la théorie des possibilités (Sallak *et al.*, 2008). Néanmoins, dans certaines méthodes, telles que l'analyse par arbre de défaillances, la propagation des probabilités de la base vers le sommet pour estimer la probabilité de l'évènement redouté est mathématiquement faisable. Cependant, la fiabilité des résultats dépend de l'estimation des probabilités affectées aux événements initiateurs (événements de base).

2.5.1.3 Non-exhaustivité

Il est quasiment impossible de tendre vers l'exhaustivité dans la phase d'investigation sur les causes et les conséquences des scénarios d'accident. Généralement, on se contente des causes et des conséquences les plus significatives.

La plupart des méthodes d'analyse des risques visent l'exhaustivité par l'utilisation de mots clés qui évoquent les défaillances à envisager. L'expérience montre qu'une utilisation rigoureuse de ces listes en groupe de travail, bien que nécessaire, peut s'avérer rapidement fastidieuse sans pour autant garantir la prise en compte de toutes les situations dangereuses : phases transitoires spécifiques, risque d'effet domino, perte d'utilités, *etc.* (Mazouni, 2008).

2.5.1.4 Non considération du fonctionnement des systèmes non-cohérents

Selon Kaufmann (Kaufmann *et al.*, 1975), « *un système est dit cohérent quand sa fonction de structure est monotone* ». Autrement dit, une nouvelle défaillance d'un composant ne remet pas en marche un système en état de panne ; de même, la réparation d'un composant défaillant ne remet pas en panne un système en marche. Par conséquent, pour pouvoir analyser un système non-cohérent, il est impératif de considérer non plus des ensembles d'événements, mais plutôt des séquences d'événements.

2.5.1.5 Non considération des défaillances en mode commun

L'analyse causale d'un sous-système ou d'un composant pris séparément n'est pas complète pour analyser le comportement de systèmes complexes caractérisés par des boucles fermées de rétro-action. Dans ce cas, le raisonnement causal linéaire devient circulaire (Rasmussen et Svedung, 2000).

La plupart des méthodes d'analyse des risques sont caractérisées par une causalité linéaire. Cependant, il existe tout de même un certain nombre de méthodes complémentaires telles

que l'Analyse des Défaillances de Mode Commun qui, comme son nom l'indique, permet d'examiner les défaillances simultanées relatives à des systèmes interagissant.

2.5.2 Critères de choix d'une méthode d'analyse des risques

Nous avons retenu l'essentiel des critères pesant dans la mise en œuvre d'une méthode plutôt qu'une autre dans l'étude d'un système donné :

- Domaine de l'étude
- Stade de l'étude (spécification, conception, ...)
- Perception du risque dans ce domaine
- Culture de la Sûreté de Fonctionnement de l'organisation
- Caractéristiques du problème à analyser
- Niveau envisagé de la démonstration de la sécurité
- Savoir-faire des intervenants
- Nature des informations disponibles (spécifications du système et de ses interfaces, contraintes, ...)
- Retour d'expérience et bases de données disponibles
- Moyens humains, logistiques et autres
- Délais et autres contraintes de management de projet

Toutefois, l'utilisation séparée d'une seule méthode d'analyse des risques peut ne pas apporter une démonstration définitive de la réalisation des objectifs de sécurité. En effet, il est nécessaire de combiner plusieurs méthodes pour une meilleure complétude et une bonne cohérence en termes de résultats.

2.6 Conclusion

Nous avons essayé tout au long de ce chapitre de mieux situer la notion d'évaluation des risques des systèmes complexes. Nous avons d'abord clarifié les concepts clés à savoir

le danger, le risque et la sécurité à travers des définitions issues principalement des normes. Ensuite, nous avons présenté rapidement les principales méthodes d'évaluation des risques sachant qu'il existe d'autres méthodes moins utilisées dans un contexte industriel telles que : Analyse des Défaillances de Mode Commun, Modèles de Conséquences, Listes des contrôles, Technique de Delphi, Indice de danger, Comparaison par paires, Analyse transitoire, *etc.*

Après avoir essayé de déceler les points forts et points faibles de ces méthodes d'analyse des risques, nous avons trouvé intéressant de proposer des critères de choix de la méthode la plus convenable à une étude donnée. Il s'est avéré ainsi qu'aucune de ces méthodes n'est utilisable directement dans le cadre de notre étude. Il nous faut donc combiner plusieurs méthodes pour une meilleure complétude de la méthodologie à proposer.

Chapitre 3

Méthodologie pour l'évaluation des risques fondée sur les réseaux de Petri

Sommaire

3.1 Introduction

Nous avons présenté dans le chapitre précédent quelques approches d'évaluation des risques tant qualitatives que quantitatives, tant semblables que différentes. En effet, ces approches ont toutes le même objectif qu'est d'évaluer le risque mais chacune propose un point de vue sépcifique et nécessite des connaissances techniques et physiques de l'implémentation du système, notamment des aspects dynamiques, qui sont aussi un véritable nid à risques.

La Commission Européenne, souhaitant harmoniser le système ferroviaire, ne peut entreprendre cette démarche qu'à un niveau de description qui le permet, c'est-à-dire le niveau fonctionnel ; ce qui rend caduques les approches d'évaluation des risques.

Dans ce chapitre, nous commençons par analyser le modèle fonctionnel du système ferroviaire développé par l'AEIF. Ensuite, nous proposons une méthodologie de raffinement progressif de ce modèle fonctionnel vers des modèles dynamiques exploitables. Une telle décomposition permettra par la suite d'évaluer les niveaux de risque et la manière de les répartir aux instances responsables de l'implémentation des fonctions.

3.2 Décomposition fonctionnelle

3.2.1 Architecture ferroviaire fonctionnelle

Selon la Directive Sécurité (dir, 2004a), le système ferroviaire peut être défini comme « l'ensemble des sous-systèmes fonctionnels, structurels et logiques ». Cet ensemble, constitué par les infrastructures ferroviaires, comprend non seulement les lignes et installations fixes du réseau ferroviaire, les matériels roulants de toutes catégories et origines qui parcourent ces infrastructures ; mais aussi la gestion et l'exploitation du système. L'AEIF a produit des fonctions de départ pour une architecture générique du système ferroviaire (Gigantino, 2002). Ces fonctions contiennent la plupart des Paramètres Fondamentaux (BP - BASIC PARAMETERS) pour l'interopérabilité ; constituants de base du système ferroviaire.

L'analyse fonctionnelle du système ferroviaire, développée par l'AEIF, couvre la chaîne complète du transport ferroviaire. Elle représente aussi une décomposition systématique et cohérente des fonctions jusqu'à quatre niveaux de décomposition respectant les exigences fonctionnelles de décomposition. A cet effet, douze fonctions ferroviaires ont été définies afin de représenter le système ferroviaire dans sa globalité (Rafrafi, 2007).

Fonction	Description
F1	Support and Guide the Train
F2	Supply the train
F3	Load Freight
F4	Load Passengers
F5	Move rolling stock
F6	Maintain and Provide data on rolling stock, infrastructure and time table
F7	Prepare operation of train
F8	Operate a train
F9	Evaluate transport quality
F15	Provide service for passengers
F16	Provide Service for freight
F17	Manage human resources

Tableau 3.1: Fonctions ferroviaires établies par l'AEIF (Rafrafi *et al.*, 2006)

Cette méthode d'analyse proposée par l'AEIF est basée sur une analyse du système struc-

turée selon différents points de vue dédiés chacun à un aspect du système : Fonctionnel, Structurel et Logique 3.1, avec des spécifications et des exigences bien définies (Chatel *et al.*, 2003).

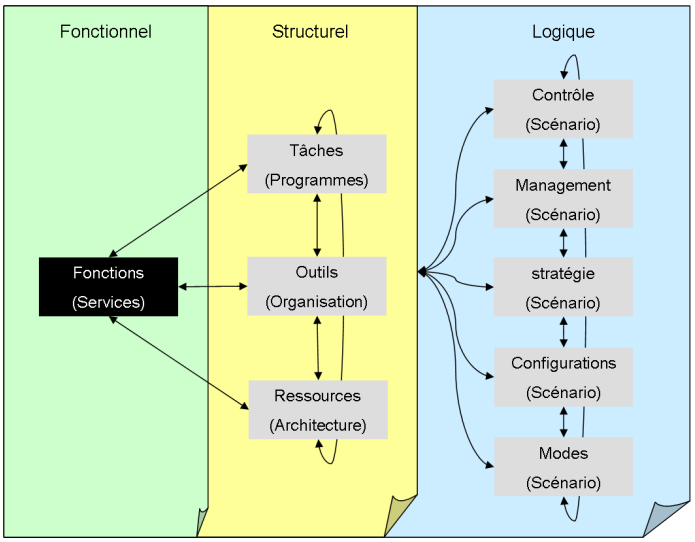

FIGURE 3.1: Matrice d'analyse ferroviaire

Cette méthode d'analyse systémique est donc fondée sur une matrice à trois perspectives :

- Aspect **Fonctionnel**. Cette analyse vise à identifier les fonctions du système et leurs définitions, caractéristiques et relations. Elle ne tient compte d'aucune notion de temps. Les invariants et propriétés de sûreté du système sont liés à ce point de vue. L'utilisation des entrées, dans certaines conditions, et la génération des sorties, qui doivent respecter un certain nombre de conditions, sont les issues principales à cette étape d'analyse (Chatel *et al.*, 2003).
- Aspect **Structurel**. Il est principalement lié aux tâches, ressources et dispositifs alloués pour exécuter les fonctions du système. Le réseau des ressources constitue l'architecture ferroviaire. Tous les constituants de l'architecture doivent fonctionner sous un ensemble de contraintes comme la sécurité et l'interopérabilité.
- Aspect **Logique**. Cet aspect couvre le mode de fonctionnement du système (nominal, dégradé), sa configuration et des contextes opérationnels. Ces paramètres sont organisés suivant un scénario (par exemple scénario des changements de configurations) et

interagissent continuellement.

3.2.2 Vers une modélisation à niveaux

Notre point de départ étant un modèle en couches où chaque couche dispose de paramètres et contraintes spécifiques, l'approche proposée pour l'évaluation de la sécurité est basée sur l'identification de la probabilité du risque pour chaque fonction du système tout en respectant les règles suivantes :

- les différents ensembles fonctionnels doivent être aussi indépendants que possible avec un minimum d'effets interactifs sur d'autres ensembles ;
- la décomposition du système en (sous-)fonctions au niveau bas où la communication entre (sous-)fonctions doit être réduite au maximum.

Nous pouvons considérer que cette approche est utile dans le sens où elle permet de fournir à chaque Gestionnaire d'Infrastructure (GI) ou Entreprise Ferroviaire (EF) un niveau de fiabilité pour chaque fonction.

Etant fondée sur une décomposition fonctionnelle du système, notre approche se déroule en quatre étapes (Rafrafi *et al.*, 2006) :

1. Construire le modèle fonctionnel SADT correspondant à l'architecture ferroviaire développée par l'AEIF.
2. Choisir le critère d'acceptation des risques qui sera adopté par la Commission Européenne dans le but de se conformer à la réglementation en vigueur.
3. Transformer le critère d'acceptation des risques en Indice de Sécurité S qui est un pourcentage relatif à la fiabilité requise pour le système. La génération de cet indice S renvoie un Indice de Fiabilité φ_j, relatif à chaque fonction.
4. Propager l'Indice de Sécurité dans la décomposition fonctionnelle. Le mode de calcul de cet indice est défini par les experts du domaine.

Pour ce faire, nous avons formulé l'objectif de départ suivant : développer une approche de décomposition du système qui permette une allocation des objectifs de sécurité en tenant

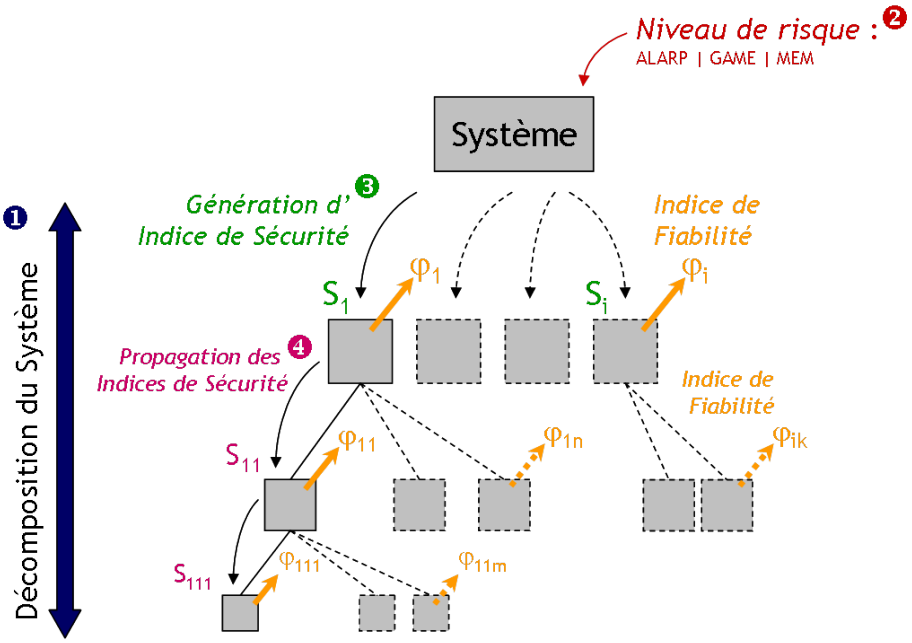

FIGURE 3.2: Approche en 4 étapes

compte des performances du système en termes de fiabilité. En d'autres termes, après avoir défini, à partir des documents réglementaires (directives, STI, normes ...), la probabilité de risque allouée aux fonctions ferroviaires, une approche verticale ascendante est opérée sur le système afin de considérer son risque global (Rafrafi et El Koursi, 2008a). Ce niveau de risque doit respecter les objectifs de sécurité conformément au critère d'acceptation des risques adopté.

Si des dangers sont identifiés avec différents niveaux de détail, à savoir des dangers de haut niveau d'un côté et des sous-dangers détaillés de l'autre, il convient de prendre des précautions pour éviter leur classification erronée en tant que dangers associés à des risques largement acceptables. La contribution de tous les dangers associés à des risques largement acceptables ne peut pas dépasser une certaine proportion (par ex. $y\%$) du risque global au niveau du système. Cette vérification est nécessaire pour éviter de rendre la justification caduque en subdivisant les dangers en de nombreux sous-dangers de bas niveau. En effet, si un danger est exprimé sous la forme d'un grand nombre de sous-dangers « plus petits », chacun de ces sous-dangers peut facilement être classé comme étant associé à des risques

largement acceptables s'il est évalué indépendamment, alors que ces sous-dangers évalués ensemble (en tant qu'un danger de haut niveau) sont associés à un risque significatif. La valeur de la proportion (par ex. $y\%$) dépend des critères d'acceptation des risques applicables au niveau du système. En adoptant le critère GAME, cette valeur sera être estimée sur la base de l'expérience opérationnelle de systèmes de référence similaires.

L'idée de notre approche est de considérer le système étudié comme l'objet d'une révision à intervalles réguliers, en tenant compte de l'évolution générale de la sécurité ferroviaire.

En fonction des choix techniques ayant présidé à la conception d'un système, de ses sous-systèmes et de ses équipements, de nouveaux dangers peuvent être identifiés pendant la « *démonstration de conformité aux exigences de sécurité* ». Ces nouveaux dangers, ainsi que les risques associés, doivent être considérés comme de nouveaux éléments pour une nouvelle boucle du processus itératif d'appréciation des risques.

Il s'agit donc de prendre en compte les nouvelles fonctions intervenant dans un système ferroviaire pour toujours répondre aux exigences de sécurité du système dans sa globalité. Ainsi, les indices de sécurité attribués à chaque fonction sont mis à jour au moyen d'une redistribution transversale. La vision homogène de chaque niveau de fonctions est exigée pour garantir la conformité de l'approche à la directive européenne de sécurité.

3.2.3 Intégration des paramètres fondamentaux

Le niveau le plus bas des fonctions concerne les paramètres fondamentaux (BP) du système ferroviaire. Ces composants relèvent de toute condition réglementaire, technique ou opérationnelle, critique sur le plan de l'interopérabilité et qui doit faire l'objet d'une décision avant l'élaboration des projets de STI par l'organisme commun représentatif (dir, 2001).

Selon la directive européenne de sécurité (dir, 2004a), les Objectifs de Sécurité Communs (OSC) définissent les niveaux de sécurité qui doivent être au moins atteints par les différentes

parties du système ferroviaire et le système dans son ensemble dans chaque Etat membre, exprimés sous forme de critères d'acceptation de risques suivants :

- les risques individuels auxquels sont exposés les passagers, le personnel, y compris le personnel des contractants, les utilisateurs des passages à niveau et autres, et - sans préjudice des législations nationales et internationales existantes en matière de responsabilités -, les risques individuels auxquels sont exposées les personnes non autorisées se trouvant sur les installations ferroviaires ;
- les risques pour la société.

Afin d'évaluer si les risques maîtrisés par l'application de l'estimation des risques explicites sont acceptables ou non, des critères explicites d'acceptation des risques sont nécessaires.

Ceux-ci peuvent être définis à différents niveaux d'un système ferroviaire. Ils peuvent être considérés comme une « *pyramide de critères* » (*cf.* Figure 3.3) telle que définie dans (Jovicic, 2009). En partant des critères d'acceptation des risques de haut niveau (exprimés par exemple comme des risques sociétaux ou individuels), la démarche descendante atteint les sous-systèmes et composants couvrant les systèmes techniques et comprenant les opérateurs humains pendant les activités d'exploitation et de maintenance du système et des sous-systèmes.

L'acceptation finale des risques calculés se base sur la comparaison du niveau de risque acceptable avec le niveau de risque maximum, d'une part pour le sytème global et d'autre part, pour les paramètres fondamentaux.

Bien que les Critères d'Acceptation des Risques (CAR)contribuent à réaliser les performances de sécurité du système, et qu'ils soient donc liés aux OSC, il est très difficile d'élaborer un modèle mathématique entre eux.

Cette pyramide validée par l'ERA rejoint donc notre démarche pour l'évaluation de la sécurité.

Le niveau auquel sont définis les critères d'acceptation des risques doit correspondre à l'importance et à la complexité du changement significatif. Par exemple, il n'est pas néces-

saire d'évaluer le risque global du système ferroviaire lorsque l'on modifie un type d'essieu sur le matériel roulant. La définition des critères d'acceptation des risques peut se focaliser sur la sécurité du matériel roulant. Réciproquement, des changements ou des ajouts importants apportés à un système ferroviaire ne doivent pas être évalués uniquement sur la base des performances de sécurité des fonctions ou changements ajoutés. Il convient également de vérifier, au niveau du système ferroviaire, que le changement est acceptable dans son ensemble.

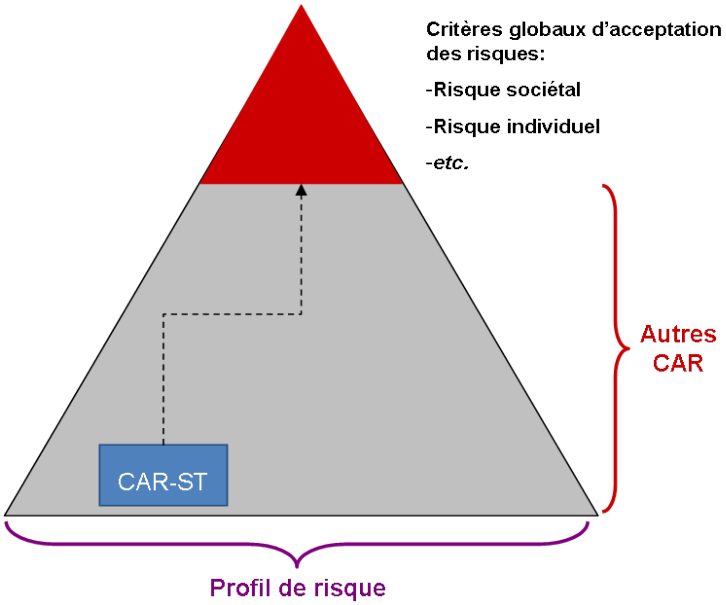

FIGURE 3.3: Pyramide des critères d'acceptation des risques (Jovicic, 2009)

Afin d'étudier la complémentarité des trois classes d'architecture, *logique* résultant de la projection d'une architecture *fonctionnelle* sur une architecture *structurelle* - associée à la structure du système - (Cauffriez, 2005), il tient lieu d'étudier d'une part, la caractérisation, l'identification et la représentation des dépendances au sein de l'architecture ferroviaire fonctionnelle ; et d'autre part, de quantifier des paramètres en prenant en compte les aspects dynamiques.

A cet effet, la technique de la propagation des contraintes semble s'adapter particulièrement à notre approche de décomposition fonctionnelle puisqu'il s'agit, à chaque étape, de considérer les exigences de sécurité dans le transport ferroviaire (Rafrafi et El-Koursi, 2008;

Rafrafi et El Koursi, 2008b). D'une façon générale, la progagation des contraintes s'attaque au problème d'allocation des ressources, analogue à notre problème d'allocation des objectifs de sécurité. L'un des intérêts majeurs de cette technique est que les contraintes sont utilisées dans un processus déductif en ce sens que la propagation peut permettre de détecter rapidement une inconsistance et donc d'accélérer le traitement du problème. Par contre, vue la complexité du système, plusieurs solutions d'affectation risquent d'être éligibles simultanément. En d'autres termes, il n'est pas impossible que plusieurs répartitions des risques sur les fonctions de base du système de transport conduisent à un même niveau global de sécurité, tout en vérifiant les contraintes locales.

Se fait donc sentir le besoin de s'orienter vers une technique plus formelle qui prenne en compte tant l'explosion combinatoire que les contraintes temporelles associées au modèle. Le modèle ferroviaire étant décomposable en couches, nous proposons de modéliser ces dernières à l'aide d'un outil unificateur permettant de gérer les aspects dynamiques, les capacités d'évaluation et la facilité de composition.

3.3 Approche modulaire

Dans le cadre de notre démarche d'évaluation du risque global des systèmes ferroviaires (CF. Section 3.6 page 115), il devient inconditionnel de gérer la complexité des systèmes.

Le modèle fonctionnel étant un modèle en couches, un raffinement de manière modulaire s'y prête. Le raffinement modulaire est caractérisé par une relation de collage entre les états de deux systèmes de transitions et par un ensemble de relations qui lient ces deux systèmes de transitions. Quels sont les objectifs d'une approche modulaire ? Quelles en sont les caractéristiques ?

La méthodologie à base de composants est une technique prometteuse et implique la méthode développée de la conception orientée objet. Elle utilise des concepts hiérarchiques et modulaires pour concevoir et analyser des systèmes.

Afin de réduire le coût de production d'un système, cette approche se sert de composants *indépendants*, *interactifs* et *réutilisables*. La littérature de l'ingénierie à base de composants a différencié plusieurs approches (Gössler *et al.*, 2007; Bastide *et al.*, 2004; Heck *et al.*, 2009) qui se sont concentrées sur les aspects du développement de composants. Cependant, la réutilisation de composants disponibles, prêts à l'emploi diminue le temps requis pour la modélisation de nouveaux systèmes (Seyler et Aniorte, 2002). Cela peut être fait en choisissant les composants appropriés basés sur les besoins et ensuite leur assemblage pour construire un nouveau modèle.

Il existe différentes méthodes logicielles pour la spécification des composants ; du Langage de Description d'Interface (CORBA, *etc.*), aux méthodes formelles telles les Réseaux de Petri (Chachkov et Buchs, 2001). Malgré les différences entre ces méthodes, elles ont un concept commun : un composant est une boîte noire à laquelle on a accès par le biais d'interface (Masri, 2009).

Dans cette section, nous précisons les caractéristiques principales que doit vérifier une approche à base de composants.

3.3.1 Objectifs d'une approche modulaire

L'analyse des applications de cette approche révèle que les techniques modulaires sont employées pour répondre à deux types d'exigences :

- gérer des niveaux de complexité que les méthodes centralisées classiques ne sont pas aptes à traîter.
- apporter de nouvelles propriétés telles que la flexibilité ou la possibilité de distribution qu'un traitement classique ne possède pas.

3.3.2 Gestion de la complexité

Le problème de la simulation peut s'avérer très complexe ou impossible. L'outil numérique atteignant ses limites, le nombre de paramètres utilisés impliquant des temps de calculs prohibitifs ; les relations entrant en jeu entraînent des instabilités numériques.

Une idée naturelle, face à la complexité, consiste à décomposer le problème afin d'identifier des sous-problèmes plus simples à résoudre. La complexité se situe alors dans la nature des interactions entre les différents composants dont il faut contrôler la stabilité. Cette complexité est alors considérée comme une propriété émergente issue d'un échange d'informations entre composants autonomes.

Même si l'approche modulaire est plus coûteuse en temps de calculs car elle conduit à un plus grand nombre d'équations à résoudre, ceci est atténué par la possibilité de distribuer et de calculer en parallèle des sous-systèmes relativement simples.

3.3.3 Propriétés

Une modélisation modulaire permet, en plus de la gestion de la complexité, de conférer au modèle des propriétés nouvelles. Pour la plupart des systèmes, l'interaction n'intervient qu'au niveau graphique au moment des assemblages. Le système est donc fermé et, en général, adapté à une seule classe de problème. Cependant, un modèle global construit par assemblage de modules élémentaires peut être modifié très simplement par le remplacement d'un de ces modules. Le modèle est flexible et peut donc être modifié au cours de la simulation.

3.3.3.1 Généricité

La généricité est utilisée dans l'ingénierie à base de composants pour augmenter le temps de productivité et la qualité de développement des systèmes. Le composant générique se réfère à un composant qui met en œuvre un processus ou une partie d'un jeu de processus et s'adapte à des besoins différents.

La générécité d'un composant est basée sur son indépendance. C'est un concept important pour des méthodes de haut niveau parce qu'il peut augmenter leur niveau d'abstraction.

Les composants génériques sont utilisés pour construire des systèmes de composants standards. On peut voir un composant générique comme un élément paramétrable. Les paramètres devraient être indiqués et une version spécifique du composant est créée et utilisée.

Un autre avantage consiste en ce qu'un composant générique peut être représenté comme une usine générique, cela créera tant de composants au besoin pour l'application. Ainsi, le principal objectif de la généricté est d'intégrer les approches à base de composants aux approches techniques.

3.3.3.2 Modularité

Les modèles modulaires sont plus faciles à concevoir comparés aux modèles complexes semblables. « *La modularité a un système complexe composé des sous-systèmes plus petits qui peuvent être gérés indépendamment* » (Langlois, 2002).

Huang (Huang et Kusiak, 1998) présente la modularité comme étant « *utilisée pour décrire l'utilisation d'unités communes pour créer les variantes d'un système* ». L'objectif de la modularité est la capacité d'identifier des entités homogènes, compatibles et indépendantes afin de satisfaire les besoins d'un système ou une application.

La conception modulaire aspire à organiser des systèmes complexes comme un jeu de composants ou modules. Ces composants peuvent être développés indépendamment et assemblés ensemble par la suite.

Ils peuvent être des unités séparables ou inséparables (Foster, 1995). La décomposition d'un modèle de système en modules plus petits a les avantages suivants :

1. Un modèle modulaire peut être très près du système réel, puisqu'il reflète la structure hiérarchique inhérente au système.
2. Il est possible de se concentrer sur chaque composant comme un petit problème.

3. Réutiliser des composants agissant seuls permet une réduction des coûts.
4. Les composants trop complexes peuvent perdre certains de leurs détails et leurs interactions peuvent être affectées. Un composant peut être divisé en composants plus petits jusqu'à obtenir des modules de taille gérable.
5. Le modèle modulaire permet d'évaluer chaque composant séparément.
6. Les changements de mise en œuvre et corrections sur des composants simples sont plus faciles à entreprendre.
7. La documentation de la structure modulaire est plus facile.

3.3.3.3 Réutilisabilité

Le concept de composant réutilisable est généralement semblable à celui de composant générique. L'implication de réutilisabilité est que les composants disponibles doivent donner assez d'*informations* pour faciliter l'assemblage des composants dans un nouveau système.

Les informations doivent détailler la configuration et la dépendance. Ainsi, pour faire le bon choix quant à la sélection et la réutilisation des composants, les informations suivantes sont exigées :

1. *Spécification opérationnelle* : l'interaction sémantique du composant ;
2. *Contexte d'opération* : où et comment le composant sera utilisé ? ;
3. *Propriétés non-fonctionnelles* : description des propriétés comme la performance, la sécurité et la fiabilité ;
4. *Interfaces exigées et ressources* : la fonctionnalité et les ressources nécessaires pour le composant dans l'exécution de sa fonctionnalité.

Puisque tous les systèmes réels sont faits de composants, des systèmes à base de composants sont faits de composants multiples (Brown et Wallnan, 1996) qui :

- sont prêts et disponibles, provenant d'une source commerciale ou réutilisés, d'un autre système ;

- ont une fonctionnalité et complexité combinées significatives ;
- sont indépendants et peuvent être exécutés indépendamment ;
- seront utilisés tels quels sans modification ;
- doivent être combinés à d'autres composants pour obtenir la fonctionnalité désirable.

3.3.3.4 Abstraction des composants

On considère les composants modélisés comme la boîte noire où la fonctionnalité interne est cachée, tandis que les interfaces représentent le service que l'on peut associer à ce composant. Chaque composant ou module est caractérisé par son comportement interne. Ses interfaces sont choisies pour révéler le moins possible sa mise en œuvre interne.

L'abstraction de composants est utile pour réduire la complexité de conception par décomposition d'un problème en composants connectés. Elle décrit le comportement fonctionnel des composants (Sametinger, 1997), c'est-à-dire les composants sont considérés comme spécifiques à une application.

L'abstraction se focalise sur les caractéristiques importantes des composants du point de vue du concepteur. Ainsi, pendant la conception de composants, nous devons nous concentrer sur la bonne définition du service offert par le composant et par ses interfaces ainsi que les paramètres à adapter pour l'application des exigences ; plutôt que de passer du temps pour la description de son comportement interne. Cela peut être réalisé en donnant des noms appropriés aux interfaces et aux paramètres et en les documentant.

Tous ces avantages nous poussent à utiliser l'approche à base de composants pour la modélisation d'une approche d'évaluation des risques. La réutilisation des composants est très importante dans la modélisation de la plupart des parties de système. Avec la réutilisation des composants déjà modélisés, le temps et le coût de modélisation sont réduits.

Un bon modèle modulaire se révéle être donc un modèle *générique* ayant une capacité à

faciliter la *composition* et l'*abstraction*. Ces deux propriétés, outre l'étude comportementale du système, ne sont autres que les caractéristiques des réseaux de Petri.

3.4 Réseaux de Petri

Pour notre démarche de modularisation, deux grandes familles, qui ne sont évidemment pas étanches, peuvent se distinguer. Elles correspondent à trois domaines sémantiques : la *sémantique discrète* (RdP Places Transitions, RdP Prédicats Transitions) pour les comportements qui peuvent se représenter par des graphes finis ou dénombrables d'états ; la *sémantique temporelle* (RdP temporels) pour les comportements liés au temps et la *sémantique stochastique* (RdP Stochastique) pour les comportements qui incluent des distributions de franchissement et conduisent à des processus stochastiques (chaînes de Markov, *etc.*).

3.4.1 Réseaux de Petri Places/Transitions

Définition Un réseau de Petri places/transitions R est un triplet (P, T, W) défini par la donnée :

- d'un ensemble fini non vide de places $P = p_1, \ldots, p_m$, où $|P| = M$;
- d'un ensemble fini non vide de transitions $T = t_1, \ldots, t_n$, où $|T| = N$, avec $\mathbb{P} \cap \mathbb{T} = \emptyset$;
- d'une relation d'incidence $W : P \times T \cap T \times P \mapsto N$ correspondant aux arcs :
  - $W(p,t)_{p \in P, t \in T}$ contient la valeur entière associée à l'arc allant de p à t ;
  - $W(t,p)_{p \in P, t \in T}$ contient la valeur entière associée à l'arc allant de t à p ;
  - dans le cas où une place p n'est pas reliée à la transition t, on a simplement $W(t,p) = 0$ et $W(p,t) = 0$.

3.4.2 Réseaux de Petri Temporels

RdP Temporels Les RdP temporels ont été introduits par Merlin (Merlin, 1974).

Un réseau de Petri temporel est une paire $< R, I >$ où :

- R est un réseau de Petri $< P, T, Pre, Post >$ auquel est associé un marquage initial M_0,
- I est la fonction d'intervalle initial qui associe à chaque transition un intervalle fermé rationnel $I(t) = [a, b]$ qui décrit une durée de sensibilisation de la transition t.

RdP temporisés Introduits par Ramchandani (Ramchandani, 1973), les réseaux de Petri temporisés sont caractérisés par des temporisations d'abord associées aux transitions (*t-temporisés*), puis aux places (*p-temporisés*). La temporisation représente alors la durée minimale de tir ou le temps de séjour minimum d'un jeton dans une place (ou durée exacte avec une règle de fonctionnement au plus tôt). Les RdP t-temporisés et p-temporisés sont équivalents et sont une sous-classe des réseaux de Petri temporels (Cassez et Roux, 2003).

Cette classe sera utilisée pour la modélisation de la couche structurelle (*cf.* 3.6.3.1 page 122).

3.4.3 Réseaux de Petri Stochastiques

3.4.3.1 Considérations préliminaires et définitions

Sur des réseaux de Petri étendus temporellement, on peut introduire la notion de trajectoire temporisée $\sum_{temp}$ qui représente une séquence de marquages avec la séquence des tirs de transitions et les dates d'entrée dans les marquages :

$$\sum_{temp} = \{(\tau_0, M_{(0)}); (\tau_1, M_{(1)}); ; (\tau_l, M_{(l)}); (\tau_{l+1}, M_{(l+1)})\} \tag{3.1}$$

$M_{(l)}$ et le l^{ime} marquage atteint ; $t_{(l)}$ est le l^{ime} tir de transition, $\tau_{(l)}$ est la date d'entrée dans le marquage, $\tau_{l+1} - \tau_l$ est la durée du séjour dans le marquage $M_{(l)}$. Pour l'observation de la trajectoire à partir de τ_l et jusqu'à τ_{l+1}, le déroulement depuis τ_0 jusqu'à τ_l consitue l'histoire notée Z_l.

Les réseaux de Petri stochastiques sont des réseaux de Petri étendus temporellement dont l'ensemble des trajectoires temporisées est muni d'une mesure de probabilité telle que le couple (marquage, instant d'entrée dans le marquage) constitue un processus stochastique (Juanole et Gallon, 1998). L'étude de ce processus stochastique suppose que, pour tout l, $Z(l)$ et $M(l)$ et pour toutes les transitions sensibilisées en $M(l)$; on peut définir de manière unique la probabilité, appelée aussi *noyau* de l'équation 3.2.

$$D_k(x/Z_{(l)}, M_{(l)}) = \text{Prob}\{t_k \text{tirée}, \tau_{l+1} - \tau_l \leq x/Z_{(l)}, M_{(l)}\} \tag{3.2}$$

Le noyau permet d'exprimer la probabilité que la transition t_k soit la prochaine transition tirée, limite de $D_k(x/Z_{(l)}, M_{(l)})$ lorsque $x \longrightarrow \infty$, ainsi que la distribution du temps de séjour dans $M_{(l)}$ ($D_k(x/Z_{(l)}, M_{(l)})$, la somme portant sur l'ensemble des transitions sensibilisées en $M_{(l)}$).

3.4.3.2 Définition

Un réseau de Petri stochastique est un réseau de Petri marqué et dans lequel, d'une part, on associe, à toute transition t_k, une variable temporelle aléatoire k caractérisée par une fonction de réparation $F_k(x/M_{(l)})$; et, d'autre part, on définit une politique d'exécution qui permet de calculer le noyau $D_k(x/Z_{(l)}, M_{(l)})$ et donc de caractériser le processus stochastique du marquage.

3.4.3.3 Politique d'exécution et processus stochastique

La politique d'exécution comprend deux volets : la sélection de la transition à tirer dans un marquage [1] ; la prise en compte, dès l'instant d'entrée dans un marquage, de l'histoire ou mémoire temporelle [2].

1. Ceci se pose lorsque plusieurs transitions sont simultanément sensibilisées dans un marquage
2. Ceci se pose dans tout marquage

En ce qui concerne la sélection de la transition à tirer, on distingue deux techniques : la compétition, qui consiste à tirer la transition dont la variable temporelle aléatoire est statistiquement la plus petite [3] ; la présélection, qui consiste à attribuer aux transitions des probabilités de franchissement.

Par ailleurs, afin de prendre en compte de la mémoire temporelle, on distingue trois techniques : la réinitialisation qui consiste en une remise à zéro de la mémoire temporelle (après le tir d'une transition, toutes les transitions simultanément sensibilisées avec cette dernière voient leur fonction de répartition initialisée) ; la mémoire de toutes les périodes de sensibilisation qui considère que la mémoire temporelle d'une transition commence dès qu'elle devient sensibilisée pour la première fois et se maintient - même lorsqu'elle est désensibilisée - , jusqu'à ce qu'elle soit effectivement tirée. La mémoire de la dernière période de sensibilisation qui considère que la mémoire est opérationnelle uniquement tant que la transition reste sensibilisée (Juanole et Gallon, 1998).

Les combinaisons techniques pour la prise en compte de la mémoire temporelle reposent sur les principes telles que la combinaison de la présélection avec la réinitialisation sont intéressantes pour modéliser des activités conflictuelles qui ne peuvent se dérouler en parallèle. Par contre, la combinaison de la présélection avec les techniques de mémoire temporelle ne peut être envisagée. En effet, suivant la présélection effectuée, on pourrait aboutir à la situation aberrante où plusieurs activités se déroulent en parallèle et où l'activité présélectionnée a la durée la plus longue ; ce qui empêcherait des activités plus courtes d'induire un changement de marquage.

En ce qui concerne la compétition, sa combinaison avec la mémoire de toutes les périodes de sensibilisation est intéressante pour modéliser la préemption (ordonnancement, sûreté de fonctionnement), sa combinaison avec la mémoire de la dernière sensibilisation est intéressante pour la modéliser.

La nature du processus stochastique de marquage dépend évidemment de la technique

3. Notons que l'on ne peut appliquer cette technique si on a des transitions simultanément sensibilisées avec des distributions déterministes identiques

de prise en compte de la mémoire temporelle :

- si on considère la réinitialisation, le noyau ne dépend plus de l'histoire $D_k(x/M_{(l)})$ et donc le processus stochastique du marquage est un processus semi-markovien quelles que soient les fonctions de répartition des variables temporelles aléatoire γ_k (chaque marquage est un point de régénération). Avec la présélection, on a : $D_k(x/M_{(l)}) = q_k F_k(x/M_{(l)})$, q_k étant la probabilité du choix t_k ; avec la compétition, on a l'équation 3.3.

$$D_k(x/M_{(l)}) = \int x 0 \Pi_{j \neq k}(1 - F_j(u/M_l)) dF_k(u/M_l) \tag{3.3}$$

- si on considère la mémoire de toutes les périodes de sensibilisation ou de la dernière sensibilisation (dans des cas, seule la technique de compétition peut être envisagée), le noyau dépend de l'histoire $Z_{(l)}$ et donc, on ne peut conclure à ce niveau sur le type du processus stochastique (Juanole et Gallon, 1998). Cela dépend des types de fonctions de répartition des γ_k qui doivent être évaluées en fonction de leur âge a_k). Le noyau a une expression identique à celle indiquée ci-dessus dans le cas d'une réinitialisation avec compétition, les fonctions de répartition des γ_k apparaissant avec leur âge.

Cette classe sera utilisée pour la modélisation de la couche fonctionnelle (*cf.* 3.6.3.2 page 122).

3.4.4 Réseaux de Petri Prédicats Transitions

Les réseaux de Petri Prédicats/Transitions modélisent la structure physique du système ferroviaire.

Donnons une définition simplifiée des RdP à Prédicats/Transitions (Genrich, 1986).

Au RdP ordinaire, on associe une annotation $A =< Const, V, Ats, Ata, Ac >$ où $Const$ est un ensemble de constantes, V est un ensemble de variables formelles qui seront substituées par des constantes de $Const$ lors des franchissements des transitions.

$Ats : T \rightarrow Ls(Const, V)$ est une application associant à chaque transition des prédicats conditions utilisant à la fois des constantes et des variables formelles.

$Ata : T \rightarrow La(Const, V)$ est une application associant à chaque transition une action sous la forme d'une suite d'affectations de variables formelles à des valeurs.

Ac est une application associant à chaque arc une somme formelle de *n-uplets* correspondant au poids de l'arc.

$M0$ est le marquage initial des places. C'est une application qui associe à chaque place une somme formelle de *n-uplets* de constantes.

Cette classe sera utilisée pour la modélisation de la couche logique (*cf.* Section 3.6.3.3 page 123).

3.4.5 Fonctionnement d'un RdP

Le marquage des places d'un réseau de Petri représente l'état du système modélisé à un instant donné. Ce marquage peut être modifié au fur et à mesure de l'occurence de tirs de transitions. Pour pouvoir être tirée, une transition doit être validée (Bourdeaud'huy et Yim, 2004).

Pour un marquage M, une transition t est dite *tirable*, ou franchissable ou sensiblisée si et seulement si l'équation 3.4 est vérifiée.

$$\forall p_i \in \mathbb{P}, M(p_i) \geq Pr(p_i, t) \tag{3.4}$$

En d'autres termes, pour toutes les places p_i, entrées de t, le nombre de jetons dans p_i, $M(p_i)$, est supérieur ou égal au poids de l'arc allant de p_i à t.

Après avoir vu comment modéliser l'évolution du système grâce au tir des transitions, il reste à déterminer quand ces évolutions se produisent effectivement.

Pour un événement donné, cela revient à évaluer le délai qui s'écoule entre le moment où l'événement devient possible c'est-à-dire quand la transition devient valide, et l'instant où il se produit effectivement, c'est-à-dire la transition est tirée (*cf.* Figure 3.4).

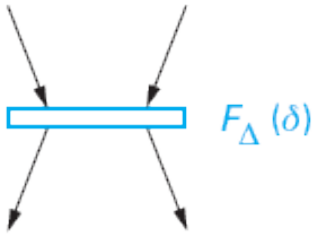

FIGURE 3.4: Loi du délai de tir d'une transition

Aucune hypothèse particulière n'est nécessaire sur la nature de ce délai qui peut être aussi bien déterministe que stochastique :

- un délai déterministe correspond à un événement qui se produit après un délai constant ;
- un délai stochastique correspond à un événement qui se produit après un délai aléatoire δ régi par la fonction de répartition $F_\Delta(\delta)$ attachée à l'événement en question.

3.5 Modélisation à base de composants

3.5.1 Décomposition du modèle en composants interconnectés

Dans notre approche, nous allons décomposer le système en un graphe de composants interconnectés par leurs interfaces. Nous allons donc exposer la décomposition proposée dans cette optique. Il s'agit de composants « *conceptuels* » (Andreu *et al.*, 2004).

3.5.1.1 Principe de décomposition

Deux composants fondamentaux s'imposent : la place et la transition. Leur interconnexion est traduite dans le modèle par les arcs orientés. Nous considérons ces arcs comme le support des flux d'entrées/sorties, *i.e.* flux de jetons, entre les composants ; ce support exprimant en

terme de propagation, *i.e.* de flux de jetons, tant de contraintes telles la pondération des arcs entrants d'une transition, que de conséquences telles la pondération des arcs sortants d'une transition.

Les flux de jetons résultants (entrants et sortants) sont alors issus des interconnexions de la place avec ses transitions aval et amont. Le « *pivot* » est la transition. Chaque transition amont (resp. aval) apporte (resp. retire) un flux de jetons ; l'ensemble des flux entrants (resp. sortants) d'une place est alors exprimé par un vecteur d'entrée (resp. de sortie) dont la dimension correspond au nombre de transitions amont (resp. aval) de la place. Chaque transition apportant potentiellement un nombre différent de jetons, directement spécifié par le poids de l'arc correspondant, il est nécessaire d'associer un poids à chaque flux (Andreu *et al.*, 2004).

Le type d'arc est également important puisqu'il influe sur la propagation du flux ; un arc inhibiteur et un arc de test ne spécifient pas les mêmes contraintes et reposent sur des règles de propagation différentes.

3.5.1.2 La transition

Le composant transition est structuré autour d'un port d'entrée, d'une zone interne et d'un port de sortie.

Port d'entrée Un port d'entrée est constitué de cinq vecteurs et un intervalle de temps.

- un vecteur Me de dimension n, où n est le nombre d'arcs entrants. Ce vecteur supporte donc la connexion avec les places amont. Chaque élément du vecteur $Me(i)$ désigne la source du jeton (flux entrant) de l'arc considéré, *i.e.* il apporte directement le marquage de la place amont désignée.
- un vecteur Ap de dimension n, où n est le nombre d'arcs entrants. Ce vecteur exprime les contraintes sur les flux entrants. Chaque élément du vecteur $Ap(i)$ exprime le poids

associé à l'arc entrant désigné, *i.e.* il exprime directement la contrainte sur le marquage de la place amont désignée par $Me(i)$.

- un vecteur At de dimension n, où n est le nombre d'arcs entrants. Ce vecteur exprime le type des arcs entrants. Chaque élément du vecteur $At(i)$ exprime le type associé à l'arc entrant désigné, *i.e.* il permet d'exprimer la règle de propagation sur cet arc.
- un vecteur As de dimension m, où m est le nombre d'arcs sortants. Ce vecteur supporte donc la connexion avec les places aval. Chaque élément du vecteur $As(i)$ exprime directement le poids de l'arc sortant désigné, duquel sera déduit le nombre de jetons à déposer dans la place cible.
- un vecteur Ct de dimension k, où k est le nombre de termes de la condition associée à la transition. En effet, la condition peut être décrite comme un produit de termes.
- un intervalle de temps I, décrit par deux bornes T_{min} et T_{max}.

Zone interne Elle comprend un compteur de temps. Etant relatif, il s'agit du temps écoulé depuis la sensibilisation de la transition.

Port de sortie Un port de sortie est constitué de deux vecteurs.

- Un premier vecteur AJs (AjoutJetons) de dimension m, où m est le nombre d'arcs sortants. Ce vecteur supporte donc la connexion avec les places aval, en termes de jeton à ajouter à ces places. Chaque élément du vecteur $AJs(i)$ transporte le flux de jeton sortant correspondant à l'arc désigné, *i.e.* il exprime directement le nombre de jetons à déposer dans la place cible désignée.
- Un second vecteur RJs (RetraitJetons) de dimension n, où n est le nombre d'arcs entrants. Ce vecteur supporte donc la connexion avec les places amont, en termes de jetons à retirer de ces places. Chaque élément du vecteur $RJs(i)$ transporte le flux de jeton entrant correspondant à l'arc désigné, *i.e.* il exprime directement le nombre de jetons à retirer de la place source désignée.

Le composant transition supporte aussi les règles d'évolution du modèle au sens de l'évaluation et du tir de cette transition.

3.5.1.3 La place

La place est également traduite en un composant sur lequel s'exerce la propagation de jetons induite par le tir des transitions auxquelles il est connecté. La propagation de flux résulte par un flux de jetons à ajouter et/ou à retirer (Andreu *et al.*, 2004).

Autant que le composant transition, le composant place est structuré autour d'un port d'entrée, d'une zone interne et d'un port de sortie.

Port d'entrée

- le flux entrant de jetons, en terme de jetons à ajouter. Il est décrit par un vecteur AJe (AjoutJetons) de dimension n, où n est le nombre d'arcs entrants. Ce vecteur supporte donc la connexion avec les transitions amont. Chaque élément du vecteur $AJe(i)$ apporte le flux de jeton entrant correspondant à l'arc désigné, *i.e.* il apporte directement les jetons issus du tir de la transition amont désignée par l'arc.
- le flux sortant de jetons, en terme de jetons à retirer. Il est décrit par un vecteur RJe (RetraitJetons) de dimension k, avec k étant le nombre d'arcs sortants. Ce vecteur supporte donc la *retro-connexion* avec les transitions aval. Chaque élément du vecteur $RJe(i)$ retire le flux de jeton sortant correspondant à l'arc désigné, *i.e.* il retire directement les jetons issus du tir de la transition aval désignée par l'arc.

Zone interne La zone interne comprend l'état, décrit en terme de jetons présents dans la place.

Port de sortie A travers le port de sortie, le composant place extériorise son état courant, *i.e.* port qui supporte donc la *connexion-avant* avec les transitions aval (Andreu *et al.*, 2004). Cela est décrit par un entier Ms, image du marquage, de dimension 1 car indépendant du nombre d'arcs sortants.

Revenons sur le partitionnement des règles d'évolution du modèle, entre le composant place et le composant transition.

3.5.1.4 Partitionnement des règles d'évolution du modèle

Telles que nous venons de les décrire, les règles d'évolution sont réparties entre les deux types de composants afin de respecter l'approche composant, *i.e.* que chacun assure l'évolution de son propre état. Ce partitionnement attribue au composant transition non seulement la responsabilité de l'évaluation de la *franchissabilité* et du tir des transitions mais aussi la responsabilité de l'évolution de l'état du graphe de marquage.

(Kusiak, 2002) s'est intéressé à la conception modulaire et a défini trois types de modularités :

- échanges de composants : c'est le cas où deux modules alternatifs de base ou plus peuvent être assemblés avec le même module en créant différentes variantes de produits appartenant à la même famille de produits,
- partage de composants : c'est le cas complémentaire du précédent, avec différents modules assemblés au même composant de base en créant différentes variantes de produits appartenant à différentes familles de produits,
- « bus modularity » : elle est utilisée quand un module, ayant au moins deux interfaces, peut être partagé avec n'importe quel composant d'un ensemble de composants de base.

L'interface du module accepte toute combinaison de composants de base. Kusiak soutient également que la modularité dépend de deux caractéristiques de conception de composants, à savoir : la similitude entre architecture physique et fonctionnelle et la minimisation des interactions entre les composants physiques.

Dans le cadre de notre étude, nous distinguons trois modules :

- un module *structurel* qui modélise les moyens (ressources ou acteurs) du système principal ; ce module est orienté matériel et donne une approche par composants du modèle ;
- un module *fonctionnel* qui modélise les activités du système principal et ses interactions avec l'environnement extérieur ; ce module donne le caractère dynamique du modèle ;
- un module *logique* qui gère les contraintes de sécurité.

Selon (Tiennot *et al.*, 2008), en plus de fournir un bon niveau de fiabilité au modèle lui-même, l'approche modulaire accélère la modélisation en général.

3.5.2 Règles de modélisation

3.5.2.1 Modules

Un module est constitué d'un ensemble de places et de transitions instantanées ou temporisées. Les transitions représentent les évènements qui conduisent à l'évolution de l'état du composant. Quand l'occurrence d'un événement conduit à l'évolution simultanée de l'état de plusieurs composants, elle peut être représentée par une transition commune aux modules associés à ces composants. La seule condition imposée à chaque module est qu'il doit avoir son invariant de marquage égal à 1. Cette condition facilite la description des interactions entre les modules et permet une formalisation de ces interactions, basée sur la logique booléenne.

Une telle condition, bien qu'elle exclut à première vue l'exploitation des symétries dans le modèle, n'est pas très contraignante dans la mesure où de telles symétries sont rares dans des modèles de sûreté de fonctionnement décrivant de façon fine le comportement des systèmes (Kaaniche, 1999).

Modules fonctionnels L'aspect fonctionnel assure la dynamique des éléments physiques du système. Il représente et coordonne les activités du processus.

Les blocs fonctionnels (*cf.* Figure 3.5) sont représentés par des rectangles avec les coins arrondis : ils décrivent le comportement du système sous la forme de fonctions associées au système étudié.

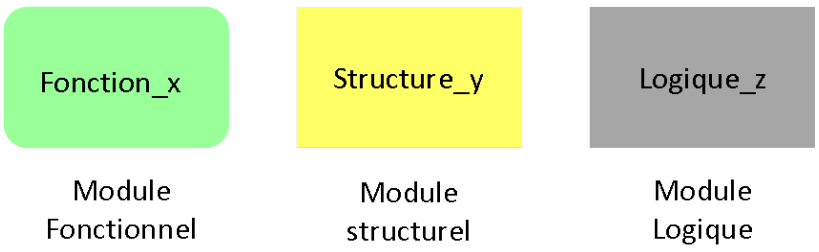

FIGURE 3.5: Les éléments de base du formalisme proposé

Les blocs fonctionnels ne possèdent pas de propriétés hiérarchiques. Ils sont liés à des

sous-blocs, donc d'un niveau inférieur. Nous distinguons les blocs parents de niveau 0 des blocs de niveau N-1, N-2 ...

La représentation fonctionnelle hiérarchique est le résultat de l'application de l'approche *Top-Down*. Les fonctions et leurs interconnexions sont représentées à différents niveaux de complexité. Ces niveaux peuvent être caractérisés par le concepteur pour avoir une idée du fonctionnement global du système.

Par ailleurs, la représentation fonctionnelle a l'intérêt de pouvoir présenter toutes les fonctions élémentaires et de servir de base pour une première visualisation architecturale. Nous pouvons considérer que cette représentation purement relationnelle facilitera les échanges entre les membres des équipes de conception et servira aux instances d'appui les moins techniques pour une meilleure compréhension du système, sans rentrer dans les détails.

La Figure 3.6 montre une représentation fonctionnelle hiérarchique. Les niveaux 0, -1, -2, *etc.*, sont ceux de la décomposition hiérarchique du fonctionnement du système.

Modules structurels La représentation structurelle répond aux insuffisances de la représentation précédente. On fait évoluer la représentation fonctionnelle du système vers une hypothèse d'architecture opérationnelle grâce à l'agrégation et au regroupement des blocs élémentaires en blocs plus complexes que l'on va pouvoir :

- proposer selon une organisation de fonctions, dans la perspective de définir des composants plus conformes aux pratiques industrielles ;
- définir et spécifier en précisant toutes les entrées/sorties ;
- spécifier comme une fourniture multi-fonctionnelle.

Cette représentation architecturale, par sa cohérence technique et opérationnelle, doit permettre de formuler des hypothèses sur l'implémentation du système et sur les éventuelles actions ou activités nécessaires pour la réaliser.

Les blocs structurels (*cf.* Figure 3.5) sont représentés par des rectangles. Ils permettent la décomposition structurelle et hiérarchique du système. Ils admettent tous types de canaux d'entrée/sortie.

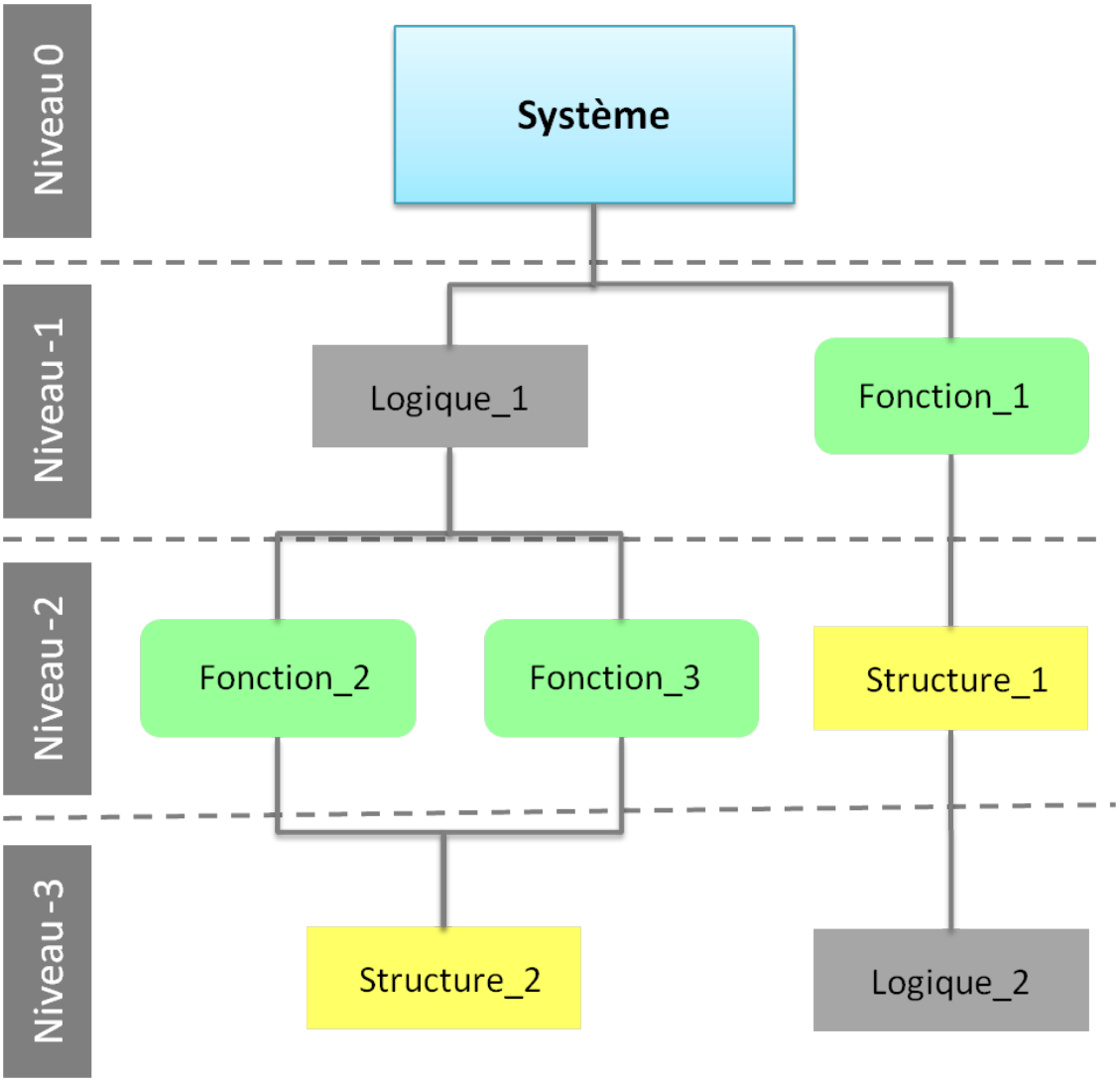

FIGURE 3.6: Décomposition fonctionnelle représentée sous la forme d'un arbre du système

Les blocs structurels peuvent contenir d'autres blocs structurels, des blocs fonctionnels. L'utilisation de blocs structurels est bien caractérisée à deux niveaux différents du processus de conception :

- Au stade de la décomposition fonctionnelle où ils permettent d'établir des dépendances hiérarchiques et de décliner chaque fonction en plusieurs sous-ensembles,
- Au stade de « l'architecture » des fonctions où ils permettent de regrouper et d'agréger d'autres blocs afin de composer éventuellement des *composants du système*.

Modules logiques Représentés par des rectangles gris, les modules logiques peuvent être raccordés à toutes sortes de modules : fonctionnels, structurels et/ou logiques.

Ils assurent la sécurité du système à tous les niveaux (*cf.* Figure 3.6).

La superposition de la décomposition fonctionnelle à plusieurs niveaux à l'arbre de système composé par les modules élémentaires génère une nouvelle vision modulaire du système présentée en Figure 3.7.

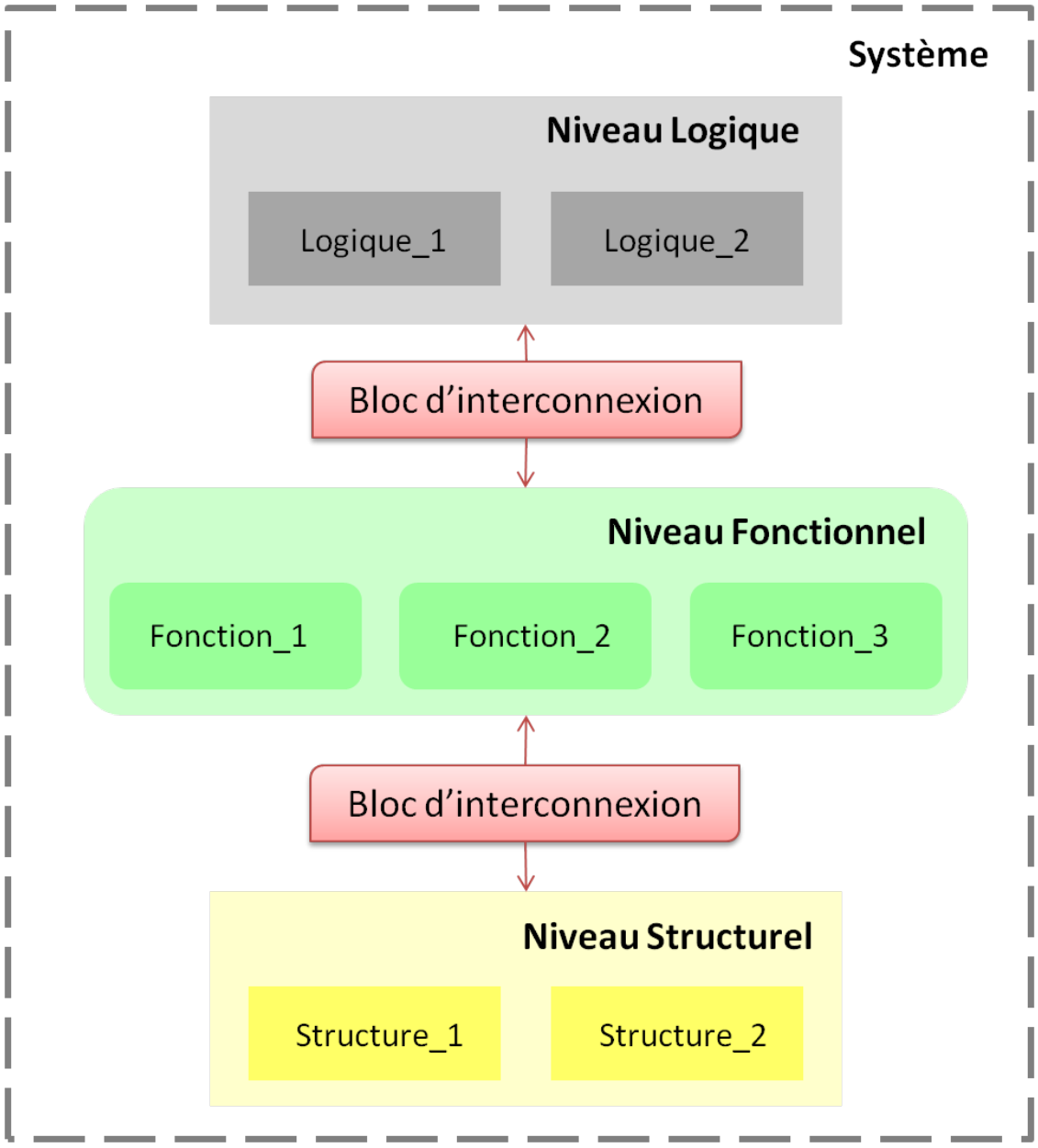

FIGURE 3.7: Décomposition hiérarchique du système

3.5.2.2 Règles de modélisation

Les règles de modélisation permettent de combiner les modules entre eux en garantissant leur compatibilité.

Notre approche est basée sur des modules autonomes et asynchrones - les modules étant indépendants. Autrement dit, les transitions internes ne doivent pas être contrôlées par des ressources appartenant à d'autres modules. Ainsi, chaque module est défini par une ou plusieurs places d'entrée. D'autre part, les sorties d'un module sont représentées par des transitions qui envoient les jetons aux autres modules d'une façon asynchrone.

Par ailleurs, afin d'assurer la généricité de notre approche, les nœuds du RdP, situés à l'extérieur des modules, ne doivent appartenir à aucune classe particulière de RdP.

La Figure 3.8 illustre un module élémentaire respectant les règles de modélisation. Les transitions externes appartiennent aux RdP Places/Transitions.

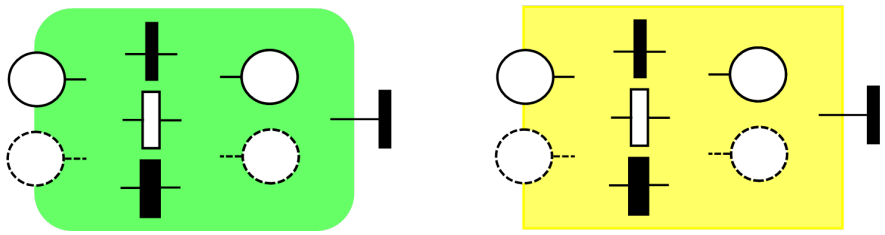

FIGURE 3.8: Modules élémentaires

Couplage des modules Les trois couches identifiées pour le système sont en constante interaction.

Des mécanismes élémentaires sont utilisés pour le couplage des modules :

1. les places pouvant contenir des jetons,
2. les flux de jetons entre places transitant par des transitions,
3. les marquages au niveau des places,
4. les tests de marquages, qui sont utilisés quand l'occurrence d'un évènement dans un composant est conditionnée par l'état d'autres composants,

5. les transitions communes, qui modélisent des évènements communs à plusieurs modules,
6. les variables utilisées notamment par l'envoi ou la réception de messages pour valider le tirage des transitions,
7. les blocs d'interconnexion.

Les blocs d'interconnexion modélisent les conséquences d'un évènement se produisant dans un composant source sur l'état d'autres composants. Ces conséquences peuvent être conditionnées par l'état d'autres composants du système. Les tests de marquage sont alors utilisés pour traduire ces conditions. Un bloc relie un ou plusieurs modules sources à un ou plusieurs modules de sortie. Il est constitué d'une place d'entrée et d'un ensemble de transitions instantanées.

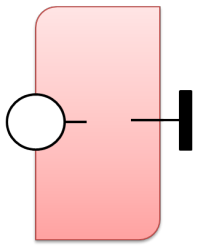

FIGURE 3.9: Bloc d'interconnexion modulaire

Des blocs d'interconnexion génériques peuvent être définis pour modéliser certains types d'interaction. Par exemple, l'arrêt des répliques logicielles quand le calculateur défaille, la relance automatique du logiciel suite à une détection d'erreur, *etc.*

Dans le cas d'une interaction complexe, il est souvent plus utile et efficace de modéliser cette interaction par plusieurs blocs élémentaires disposés en série (*cf.* Figure 3.10) ou en parallèle (*cf.* Figure 3.11) au lieu d'utiliser un bloc unique. Quelques précautions sont nécessaires pour éviter de faire des erreurs lors de la définition et de l'enchaînement de ces blocs. En particulier, des conflits entre les transitions instantanées des différents blocs peuvent apparaître et des priorités de franchissement doivent être définies pour gérer ces conflits. Un ensemble de règles de construction pour guider la décomposition doit être mis en place.

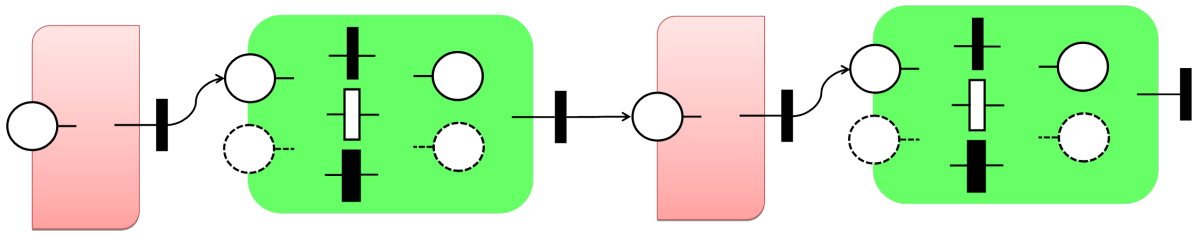

FIGURE 3.10: Disposition des modules en série

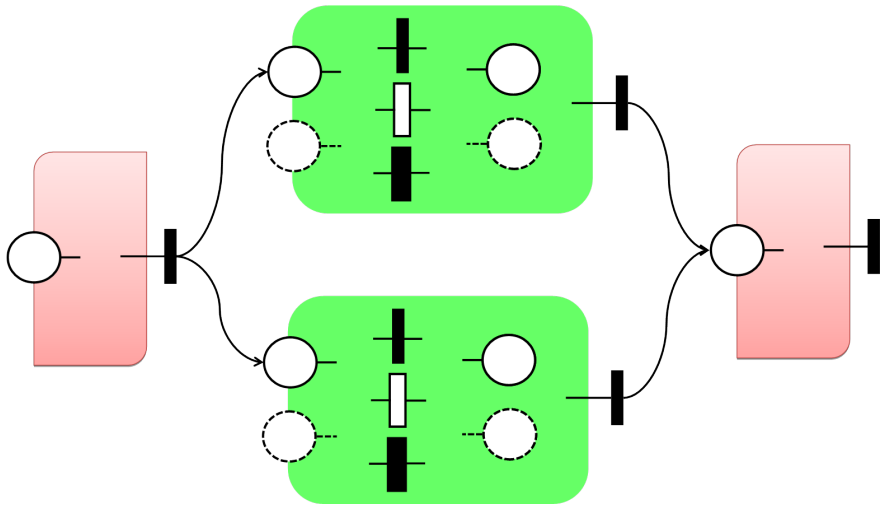

FIGURE 3.11: Disposition des modules en parallèle

3.5.3 Comportement du modèle

3.5.3.1 Spécification de la dynamique

Certaines spécifications de la dynamique du système étudié sont à considérer. Elles peuvent affecter deux aspects :

- les instants de tir : cette caractérisation peut être :
  - déterministe : la durée de sensibilisation est fixe lorsqu'on connaît d'une manière exacte l'instant de tir de la transition comme par exemple pour les transitions immédiates où le franchissement doit se faire dès la sensibilisation de la transition.

- stochastique : la distribution est probabiliste lorsque la durée de sensibilisation obéit à une fonction aléatoire.
- les probabilités de franchissement : cette caractérisation intervient lorsque plusieurs alternatives sont présentes. En effet, quand plusieurs transitions sont en conflit et quand la proportion de franchissement de chacune de ces transitions est connue *a priori*, on peut associer des probabilités à chacune de ces transitions de manière à guider le choix entre les branches concurrentes.

3.5.3.2 Modélisation de la dynamique

Nous allons procéder par modélisation pour l'étude de la répartition et l'évaluation du risque. En termes d'outillage, plusieurs outils existent mais diffèrent de par le type de modèles supportés et les techniques de simulation utilisées.

Plateforme logicielle : TimeNet TimeNet a été développé à l'Université Technique de Berlin suite à la collaboration de plusieurs projets de recherche. Il a l'avantage de fournir une interface utilisateur graphique pour la spécification du modèle et l'analyse spécialisée ; les composants de simulation sont utilisés pour l'évaluation automatisée du modèle. La mise en œuvre de l'analyse et les composants de simulation est basée sur des résultats de recherche récents.

TimeNet est un progiciel pour la modélisation et l'évaluation de réseaux de Petri stochastiques dans lequel les délais de tir des transitions peuvent être exponentiellement distribués, déterminés. Les modèles peuvent être spécifiés avec une interface utilisateur graphique. Quant aux mesures des résultats, elles peuvent être définies au niveau modèle dans une syntaxe d'un but particulier. Les modèles continus ainsi que ceux discrets sont soutenus.

Nous avons défini une méthode de construction modulaire qui permet, d'une manière systématique, la construction et la validation progressive du modèle de sûreté de fonctionnement d'un système, par différentes classes de réseaux de Petri. Cette méthode est basée

sur une idée originale : l'approche modulaire de construction, qui consiste à aboutir à une forme optimale du modèle par RdP et à faciliter sa validation progressive.

3.6 Etude de cas : Système Mini Métro

Le système que nous allons adopter comme exemple illustratif pour notre méthodologie d'évaluation du risque ferroviaire est la ligne 1 du système de transport *mini-métro* de l'aéroport de Roissy Charles de Gaulle.

3.6.1 Présentation du système

L'introduction de l'électronique a vraiment commencé avec le premier métro entièrement automatique sans conducteur, que l'on nomme VAL pour Véhicule Automatique Léger [4].

3.6.1.1 Niveau de sécurité

Après des études supervisées par les experts du domaine, les conclusions quant au niveau de sécurité prévisionnel sont les suivantes :

- En intégrant la spécificité du système de transport MINI METRO dont l'évènement redouté est « *mort d'homme suite à dysfonctionnement dangereux et non détecté des automatismes de sécurité ET présence d'une situation dangereuse* ».
- En prenant comme hypothèse que les probabilités d'occurrence des situations dangereuses sont comprises entre les valeurs $3 * 10^{-5}/h$ et $1,3 * 10^{-3}/h$.

Le niveau de sécurité prévisionnel de la ligne 1 du système MINI METRO de l'aéroport Roissy Charles de Gaulle, est compris entre $1,34 * 10^{-11}/h$ et $3,5 * 10^{-8}/h$. Du fait que l'ensemble de ces fonctions de sécurité sont réalisées à partir des mêmes ressources matérielles

4. Le premier VAL a été inauguré à Lille en 1983. Il équipe aujourd'hui les villes de Taipei, Toulouse, Rennes et depuis Janvier 2006, Turin. Concernant le déploiement du VAL, il y a au moins 119 km de lignes déployées dans le monde et plus de 830 voitures sont en exploitation ou en construction.

(automates programmables de sécurité), le chiffre le plus pénalisant est retenu, soit $3,5 * 10^{-8}/h$. Ces valeurs sont associées aux fonctions et évènements redoutés (*Collision d'un véhicule sur un voyageur* et *Collision véhicule*).

Le niveau de sécurité le plus faible $3,5 * 10^{-8}/h$ est celui de la fonction *Contrôle-Commande*. Ceci s'explique par le fait qu'il s'agit de la seule fonction de sécurité, gérée par automate programmable, pour laquelle les freins interviennent dans la mise en état de sécurité. Pour cette fonction, le non lâché des freins est considéré comme un évènement redouté.

Ces valeurs de niveaux de sécurité prévisionnels, basés sur les critères des experts, ont été calculés en retenant :

- une probabilité de défaillance horaire pour les probabilités d'occurence des situations dangereuses,
- une probabilité de défaillance calculée avec les durées représentatives des opérations de détection des défaillances qui conduisent à la réalisation de l'évènement « dysfonctionnement dangereux du système de sécurité ». Ces durées sont comprises entre une heure et une semaine (ces défaillances ont été désignées sous le terme « défaillances dangereuses non détectées »).

Les valeurs des niveaux de sécurité calculés pour les automates programmables sont compris entre les valeurs de $1 * 10^{-7}$ et $2,3 * 10^{-6}$ selon les fonctions de sécurité étudiées. Ce niveau de sécurité, dans le cas de la fonction cantonnement (F1), est supporté à plus de 85% par les modules de sortie. La raison de cette contribution aussi importante est dûe au fait que les dysfonctionnements dangereux pour la sécurité des modules d'entrée et des modules CPU sont détectés par le fonctionnement dynamique du système (de l'ordre de 30 secondes). Dans le cas des modules de sortie et des éléments qui leur sont associés, ces dysfonctionnements dangereux pour la sécurité, ne peuvent être détectés que par le test journalier et manuel des sorties.

En intégrant une architecture qui permettrait de tester de façon indépendante et dynamique ces sorties, et en reprenant les mêmes hypothèses de réaction suite à dysfonctionnement détecté, le niveau de sécurité de cette fonction évoluerait comme illustré par le Tableau 3.2.

	Test journalier	**Test horaire**	**Test toutes les 20min**
Niveau de sécurité de la fonction cantonnment	$PFD_{AVG} = 3,6 * 10^{-7}$	$PFD_{AVG} = 3,5 * 10^{-10}$	$PFD_{AVG} = 8,5 * 10^{-11}$

Tableau 3.2: Evolution du niveau de sécurité

Cette affirmation est faite sous réserve que le test indépendant et dynamique des modules de sortie ait un taux de couverture des défaillances de 100%. De plus, cette affirmation n'intègre pas les erreurs systématiques, les dysfonctionnements de mode commun et les erreurs logicielles.

3.6.2 Fonction Cantonnement

La fonction cantonnement a pour objectif d'éviter le tamponnement des véhicules. Dans cette optique, l'ensemble de la voie est découpé en tronçons. Ces tronçons sont dénommés *cantons* sur les zones d'accélération et les zones principales (CP) où la vitesse est constante ; et *zones* sur les zones de décélération (DC). Le terme cantonnement s'applique dans cet exemple indifféremment aux cantons et aux zones.

Le tamponnement de véhicules suppose une collision avec une vitesse supérieure à $1m/s$. Lorsque les vitesses des véhicules sont inférieures à $1m/s$ (véhicule en station $-0,3m/s$), le cantonnement est géré par les automates fonctionnels. Dans le cas contraire, le cantonnement est géré par les automates de sécurité.

Les fonctions de cantonnement sont :

- détection d'occupation de canton,
- logique de cantonnement,
- commande sécuritaire des sorties.

3.6.2.1 Fonction « Détection d'occupation de canton »

Faute de pouvoir utiliser une détection continue de présence des véhicules, on emploie un bloc à reddition, où la libération d'un canton est assurée par l'engagement du canton en aval. Ce principe permet de détecter un éventuel rapprochement des véhicules entre eux.

Le MINI METRO est équipé d'un dispositif de cantonnement géré par l'automate de sécurité, qui détecte les dysfonctionnements de l'entraînement des véhicules. Ce dernier se traduit par des rattrapages ou rétrogrades.

Le respect du cantonnement est assuré par deux chaînes indépendantes (redondance sécuritaire active) gérant chacune l'activation des cantons et la détection des passages des véhicules.

Ainsi, l'activation et la désactivation des différents cantons est faite sur le front descendant des capteurs associés aux cantons. Les signaux sont analysés en *cohérence* - information capteur i chaîne 1 et chaîne 2 identiques - et en *sécurité* - occupation canton autorisée - . Les capteurs sont répartis le long de la voie comme suit :

- tous les 92 mètres en moyenne sur les CP,
- tous les 8 mètres en moyenne sur les DC.

Les séquences d'activation et de désactivation des capteurs sont réalisées à chaque passage de véhicule, soit à des intervalles de temps espacés de 18 secondes minimum à 36 secondes maximum en moyenne. Ces intervalles correspondent respectivement au trafic maximum et au trafic minimum.

3.6.2.2 Fonction « Logique de cantonnement »

La logique de cantonnement interdit en général l'occupation simultanée de deux cantons successifs : c'est le principe de cantonnement fixe. Les équations logiques d'action peuvent différer suivant les modes de marche du système (vitesse du vent supérieure à 20m/s ou inférieure à 20m/s) dont la sélection est effectuée par l'opérateur.

La logique de cantonnement gère trois types de situations en fonction des différents cas se présentant en entrée de chaque chaîne. L'occupation d'un canton est repérée par le chiffre 1 et la non-occupation par le chiffre 0.

Ces trois types de situations sont représentées par la Figure 3.12, Figure 3.13 et Figure 3.14.

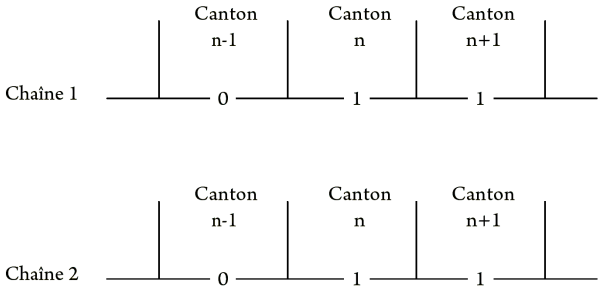

FIGURE 3.12: Défaut réel de cantonnement

Les deux cantons n et $n+1$ sont occupés simultanément.

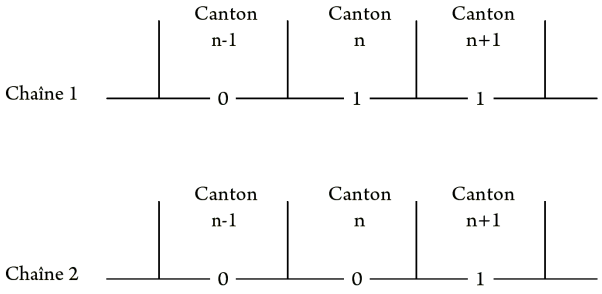

FIGURE 3.13: Présomption de défaut de cantonnement

Dans ce cas, la chaîne 1 conclut à l'occupation d'un canton alors que la chaîne 2 conclut

à la non-occupation du canton. Il y a alors présomption de panne sur une chaîne.

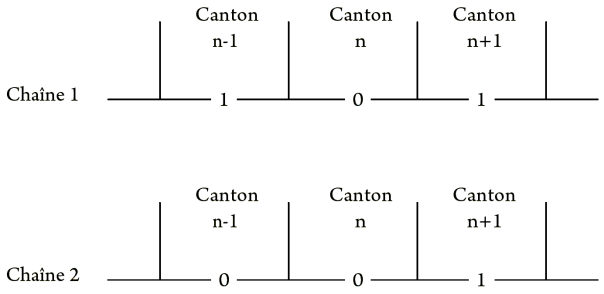

FIGURE 3.14: Défaut de cohérence

Les différent états d'occupation de cantons sont échangés et comparés à chaque cycle, le défaut de discordance n'est activé qu'après constation de la persistance de la discordance au-delà de 1,5 seconde.

3.6.2.3 Fonction « Commande sécuritaire des sorties »

En cas de défaut, quatre zones de mémoire du processeur sont modifiées (*cf.* Tableau 3.3) et les traitements associés provoquent des effets différents en fonction des différentes combinaisons de défauts.

La mémoire défaut de cantonnement est mise à 1 lorsque deux cantons successifs sont occupés.

La mémoire défaut de cohérence est mise à 1 lorsque les informations d'occupation dun canton issues de la chaîne 1 et de la chaîne 2 sont différentes. Elle provoque la réduction des seuils de vitesse à 1,5m/s.

Les défauts sont mémorisés. Les entraînements et les coins concernés resteront dans l'état sécuritaire tant que l'opérateur n'aura pas éliminé, ou provisoirement simulé, et inhibé le défaut.

	Cas 1	Cas 2	Cas 3
Chaîne 1 Chaîne 2	$0--1--1$ $0--1--1$	$0--1--1$ $0--0--1$	$1--0--1$ $0--0--1$
Zone mémoire de défauts – Défaut Cant 1 = 1 – Défaut Cant 2 = 1 – Défaut Cohérence = 0 – Défaut Moteur = 0	– Défaut Cant 1 = 1 – Défaut Cant 2 = 0 – Défaut Cohérence = 1 – Défaut Moteur = 1	– Défaut Cant 1 = 0 – Défaut Cant 2 = 0 – Défaut Cohérence = 0 – Défaut Moteur = 1	
Conséquence – Arrêt des moteurs – Lâché des freins – Levée des coins	– Arrêt des moteurs – Lâché des freins – Levée des coins – Réductions des seuils de survitesse	– Arrêt des moteurs par le fonctionnel – Réduction des seuils de survitesse	

Tableau 3.3: Zones de mémoire du processeur

3.6.3 Modularisation du mini métro

En se plaçant d'un point de vue « Train en N-1 qui veut passer à N », il s'agit dans cette section de représenter la règle : *Continuer si N est vide.*

Pour cela, nous décomposons le système en 3 niveaux :

- Niveau *Structurel.* Il illustre la structure du système ferroviaire : circulation des trains, rails, zones, câbles, vitesse, détection de collision. Ce niveau est représenté par des *RdP temporels.*
- Niveau *Fonctionnel.* Il modélise les incertitudes relatives aux composants physiques (détection des capteurs, efficacité des freins). Les taux de défaillances sont modélisés grâce à des *RdP Stochastiques.*
- Niveau *Logique.* Ce niveau dénote les règles logiques permettant de réagir face aux défaillances détectées dans un plus bas niveau, durant le fonctionnement du système. Ce niveau est basé sur des *RdP Prédicats/Transitions.*

3.6.3.1 Niveau Structurel

1. Module *Parcours*. Il schématise le parcours d'une zone N. Les RdP sont utilisés comme le montre la Figure 3.15. La transition intérieure correspond au temps de parcours de la zone. Les intervalles des transitions temporelles dépendent de la zone considérée (accélération, décélération, zone principale).

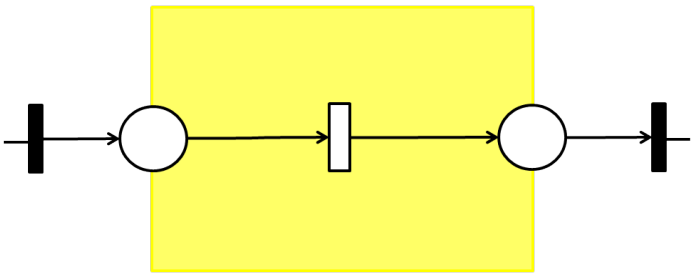

FIGURE 3.15: Module Parcours

2. Module *Passage*. Il illustre le passage du train d'une zone N-1 à une zone N. Ce passage peut être interdit par le niveau *Logique*, par le biais d'une place ressource qui modélise l'activation du frein de la zone en question.

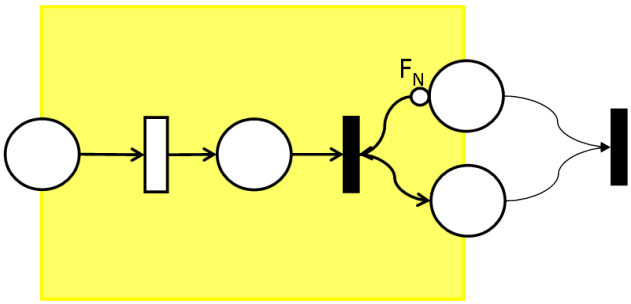

FIGURE 3.16: Module Passage de N-1 à N

3.6.3.2 Niveau Fonctionnel

1. Module *Capteur*. Ce module est probablement le plus important puisqu'il détecte le train à son entrée de zone et transmet l'information au niveau logique. Comme les capteurs peuvent détecter les défaillances, les transitions qui leur correspondent sont probabilistes.

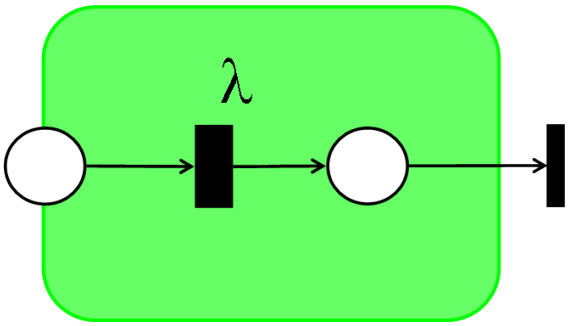

FIGURE 3.17: Module Capteur

2. Module *Frein*. Utilisé pour transmettre l'ordre d'activation du frein du niveau logique au niveau structurel. Dans la Figure reffig :modulefrein, la défaillance du composant frein n'est pas prise en compte mais une telle panne fait l'objet d'un affinement du module.

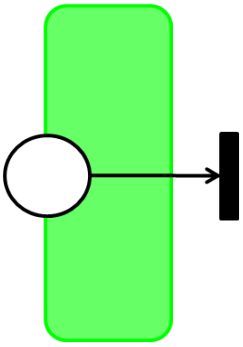

FIGURE 3.18: Module frein

3.6.3.3 Niveau Logique

Le contrôleur de sécurité est basé sur la détection des défaillances afin d'assurer la sécurité du système dans sa globalité. La logique de sécurité est vérifiée par le module de sécurité illustré par la Figure 3.19. Si un train est détecté à l'entrée de la zone N, le module vérifie si un train est déjà présent dans N. Si oui, le module frein est activé, sinon, la mémoire interne est à mise à jour.

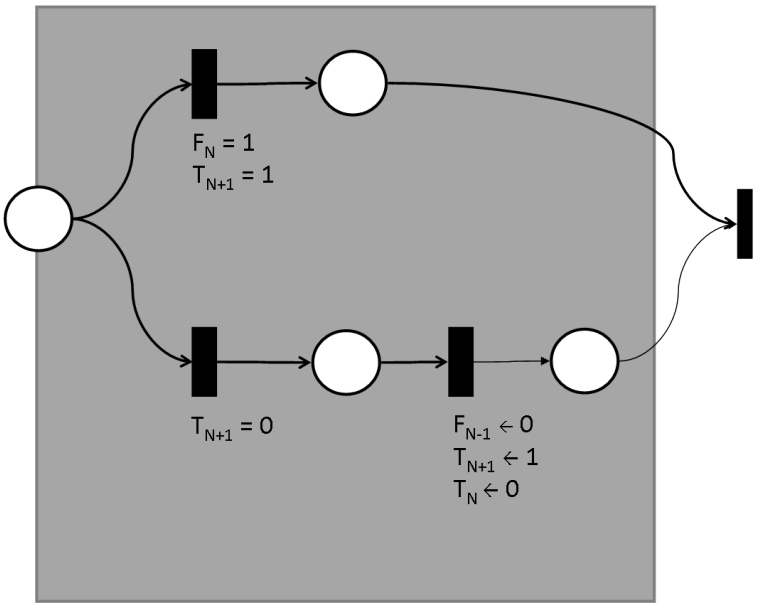

FIGURE 3.19: Module Sécurité

3.6.3.4 Modèle global du mini métro

Le modèle global illustré par la Figure 3.20 montre le parcours d'un train entre les zones N-1 et N+1. Les modules précédemment présentés ont été combinés selon les règles de modélisation présentées précédemment (*cf.* Section 3.5.2.2).

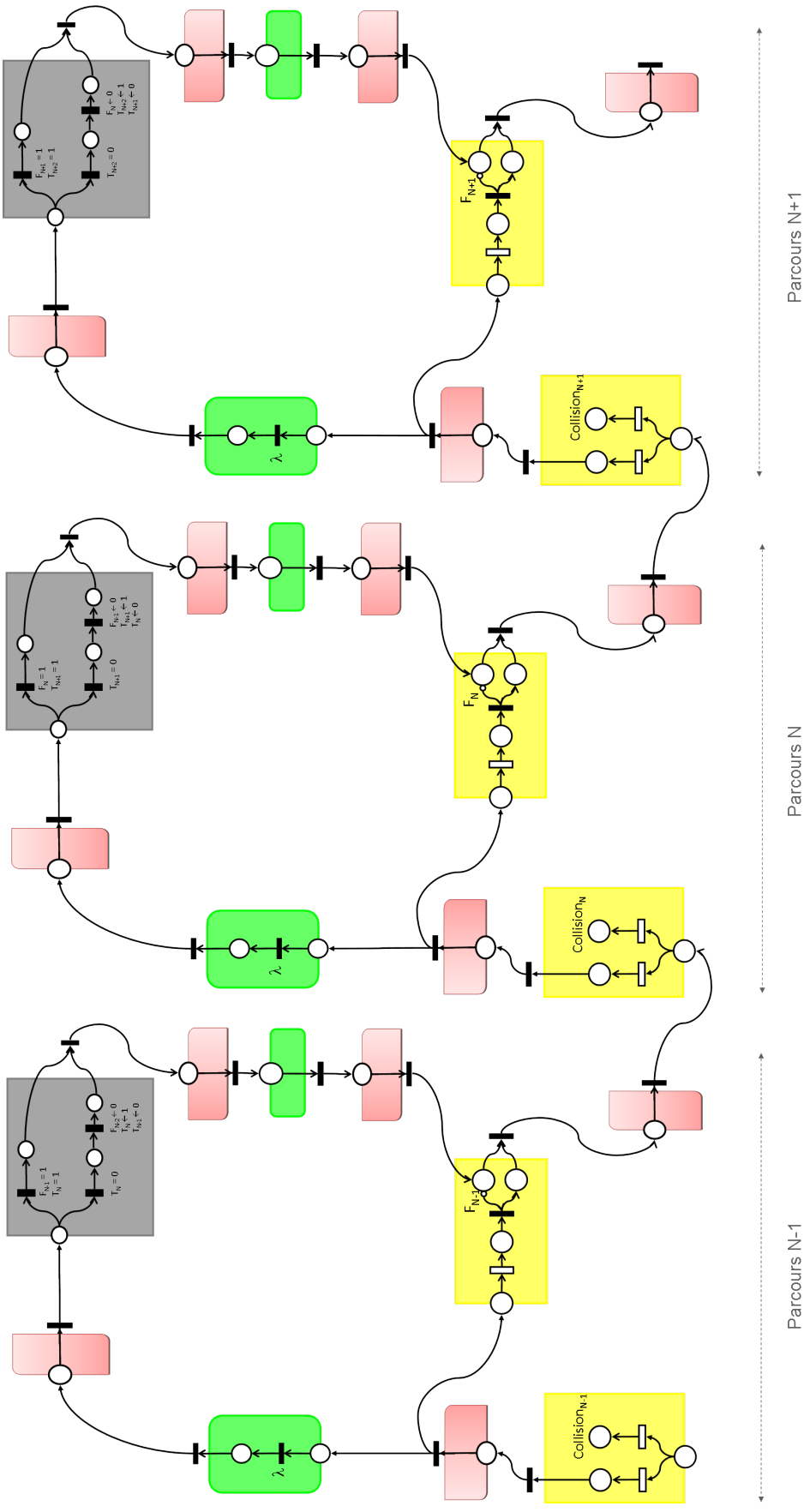

FIGURE 3.20: Parcours du mini métro entre les zones N-1 et N+1

Il convient de noter que le module *Parcours* a été affiné afin de modéliser la collision si la logique de cantonnement n'est pas respectée.

3.7 Conclusion

L'analyse de la décomposition ferroviaire fonctionnelle nous a permis l'identification de trois couches qui composent le système ferroviaire : structurelle, fonctionnelle et logique. Le raffinement modulaire de ce modèle en couches met en exergue sa capacité à faciliter la composition et l'abstraction. Ainsi, un outil unificateur en découle : les réseaux de Petri.

Bien que caractérisée par une sémantique de franchissement propre, chaque classe de réseau de Petri utilise un jeton permettant d'activer des blocs un peu à la manière dont on active les fonctions dans une décomposition fonctionnelle, mais avec des aspects immédiats et stochastiques (Rafrafi *et al.*, 2008a).

De là, découlent les choix d'affectation des classes de réseaux de Petri aux différents niveaux : des réseaux de Petri temporels pour le niveau structurel ; des réseaux de Petri stochastiques pour le niveau fonctionnel et des réseaux de Petri prédicats/transitions pour le niveau logique.

Nonobstant cette approche, nous pouvons envisager l'abstraction du modèle réseau de Petri en représentant chaque module par un coefficient, afin de regrouper les modules selon des critères divers dans une démarche d'allocation d'objectifs de sécurité.

Conclusion Générale et Perspectives

La sécurité a de longue date été la préoccupation majeure des opérateurs ferroviaires. Elle a été de la responsabilité de l'opérateur prenant en charge l'exploitation des trains et la gestion de l'infrastructure. Les acteurs ferroviaires étant de plus en plus nombreux, il est primordial de maîtriser les risques internes, mais aussi d'intégrer les risques partagés avec d'autres acteurs ayant des cultures différentes de la sécurité. Bien que le niveau de sécurité des transports ferroviaires en Europe soit de très haut niveau, le développement de ce nombre d'acteurs nécessite beaucoup d'efforts pour maintenir, voire améliorer, le niveau de sécurité des transports ferroviaires européens.

Pour appréhender notre problématique, nous avons organisé notre étude en trois temps.

D'abord, nous avons soulevé le contexte ferroviaire à travers les concepts d'interopérabilité et de sécurité ferroviaire, auxquelles aspire la Commission Européenne. En effet, de la directive 91/40/CE à la directive 2010/409/UE, en passant par la directive clé 2004/49/CE, toutes ont été mises en place afin de participer à une démarche d'harmonisation du secteur ferroviaire dans un contexte d'interopérabilité. La norme 61508 et ses applications ferroviaires soit la EN 50126, EN 50128 et EN50129 sont les normes clés du contexte industriel. Cependant, malgré la variété des textes, le seul niveau pouvant être utilisé pour l'évaluation de la sécurité et du risque demeure global.

Risque Vs Sécurité ? Il était primordial de distinguer la notion de *sécurité* ou l'*absence de risque inacceptable* de la notion de *risque*, qui est associé à la *probabilité d'occurence d'un*

danger et la *gravité des conséquences qui découlent de ce dernier*. Ainsi, le risque serait un paramètre clé dans la détermination du niveau de sécurité.

Dans le deuxième chapitre, nous nous sommes intéressés aux méthodes qualitatives et quantitatives d'évaluation des *risques*, point de départ de notre démarche. Il s'est avéré que, les méthodes existantes, dans un souci de complétude de la méthodologie proposée, ne sont pas compatibles entre elles.

La Commission Européenne, souhaitant harmoniser le système ferroviaire, ne peut entreprendre cette démarche qu'à un niveau de description qui le permet, c'est-à-dire le niveau fonctionnel ; ce qui rend caduques les approches d'évaluation des risques.

Ainsi, afin de répondre à la problématique d'évaluation de la sécurité des systèmes ferroviaires, nous avons proposé, dans le troisième chapitre, une méthodologie pour l'évaluation des risques basée sur les réseaux de Petri.

Une première contribution de cette approche est de considérer la décomposition ferroviaire fonctionnelle comme la phase amont de notre méthodologie. Ce qui nous a permis l'identification de trois couches qui composent le système ferroviaire : structurelle, fonctionnelle et logique. Le raffinement modulaire de ce modèle a appuyé sa capacité à faciliter la composition et l'abstraction. Ces deux propriétés qualifient les réseaux de Petri.

Bien que caractérisée par une sémantique de franchissement propre, chaque classe de réseau de Petri utilise un jeton permettant d'activer des blocs un peu à la manière dont on active les fonctions dans une décomposition fonctionnelle, mais avec des aspects immédiats et stochastiques.

De là, découlent les choix d'affectation des classes de réseaux de Petri aux différents niveaux : des réseaux de Petri temporels pour le niveau structurel ; des réseaux de Petri stochastiques pour le niveau Fonctionnel et des réseaux de Petri prédicats/transitions pour le niveau logique.

Enfin, à notre connaissance, l'approche proposée n'avait pas été jusqu'alors explorée

car jugée trop coûteuse. Notre travail montre que l'utilisation de techniques avancées de modélisation et d'analyse permet de dépasser cette limite. Nous allons poursuivre l'expérience à plus grande échelle pour pouvoir évaluer plus systématiquement les coûts et bénéfices de l'approche.

Cette perspective rejoint l'approche IMRI (*Initial Mishap Risk Index*) déjà proposée, dans des travaux antérieurs (Rafrafi et El-Koursi, 2007; Rafrafi *et al.*, 2008b). Cette approche consiste à déceler les fonctions de base, de plus bas niveau qui serviront pour définir la cohérence et la fiabilité de la décomposition fonctionnelle. La seconde étape consiste à attribuer un IMRI à chaque fonction. Dans le système ferroviaire, les IMRI attribués aux différentes fonctions ne seront pas forcément les mêmes puisqu'ils vont dépendre de la criticité de la fonction.

En guise de perspectives, l'objectif est de calquer l'approche IMRI sur l'approche modulaire afin de n'en faire qu'une méthodologie pour l'évaluation des risques et l'allocation des objectifs de sécurité.

Certes, cette thèse ne permet pas la généralisation des résultats atteints pour tous les systèmes ferroviaires, de différentes tailles ou de différentes origines ; mais elle participe au débat récent et émergent sur l'harmonisation des systèmes ferroviaires à l'échelle Européenne.

Cette thèse a montré que ce débat n'est qu'à ses premières ébauches et que le défi n'est pas complètement relevé. Beaucoup de travail reste devant nous, tant sur le point empirique que sur le point théorique, avant d'aboutir à une véritable conceptualisation de l'harmonisation en matière d'interopérabilité et de sécurité ferroviaire.

Annexe A

Glossaire Technique

A

Acceptation du risque (CEI, 2002) Décision d'accepter un risque. Le verbe « accepter » a été choisi pour exprimer l'idée selon laquelle l'acceptation est prise dans le sens fondamental que donne le dictionnaire. L'acceptation du risque dépend des critères de risque.

Accident (dir, 2004a) Événement indésirable ou non intentionnel et imprévu, ou un enchaînement particulier d'événements de cette nature, ayant des conséquences préjudiciables ; les accidents sont ventilés suivant les types ci-après : collisions, déraillements, accidents aux passages à niveau, accidents de personnes causés par le matériel roulant en marche, incendies et autres.

Accident grave (dir, 2004a) Toute collision de train ou tout déraillement de train faisant au moins un mort ou au moins cinq personnes grièvement blessées ou d'importants dommages au matériel roulant, à l'infrastructure ou à l'environnement, et tout autre accident similaire ayant des conséquences évidentes sur la réglementation ou la gestion de la sécurité ferroviaire. On entend par « importants dommages » des dommages qui peuvent être immédiatement estimés par un organisme d'enquête à un total d'au moins 2 millions d'euros.

Accident majeur (dir, 1997) Un événement tel qu'une émission, un incendie ou une explosion d'importance majeure résultant de développements incontrôlés survenus au cours de l'exploitation d'un établissement, entraînant pour la santé humaine, à l'intérieur ou à l'extérieur de l'établissement, et/ou pour l'environnement un danger grave, immédiat ou différé, et faisant intervenir une ou plusieurs substances dangereuses.

Agence (dir, 2004a) Agence ferroviaire européenne, c'est-à-dire l'agence communautaire pour la sécurité ferroviaire et l'interopérabilité.

Analyse des risques (CEI, 1999)

1. Utilisation systématique d'informations pour identifier les sources et pour estimer le risque. L'analyse du risque fournit une base à l'évaluation du risque, au traitement du risque et à l'acceptation du risque.
2. Utilisation des informations disponibles pour identifier les phénomènes dangereux et estimer le risque.

Appréciation du risque (CEI, 2002) Ensemble du processus d'analyse du risque et d'évaluation du risque.

Autorité de sécurité (dir, 2004a) Organisme national chargé des tâches relatives à la sécurité des chemins de fer conformément à la présente directive ou tout organisme binational chargé de ces tâches par les États Membres de manière à assurer un régime unifié en matière de sécurité sur des infrastructures transfrontières spécialisées.

B

Barrière de sécurité (de Travail et de Réflexion, 2003)

1. Tout dispositif instrumental mécanique ou procédural, permettant de prévenir ou de réduire la probabilité d'occurrence d'un événement redouté ou d'en limiter les conséquences.

2. Une barrière de sécurité de prévention permet de prévenir ou de limiter l'occurrence de l'événement redouté. Une barrière de sécurité de protection permet de diminuer les conséquences de l'événement redouté.

Barrière de sécurité intrinsèque (de Travail et de Réflexion, 2003) Liée à la conception intrinsèquement sûre du procédé ou des équipements. Cette notion s'applique surtout au matériel électrique utilisé en atmosphère explosive.

Barrière de sécurité manuelle (de Travail et de Réflexion, 2003) Nécessite une action manuelle humaine pour atteindre l'état de sécurité.

Barrière de sécurité passive (de Travail et de Réflexion, 2003) Ne nécessite pas l'apport d'une source d'énergie extérieure et l'intervention d'un système mécanique pour que la barrière joue son rôle (cuvette de rétention, arrête-flamme, ...). A contrario, une barrière de sécurité active a besoin d'énergie.

Barrière organisationnelle de sécurité (de Travail et de Réflexion, 2003) Une barrière organisationnelle de sécurité est constituée d'un ensemble de procédures et d'organisations inclus dans le système de gestion (« management ») de l'entreprise qui s'oppose à l'enchaînement d'événements susceptibles d'aboutir à un accident.

Barrière physique (de Travail et de Réflexion, 2003) Barrière provenant d'un processus physique et naturel, comme les conditions climatiques, la dissipation naturelle de la chaleur.

Barrière technique de sécurité (de Travail et de Réflexion, 2003) Une barrière technique de sécurité est constituée d'un dispositif de sécurité ou d'un système instrumenté de sécurité qui s'oppose à l'enchaînement d'événements susceptibles d'aboutir à un accident.

C

Cas spécifique (dir, 2001) Toute partie du système ferroviaire transeuropéen conventionnel qui nécessite des dispositions particulières dans les STI, temporaires ou définitives, en

raison de contraintes géographiques, topographiques, d'environnement urbain ou de cohérence vis-à-vis du système existant. Ceci peut comprendre notamment les lignes et réseaux ferroviaires isolés du réseau du reste de la Communauté, le gabarit, l'écartement ou l'entraxe des voies, le matériel roulant destiné à un usage strictement local, régional ou historique et le matériel roulant en provenance ou à destination de pays tiers sous réserve que ce matériel ne franchisse pas la frontière entre deux États membres.

Causes (dir, 2004a) Actions, omissions, événements ou conditions, ou une combinaison de ceux-ci, qui ont conduit à l'accident ou l'incident.

Communication relative au risque (CEI, 2002) Échange ou partage d'informations concernant le risque entre le décideur et d'autres parties prenantes. Les informations peuvent concerner l'existence, la nature, la forme, la probabilité, la gravite, l'acceptabilité, le traitement, ou d'autres aspects du risque.

Conséquences (CEI, 2002) Résultat d'un événement. Il peut y avoir une ou plusieurs conséquences d'un événement. Les conséquences peuvent englober des aspects positifs et des aspects négatifs. Cependant, les conséquences sont toujours négatives pour les aspects lies à la sécurité. Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Constituants d'interopérabilité (dir, 2001) Tout composant élémentaire, groupe de composants, sous-ensemble ou ensemble complet de matériels incorporés ou destinés à être incorporés dans un sous-système, dont dépend directement ou indirectement l'interopérabilité du système ferroviaire transeuropéen conventionnel. La notion de « constituant » recouvre des objets matériels mais aussi immatériels comme les logiciels.

Constituants d'interopérabilité (dir, 2004a) Tout composant élémentaire, groupe de composants, sous-ensemble ou ensemble complet d'équipements incorporés ou destinés à être incorporés dans un sous-système, dont dépend directement ou indirectement l'interopérabilité du système ferroviaire à grande vitesse ou conventionnel, tels qu'ils sont définis dans

les directives `96/48/CE` et `2001/16/CE`. La notion de « constituant » recouvre des objets matériels mais aussi immatériels comme les logiciels.

Critères de risque (CEI, 2002) Termes de référence permettant d'apprécier l'importance des risques. Les critères de risque peuvent comprendre les coûts et les avantages, les exigences d'ordre légal et réglementaire, les aspects socio-économiques et environnementaux, les préoccupations des parties prenantes, les priorités et d'autres éléments pour l'appréciation.

D

Danger (de Travail et de Réflexion, 2003)

1/ Situation, condition ou pratique qui comporte en elle-même un potentiel à causer des dommages aux personnes, aux biens ou à l'environnement. Une falaise est un danger, un flacon d'acide sulfurique est un danger.

2/ Source ou situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété, à l'environnement du lieu de travail ou une combinaison de ces éléments.

Défaillance (CEI, 2000)

1. Cessation de l'aptitude d'une entité à accomplir les fonctions requises. C'est la transition entre l'état de bon fonctionnement et l'état de panne. Dans le langage commun, on parle de panne.
2. Cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise

NOTE – L'accomplissement d'une fonction requise exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportements à éviter. L'occurrence d'un comportement à éviter est une défaillance.

NOTE – Les défaillances sont soit aléatoires (dans le matériel) soit systématiques (dans le logiciel ou le matériel).

Défaillance bénigne ou mineure (Laprie, 1994) Sa conséquence est du même ordre de grandeur que le bénéfice procuré par le service délivré en l'absence de défaillance.

Défaillance catastrophique (Laprie, 1994) Sa conséquence est incommensurablement supérieure au bénéfice procuré par le service délivré en l'absence de défaillance.

Défaillance cohérente (Laprie, 1994) Tous les utilisateurs du système ont le même perception des défaillances.

Défaillance en valeur (Laprie, 1994) La valeur du service délivré n'est pas conforme à la spécification.

Défaillance incohérente (Laprie, 1994) Les utilisateurs du système peuvent avoir des perceptions différentes des défaillances.

Défaillance temporelle (Laprie, 1994) Les conditions temporelles de délivrance du service ne sont pas conformes à la spécification.

Défaillances séquentielles (Laprie, 1994) Elles ne surviennent pas dans la même fenêtre temporelle prédéfinie.

Défaillances simultanées (Laprie, 1994) Elles surviennent dans une fenêtre temporelle prédéfinie.

Défense en profondeur (de Travail et de Réflexion, 2003) Le concept de défense en profondeur est une méthode de raisonnement et un cadre général permettant d'examiner plus complètement l'ensemble d'une installation, tant pour la concevoir que pour l'analyser dans le but d'en réduire ou maîtriser les risques le plus en amont possible.

Dispositif de sécurité (de Travail et de Réflexion, 2003) Élément unitaire ayant pour objectif de remplir une fonction de sécurité, sans apport d'énergie extérieure au système dont il fait partie. Ces dispositifs peuvent être classés en 2 catégories :

- dispositif passif : dispositif qui ne met en jeu aucun système mécanique et qui n'a pas besoin d'apport d'énergie pour remplir sa fonction. Exemples : on peut citer une cuvette de retention, un disque de rupture, un arrête-flamme ;
- dispositif actif : dispositif qui n'est pas passif. Exemples : on peut citer une soupape de décharge, un clapet excès de débit.

Dommage (CEI, 1999) Blessure physique ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement.

E

Échelle de criticité (de Travail et de Réflexion, 2003) Combinaison d'une échelle de gravité et d'une échelle de probabilité liées à l'évaluation des risques d'un évènement redouté, exprimée souvent sous forme d'une matrice de criticité.

Effets (de Travail et de Réflexion, 2003) Manifestation sur les personnes, les biens ou l'environnement des conséquences d'un évènement redouté. Pour l'homme, on définira des effets létaux et irréversibles. Au niveau matériel, seront pris en compte les dégâts réparables et la destruction complète d'équipements.

Éléments I.P.S. – Importants pour la Sécurité (de Travail et de Réflexion, 2003) Pour être qualifié d'important pour la sécurité (IPS), un élément (opération ou équipement) doit être choisi parmi les barrières de défense destinées à prévenir l'occurrence ou à limiter les conséquences d'un évènement redouté susceptible de conduire à un accident majeur potentiel. Les éléments IPS sont déterminés vis-a-vis d'un scénario d'accident majeur bien défini. Pour un scénario d'accident majeur donné, il n'y a pas nécessairement unicité de l'élément IPS. Les éléments IPS ne sont pas forcement des barrières de défense ultimes.

Entreprise ferroviaire (dir, 2004a) Entreprise ferroviaire au sens de la directive `2001/14/CE` et toute autre entreprise à statut public ou privé, dont l'activité est la fourniture de services

de transport de marchandises et/ou de passagers par chemin de fer, la traction devant obligatoirement être assurée par cette entreprise ; ceci englobe également les entreprises qui fournissent uniquement la traction.

Enquête (dir, 2004a) Procédure visant à prévenir les accidents et incidents et consistant à collecter et analyser des informations, à tirer des conclusions, y compris la détermination des causes et, le cas échéant, à formuler des recommandations en matière de sécurité.

Enquêteur principal (dir, 2004a) Personne responsable de l'organisation, de la conduite et du contrôle d'une enquête.

Erreur (Laprie, 1994) Partie de l'état du système qui est susceptible d'entraîner une défaillance : une erreur affectant le service est une indication qu'une *défaillance* survient ou est survenue. La cause adjugée ou supposée d'une erreur est une *faute*.

Erreur détectée (Laprie, 1994) Par un algorithme ou un mécanisme de détection.

Erreur latente (Laprie, 1994) Une erreur est latente tant qu'elle n'a pas été reconnue en tant que telle.

Erreurs coïncidentes (Laprie, 1994) (Avizienis et Laprie, 1986) Elles sont créées sur la même entrée.

Estimation du risque (CEI, 2002) Processus utilisé pour affecter des valeurs à la probabilité et aux conséquences d'un risque. L'estimation du risque peut considérer le coût, les avantages, les préoccupations des parties prenantes, et d'autres variables requises selon le cas pour l'évaluation du risque.

Étude de dangers (de Travail et de Réflexion, 2003) Ensemble des réflexions, travaux, déterminations expérimentales destiné à :

- identifier les situations qui présentent un certain potentiel à causer des dommages aux personnes, aux biens, à l'entreprise, et à l'environnement ;

- en évaluer les conséquences ;
- définir les moyens tant internes qu'externes a mettre en place pour réduire les risques et gérer les conséquences.

Évaluation du risque (CEI, 1999)

1. Processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque. L'évaluation du risque peut être utilisée pour appuyer la décision d'accepter ou de traiter le risque.
2. Procédure fondée sur l'analyse du risque pour décider si le risque tolérable est atteint.

Évènement (CEI, 2002) Occurrence d'un ensemble particulier de circonstances. L'évènement peut être certain ou incertain. La probabilité associée a l'évènement peut être estimée sur une période de temps donnée.

Évènement dangereux (CEI, 1999) Déclencheur qui fait passer de la situation dangereuse au dommage.

Évènement redouté (de Travail et de Réflexion, 2003) L'évènement redouté résulte de la combinaison de dérivés de paramètres de fonctionnement ou de défaillances d'éléments (équipements ou actions humaines), appelées évènements indésirables conduisant à la matérialisation du danger. Dans l'enchaînement d'évènements conduisant à un scénario d'accident majeur, l'évènement redouté constitue le moment à partir duquel la séquence d'évènements devient accidentelle.

Exploitant (dir, 1997) Toute personne physique ou morale qui exploite ou détient l'établissement ou l'installation, ou, si cela est prévu par la législation nationale, toute personne qui s'est vue déléguer àa l'égard de ce fonctionnement technique un pouvoir économique déterminant.

F

Faute active/Faute dormante (Laprie, 1994) Une faute est active lorsqu'elle produit uen erreur.

Une faute active est soit une faute interne qui était préalablement et qui a été activée par le processus de traitement, soit une faute externe.

Une faute interne peut décrire un cycle entre ses états dormant et actif.

Faute accidentelle (Laprie, 1994) Qui apparaît ou est créée de manière fortuite (*distinction selon nature).*

Faute intentionnelle (Laprie, 1994) Créée délibérément, avec une intention qui peut être présumée nuisible (*distinction selon nature*).

Faute physique (Laprie, 1994) Due à des phénomènes physiques adverses *(distinction selon origine/cause phénoménologique)*. Elle ne peut affecter directement que des composants matériels.

Faute humaine (Laprie, 1994) Résulte d'imperfections humaines *(distinction selon origine/cause phénoménologique)*. Elle peut affecter n'importe quel type de composant.

Faute interne (Laprie, 1994) Partie de l'état d'un système qui, lorsqu'activée par les traitements, produit une ou des erreurs *(distinction selon origine/frontières du système)*.

Faute externe (Laprie, 1994) Résulte de l'inférence ou des interactions du système avec son environnement physique ou humain *(distinction selon origine/frontières du système)*.

Faute de conception (Laprie, 1994) Résulte d'imperfections commises soit au cours du développement du système, soit au cours de modifications ultérieures *(distinction selon origine/phase de création)*.

Faute opérationnelle (Laprie, 1994) Apparaît durant l'exploitation du système *(distinction selon origine/phase de création).*

Faute permanente (Laprie, 1994) Dont la présence n'est pas reliée à des conditions ponctuelles, internes (processus de traitement) ou externes (environnement) *(distinction selon persistance temporelle).*

Faute temporaire (Laprie, 1994) Présente pour une durée limitée *(distinction selon persistance temporelle).*

Fautes corrélées (Laprie, 1994) Elles sont attribuées à une cause commune.

Fautes indépendantes (Laprie, 1994) Elles sont attribuées à des causes différentes.

Fonction de sécurité (de Travail et de Réflexion, 2003) Fonction ayant pour but la prévention, la détection et la protection d'évènements majeurs redoutes. Les fonctions de sécurité identifiées peuvent être assurées à partir de barrières techniques de sécurité, de barrières organisationnelles (activités humaines), ou plus généralement par la combinaison des deux.

G

Gestion du risque (de Travail et de Réflexion, 2003) Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque. Dans le guide ISO 73 (CEI, 2002), le mot *gestion* a été remplacé par *management.*

Gestionnaire de l'infrastructure (dir, 2004a) Entité ou entreprise chargée en particulier de l'établissement et de l'entretien de l'infrastructure ferroviaire, ou d'une partie de celle–ci, telle qu'elle est définie à l'article 3 de la directive `91/440/CEE` ; ceci peut comprendre également la gestion des systèmes de régulation et de sécurité de l'infrastructure. Les fonctions du gestionnaire de l'infrastructure sur un réseau ou une partie de réseau peuvent être attribuées à des entités ou des entreprises différentes.

Gravité (de Travail et de Réflexion, 2003) Mesure des conséquences d'un accident.

I

Identification des risques (CEI, 2002) Processus permettant de trouver, lister et caractériser les éléments du risque. Les éléments peuvent inclure les sources, les événements, les conséquences et la probabilité. L'identification des risques peut également identifier les préoccupations des parties prenantes.

Incident (dir, 2004a) Tout événement, autre qu'un accident ou un accident grave, lié à l'exploitation de trains et affectant la sécurité d'exploitation.

Interopérabilité (dir, 2001) Aptitude du système ferroviaire transeuropéen conventionnel à permettre la circulation sûre et sans rupture de trains en accomplissant les performances requises pour ces lignes. Cette aptitude repose sur l'ensemble des conditions réglementaires, techniques et opérationnelles qui doivent être remplies pour satisfaire aux exigences essentielles.

M

Maîtrise du risque (CEI, 2002) Actions de mise en oeuvre des décisions de management du risque. La maîtrise du risque peut impliquer la surveillance, la réévaluation et la mise en

conformité avec les décisions.

Management du risque (CEI, 2002) Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque.

Matrice de criticité (de Travail et de Réflexion, 2003) La matrice de criticité est obtenue en combinant la probabilité et la gravité. La cotation est alors réalisée à partir d'échelles qualitatives en termes de gravité et, le plus souvent, de probabilité.

Mesure de prévention (de Travail et de Réflexion, 2003) Méthodes utilisées pour réduire la probabilité d'un événement redouté. Les mesures de prévention comprennent par exemple la prévention intrinsèque, l'information et la formation.

Mesure de protection (de Travail et de Réflexion, 2003) Méthodes utilisées pour réduire la gravité des conséquences d'un événement. Les mesures de protection comprennent par exemple l'utilisation de dispositifs de protection, d'équipements de protection individuelle.

Méthodes de Sécurité Communes (MSC) (dir, 2004a) Méthodes élaborées pour décrire comment évaluer les niveaux de sécurité, la réalisation des objectifs de sécurité et la conformité à d'autres exigences en matière de sécurité.

Mise en service (dir, 2004b) Ensemble des opérations par lesquelles un sous-système est mis en état de fonctionnement nominal.

N

« **Noeud papillon** » (de Travail et de Réflexion, 2003) Schéma conceptuel développé par SHELL pour représenter les différentes étapes de la gestion des risques dans une installation.

Il part de l'identification des dangers, décrit les différentes circonstances (ou menaces) ainsi que les barrières (ou cause d'escalation) pour aboutir à l'événement. De là, un certain nombre de mesures de prévention permettent d'atténuer les conséquences qui seront *in fine* traitées par l'organisation de gestion de crise de l'établissement.

O

Objectifs de Sécurité Communs (OSC) (dir, 2004a) Niveaux de sécurité que doivent au moins atteindre les différentes parties du système ferroviaire (comme le système ferroviaire conventionnel, le système ferroviaire à grande vitesse, les tunnels ferroviaires de grande longueur ou les lignes uniquement utilisées pour le transport de marchandises) et le système dans son ensemble, exprimés sous forme de critères d'acceptation des risques.

Optimisation du risque (CEI, 2002) Processus visant, pour un risque, à minimiser les conséquences négatives et à maximiser les conséquences positives et leurs probabilités respectives. Dans le contexte de la sécurité, l'optimisation du risque est localisée sur la réduction du risque. L'optimisation du risque suit les critères de risque, en incluant le coût et les exigences légales. Les risques associés à la maîtrise du risque peuvent être considérés.

Organisme commun représentatif (dir, 2001) Organisme réunissant des représentants des gestionnaires de l'infrastructure, des entreprises ferroviaires et de l'industrie, chargé d'élaborer les STI. Les « gestionnaires de l'infrastructure » sont ceux visés aux articles 3 et 7 de la directive `91/440/CEE`.

Organismes notifiés (dir, 2004a) Organismes chargés d'évaluer la conformité ou l'aptitude à l'emploi des constituants d'interopérabilité ou d'instruire la procédure de vérification CE des sous-systèmes, tels qu'ils sont définis dans les directives 96/48/CE et 2001/16/CE.

P

Paramètre fondamental (dir, 2004b) Toute condition réglementaire, technique ou opérationnelle, critique au plan de l'interopérabilité et qui doit faire l'objet d'une décision ou d'une recommandation avant la mise au point des projets complets de STI.

Perception du risque (CEI, 2002) Manière dont une partie prenante considère un risque à partir d'un ensemble de valeurs ou de préoccupations. La perception du risque dépend des besoins exprimés, questions et connaissances des parties prenantes. La perception du risque peut différer des données objectives.

Politique de gestion des risques Majeurs (de Travail et de Réflexion, 2003) Si l'on considère le modèle classique de l'exposition à un danger constitué de la source de danger (l'installation industrielle), du vecteur de propagation des conséquences, la politique de gestion des risques se dessine selon les 3 principes généraux complémentaires que sont :

1. La réduction des risques à la source (action sur le potentiel de danger).
2. La limitation des effets d'un accident (action sur le vecteur de propagation).
3. La limitation des conséquences (action sur l'exposition des cibles).

Ainsi, ces principes se déclinent au niveau des pouvoirs publics selon une démarche en quatre volets présentée dans la figure ci-dessous :

1. la réduction du risque à la source,
2. la maîtrise de l'urbanisation,
3. l'organisation des secours,
4. l'information du public.

Prise de risque (CEI, 2002) Acceptation de la charge d'une perte, ou du bénéfice d'un gain, d'un risque particulier. La prise de risque inclut l'acceptation des risques qui n'ont pas été identifiés. La prise de risque n'inclut pas les traitements effectués par le biais des assurances, ou le transfert par d'autres moyens. Il peut exister une variabilité dans le degré d'acceptation et cela dépend des critères de risque.

Probabilité (de Travail et de Réflexion, 2003) Degré de vraisemblance pour qu'un événement se produise.

Q

Quantified Risk Assessment (QRA) (de Travail et de Réflexion, 2003) Cette approche probabiliste étudie la totalité des scénarii d'accidents. A chaque scénario, elle attribue une probabilité (fréquence) d'occurrence, en identifie les effets et les répercussions sur la population exposée tant à l'intérieur qu'à l'extérieur du site. Cette évaluation permet d'identifier autour du site industriel des zones où les probabilités de dommages matériels iront en décroissant et de tracer les courbes d'iso-probabilité correspondant à un effet, par exemple la courbe de probabilité $10^{-6}/an$ d'avoir une surpression de 140m bar. Elle permet également de tracer la courbe fréquence/population affectée (F/N) de ce site. Cette approche permet d'étudier l'impact sur le niveau du risque de différentes barrières de sécurité.

R

Réaménagement (dir, 2004b) Travaux importants de modification d'un sous-système ou d'une partie de sous-système améliorant les performances globales du sous-système.

Réduction du risque (CEI, 2002) Actions entreprises en vue de diminuer la probabilité, les conséquences négatives, ou les deux associées à un risque.

Réduction du risque à la source (de Travail et de Réflexion, 2003) Par réduction des risques à la source, il faut entendre :

- soit de la réduction au minimum des potentiels de danger (quantité de substances, pression, température, ...).

– soit de la mise en oeuvre des techniques, procédés et mesures de sécurité qui permettent d'assurer la maîtrise des risques (réduction de la probabilité d'occurrence des événements accidentels et atténuation de leur gravité).

Règles nationales de sécurité (dir, 2004a) Toutes les règles qui contiennent des exigences en matière de sécurité ferroviaire, qui sont imposées au niveau des États membres et sont applicables à plus d'une entreprise ferroviaire, quel que soit l'organisme qui les prescrit.

Renouvellement (dir, 2004b) Travaux importants de substitution d'un sous-système ou d'une partie de sous-système ne modifiant pas les performances globales du sous-système.

Risque (de Travail et de Réflexion, 2003)

1. Possibilité de survenance d'un dommage résultant d'une exposition à un danger. Le risque est la composante de la probabilité d'occurrence d'un événement redouté (incident ou accident) et la gravité de ses conséquences.
2. Combinaison de la probabilité et de la (les) conséquence(s) de la survenue d'un événement dangereux spécifié.
3. Probabilité qu'un effet spécifique se produise dans une période donnée ou dans des circonstances déterminées (dir, 1997).
4. Combinaison de la probabilité d'un événement de ses conséquences. Le terme « risque » est généralement utilisé uniquement lorsqu'il existe au moins la possibilité de conséquences négatives. Dans certaines situations, le risque provient de la possibilité d'un écart par rapport au résultat ou à l'événement attendu à ce qui était attendu.
5. Combinaison de la probabilité d'un dommage et de sa gravité (CEI, 1999).
6. Espérance mathématique de pertes en vies humaines, blessés, dommages aux biens et atteinte à l'activité économique au cours d'une période de référence et dans une région donnée, pour un aléa particulier. Le risque est le produit de l'aléa par la vulnérabilité

Risque acceptable (CEI, 2002) Niveau de gravité des conséquences et de probabilité d'occurrence d'un événement redouté considéré comme acceptable par les parties prenantes.

Risque résiduel (CEI, 1999)

1. Risque subsistant après le traitement du risque.
2. Risque subsistant après que des mesures de prévention ont été prises.

Risque tolérable (de Travail et de Réflexion, 2003) Risque accepté dans un certain contexte et fondé sur des valeurs admises par la société. Le risque tolérable est le résultat de la recherche d'un équilibre optimal entre une sécurité absolue idéale et les exigences technico-économiques.

S

Scénario (d'accident, d'incident) (de Travail et de Réflexion, 2003) Combinaison logique et chronologique de dérivés de paramètres de fonctionnement ou de défaillances d'éléments (équipements, procédures ou actions humaines) aboutissant à l'événement redouté et à la matérialisation du danger. Des scénarios spécifiques dits « de référence » peuvent être élaborés pour des secteurs d'activités particuliers.

Scénario d'accident majeur (de Travail et de Réflexion, 2003) Enchaînement d'événements indésirables, aboutissant à un accident majeur.

Sécurité (de Travail et de Réflexion, 2003) *Safety*, aptitude d'un système à fonctionner en maîtrisant à un niveau acceptable les risques pour les personnes, les biens, l'environnement et l'entreprise.

1. Absence de risque de dommage inacceptable. Le risque est acceptable, s'il a été réduit à un niveau tolérable pour un organisme en regard de ses obligations légales et de sa propre politique de santé et de sécurité au travail.
2. la sécurité est obtenue en réduisant le risque à un niveau tolérable.

Sécurité positive (principe) (de Travail et de Réflexion, 2003) Conception d'une barrière de sécurité telle qu'en cas du manque d'énergie ou de signal d'activation, elle mette l'installation dans un état sûr.

Seuil des effets (de Travail et de Réflexion, 2003) Valeur limite d'une grandeur représentative d'un effet sur les personnes, les biens ou l'environnement correspondant à un niveau d'intensité de l'effet. Les grandeurs retenues pour caractériser les risques majeurs sont :

- La dose de toxicité,
- Les flux thermiques ou la dose thermique,
- Les niveaux de surpression aérienne.

Pour chacune de ces manifestations, des seuils de létalité et d'effets irréversibles sont retenus.

Situation dangereuse (CEI, 1999) Situation dans laquelle des personnes, des biens ou l'environnement sont exposés à un ou plusieurs phénomènes dangereux.

Sous-systèmes (dir, 2001) Résultat de la division du système ferroviaire transeuropéen conventionnel comme indiqué à l'annexe II. Ces sous-systèmes pour lesquels des exigences essentielles doivent être définies, sont de nature structurelle ou fonctionnelle.

Spécification européenne (dir, 2001) Spécification technique commune, un agrément technique européen ou une norme nationale transposant une norme européenne.

Spécifications Techniques d'Interopérabilité (STI) (dir, 2004a) Spécifications dont chaque sous-système ou partie de sous-système fait l'objet en vue de satisfaire aux exigences essentielles et assurer l'interopérabilité des systèmes ferroviaires transeuropéens à grande vitesse et conventionnel.

Sûreté de fonctionnement (Villemeur *et al.*, 1988) Propriété d'un système qui permet à un utilisateur de placer une confiance justifée dans le service qu'il lui délivre.

Système ferroviaire (dir, 2004a) Ensemble des sous-systèmes pour les domaines structurels et fonctionnels ainsi que la gestion et l'exploitation du système dans son ensemble.

Système ferroviaire existant (dir, 2004b) Ensemble, constitué par les infrastructures ferroviaires, comprenant les lignes et les installations fixes, du réseau ferroviaire existant, et les matériels roulants existants de toutes catégorie et origine qui parcourent ces infrastructures.

Système de gestion de la sécurité (SGS) (dir, 2004a) Organisation et dispositions établies par un gestionnaire de l'infrastructure ou une entreprise ferroviaire pour assurer la gestion sûre de ses activités.

Système de gestion de la sécurité (SGS) (de Travail et de Réflexion, 2003) Système de gestion de la sécurité qui doit être mis en place par l'exploitant d'une installation classée relevant de la Directive SEVESO.

Système de management du risque (CEI, 2002) Ensemble d'éléments du système de gestion d'un organisme concerné par le management des risques. Les éléments du système de management peuvent inclure la planification stratégique, la prise de décision et d'autres processus vis-à-vis du risque. La culture de l'organisme se reflète dans son système de management du risque.

Système ferroviaire transeuropéen conventionnel (dir, 2001) Ensemble constitué par les infrastructures ferroviaires, comprenant les lignes et les installations fixes, du réseau transeuropéen de transport, construites ou aménagées pour le transport ferroviaire conventionnel et le transport ferroviaire combiné, et les matériels roulants conçus pour parcourir ces infrastructures.

T

Traitement du risque (CEI, 2002) Processus de sélection et de mise en œuvre des mesures visant à modifier le risque. Le terme traitement du risque est parfois utilisé pour les

mesures elles-mêmes. Les mesures de traitement du risque peuvent inclure le refus du risque, son optimisation ou son transfert.

Transfert du risque (CEI, 2002) Partage avec une autre partie de la charge de la perte ou du bénéfice du gain d'un risque. Les exigences légales ou réglementaires peuvent limiter, interdire ou imposer le transfert de certains risques. Le transfert du risque peut être effectué par des assurances ou d'autres accords contractuels. Le transfert du risque peut créer de nouveaux risques ou modifier les risques existants. Le déplacement de la source n'est pas un transfert du risque (de Travail et de Réflexion, 2003).

Annexe B

Cadre législatif et réglementaire

La Commission Européenne (CE) a émis une série de directives qui portent sur :

- La séparation des activités de gestion des infrastructures de celles d'exploitation des trains,
- Les conditions d'accès aux infrastructures, obtention de licence et de certificat de sécurité,
- L'harmonisation technique et opérationnelle, dite interopérabilité du réseau transeuropéen à grande vitesse,
- L'harmonisation technique et opérationnelle, dite interopérabilité du réseau conventionnel,
- La sécurité de fonctionnement de ces réseaux.

La mise en œuvre des directives qui portent sur l'interopérabilité des réseaux à grande vitesse et conventionnel a nécessité la mise en place de deux organes : le *Comité Article 21* des Etats Membres qui valide les travaux et l'*Organisme commun représentatif*, qui propose à la Commission et au Comité les textes réglementaires dits *Spécifications Techniques d'Interopérabilité* (STI) portant sur l'harmonisation technique et opérationnelle du réseau ferroviaire européen.

B.1 Paquets ferroviaires

B.1.1 1er paquet : Paquet *Infrastructure*

Il s'agit de trois directives adoptées par le Conseil européen le 26 février 2001 et qui devaient être transposées en droit national avant le 15 mars 2003.

- La directive `2001/12/CE` modifie la directive `91/440/CEE`. Cette directive prévoit l'ouverture de l'accès au réseau transeuropéen de fret ferroviaire (RTEFF), et dans ce but, prévoit des mesures pour éviter toute discrimination dans l'accès à l'infrastructure. Elle impose non seulement la séparation des entités assurant l'exploitation des services ferroviaires de celles chargées de gérer l'infrastructure, mais aussi que les fonctions de répartition des capacités ferroviaires, de perception des redevances d'usage de l'infrastructure et de délivrance des licences soient assurées par des organismes indépendants. Elle impose, en outre, la séparation au moins comptable des activités de transport de voyageurs et de marchandises.
- La directive `2001/13/CE` modifie la directive `95/18/CE`. Elle définit les conditions d'attribution des licences permettant l'exploitation de services de fret ferroviaire sur le RTEFF.
- La directive `2001/14/CE` remplace la directive `95/19/CE`. Elle organise la répartition des capacités ferroviaires, la tarification des *sillons* et la certification en matière de sécurité.

Le premier paquet de 1999 porte sur l'utilisation du réseau (licence, document de référence...), et du trafic fret transeuropéen. Son application en France entre en vigueur le 15 mars 2003 et marque l'ouverture du réseau ferroviaire français à la concurrence sur certains axes dans le cadre de trafics internationaux. Seules les Entreprises Ferroviaires (EF) ou les regroupements internationaux d'EF peuvent avoir accès au réseau ferré national sous réserve :

- *D'obtenir la licence d'*EF. La licence est le document par lequel un Etat Membre de l'Union Européenne reconnaît à une entreprise la qualité d'EF. La licence d'EF est valide

dans les pays de l'Union européenne, et le demeure tant que son titulaire satisfait aux capacités professionnelles et financières et à la couverture des risques.

- *D'obtenir le certificat de sécurité.* L'obtention du certificat de sécurité dépend du respect des conditions relatives à l'aptitude physique et professionnelle, au management de la sécurité (formation du personnel affecté aux fonctions de sécurité sur le réseau ferré national, réglementation de sécurité sur le réseau ferré national et à ses modalités d'application), aux règles techniques et de maintenance applicables aux matériels utilisant le réseau ferré national. Contrairement à la licence, un seul certificat de sécurité n'est pas valable pour chaque État de l'Union Européenne. L'EF sera donc dans l'obligation de demander un certificat de sécurité pour chaque Etat qu'elle traversera ou desservira.
- *De disposer de la capacité d'infrastructure*, en réalisant une demande de sillon auprès des Gestionnaires d'Infrastructure (GI).

Ce premier paquet a fait l'objet en 2006 d'un rapport d'évaluation sur l'état de transposition en droit national réalisée par les États Membres. Il apparaît que tout n'était pas encore fait en dépit de louables efforts, notamment concernant l'existence d'un organisme de contrôle indépendant ou des modalités du droit d'accès aux infrastructures. Le Grand Duché du Luxembourg était le seul à ne pas avoir encore transposé les directives du premier paquet. Un point noir concernait les subventions croisées entre transport de voyageurs de service public et le transport de marchandises sensé être autonome. Enfin, la Commission ne semble pas satisfaite de la séparation institutionnelle des gestionnaires d'infrastructure, certains restant « trop liés »- selon elle - à leur ancienne maison mère, artifice permettant à certains Etats Membres de retarder au maximum l'arrivée de nouveaux entrants.

B.1.2 2ème paquet

Le 23 janvier 2002, la Commission Européenne adopte le deuxième paquet ferroviaire, qui contient une communication et une série de propositions visant à ouvrir les marchés transport

de marchandises par rail dans l'Union Européenne. Le paquet contient une proposition visant à créer une Agence Ferroviaire Européenne ; une proposition de directive sur la sécurité des chemins de fer ainsi qu'une proposition visant à ouvrir le marché pour le transport national de marchandises par rail. Ces propositions ont été adoptées par le Parlement européen et le Conseil des ministres en avril 2004, et sont entrées en vigueur. Les éléments principaux de ce paquet sont :

- Directive relative à la sécurité.
- Modification des directives concernant l'interopérabilité.
- Règlement relatif à l'Agence Ferroviaire Européenne, qui s'est concrétisé par la création de cette agence en mai 2004.
- Recommandation concernant l'adhésion à la COTIF, un organisme qui gère les relations juridiques entre réseaux d'États.
- Modification de la directive `91/440/CEE`.

B.1.3 3ème paquet

La CE adopte un troisième paquet ferroviaire le 3 mars 2004. Ce paquet consiste en quatre propositions :

- une directive pour l'ouverture du marché pour le transport international de passagers, par rail,
- un règlement sur les droits et les obligations des passagers dans le trafic ferroviaire international,
- un règlement sur la qualité du fret ferroviaire,
- une directive pour les licences de conducteurs de train.

B.2 Directives clés pour l'interopérabilité et la sécurité

B.2.1 Directive 91/440/CEE du 29 juillet 1991

La directive du 29 juillet 1991 relative au *développement de chemins de fer communautaires* (91/440/CEE) est le texte fondateur de l'organisation des transports ferroviaires européens (dir, 1991). Elle vise à faciliter l'adaptation des chemins de fer communautaires aux exigences du marché unique et à accroître leur efficacité.

Pour ce faire, elle se fixe comme objectifs :

- la garantie de l'indépendance de gestion des EF ;
- la séparation de la gestion de l'infrastructure ferroviaire et de l'exploitation des services de transport des EF, la séparation comptable étant obligatoire, la séparation organique ou institutionnelle facultative ;
- l'assainissement de la structure financière des EF ;
- la garantie de droits d'accès aux réseaux ferroviaires des États Membres pour les regroupements internationaux d'EF effectuant des transports combinés internationaux de marchandises.

L'article 8 pose la mise en place d'une redevance d'utilisation de l'infrastructure ferroviaire pour les EF, au profit du gestionnaire d'infrastructure (GI).

En France, c'est le Décret n°98-1190 du 23 décembre 1998 relatif à l'utilisation de certains transports internationaux de l'infrastructure du réseau ferré national qui a permis de transposer au droit français les directives du Conseil des Communautés européennes 91/440 du 29 juillet 1991, 95/18 et 95/19 du 19 juin 1995.

B.2.2 Directive 96/48/CE du 23 juillet 1996

La directive 96/48/CE qui traite de l'*Interopérabilité du réseau transeuropéen à grande vitesse* a été publiée en 1996 par la Commission Européenne (CE) (dir, 1996). Elle a constitué

les organes nécessaires à la démarche visant l'intéropérabilité, et l'Association Européenne pour l'Interopérabilité Ferroviaire (AEIF) a préparé les STI sous le contrôle de la Commission et des Etats Membres dès cette année là. Elle définit les sous-systèmes qui composent le réseau :

- Infrastructure ;
- Énergie ;
- Contrôle-Commande ;
- Opération ;
- Maintenance ;
- Matériel roulant ainsi que la notion de composant participant à l'interopérabilité du sous-système dans lequel il est inclus.

Chaque STI définit pour chaque sous-système :

- Les paramètres à appliquer pour tout nouveau constituant ou sous-système implanté sur le réseau à grande vitesse,
- Les modes de convergence retenus et les dérogations éventuelles liées à la situation géographique ou à d'autres contraintes actuellement insurmontables,
- Les modalités de vérification de la conformité des composants ou de chaque sous-système concerné.

Les STI sont également accompagnées d'un rapport qui justifie, en particulier sur le plan économique, les choix proposés par l'AEIF.

Bien que l'adoption des STI soit toute récente, on peut constater que toutes les lignes nouvelles en cours de construction auront, à leur mise en service, des caractéristiques conformes aux paramètres des STI. De même, les matériels roulants en cours de construction, commandés pendant la période d'élaboration des STI, prennent en compte les paramètres des STI dans la mesure où ils étaient définis. Pour officialiser cette démarche, la Commission avait publié une recommandation le 21 mars 2001 portant sur les principaux paramètres des futures STI.

Une mention particulière doit être faite pour le système de *Contrôle-Commande* qui est défini par la directive comme devant être ERTMS - *European Railway Traffic Management System* -, ce que décrit la STI correspondante. L'implantation d'un nouveau système de signalisation en Europe pose à l'évidence de nombreux problèmes de compatibilité des matériels roulants et des infrastructures équipées et non encore équipées, et les coûts associés sont particulièrement importants. Pour résoudre cette difficulté, un plan de déploiement de ERTMS en Europe a été élaboré par la Commission, aidée par l'AEIF, sur la base des propositions des États Membres.

B.2.3 Directive 2001/16/CE du 19 mars 2001

La directive 2001/16 a pour titre : l'*Interopérabilité du système ferroviaire conventionnel transeuropéen* (dir, 2001).

Cette directive reprend les orientations de la directive Grande Vitesse pour les adapter au rail conventionnel, prend en compte le retour d'expérience acquise au cours des quatre années de préparation des STI Grande Vitesse et introduit quelques domaines nouveaux :

- Le réseau télématique et la transmission d'informations,
- La qualification des personnels.

Elle définit un programme de travail qui comporte les étapes principales suivantes :

- Élaboration d'une architecture représentative du système ferroviaire qui doit garantir la cohérence entre les STI,
- Méthode d'évaluation économique coûts-bénéfices des paramètres des STI,
- Adoption d'un référentiel d'interopérabilité transitoire sur la base des informations fournies par les États Membres,
- Élaboration des STI visant le Contrôle-Commande et la signalisation, les applications télématiques au service du fret, l'exploitation et la gestion du trafic, les wagons pour le fret et les nuisances sonores,

– Élaboration des autres STI visant principalement les activités et les équipements liés au service passagers.

B.2.4 Directive 2004/49/CE du 29 avril 2004

Les réflexions sur l'harmonisation du secteur ferroviaire ont abouti à l'adoption d'une directive sur la sécurité dans le cadre du deuxième paquet ferroviaire. La directive 2004/49/CE (dir, 2004a) du Parlement Européen et du Conseil du 29 Avril 2004 concerne la sécurité des chemins de fer communautaires et modifie la directive 95/18/CE du Conseil concernant les licences des entreprises ferroviaires, ainsi que la directive 2001/14/CE concernant la répartition des capacités d'infrastructure ferroviaire, la tarification de l'infrastructure ferroviaire. Cette directive de sécurité a été adoptée en vue de répondre aux objectifs construits sur deux axes : d'une part, l'identification claire des responsabilités des acteurs aux niveaux national et européen, et d'autre part, la mise en place d'un cadre de travail commun permettant d'élaborer progressivement des règles de sécurité européennes.

L'objectif premier de la directive est de faciliter le processus de migration vers un réseau européen unique plus attractif, plus compétitif et plus sûr.

La directive *Sécurité* porte sur quatre domaines fondamentaux liés au développement de chemins de fer sûrs en Europe.

Tout d'abord, elle vise à moderniser et harmoniser les structures réglementaires en matière de sécurité, de même que le contenu des règles de sécurité au sein des Etats Membres et au niveau européen, et ce, afin de veiller à ce que les responsabilités soient clairement établies et réparties équitablement, la sécurité étant la ligne directrice d'un bout à l'autre du processus de restructuration. La directive stipule que les gestionnaires d'infrastructure et les entreprises ferroviaires portent la responsabilité immédiate et opérationnelle de la sécurité sur les réseaux ferrés, de même que du contrôle des risques. Elle prévoit la création au sein des Etats Membres, d'instances responsables de la réglementation et du contrôle de

la sécurité, ainsi que de la coordination au niveau européen dans ce domaine. Notamment, les Etats doivent désigner des Autorités Nationales de Sécurité (ANS). Ces autorités doivent délivrer les autorisations de mise en service des équipements et des matériels roulants, en s'assurant qu'ils satisfont les exigences communautaires en matière d'interopérabilité et de sécurité. Elles doivent également délivrer, renouveler, modifier ou révoquer les certificats de sécurité des opérateurs ferroviaires.

Le deuxième domaine abordé par la directive est l'élimination des barrières existantes vis-à-vis de l'ouverture du marché. Le certificat de sécurité accordé à l'entreprise ferroviaire en vue d'une exploitation sur un réseau bien défini, est reconnu comme le moyen permettant d'accéder à l'infrastructure en question. Cette directive développe le concept de certificat de sécurité grâce à l'introduction d'exigences communes et d'éléments communs comme le système de gestion de la sécurité. Le certificat de sécurité comporte deux parties, l'une générale (qui couvre le système de gestion de la sécurité), l'autre, spécifique au territoire (qui couvre les règles et procédures nationales, le personnel et le matériel roulant). Le but final est d'établir un certificat de sécurité unique dont la partie générale est valable partout au sein de la Communauté.

Le troisième domaine qu'aborde la directive se rapporte à la transparence, à l'information et à l'application des processus *ad hoc* au niveau de la réglementation ferroviaire. La directive introduit des principes communs en matière de décision de la part des instances ferroviaires, requiert l'élaboration de règles et réglementations, prévoit des échéanciers et comporte des dispositions obligatoires pour que tous les intervenants puissent faire appel, quelle que soit la décision. Des Indicateurs de sécurité Communs (ISC) sont fixés par la directive et sont développés par le biais d'une procédure comitologique commune. Ces indicateurs permettent de suivre le développement de la sécurité ferroviaire au sein des Etats Membres aussi bien qu'au niveau de l'Union Européenne.

Le quatrième domaine que traite la directive porte sur les enquêtes en cas d'accident ou d'incident. Les Etats doivent désigner un organisme d'enquête indépendant même des

autorités de sécurité. Il est chargé de mener des enquêtes sur les accidents graves survenus sur le système ferroviaire ou les accidents et incidents qui, dans des circonstances légèrement différentes, auraient pu conduire à des accidents graves. Ces enquêtes de sécurité sont distinguées des enquêtes judiciaires : l'enquête sécurité a pour but de déterminer les causes profondes de façon à éviter tout nouvel accident ou incident, tandis que l'enquête policière vise à trouver la personne responsable d'un acte criminel - si c'est le cas. Ces enquêtes aident à détecter et éviter les défaillances techniques, les carences opérationnelles et de la gestion grâce à la diffusion des informations dans l'ensemble du secteur après n'importe quel accident ou incident.

De nombreux textes européens ont été publiés en 2009 :

- le règlement `352/2009` du 24 avril 2009 concernant l'adoption d'une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques ;
- la décision `2009/460/CE` du 5 juin 2009 relative à l'adoption d'une méthode de sécurité commune pour évaluer la réalisation des objectifs de sécurité.

B.2.5 Directive `2010/409/ue` du 19 juillet 2010

Cette directive fixe les valeurs de la première série d'objectifs de sécurité communs sur la base de valeurs nationales de référence.

Selon ce texte, pour chaque catégorie de risque ferroviaire, le niveau maximal acceptable du risque dans un État Membre doit être :

1. la Valeur Nationale de Référence (VNR) si celle-ci est égale ou inférieure à l'Objectif de Sécurité Commun correspondant ;
2. l'OSC si la VNR est supérieure à l'OSC correspondant.

La première série d'OSC énoncée par la Commission Européenne doit être considérée comme la première étape d'un processus consistant à mettre en place un cadre harmonisé et transparent en vue de contrôler et de maintenir les performances en matière de sécurité des chemins de fer européens.

B.3 Application nationale

Le décret 2006-1279 du 19 octobre 2006 relatif à la sécurité des circulations ferroviaires et à l'interopérabilité du système ferroviaire transpose, pour l'essentiel, les deux directives européennes 2004/49/CE et 2004/50/CE du Parlement européen et du Conseil du 29 avril 2004.

Il fournit un cadre rénové à l'organisation et au contrôle de la sécurité ferroviaire sur un réseau désormais ouvert à la concurrence dans le domaine du fret.

Il précise en particulier les modalités suivant lesquelles l'Etablissement Public de Sécurité Ferroviaire (EPSF), établissement public de l'Etat créé par la loi 2006-10 du 5 janvier 2006 relative à la sécurité et au développement des transports, contrôle les différentes entreprises ferroviaires autorisées à circuler sur le réseau ferré national, le Réseau Ferré de France (RFF), notamment les entreprises de fret.

Il prévoit également le contrôle par cet établissement de la sécurité de l'infrastructure ferroviaire par une procédure d'agrément du gestionnaire d'infrastructure ; cette procédure concerne aussi les projets d'infrastructure ferroviaire réalisés et exploités par un partenaire privé ou un délégataire.

Le décret fixe également un cadre nouveau pour la réglementation de sécurité des autres réseaux ferroviaires pour lesquels la réglementation de sécurité était souvent obsolète.

Enfin, il tire les conséquences de l'harmonisation des dispositions régissant l'interopérabilité du système ferroviaire communautaire destinées à faciliter les transports ferroviaires à l'échelle européenne.

Sur la base de ce décret, des arrêtés d'application doivent intervenir, soit pour adapter ceux pris sur la base du décret 2000-286 du 30 mars 2000 abrogé, soit pour préciser les nouvelles règles et procédures découlant du nouveau décret en ce qui concerne notamment :

– les conditions de délivrance des agréments, certificats et attestations de sécurité ;

- les modalités de réalisation et de mise en exploitation des systèmes et sous-systèmes ferroviaires ;
- les règles techniques et de sécurité ferroviaire applicables relevant de la responsabilité de l'Etat.

B.4 Acteurs

Comme dans le domaine aérien, le transport ferroviaire se restructure en identifiant et clarifiant les responsabilités des acteurs. Cette restructuration a nécessité la création de nouveaux acteurs afin d'harmoniser le développement du secteur ferroviaire (Ex. AFE, ANS)

B.4.1 Agence Ferroviaire Européenne

L'Agence Ferroviaire Européenne (AFE ou ERA - *European Railway Agency*) est une institution européenne qui a une double mission dans les domaines de la sécurité et de l'interopérabilité ferroviaire. Cet organisme dont le siège est situé à Valenciennes (Nord, France) emploit une centaine de personnes. Il est opérationnel depuis 2005. Son budget est évalué à environ 14,5 millions d'euros par an.

L'agence a été créée par le règlement `881/2004/CE` du Parlement européen et du Conseil du 29 avril 2004 instituant une Agence Ferroviaire Européenne.

Son conseil d'administration comprend 25 représentants des États Membres, 4 représentants de la Commission et 6 représentants du secteur ferroviaire, sans droit de vote.

Cette agence a pour tâche principale d'harmoniser les règles techniques et les règles de sécurité nationales, trop souvent incompatibles entre elles, et d'établir progressivement des objectifs de sécurité communs à tous les réseaux de chemins de fer européens. Cela est destiné à créer un marché ferroviaire véritablement intégré, et capable d'être compétitif avec les autres modes de transport, tout en conservant son niveau élevé de sécurité.

B.4.2 Organismes notifiés

La directive 96/48/CE (dir, 1996) préconise la création d'organisme notifié chargé de délivrer des certificats d'exploitation ferroviaire. Chaque État Membre a notifié, selon la directive, à la Commission Européenne un ou plusieurs organismes qualifiés pour l'évaluation et la certification.

Ces organismes notifiés réalisent les tâches suivantes :

- évaluer la conformité ou l'aptitude à l'emploi des constituants d'interopérabilité ;
- effectuer la vérification des sous-systèmes.

La preuve de la conformité à la directive 96/48/CE et aux STI connexes doit être recherchée dans la documentation pertinente. La directive 96/48/CE demande aux organismes notifiés de coopérer étroitement pour coordonner leurs activités. Le groupe de coordination des organismes notifiés *NB-Rail*, établi à cet effet, constitue le forum réunissant les organismes notifiés à l'égard de la directive 96/48/CE pour examiner ensemble les problèmes qui peuvent surgir en relation avec l'évaluation de la conformité/de l'aptitude à l'emploi des constituants d'interopérabilité et la vérification des sous-systèmes, et pour proposer des solutions à ces problèmes. Après leur adoption conformément à la procédure décrite à l'article 21 de la directive 96/48/CE, les solutions proposées deviennent des Recommandations A l'Emploi (RAE). Les RAE ne remplacent pas la législation européenne, mais la complètent en fournissant aux organismes notifiés un soutien et des informations supplémentaires sur des questions techniques.

Il est à noter que le rôle principal des organismes notifiés est de vérifier la conformité aux STI.

B.4.3 Autorité Nationale de Sécurité

L'Autorité Nationale de Sécurité (ANS)est l'organe collégial qui intervient en qualité d'autorité compétente pour l'octroi d'habilitations, d'attestations et d'avis. Elle suit également

la mise en place, le contrôle et l'amélioration de la protection des environnements et des données. L'ANS consacre la majorité de son temps à la délivrance des habilitations de sécurité. Elle délivre le certificat de sécurité et veille à ce que les performances sécurité des réseaux soient conformes aux exigences européennes.

Chaque État Membre établit une autorité de sécurité, indépendante des EF, des GI, des demandeurs de certification et des entités adjudicatrices. Cette autorité répond rapidement aux requêtes et demandes, communique ses demandes d'information sans délai et adopte toutes ses décisions dans un délai de quatre mois après que toutes les informations demandées ont été fournies.

L'autorité de sécurité effectue aussi toutes les inspections et enquêtes nécessaires pour l'accomplissement de ses tâches et a accès à tous les documents appropriés ainsi qu'aux locaux, installations et équipements des GI et des EF.

Chaque année, l'autorité de sécurité publie un rapport concernant ses activités de l'année écoulée et le transmet à l'agence au plus tard le 30 septembre.

B.4.4 Gestionnaire d'Infrastructure

Tel que défini dans l'article 3 de la directive `2004/49/CE` (dir, 2004a), le Gestionnaire d'Infrastructure (GI) est « *toute entité ou entreprise chargée en particulier de l'établissement et de l'entretien de l'infrastructure ferroviaire, ou d'une partie de celle-ci; ceci peut comprendre également la gestion des systèmes de régulation et de sécurité de l'infrastructure. Les fonctions du gestionnaire de l'infrastructure sur un réseau ou une partie de réseau peuvent être attribuées à des entités ou des entreprises différentes.* ».

Créé en 1997, le Réseau Ferré de France (RFF) est un établissement public national à caractère industriel et commercial. Cet établissement a pour objet, conformément aux principes du service public et dans le but de promouvoir le transport ferroviaire en France dans une logique de développement durable, l'aménagement, le développement, la cohérence

et la mise en valeur de l'infrastructure du réseau ferré national. RFF met en œuvre, sous le contrôle de l'Etat, le schéma d'orientation du réseau ferroviaire pour l'aménagement et le développement du territoire. Compte tenu des impératifs de sécurité et de continuité du service public, la gestion du trafic et des circulations sur le réseau ferré national ainsi que le fonctionnement et l'entretien des installations techniques et de sécurité de ce réseau sont assurés par la Société Nationale des Chemins de Fer français pour le compte et selon les objectifs et principes de gestion définis par RFF. Il la rémunère à cet effet.

B.4.5 Entreprise Ferroviaire

Une Entreprise Ferroviaire (EF) peut être définie, selon l'article 3 de la directive 2004/49/CE (dir, 2004a) comme étant « *une entreprise ferroviaire au sens de la directive 2001/14/CE et toute autre entreprise à statut public ou privé, dont l'activité est la fourniture de services de transport de marchandises et/ou de passagers par chemin de fer, la traction devant obligatoirement être assurée par cette entreprise ; ceci englobe également les entreprises qui fournissent uniquement la traction* ».

Le personnel des EF, exerçant une fonction de sécurité sur le réseau ferré national, doit répondre à des conditions d'aptitudes définies par l'Arrêté du 30 juillet 2003. Cet arrêté fixe les conditions d'aptitude physique et professionnelle à remplir par le personnel pour être habilité à exercer, même à titre occasionnel, des fonctions relatives à la sécurité des usagers, des personnels et des tiers sur le réseau ferré national ainsi que les règles relatives à la formation, l'évaluation des compétences professionnelles et l'habilitation de celui-ci.

Annexe C

Valeurs attribuées à la première série d'OSC

(*) Lors de l'extraction des données, celles sur le nombre de passages à niveau et de km-voies, qui sont nécessaires au calcul de cet OSC, n'étaient pas assez fiables (par exemple, la plupart des EM ont indiqué des km-lignes au lieu de km-voies, etc.).

Catégorie de risque	OSC	Valeur de l'OSC(*10^{-9})	Unité de mesure
Risques pour les passagers	OSC 1.1	250,0	Nombre annuel de MBGP de passagers résultant d'accidents importants/Nombre annuel de km-train de voyageurs
	OSC 1.2	2,01	Nombre annuel de MBGP de passagers résultant d'accidents importants/Nombre annuel de km-voyageurs
Risques pour le personnel	OSC 2	77,9	Nombre annuel de MBGP de membres du personnel résultant d'accidents importants/ Nombre annuel de km-trains
Risques pour les utilisateurs de passage à niveau	OSC 3.1	743,0	Nombre annuel de MBGP d'utilisateurs de passage à niveau résultant d'accidents importants/Nombre annuel de km-trains
	OSC 3.2	n.d. (*)	Nombre annuel de MBGP d'utilisateurs de passage à niveau résultant d'accidents importants/[(Nombre annuel de km-trains Œ Nombre de passages à niveau)/km-voie]
Risques pour les tiers	OSC 4	18,5	Nombre annuel de MBGP de personnes appartenant à la catégorie « tiers » résultant d'accidents importants/Nombre annuel de km-trains
Risques pour les personnes non autorisées sur les emprises ferroviaires	OSC 5	2030,0	Nombre annuel de MBGP de personnes non autorisées sur les emprises ferroviaires résultant d'accidents importants/Nombre annuel de km-trains
Risques pour la société dans son ensemble	OSC 6	2510,0	Nombre annuel total de MBGP résultant d'accidents importants/Nombre annuel de km-trains

Tableau C.1: Valeurs attribuées à la première série d'OSC

Annexe D

Liste générique des dangers pour l'exploitation d'un système ferroviaire

SPH 01	Mauvaise définition initiale de la vitesse limite (en fonction de l'infrastructure)
SPH 02	Mauvaise définition de la vitesse limite (en fonction du train)
SPH 03	Mauvaise définition de la distance de freinage / du profil de vitesse / des courbes de freinage
SPH 04	Décélération insuffisante (causes physiques)
SPH 05	Commande de vitesse / de freinage incorrecte / inadéquate
SPH 06	Vitesse enregistrée incorrecte (mauvaise vitesse du train)
SPH 07	Erreur de communication de la vitesse du train
SPH 08	Démarrage du train
SPH 09	Direction de déplacement incorrecte / mouvement intentionnel en sens inverse (combinaison de SPH 08 et SPH 14)
SPH 10	Enregistrement incorrect de la position relative/absolue
SPH 11	Erreur de détection du train
SPH 12	Perte d'intégrité du train

SPH 13	Itinéraire incorrect possible du train
SPH 14	Erreur de transmission / de communication de l'horaire/ de l'AM (autorité de mouvement)
SPH 15	Défaillance structurelle de la voie
SPH 16	Composant d'aiguillage cassé
SPH 17	Commande d'aiguillage incorrecte
SPH 18	État incorrect de l'aiguillage
SPH 19	Objet de système sur la voie / dans l'enveloppe de dégagement (ED) (hormis ballast)
SPH 20	Objet étranger sur la voie / dans l'ED
SPH 21	Usager de la route sur PN
SPH 22	Effet de sillage sur le ballast
SPH 23	Impact de forces aérodynamiques sur le train
SPH 24	Équipement / élément / chargement du train enfreint l'ED du train
SPH 25	Dimensions incorrectes de l'ED du train (bord de voie)
SPH 26	Distribution incorrecte de la charge
SPH 27	Roue cassée, essieu cassé
SPH 28	Échauffement d'un essieu / d'une roue / d'un appui
SPH 29	Défaillance d'un bogie / d'une suspension / d'un amortisseur
SPH 30	Défaillance du châssis / de la carrosserie d'une voiture
SPH 31	Accès non autorisé (du point de vue de la sécurité)
SPH 32	Personne autorisée traverse la voie
SPH 33	Personnel au travail sur la voie
SPH 34	Personne non autorisée accède à la voie (négligence)
SPH 35	Chute d'une personne depuis le quai sur la voie
SPH 36	Sillage / personne trop proche du bord du quai
SPH 37	Personnel au travail près de la voie, par exemple sur la voie voisine

SPH 38	Personne quitte le train intentionnellement (hormis échange de passagers)
SPH 39	Personne tombe par une porte (latérale)
SPH 40	Personne tombe par la porte arrière de la dernière voiture
SPH 41	Train démarre / roule avec des portes ouvertes (sans enfreindre l'ED)
SPH 42	Personne tombe sur la passerelle entre deux voitures
SPH 43	Passager se penche par la porte
SPH 44	Passager se penche par la fenêtre
SPH 45	Personnel / accompagnant de train se penche par la porte
SPH 46	Personnel / accompagnant de train se penche par la fenêtre
SPH 47	Personnel de manoeuvre sur véhicule se penche depuis le marchepied
SPH 48	Personne tombe/descend du quai dans l'écart entre le véhicule et le quai
SPH 49	Personne tombe du train / quitte le train en l'absence d'un quai
SPH 50	Personne tombe dans la zone de porte lors d'un échange de passagers
SPH 51	Fermeture des portes alors qu'une personne se trouve entre les portes
SPH 52	Mouvement du train pendant échange de passagers
SPH 53	Possibilité de personne blessée à bord
SPH 54	Risque d'incendie / d'explosion (dans le train / à proximité du train) - catégorie accident, conséquence de SPH 55, SPH 56
SPH 55	Température inappropriée (dans le train)
SPH 56	Intoxication / asphyxie (dans le train / à proximité du train)
SPH 57	Électrocution (dans le train / à proximité du train)
SPH 58	Personne tombe sur le quai (hormis échange de passagers)
SPH 59	Température inappropriée (sur le quai)
SPH 60	Intoxication / asphyxie (sur le quai)
SPH 61	Électrocution (sur le quai)

Liste des figures

Liste des tableaux

Liste des acronymes

ACB	Analyse Coûts/Bénéfices
AdR	Analyse de Risque
AEIF	Association Européenne pour l'Interopérabilité Ferroviaire
AFE	Agence Ferroviaire Européenne
AFNOR	Association Française de Normalisation
ALARP	As Low As Reasonably Practicable
AMDE	Analyse des Modes de Défaillance et leurs Effets
AMDEC	Analyse des Modes de Défaillance, leurs Effets et leur Criticité
ANS	Autorité Nationale de Sécurité
APR	Analyse Préliminaire des Risques
BP	Basic Parameter
CAR	Critère d'Acceptation des risques
CE	Commission Européenne
CEI	Commission Electrotechnique Internationale
CENELEC	Comité Européen de la Normalisation Electrotechnique
CERTIFER	Agence de Certification Ferroviaire
COFRAC	Comité Français d'Accréditation
COTIF	Convention relative aux Transports Internationaux Ferroviaires

CP	Câble principal
CSP	Constraint Satifaction Problem
D	Danger
DC	Zone de décélération
DTT	Direction des Transports Terrestres
E/E/PE	Electriques/Electroniques/Electroniques programmables de sécurité
EA	Evènement Amorce
EC	Evènement Contact
EF	Entreprise Ferroviaire
EI	Événement Initiateur
EN	European Norm (Norme Européenne)
EPSF	Etablissement Public de Sécurité Ferroviaire
ER	Événement Redouté
ERA	European Railway Agency - Agence Ferroviaire Européenne
ERTMS	European Rail Traffic Management System
ESTAS	Evaluation des Systèmes de Transport Automatisés
ETA	Event Tree Analysis
FAST	Function Analysis System Technique
FHA	Functional Hazards Analysis
FTA	Fault Tree Analysis
GAME	Globalement Au Moins Equivalent
GI	Gestionnaire d'Infrastructure
GSPN	Generalized Stochastic Petri Net
HAZOP	Hazard and Operability study
HSE	Health and Safety Executive
IMRI	Initial Mishap Risk Index

INRETS	Institut National de Recherche sur les Transports et leur Sécurité
ISC	Indicateurs de Sécurité Communs
MdR	Maîtrise des Risques
MEM	Minimum Endogenous Mortality
MSC	Méthodes de Sécurité Communes
NF	Norme Française
OHSAS	Occupational Health and Safety Assessment Series
OSC	Objectifs de Sécurité Communs
OTIF	Organisation intergouvernementale pour les Transports Internationaux
RAMS	Reliability, Availability, Maintainability and Safety
RdP	Réseau de Pétri
RFF	Réseau Ferré de France
ROSA	Railway Optimisation Safety Analysis
RTEFF	Réseau TransEuropéen de Fret Ferroviaire
SADT	Structured Analysis and Design Technic
SAMNET	SAfety Management and interoperability thematic NETwork for railways systems
SD	Situation Dangereuse
SdF	Sûreté de Fonctionnement
SGS	Système de Gestion de la Sécurité
SIL	Safety Integrity Level
SMS	Système de Management de la Sécurité
SPH	Starting Point Hazards
STI	Spécification Technique d'Interopérabilité
UE	Union Européenne
UIC	Union Internationale des Chemins de Fer

VAL	Véhicule Automatique Léger
VRN	Valeur de Référence Nationale
VSL	Value-of-statistical-life

Bibliographie

European Railway Traffic Management system. `http://www.ertms.com`.

Union Internationale des Chemins de fer. `http://www.uic.org`.

Directive 91/440/ec of 29 july 1991 on the development of the community's railways. *Official Journal of European Communities*, L237:25–28, 24 August 1991.

Directive 96/48/ec of 23 july 1996 on the interoperability of the trans-european high-speed rail system. *Official Journal of European Communities*, L235, 17 September 1996.

Directive 96/82/ce du 9 décembre 1996 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses. Rapport technique, 14 Janvier 1997.

Directive 2001/16/ce du 19 mars 2001 relative à l'interopérabilité du système ferroviaire transeuropéen conventionnel. Rapport technique, Avril 2001.

Directive 2004/49/ce du 29 avril 2004 concernant la sécurité des chemins de fer communautaires et modifiant la directive 95/18/ce du conseil concernant les licences des entreprises ferroviaires, ainsi que la directive 2001/14/ce concernant la répartition des capacités d'infrastructure ferroviaire, la tarification de l'infrastructure ferroviaire et la certification en matière de sécurité. Rapport technique, Juin 2004a.

Directive 2004/50/ce du 29 avril 2004 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 européen et du conseil relative à l'interopérabilité du système ferroviaire transeuropéen conventionnel. Rapport technique, 21 Juin 2004b.

T. AGERWALA et M. FLYNN : Comments on capabilities, limitations and ŞcorrectnessŤ of Petri nets. *ACM SIGARCH Computer Architecture News*, 2(4):86, 1973.

T.K.M. AGERWALA : *Towards a theory for the analysis and synthesis of systems exhibiting concurrency.* Thèse de doctorat, The Johns Hopkins University, 1975.

M. AJMONE MARSAN, G. CONTE et G. BALBO : A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems. *ACM Transactions on Computer Systems (TOCS)*, 2(2):93–122, 1984.

D. ANDREU, N. BRUCHON et T. GIL : Du Modèle à l'exécution : Traduction Automatique d'un Réseau de Petri Interprété en Langage VHDL. Rapport technique, Rapport de Recherche LIRMM, 2004.

A. AVIZIENIS et J.C. LAPRIE : Dependable computing : From concepts to design diversity. *Proceedings of the IEEE*, 74(5):629–638, 1986.

M. BALAKRISHNAN et K.S. TRIVEDI : Componentwise decomposition for an efficient reliability computation of systems with repairable components. pages 259–68, 1995.

G. BALBO : Stochastic Petri nets : Accomplishments and open problems. *In Computer Performance and Dependability Symposium, 1995. Proceedings., International*, pages 51–60, 1995.

G. BALBO, S.C. BRUELL et S. GHANTA : Combining queueing networks and generalized stochastic petri nets for the solution of complex models of system behavior. *IEEE Transactions on Computers*, 37(10):1251–1268, 1988.

R. BASTIDE, E. BARBONI et A. SCHYN : Component-based behavioural modelling with high-level petri nets. *In Third Workshop on Modellingof Objects, Components and Agents (MOCAŠ04)*. Citeseer, 2004.

J. BATUT : Fiabilité prévisionnelle du réseau à très haute tension d'edf. *In 5ème Colloque international de fiabilité et de maintenabilité, Biarritz*, 1986.

T. BEDFORD et R. COOKE : *Probabilistic Risk Analysis : foundations and methods.* Cambridge University Press, 2001.

J. BEUGIN : *Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé.* Thèse de doctorat, LAMIH, Université de Valenciennes et du Hainaut-Cambrésis., 2006.

A.E. BOARDMAN, D.H. GREENBERG, A.R. VINING et D.L. WEIMER : *Cost-benefit analysis : concepts and practice.* Bepress, 2006.

T. BOURDEAUD'HUY et P. YIM : Synthèse de réseaux de Petri à partir d'exigences. *In Actes de la 5me conf. francophone de Modélisation et Simulation*, pages 413–420, 2004.

D. BOUYSSOU et J.C. VANSNICK : Utilité cardinale dans le certain et choix dans le risque. *Revue économique*, 41(6):979–1000, 1990.

A.W. BROWN et KC WALLNAN : Engineering of component-based systems. *In iceccs*, page 414. Published by the IEEE Computer Society, 1996.

S. BROWN : Overview of iec 61508. design of electrical/electronic/programmable electronic safety-related systems. *Computing & Control Engineering Journal*, 11(1):6–12, 2000.

F. CASSEZ et O.H. ROUX : Traduction structurelle des réseaux de petri temporels vers les automates temporisés. *In* Hermès SCIENCE, éditeur : *4ème Colloque Francophone sur la modélisation des Systèmes Réactifs (MSRŠ03)*, 2003.

L. CAUFFRIEZ : *Méthodes et Modèles pour l'Evaluation de la Sûreté de Fonctionnement de Systèmes Automatisés Complexes- Application à l'exploitation de Lignes de Production, Application à la conception de Systèmes Intelligents Distribués.* Thèse de doctorat, LAMIH, Université de Valenciennes et du Hainaut-Cambrésis., 2005.

Commission Electrotechnique Internationale CEI : Guide iso/cei 51, aspects liés à la sécurité – principes directeurs pour les inclure dans les normes, 1999.

Commission Electrotechnique Internationale CEI : *Functional safety of electrical/electronic/programmable electronic safety-related systems*, volume IEC 61508-1 to 7. 2000.

Commission Electrotechnique Internationale CEI : Guide iso/cei 73, management du risque – vocabulaire – principes directeurs pour l'utilisation dans les normes, 2002.

Comité Européen de Normalisation Electrotechnique CENELEC : *EN50128 : Railway applications. Communications, signalling and processing systems. Software for railway control and protection systems.* CENELEC, 1998.

Comité Européen de Normalisation Electrotechnique CENELEC : *EN50129 : Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling.* CENELEC, 1999.

Comité Européen de Normalisation Electrotechnique CENELEC : *EN50126 : Applications ferroviaires : Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS).* CENELEC, 2000.

S. CHACHKOV et D. BUCHS : From formal specifications to ready-to-use software components : The concurrent object oriented petri net approach. *In International Conference on Application of Concurrency to System Design, Newcastle, IEEE Computer Society Press*, pages 99–110. Citeseer, 2001.

R. CHAMPAGNAT : *Supervision des systèmes discontinus : définition d'un modèle hybride et pilotage en temps-réel.* Thèse de doctorat, Université Paul Sabatier de Toulouse, 1998.

V. CHATEL, EM EL KOURSI, C. FELIOT et U. HUISMANN : Functional analysis of the sub-system of energy and infrastructure of conventional rail. *In Systems, Man and Cybernetics, 2002 IEEE International Conference on*, volume 3, page 6. IEEE, 2003.

G. CHIOLA, G. FRANCESCHINIS, R. GAETA et M. RIBAUDO : Greatspn 1.7 : graphical editor and analyzer for timed and stochastic petri nets. *Perform. Eval.*, 24(1-2):47–68, 1995. ISSN 0166-5316.

G. CHIOLA, M.A. MARSAN, G. BALBO et G. CONTE : Generalized stochastic Petri nets : a definition at the net leveland its implications. *IEEE Transactions on Software Engineering*, 19(2):89–107, 1993.

Muppala J. CIARDO, G. et K. TRIVEDI : Spnp : stochastic petri net package. *In Third International Workshop on Petri Nets and Performance Models, PNPM89*, pages 142–151, 1989.

A. DE BLAEIJ, R. FLORAX, P. RIETVELD et E. VERHOEF : The value of statistical life in road safety : a meta-analysis. *Accident Analysis & Prevention*, 35(6):973–986, 2003.

Groupe de Travail et de RÉFLEXION : Glossaire technique. Rapport technique, INERIS, 8 Juillet 2003.

C.F. DESIENO et L.L. STINE : A probability method for determining the reliability of electric power systems. *IEEE Transaction on Power Aparatus and Systems*, 83:174–181, 1964.

A. DESROCHES, A. LEROY, J.-F. QUARANTA et F. VALLÉ : Dictionnaire d'analyse et de gestion des risques. *In* LAVOISIER, éditeur : *Collection Management et Informatique*. Hermès, 2006.

M. Diaz et AL. : *Les réseaux de Petri - Modèles fondamentaux.* Hermes Science, Traité IC2 Information-Commande-Communication, 2001.

M. Diaz et AL. : *Vérification et Mise en œuvre des réseaux de Petri.* Hermes Science, Traité IC2 Information-Commande-Communication, 2003.

DIRECTION DES RISQUES ACCIDENTELS : *Analyse des risques et prévention des accidents majeurs : Synthèse vis-à-vis de l'étude de danger*. INERIS, 2004.

A. DUBI : *Monte Carlo applications in systems engineering.* Wiley, 2000.

C.A. ERICSON : *Hazard analysis techniques for system safety.* John Wiley and Sons, 2005.

B. FISCHHOFF et I. FISCHOFF : Will they hate us ? anticipating unacceptable risks. *Risk Management : An International Journal*, 3(4):7–18, 2001.

I. FOSTER : *Designing and building parallel programs : concepts and tools for parallel software engineering.* Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA, 1995.

R. GARNIER : *Une méthode efficace d'accélération de la simulation des réseaux de pétri stochastiques.* Thèse de doctorat, Université Bordeaux I, 1998.

H.J. GENRICH : Predicate/transition nets. *Advances in Petri Nets*, 254:207–2471, 1986.

A. GIGANTINO : Report on the representative architecture. Rapport technique, Association Européenne pour l'Interopérabilité Ferroviaire, 2002.

F. GLOVER et M. LAGUNA : Tabu search, modern heuristic techniques for combinatorial problems, 1993.

S.W. GOLOMB et L.D. BAUMERT : Backtrack programming. *Journal of the ACM (JACM)*, 12 (4):516–524, 1965.

G. GÖSSLER, S. GRAF, M. MAJSTER-CEDERBAUM, M. MARTENS et J. SIFAKIS : An approach to modelling and verification of component based systems. *SOFSEM 2007 : Theory and Practice of Computer Science*, pages 295–308, 2007.

B.S. HECK, L.M. WILLS et G.J. VACHTSEVANOS : Software technology for implementing reusable, distributed control systems. *Applications of Intelligent Control to Engineering Systems*, pages 267–293, 2009.

L. HOEGBERG : Risk perception, safety goals and regulatory decision-making. *Reliability Engineering & System Safety*, 59(1):135–139, 1998.

C.C. HUANG et A. KUSIAK : Modularity in design of products and systems. *IEEE Transactions on Systems, Man and Cybernetics, Part A : Systems and Humans*, 28(1):66–77, 1998.

INERIS-DRA : *Analyse des Risques et Prévention des Accidents Majeurs (DRA-34)*. INERIS, Direction des Risques Accidentels, 2003.

D. JOVICIC : Exemples dŠappréciation des risques et dŠoutils possibles pour faciliter lŠapplication du règlement msc. Rapport technique, Agence Ferroviaire Européenne, 2009.

G. JUANOLE et L. GALLON : Analyses qualitatives et quantitatives basées sur des Réseaux de Petri stochastiques et concept d'Automate Quotient Quantifié. *In Modélisation et vérification des processus parallèles. Ecole d'été*, pages 93–107, 1998.

M. KAANICHE : *Evaluation de la sûreté de fonctionnement informatique. Fautes physiques, fautes de conception, malveillances.* Thèse de doctorat, Institut National Polytechnique, 1999.

A. KAUFMANN, D. GROUCHKO et R. CRUON : *Modèles mathématiques pour l'étude de la fiabilité des systèmes.* Masson, 1975.

C. KERMISCH et P.E. LABEAU : Approche dynamique de la fiabilité des systèmes. *Rapport MNFD*, 10, 2002.

S. KIRKPATRICK, C.D. GELATT JR et M.P. VECCHI : Optimization by simulated annealing. *Science*, 220(4598):671–680, 1983.

H. KUMAMOTO, E.J. HENLEY et Society RELIABILITY : *Probabilistic risk assessment and management for engineers and scientists*. IEEE press, 1996.

A. KUSIAK : Integrated product and process design : a modularity perspective. *Journal of Engineering Design*, 13(3):223–231, 2002.

R.N. LANGLOIS : Modularity in technology and organization. *Journal of Economic Behavior & Organization*, 49(1):19–37, 2002.

J.C. LAPRIE : Concepts de base de la tolérance aux fautes. *In* MASSON, éditeur : *Informatique tolérante aux fautes*, volume 15 de *Arago*. Observatoire Français des Techniques Avancées, Mars 1994.

B. LE TRUNG : Des principes de sécurité GAME, MEM, ALARP : The GAME, MEM and ALARP principles of safety. *Recherche-Transports-Sécurité*, 68:48–62, 2000.

M. MALHOTRA et KS TRIVEDI : Power-hierarchy of dependability-model types. *Reliability, IEEE Transactions on*, 43(3):493–502, 1994.

A. MASRI : *Towards the Distributed Control of Manufacturing Systems : A Component-Based Approach for Modeling Communication Architectures*. Thèse de doctorat, Ecole Centrale de Lille, 2009.

M. MAZOUNI : *Pour une meilleure approche du management des risques : de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision*. Thèse de doctorat, Institut National Polytechnique de Lorraine, 2008.

M. MEDJOUDJ : *Contribution à l'analyse des systèmes pilotés par calculateurs : Extraction de scénarios redoutés et vérification de contraintes temporelles*. Thèse de doctorat, Université Paul Sabatier, Toulouse, 2006.

RE MELCHERS : On the alarp approach to risk management. *Reliability Engineering and System Safety*, 71(2):201–208, 2001.

P.M. MERLIN : A study of the recoverability of computing systems. 1974.

E.J. MISHAN et E. QUAH : *Cost-benefit analysis*. Routledge, 2007.

M. K. MOLLOY : Performance analysis using stochastic petri nets. *IEEE Trans. Comput.*, 31 (9):913–917, 1982.

U. MONTANARI : Networks of constraints : Fundamental properties and applications to picture processing. *Information sciences*, 7:95–132, 1974.

E. MORIN : *Introduction à la pensée complexe*. Esf, 1994.

T. MURATA : Petri nets : Properties, analysis and applications. *In Proceedings of the IEEE*, volume 77(4), pages 541–580, 1989.

S.O. NATKIN : *Les réseaux de Petri stochastiques et leur application à l'évaluation des systèmes informatiques*. Thèse de doctorat, Conservatoire National des Arts et Métiers de Paris, 1980.

OHSAS : 18001 : Systèmes de management de la santé et de la sécurité au travail. *British Standards Institution*, 1999.

D.W. PEARCE : *Cost-benefit Analysis*. Macmillan, 1983.

U. PERSSON, A. NORINDER, K. HJALTE et K. GRALÉN : The value of a statistical life in transport : Findings from a new contingent valuation study in sweden. *Journal of Risk and Uncertainty*, 23 (2):121–134, 2001.

C.A. PETRI : Kommunikation mit automaten. *Bonn : Institut fur Instrumentelle Mathematik, Schriften des IIM Nr*, 2:65–377, 1962.

M. RAFRAFI : *Communiquer, Naviguer, Surveiller : Innovations pour des transports plus sûrs, plus efficaces et plus attractifs*, volume 112 de *Actes INRETS*, chapitre Une Démarche Harmonisée pour l'Allocation des Objectifs de Sécurité Basée sur une Approche Fonctionnelle, pages 27–39. INRETS, 2007.

M. RAFRAFI, T. BOURDEAUD'HUY et E.-M. EL-KOURSI : Risk apportionment methodology based on functional analysis. *In Computational Engineering in Systems Applications, IMACS Multi-conference on*, pages 1103–1109, 2006.

M. RAFRAFI, T. BOURDEAUD'HUY et E.-M. EL-KOURSI : Stochastic petri nets for risk assessment. *In Formal Methods for Automation and Safety in Railway and Automotive Systems, FORMS/FORMAT 2008*, Octobre 2008a.

M. RAFRAFI et E.-M. EL-KOURSI : Functional hazard analysis for railway safety. *In* Eckehard Schneider Géza Tarnai (EDS.), éditeur : *Formal Methods for Automation and Safety in Railway and Automotive Systems "FORMS/FORMAT2007"*, pages 164–73, 2007.

M. RAFRAFI et E.-M. EL-KOURSI : Programmation par contraintes pour l'allocation des objectifs de sécurité : Application au transport ferroviaire. *In Actes 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, LM16*, Octobre 2008.

M. RAFRAFI et E.-M. EL KOURSI : Risk apportionment for railway safety. *In Fourth Working on Safety Conference, WOS'2008*, Octobre 2008a.

M. RAFRAFI et E.-M. EL KOURSI : Risk apportionment for railway system using constraint programming. *In Sixth International Conference in Computer Simulation Risk Analysis and Hazard Mitigation : Risk Analysis'2008*, Mai 2008b.

M. RAFRAFI, E.-M. EL-KOURSI et T. BOURDEAUD'HUY : Safety levels apportionement in railway system. *IJR International Journal of Railway*, 1(4):157–168, Décembre 2008b.

C. RAMCHANDANI : *Analysis of asynchronous concurrent systems by timed Petri nets.* Thèse de doctorat, Massachusetts Institute of Technology, 1973.

J. RASMUSSEN et I. SVEDUNG : *Proactive risk management in a dynamic society.* Swedish Rescue Services Agency Karlstad, Sweden, 2000.

F. REDMILL : Iec 61508-principles and use in the management of safety. *Computing & Control Engineering Journal*, 9(5):205–213, 1998.

AL REIBMAN et M. VEERARAGHAVAN : Reliability modeling : an overview for system designers. *Computer*, 24(4):49–57, 1991.

M. SADOU : *Aide à la conception des systèmes embarqués sûrs de fonctionnement.* Thèse de doctorat, INSA de Toulouse, 2007.

M. SALLAK, C. SIMON et J.F. AUBRY : A fuzzy probabilistic approach for determining safety integrity level. *IEEE Transactions on Fuzzy Systems*, 16(1):239–248, 2008.

J. SAMETINGER : *Software engineering with reusable components*. Springer Verlag, 1997.

H. SCHÄBE : Different approaches for determination of tolerable hazard rates. *In ESREL 2001 Conference proceedings*, volume 1, pages 435–442, 2001.

R. SCHOENIG et J.F. AUBRY : *Définition d'une méthodologie de conception des systèmes mécatroniques sûrs de fonctionnement*. Thèse de doctorat, Institut National Polytechnique de Lorraine, 2004.

F. SEYLER et P. ANIORTE : A component meta model for reused-based system engineering. *In Workshop in Software Model Engineering, Dresden, Germany*. Citeseer, 2002.

M. STAMATELATOS, G. APOSTOLAKIS, H. DEZFULI, C. EVERLINE, S. GUARRO, P. MOIENI, A. MOSLEH, T. PAULOS et R. YOUNGBLOOD : Probabilistic risk assessment procedures guide for nasa managers and practitioners. *Office of Safety and Mission Assurance NASA Headquarters, Washington, DC. March*, 31, 2002.

R. TIENNOT, Y. CHAABI et P. BERTHO : Etude et certification d'un système instrumenté de sécurité sous-marin. *In 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*, Octobre 2008.

Y. VERNAT : Formalisation et qualification de modèles par contraintes en conception préliminaire. 2004.

A. VILLEMEUR, P. CASEAU et Arnould D'HARCOURT : *Sûreté de fonctionnement des systèmes industriels : fiabilité, facteurs humains, informatisation*. Eyrolles, 1988.

W.K. VISCUSI et J.E. ALDY : The value of a statistical life : A critical review of market estimates throughout the world. *Journal of Risk and Uncertainty*, 27(1):5–76, 2003.

P. ZIEGLER et H. SZCZERBICKA : A structure based decomposition approach for GSPN. *In Petri Nets and Performance Models*, pages 261–270. Published by the IEEE Computer Society, 1995.

Titre : ***Une approche harmonisée pour l'évaluation de la sécurité des systèmes ferroviaires : De la décomposition fonctionnelle au modèle comportemental***

Les systèmes complexes ferroviaires étant de plus en plus contraints par des autorités de décision placées à un haut niveau d'abstraction, il devient problématique d'imposer des critères à une autre échelle que fonctionnelle. Ainsi, dès lors que l'on descend plus bas, nous sommes confrontés à des spécificités des systèmes nationaux qui font perdre la généralité du travail des décisionnaires Européens. Le problème est qu'à chaque niveau d'abstraction, des méthodes d'évaluation du risque existent, mais sans être compatibles entre elles. Par ailleurs, la combinaison des couches et la vision fonctionnelle du système ne prennent pas en compte l'impact des fonctions les unes sur les autres, ni le lien entre le niveau global et les composants afin d'allouer la sécurité. Nous proposons donc une démarche harmonisée d'évaluation du risque, capable de répartir les contraintes définies au niveau fonctionnel abstrait sur les entités qui implémentent les systèmes avec leurs spécificités. Notre contribution est méthodologique. Elle part d'un modèle fonctionnel du système ferroviaire constitué en couches. Le but étant de représenter ce système sans dépendance entre les fonctions, il a fallu les traduire indépendamment des autres en faisant apparaître les entrées/sorties comme des places/transitions d'un réseau de Petri. A chaque couche de la décomposition correspond une classe de réseau de Petri. Ainsi, à la couche structurelle, nous associons les réseaux de Petri Temporels ; à la couche fonctionnelle les réseaux de Petri Stochastiques et à la couche logique les réseaux de Petri Prédicats/Transitions.

Mots clés : *Interopérabilité ferroviaire, Objectifs de Sécurité Communs, Acceptation du risque, Evaluation du risque, Approche modulaire, Réseau de Petri*

Title : ***A harmonized approach for safety assessment in railways : from a functional decomposition to a behavioral model***

The railway systems are being more and more forced by decision authorities. As they are placed at a high level of abstraction, it becomes problematic to impose another criterion or scale. In fact, since we come down lower, we are confronted with specificities of the national systems which make lose the majority of the work of the European decision-makers. The issue is that, at every level of abstraction, risk assessment methods exist, but without being compatible. Besides, the combination of layers and the functional vision of the railway system do not take into account the impact of some functions on the others, nor the link between the global level of risk and the components to assign the safety. Thus, we propose a harmonized approach for risk assessment. This approach allows us to distribute the constraints defined at the abstract functional level on the entities which implement both the systems and their specificities. Our contribution is methodological. It leaves a functional model of the layered railway system. The purpose is to represent this system without any dependencies between the functions. For instance, it was necessary to translate them independently by creating entrances/exits as places/transitions of a Petri net. A Petri net class corresponds to each layer. To the structural layer, we associate the time Petri net ; to the functional layer, the stochastic Petri nets and to the logical layer, the predicate transitions nets.

Keywords : *Railway interoperability, Common Safety Targets, Risk acceptatbility, Risk assessment, Modular approach, Petri Nets*