HAL
open science

Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé

Julie Beugin

To cite this version:

Julie Beugin. Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé. Automatique / Robotique. Université de Valenciennes et du Hainaut-Cambresis, 2006. Français. NNT : . tel-00132452

HAL Id: tel-00132452

https://theses.hal.science/tel-00132452v1

Submitted on 21 Feb 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

N° d'ordre : 06-35

THÈSE

Présentée à

L'UNIVERSITÉ DE VALENCIENNES

ET DU HAINAUT-CAMBRÉSIS

Pour l'obtention du grade de

Docteur en Automatique et Informatique des Systèmes Industriels et Humains

Mention Automatique Industrielle et Humaine

Par

Julie BEUGIN

Ingénieur de l'École Nationale Supérieure d'Ingénieurs en Informatique, Automatique, Mécanique, Énergétique et Électronique

Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé

Soutenue publiquement le 20 Décembre 2006 devant le jury composé de :

M.	Joaquín	**RODRIGUEZ**	Directeur de recherche, INRETS-ESTAS	Rapporteur
M.	Jean-Marc	**THIRIET**	Professeur, LAG, INPG (Grenoble)	Rapporteur
M.	Christophe	**CASSIR**	Docteur, Agence Ferroviaire Européenne	Examinateur
M.	Philippe	**CHARPENTIER**	Docteur, INRS (Nancy)	Examinateur
M.	Christian	**TAHON**	Professeur, LAMIH, UVHC	Examinateur
M.	Laurent	**CAUFFRIEZ**	Maître de conférences (HDR), LAMIH, UVHC	Co-directeur
Mme	Dominique	**RENAUX**	Maître de conférences, LAMIH, UVHC	Co-directeur
M.	Frédéric	**VANDERHAEGEN**	Professeur, LAMIH, UVHC	Co-directeur

Laboratoire d'Automatique, de Mécanique et d'Informatique industrielles et Humaines

UMR CNRS 8530, UVHC Le Mont Houy 59313 VALENCIENNES Cedex 9

UMR CNRS 8530

Avant-propos

Les travaux présentés dans ce mémoire ont été réalisés au Laboratoire d'Automatique, de Mécanique et d'Informatique industrielles et Humaines (LAMIH), unité mixte de recherche du Centre National de la Recherche Scientifique (CNRS), située au sein de l'Université de Valenciennes et du Hainaut-Cambrésis (UVHC).

Je tiens à adresser tous mes remerciements à Monsieur Laurent CAUFFRIEZ, Maître de Conférences habilité à diriger les recherches, Madame Dominique RENAUX, Maître de Conférences, et Monsieur Frédéric VANDERHAEGEN, Professeur et directeur de l'équipe Système Homme-Machine (SHM), pour avoir accepté de diriger cette thèse.

J'exprime ma profonde gratitude à Messieurs Joaquín RODRIGUEZ, directeur de recherche à l'INRETS-ESTAS de Villeneuve d'Ascq (Institut National de Recherche sur les Transports et leur Sécurité - Évaluation des Systèmes de Transports Automatisés et de leur Sécurité), et Jean-Marc THIRIET, Professeur au LAG (Laboratoire d'Automatique de Grenoble), qui m'ont fait l'honneur d'être rapporteurs de ce mémoire de thèse.

Je remercie également Messieurs Christophe CASSIR, responsable de projets à l'Agence Ferroviaire Européenne de Valenciennes, Philippe CHARPENTIER, chef du laboratoire Sûreté des Systèmes Automatisés à l'INRS de Nancy (Institut National de Recherche et de Sécurité), et Christian TAHON, Professeur au LAMIH, d'avoir accepté de faire partie de mon jury.

Je voudrais exprimer toute ma reconnaissance à Monsieur le Professeur Patrick MILLOT pour m'avoir accueillie en 2002 au sein du LAMIH qu'il dirigeait alors, pour son soutien et pour les conseils qu'il m'a donnés.

L'expérience que j'ai acquise dans le domaine de la sécurité des transports guidés m'est en grande partie due à Messieurs Jean-Paul SCHNEIDER et Jean-Paul RICHARD de la RATP (Régie Autonome des Transports Parisiens) qui m'ont permis d'effectuer une semaine de formation à la RATP sur la gestion de la circulation des transports urbains (dans le cadre du

projet européen UGTMS –Urban Guided Transport Management system–). Je tiens à leur adresser mes plus vifs remerciements ainsi qu'à toutes les personnes qui ont participé à cette formation. Mesdames Nathalie DUQUENNE, et Anca STUPARU de l'INRETS, m'ont également apporté de nombreuses remarques dans ce domaine, je leur en suis très reconnaissante.

J'adresse également tous mes remerciements à l'ensemble des personnes et amis que j'ai pu côtoyer durant ces années de thèse au LAMIH, pour leur soutien et leur bonne humeur. Je pense notamment à Vincent, Hélène, Marie-Pierre, Sébastien, Jimmy, Djamel, Pierre, François, Mélany, Julien, Philippe D.S., Philippe P., Abir. J'espère que vous me pardonnerez pour toutes les fois où je ne vous ai pas immédiatement répondu en raison de ces fameux bouchons d'oreilles dont je ne peux me séparer pour me concentrer. J'ai indirectement expérimenté le hard rock, mais je n'ai pas réussi à l'adopter comme ambiance de travail (désolée pour toutes mes réclamations à ce sujet ;-)…).

Je tiens à remercier chaleureusement toute ma famille pour leur soutien et mes amis pour leur compréhension face à mes rares apparitions en groupe. J'exprime enfin toute mon affection à Aurélien qui a su, pendant cette période d'études, me supporter avec tendresse et m'attendre. Je lui dédie ce mémoire.

Table des matières

AVANT-PROPOS **3**

INTRODUCTION GENERALE **9**

CHAPITRE 1. ANALYSE SYSTEMIQUE DE LA SURETE DE FONCTIONNEMENT ET MAITRISE DES RISQUES DES SYSTEMES COMPLEXES **13**

INTRODUCTION **14**
1.1 LA SYSTEMIQUE : SCIENCE FONDAMENTALE CONTRIBUANT A L'ETUDE DES SYSTEMES COMPLEXES **15**
1.1.1 La notion de complexité des systèmes *15*
1.1.2 La systémique *16*
1.1.3 L'approche systémique et l'ingénierie système *17*
1.2 ANALYSE DE LA SURETE DE FONCTIONNEMENT DES SYSTEMES COMPLEXES **19**
1.2.1 Les concepts de la sûreté de fonctionnement *19*
1.2.2 Les moyens de la sûreté de fonctionnement *21*
1.2.3 Analyses qualitatives *23*
1.2.3.1 Les méthodes d'analyse fonctionnelle et structurelle 23
1.2.3.2 Les méthodes d'analyse des défaillances 24
1.2.3.3 Les réseaux bayésiens 26
1.2.4 Analyses quantitatives *27*
1.2.4.1 De l'analyse statique à l'analyse dynamique : approche par simulation de Monte Carlo 27
1.2.4.2 Approche bayésienne 29
1.3 MAITRISE DES RISQUES DES SYSTEMES COMPLEXES **31**
1.3.1 Terminologie et base des études de sécurité *31*
1.3.1.1 Définitions, caractéristiques et critères liés à la notion de danger 31
1.3.1.2 Le concept de sécurité et le concept connexe de risque 34
1.3.2 La gestion des risques des systèmes *36*
1.3.2.1 Le processus de gestion des risques 36
1.3.2.2 L'acceptation du risque des systèmes 38
1.3.2.3 Les moyens de prévention et de protection contre le risque 39
1.3.3 L'évaluation du risque *40*
1.3.3.1 Principes 40
1.3.3.2 Les objectifs de sécurité 41
1.4 CONCLUSION **41**

CHAPITRE 2. LA PROBLEMATIQUE DE L'EVALUATION DE LA SECURITE DES LA CONCEPTION D'UN SYSTEME COMPLEXE DE TRANSPORT GUIDE **43**

INTRODUCTION **44**
2.1 LES RISQUES LIES A L'EXPLOITATION DES SYSTEMES DE TRANSPORT GUIDE **45**
2.1.1 Les risques génériques *45*
2.1.2 Les risques pouvant être atténués par les systèmes de transport guidé *48*
2.1.2.1 Les risques liés à la circulation des trains 48
2.1.2.2 Les risques liés au matériel 49
2.1.2.3 Les risques liés aux opérateurs 49
2.2 LES MOYENS DE REDUCTION DES RISQUES EXISTANT DANS LE DOMAINE DES TRANSPORTS GUIDES **50**
2.2.1 Les moyens de prévention des risques *50*

2.2.1.1 Gestion des risques liés à la circulation des trains : principe de la signalisation 50
2.2.1.2 Gestion des risques liés au matériel 55
2.2.1.3 Gestion des risques liés aux opérateurs 56
2.2.2 Les moyens de protection contre le risque 56
2.3 L'EVALUATION ET L'ACCEPTABILITE DES RISQUES GENERES PAR UN SYSTEME DE TRANSPORT GUIDE 57
2.3.1 Contexte législatif et normatif de la sécurité des systèmes de transport guidé européens 57
2.3.2 Principes d'acceptation du risque 58
2.3.3 Le concept de niveau d'intégrité de sécurité (SIL) 59
2.3.4 L'analyse des risques centrée sur les SILs 62
2.3.5 Les méthodes d'allocation des SILs aux fonctions de sécurité 63
2.3.5.1 Les méthodes quantitatives 63
2.3.5.2 Les méthodes qualitatives 66
2.4 DISCUSSION 68
2.5 CONCLUSION 69

CHAPITRE 3. PROPOSITION D'UNE APPROCHE POUR L'EVALUATION DE LA SECURITE DES SYSTEMES COMPLEXES DE TRANSPORT GUIDE 71

INTRODUCTION 72
3.1 L'ASPECT QUANTITATIF LIE AUX SILS, APPLICATION AU DOMAINE DES TRANSPORTS GUIDES 73
3.1.1 Différentes interprétations selon différents indicateurs 73
3.1.1.1 Les indicateurs employés pour les systèmes faiblement sollicités 73
3.1.1.2 Les indicateurs employés pour les systèmes fortement sollicités 75
3.1.2 Un indicateur quantitatif cohérent et approprié aux systèmes de transport guidé 76
3.2 METHODES DE QUANTIFICATION DES PROFILS DE RISQUE SELON LA COMBINAISON DES SILS 77
3.2.1 Représentation des profils de risque 77
3.2.2 La prise en compte des dépendances entre les fonctions de sécurité combinées 79
3.2.3 La combinaison des SILs 80
3.2.3.1 Approche basée sur des règles de combinaison : mise en place d'une algèbre des SILs 80
3.2.3.2 Approche liée aux événements rares : approche par simulation de Monte Carlo biaisée 81
3.2.4 Mise en œuvre et comparaison des méthodes de combinaison des SILs 82
3.3 LA MODELISATION DE LA COMPLEXITE D'UN SYSTEME DE TRANSPORT GUIDE 85
3.3.1 Déclinaisons de la complexité d'un système de transport guidé 85
3.3.2 Le concept de « situation d'exploitation » 86
3.3.3 Le modèle générique d'une situation d'exploitation support à la modélisation du système de transport guidé 88
3.3.4 Démarche de discrétisation pour la modélisation de l'évolution dynamique du système 91
3.4 METHODE DE SIMULATION POUR L'OBTENTION DE SCENARIOS DE RISQUE 93
3.4.1 Présentation de la méthode dédiée à la simulation de l'évolution des situations d'exploitation 93
3.4.2 Génération aléatoire de défaillances dangereuses 95
3.4.3 Technique d'injection de défaillances dangereuses 95
3.4.4 Identification des scénarios de risque 95
3.4.5 La simulation en tant que moyen de validation de la sécurité du système 96
3.5 CONCLUSION 96

CHAPITRE 4. SIMULATION D'UN SYSTEME DE TRANSPORT GUIDE POUR LA VALIDATION DE L'APPROCHE PROPOSEE 99

INTRODUCTION 100
4.1 PRESENTATION DU SYSTEME DE TRANSPORT GUIDE 100
4.1.1 Cartographie du réseau 100
4.1.2 Les fonctionnalités liées au cantonnement 101

4.1.3 Les fonctionnalités liées aux enclenchements d'itinéraires *102*
4.1.4 La transmission des données du sous-système sol au sous-système bord *104*
4.2 MODELISATION DU SYSTEME SELON LE CONCEPT DE SITUATION D'EXPLOITATION ET DEVELOPPEMENT DE LA MAQUETTE LOGICIELLE DU SYSTEME 105
4.2.1 L'instanciation des classes du modèle de situation d'exploitation *105*
4.2.2 La génération dans le temps de défaillances dangereuses du système par simulation de Monte Carlo biaisée *109*
4.2.2.1 La prise en compte des dépendances des fonctions de sécurité 109
4.2.2.2 La prise en compte de la duplication des fonctions de sécurité 110
4.2.2.3 Mise en œuvre de la simulation de Monte Carlo biaisée 111
4.2.3 La simulation du contexte opérationnel intégrant des événements dangereux *112*
4.2.3.1 Présentation de la maquette logicielle reproduisant le fonctionnement du système 112
4.2.3.2 L'influence des défaillances dangereuses sur la simulation de la maquette logicielle..... 113
4.3 IDENTIFICATION ET EVALUATION DES SCENARIOS OBTENUS PAR SIMULATION 113
4.3.1 Les profils de risque établis a priori *113*
4.3.2 Evaluation préalable : analyse quantitative sans prise en compte du contexte opérationnel..... *117*
4.3.3 Analyse qualitative des situations d'exploitation *121*
4.3.4 Analyse quantitative des situations d'exploitation *123*
4.3.4.1 Optimisation nécessaire du temps d'exécution des simulations 123
4.3.4.2 Résultats de l'évaluation pour les deux cas d'étude retenus 124
4.3.5 Discussion *126*
4.4 CONCLUSION 127

CHAPITRE 5. PERSPECTIVES 129

INTRODUCTION 130
5.1 L'UTILISATION QUANTITATIVE DES SILS 131
5.1.1 Intégration de facteurs liés au diagnostic dans le calcul des SILs *131*
5.1.2 Le SIL vu comme un paramètre incertain *132*
5.2 DEFINITION DE VARIABLES D'INFLUENCE SUPPORT D'AIDE A LA DECISION 133
5.2.1 Mise en évidence de critères opérationnels *133*
5.2.2 La prise en compte de la composante de coût dans la décision d'acceptation du risque *134*
5.3 PRISE EN COMPTE DES FACTEURS HUMAINS DANS L'EVALUATION DE LA SECURITE GLOBALE 135
5.3.1 Spécificités des facteurs humains dans le domaine des transports guidés *135*
5.3.2 Une approche basée sur la méthode Safe-SADT pour la quantification de l'erreur humaine associée à une tâche donnée *137*
5.3.2.1 Intérêts de la méthode Safe-SADT 137
5.3.2.2 Esquisse d'une méthode Safe-SADT^{+} tenant compte des facteurs humains 137
5.4 CONCLUSION 139

CONCLUSION GENERALE 141

REFERENCES BIBLIOGRAPHIQUES 145

ANNEXES 154

ANNEXE A. THEORIE DU TRANSPORT DE PARTICULES APPLIQUEE A LA DYNAMIQUE DES SYSTEMES – EVALUATION PAR SIMULATION DE MONTE CARLO 154
A.1 Théorie du transport de particules appliquée à la dynamique des systèmes *154*
A.2 Algorithme d'évaluation par simulation de Monte Carlo biaisée *158*

ANNEXE B. FONCTIONS REALISEES PAR LES PRINCIPAUX SYSTEMES DE TRANSPORT GUIDE EXISTANTS 159

ANNEXE C. TERMINOLOGIE RELATIVE A L'ETUDE DES DEFAILLANCES DANGEREUSES D'UN SYSTEME DE SECURITE 165
C.1 La typologie des défaillances 165
C.2 Les tests périodiques 165
C.3 Les tests de diagnostic 166
C.4 Le taux de couverture des tests de diagnostic 166
C.5 La proportion de défaillances en sécurité 167

ANNEXE D. EXEMPLE D'INSTANCIATION DES CLASSES DU MODELE DE SITUATION D'EXPLOITATION RELATIVES A L'OPERATEUR HUMAIN 168
D.1 La classe « activité » 168
D.2 La classe « équipe d'opérateurs » 168
D.3 La classe « mode d'exploitation » 169

ANNEXE E. FONCTION DE STRUCTURE DU SYSTEME ETUDIE 170
E.1 Caractéristiques des fonctions de sécurité du système 170
E.2 Désignation des fonctions de sécurité dupliquées 171
E.3 Fonction de structure 172

INDEX DES FIGURES 176

INDEX DES TABLEAUX 177

Introduction générale

Les transports guidés urbains (métros, tramways, trains express urbains tels les RER–Réseaux Express Régionaux–) et non urbains (trains circulant sur le réseau ferré national) font l'objet de développements de plus en plus poussés en raison de leur qualité de transports de masse peu polluants et des indéniables avantages qu'ils procurent : diminution de l'encombrement automobile des villes, coûts de transport plus abordables face au prix croissant du carburant automobile et aux tarifs élevés des vols aériens, et gain en terme de temps de transport. Ils évoluent notamment pour assurer les performances de rapidité, pour permettre la possible circulation de trains hétérogènes (trains à grande vitesse, transports de marchandises), et pour garantir la qualité de services attendue par les usagers (confort, proximité, fréquence des trains, informations en temps réel) dont le flux ne cesse de croître. Ainsi la capacité des lignes de transport existantes, en particulier les lignes de chemin de fer qui prédominent dans les transports guidés, augmente, et la gestion et l'exploitation de ces lignes tendent à être optimisées ou renouvelées par l'emploi de nouvelles installations automatiques de contrôle-commande et de communication. Les concepteurs ont recours massivement aux technologies innovantes pour répondre à ces besoins et par la même occasion pour répondre aux contraintes économiques et aux contraintes d'interopérabilité liées à l'ouverture internationale des marchés.

Ces développements s'accompagnent d'une amélioration continue de la sécurité qui reste la préoccupation principale dans ce domaine d'activités source de risques, où les accidents peuvent engendrer d'importants dégâts sur le système et l'environnement, et causer un nombre élevé de victimes. Assurer la sécurité est d'autant plus recherché que l'occurrence d'accidents peut entraîner une perte de confiance des utilisateurs dans le système de transport dans le sens où ces événements choquent l'opinion publique qui n'accepte pas d'encourir de tels risques en toute légitimité. La sécurité consiste alors à maîtriser les risques, leur élimination totale étant illusoire. La maîtrise des risques implique d'une part, la prévision des risques, et d'autre part, la réduction de ces risques par la diminution de leur occurrence, et l'atténuation de leurs conséquences grâce à différents moyens. Ces moyens se rapportent à la mise en place de sous-systèmes de sécurité sûrs de fonctionnement inclus parmi les moyens

de gestion des risques impliquant des moyens de prévention (avant l'accident) et de protection (après l'accident) contre les risques. La sécurité peut alors être évaluée selon l'estimation du risque résiduel grâce aux méthodes et outils de la sûreté de fonctionnement, et être jugée satisfaisante ou non en comparaison de critères d'acceptation du risque définis par les autorités de transport et les normes en vigueur.

Face aux évolutions technologiques, économiques et sociales évoquées ci-dessus, et face aux performances élevées demandées, les systèmes de transport guidé deviennent de plus en plus complexes. Cette complexité rend encore plus difficile la démonstration de la sécurité qui s'appuie sur l'identification des dangers pouvant aboutir, selon des scénarios d'évolution possibles, à des événements redoutés (les accidents par exemple). Ces dangers sont envisagés aussi bien au niveau des dysfonctionnements du système complexe de transport guidé, en particulier de ses sous-systèmes de sécurité prévus lors de la conception, qu'au niveau de l'environnement d'exploitation du système. Des directives et normes de sécurité, relatives au domaine d'activités étudié [Directive 49/CE 2004] [Directive 50/CE 2004] [CENELEC 2000, 1998, 1999] imposent en outre le respect de niveaux de sécurité contraignants (sous forme de SILs–Safety Integrity Levels–), généralement attribués aux fonctions des systèmes de sécurité pour assurer ce qui est dénommé la « sécurité fonctionnelle ». A l'aide de ces niveaux de sécurité, une définition harmonisée des exigences de sécurité pour les divers constructeurs et exploitants, est certes possible. Cependant le respect des exigences de chacune des fonctions de sécurité analysées séparément, même si la satisfaction de ces exigences contribue à assurer la sécurité du système de transport guidé, ne permet pas d'évaluer la sécurité de l'ensemble du système complexe, ce dernier comportant de nombreuses interactions fonctionnelles. L'évaluation de la sécurité, face à cette complexité, nécessite une approche globale. Les travaux de recherche menés dans le cadre de cette thèse se sont appuyés sur cette considération pour adopter une démarche systémique et probabiliste ayant pour but d'évaluer la sécurité, en phase de conception, des systèmes complexes de transport guidé.

Le premier chapitre présente la science fondamentale des systèmes, la systémique, contribuant à l'étude des systèmes complexes. La démarche méthodologique préconisée par la systémique, consiste principalement à considérer un système dans sa globalité et selon la mission qu'il doit délivrer, points de vue qui sont pris en compte pour exposer les concepts et méthodes de la sûreté de fonctionnement et les fondements de la maîtrise des risques des systèmes complexes.

Le deuxième chapitre s'appuie sur une démarche de gestion des risques pour décrire et montrer comment les différents sous-systèmes de sécurité existant aujourd'hui dans le domaine des transports guidés ainsi que leurs diverses fonctionnalités, apparaissent comme des moyens de prévention et de protection contre les risques présents. Cette démarche de gestion des risques devient problématique lors de l'estimation du risque résiduel concourant à l'évaluation de la sécurité. En effet, même si les normes de sécurité comme la norme générique IEC 61508 [IEC 61508 2000] apportent différentes prescriptions liées principalement à la définition d'exigences de sécurité exprimées en terme de SILs et aux différentes modalités qui permettent leur application, la complexité des systèmes reste un frein à la mise en œuvre de la démarche de gestion des risques.

Pour entreprendre l'évaluation de la sécurité d'un système complexe de transport guidé, le troisième chapitre propose une approche d'analyse de la sécurité globale qui considère : les SILs alloués aux différentes fonctions de sécurité du système, les dépendances entre ces fonctions, la duplication de ces fonctions sur l'ensemble d'une ligne de transport, l'évolution dynamique des états des fonctions de sécurité dont les défaillances constituent des événements dangereux, et l'évolution dynamique du système sur son domaine d'exploitation. Dans un premier temps, l'aspect quantitatif lié aux SILs, source de confusion, est clairement présenté pour proposer un moyen de quantification des profils de risque liés au système, ce moyen étant basé sur ce qui est nommé la *combinaison des SILs*. Dans un deuxième temps, la modélisation des différents aspects de complexité d'un système de transport guidé est entreprise au moyen du concept de *situation d'exploitation*, apport original de ces travaux de recherche. Enfin une méthode de simulation est proposée pour mettre en œuvre dans son contexte environnemental le système modélisé.

Dans le quatrième chapitre, un système de transport guidé donné est étudié pour valider l'approche d'évaluation de la sécurité. Le fonctionnement de ce système est d'abord décrit, notamment les fonctionnalités envisagées pour assurer la sécurité. Puis la modélisation du système est effectuée selon la démarche basée sur le concept de situation d'exploitation. Les conditions de sécurité modélisées sont ensuite testées par le biais d'une maquette logicielle développée pour cette étude et qui permet la simulation de l'évolution dynamique du système dans son environnement opérationnel. Les résultats des campagnes expérimentales menées sont ensuite présentés et leur pertinence est discutée.

Le cinquième chapitre envisage plusieurs perspectives de recherche, lesquelles portent d'abord sur l'amélioration de la prise en compte des exigences de SIL, par l'intégration de contraintes supplémentaires dans leur analyse, et par la proposition d'une autre piste de quantification des profils de risque mieux adaptée aux intervalles probabilistes liés aux SILs. Des variables d'influence sur le risque sont ensuite analysées pour mener une évaluation plus approfondie de la sécurité en termes de gravité. Enfin, dans des perspectives plus larges, ces travaux projettent d'inclure les facteurs humains dans l'approche de sécurité en tentant d'apporter une démarche de quantification de l'erreur humaine associée à une tâche donnée.

Chapitre 1. Analyse systémique de la sûreté de fonctionnement et maîtrise des risques des systèmes complexes

Sommaire

INTRODUCTION 14

1.1 LA SYSTEMIQUE : SCIENCE FONDAMENTALE CONTRIBUANT A L'ETUDE DES SYSTEMES COMPLEXES 15

1.1.1 La notion de complexité des systèmes 15

1.1.2 La systémique 16

1.1.3 L'approche systémique et l'ingénierie système 17

1.2 ANALYSE DE LA SURETE DE FONCTIONNEMENT DES SYSTEMES COMPLEXES 19

1.2.1 Les concepts de la sûreté de fonctionnement 19

1.2.2 Les moyens de la sûreté de fonctionnement 21

1.2.3 Analyses qualitatives 23

1.2.3.1 Les méthodes d'analyse fonctionnelle et structurelle 23

1.2.3.2 Les méthodes d'analyse des défaillances 24

1.2.3.3 Les réseaux bayésiens 26

1.2.4 Analyses quantitatives 27

1.2.4.1 De l'analyse statique à l'analyse dynamique : approche par simulation de Monte Carlo 27

1.2.4.2 Approche bayésienne 29

1.3 MAITRISE DES RISQUES DES SYSTEMES COMPLEXES 31

1.3.1 Terminologie et base des études de sécurité 31

1.3.1.1 Définitions, caractéristiques et critères liés à la notion de danger 31

1.3.1.2 Le concept de sécurité et le concept connexe de risque 34

1.3.2 La gestion des risques des systèmes 36

1.3.2.1 Le processus de gestion des risques 36

1.3.2.2 L'acceptation du risque des systèmes 38

1.3.2.3 Les moyens de prévention et de protection contre le risque 39

1.3.3 L'évaluation du risque 40

1.3.3.1 Principes 40

1.3.3.2 Les objectifs de sécurité 41

1.4 CONCLUSION 41

Chapitre 1. Analyse systémique de la sûreté de fonctionnement et maîtrise des risques des systèmes complexes

Introduction

La conception de systèmes homme-machine en vue d'une utilisation donnée est de plus en plus difficile à maîtriser face au développement accru des technologies d'automatisation d'informatisation et de communication. En effet, les démarches d'analyse et d'intégration de ces systèmes dans leur environnement se heurtent à leur complexité intrinsèque. Dans ce contexte, le comportement des systèmes est difficilement prévisible notamment en raison des dysfonctionnements pouvant affecter aléatoirement leurs différents constituants et des erreurs commises par les opérateurs humains interagissant avec le système.

La systémique fournit une démarche méthodologique pour la conception et la maîtrise du fonctionnement des systèmes complexes. Celle-ci est exposée dans la première partie de ce chapitre après avoir défini la notion de complexité.

La sûreté de fonctionnement focalise sur l'analyse des défaillances d'un système. La deuxième partie de ce chapitre expose les concepts de cette science des défaillances et présente, dans le cadre de l'ingénierie système, les différentes techniques et méthodes qui contribuent à l'analyse de sûreté de fonctionnement des systèmes complexes.

La maîtrise des risques dont les fondements reposent sur l'approche systémique, s'attache plus particulièrement à l'analyse et la gestion des différents modes de fonctionnement ou de dysfonctionnement du système qui peuvent affecter la sécurité des biens, des personnes et de l'environnement. La dernière partie de ce chapitre en détaille les grands principes.

1.1 La systémique : science fondamentale contribuant à l'étude des systèmes complexes

1.1.1 La notion de complexité des systèmes

La complexité (du latin *complexus* signifiant *ce qui est tissé ensemble*) est une notion qui 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 de l'homme, les sciences sociales… Ces travaux sont à la base de ce qui deviendra *la systémique* [Le Moigne 1994]. 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 1990], 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. Ceci se rapporte à la notion d'**émergence** qui est résumée par Narbonne [2005] par « le tout est quelque chose de plus que la somme des parties ». Ces propriétés émergentes s'inscrivent dans trois types d'organisations [Le Moigne 1990]:

- l'*éco-organisation* (l'organisation active qui exprime le fonctionnement ouvert dans l'environnement),
- l'*auto-organisation* (l'organisation autonome du système),
- la *ré-organisation* (l'organisation évolutive du système selon des transformations dans l'espace, dans le temps, ou des transformations de forme du système).

Ces propriétés mettent en avant l'aspect dynamique du système complexe.

Reposant sur ce concept d'organisation, la *modélisation* permet d'appréhender la complexité d'un système. La complexité modélisée repose sur des représentations mentales et intelligibles du système complexe global –appelées modèles– à partir desquelles tout raisonnement devient possible. Le modèle ne représente pas la réalité du système mais il est la construction de la connaissance de cette réalité. La modélisation d'un système complexe repose sur l'utilisation de l'approche systémique.

1.1.2 La systémique

La *systémique* est une science qui est apparue à la rencontre de travaux de recherche transdisciplinaires menés principalement par L.V. Bertalanffy (1901-1972), chercheur en biologie autrichien qui proposa *la théorie générale des systèmes*, et N. Wiener (1894-1964), mathématicien américain qui fonda la science de la *cybernétique* [Narbonne 2005].

La *théorie générale des systèmes* dégage des principes explicatifs des systèmes « ouverts », selon des propriétés d'organisation et d'émergence (évoquées précédemment), à partir desquelles des phénomènes complexes pourraient être modélisés. Elle adhère au fait qu'il n'y a pas de solution unique aux problèmes rencontrés dans les systèmes ouverts.

La *cybernétique* (du mot grec *kubernetes* signifiant *le pilote d'un navire*) est la science de la communication et de la commande des systèmes vivants ou artificiels, issue de la théorie de l'information. Elle recherche non pas à définir la structure d'un système mais à comprendre son comportement en considérant les actions (fonctions ou processus) du système comme des « boîtes noires » sur lesquelles s'appliquent des entrées et des sorties, et qui, selon des contraintes environnementales, fonctionnent et évoluent dans le temps pour atteindre une finalité (bases de la dynamique des systèmes). Ainsi elle se concentre sur les interactions au sein des systèmes pouvant consister en des échanges de matières, d'énergie ou d'informations selon des interfaces de communication. Dans ces interactions, se distinguent les interactions dites de « feedback » ou bouclage, concernant la rétroaction d'informations ou le recyclage de matières ou d'énergie, caractéristiques de l'auto-organisation d'un système.

Qualifiée de théorie du système général par Le Moigne [1994] (le système devant être abordé dans son ensemble), la *systémique* et les sciences dont elle dérive, reposent sur la notion de système (du mot grec *sustêma* signifiant *ensemble cohérent*) qu'il convient de définir. De la littérature abondante sur ce sujet, la définition de De Rosnay [1975] semble être la plus

satisfaisante : « un système est un ensemble d'éléments en interaction dynamique, organisés en fonction d'un but ». La systémique s'attache à comprendre un système complexe selon :

- l'analyse globale du système plutôt que l'analyse des éléments du système pris séparément.
- la mise en évidence des interactions au sein du système, c'est-à-dire les relations existant entre les éléments du système, pris deux à deux, et celles existant entre les éléments du système et l'environnement. Ces interactions traduisent le comportement du système et sont arborescentes (relations hiérarchiques) ou rétromettantes (relations de bouclage) [Le Moigne 1994]. La complexité d'un système est en partie due à ces dernières engendrant très souvent des comportements imprévisibles.
- l'organisation du système en différentes parties qui évoluent et se transforment pour atteindre un but qui leur est propre (notion de téléologie ou téléonomie). La conjonction de ces parties apporte de nouvelles propriétés au système, dites propriétés émergentes, et permet la représentation du système en plusieurs niveaux organisationnels (sous-systèmes) dépendants les uns des autres. Le système peut alors être structuré de manière organique (relations entre ses éléments) et fonctionnelle (interactions entre ses fonctions).

Il est à noter que la communauté systémique française est représentée par l'AFSCET (Association Française de Science des Systèmes Cybernétiques Cognitifs et Techniques) et en Europe, par l'association UES (Union Européenne de Systémique) et le programme MCX (Programme Européen de Modélisation de la Complexité).

1.1.3 L'approche systémique et l'ingénierie système

L'approche systémique permet de rendre intelligible un système qualifié de complexe par la construction d'un modèle de ce système. Étant dépendantes du modélisateur, les représentations d'un modèle ne sont pas uniques. Cette opération de modélisation permet d'induire des connaissances sur un système complexe, dans l'objectif d'entreprendre des actions futures sur ce système. Elle relève de démarches méthodologiques qui s'appuient sur le raisonnement analogique (transfert de connaissances d'une discipline à une autre), le langage graphique et la simulation (expérimentation sur le modèle).

Quel que soit le système complexe considéré, Le Moigne [1990] [1994] définit une démarche de modélisation en neuf niveaux, chacun étant positionné dans un référentiel Espace-Temps-Forme, et marquant une finalité donnée pour le système global. Ainsi, pour construire

progressivement son modèle, le modélisateur peut considérer les niveaux suivants :

1. le système est passif et il est reconnaissable par ses frontières avec l'environnement,
2. le système est actif, il est alors caractérisé par des entrées et des sorties,
3. le système est actif et régulé (relations de bouclage),
4. le système s'informe, l'information faisant suite à une boucle de rétroaction,
5. le système décide de son activité,
6. le système a une mémoire des informations,
7. le système coordonne ses activités d'information, de décision, et d'opération,
8. le système est capable d'imaginer et de s'auto-organiser,
9. le système est capable de s'auto-finaliser et donc de s'adapter (modélisation de la conscience).

Concernant les processus industriels et organisationnels, l'approche systémique utilise un cadre méthodologique qu'est l'**ingénierie système** ou ingénierie par approche systémique. L'ingénierie système, mise en avant en France par l'AFIS (Association Française d'Ingénierie Système) et, de manière internationale, par l'INCOSE (International Council on Systems Engineering), est dédiée à la maîtrise des différentes étapes du cycle de vie d'un système complexe, de la conception à la mise en exploitation et au démantèlement. S'appuyant sur ce cadre méthodologique, différents auteurs [Cicotelli 1999] [Blaise, Lhoste et al. 2003] [Cauffriez, Benard et al. 2006], mettent en avant quatre aspects caractérisant la complexité des systèmes socio-techniques (ou système homme-machine) basés sur des techniques d'automatisation : les aspects fonctionnels, comportementaux, structurels et technologiques de la complexité.

Dans un but plus spécifique tel le diagnostic d'un système, la représentation des connaissances de bon fonctionnement d'un système complexe technique sont exprimées au travers d'approches multi-modèles [Lind 1994] [Chittaro, Guida et al. 1993], un modèle se rapprochant des déclinaisons de la complexité mentionnées ci-dessus. Selon ces approches, les modèles visent à exprimer les connaissances fondamentales du système (à partir d'un modèle structurel construit selon les relations entre les éléments, et un modèle comportemental construit à partir des comportements des éléments) et les connaissances d'interprétation, ces dernières permettant de donner des interprétations des connaissances fondamentales en terme de fonctions et de buts pour le système (un modèle fonctionnel et un modèle téléologique sont alors construits).

Les connaissances liées au mauvais fonctionnement d'un système nécessitent d'être également prises en compte dans les activités de l'ingénierie système. Du fait des défaillances pouvant apparaître dans un système, des comportements imprévisibles peuvent émerger et affecter les performances et la sécurité du système, des personnes et de l'environnement en interaction avec le système. Pour prévoir, évaluer, et maîtriser ces comportements, l'ingénierie système s'appuie sur les disciplines dépendantes que sont la sûreté de fonctionnement et la maîtrise des risques. Les sections suivantes y sont consacrées.

1.2 Analyse de la sûreté de fonctionnement des systèmes complexes

1.2.1 Les concepts de la sûreté de fonctionnement

Un système sujet à des défaillances internes est susceptible de se comporter de telle sorte qu'il ne puisse pas remplir les fonctions pour lesquelles il a été conçu. La sûreté de fonctionnement permet d'analyser et d'évaluer ces comportements par différents moyens en s'inscrivant nécessairement dans une démarche systémique pour supporter la complexité des systèmes. De ce point de vue, la notion de *service* délivré par un système est introduite dans [Laprie, Arlat et al. 1995] pour désigner le comportement du système par rapport à ce qu'en attend un utilisateur extérieur. S'appuyant sur cette notion de service, les auteurs définissent alors la sûreté de fonctionnement d'un système informatique, ou de manière générale, un système homme-machine par *la propriété qui permet aux utilisateurs d'un système de placer une confiance justifiée dans le service qu'il leur délivre*.

Le concept de sûreté de fonctionnement est d'abord apparu dans les domaines à hauts risques tels l'aérospatiale, l'aéronautique et le nucléaire vers le milieu du siècle dernier. Les études statistiques qui étaient alors menées, aspiraient à renforcer la sécurité des systèmes par l'amélioration de la fiabilité des équipements dont les défaillances pouvaient mener à des accidents catastrophiques. De ces études, un constat fort s'imposa : il se résume dans le fait que pour améliorer la fiabilité d'un système, il ne faut pas seulement tenir compte de son maillon le plus faible, mais de l'ensemble des composants du système en interaction [Villemeur 1988]. Ainsi sont apparues, dans les années 1960, de nouvelles techniques et méthodes comme les modèles de fiabilité prévisionnelle ou les méthodes probabilistes (telle la méthode de l'arbre de défaillances) qui, employées dès la phase de conception des systèmes, permirent de réduire de manière significative les coûts d'entretien et de maintenance liés à la phase d'exploitation. Les préoccupations concernant la rentabilité des investissements

engagés pour produire des biens et des services conduisirent à la formalisation des notions de disponibilité et de maintenabilité [Zwingelstein 1999]. La gestion de la qualité des systèmes, l'utilisation d'indicateurs de performance (tel le temps moyen de bon fonctionnement dont l'acronyme anglais *MUT–Mean Up Time–* est plus connu, le temps moyen de réparation *MTTR–Mean Time To Repair–*, etc.), la prise en compte des défaillances dues aux facteurs humains et les techniques de fiabilité logicielle liées à l'apparition de l'informatique, soulignent les efforts menés depuis des décennies pour concevoir des systèmes toujours plus sûrs.

La **fiabilité**, la **maintenabilité**, la **disponibilité**, et la **sécurité** sont les quatre paramètres fondamentaux de la sûreté de fonctionnement (qualifiés de paramètres FMDS). Ceux-ci permettent de définir les objectifs attendus d'un système et/ou d'évaluer la qualité du service délivré par un système pour cibler les points critiques à améliorer. Ils se définissent de la manière suivante [Villemeur 1988] :

- la **fiabilité** est l'aptitude d'une entité E à accomplir une fonction requise dans des conditions d'utilisation données, pendant une durée donnée. Elle s'exprime selon la probabilité *R(t)* (du terme anglais *Reliability* désignant la fiabilité) définie de la manière suivante:

$$R(t) = P\{E \text{ non défaillante sur } [0,t[\} \tag{1.1}$$

- la **maintenabilité** est l'aptitude d'une entité E à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits. Elle concerne les systèmes réparables et s'exprime selon la probabilité *M(t)* (du terme anglais *Maintainability* désignant la maintenabilité) définie de la manière suivante :

$$M(t) = P\{E \text{ est réparée sur } [0,t[\} \tag{1.2}$$

- la **disponibilité** est l'aptitude d'une entité E à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné. Elle est dépendante de la fiabilité et de la maintenabilité de l'entité, et s'exprime selon la probabilité *A(t)* (du terme anglais *Availability* désignant la disponibilité) définie de la manière suivante :

$$A(t) = P\{E \text{ non défaillante à l'instant } t\} \tag{1.3}$$

- la **sécurité** est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques. Elle est dépendante de la fiabilité,

de la disponibilité et de la maintenabilité de l'entité et s'exprime selon la probabilité *S(t)* définie de la manière suivante :

$$S(t) = P\{E\ n'ait\ aucune\ défaillance\ catastrophique\ entre\ 0\ et\ t\} \quad (1.4)$$

Du fait de l'informatisation des systèmes, de nouveaux événements critiques sont à prendre en compte telle l'intrusion de personnes malveillantes dans les systèmes informatiques. Ainsi, deux aspects concernent le paramètre sécurité : la *sécurité-innocuité*, liée à la non occurrence de conséquences catastrophiques pour l'environnement, et la *sécurité-confidentialité*, liée à la non occurrence de divulgations non autorisées des informations et au respect de l'intégrité de ces informations (notions tentant de transcrire la distinction entre les deux termes anglais *safety* et *security*) [Laprie, Arlat et al. 1995]. Dans ce mémoire, nous nous intéressons uniquement au premier aspect de la sécurité, notion fondamentale de la maîtrise des risques détaillée dans la troisième partie de ce chapitre, le second étant spécifique à l'ingénierie des logiciels.

Les concepts de la sûreté de fonctionnement peuvent être résumés et illustrés par la Figure 1.1 issue de [Desroches, Leroy et al. 2003].

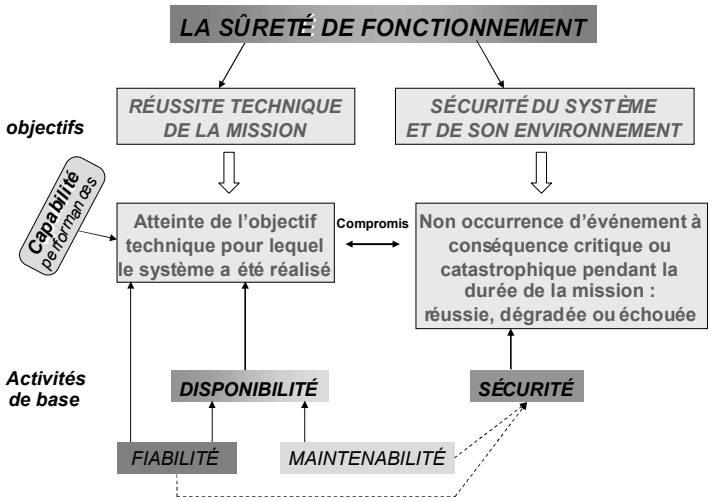


Figure 1.1 Les concepts de la sûreté de fonctionnement [Desroches, Leroy et al. 2003]

1.2.2 Les moyens de la sûreté de fonctionnement

Les techniques et méthodes actuelles, permettant le développement d'un système sûr de fonctionnement, sont ancrées dans l'ingénierie système. Elles constituent différents *moyens* appliqués à chaque phase du cycle de vie du système : des spécifications et de la conception, en passant par la réalisation et l'exploitation, jusqu'à la mise hors service et le démantèlement du système. Ces moyens agissent sur les *fautes*, les *erreurs*, et les *défaillances* (une erreur caractérise l'état du système susceptible d'entraîner une défaillance, et la faute est la cause de

l'erreur). Celles-ci rendent inacceptable le service d'un système et sont qualifiées d'*entraves* à la sûreté de fonctionnement. Les moyens de la sûreté de fonctionnement sont classés en trois catégories [Laprie, Arlat et al. 1995] :

- L'**évitement** des fautes par la **prévention** et l'**élimination** des fautes. La prévention permet d'éviter l'occurrence ou l'introduction de fautes en phase de spécification et de conception. L'élimination permet la correction des fautes par des techniques de vérification, par des techniques de tests ou par des techniques de diagnostic.
- La **prévision** des fautes. Elle permet d'estimer l'occurrence et les conséquences des fautes par des évaluations ordinales (identification et classement des défaillances) ou probabilistes.
- La **tolérance** aux fautes. Elle permet au système de fournir un service malgré les fautes, le mode de fonctionnement du système est alors qualifié de *mode dégradé*. Elle utilise des techniques de recouvrement d'erreur par reprise, où le système est ramené à un point de fonctionnement avant l'erreur ; par poursuite, où le système est amené dans un nouvel état à partir duquel il peut continuer son fonctionnement; ou par compensation, où des redondances sont utilisées.

En phase de spécification et de conception du système, les analyses de sûreté de fonctionnement cherchent à mettre en oeuvre les différents moyens exposés ci-dessus pour assurer la sûreté du système. En particulier, les analyses qualitatives s'appuient sur des analyses fonctionnelles et structurelles du système pour faire ressortir d'une part, les éléments critiques pour le fonctionnement du système, l'influence des dysfonctionnements du matériel ou du logiciel sur le système, les tests de validation à prévoir et la répartition des tâches entre l'homme et le système. D'autre part elles mettent en évidence les contraintes de conception concernant le partitionnement entre le logiciel et le matériel et les contraintes concernant l'intégration de fonctions permettant d'assurer les objectifs de sûreté [Vallée 2003].

Les analyses quantitatives se concentrent sur l'évaluation *a priori* des objectifs de sûreté également lors des phases de spécification et de conception du système. Ces analyses peuvent être *statiques*, c'est-à-dire que la structure et de la logique de fonctionnement du système sont examinées sans tenir compte de l'évolution possible du système dans le temps. Elle peuvent également être *dynamiques*, c'est-à-dire que la structure et de la logique de fonctionnement du système sont examinées en tenant compte de son évolution dans le temps et en intégrant par exemple des évolutions fonctionnelles ou structurelles appelées reconfigurations [Zwingelstein 1999] [Pasquet 1999].

Basées sur toutes les phases du cycle de vie, des techniques de type formel se placent au niveau de l'évitement de fautes. Elles sont fortement utilisées dans le développement des systèmes critiques pour la sécurité en raison de leur capacité à traiter un grand nombre d'erreurs. Lors des phases de tests, se distinguent les techniques SRE (*Software Reliability Engineering*, ou sûreté logicielle) d'origine essentiellement anglo-saxonne [Everett, Keene et al. 1998] qui concernent l'évitement et la prévision de fautes. Ces techniques, pour la plupart dédiées aux logiciels, ne sont pas développées dans ce chapitre mais sont détaillées dans les ouvrages suivants : [Peled 2001] et [Monin 2000] qui traitent de la spécification formelle, la vérification formelle et le test, [Abrial 1996] et [Habrias 2001] qui exposent la méthode formelle B, et [Musa 1998] et [Bedford et Cooke 2001] qui abordent les techniques SRE.

Les analyses qualitatives et quantitatives de la sûreté de fonctionnement vont maintenant être abordées.

1.2.3 Analyses qualitatives

1.2.3.1 Les méthodes d'analyse fonctionnelle et structurelle

Les méthodes d'analyse fonctionnelle, reprenant les spécifications du cahier des charges d'un système, permettent d'obtenir un modèle de conception, support à l'analyse prévisionnelle des défaillances d'un système. Le formalisme des méthodes d'analyse fonctionnelle (le modèle fonctionnel) donne lieu à une représentation, généralement graphique, du système à partir de ses fonctions et sous-fonctions, réalisées par des matériels spécifiques, des relations entre ces fonctions, et de la décomposition hiérarchique de ces fonctions jusqu'à un niveau suffisant d'étude. Les méthodes classiques d'analyse fonctionnelle, tirées de l'ingénierie des systèmes, telles les méthodes SADT, RELIASEP, APTE, FAST, MERISE, SA/RT et GRAFCET sont présentées dans [Zwingelstein 1995].

Les méthodes d'analyse structurelle s'appuient majoritairement sur des modèles orientés objets, ces derniers pouvant également modéliser le comportement du système par la prise en compte des interactions existant au sein du système. Le système complexe est vu, dans les modèles à objets ou modèles orientés objets, comme un ensemble d'entités ou de composants –les *objets*– reliés entre eux, et réalisant un ou des services à un niveau hiérarchique supérieur (notion de *niveaux d'abstraction*). Un objet est associé à un *état* décrit par différents attributs, et par des *opérations* permettant d'établir des relations avec d'autres objets, créant ainsi la structure du modèle à objets. Une *classe* désigne des objets de propriétés communes et

l'*instance* d'une classe est un objet construit sur le modèle de cette classe. L'ensemble des objets et classes du modèle constituent les *abstractions* des entités réelles du système. Elles permettent d'appréhender la complexité du système par l'identification des propriétés ou opérations essentielles du système tout en ignorant provisoirement le reste des informations. Des mécanismes d'abstraction (les relations d'abstractions, d'héritage, d'agrégation, d'utilisation, d'instanciation et de méta-classe) établissent les dépendances possibles entre plusieurs classes [Booch 1994]. Le comportement des objets et les dépendances qui les lient, permettent la structuration d'un système complexe. Il est à noter que le langage graphique UML (*Unified Modeling Language*, pour langage de modélisation unifié) est un langage normalisé, développé dans les années 1990 à partir de la combinaison d'autres langages orientés objets, rendant possible la formalisation des modèles à objets au travers de différents diagrammes. Les méthodes orientées objets, à base de modèles à objets, prédominent dans la conception et l'analyse des logiciels. Les objets peuvent toutefois être assimilables à des composants physiques (vannes ou capteurs par exemple) ou à des paramètres de sûreté de fonctionnement. C'est notamment le cas pour l'abstraction de « situation de travail » proposée par [Hasan 2002] pour la mise en place de la sécurité en phase de conception de systèmes industriels complexes socio-techniques.

Ces deux classes de méthodes aident à la connaissance des différentes fonctions du système et de son comportement mais ne font pas apparaître les processus ou mécanismes physiques qui peuvent mener aux défaillances du système.

1.2.3.2 Les méthodes d'analyse des défaillances

S'appuyant sur les analyses précédentes, les défaillances, les modes de défaillance (manières selon lesquelles un système peut défaillir), les conséquences des défaillances, et les scénarios causaux intégrant ces défaillances, sont mis en évidence par diverses techniques et méthodes de sûreté de fonctionnement. Les méthodes qui prédominent dans les outils d'ingénierie système font l'objet de nombreux ouvrages tels [Pagès 1980], [Villemeur 1988] [Lyonnet 2000], [Andrews et Moss 1993], [Kumamoto et Henley 1996] et [Rausand et Høyland 2004], et apparaissent depuis peu dans une norme internationale dédiée à la sûreté de fonctionnement [IEC 60300-3-1 2003] (cf. Tableau 1.1).

Des méthodes comme l'AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité), l'HAZOP (Hazard and Operability Studies) ou l'arbre des conséquences,

utilisent une démarche inductive (qualifiée d'analyse *bottom-up*) [Sourisse et Boudillon 1996], c'est-à-dire que partant d'une défaillance donnée, elles cherchent à mettre en évidence les effets sur le système étudié. Les méthodes comme l'arbre de défaillances, les graphes de Markov ou les réseaux de Petri, utilisent une démarche déductive (qualifiée d'analyse *top-down*) [Sourisse et Boudillon 1996], démarche qui cherche à mettre en évidence les causes d'une défaillance donnée. Certaines méthodes comme le diagramme de fiabilité ou la table de vérité sont mixtes.

Méthodes d'analyse	**Analyse qualitative**	**Analyse quantitative**	**Allocation d'objectifs de sûreté**
Prédiction du taux de défaillance	Possible pour l'analyse de stratégie de maintenance	Calcul du taux de défaillance et du MTTF (Mean Time To Failure) pour les composants et équipements électroniques	Applicable aux systèmes séries sans redondance
Arbre de défaillances	Combinaisons de défaillances	Calcul de la fiabilité, de la disponibilité et des contributions relatives des sous-systèmes à l'indisponibilité du système	Applicable si le comportement du système dépend peu du temps et si le système possède peu de dépendances
Arbre de conséquences	Séquences de défaillances	Calcul du taux de défaillance	Possible
Diagramme de fiabilité	Chemins de succès	Calcul de la fiabilité et de la disponibilité	Applicable si les blocs sont indépendants
Graphe de Markov	Séquences de défaillances	Calcul de la fiabilité et de la disponibilité	Applicable
Réseaux de Petri	Séquences de défaillances	(Permet la description du système pour une analyse par graphe de Markov)	Applicable
AMDEC	Effets des défaillances	Calcul du taux de défaillances et de criticité	Applicable pour les systèmes où les défaillances indépendantes sont prédominantes
HAZOP	Causes et conséquences des déviations	–	Permise
Analyse de fiabilité humaine	Impact des performances humaines sur l'exploitation du système	Calcul de probabilités d'erreur de tâches humaines	Permise
Analyse résistance-contrainte	Utilisable en tant que moyen d'évitement de fautes	Calcul de la fiabilité des composants (électro-) mécaniques	–
Table de vérité (analyse de fonction de structure)	Possible	Calcul de la fiabilité et de la disponibilité	–
Méthode de fiabilité statistique	Impact de fautes	Estimation statistique de la fiabilité avec intervalles de confiance	Possible

Tableau 1.1 Principales méthodes de sûreté de fonctionnement d'après [IEC 60300-3-1 2003]

Ces méthodes mènent également, comme le montre le Tableau 1.1, à l'évaluation quantitative des paramètres de sûreté, celle-ci étant probabiliste, et permettent l'allocation d'objectifs de sûreté de fonctionnement. Ces points font l'objet de la section 1.2.4.

1.2.3.3 Les réseaux bayésiens

Une alternative intéressante aux méthodes déductives consiste en l'utilisation de réseaux bayésiens. Les réseaux bayésiens, issus de la théorie des graphes, sont des graphes acycliques orientés. Ils sont constitués de nœuds n_i ($i=1,2,\ldots$) associés à des événements possédant un nombre fini d'états mutuellement exclusifs $\left\{ e_1^i,\ldots,e_s^i \right\}$ (en logique booléenne 'vrai' et 'faux' par exemple), et d'arcs a_{ij} indiquant les relations de causalité entre chaque nœud connecté. Les réseaux bayésiens, dans le cadre des systèmes complexes, sont particulièrement utilisés dans un but d'aide à la décision et plus précisément dans l'élaboration de stratégies de maintenance au travers du diagnostic de fautes lié à l'observation d'un état de panne du système [Maalej, Delcroix et al. 2003] [Delcroix, Piechowiak et al. 2003].

Les réseaux bayésiens peuvent représenter les relations de dépendances entre un événement redouté (la défaillance d'un système ou un accident) et les causes de cet événement de manière plus générale qu'un arbre de défaillances, par exemple, ces causes n'étant pas obligatoirement binaires (fonctionnement ou défaillance) ou connectées par des portes logiques. Les causes de l'événement redouté peuvent être regroupées en facteurs organisationnels, en facteurs humains et en facteurs techniques [Rausand et Høyland 2004] (cf. Figure 1.2).

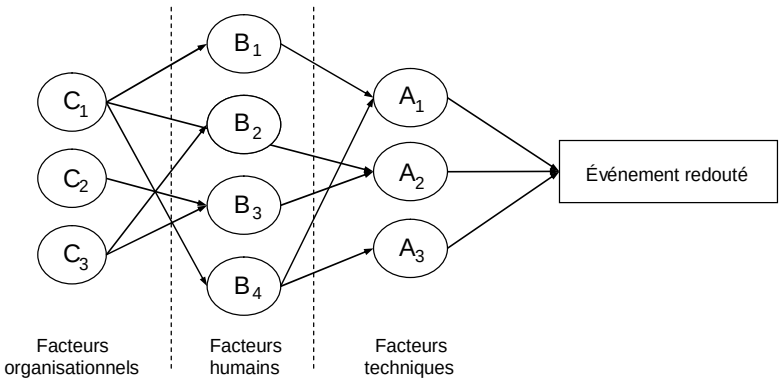


Figure 1.2 Exemple de réseau bayésien

1.2.4 Analyses quantitatives

1.2.4.1 De l'analyse statique à l'analyse dynamique : approche par simulation de Monte Carlo

La plupart des méthodes d'évaluation probabiliste de sûreté de fonctionnement des systèmes complexes focalisent sur l'évaluation analytique prévisionnelle des paramètres de fiabilité, maintenabilité et disponibilité. Cette évaluation s'effectue au travers de méthodes *statiques* telles les méthodes d'arbre de défaillances, de diagramme de fiabilité et d'arbre de conséquences, ou de méthodes *dynamiques* telle la méthode de l'espace des états [Rausand et Høyland 2004]. Cette dernière, développée pour l'analyse des processus stochastiques de type markovien (prise en compte uniquement de l'état présent indépendamment des états passés d'un système), modélise les transitions entre les différents états d'un système.

Dans l'analyse dynamique des systèmes complexes, l'utilisation de méthodes analytiques est problématique, le domaine des défaillances pouvant être difficilement exprimé ou approché par une expression mathématique. Interviennent alors les méthodes de simulation permettant la résolution numérique d'un problème de nature complexe, comme la Simulation de Monte Carlo (SMC), adaptable dans un grand nombre de cas insolubles analytiquement.

Élaborée par J.V. Newmann and S. Ulam après la seconde guerre mondiale, ère du développement des calculateurs, la SMC a été introduite en physique de la matière pour la résolution rapide et approchée de problèmes mathématiques de type probabiliste ou aléatoire tels le mouvement thermique des particules, ou de type déterministe tels le calcul d'intégrales multidimensionnelles. Reposant d'une manière générale, sur la génération de nombres aléatoires à partir de lois de probabilité, la SMC permet de simuler l'évolution temporelle d'un système complexe à partir d'un modèle stochastique dans lequel les paramètres liés aux composants de ce système sont connus. Pour cela, des événements stochastiques correspondant aux changements d'état du système (appelés transitions), sont tirés aléatoirement à partir des distributions de probabilité des composants du système (les distributions sont dites échantillonnées). Ces états peuvent être des états de pannes ou différents états liés aux modes de fonctionnement des composants. Une évolution possible du système sur une durée de vie T_M, correspond à un scénario ou une *histoire.*

Le principe d'une SMC consiste à générer plusieurs histoires du système de manière à évaluer statistiquement (par estimation de la moyenne) les paramètres probabilistes de sûreté de fonctionnement selon les informations d'état du système à chaque instant de la simulation, pour l'ensemble des évolutions obtenues. Le choix du nombre d'histoires dépend à la fois de l'incertitude statistique ou de l'erreur maximale voulue dans les résultats, et du temps de calcul dédié à l'obtention de ces résultats. Lorsqu'un nombre important d'histoires contient peu de transitions, comprenant de ce fait peu d'information (cas des systèmes très fiables), des techniques de *réduction de la variance* [Rubinstein 1981] [Fishman 1996] [Marseguerra et Zio 2002], permettent de se substituer aux techniques de la SMC dite *analogique* (ou analogue).

Les algorithmes d'une SMC analogique, pour la simulation de l'évolution dynamique des systèmes et l'évaluation de leurs critères de sûreté de fonctionnement, sont basés sur les modèles mathématiques dérivés de la théorie du transport de particules neutres [Dubi 2000] [Labeau 2000] (cf. Annexe A). Ils se concentrent sur l'évaluation d'un taux de réaction transposable à l'équation (1.5) dans le domaine de la dynamique des systèmes.

$$G(t) = \sum_{k \in \Gamma} \int_0^t \psi_k(\tau).R_k(t-\tau).d\tau \tag{1.5}$$

$G(t)$ est l'expression générale, à l'instant *t*, de la probabilité associée aux critères de sûreté tels la défiabilité ou l'indisponibilité, $\psi_k(\tau)$ est la densité de probabilité d'entrée du système dans un état défaillant *k* au temps τ, encore appelée densité de collision, et Γ est l'ensemble des états défaillants du système. La fonction $R_k(t-\tau)$ est un estimateur de *G(t)* égal à l'unité dans le cas de l'évaluation de la défiabilité, ou désigne la probabilité que le système ne sorte pas de l'état *k* avant *t* sachant qu'il y est entré à $\tau < t$, dans le cas de l'indisponibilité [Marseguerra et Zio 2002]. Une SMC analogique permet l'évaluation de $G(t)$ par la génération de *N* histoires – selon deux approches : l'approche directe et l'approche indirecte [Labeau et Zio 2002] – à partir desquelles des compteurs relèvent les états défaillants, sur chaque pas de temps de la durée de mission du système T_M discrétisée.

L'approche par SMC permet, en outre, de traiter l'aspect dynamique de certains types de modélisation. Les réseaux de Petri stochastiques développés par le LAPS (Laboratoire d'Automatique, Productique et Signal) de Bordeaux, intègrent des lois d'évolutions pour les différents composants du système modélisé, et se servent de l'approche directe pour mettre en

œuvre leur simulation [Dutuit, Châtelet et al. 1997] [Signoret et Chabot 2002]. L'approche indirecte a été récemment adaptée à la méthode DDET (Discret Dynamic Event Trees, méthodes des arbres d'événements dynamiques discrets). Utilisée dans le domaine nucléaire, la méthode DDET est basée sur des arbres d'événements continus rendus discrets par la discrétisation de la variable de temps [Labeau, Smidts, et al. 2000]. Elle prend en compte, en plus des états du système, les processus physiques liés à ce système, multipliant ainsi les scénarios possibles. La combinaison des deux méthodes a donné naissance à la méthode germanique MCDET (Monte Carlo Dynamic Event Tree) permettant le traitement probabiliste de la méthode initiale [Hofer, Kloos et al. 2002].

1.2.4.2 Approche bayésienne

Dans un réseau bayésien représentant une structure causale entre divers états ou événements, chacun des nœuds d'un réseau est associé à une table de probabilités conditionnelles P_i codant la distribution d'une variable aléatoire V_i conditionnellement aux nœuds parents. Cette structure est associée à une représentation probabiliste permettant de calculer, à partir d'algorithmes d'inférence liés à l'ordonnancement des réseaux, des probabilités conditionnelles d'événements [Becker et Naïm 1999].

Le mécanisme d'inférence bayésienne utilise, comme son nom l'indique, le théorème de Bayes énoncé dans l'équation (1.6) (ou théorème de probabilité des causes), où *P(A/B)* (probabilité de A sachant B) est une probabilité conditionnelle *a posteriori* qui représente le degré de croyance en l'événement A sachant l'observation de l'événement *B* ; *P(A)* étant le degré de croyance *a priori* avant l'observation de *B*. Le terme *P(B/A)*, pour un *B* connu, est appelée la fonction de vraisemblance de *A* et *P(B)* est la probabilité *a priori* de *B* [Procaccia et Suhner 2003]. Lorsque plusieurs événements indépendants $\{A_1,\ldots A_n\}$ sont la cause de l'événement observé *B*, le théorème de Bayes s'énonce selon l'équation (1.7).

$$P(A/B) = \frac{P(A) \times P(B/A)}{P(B)} \tag{1.6}$$

$$P(A_i/B) = \frac{P(A_i) \times P(B/A_i)}{\sum_j P(A_j) \times P(B/A_j)} \tag{1.7}$$

Des travaux récents du CRAN (Centre de Recherche en Automatique de Nancy) [Weber, Cerisier et al. 2005], ont permis d'intégrer dans les graphes une dimension temporelle menant

à la création de réseaux bayésiens dynamiques (RBD) et pouvant servir de support à l'évaluation probabiliste de graphes de Markov. Les RBD intègrent des arcs temporels qui associent deux nœuds représentant la même variable à deux pas de temps différents. La Figure 1.3 illustre ce principe avec un exemple simple de graphe de Markov pour un composant ayant un taux de défaillance λ et un taux de réparation μ (un exemple de réseau bayésien associé à un arbre de défaillances est également donné). Dans cette figure, les nœuds A_{k-1} et A_k traduisant la notion de temporalité, représentent la variable aléatoire V_A, qui est la durée de fonctionnement du composant A aux pas de temps *k-1* et *k*. La même variable considérée à deux pas de temps différents permet l'implémentation d'une distribution de probabilité associée et traduit les transitions d'états. A chaque itération, la distribution de probabilité de $V_A(k-1)$ est utilisée comme une nouvelle observation de $V_A(k)$. En remarque, le nœud A_k est conditionnellement indépendant de l'état passé, ce qui traduit la propriété des systèmes markoviens. Des tables de probabilités conditionnelles sont associées à chaque nœud et comprennent, dans le cas d'une étude de sûreté de fonctionnement d'un système, les relations déterministes (causales) ou probabilistes liées aux défaillances du système.

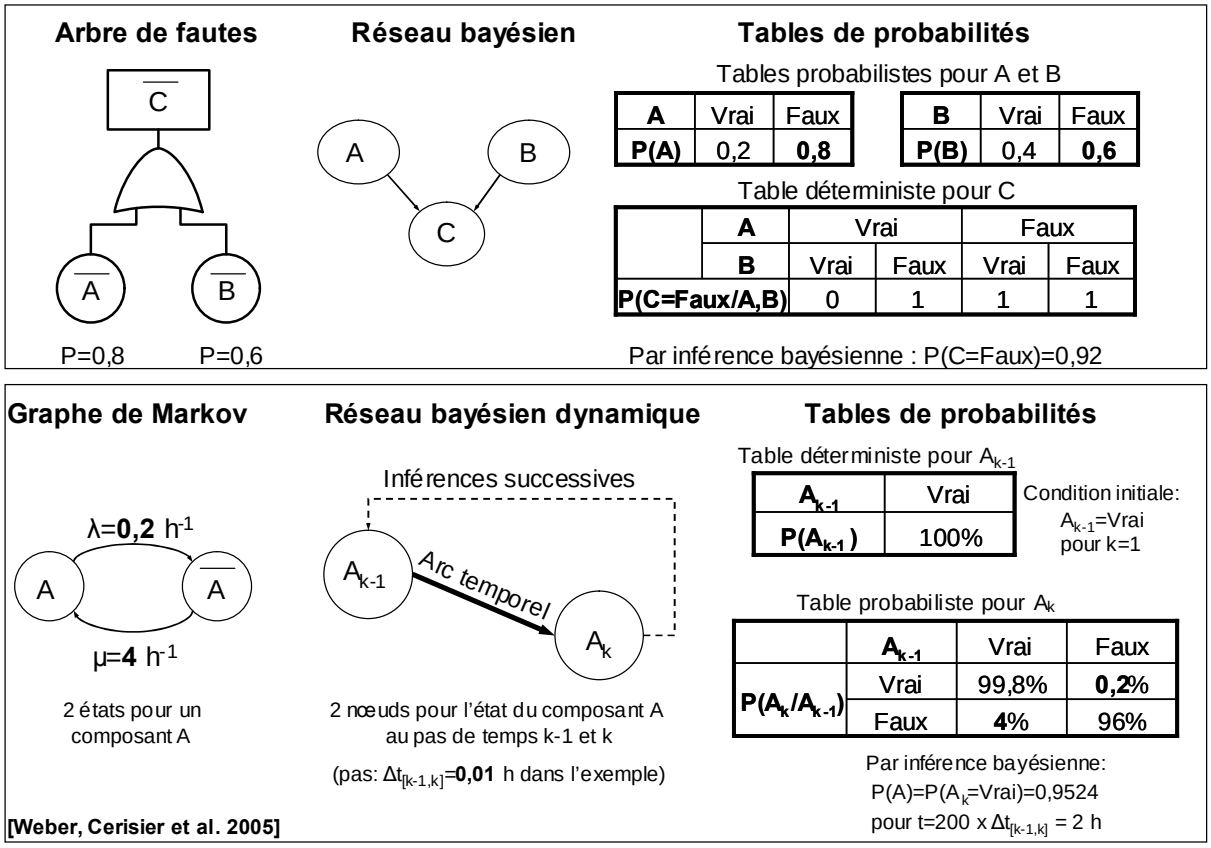


Figure 1.3 Équivalence entre quelques méthodes de sûreté de fonctionnement et les réseaux bayésiens

Les différentes approches consacrées à l'analyse de sûreté de fonctionnement des systèmes qui viennent d'être présentées dans la deuxième partie de ce chapitre, se situent au cœur des projets menés par l'association européenne ESReDA (European Safety, Reliability and Data Association), et par l'association internationale ESRA (European Safety and Reliability Association), celles-ci ayant pour but de promouvoir la recherche autour de la thématique de la sûreté de fonctionnement. La maîtrise des risques est liée à cette thématique dans le sens où elle s'attache à l'évaluation et au maintien de la sécurité d'un système en s'appuyant sur les méthodes de sûreté de fonctionnement. L'institut français IMdRSdF (Institut de Maîtrise des Risques et de Sûreté de Fonctionnement) regroupe d'ailleurs ces deux disciplines dans ses activités, et compte de nombreux industriels et laboratoires de recherche parmi ses membres, dont le LAMIH. La maîtrise des risques, qui se consacre aux comportements prévisibles et imprévisibles concernant la sécurité (ces derniers étant sources de risques), est exposée dans la partie suivante.

1.3 Maîtrise des risques des systèmes complexes

1.3.1 Terminologie et base des études de sécurité

1.3.1.1 Définitions, caractéristiques et critères liés à la notion de danger

Le *danger* désigne une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction du système ou d'une partie du système), à l'environnement, ou aux personnes. 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 [Desroches 1995] [IEC 61508 2000]. Les dangers liés à un système sont soit inhérents au fonctionnement ou au dysfonctionnement du système, soit extérieurs au système. Dans ce dernier cas, ils peuvent provenir de conditions naturelles difficiles, ou d'actions humaines externes contre le système (telles les actions d'imprudence, de malveillance ou de terrorisme). La nature d'un danger se rapporte à un état appréhendable par nos sens (exemple : la chaleur, un environnement gazeux) ou non (exemple : le comportement fautif d'une personne). De nombreux termes sont employés, selon différents auteurs ou normes, autour de la notion de danger et la rendent ambiguë. Le

Tableau 1.2 en présente une liste non exhaustive et propose, pour plus de clarté, une classification de ces différents termes en quatre catégories : l'événement source du danger, l'état de danger, l'événement résultant du danger, et l'état résultant du danger.

L'**événement source** du danger est une défaillance ou une dérive du système par rapport à ses conditions d'exploitation normales ou un événement extérieur qui conduit à un danger, ou plus précisément, à une situation dangereuse déterminée. L'évolution de cette situation aboutit potentiellement, selon un processus particulier, à un **événement résultant** qui aurait dû être évité. D'après [Kumamoto et Henley 1996], la situation dangereuse est similaire à la notion de *scénario* (également appelé séquence), dit scénario causal ou scénario d'accident, menant à un événement redouté. Ce dernier conduit à des **états résultants** du danger qui correspondent aux conséquences directes et indirectes du danger, évoquées dans la définition du danger ci-dessus.

1. Événement source		- Événement initiateur - Événement d'origine - Événement déclencheur - Événement dangereux
2. <u>Danger</u> (État de danger)	**Interne**	- Situation dangereuse (du système) - Activité dangereuse - Nuisance
	Externe	- Situation dangereuse (de l'environnement) - Phénomène dangereux - Menace, situation menaçante - Comportement dévié - Agression externe
3. Événement résultant		- Événement redouté - Événement potentiellement redouté - Événement indésiré - Événement inacceptable - Accident
4. État résultant		- Dommage - Conséquence néfaste - Effet redouté - Préjudice

Tableau 1.2 Classification des termes employés autour de la notion de danger

Le modèle du « nœud papillon » développé lors du projet ARAMIS[1] [Chevreau, Wibo et al. 2005] [De Dianous et Fiévez 2005] schématise les scénarios d'accident menant à un événement redouté (ER) qui se propagent ensuite en conséquences de degrés divers (cf. Figure 1.4). L'ER est l'événement central du modèle (explosion, collision entre deux véhicules, par exemple) dont l'occurrence dépend de l'enchaînement ou la combinaison d'événements dangereux internes liés aux dysfonctionnements du système (défaillance d'un

[1] Accidental Risk Assessment Methodology for Industries in the framework of SEVESO II directive (projet de recherche mené sur la période 2002-2004 et coordonné par l'INERIS - Institut National de l'Environnement Industriel et des Risques - en relation avec la Direction Générale de la Recherche de la Commission Européenne)

équipement, par exemple) ou d'événements dangereux externes liés à l'environnement (vibrations, par exemple).

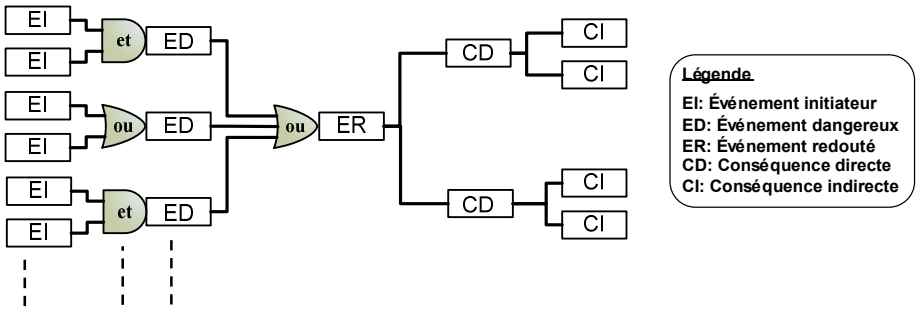


Figure 1.4 Modèle du « nœud papillon » [Chevreau, Wibo et al. 2005][De Dianous et Fiévez 2005]

Il est à noter que la notion d'événement dangereux est le plus souvent réduite à l'acception plus courante de danger bien que la définition ci-dessus introduise le danger en terme d'état et non d'événement (dans la suite, « danger » sera plus commodément employé pour « événement dangereux »). Les événements initiateurs, quant à eux, apparaissent comme étant des événements (défaillances, erreurs humaines, par exemple) menant à un événement dangereux.

Un autre modèle employé pour la schématisation des scénarios d'accident repose sur la méthode du diagramme de causes-conséquences menant à plusieurs ER [Villemeur 1988]. Le modèle focalise non pas sur un ER particulier, comme précédemment, mais sur différents dispositifs, dits de sécurité, pouvant empêcher l'occurrence d'ER distincts (cf. Figure 1.5).

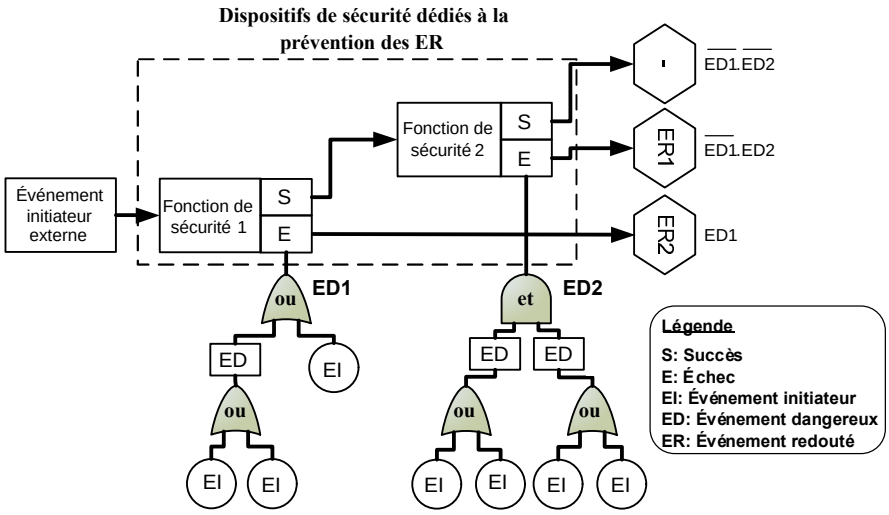


Figure 1.5 Modèle du diagramme causes-conséquences [Villemeur 1988]

La partie supérieure du modèle reprend le formalisme de la méthode de l'arbre de conséquences. Celui-ci débute par un événement initiateur externe qui peut progresser en plusieurs enchaînements possibles (les scénarios) constitués d'actions réussies ou non des dispositifs de sécurité, appelées succès ou échecs. Les échecs désignent en fait des événements dangereux (ED) issus d'autres événements dangereux ou d'événements initiateurs, et les succès, explicités par la notation de complémentarité $\overline{ED}$, désignent des actions de prévention empêchant l'évolution d'un événement initiateur en événement redouté. Dans ce cas, le scénario atteint un état sûr.

La partie inférieure du modèle reprend le formalisme de l'arbre de défaillances. Celui-ci décrit les causes élémentaires des dysfonctionnements des dispositifs de sécurité. Les causes élémentaires sont classifiées, selon le modèle de Embrey de la Figure 1.6 [Embrey 1992], en trois catégories : les causes liées aux erreurs humaines, aux défaillances matérielles ou logicielles, et les causes externes provenant de l'environnement d'exploitation du système. La base du modèle met en avant l'influence de l'organisation humaine et de la gestion des risques sur les accidents, la gestion du risque étant détaillée dans la suite.

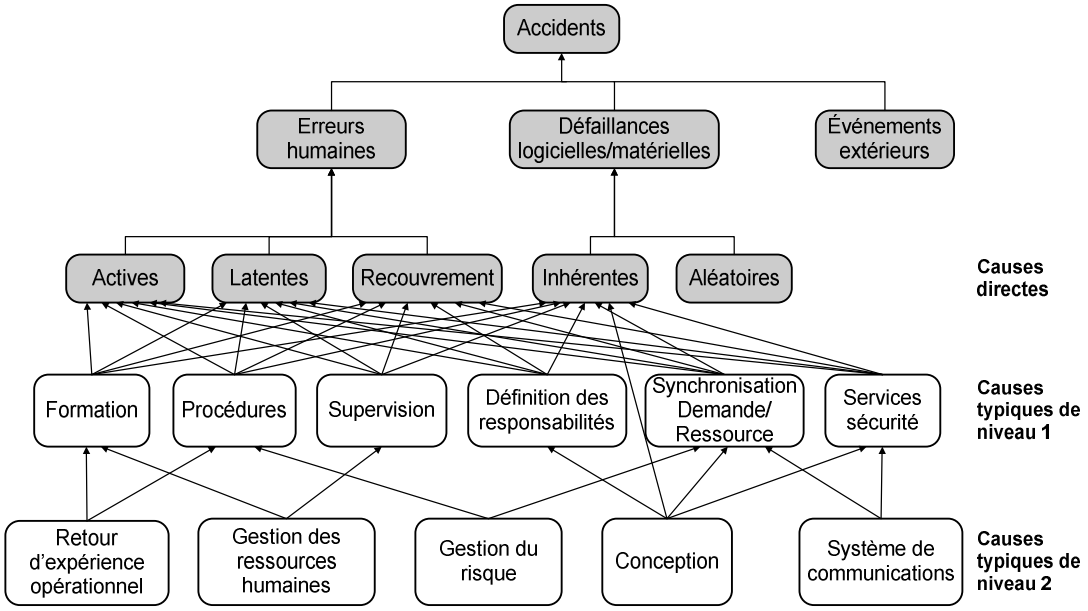


Figure 1.6 Modèle générique de Embrey classifiant les causes d'un accident [Embrey 1992]

1.3.1.2 Le concept de sécurité et le concept connexe de risque

Dans le domaine de la maîtrise des risques, le concept de sécurité concerne la sécurité-innocuité [Laprie, Arlat et al. 1995], définie au paragraphe 1.2.1. Dans [Desroches, Leroy et

al. 2003] il est précisé que la sécurité concerne *la non-occurrence d'événements pouvant diminuer ou porter atteinte à l'intégrité du système et de son environnement, pendant toute la durée de l'activité du système, que celle-ci soit réussie, dégradée ou ait échouée*. Garantir la sécurité consiste à mettre en œuvre des moyens évitant l'apparition de dangers, ceux-ci pouvant mener à des événements redoutés tels des accidents. La perception, par la société, des dommages potentiels liés à une situation dangereuse, se rapporte à la notion de *risque*. La sécurité s'énonce alors par l'*absence de risque inacceptable*, définition qui est celle de la norme générique de sécurité IEC 61508 [2000].

Qualitativement, le risque se caractérise par :

- l'ampleur des dommages, suite à un événement redouté, selon un critère de gravité, le plus souvent traduit par des termes comme catastrophique, critique, marginal, mineur, insignifiant. Ce critère tient compte de l'appréciation des conséquences en terme de pertes humaines (décès, blessures, ou invalidités) ou en termes économiques avec par exemple des coûts liés à une reconstruction, à une dégradation ou une perte d'exploitation (ou échec de la mission du système). Les conséquences sont éventuellement considérées au travers de leur impact médiatique ou juridique.
- le caractère incertain lié à l'apparition d'un événement redouté provoquant le dommage, depuis une situation dangereuse déterminée. Il peut s'exprimer par des termes comme fréquent, probable, occasionnel, rare, improbable, invraisemblable.

Quantitativement, le risque s'énonce par la mesure du danger au travers de la combinaison de la probabilité d'occurrence P d'un événement redouté ER et de la gravité de ses conséquences G, permettant d'obtenir un diagramme occurrence-gravité. A noter que la combinaison de l'occurrence et de la gravité d'un risque se rapporte à la *criticité* de ce risque.

Lors de l'analyse des dangers d'un système complexe, plusieurs événements ER_i sont à prendre en compte. Kumamoto et Henley [1996] présentent une approche du risque multicritères, en introduisant le principe de *profil de risque* pour définir les alternatives de risque (scénarios). Le risque se définit alors de manière ensembliste par l'union de plusieurs profils de risque (cf. équation (1.8)) indiquant le fait que, selon différentes conditions, le système peut générer plusieurs événements redoutés. Un profil de risque i comporte un scénario causal SC_i désignant à la fois, des conditions particulières (combinaisons ou/et

interactions d'événements) menant à un événement redouté, et la propagation de cet événement en dommages de gravité G_i (cf. équation (1.9)). Le profil de risque intègre également un facteur important pour la gestion des risques : la taille de la population affectée par l'événement redouté, impliquant les notions de *risque individuel* (dans ce cas, le risque est généralement exprimé en terme de fréquence de décès par an et par individu) et de *risque collectif* (dans ce cas, le risque se rapporte à un nombre de décès fonction de l'événement redouté). Cette formulation du risque fournit des informations utiles basées sur le déroulement de scénarios causaux, la vraisemblance selon laquelle ils aboutissent à un événement redouté, et l'identification et l'étendue de leurs conséquences, permettant au décideur de proposer des mesures de réduction du risque selon la situation.

$$risque = \{profil\ de\ risque\ i \mid i = 1,...,n\} \tag{1.8}$$

$$Profil\ de\ risque\ i = (V_i, ER_i, G_i, SC_i, P_i) \tag{1.9}$$

<u>Critères d'un profil de risque:</u>

- V vraisemblance (probabilité, fréquence)
- ER événement redouté
- G gravité des conséquences
- SC scénario causal
- P population affectée

L'assurance de la sécurité d'un système implique la mise en place d'un processus de gestion des risques. Il permet d'une part, d'intervenir de manière prévisionnelle sur la conception du système dangereux analysé (analyse *a priori*), et d'autre part, de maîtriser les risques liés à la phase d'exploitation, en maintenant les objectifs de sécurité alloués au système.

1.3.2 La gestion des risques des systèmes

1.3.2.1 Le processus de gestion des risques

Régie par des principes d'assurance qualité, la gestion des risques examine les différentes phases du cycle de vie d'un système pour évaluer, implémenter, documenter et contrôler les conditions de sécurité [Planchette 2002].

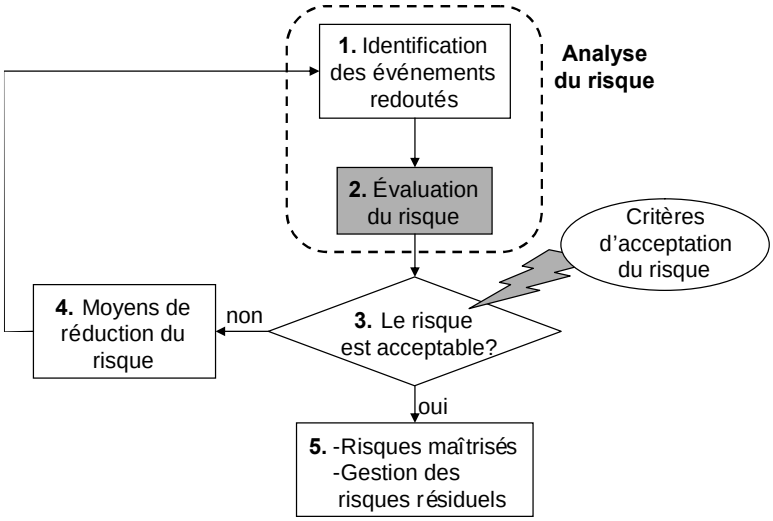


Figure 1.7 Processus de gestion des risques

Elle s'articule autour des activités présentées dans l'organigramme de la Figure 1.7 dont les quatre premières se rapportent à des analyses effectuées en phase de conception du système. Celles-ci sont les suivantes :

1. Cette activité correspond à la recherche des événements redoutés *a priori* susceptibles de se produire durant la mission du système, en tenant compte des conditions prévues d'exploitation.
2. L'évaluation du risque se concentre sur l'obtention des profils de risque. Elle s'appuie généralement sur les techniques probabilistes issues des méthodes de sûreté de fonctionnement exposées dans la deuxième partie du chapitre. Elle est importante car elle conditionne la sécurité du système, sécurité qui est autant que possible maintenue dans le temps grâce à la dernière étape du processus de gestion des risques.
3. À ce stade, le processus de gestion du risque arrive à un nœud de décision s'appuyant sur les résultats de l'activité précédente d'évaluation du risque. Les différents profils de risque établis pour le système global sont comparés à un critère d'acceptation du risque défini (cf. paragraphe 1.3.2.2). Lors de l'inadéquation des profils de risque au critère d'acceptation, des moyens contre le risque sont exigés et mis en place durant la quatrième étape. Les premières étapes sont alors réexaminées ou complétées. Lorsque le risque, dit résiduel, est acceptable (l'état de non risque étant illusoire), la gestion du risque demeure en étape 5.
4. Cette activité repose sur la proposition de différentes alternatives pour contrôler et réduire le risque notamment par des moyens de prévention et de protection des accidents (cf. paragraphe 1.3.2.3).

5. La maîtrise des risques résiduels instaure une traçabilité des actions et événements (retour d'expérience) lors de l'exploitation et de la maintenance. Elle préconise également une surveillance des dispositifs de sécurité vis-à-vis de leurs défaillances et des déviations humaines, appelées franchissements de barrières, pouvant les affecter [Polet 2002]. Par l'utilisation d'inspections, d'indicateurs, et de tableaux de bord mesurant les tendances de ces indicateurs [Planchette 2002], elle permet d'éviter toute dérive et d'anticiper les événements précurseurs de dangers. Cette activité aide à garder le risque à un niveau acceptable durant l'exploitation du système.

Les paragraphes suivants se focalisent sur les activités 3 et 4 du processus de gestion des risques. La deuxième étape d'évaluation du risque, activité pivot de ce processus, est ensuite abordée.

1.3.2.2 L'acceptation du risque des systèmes

L'acceptation du risque est une notion qui est établie par la législation. Les autorités imposent des critères qui permettent aux décideurs de qualifier le risque évalué comme étant acceptable ou inacceptable. Ces critères utilisent les statistiques d'incidents ou d'accidents subis par des systèmes similaires au système analysé (risque *a posteriori*) et le risque provenant des événements naturels (inondations, tremblements de terre, maladies) en tant que bornes supérieures pour les risques liés au système. Ils considèrent également les risques connus et tolérés par l'opinion publique selon le secteur d'activité. Par exemple, un accident d'avion causant une centaine de victimes bouleversera beaucoup plus la population que plusieurs accidents automobiles, sur une période d'un an, causant plusieurs milliers de morts. Leur mise en place dénote cependant une certaine part de subjectivité.

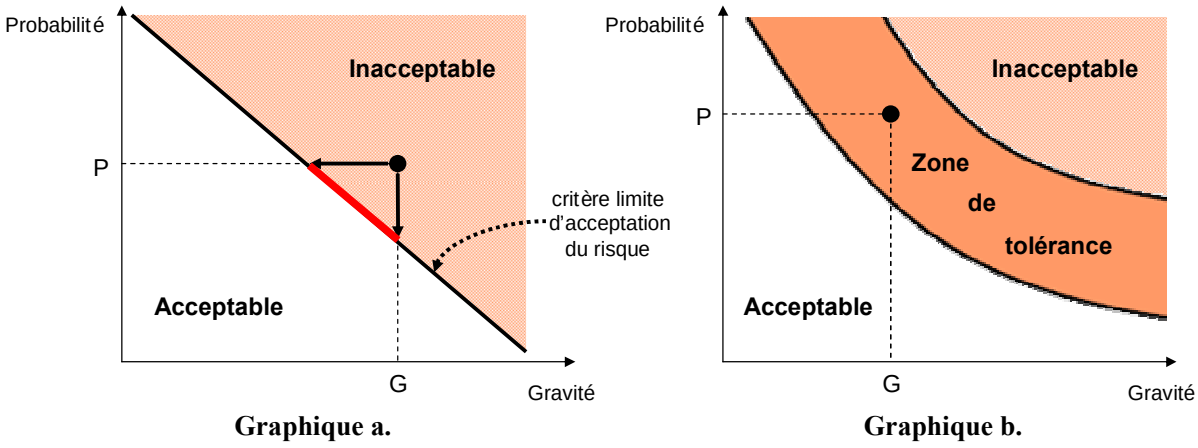


Figure 1.8 Diagrammes illustrant des principes d'acceptation du risque

Un premier principe d'acceptation du risque rencontré concerne l'établissement d'une limite dans un plan occurrence-gravité, déterminant une zone d'acceptation et une zone de rejet du risque (cf. Figure 1.8.a.). Ce principe traduit le fait que la probabilité d'un accident est inversement proportionnelle à la gravité de ses conséquences [Bedford et Cooke 2001]. Un second principe, se basant sur le premier, introduit une zone de tolérance au risque (cf. Figure 1.8.b.). Lorsque le risque initial d'un événement redouté, caractérisé par le point de coordonnées (G,P), est situé dans cette zone, il est toléré si toutes les mesures possibles de réduction du risque ne permettent pas d'atteindre la zone d'acceptabilité. Une autre raison, souvent d'ordre économique, peut justifier cette tolérance. En effet, si les moyens de réduction du risque sont disproportionnés par rapport à l'amélioration du risque obtenue, le risque appartenant à cette zone sera, dans ces conditions, laissé tel quel. Dans tous les cas, le risque toléré demande des procédures de contrôle adaptées [Desroches, Leroy et al. 2003].

Lorsqu'un risque est qualifié d'inacceptable, plusieurs alternatives sont possibles : soit diminuer la probabilité de l'événement redouté (possible par les moyens de prévention), soit diminuer la gravité (possible par les moyens de protection). Une combinaison de ces mesures est également possible, permettant alors de franchir la limite d'acceptation du risque, selon le segment mis en évidence sur la Figure 1.8.a., vers la zone d'acceptabilité. Après avoir détaillé l'étape d'acceptation du risque du processus de gestion des risques, l'étape de réduction des risques est exposée.

1.3.2.3 Les moyens de prévention et de protection contre le risque

La **prévention** des accidents potentiels porte sur l'élimination des dangers ou sur la diminution de l'occurrence d'événements redoutés soit en améliorant la sûreté de fonctionnement des dispositifs opérationnels de contrôle (meilleure fiabilité, disponibilité ou redondance des composants), soit en implantant des moyens empêchant l'apparition ou la propagation des dangers en accident (systèmes de sécurité, procédures, barrières).

La **protection** se rapporte, lors de l'échec des moyens de prévention, à l'atténuation des conséquences d'un accident par des moyens limitant au maximum les dommages (tels les systèmes de secours, les procédures d'urgences, le confinement). A noter que les moyens de protection hors site, extérieurs aux systèmes, sont appelés moyens de sauvegarde [Desroches 1995].

Lorsque les moyens de prévention et de protection se succèdent en série, la réduction du risque est qualifiée de « défense en profondeur ». Les moyens de réduction des risques peuvent être illustrés par le modèle de Cauffriez [2005] qui expose différents niveaux de sûreté des installations automatisées. Ces niveaux représentent des moyens pouvant être mis en œuvre contre les risques issus d'un système dont les activités (le processus physique) sont contrôlées par le système d'automatisation (cf. Figure 1.9). Ces moyens permettent de contrôler le risque résiduel dans le temps et d'établir un profil de risque global acceptable pour le système.

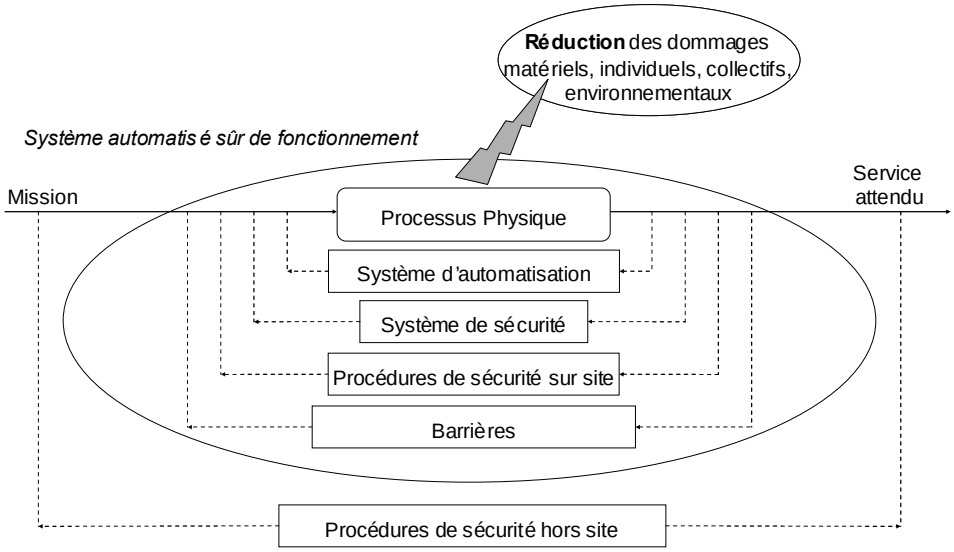


Figure 1.9 Différents niveaux de sûreté des installations automatisées [Cauffriez 2005]

La section suivante est dédiée à l'étape clé de la gestion des risques en raison de son incidence sur les décisions de conception concernant la sécurité : l'évaluation du risque.

1.3.3 L'évaluation du risque

1.3.3.1 Principes

Les méthodes d'évaluation du risque cherchent à décrire et/ou quantifier le risque. Elles focalisent d'une part sur l'identification des dangers externes et internes à l'aide, le plus souvent, de méthodes comme l'APD, l'AMDEC ou l'HAZOP, guidées par le jugement d'experts et le retour d'expérience. Au préalable, les différentes caractéristiques du système analysé (frontières du système, services délivrés à partir de la réalisation de fonctions spécifiées, conditions d'utilisation, propriétés des composants) sont nécessairement bien définies pour permettre une identification des dangers de manière la plus exhaustive possible.

D'autre part, les divers enchaînements des événements dangereux sont recherchés et représentés au travers de séquences causales menant aux ER (événements redoutés identifiés dans la première étape de la gestion des risques). Les méthodes employées, s'appuyant sur des arbres de conséquences et des arbres de défaillances, ont précédemment été évoquées lors de la définition des scénarios. A partir des informations provenant de ces analyses, les études qui suivent se concentrent sur l'obtention de la probabilité d'occurrence *a priori* des ER, dès la phase de conception du système à risque. L'activité d'évaluation du risque se rapporte donc essentiellement à une évaluation probabiliste du risque (dénommée par l'abréviation EPR) basée sur la quantification probabiliste des scénarios.

Les moyens envisagés pour réduire les risques estimés non acceptables, sont par ailleurs associés à des objectifs de sécurité que l'évaluation du risque cherche à démontrer.

1.3.3.2 Les objectifs de sécurité

Les objectifs de sécurité sont des objectifs intermédiaires attribués aux systèmes de prévention et de protection contre le risque pour satisfaire les critères d'acceptation du risque. Ils permettent de spécifier les attentes aussi bien à l'échelle sous-système 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 au 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 Henley 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].

1.4 Conclusion

Ce chapitre a souligné la nécessité d'utiliser les approches de la systémique pour appréhender la complexité grandissante des systèmes. En fournissant les concepts théoriques pour l'analyse du comportement d'un système complexe, elles contribuent à leur compréhension. Cette considération s'applique nécessairement aux études de sûreté de fonctionnement et de maîtrise des risques qui examinent les systèmes complexes homme-machine en intégrant leurs défaillances potentielles. Les défaillances humaines et techniques qui apparaissent au sein de

ces systèmes, mènent à des comportements difficilement prévisibles qui doivent pourtant être évités ou maîtrisés.

Le premier point abordé dans ce chapitre se concentre sur la définition de la notion de complexité et sur le rôle de la systémique dans l'analyse des systèmes complexes. L'ingénierie système qui fournit un cadre méthodologique à l'analyse des systèmes homme-machine est également évoquée.

La sûreté de fonctionnement, ses concepts, ses moyens et ses méthodes sont ensuite présentés sous l'angle de la systémique. Ainsi les méthodes qualitatives de sûreté de fonctionnement permettent une analyse fonctionnelle et structurelle des systèmes. Les méthodes quantitatives, quant à elles, rendent possible l'évaluation des critères FMDS (Fiabilité, Maintenabilité, Disponibilité, et Sécurité) pour justifier de l'atteinte ou non des objectifs de sûreté de fonctionnement.

Enfin la maîtrise des risques, qui se concentre sur l'évaluation et le maintien de la sécurité d'un système, est exposée. Les études menées dans cette discipline tiennent compte de l'environnement du système, source de perturbations.

En conclusion, la modélisation des comportements de fonctionnement et de dysfonctionnement des systèmes complexes, selon une approche systémique, est à privilégier et à envisager dès la conception des systèmes. Cette approche intègre l'ensemble des interactions qui peuvent exister dans un système, celui-ci évoluant dans un environnement particulier. Ces caractéristiques sont à considérer pour l'étude et l'évaluation de la sécurité des systèmes de transport guidé, objets de nos travaux de recherche. Le deuxième chapitre s'attache à décrire les différents moyens de sécurité actuels mis en œuvre dans les systèmes de transport guidé et explique la problématique d'évaluation de la sécurité de ces systèmes.

Chapitre 2. La problématique de l'évaluation de la sécurité dès la conception d'un système complexe de transport guidé

Sommaire

INTRODUCTION 44
2.1 LES RISQUES LIES A L'EXPLOITATION DES SYSTEMES DE TRANSPORT GUIDE 45
2.1.1 Les risques génériques 45
2.1.2 Les risques pouvant être atténués par les systèmes de transport guidé 48
2.1.2.1 Les risques liés à la circulation des trains 48
2.1.2.2 Les risques liés au matériel 49
2.1.2.3 Les risques liés aux opérateurs 49
2.2 LES MOYENS DE REDUCTION DES RISQUES EXISTANT DANS LE DOMAINE DES TRANSPORTS GUIDES 50
2.2.1 Les moyens de prévention des risques 50
2.2.1.1 Gestion des risques liés à la circulation des trains : principe de la signalisation 50
2.2.1.2 Gestion des risques liés au matériel 55
2.2.1.3 Gestion des risques liés aux opérateurs 56
2.2.2 Les moyens de protection contre le risque 56
2.3 L'EVALUATION ET L'ACCEPTABILITE DES RISQUES GENERES PAR UN SYSTEME DE TRANSPORT GUIDE 57
2.3.1 Contexte législatif et normatif de la sécurité des systèmes de transport guidé européens 57
2.3.2 Principes d'acceptation du risque 58
2.3.3 Le concept de niveau d'intégrité de sécurité (SIL) 59
2.3.4 L'analyse des risques centrée sur les SILs 62
2.3.5 Les méthodes d'allocation des SILs aux fonctions de sécurité 63
2.3.5.1 Les méthodes quantitatives 63
2.3.5.2 Les méthodes qualitatives 66
2.4 DISCUSSION 68
2.5 CONCLUSION 69

Chapitre 2. La problématique de l'évaluation de la sécurité dès la conception d'un système complexe de transport guidé

Introduction

Dans les systèmes de transport guidé, la sécurité est assurée par l'utilisation de divers systèmes qui, étant testés et éprouvés efficacement depuis plusieurs années, sont considérés comme garants de la sécurité du système de transport dans son ensemble. Les critères de conception de ces systèmes de sécurité ont d'ailleurs fait l'objet de nombreuses normes qui prescrivent précisément, en regard des différentes technologies employées, leurs conditions de conception et de test pour attester de leur caractère sécuritaire [Schäbe 2002]. Même si cette approche basée sur l'expérience réduit les accidents, elle ne permet pas de garantir que le niveau de sécurité du système global est suffisant, celui-ci reposant sur les systèmes de sécurité évoqués, opérant conjointement contre les risques. La mise en oeuvre d'un processus de gestion des risques appliqué aux systèmes de transport guidé, comme celui exposé au premier chapitre, s'avère nécessaire.

La première partie de ce chapitre porte sur l'activité initiale du processus de gestion des risques. Elle vise à *identifier les différents événements redoutés* associés aux risques pouvant exister lors de l'exploitation des systèmes de transport guidé, c'est-à-dire les différents types accidents pouvant survenir.

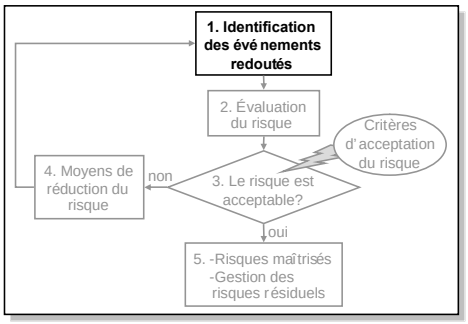
La deuxième partie de ce chapitre détaille les *moyens de réduction des risques* envisagés dans la gestion des risques de ces systèmes. La norme générique de sécurité IEC 61508 [IEC 61508 2000] relative aux systèmes E/E/PE (Électrique/Électronique/Électronique Programmable) qualifie par les termes « sécurité fonctionnelle » le fonctionnement de chaque sous-système assurant la sécurité du système global. Elle se rapporte aux activités d'*évaluation du risque* et de *prise de décision* vis-à-vis des profils de risque obtenus. Elle gouverne la sécurité fonctionnelle des systèmes complexes de transport guidé où des objectifs de sécurité exprimés

en terme de SIL (Safety Integrity Level) sont employés pour aider à la mise en œuvre de ces deux activités [CENELEC 2000, 1998, 1999], celles-ci étant particulièrement difficiles à entreprendre dans le cas des systèmes complexes de transport guidé.

La troisième partie du chapitre expose les activités d'évaluation et prise de décision centrées sur le concept de SIL (la dernière activité du processus de gestion des risques relative à la gestion des risques résiduels n'est pas traitée, cette dernière sortant du cadre de ce chapitre). Ce concept sera défini et les méthodes existantes d'allocation des SILs aux fonctions de sécurité seront présentées.

La quatrième partie de ce chapitre examine l'intérêt de mettre en œuvre une démarche systémique d'évaluation de la sécurité basée sur les SILs. Cette démarche s'appuie sur les techniques et méthodes de sûreté de fonctionnement et de maîtrise des risques exposées au chapitre précédent, celles-ci gouvernant les études de sécurité des systèmes homme-machine.

2.1 Les risques liés à l'exploitation des systèmes de transport guidé[2]



2.1.1 Les risques génériques

Les risques existant dans un système de transport guidé peuvent affecter soit un unique individu (risque individuel), soit plusieurs personnes (risque collectif), soit le système (les trains et les infrastructures liées aux voies de circulation), soit l'environnement. Une classification de ces risques a été proposée dans [Hadj-Mabrouk, Stuparu et al. 1998]. Celle-ci distingue trois catégories de risques, plus précisément trois catégories d'accidents: *les accidents utilisateur, les accidents système et les accidents utilisateur/système*. Cette classification peut être complétée avec la catégorie *accident environnement/système*. La Figure 2.1 détaille les différents accidents observés dans le domaine des transports guidés, classés selon les catégories ci-dessus.

[2] Pour plus de détails relatifs à la culture des systèmes de transports ferroviaires, les sites Internet suivants, de l'encyclopédie libre Wikipédia, sont recommandés : http://fr.wikipedia.org/wiki/Portail:Ferrovip%C3%A9dia ou http://en.wikipedia.org/wiki/Category:Rail_transport

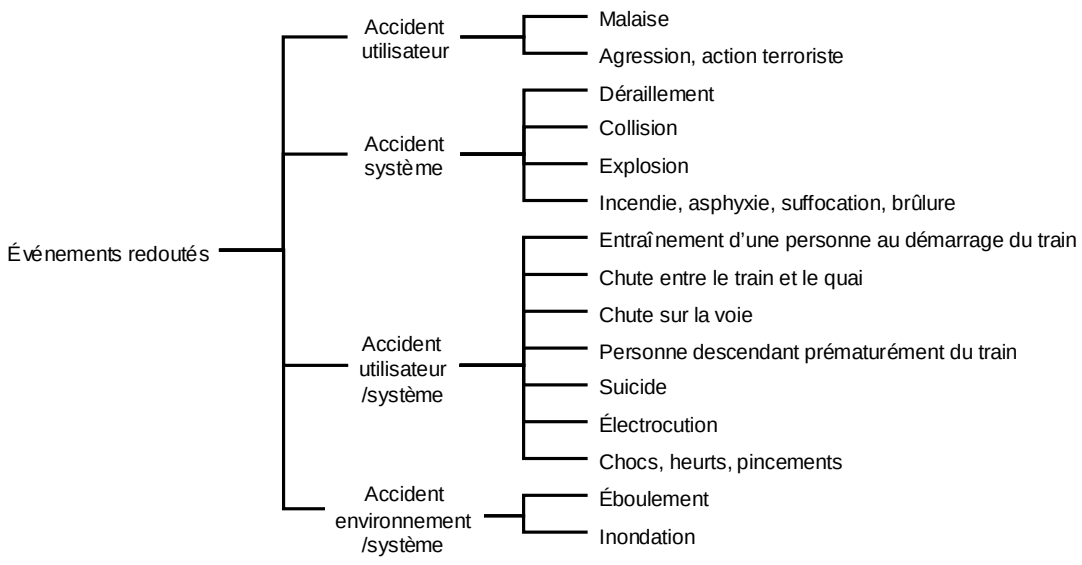


Figure 2.1 Classification des événements redoutés existant dans le domaine des transports guidés, adaptée de [Hadj-Mabrouk, Stuparu et al. 1998]

Les quatre catégories de la Figure 2.1 se décrivent comme suit :

- *Les accidents utilisateur* : Ils sont associés aux dommages causés à un ou plusieurs usagers situés au sein du système alors qu'aucun problème de fonctionnement du système ne soit survenu, et qu'aucune action de cet ou ces usagers n'ait été constatée. Ils regroupent les malaises (lors d'une bousculade, par exemple) et les agressions ou les actions terroristes. Ces risques ne peuvent majoritairement pas être réduits.

- *Les accidents système* : Ils sont associés aux dommages causés au système et aux usagers ou personnels lors d'un accident initié par le système lui-même. Sont classés dans cette catégorie les déraillements, les collisions et les incendies (lors du transport de marchandises dangereuses ou de surchauffe matérielle, par exemple). Ces accidents sont issus soit de défaillances physiques (défaillance d'un équipement, par exemple), soit de défaillances liées au sous-système logiciel (mauvaise décision calculée, mauvaises informations transférées, par exemple), soit d'erreurs commises par des opérateurs intervenant dans le système lors de l'exploitation ou la maintenance.

- *Les accidents utilisateur/système* : Ils sont associés aux dommages causés à une ou plusieurs personnes situées au sein du système, lors d'une action effectuée par cet ou ces usagers durant le fonctionnement normal du système. Cette action est soit volontaire (descente prématurée du train, suicide, par exemple), soit involontaire (chute, pincement, par exemple). L'utilisateur est initiateur du dommage et il est le seul à même d'éviter le risque par un comportement raisonnable et prudent.

- *Les accidents environnement/système* : Ils sont associés aux dommages causés au système et aux usagers lors de conditions environnementales dites de catastrophes naturelles. Ces risques sont réduits pour les usagers, selon une gestion post-accident optimisée (plan d'évacuation, par exemple), mais pas pour le système qui peut subir de nombreux dégâts.

L'ensemble de ces risques dépend du type de transport guidé considéré. En effet les risques considérés pour le transport de voyageurs ne sont pas perçus de la même manière que les risques engendrés par le transport de marchandises [Rodriguez 2004]. Les uns sont, pour la plupart, des risques humains, les autres sont des risques matériels qui peuvent être humains dans le cas du transport de marchandises dangereuses pouvant affecter la population alentour.

Ces risques dépendent également du type de réseaux de transport sur lesquels se font les circulations. Les différents réseaux de transport et leurs principaux facteurs d'influence sur le risque sont les suivants:

- Le *réseau à grande vitesse* où circulent, en Europe, des trains comme le TGV–Train à Grande Vitesse– (France), le Thalys (France, Belgique, Allemagne), l'Eurostar (France, Angleterre, Belgique), l'ICE –Inter City Express– (Allemagne), et le Pendolino (Italie). Sur ces réseaux, les trains circulent à des vitesses commerciales pouvant dépasser les 300 km/h. Ces vitesses élevées posent des problèmes pour l'anticipation des dangers extérieurs par les conducteurs et pour l'arrêt des trains qui demande une distance de freinage importante. Elles nécessitent des infrastructures et équipements adaptés comme, par exemple, l'absence d'interaction avec le trafic routier (pas de passages à niveau), des barrières de deux mètres autour des voies empêchant l'entrée d'un animal ou d'un homme dans la zone de circulation, un tracé comportant des courbures larges, un équipement de signalisation embarqué en cabine étant donné l'impossibilité de percevoir les signaux extérieurs [Fremaux et Noé 2002].

- Le *réseau conventionnel* où circulent des wagons (transport de marchandises) ou des voitures (transport de voyageurs) à des vitesses commerciales plus modérées, de l'ordre des vitesses observées dans le trafic routier. Les matériels roulants circulant sur ces réseaux sont qualifiés de « lourds » et nécessitent des distances de freinage relativement grandes. Ils interagissent avec le réseau routier au travers des passages à niveau qui sont des infrastructures supplémentaires sources de risques.

- Le *réseau urbain et suburbain* où circulent les métropolitains (métro), les RER –Réseau Express Régional– et les tramways, qui englobent une grande part des transports en

commun (les autobus complétant cet ensemble). La vitesse autorisée sur ces réseaux est plus faible que sur les réseaux précédents et les véhicules y circulant sont plus légers ; la distance de freinage est donc plus petite. Ce réseau fait cependant transiter un flux de personnes très dense sur un maillage moins étendu que les réseaux précédents et plus serré. Les accidents éventuels peuvent donc causer de nombreux dommages humains mais également matériels en raison de la quasi-totalité du parcours des trains qui, particulièrement dans le cas des métros, se fait en tunnel.

Les risques existant dans les transports guidés ont été présentés de manière générique selon la classification de la Figure 2.1. Nous nous focalisons dans la suite de ce chapitre sur les risques de la catégorie « accident système », ces risques pouvant être atténués par les systèmes de sécurité du système de transport en raison de leur caractère intrinsèque.

2.1.2 Les risques pouvant être atténués par les systèmes de transport guidé

2.1.2.1 Les risques liés à la circulation des trains

Une grande partie des fonctions de sécurité implantées dans les systèmes de transport guidé a pour objectif de pallier les risques liés à la circulation des trains. Ces risques se rapportent principalement aux déraillements et aux collisions. Les premiers sont liés à une survitesse, à un rail cassé, à une surchauffe au niveau des essieux (risques pouvant être réduits par un système de sécurité) ou à un obstacle sur la voie (risque détectable ou non suivant les équipements utilisés). Les seconds sont plus compliqués à gérer en raison des différentes situations provoquant divers types de collisions:

- la collision par mauvais sens de marche ou collision «nez-à-nez » : elle concerne deux trains sur la même voie dont l'un se dirige vers le premier dû à une erreur d'itinéraire l'orientant dans le mauvais sens de marche. Cette situation mène à la collision frontale qui est évitable avec une gestion correcte des itinéraires.
- la collision par rattrapage : elle concerne le rattrapage d'un train par un autre situé sur la même voie, dans le même sens de marche et ayant une vitesse plus élevée. Cette situation est évitable en imposant une distance d'arrêt suffisante entre les trains.
- la collision par « prise en écharpe » : elle concerne la collision à une intersection de voies entre un train qui s'engage sur une nouvelle voie et un autre train arrivant sur cette voie. Cette situation mène à une collision latérale. Ce risque est géré par les systèmes de sécurité supervisant l'établissement des itinéraires.

- La collision par dérive: elle concerne le mouvement d'un train normalement immobilisé sur une voie inclinée mais qui, suite à un problème de freins, se déplace vers un autre train en amont ou en aval.
- La collision avec des obstacles fixes : elle concerne la collision d'un train avec un obstacle permanent (contre un butoir, par exemple) ou non permanent (contre un autre véhicule stationné en fin de voie, un véhicule automobile à un passage à niveau, un élément de l'infrastructure positionné de sorte qu'il se trouve dans le gabarit des trains, par exemple).

Ces risques sont dépendants des risques liés au matériel et des risques relatifs aux opérateurs. Ceux-ci sont décrits ci-dessous.

2.1.2.2 Les risques liés au matériel

Les risques liés au matériel sont relatifs à :

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

2.1.2.3 Les risques liés aux opérateurs

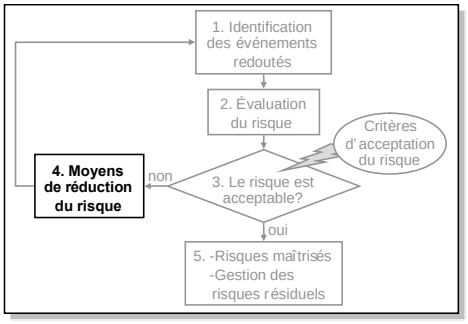
Des opérateurs humains interviennent dans les systèmes de transport guidé en tant qu'agents de maintenance, agents de régulation et agents de conduite. Les conducteurs accomplissent différentes tâches de conduite selon le niveau d'automatisation du système d'exploitation (exploitation manuelle, exploitation assistée par un système automatisé d'aide à la conduite). Ils peuvent être amenés à commettre des erreurs telles un non respect des signaux affichés (franchissement non autorisé d'un signal dit fermé, par exemple), le dépassement de la vitesse autorisée, ou le non respect d'une procédure. Les risques liés aux opérateurs sont mis en avant dans [Hadj-Mabrouk, Hadj-Mabrouk et al. 2001]. Cependant la plupart des erreurs humaines

sont contrôlées par des systèmes de sécurité qui s'opposent aux actions humaines contraires à la sécurité. L'analyse et le contrôle de l'erreur humaine dans les systèmes homme-machine ne sont pas développés dans ce chapitre. L'ouvrage de Vanderhaegen [2003] apporte de nombreux éléments à ce sujet.

D'autres risques non liés à une erreur peuvent provenir d'un trouble physique de l'opérateur de conduite, comme par exemple un malaise ou un arrêt cardiaque. Ceux-ci sont pris en compte dans les moyens de réduction des risques des systèmes de transport guidé exposés dans la deuxième partie de ce chapitre.

La quasi-totalité des risques liés à l'opérateur humain sont gérés par des *moyens de prévention du risque*, première alternative de réduction du risque évitant ou empêchant l'occurrence d'un accident. Les *moyens de protection contre le risque*, comme seconde alternative de réduction du risque, interviennent une fois l'accident survenu. Ces moyens de réduction du risque sont exposés ci-après dans le cadre des transports guidés.

2.2 Les moyens de réduction des risques existant dans le domaine des transports guidés



2.2.1 Les moyens de prévention des risques

2.2.1.1 Gestion des risques liés à la circulation des trains : principe de la signalisation

La norme EN 50129 [CENELEC 1999] définit le système de signalisation, sous-système du système de transport guidé global, comme étant un *type particulier de système utilisé dans le domaine ferroviaire pour commander, contrôler et protéger l'exploitation des trains*. De manière générale, la signalisation est un principe lié à la sécurité des transports guidés qui se rapporte à :

- un ensemble d'équipements de haute fiabilité, répartis sur les trains et les voies, permettant le contrôle et la commande de la circulation des trains ;
- et un ensemble de règles et de procédures, acquises en formation et appliquées par les opérateurs, en fonction des informations fournies par les équipements de signalisation ;

ceci dans le but de garantir la sécurité du système de transport en évitant tout accident lors de la circulation des trains.

La fonction fondamentale de la signalisation consiste à interdire la présence de deux trains au même endroit et au même moment. Elle repose sur la gestion des itinéraires des trains pour éviter tout conflit de trajectoire, et sur l'établissement d'une distance de sécurité suffisante entre les trains pour garantir, devant chacun d'entre-eux, un espace continuellement dégagé leur permettant si nécessaire de s'arrêter. Pour cela, différents systèmes de signalisation ont été conçus sur les dernières décennies du fait, notamment, de l'évolution des technologies, comme le développement de l'informatique. Bien que différents, ils se décomposent tous en deux sous-systèmes principaux (cf. Figure 2.2): le sous-système bord embarqué dans les différents trains, et le sous-système sol déployé tout le long de la ligne de transport et relié aux postes de commande et de régulation supervisant les itinéraires [Berbineau 2001].

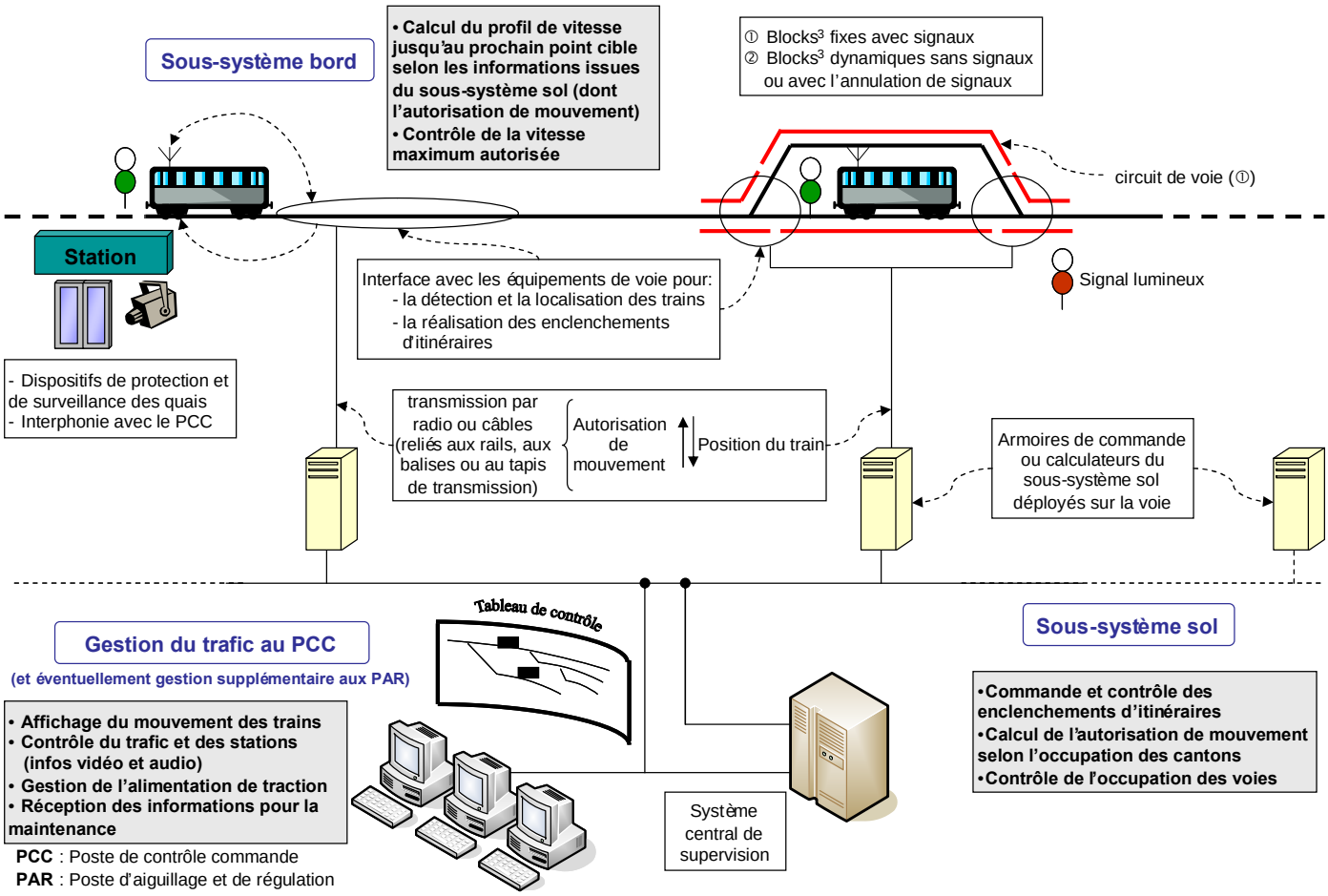


Figure 2.2 Architecture générale d'un système de signalisation

[3] Le terme *block* (de l'anglais *to block*, fermer) désigne un canton.

Le fonctionnement des sous-systèmes bord et sol peut être caractérisé par deux principes: le **cantonnement** et les **enclenchements d'itinéraires**.

a) Le cantonnement

Afin de maintenir une distance de sécurité suffisante entre les trains, pour éviter le rattrapage d'un train par un autre, l'espacement entre trains est géré par un principe de cantonnement. Celui-ci impose la présence d'un unique train sur une section de voie appelée canton. L'ensemble d'une ligne de transport est ainsi découpé en plusieurs cantons dont la longueur dépend de la géométrie de la ligne et de la densité du trafic. Une section inoccupée (appelée zone de chevauchement, section tampon ou *overlap*) peut également être imposée entre deux trains, comme dans le cas de la circulation des métros parisiens.

L'élément de base permettant la détermination de l'occupation d'une section est le *circuit de voie* qui est un circuit électrique formé d'un émetteur et d'un récepteur reliés aux rails de la section. Lors du passage d'un train, un court-circuit créé par les essieux et les roues, indique la présence d'un train sur cette section. Ces circuits permettent également de détecter un rail cassé, de vérifier l'intégrité d'un train (i.e. la présence de l'ensemble des éléments constituant le train) et de transférer aux trains, via les essieux, des informations sous forme de signaux ayant une fréquence modulée comme des données de limitation de vitesse.

Chaque circuit de voie associé à un canton est délimité par des signaux lumineux, dit *signaux d'espacement*, qui interdisent automatiquement l'entrée d'un train dans un canton occupé. Un circuit de voie associé à un signal lumineux désignant son état d'occupation (généralement un signal rouge, dit fermé, représente un circuit de voie occupé, et un signal vert, dit ouvert, représente un circuit de voie inoccupé) constituent un *block automatique lumineux*.

L'apparition de nouvelles technologies telles les technologies d'informatisation et de communication (avec notamment l'emploi des ondes radio) [Berbineau 2001] tendent à faire évoluer le principe du cantonnement qui s'appuie à la base sur des sections de voie fixes. L'idée est d'utiliser des *cantons mobiles* [IEC 60050-821 1998] [Fransson 2001], sortes de zones logiques créées dynamiquement selon la connaissance de la position exacte des trains (cf. b)*i*) concernant la localisation des trains). Ils permettent de laisser une distance de sécurité variable entre chaque train, celle-ci s'approchant de la distance de sécurité minimale qu'est la distance de freinage. Le système MAGGALY (Métro Automatique à Grand Gabarit de l'Agglomération LYonnaise) est basé sur ce principe des cantons mobiles.

Le but des cantons mobiles est de réduire l'intervalle entre les trains mais aussi, de réduire les équipements déployés au sol et *a fortiori* les pannes de ces équipements. En effet, avec ce principe, les signaux au sol et les circuits de voie peuvent être supprimés et remplacés par des indications affichées sur le pupitre de contrôle d'un train, appelé Cabsignal (pour signalisation cabine).

La convergence ou le croisement de plusieurs voies peuvent de surcroît mener à une collision frontale ou latérale entre deux trains franchissant l'intersection. Des contraintes de parcours doivent alors être imposées aux trains. Celles-ci sont gérées par le principe de l'enclenchement d'itinéraires détaillé ci-dessous.

b) Les enclenchements d'itinéraires

L'enclenchement d'itinéraires désigne le processus visant à protéger le système de transport des itinéraires conflictuels aux intersections du réseau de transport [Duquenne 2003]. Ce processus nécessite de connaître : *i)* la localisation de chaque train et *ii)* les informations sur leur parcours (notamment les limites des parcours). Il nécessite également, avant le passage d'une jonction par un train, que les aiguilles des appareils de voie (ou aiguillages) rencontrées, soient positionnées correctement et verrouillées dans cette position jusqu'à ce que le train ait fini son parcours, et que les différents signaux lumineux gérant la jonction, dit *signaux de manœuvre*, soient configurés de telle sorte qu'un et un seul train franchisse cette jonction. L'ensemble des équipements vérifiant les informations de parcours des différents trains et configurant les dispositifs de voie pour les différents itinéraires, se rapporte au système d'enclenchement (la dénomination « enclenchement » désigne souvent le système d'enclenchement et non le processus d'enclenchement). L'enclenchement est géré par des opérateurs depuis des postes d'aiguillage locaux à l'aide de systèmes d'enclenchement mécaniques ou électriques. Il peut aussi être automatisé et géré par des calculateurs numériques intégrés au système sol. La centralisation possible de ces derniers permet le contrôle et la commande des enclenchements à distance.

i) La localisation d'un train est possible grâce aux circuits de voie comme exposé précédemment. Elle est imprécise puisque le train a une position indéterminée sur la section de voie occupée. Pour affiner la localisation, des balises peuvent être implantées sur la voie. Celles-ci ont également pour fonction de transmettre une position de référence (position

absolue) au système bord qui calcule ensuite sa position en fonction de ce repère (position relative) selon la distance qu'il parcourt (obtenue grâce aux informations issues d'un odomètre ou d'une roue phonique, par exemple) et/ou grâce à la position du train qui le précède (à l'aide d'un radar, par exemple). Dans ce cas, les circuits de voie deviennent inutiles. Ils peuvent cependant être conservés pour attester de l'intégrité des trains étant donné que seule la motrice possède les équipements dédiés à la localisation ; si une voiture s'en détache, la motrice ne décèle pas ce problème et ce convoi demeure non détectable (dans les systèmes futurs comme le ERTMS/ETCS niveau 3, le système bord possèdera la fonction de vérification d'intégrité).

ii) Dans les systèmes les plus récents (cf. annexe B), les informations de parcours sont transmises aux trains par divers moyens (par les rails, par balises, par boucles ponctuelles, par tapis de transmission ou par radio) qu'ils soient proches d'une intersection ou non. Ces informations sont appelées *autorisation de mouvement* et interfèrent avec l'enclenchement [UGTMS D9 2004]. Une autorisation de mouvement contient des indications sur le trajet futur d'un train, à savoir:

- la distance qu'il doit parcourir jusqu'à une position cible fonction de l'occupation des cantons par les autres trains. La suite du trajet n'est pas encore prévue après ce point. Le point cible suivant est transmis au fur et à mesure du mouvement du train vers la cible actuelle (transmission continue par rails, par tapis de transmission ou par radio) ou transmis au point cible suivant (transmission ponctuelle par balise).
- la vitesse qu'il devra avoir à cette position cible. Connaissant la prochaine vitesse au point cible donné, le système bord est capable de calculer un profil de vitesse optimisé lui permettant de ralentir un minimum. Il a également pour fonction de contrôler si ce profil de vitesse est respecté par le conducteur, selon les différentes informations de vitesse mesurées par divers capteurs intégrés au train (ceci est valable pour les systèmes qui ne sont pas entièrement automatisés, i.e. sans conducteur). Dans le cas contraire un freinage d'urgence est déclenché.

Ces informations d'autorisation de mouvement sont établies en fonction des caractéristiques des voies (paramètres locaux de restriction de vitesse, de pente, position des jonctions…), et de la performance des trains (longueur, accélération, décélération…), et sont mises à jour selon la progression des trains sur le réseau de transport. En résumé, une autorisation de mouvement permet la réservation d'un itinéraire affecté à un et un seul train, itinéraire qui est

libéré après le passage du train. L'itinéraire est soit constitué de cantons réservés, soit mis à jour dynamiquement en fournissant des points cibles au train.

En complément à cette section, l'annexe B présente différents types de systèmes de signalisation existant. Elle s'étend sur les propriétés et fonctions de systèmes récents comme le système ERTMS (European Railway Traffic Management System), concernant les réseaux conventionnels ou grande vitesse, ou le système SACEM (Système d'Aide à la Conduite à l'Exploitation et à la Maintenance), concernant les réseaux urbains.

2.2.1.2 Gestion des risques liés au matériel

La gestion des risques liés au matériel repose sur l'efficacité des opérations de maintenance et, de plus en plus, sur l'utilisation de systèmes de diagnostic ou d'aide à la maintenance. Ceux-ci, embarqués à l'intérieur des trains, permettent de guider l'opérateur de maintenance dans sa tâche de réparation. L'emploi de ces systèmes s'explique par la difficulté croissante à maintenir les dispositifs de contrôle et de commande des systèmes de transport qui deviennent de plus en plus complexes, notamment du fait de l'utilisation de l'électronique et de l'informatique.

Un système de diagnostic consiste en un certain nombre de calculateurs embarqués tout au long d'un train (dans la motrice et dans les différentes voitures) et reliés entre eux par un réseau informatique. Les calculateurs reçoivent des informations (fonctionnement normal ou alarmes déclenchées par le dépassement d'un seuil donné) provenant des dispositifs qui supervisent les différentes parties du train. Dans les systèmes récents, les informations reçues sont analysées en temps réel pour éventuellement déduire l'origine des problèmes détectés [Cau 2003]. La surveillance porte, par exemple, sur les boîtes d'essieux, les freins, les différents signaux échangés, le statut des portes ou de la climatisation, etc., par le biais de données issues de divers capteurs. Le réseau informatique transfère les informations de bon ou de mauvais fonctionnement au conducteur puis au poste de contrôle-commande, par l'intermédiaire du système de transmission train-sol, pour compléter la base de données de diagnostic du système sol.

2.2.1.3 Gestion des risques liés aux opérateurs

La plupart des erreurs humaines sont contrôlées par les équipements de sécurité liés au système de signalisation, comme le sous-système d'enclenchement qui empêche l'établissement d'itinéraires conflictuels. De même, lorsqu'un train enregistre une survitesse ou le franchissement d'un signal fermé, suite à une action erronée du conducteur (ces deux types d'erreurs humaines sont les plus observées dans les transports guidés [Andersen 1999]), le train est ramené dans un état sûr grâce au déclenchement automatique d'un arrêt d'urgence par les sous-systèmes bord de sécurité ayant détecté les actions contraires à la sécurité. Il s'agit de l'application des principes de *sécurité intrinsèque* visant à obtenir une configuration sûre du système à partir de comportements de dysfonctionnement identifiés et connus *a priori* [Bied-Charreton 1998].

Hormis l'erreur humaine, les autres risques liés aux opérateurs, comme indiqué au paragraphe 2.1.2.3, concernent les troubles physiques de l'opérateur de conduite pouvant l'empêcher d'assurer le pilotage du système. Pour cela, les trains disposent d'un dispositif qualifié de veille automatique ou d'« homme mort » (correspondant à une pédale ou un commutateur proche du pupitre de commande) qui doit être activé par le conducteur toutes les trente secondes, lui permettant ainsi d'indiquer au système qu'il est bien conscient. Au terme de ces trente secondes, si le dispositif n'a pas été activé, un signal est émis, puis l'arrêt d'urgence est déclenché.

Les moyens de prévention des risques, exposés ci-dessus, sont associés à des moyens de protection contre les risques qu'il convient d'évoquer. Ces moyens sont vitaux en cas d'accident, même si l'occurrence d'un tel événement est évitée au maximum grâce au contrôle continu des déplacements des trains mis en place en prévention.

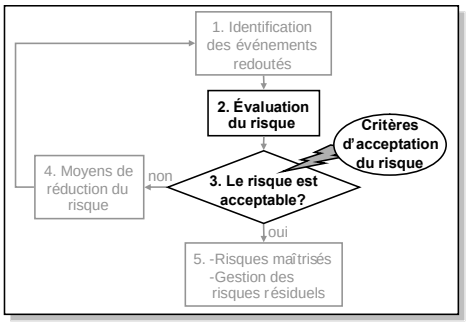
2.2.2 Les moyens de protection contre le risque

Les moyens de protection réduisent les conséquences d'un accident n'ayant pas pu être évité, autrement dit, ce sont des moyens de sécurité passive. Ils reposent sur la gestion des collisions et des déraillements par le contrôle du comportement de la structure des trains lors de l'accident. Lors d'une collision, un train peut être conçu pour limiter sa décélération et répartir la déformation liée au choc de telle sorte que les parties du train occupées par les voyageurs ne subissent pas ou peu l'écrasement de la structure, contrairement aux parties du train inoccupées qui absorbent l'énergie de l'accident [Tyrell 2001]. De plus, la répartition de

la masse des voitures et leur articulation entre-elles peuvent contribuer à éviter le chevauchement des trains entrés en collision et empêcher le renversement d'un train qui a déraillé. Sur les TGV, par exemple, les rames sont rigides en torsion leur évitant ainsi, en cas de déraillement, de se désarticuler.

La troisième partie de ce chapitre se consacre aux activités d'évaluation et d'acceptabilité des risques (objet de la prise de décision), étapes problématiques de la gestion des risques des systèmes complexes de transport guidé. Pour être accepté voire toléré, un risque doit d'abord être évalué. Ces étapes sont donc dépendantes. Elles sont de plus réglementées, notamment au niveau européen, par des directives et normes concernant la sécurité. Celles-ci seront abordées en premier lieu.

2.3 L'évaluation et l'acceptabilité des risques générés par un système de transport guidé



2.3.1 Contexte législatif et normatif de la sécurité des systèmes de transport guidé européens

La sécurité fait partie intégrante des récentes directives européennes [Directive 49/CE 2004] [Directive 50/CE 2004], à valeur législative, préconisant un réseau ferroviaire européen dans lequel les futurs systèmes de transport seront interopérables, c'est-à-dire capables de circuler sur l'ensemble des sections du réseau ferré appartenant aux divers états membres. Ces directives fixent des objectifs d'harmonisation entre les différents partenaires en établissant essentiellement des processus de certification, des procédures, des techniques et des méthodes d'analyses communs. Les objectifs référent notamment à l'usage de méthodes unifiées d'évaluation de la sécurité et à la rédaction d'un document conséquent, le *dossier de sécurité*, qui détaille l'ensemble de la gestion des risques. Pour permettre d'atteindre ces objectifs, les directives imposent l'adoption de Spécifications Techniques d'Interopérabilité (STI). Elles se présentent sous la forme de projets élaborés et révisés, anciennement, par l'Association Européenne pour l'Interopérabilité Ferroviaire (AEIF) regroupant des entreprises et des gestionnaires d'infrastructures ferroviaires, et depuis peu (juin 2005), par l'Agence Ferroviaire Européenne siégeant à Valenciennes (AFE). Les STI aident à gérer la complexité du système ferroviaire global en fournissant des solutions techniques visant à assurer les exigences

d'interopérabilité des différents sous-systèmes (l'infrastructure, l'énergie, la maintenance, le contrôle-commande, la signalisation, le matériel roulant, l'exploitation et la gestion du trafic, les applications télématiques au service des passagers et du fret). Les STI sont applicables par le biais des normes européennes harmonisées (ou en cours d'harmonisation par rapport à l'orientation prise par les STI). En particulier, les normes EN 50126, EN 50128, EN 50129 [CENELEC 2000] [CENELEC 1998] [CENELEC 1999] traitent à différents niveaux des aspects sécuritaires pour les systèmes ferroviaires. Les exigences requises au travers de l'architecture à trois niveaux (directives/STI/normes), sont délicates à démontrer en raison d'un bon nombre de questions relatives aux normes, bases de cette architecture. Les méthodes d'évaluation de la sécurité demandent notamment à être approfondies. C'est dans cette optique que différents projets européens comme SAMRAIL[4], UGTMS[5], et MODUrban[6] (ces deux derniers impliquant le LAMIH et intégrant la problématique de cette thèse, ont notamment permis de présenter dans ce chapitre, les éléments de sécurité ferroviaire) s'attachent à rechercher une nouvelle approche unifiée pour la sécurité des transports guidés qui pourrait être intégrée aux normes. Ces normes fournissent toutefois un cadre pour l'évaluation de la sécurité avec notamment la définition de principes d'acceptation du risque.

2.3.2 Principes d'acceptation du risque

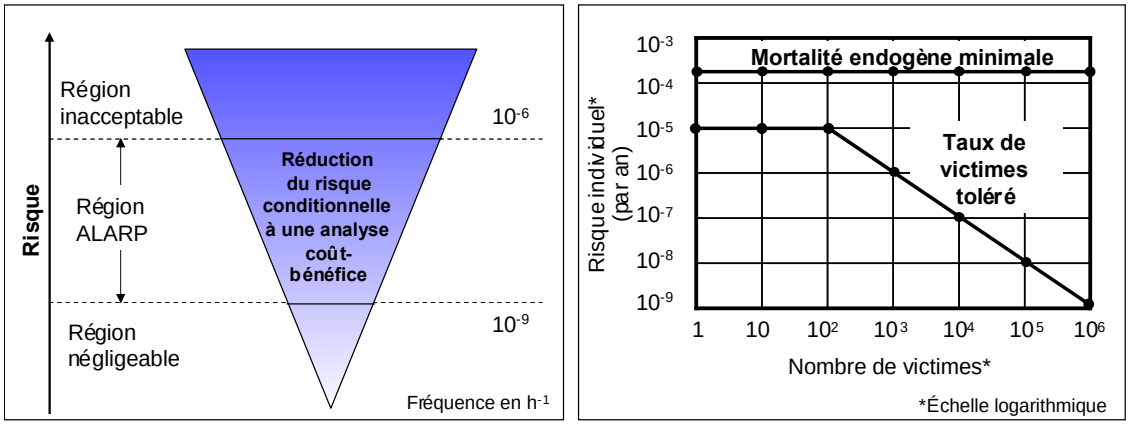
Trois principes d'acceptation du risque dans le domaine des transports guidés sont énoncés dans la norme EN 50126 [CENELEC 2000]:

- Le premier concerne le principe anglais ALARP (*As Low As Reasonably Practicable*, « aussi bas que raisonnablement possible ») illustré à la Figure 2.3.a. Ce principe est identique au principe ALARA (*As Low As Reasonably Attainable/Achievable*) utilisé dans le domaine nucléaire [Melchers 2001]. Il intègre une zone d'acceptation du risque, une zone de rejet du risque, et une zone, appelée région ALARP, dans laquelle les objectifs globaux de sécurité sont fixés en fonction du ratio de l'amélioration du risque sur les coûts investis. Cette zone peut être délimitée par des fréquences données (comme les valeurs indicatives de fréquence contenues dans la Figure 2.3.a). Si le risque analysé se trouve dans cette zone, les moyens à mettre en œuvre pour atteindre le niveau de sécurité désiré doivent être évalués ainsi que la réduction du risque qu'ils apportent. En effet, il est inutile

[4] Safety Management in Railways [SAMRAIL 2004], projet inscrit dans le 5ème PCRD (Programme Cadre de Recherche et de Développement européen)
[5] Urban Guided Transport Management System [UGTMS D6 2003], projet inscrit dans le 5ème PCRD
[6] MODular Urban guided rail system, projet inscrit dans le 6ème PCRD

d'employer d'énormes moyens (financiers, humains, matériels) pour une faible amélioration.

- Le second concerne le principe allemand MEM (*Mortalité Endogène Minimale*) illustré à la Figure 2.3.b. Celui-ci fixe les objectifs globaux de sécurité par référence à la mortalité endogène minimale d'un individu, c'est-à-dire le risque ambiant R_{MEM} pour une personne âgée de 5 à 15 ans (fixé à 2.10^{-4}/an [CENELEC 2000]). Les risques liés aux systèmes techniques sont considérés comme contribuant à 5% du risque individuel, donc la limite de risque toléré est fixée à $0.05 \times R_{MEM}$. Cette limite devient de plus en plus restrictive en proportion de la taille de la population pouvant être affectée.



Graphique a. **Graphique b.**

Figure 2.3 Critères d'acceptation du risque ALARP et MEM d'après [CENELEC 2000]

- Le dernier concerne le principe français GAME (*Globalement Au Moins Équivalent*). Celui-ci impose, pour un nouveau système, le respect des mêmes exigences de sécurité qu'atteint un système équivalent existant. Ce principe nécessite de connaître les objectifs de sécurité et le comportement relatif à la sécurité du système de référence.

De plus, un aspect important examiné dans les normes de sécurité ferroviaire EN 50126, EN 50128, EN 50129 [CENELEC 2000] [CENELEC 1998] [CENELEC 1999] et relevant des spécifications de sécurité, concerne l'utilisation de niveaux d'intégrité de sécurité conduisant l'analyse des risques.

2.3.3 Le concept de niveau d'intégrité de sécurité (SIL)

Les SILs (*Safety Integrity Levels*, niveaux d'intégrité de sécurité) sont des objectifs de sécurité dans les systèmes de transport guidé [CENELEC 2000] [CENELEC 1998] [CENELEC 1999]. Ils se caractérisent par des indicateurs discrets positionnés sur une échelle

à quatre niveaux. Sur cette échelle, le SIL 4 désigne le degré de sécurité le plus contraignant du fait de l'exigence forte de sécurité imposée, et le SIL 1 désigne l'exigence la plus faible. Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisées par des systèmes E/E/PE (Électrique/Électronique/Électronique Programmable) relatifs à la sécurité [IEC 61508 2000]. L'utilisation des SILs permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en complément des défaillances inhérentes au système opérationnel menant aux événements dangereux identifiés durant l'analyse des risques évoquée au premier chapitre. Les SILs sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances dangereuses de ces fonctions (cf. Annexe C), c'est-à-dire les défaillances pouvant provoquer des accidents. Cette étude différencie les défaillances de caractère *systématique* et les défaillances de caractère *aléatoire* [IEC 61508 2000].

Les *défaillances systématiques* sont des défaillances latentes qui se révèlent durant la phase d'exploitation du système opérant sous certaines conditions. Les défauts logiciels et les erreurs de conception se rapportent à cette définition ainsi que certaines défaillances matérielles liées à l'environnement (température élevée, perturbations électriques ou vibratoires, par exemple). Les défaillances systématiques peuvent uniquement être corrigées par des modifications de la conception, du processus de fabrication du système, des procédures d'exploitation, ou de la documentation. Elles ne sont pas quantifiables du fait de leurs causes difficilement prévisibles [Charpentier 2002] [IEC 61508 2000]. Afin de les limiter ou de les éliminer, l'activité d'assurance qualité de la gestion des risques tient une place importante dans la gestion de ces défaillances. Bien que cette activité soit laborieuse lorsque le SIL requis est élevé, elle permet d'empêcher l'occurrence de ces défaillances systématiques.

Les *défaillances aléatoires* concernent les défaillances du matériel. De par leur caractère probabiliste, ces défaillances sont quantifiables comme l'indique la partie 4 de la norme IEC 61508 [2000]. Celle-ci définit ainsi des exigences quantitatives pour chaque SIL, résumées dans le Tableau 2.1. Dans ce tableau, les fonctions ou systèmes de sécurité sont différenciés selon leur mode de fonctionnement par l'utilisation de deux paramètres de sûreté de fonctionnement : le PFD_{avg} (*Average Probability of Failure on Demand*, probabilité moyenne de défaillance à la demande) et le *PFH* (*Probability of a dangerous Failure per Hour*,

probabilité de défaillance dangereuse par heure). Chaque SIL voit, de plus, ces exigences quantitatives délimitées par une borne minimale et une borne maximale.

Niveaux d'intégrité de sécurité	**Faible sollicitation**	**Demande continue / Forte sollicitation**
	Probabilité moyenne de défaillance à la demande (PFD_{avg})	**Probabilité de défaillance dangereuse par heure (PFH)**
SIL 4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$10^{-9} \leq PFH < 10^{-8}$
SIL 3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10^{-8} \leq PFH < 10^{-7}$
SIL 2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$10^{-7} \leq PFH < 10^{-6}$
SIL 1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$10^{-6} \leq PFH < 10^{-5}$

Tableau 2.1 Tableau de SILs selon le mode de fonctionnement des fonctions ou systèmes de sécurité

Le mode de fonctionnement qui correspond à la fréquence prévue de demandes du système de sécurité par le système opérationnel, se répartit en deux modes, à savoir :

- *Le mode de fonctionnement à faible sollicitation* qui implique une demande épisodique du système de sécurité qui peut être le système de freinage d'urgence d'un train, par exemple. Il est considéré lorsque la fréquence de demande n'est pas plus grande qu'une par an, et est au plus égale à deux fois la fréquence des tests périodiques [IEC 61508 2000]. Ce mode est généralement attribué aux systèmes de protection, activés lors de l'occurrence d'un événement redouté. A partir de l'architecture du système de sécurité réalisant la fonction de sécurité faiblement sollicitée, la moyenne de la probabilité de défaillance à la demande PFD_{avg} (*Average Probability of Failure on Demand*) est évaluée sur un intervalle de temps [0, t [.

- *Le mode de fonctionnement continu ou à forte sollicitation* implique une forte demande du système de sécurité qui peut être le contrôle continu de vitesse d'un train, par exemple. Il est considéré lorsque la fréquence de demande est élevée ou continue, » c'est-à-dire lorsqu'elle est plus grande que une par an ou supérieure à deux fois la fréquence des tests périodiques [IEC 61508 2000]. Ce mode est généralement attribué aux systèmes de prévention d'événements redoutés. A partir de l'architecture du système de sécurité réalisant la fonction de sécurité fortement sollicitée, la probabilité de défaillance dangereuse par heure *PFH* (*Probability of a dangerous Failure per Hour*) est évaluée sur un intervalle de temps [0, t [.

L'aptitude qu'a une fonction réalisée par un système de sécurité, à respecter un SIL, doit être validée lors de l'analyse des risques qui fixe les exigences de SILs, comme l'explique le

paragraphe ci-dessous. Les procédures d'exploitation, de test et de maintenance doivent aussi être conformes aux exigences de SIL.

2.3.4 L'analyse des risques centrée sur les SILs

L'analyse des risques dans le domaine des transports guidés s'appuie sur les rôles distincts que possèdent les deux entités tenues de mettre en oeuvre ce processus : l'autorité de transport, c'est-à-dire l'opérateur qui va exploiter le système, et le constructeur concevant et réalisant le système [CENELEC 2000] [CENELEC 1999] [Braband 1999] (cf. Figure 2.4). Ceci permet le partage des responsabilités entre ces deux entités.

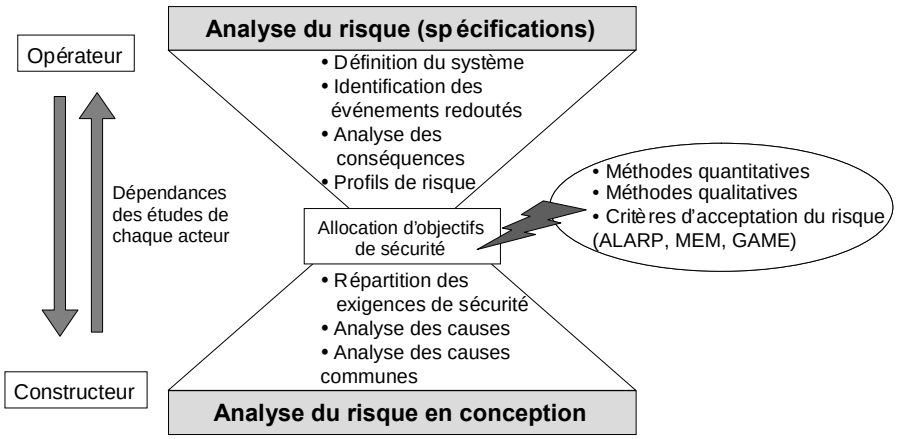


Figure 2.4 Gestion des risques dans le domaine des transports guidés, dérivée de [Braband 1999]

L'opérateur établit les spécifications du système indépendamment de la réalisation en étudiant l'aspect fonctionnel du système, notamment les fonctions de sécurité. Il détermine les différents événements redoutés du système et leurs conséquences potentielles. Il analyse les dangers menant à ces événements redoutés étant donné les défaillances possibles du système opérationnel et les événements extérieurs pouvant survenir. Enfin, il établit les niveaux de sécurité des fonctions de sécurité à mettre en place vis-à-vis de ces différents dangers. Grâce à une démarche d'allocation d'objectifs de sécurité, ces niveaux sont spécifiés à l'aide des SILs (ou des indicateurs PFD_{avg} ou PFH relatifs aux SILs). Cette allocation qui est dépendante des principes d'acceptation du risque énoncés précédemment, est souvent réalisée à l'aide de méthodes quantitatives ou qualitatives détaillées dans les paragraphes suivants. Ces méthodes attribuent pour chaque fonction de sécurité le SIL minimum à atteindre. Ce niveau est généralement conservé en raison du coût supplémentaire qu'engendrait la réalisation d'une fonction de SIL plus élevé.

Le constructeur définit, conçoit et réalise une architecture du système répondant aux exigences formulées par les spécifications. En particulier, les exigences de sécurité sont réparties sur les différents sous-systèmes de sécurité réalisant les fonctions de sécurité, puis sur les différents composants relatifs à la sécurité. Une étude des causes des défaillances des sous-systèmes opérationnels et des sous-systèmes de sécurité (défaillances détectées, non détectées, causes communes de défaillances des différents composants constituant les sous-systèmes), est alors effectuée pour mettre en évidence les défaillances dangereuses pouvant mener à un événement redouté, et pour vérifier si le niveau de sécurité est atteint pour chaque fonction de sécurité réalisée par les sous-systèmes.

2.3.5 Les méthodes d'allocation des SILs aux fonctions de sécurité

Les méthodes allouant un niveau d'intégrité de sécurité à un système de sécurité ou à une fonction de sécurité proviennent essentiellement des domaines de l'industrie de process [Summers 1998] [Stavrianidis et Bhimavarapu 2000] [Rouvroye 2001] [Smith et Simpson 2004], et de la sécurité machine [Goble 1998], [Charpentier 2002]. Les normes utilisées dans ces deux domaines, la norme IEC 61511 [IEC 61511 2003] et la norme IEC 62061 [IEC 62061/Ed.1 2005], se réfèrent à un unique système de sécurité dans le système global, appelé SIS (*Safety Instrumented System*, système instrumenté de sécurité) dans le domaine de l'industrie de process, et SRECS (*Safety-Related Electrical Control System*, système de sécurité commandé électriquement) dans le domaine de la sécurité machine. Dans le domaine des transports guidés, comme de multiples fonctions de sécurité réalisées par différents systèmes coexistent dans le système global (voir la deuxième partie de ce chapitre), l'analyse des fonctions du système de sécurité est préférée. Les méthodes qualitatives et quantitatives d'allocation des SILs, développées ci-dessous, examinent les différents dangers provenant du système opérationnel sans la prise en compte de dispositifs de sécurité. Pour réduire le risque associé à un danger donné, elles fournissent le SIL de la fonction de sécurité qui doit être implantée pour réduire la criticité du danger analysé.

2.3.5.1 Les méthodes quantitatives

La méthode de la matrice de risques utilise une matrice de risques bidimensionnelle qui est couramment employée dans le domaine des transports guidés [Schäbe et Wigger 2000] [Schäbe 2001]. En spécifiant une zone d'acceptation du risque dans un tableau de criticité (cf. Tableau 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.

Fréquence d'un événement dangereux		Niveau de risque			
Fréquent	10^{-4}				
Probable	10^{-5}			Inacceptable	
Occasionnel	10^{-6}		Indésirable		
Rare	10^{-7}				
Improbable	10^{-8}	Négligeable		Acceptable	
Invraisemblable	10^{-9}				
		Insignifiant	Marginal	Critique	Catastrophique
		Gravité des conséquences d'un événement dangereux			

Tableau 2.2 Exemple de matrice de risques ou tableau de criticité

L'échelle du paramètre de fréquence peut être adaptée au critère d'acceptation du risque délivré par l'autorité de transport. Par exemple, dans le projet UGTMS [UGTMS D6 2003], le taux d'acceptation du risque individuel (principe MEM, cf. paragraphe 2.3.2) a été adopté pour déterminer la fréquence limite entre la zone tolérable (négligeable et acceptable dans l'exemple du Tableau 2.2) et la zone intolérable (indésirable et inacceptable dans l'exemple du Tableau 2.2 où la zone indésirable peut être acceptable sous certaines conditions renvoyant au principe ALARP).

Soit le risque R_{np} (la notation *np* désignant *not protected*, est reprise de la norme IEC 61508 [2000]) lié à une défaillance du système opérationnel (l'événement dangereux) sans système de sécurité. A l'aide du tableau de criticité, R_{np} est évalué selon la combinaison du niveau de gravité G de l'événement dangereux, évalué par jugement d'experts, avec la fréquence F_{np} liée à la demande de la fonction de sécurité empêchant la situation dangereuse (i.e, la fréquence de défaillance du système opérationnel). Le risque de chaque événement dangereux identifié est ainsi classé dans la catégorie "tolérable" ou dans la catégorie "intolérable". Les événements classés en zone intolérable requièrent la création d'une fonction de sécurité pour prévenir le danger.

La détermination du niveau d'intégrité de sécurité de cette fonction dépend de la réduction du risque nécessaire pour atteindre le risque tolérable. Dans un contexte de prévention du risque, la fonction de sécurité diminue la fréquence d'occurrence de l'événement dangereux pour réduire le risque. Dans ce cas, elle doit, au minimum, ramener la fréquence de F_{np} à F_t (fréquence de risque tolérable). Bien que cette situation soit généralement préférée dans l'analyse des risques, un événement dangereux peut parfois mener à un accident. Dans ce

contexte de protection contre le risque, une fonction de sécurité diminuant la gravité est recherchée.

A partir des fréquences F_{np} et F_t, la norme IEC 61508 détaille la manière dont cette méthode peut être utilisée pour déterminer le SIL d'une fonction de sécurité faiblement sollicitée. La probabilité moyenne de défaillance à la demande de cette fonction (PFD_{avg}) est déterminée selon la procédure illustrée à la Figure 2.5. Dans cette figure, il est clairement mis en évidence que le risque initial (risque inhérent au système opérationnel, qualifié de EUC–*Equipment Under Control*– dans la norme) est réduit jusqu'à un risque toléré, par le biais du facteur PFD_{avg}. La valeur de ce facteur est bornée par la réduction du risque minimum à apporter, c'est-à-dire par l'inverse du facteur de réduction de risque *RRF*. Compte tenu de la valeur de PFD_{avg} retenue, le SIL de la fonction peut ensuite être déterminé à partir du Tableau 2.1.

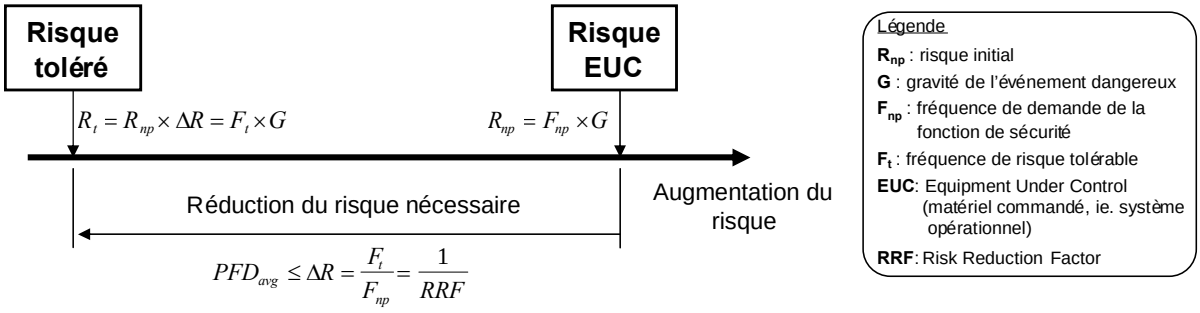


Figure 2.5 Réduction du risque par l'utilisation d'une fonction de sécurité faiblement sollicitée

Pour un système sollicitant de manière continue la fonction de sécurité, le sujet n'est pas abordé clairement dans la littérature. Dans [Schäbe et Wigger 2000] [Schäbe 2001] où le mode de fonctionnement continu est employé, la fréquence de défaillance F_{sf} d'une fonction de sécurité se substitue à la fréquence de demande F_{np} de cette fonction, abstraction faite des conditions environnementales. En fait, la fréquence F_{np} de défaillance du système opérationnel est déjà incluse dans la fréquence de défaillance de la fonction de sécurité, comme le montre la Figure 2.6. En effet, soit l'événement n'a pas de conséquence grave car la fonction de sécurité maintient le système opérationnel dans un état sécuritaire soit, à l'inverse, des conséquences critiques peuvent se produire en raison d'une défaillance de la fonction de sécurité. Dans ce cas, le risque encouru doit être réduit en ramenant F_{sf} à la fréquence de risque toléré de l'événement dangereux en question (fréquence F_t issue du Tableau 2.2). La fréquence F_{sf} obtenue permet alors de déterminer directement le SIL à partir de la colonne de droite du Tableau 2.1.

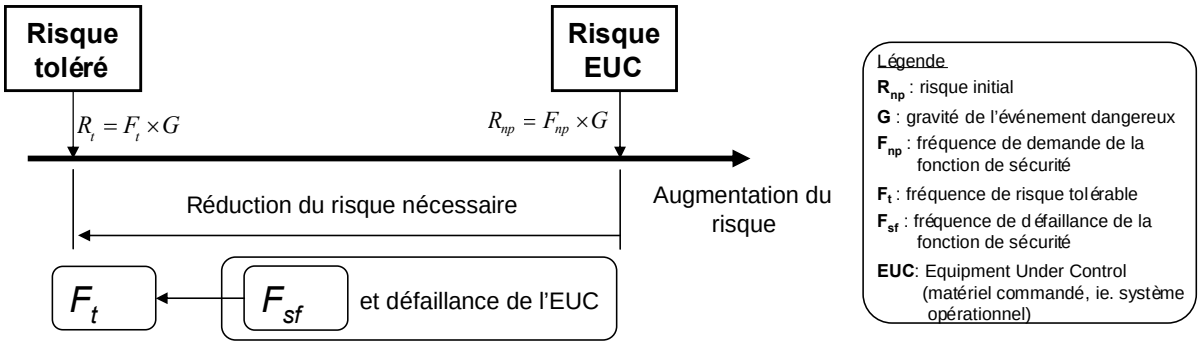


Figure 2.6 Réduction du risque par l'utilisation d'une fonction de sécurité fortement sollicitée

La méthodologie illustrée à la Figure 2.5 et à la Figure 2.6 n'est pas propre à la méthode de la matrice de risques. Elle s'intègre également dans d'autres méthodes telle la méthode LOPA (*Layer Of Protection Analysis*, analyse des couches de protection) [Dowell 1998] [Summers 2003]. Celle-ci cherche à déterminer le PFD_{avg} d'une fonction de sécurité réalisée par un SIS (*Safety Instrumented System*, système instrumenté de sécurité), compte tenu de la présence d'autres couches de protection (barrières de sécurité) élaborées dans une technologie différente de la technologie E/E/PE.

Les paramètres de fréquence intervenant notamment pour le calcul du facteur *RRF* (*Risk Reduction Factor*, facteur de réduction du risque, cf. Figure 2.5) sont délicats à calculer. En recours, des méthodes qualitatives reposant sur le jugement d'expert sont utilisées. Dans ces méthodes, la réduction du risque se révèle implicite.

2.3.5.2 Les méthodes qualitatives

a) Le graphe de risque

La méthode du graphe de risque analyse quatre facteurs de risques relatifs au danger et partagés en catégories selon leur importance: la gravité des conséquences, le temps d'exposition au danger, la possibilité d'évitement, et la probabilité d'apparition d'un accident sans fonction de sécurité. En sortie, la méthode indique la réduction de risque minimale que la fonction de sécurité doit apporter. La structure du graphe de risque dépend du domaine spécifique d'activité, d'où l'emploi de différents graphes dans les directives ou normes.

Un exemple tiré de [Goble 1998] est présenté à la Figure 2.7, où les conséquences portent uniquement sur l'atteinte à la vie de personnes. La prise en compte de dégâts matériels et de dommages causés à l'environnement nécessite l'utilisation de graphes additionnels.

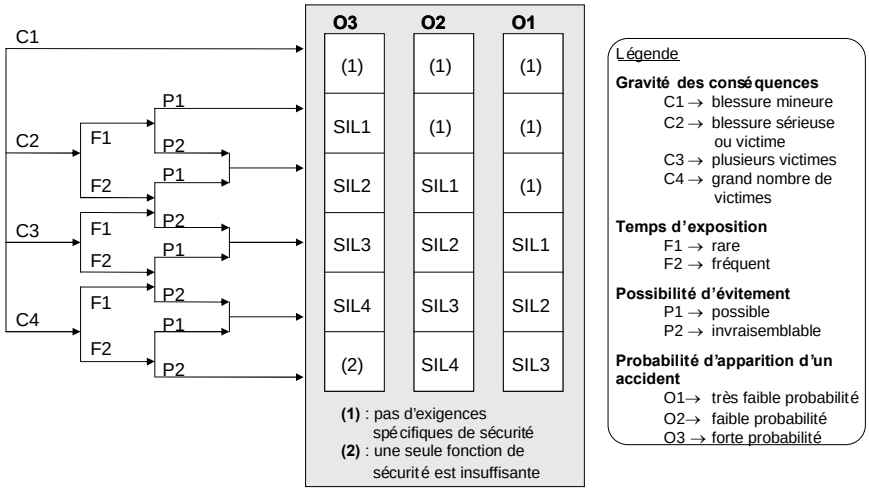


Figure 2.7 Exemple de graphe de risque

A l'aide de ce graphe de risque, la fonction de sécurité à implanter pour prévenir un danger de faible probabilité, dont les conséquences peuvent entraîner plusieurs victimes, le temps d'exposition étant rare et la possibilité d'évitement possible, sera réalisée en tenant compte des exigences relatives au SIL 1.

b) La matrice de gravité des événements dangereux

Contrairement à la méthode du graphe de risque qui ne prend en compte qu'une fonction de sécurité, la matrice de gravité des événements dangereux intègre plusieurs fonctions de sécurité sous réserve de leur indépendance. La matrice possède trois dimensions : la gravité des conséquences, la probabilité d'occurrence de l'accident potentiel et le nombre de dispositifs de sécurité qui sont déjà mis en place pour empêcher le développement du danger en un accident (cf. Figure 2.8). La fonction de sécurité supplémentaire dont le SIL est recherché, est basée uniquement sur la technologie E/E/PE. Les systèmes existants peuvent appartenir à d'autres technologies (mécanique ou pneumatique, par exemple). Comme précédemment, la structure de la matrice dépend du domaine spécifique d'activité.

Un exemple tiré de la norme [IEC 61508 2000] est présenté à la Figure 2.8. A l'aide de cette matrice, en considérant qu'un dispositif de sécurité est déjà mis en place pour prévenir un danger d'occurrence faible dont les conséquences sont critiques, le SIL de la fonction de sécurité sera réalisé en tenant compte des exigences relatives au SIL 1.

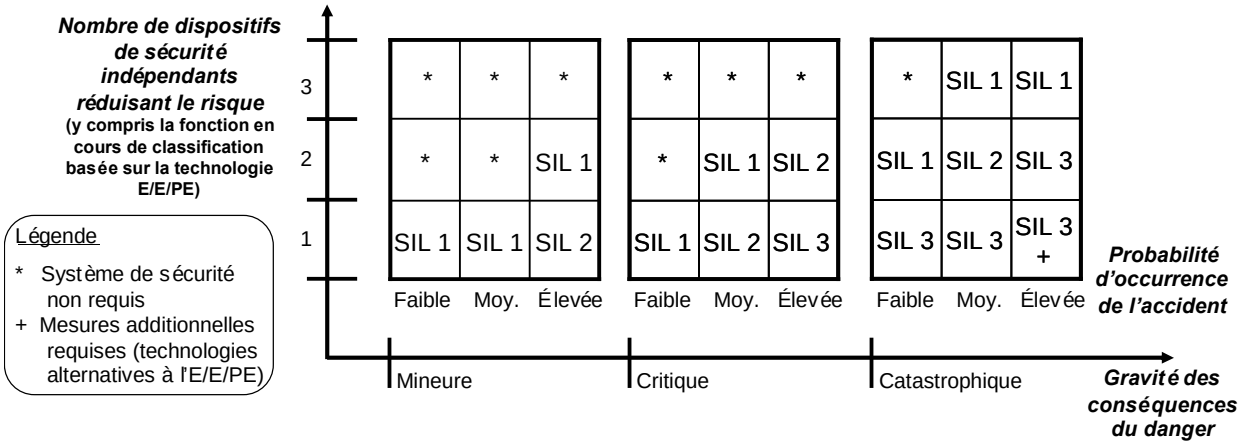


Figure 2.8 Exemple de matrice de gravité des événements dangereux

2.4 Discussion

Les niveaux d'intégrité de sécurité (SIL) alloués aux différentes fonctions de sécurité d'un système de transport guidé apparaissent comme des paramètres essentiels pour l'évaluation des risques (*a fortiori*, à l'évaluation de la sécurité) d'un tel système, système dans lequel la sécurité est essentiellement assurée par des moyens de prévention des risques matérialisés par le système de signalisation. Ces paramètres se présentent comme étant des variables dont la valeur est établie en fonction des critères d'acceptation des risques. Cependant, la manière dont sont fixées ces variables, par des méthodes comme celles que nous venons de présenter, est sujette à discussion, en particulier lorsque la plupart de ces méthodes ont été imaginées pour des domaines où la sécurité repose sur un unique système de sécurité (domaines de l'industrie de process et de la sécurité machine). A contrario, dans le domaine des transports guidés, plusieurs systèmes de sécurité coexistent. Ils sont déployés sur l'ensemble des réseaux et sont sollicités régulièrement lors de la circulation des trains, comme l'expose la description faite en début de ce chapitre. La complexité qui en résulte suppose l'existence de nombreuses interactions, de dépendances fonctionnelles, et de dépendances temporelles. Celles-ci, parallèlement à l'influence de l'environnement, nécessitent d'être envisagées pour réaliser une étude de sécurité cohérente. De ce fait, pour une analyse de sécurité globale, nous nous orientons vers la mise en place d'une démarche systémique basée sur l'évaluation des paramètres de fiabilité et de disponibilité de l'ensemble des systèmes de sécurité du système de transport, compte tenu des différents SILs alloués aux différentes fonctions de sécurité. Cette démarche est ascendante contrairement aux méthodes d'allocation des SILs précédentes

qui partent d'un critère d'acceptation du risque pour affecter des niveaux de sécurité aux fonctions de sécurité.

Cette problématique se situe au cœur des thématiques des différents projets de recherche européens consacrés au transport guidé, comme SAMRAIL, UGTMS, et MODUrban, mentionnés précédemment. Leur but est de fournir des méthodes et procédures standard garantissant que les systèmes complexes de transport guidé actuels, basés sur de nouvelles technologies, délivrent aux voyageurs empruntant ces moyens de transport, une qualité de service toujours plus élevée.

2.5 Conclusion

Le processus de maîtrise des risques exposé de manière générale au premier chapitre a été détaillé, dans ce deuxième chapitre, pour un système de transport guidé général, considéré dans son intégralité au moyen de ses sous-systèmes sol et bord. La première partie de ce chapitre a mis en évidence les différents risques existant dans ces systèmes (il s'agit de l'étape 1 du processus de gestion des risques, c'est-à-dire l'identification des événements redoutés). La deuxième partie a exposé les moyens de prévention et de protection contre le risque qui existent à l'heure actuelle dans le domaine des transports guidés (il s'agit de l'étape 4 du processus de gestion des risques, c'est-à-dire la mise en place de moyens de réduction du risque). Enfin la troisième partie a présenté les activités dépendantes d'évaluation et d'acceptabilité des risques (il s'agit des étapes 2 et 3 du processus de gestion des risques). Les SILs –Safety Integrity Levels (niveaux d'intégrité de sécurité)– issus des normes de sécurité fonctionnelle consacrées aux systèmes complexes, sont des objectifs de sécurité utiles à l'évaluation du risque et sont au centre des analyses de risque des systèmes de transport guidé. L'évaluation du risque, fonction de ces niveaux d'intégrité de sécurité, est problématique face à la complexité des transports guidés, comme l'a expliqué la discussion en fin de chapitre.

Le chapitre suivant vise à proposer une méthode qui essaie de répondre à cette problématique. Dans ce prochain chapitre, le concept de SIL, dont les diverses interprétations rendent cette notion ambiguë et difficile à appliquer, sera clarifié.

Chapitre 3. Proposition d'une approche pour l'évaluation de la sécurité des systèmes complexes de transport guidé

Sommaire

INTRODUCTION 72

3.1 L'ASPECT QUANTITATIF LIE AUX SILS, APPLICATION AU DOMAINE DES TRANSPORTS GUIDES 73

3.1.1 Différentes interprétations selon différents indicateurs 73

3.1.1.1 Les indicateurs employés pour les systèmes faiblement sollicités 73

3.1.1.2 Les indicateurs employés pour les systèmes fortement sollicités 75

3.1.2 Un indicateur quantitatif cohérent et approprié aux systèmes de transport guidé 76

3.2 METHODES DE QUANTIFICATION DES PROFILS DE RISQUE SELON LA COMBINAISON DES SILS 77

3.2.1 Représentation des profils de risque 77

3.2.2 La prise en compte des dépendances entre les fonctions de sécurité combinées 79

3.2.3 La combinaison des SILs 80

3.2.3.1 Approche basée sur des règles de combinaison : mise en place d'une algèbre des SILs 80

3.2.3.2 Approche liée aux événements rares : approche par simulation de Monte Carlo biaisée 81

3.2.4 Mise en œuvre et comparaison des méthodes de combinaison des SILs 82

3.3 LA MODELISATION DE LA COMPLEXITE D'UN SYSTEME DE TRANSPORT GUIDE 85

3.3.1 Déclinaisons de la complexité d'un système de transport guidé 85

3.3.2 Le concept de « situation d'exploitation » 86

3.3.3 Le modèle générique d'une situation d'exploitation support à la modélisation du système de transport guidé 88

3.3.4 Démarche de discrétisation pour la modélisation de l'évolution dynamique du système 91

3.4 METHODE DE SIMULATION POUR L'OBTENTION DE SCENARIOS DE RISQUE 93

3.4.1 Présentation de la méthode dédiée à la simulation de l'évolution des situations d'exploitation 93

3.4.2 Génération aléatoire de défaillances dangereuses 95

3.4.3 Technique d'injection de défaillances dangereuses 95

3.4.4 Identification des scénarios de risque 95

3.4.5 La simulation en tant que moyen de validation de la sécurité du système 96

3.5 CONCLUSION 96

Chapitre 3. Proposition d'une approche pour l'évaluation de la sécurité des systèmes complexes de transport guidé

Introduction

Le précédent chapitre a soulevé la problématique de l'évaluation de la sécurité d'un système complexe de transport guidé, cette évaluation tenant compte de niveaux d'intégrité de sécurité. Ces niveaux sont dénommés SILs (Safety Integrity Levels) et sont alloués aux différentes fonctions de sécurité qui peuvent être interdépendantes. Garantir que le niveau de sécurité est suffisant revient à démontrer que le niveau de risque est acceptable. Cependant face à la complexité d'un tel système de transport, les méthodes existantes d'évaluation des risques sont limitées étant donné la multitude de dangers potentiels à analyser, dans différentes situations possibles, en fonction des états de tous les sous-systèmes dédiés à la sécurité. Les travaux de recherche, présentés dans ce chapitre, visent à proposer une approche à la fois probabiliste et systémique dédiée à l'évaluation de la *sécurité globale* d'un système complexe de transport guidé. D'une part, cette approche est basée sur l'utilisation du concept de SIL dans l'évaluation de profils de risque. D'autre part, une modélisation du système de transport guidé est proposée pour tenir compte des différents aspects de complexité qui le caractérisent et pour permettre d'identifier ses profils de risque.

Dans les deux premières parties de ce chapitre, un cadre à la quantification de profils de risque ayant pour paramètres les SILs est présenté, les SILs étant alloués *a priori* aux fonctions de sécurité. Le concept de SIL, sujet à de nombreuses interprétations, sera approfondi dans la première partie, de manière à définir des objectifs de sécurité appropriés aux systèmes de transport guidé.

La démonstration de sécurité recherchée s'appuie sur le concept de *situation d'exploitation* permettant d'appréhender la complexité du système de transport guidé inscrit dans son environnement d'exploitation. Ce concept, développé en troisième partie de ce chapitre, est la

base de la démarche de modélisation du système tenant compte de son évolution dynamique.

Enfin, la quatrième partie du chapitre présente une méthode de simulation du système s'appuyant sur la modélisation du système de transport guidé exposée précédemment. Cette méthode se concentre sur la simulation des différentes actions de sécurité compte tenu des situations dangereuses possibles issues du système et de l'environnement. Elle vise à évaluer la robustesse du système de transport guidé face aux différents risques existants, ceci par l'intermédiaire de l'évaluation de scénarios de risque obtenus par l'injection d'événements dangereux dans le modèle simulé.

3.1 L'aspect quantitatif lié aux SILs, application au domaine des transports guidés

3.1.1 Différentes interprétations selon différents indicateurs

3.1.1.1 Les indicateurs employés pour les systèmes faiblement sollicités

La valeur probabiliste du SIL de chaque fonction de sécurité est déterminée différemment selon plusieurs normes et auteurs, et selon l'entité calculant cette valeur (l'opérateur ou le constructeur, cf. paragraphe 2.3.2.3). L'opérateur qui exploite le système spécifie les SILs selon les critères d'acceptation du risque établis par les autorités de transport. Le constructeur, qui conçoit le système incluant le système de sécurité, vérifie à partir de paramètres de sûreté de fonctionnement si ces spécifications sont respectées.

Pour déterminer la valeur probabiliste du paramètre PFD_{avg} (*Average Probability of Failure on Demand*, probabilité moyenne de défaillance à la demande) liée à un SIL donné du Tableau 2.1 (voir le deuxième chapitre), divers indicateurs sont utilisés (cf. Tableau 3.1). Calculée au niveau des spécifications de sécurité, cette valeur se rapporte à la réduction du risque à apporter, et s'exprime le plus souvent à l'aide du facteur *RRF* (*Risk Reduction Factor*, facteur de réduction du risque). Le système de sécurité conçu selon ces spécifications doit ensuite être analysé pour vérifier si ses propriétés respectent les exigences de sécurité. A ce niveau, l'obtention du paramètre PFD_{avg} nécessite le calcul du paramètre *PFD(t)* (probabilité de défaillance à la demande). Plusieurs exemples de calculs ont été développés dans [Lamy 2002] [Smith et Simpson 2004] [Zhang, Long et al. 2003] à l'aide des méthodes des diagrammes de fiabilité, des arbres de défaillance ou des graphes de Markov.

Mode de fonctionnement à faible sollicitation				
Indicateurs rencontrés		**Équations associées**		**Références**
PFD(t)	Probability of Failure on Demand (probabilité de défaillance à la demande)	Calculs au niveau de l'analyse de conception du système	$PFD(t) = 1 - R(t) - PFS(t)$ - $1-R(t) = PFD(t) + PFS(t)$ - $R(t)$: Reliability, fiabilité - PFS : Probability of Failing Safely, probabilité de défaillance non dangereuse	[Goble 1998]
			$PFD(t) = 1 - A(t)$ - $A(t)$: availability, disponibilité	[Smith et Simpson 2004]
PFD_{avg}	Average Probability of Failure on Demand (probabilité moyenne de défaillance à la demande)	Calculs au niveau des spécifications (pour l'allocation quantitative du SIL)	$PFD_{avg} = \frac{1}{RRF} = \frac{Fréquence\ de\ risque\ tolérable}{Fréquence\ de\ demande}$	[Summers 1998]
			$PFD_{avg} = \frac{1}{RRF} = \frac{Fréquence\ de\ risque\ tolérable}{Fréquence\ de\ risque\ inhérent}$ - RRF : Risk Reduction Factor	[Goble 1998]
		Calculs au niveau de l'analyse de conception du système (pour la vérification de l'exigence du SIL)	Somme de la probabilité moyenne de défaillance à la demande pour tous les sous-systèmes assurant la fonction de sécurité avec : $PFD_{avg} = F(\lambda_{DD}, \lambda_{DU}, t_{CE}, t_{GE}, MTTR, \beta)$ - $F(\ )$: fonction de ( ) - λ_{DD} et λ_{DU} : taux de défaillance dangereuse détectée et non détectée - t_{CE} et t_{GE} : temps moyen d'indisponibilité équivalent au niveau sous-système et système - $MTTR$: temps moyen de réparation - β : proportion de défaillances de cause commune	[IEC 61508 2000], partie 6
			$PFD_{avg} = \frac{1}{T}\int_0^T PFD(t)dt$ - T : intervalle de temps entre deux tests périodiques du système de sécurité	[Kosmowski et Sliwinski 2005], [Rausand et Høyland 2004], [Bukowski, Rouvroye et al. 2002]
			$PFD_{avg} = \frac{1}{\prod_{i=1}^{n} T_i}\int_0^{T_1}\ldots\int_0^{T_n} PFD_{sys}(t)dt$ - T_i : intervalle de temps entre deux tests périodiques, temps pouvant être différents selon les sous-systèmes i - sys : système	[Lamy 2002]

Tableau 3.1 Différents indicateurs quantitatifs associés à la faible sollicitation du système de sécurité

Étant donné l'évolution du paramètre *PFD(t)* dans le temps, la détermination de sa valeur moyenne sur le temps de mission de la fonction de sécurité analysée, permet d'obtenir le paramètre constant PFD_{avg}. Lorsque des tests périodiques sont réalisés sur la fonction, l'intervalle de temps entre deux tests périodiques consécutifs est préférablement employé au

temps de mission, le système réalisant la fonction de sécurité étant considéré comme neuf après ce test. Sans test périodique, le temps de mission est assimilé à la durée de vie du système.

3.1.1.2 Les indicateurs employés pour les systèmes fortement sollicités

Différents indicateurs (cf. Tableau 3.2) sont également utilisés pour déterminer la valeur probabiliste du paramètre *PFH* (*Probability of dangerous Failure per Hour*, probabilité de défaillance dangereuse par heure) liée à un SIL donné du Tableau 2.1 (voir le deuxième chapitre).

Forte sollicitation / Demande continue			
Indicateurs rencontrés		**Équations associées**	**Références**
PFH	Probability of dangerous Failure per Hour (probabilité de défaillance dangereuse par heure)	Somme des taux de défaillances dangereuses pour tous les sous-systèmes assurant la fonction de sécurité avec : $PFH = F(\lambda_{DD}, \lambda_{DU}, t_{CE}, \beta)$ - $F()$: fonction de ( ) - λ_{DD} et λ_{DU} : taux de défaillance dangereuse détectée et non détectée - t_{CE} : temps moyen d'indisponibilité équivalent au niveau sous-système et système - β : proportion de défaillances de cause commune	[IEC 61508 2000], partie 6
		$PFH = \frac{PFD(T_i)}{T_i}$ - T_i intervalle de temps entre tests périodiques, identiques pour les différents sous-systèmes	[IEC 61508 2000], parties 1 [Lamy 2002]
THR	Tolerable Hazard Rate (taux de danger tolérable)	$THR = \lambda_D = \lambda_{DD} + \lambda_{DU}$ - λ_D : taux de défaillance dangereuse - λ_{DD} et λ_{DU} : taux de défaillance dangereuse détectée et non détectée	[CENELEC 1999], [Braband 1999], [Schäbe et Wigger 2000], [Schäbe 2001], [Schäbe 2003], [Renpenning et Braband 2002]

Tableau 3.2 Différents indicateurs quantitatifs associés à la forte sollicitation du système de sécurité

Ces indicateurs concernant la phase de conception, sont basés sur des spécifications de sécurité données, et se rapportent tous à une fréquence d'événement dangereux, d'unité le plus souvent exprimée en h^{-1}. Lors de l'établissement des spécifications, les valeurs probabilistes sont directement corrélées avec les critères d'acceptation du risque. Ces derniers sont généralement énoncés sous la forme d'un tableau regroupant les différentes fréquences d'acceptation du risque, pour un individu, et pour différentes catégories d'accidents (un tel tableau peut être trouvé dans [Smith et Simpson 2004]).

3.1.2 Un indicateur quantitatif cohérent et approprié aux systèmes de transport guidé

Chaque fonction de sécurité d'un système de transport guidé peut, à première vue, être caractérisée par un mode de fonctionnement à forte sollicitation. En effet, comme exposé dans le second chapitre, la sécurité de ces systèmes est essentiellement assurée par le contrôle continu de la circulation des trains basé sur les points suivants:

- la surveillance de la vitesse des trains par rapport à un profil de vitesse déterminé, selon les limites de vitesse affectées aux sections de voies, et les caractéristiques du matériel roulant (notamment ses performances de freinage),
- le contrôle de non-franchissement du domaine limite affecté à chaque train (respect de l'autorisation de mouvement),
- le contrôle de la mise en place des autorisations de mouvement qui supposent, devant chaque train, que la position des aiguilles, l'affichage de signaux lumineux, le positionnement des éventuels passages à niveaux (dans le cas des transports guidés non urbains qui comprennent des interactions avec le trafic routier) soient établis de sorte qu'aucun itinéraire conflictuel ne soit commandé,
- l'assurance qu'aucun objet ou personne n'apparaisse face à un train et n'entrave son parcours.

Cependant certaines fonctions de sécurité, comme la localisation exacte des trains par balises ou le freinage d'urgence des trains (celui-ci intervenant en toute fin d'un scénario dangereux), ne sont pas continues puisqu'elle sont activées de manière intermittente. Toutefois, généraliser le mode de demande des fonctions de sécurité au mode continu n'est pas contradictoire avec la définition du mode de fonctionnement à forte sollicitation. En effet, celui-ci suppose continue toute fonction demandée plus d'une fois par an ou ayant une fréquence de demande supérieure à deux fois la fréquence des tests périodiques (cf. paragraphe 2.3.2.1). Cette définition se rapporte sans problème aux fonctions qui viennent d'être mentionnées intervenant nécessairement plus d'une fois par an.

L'indicateur probabiliste recherché, associé aux SILs des fonctions de sécurité des systèmes de transport guidé, repose donc sur les indicateurs présentés au Tableau 3.2. La norme EN 50129 [CENELEC 1999] stipule que le taux de défaillances dangereuses, se confondant avec le *THR* (*Tolerable Hazard Rate*, taux de danger tolérable), est employé pour les fonctions

fortement sollicitées. De plus, plusieurs analyses de sécurité conduites par Braband, Schäbe et Wigger utilisent également ce *THR* [Braband 1999] [Schäbe et Wigger 2000] [Schäbe 2001] [Shäbe 2003]. Il apparaît justifié de mener la suite de nos travaux en référant uniquement au *THR* comme indicateur probabiliste associé aux SILs des fonctions de sécurité intervenant dans les systèmes de transport guidé.

La partie suivante de ce chapitre se consacre à la proposition de méthodes de quantification de profils de risque utilisant les SILs, compte tenu des considérations ci-dessus exposées concernant l'aspect quantitatif du SIL. Elle s'appuie sur une représentation des profils de risque associant plusieurs fonctions de sécurité entre-elles.

3.2 Méthodes de quantification des profils de risque selon la combinaison des SILs

3.2.1 Représentation des profils de risque

L'établissement des différents profils de risque d'un système complexe consiste, après avoir déterminé les différents événements redoutés, à mettre en évidence les scénarios ou alternatives menant aux événements redoutés (voir le premier chapitre). Les méthodes d'allocation des SILs, présentées au deuxième chapitre, débouchent sur des scénarios mais ceux-ci sont réducteurs en raison d'un lien direct entre :

- un événement dangereux initiateur,
- une unique fonction de sécurité empêchant l'évolution de cet événement en différents événements redoutés,
- l'accident potentiel, parmi ces événements redoutés, ayant les pires conséquences possibles.

D'un point de vue quantitatif, le *THR* (*Tolerable Hazard Rate*, taux de danger tolérable) d'une fonction de sécurité peut directement être comparé à un taux de risque tolérable provenant des principes d'acceptation du risque, ce qui simplifie la démarche d'allocation des SILs en ignorant la complexité du système de transport guidé. D'un point de vue qualitatif, l'utilisation de facteurs de risques et la prise en compte du retour d'expérience souvent insuffisant, rendent cette démarche d'allocation imprécise et subjective.

Plusieurs fonctions de sécurité du système de transport agissent conjointement selon l'apparition d'événements dangereux internes (défaillances au sein du système) ou externes au système (dangers originaires de l'environnement). Les actions de sécurité forment un ensemble de scénarios qui peuvent ou non mener à des conséquences critiques selon la réussite ou non de ces actions dépendant de la fiabilité et de la disponibilité du système de sécurité réalisant les fonctions de sécurité. Par conséquent, un événement dangereux débutant un scénario particulier peut mener à plusieurs alternatives, dont les conséquences sont associées à une gravité plus ou moins élevée. De ce fait, la pire conséquence envisagée n'est pas toujours effective. La représentation des scénarios, à l'aide d'un diagramme de causes-conséquences permet d'illustrer, au travers de l'exemple présenté à la Figure 3.1, ces différentes alternatives.

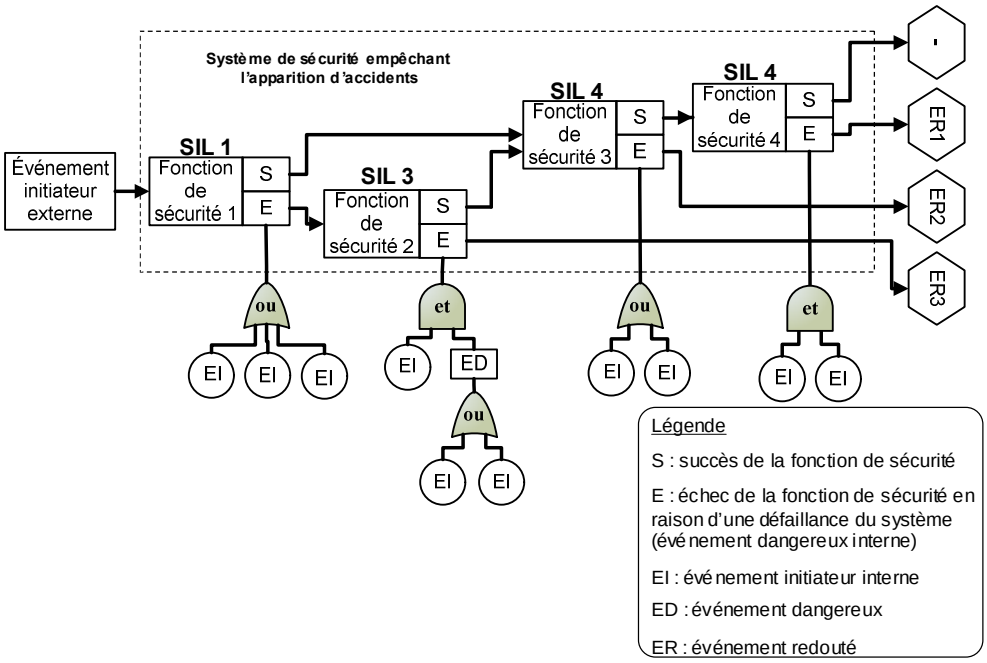


Figure 3.1 Exemple de représentation des profils de risque selon un diagramme causes-conséquences

Dans le contexte des transports guidés, le système opérationnel, c'est-à-dire le système réalisant le contrôle et la commande des opérations, et le système de sécurité ne peuvent pas réellement être séparés étant donnée leur implantation sur les mêmes équipements et leurs fonctionnalités liées (voir le deuxième chapitre). Par exemple, le sous-système qui établit l'autorisation de mouvement pour les différents trains, fixe les itinéraires de ces trains (fonction opérationnelle) tout en évitant des conflits de trajectoire (fonction de sécurité). Pour cette raison, la représentation des scénarios à la Figure 3.1 intègre l'ensemble des fonctions du système de transport en tant que fonctions de sécurité.

3.2.2 La prise en compte des dépendances entre les fonctions de sécurité combinées

Les différents scénarios représentant les actions de sécurité possibles, sont basés sur un enchaînement d'événements dangereux dépendants. Cet enchaînement est relatif au succès ou à l'échec des différentes fonctions de sécurité. Ces dépendances se répercutent sur le calcul de la probabilité des événements redoutés. En effet, la négligence de celles-ci dans les calculs peut mener à une évaluation du risque trop optimiste.

Les dépendances entre événements peuvent être illustrées au travers de la structure causale des fonctions de sécurité dépeinte par le diagramme de causes-conséquences de la Figure 3.2 (exemple issu de la Figure 3.1).

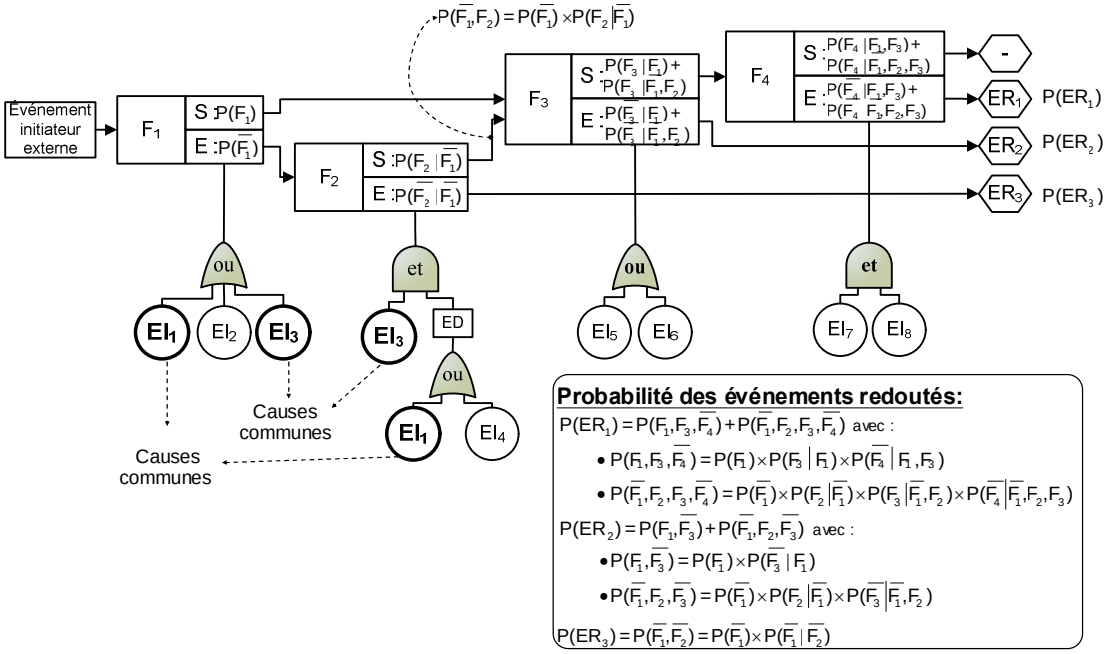


Figure 3.2 Les dépendances existant dans l'enchaînement des événements dangereux

Dans ce diagramme, la causalité apparaît dans la combinaison logique des événements de défaillance, aussi bien au niveau des causes de l'échec d'une fonction de sécurité (événements initiateurs), qu'au niveau de l'enchaînement de ces fonctions jusqu'à un événement redouté. Cet enchaînement peut contenir des dépendances conditionnelles dans le sens où l'occurrence d'un événement peut influer sur la probabilité d'occurrence d'un autre événement qui le succède. Les défaillances de causes communes peuvent notamment conditionner l'enchaînement des événements. Celles-ci sont des défaillances simultanées affectant plusieurs fonctions et dépendant d'une seule cause initiale [Charpentier 2002]. Dans

l'exemple, les fonctions F_1 et F_2 possèdent des défaillances de causes communes résultant de l'emploi de sous-systèmes communs. De même, les systèmes en redondance active font généralement l'objet de défaillances de causes communes en raison de la charge supplémentaire que provoque la défaillance de l'un des deux sous-systèmes sur l'autre sous-système resté en fonctionnement. Ce type de dépendances est souvent évité par une diversification fonctionnelle et matérielle des sous-systèmes.

Compte tenu de la structure causale pouvant exprimer les dépendances entre des fonctions de sécurité, une méthodologie dédiée à la recherche du SIL résultant de la combinaison des fonctions de sécurité, appelée plus simplement *combinaison des SILs*, peut être élaborée pour évaluer le risque. Nous avons d'abord considéré la possibilité de mettre en place une « algèbre des SILs » basée sur des règles de combinaison des SILs. En raison de la rareté de l'occurrence des défaillances des fonctions de sécurité spécifiée par un SIL donné, une approche de simulation de Monte Carlo biaisée a également été envisagée. L'analyse comparative des deux méthodes est ensuite effectuée.

3.2.3 La combinaison des SILs

3.2.3.1 Approche basée sur des règles de combinaison : mise en place d'une algèbre des SILs

La combinaison de fonctions de sécurité ayant différents SILs est analysée dans la deuxième partie de la norme IEC 61508, et apparaît dans les références [Kosmoski et Sliwinski 2005] et [Schäbe 2003]. Selon les informations contenues dans ces références, nous pouvons déduire des règles générales de combinaison pour entreprendre l'évaluation du risque et par conséquent l'évaluation de la sécurité [Beugin, Renaux et al. 2005a].

Ces règles, concernant des fonctions en série (opérateur AND) ou en parallèle (opérateur OR), sont présentées dans les équations (3.1), (3.2) et (3.3), où le SIL d'une fonction i est noté $SILx_i$:

Pour 2 fonctions i et j, avec $x_i \in \{1,4\}$:

$$\underset{i,j}{AND}\left(SILx_i, SILx_j\right) \Rightarrow SIL\min\left(x_i, x_j\right) \tag{3.1}$$

$$\underset{i,j}{OR}\left(SILx_i, SILx_j \middle| x_i = x_j\right) \Rightarrow SIL\min\left(x_i + 1, 4\right) \tag{3.2}$$

$$\underset{i,j}{OR}\left(SILx_i, SILx_j \middle| x_i \neq x_j\right) \Rightarrow SIL\max\left(x_i, x_j\right) \tag{3.3}$$

Ces règles sont basées sur les contraintes de conception relatives à chaque niveau de SIL, notamment les contraintes par rapport à la proportion de défaillance en sécurité d'une fonction réalisée par un sous-système matériel [IEC 61508 2000] (cf. Annexe C). Elles s'appliquent également aux fonctions réalisées par des sous-systèmes matériel et logiciel comme l'illustrent différents exemples présentés dans [Schäbe 2003].

La formulation de ces trois règles se rattache à une classification logarithmique des intervalles de fréquences liés aux SILs (ici les intervalles de THR, *Tolerable Hazard Rate*), ceux-ci étant basés sur des puissances décimales (cf. Tableau 2.1 du deuxième chapitre). Une autre analyse de la combinaison des SILs porte sur l'utilisation d'une approche par simulation de Monte Carlo (SMC) biaisée tenant compte de la rareté d'occurrence des défaillances de sécurité.

3.2.3.2 Approche liée aux événements rares : approche par simulation de Monte Carlo biaisée

Comme indiqué au premier chapitre, les algorithmes d'une SMC analogique, pour la simulation de l'évolution dynamique des systèmes, reposent sur la génération de plusieurs histoires pour l'évaluation des paramètres de fiabilité, de disponibilité et de maintenabilité. Cependant, l'échantillonnage des instants d'occurrence des événements de sécurité pose problème en raison de la rareté de ces événements. Une solution consiste à employer les techniques de réduction de la variance incluant les techniques de biaisage. L'approche de SMC indirecte est bien adaptée aux techniques de biaisage dans le cas où les comportements de défaillance et de réparation sont modélisés par des distributions de nature identique [Labeau et Zio 2001] ; elle sera ici utilisée. Cette approche de SMC est basée sur une fonction de structure représentée par une ou plusieurs équations détaillant le comportement du système (cf. Annexe A.). La structure causale des fonctions de sécurité représente ici le comportement du système de transport guidé, elle sert donc à l'élaboration de la fonction de structure du système.

L'approche de SMC indirecte biaisée consiste en l'utilisation d'une distribution biaisée du système $\psi_i^*(t)$ au lieu d'une distribution naturelle du système $\psi_i(t)$ ($\psi_i(t)$ étant la densité de probabilité d'entrée dans l'état i à l'instant t) [Marseguerra et Zio 2002]. Ce procédé permet de forcer l'occurrence des événements rares difficilement observables dans une simulation analogique, en augmentant artificiellement les probabilités de changement d'état. Les temps

de transition et les changements d'état étant échantillonnés depuis $\psi_i^*(t)$, les poids statistiques enregistrés dans l'évaluation doivent être corrigés du facteur $\psi_i(t)/\psi_i^*(t)$ pour compenser les effets du biaisage. Ainsi l'évaluation des paramètres de sûreté est possible en forçant la fréquence d'apparition des événements rares. Ceci est généralement effectué par une augmentation importante du taux de transition entre l'état de fonctionnement des composants de sécurité d'un système, et l'état de panne de ces composants (pour un taux considéré constant). L'augmentation de la valeur des THR liés aux fonctions de sécurité fera ici l'objet de la simulation de Monte Carlo biaisée développée selon l'algorithme présenté en Annexe A.

Les deux méthodologies de combinaison des SILs qui viennent d'être présentées sont mises en œuvre sur l'exemple de la Figure 3.1 et comparées dans la section suivante.

3.2.4 Mise en œuvre et comparaison des méthodes de combinaison des SILs

Les règles mettant en place une « algèbre des SILs » sont employées pour chaque scénario de risque de la Figure 3.1. Elles s'appliquent plus particulièrement aux fonctions de sécurité qui ont mené aux événements redoutés, c'est-à-dire les fonctions en échec. En effet, toutes les fonctions présentes dans le système n'interviennent pas systématiquement dans tous les scénarios de risque.

Les résultats obtenus sont présentés au Tableau 3.3 dans lequel chaque événement redouté, résultant de la combinaison de plusieurs SILs, est lui-même associé à un SIL. Ce dernier se rapporte à un intervalle de taux de danger tolérable (THR) qui traduit les caractéristiques probabilistes de l'événement redouté associé.

Événement redouté	**Combinaison menant à l'événement**	**Application des règles** selon les fonctions qui mènent à l'événement	**Résultat**
ER_1	(F_1 and F_3 and $\overline{F_4}$) or ($\overline{F_1}$ and F_2 and F_3 and $\overline{F_4}$)	SIL_{F4} or (SIL_{F1} and SIL_{F4}) = SIL4 or (SIL1 and SIL4) = SIL4 or SIL1	SIL4
ER_2	(F_1 and $\overline{F_3}$) or ($\overline{F_1}$ and F_2 and $\overline{F_3}$)	SIL_{F3} or (SIL_{F1} and SIL_{F3}) = SIL4 or (SIL1 and SIL4) = SIL4 or SIL1	SIL4
ER_3	$\overline{F_1}$ and $\overline{F_2}$	SIL_{F1} and SIL_{F2} = SIL1 and SIL3	SIL1

Tableau 3.3 Exemple d'application des règles de combinaison des SILs selon l'exemple présenté en Figure 3.1

L'approche de simulation de Monte Carlo biaisée tenant compte de l'ensemble de la structure causale des scénarios de la Figure 3.1 est maintenant utilisée.

Les bornes minimales et maximales des THR associés aux SILs des fonctions de sécurité constituent les paramètres d'entrée de la simulation. Ces taux sont intégrés dans des distributions probabilistes de nature exponentielle modélisant la fiabilité d'une fonction. Les taux de réparation nécessaires au déroulement de l'algorithme sont considérés comme extrêmement faibles pour se placer dans le cas des systèmes non réparables. La probabilité d'échec relative à la combinaison des fonctions menant à l'ER peut ainsi être mesurées. La Figure 3.3 présente l'estimation de cette probabilité obtenue par l'approche de simulation de Monte Carlo biaisée sur une durée de 360 000 heures, soit environ 40 ans d'exploitation (temps moyen d'exploitation en transport guidé). En toute rigueur, cette probabilité d'échec devrait être ramenée à un taux qui pourrait alors être comparé aux intervalles de taux de danger tolérable (THR) relatifs au SIL. Cependant l'obtention des taux nécessite la dérivation des courbes de probabilité d'échec, action qui compte tenu de la variabilité des courbes délivrées par la SMC, mène à une courbe aux variations encore plus marquées masquant l'information recherchée.

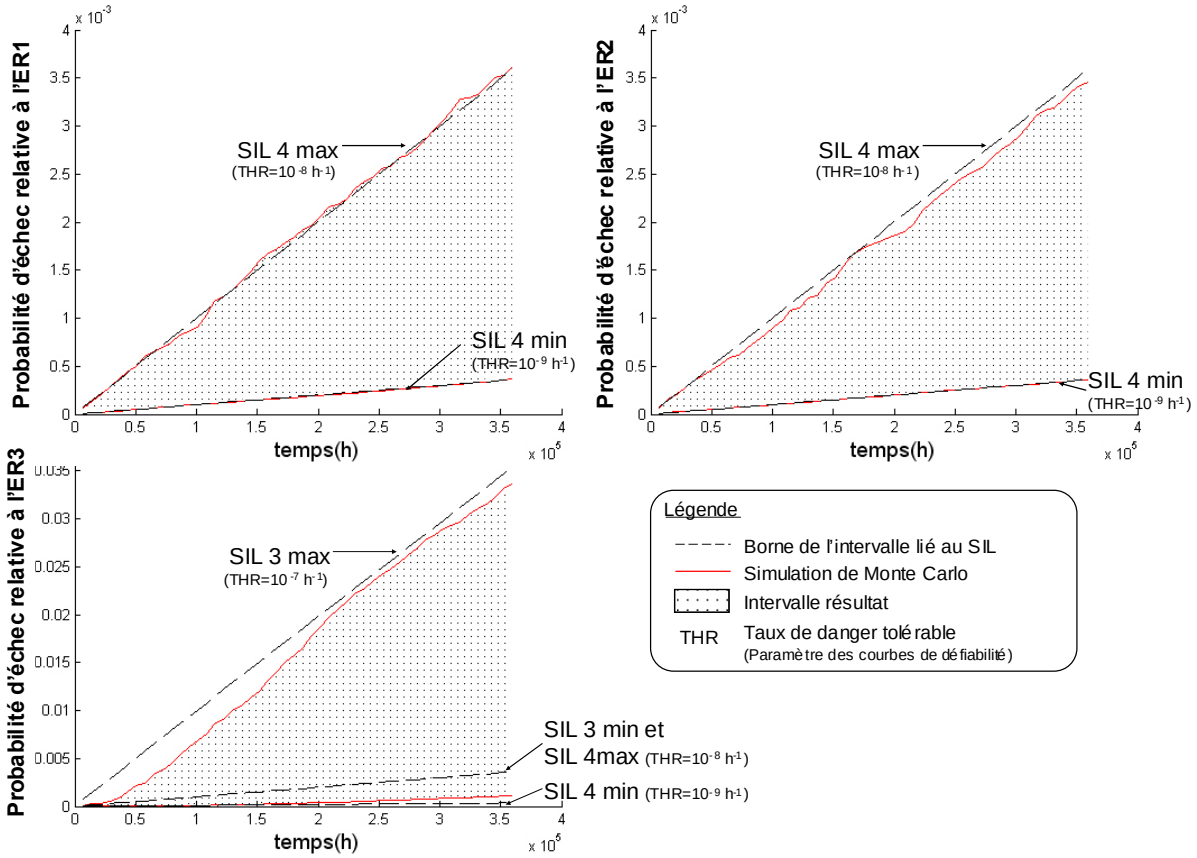


Figure 3.3 Résultats des probabilités d'échec obtenues par l'application de l'approche de SMC

Dans la Figure 3.3, les intervalles de probabilité obtenus pour chaque événement redouté sont délimités par une zone mouchetée. Pour savoir à quel SIL correspondent ces intervalles, les courbes de défiabilité associées à chaque taux délimitant les intervalles de THR liés au SIL, ont été tracées (avec l'emploi de la distribution exponentielle), ce procédé étant notre seul moyen de comparaison. Ainsi l'intervalle de la probabilité d'échec associée à l'ER_1 se situe dans l'intervalle de défiabilité correspondant au SIL 4. Il est à noter que les courbes délivrées par la SMC ont une faible variabilité autour des courbes liées aux SILs (écart maximum pouvant être estimé à 2×10^{-4} pour l'ER1 et l'ER2, et à 3×10^{-3} pour l'ER3), cette variabilité provenant de l'erreur statistique minime qu'entraîne la simulation. De même, l'intervalle de défiabilité associé à l'ER_2 se situe aussi dans l'intervalle de défiabilité correspondant au SIL 4, et l'intervalle de défiabilité associé à l'ER_3 se situe à la fois dans l'intervalle de défiabilité du SIL 3 et du SIL 4.

Comparaison des méthodes

Par rapport à la méthode précédente mettant en place des règles d'« algèbre de SILs », l'approche par SMC biaisée fournit les mêmes résultats pour ER_1 et ER_2, et des résultats plus optimistes pour ER_3 dans le sens où le SIL obtenu est meilleur d'un point de vue sécurité. Cette différence peut s'expliquer par le fait que, selon l'emploi de la règle AND de combinaison des SILs sur des fonctions formant une séquence (combinaison en série), la fonction ayant le SIL le plus faible détermine le SIL de la séquence. Ceci se rapporte à la règle du pire cas généralement utilisée dans l'évaluation des risques.

Discussion sur l'intérêt des méthodes

La première méthode utilisant des règles dites d'« algèbre des SILs » apparaît intéressante dans le sens où l'application de ces règles est simple et n'est pas assujettie à la problématique des événements rares. La deuxième méthode est plus complexe à mettre en œuvre mais s'adapte bien à l'étude de combinaison des SILs pour des structures fonctionnelles complexes. Les dépendances entre événements pouvant exister dans ces structures complexes sont en effet prises en compte grâce à la fonction de structure, aspect que n'intègre pas la méthode précédente. De ce fait, en raison de l'étude de systèmes complexes que sont les systèmes de transport guidé, l'approche par SMC biaisée prévaut sur la méthode d'« algèbre des SILs ». Elle permet, de surcroît, l'analyse dynamique d'un système en considérant des dépendances temporelles qui peuvent modifier l'ordre d'arrivée des événements (ici les événements liés à l'échec ou non des fonctions de sécurité) sur un temps de mission analysé. Les états des sous-

systèmes peuvent en effet être modifiés dans le temps selon, par exemple, des événements de défaillance ou de réparation. Cette propriété est intéressante vis-à-vis de l'aspect dynamique du système et sera également exploitée dans la suite de ce chapitre.

La troisième partie de ce chapitre détaille les principes mis en œuvre pour la modélisation d'un système complexe de transport guidé, celle-ci ayant pour finalité l'identification de profils de risque du système compte tenu de ses différents aspects de complexité. Pour cela, l'approche systémique proposée est basée sur une démarche originale qui considère le contexte environnemental dans lequel évolue le système.

3.3 La modélisation de la complexité d'un système de transport guidé

3.3.1 Déclinaisons de la complexité d'un système de transport guidé

La complexité des systèmes de transport guidé peut se décliner selon quatre aspects mis en évidence au premier chapitre:

- L'aspect fonctionnel : Les systèmes de transport guidé sont fonctionnellement complexes en raison de leurs fonctionnalités à la fois multiples et dupliquées en différents points du système. Par exemple, compte tenu de l'étendue géographique d'un tel système, plusieurs fonctions semblables sont dupliquées d'une section de voie à une autre, et d'un train à un autre, assurant ainsi les mêmes fonctionnalités d'une section à l'autre;
- L'aspect comportemental : L'agrégation d'un nombre important d'entités, dont les différents états (fonctionnement ou panne) évoluent aléatoirement dans le temps, traduit l'aspect comportemental de la complexité. Dans les systèmes de transport guidé, du fait de l'évolution dynamique des différents états des équipements des sous-systèmes sol et bord, le déplacement des trains le long des voies peut conduire à différentes situations dont certaines sont risquées;
- L'aspect structurel : Plusieurs éléments hétérogènes d'un système (composants, sous-systèmes de nature matérielle, logicielle et/ou humaine) qui interagissent continuellement ensemble et avec leur environnement (celui-ci se rapportant aux voies et aux abords des voies dans les systèmes de transport guidé), constituent l'aspect structurel de la complexité;

- L'aspect technologique : Cet aspect est relatif à la compatibilité, l'interopérabilité et l'interchangeabilité des composants. Ces notions soulignent la complexité des différentes technologies en interaction.

La méthode du diagramme de causes-conséquences, présentée au paragraphe 3.2.1, donne la possibilité de visualiser différentes séquences d'événements composées à la fois de défaillances de fonctions de sécurité et des causes de ces défaillances. Mais à ce niveau, les aspects structurel et comportemental de la complexité font défaut. Ils nécessitent : *i)* la prise en compte de la duplication des fonctions de sécurité relative à l'étendue du domaine opérationnel et du nombre de trains, et *ii)* la prise en compte de l'évolution dynamique du système dans un environnement donné :

- *i)* Pour ce point, le domaine opérationnel peut être divisé en plusieurs sous-domaines. Un sous-domaine (ou partie) restreint la frontière du système à un ensemble de fonctions de sécurité non dupliquées sur ce sous-domaine. Dès lors, selon ces conditions, l'analyse par partie des séquences d'événements représentées par un tel diagramme est plus abordable. Dans ce cas, l'entrée d'un diagramme associé à un sous-domaine donné, c'est-à-dire un événement initiateur externe, peut : soit être un danger issu de l'environnement (par exemple, un obstacle sur la voie), soit la conséquence de la défaillance d'un sous-système issue d'un autre sous-domaine (par exemple, un train se déplaçant dans une mauvaise direction).
- *ii)* Pour ce point, l'évolution dynamique du système dans son environnement est à prendre en compte. Elle intègre à la fois la dynamique discrète de l'évolution stochastique du système (défaillances et réparations), et la dynamique continue de la variation des variables physiques du système (liée aux déplacements des trains).

La démarche de modélisation que nous proposons s'appuie sur le concept de *situation d'exploitation*, concept que nous avons défini pour mettre en oeuvre les deux points soulevés ci-dessus [Cauffriez 2005] [Beugin, Renaux et al. 2005b] [Beugin, Renaux et al. 2007]. Les sections suivantes détaillent ce concept et les principes de la démarche de modélisation.

3.3.2 Le concept de « situation d'exploitation »

Le concept de *situation d'exploitation* est inspiré du concept de *situation de travail* de Hasan [2002] [Hasan, Bernard et al. 2003] consacré à la conception sûre de systèmes socio-

techniques de production. Ce nouveau concept est ici défini pour aider à la modélisation des systèmes complexes de transport guidé. Une situation d'exploitation est un modèle composé d'un ensemble de classes relatives au système de transport, à son environnement et intégrant des aspects de sécurité. La Figure 3.4 représente le modèle que nous proposons en illustrant les différentes classes qui interviennent dans le concept de situation d'exploitation et les dépendances existant entre ces classes.

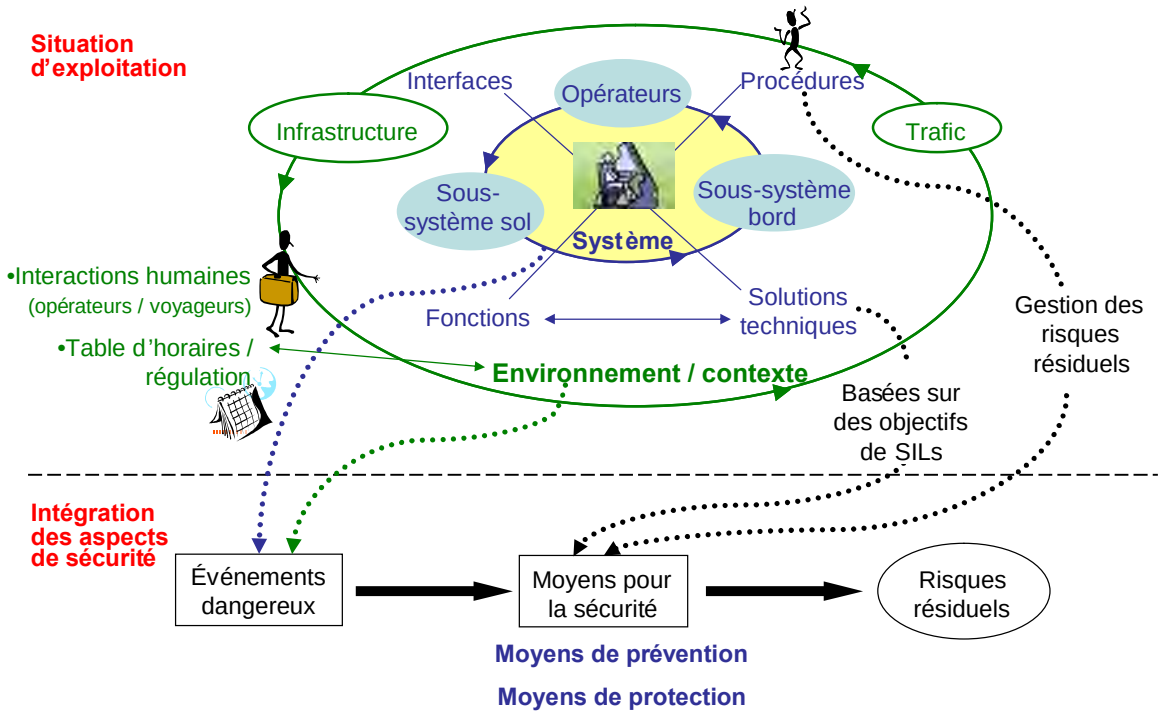


Figure 3.4 Macro vue du modèle de situation d'exploitation

Ainsi le système de transport guidé, constitué du sous-système sol et du sous-système bord, s'inscrit dans un environnement (contexte d'exploitation) qui est caractérisé par la géographie de la ligne de transport et de ses abords, et qui varie selon l'affluence des voyageurs et les stratégies de régulation. Au sein de ce système, des opérateurs humains effectuent des tâches liées à des procédures et à des informations issues des interfaces homme-machine intégrées au système. La sécurité est, elle, fonction des solutions techniques retenues qui procurent les moyens de prévention et de protection contre le risque, et de la gestion des risques résiduels.

Contrairement au concept de situation de travail de Hasan [2002] qui considère que l'ensemble du système complexe, relatif à un ensemble de machines, a une position fixe dans l'environnement, le concept de situation d'exploitation doit intégrer le fait que les différents trains (sous-système bord) se déplacent, en interaction avec le sous-système sol, au sein de

l'environnement. Ce déplacement est envisagé par la succession de plusieurs situations d'exploitation dont les paramètres évoluent d'une situation à l'autre. Avant de considérer comment s'enchaînent les situations d'exploitation, le modèle générique d'une situation d'exploitation est présenté.

3.3.3 Le modèle générique d'une situation d'exploitation support à la modélisation du système de transport guidé

Pour décrire le modèle générique d'une situation d'exploitation, le modèle du diagramme de classes du formalisme UML (*Unified Modeling Language*, pour langage de modélisation unifié) est utilisé. Dans un diagramme de classes, une classe est une abstraction utilisée pour regrouper plusieurs objets concrets selon leurs propriétés et comportements similaires, et peut-être reliée à d'autres classes dont elle dépend.

Une classe du modèle générique exposé à la Figure 3.5 possède différents attributs dont les valeurs sont affectées, une fois la classe instanciée en un objet spécifique. Ces attributs traduisent les propriétés et le comportement des objets qui sont issus de cette classe et qui sont relatifs au système de transport guidé. Le diagramme de classes de la Figure 3.5 s'appuie sur les principes présentés dans la section précédente.

Les dépendances entre classes sont représentées par des relations d'association associées à des cardinalités. La cardinalité d'une association est un couple numérique [*min*, *max*] exprimant la quantité minimale et maximale d'instances de classe pouvant intervenir dans l'association. Elle est notée « *min*..*max* », *max* pouvant être un nombre non spécifié supérieur à zéro, noté *. Les relations d'association ne sont pas orientées et se lisent dans un sens ou dans l'autre selon l'emploi à l'actif ou au passif du verbe qui les caractérise. Par exemple l'association entre la classe *situation d'exploitation* et la classe *événement dangereux* se traduit, selon le sens de lecture, par :

- un objet *événement dangereux* est déclenché par un ou plusieurs objets *situation d'exploitation*,
- un objet *situation d'exploitation* déclenche aucun, un ou plusieurs objets *événement dangereux*.

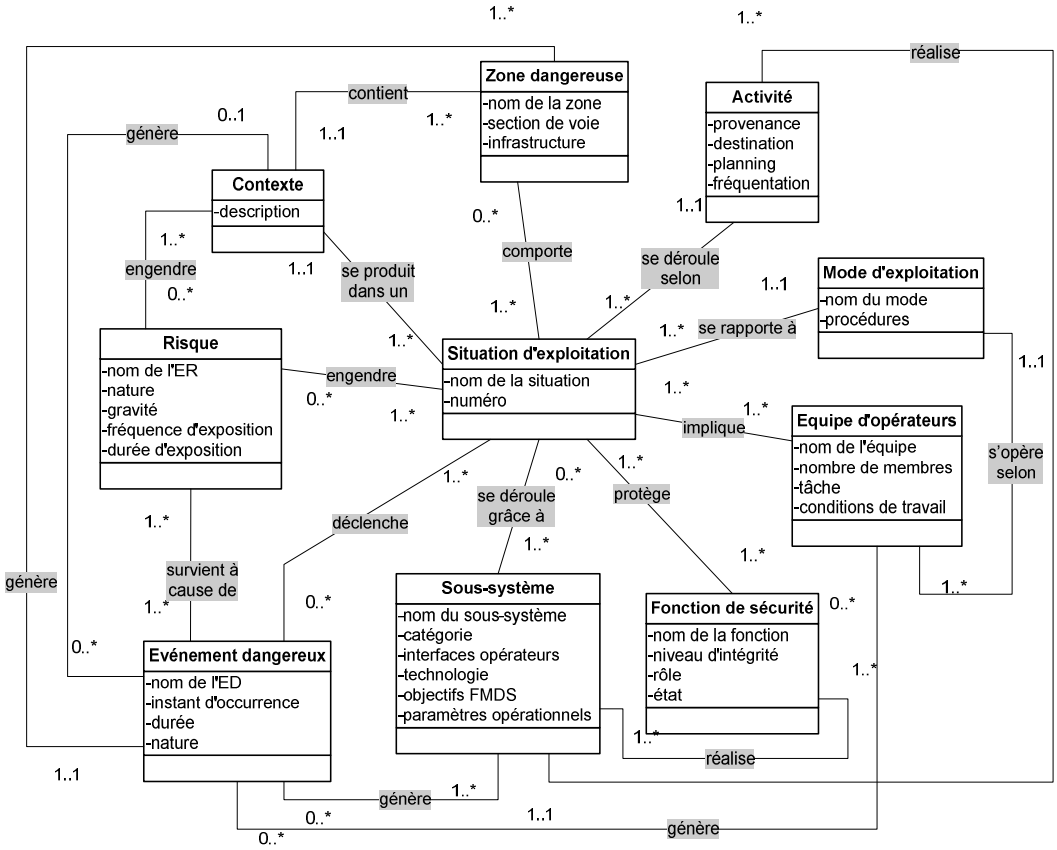


Figure 3.5 Le modèle générique d'une situation d'exploitation représenté sous la forme d'un diagramme de classes issu du formalisme UML

Les différentes classes du modèle se détaillent comme suit :

a) La classe « risque »

Elle permet de lister par leur *nom* les différents événements redoutés du système de transport guidé. La *nature* du risque se rapporte aux conséquences potentielles pouvant être humaines (risque individuel ou collectif pour les voyageurs, non voyageurs, opérateurs), matérielles, ou financières. La *gravité* concerne l'ampleur des conséquences potentielles et est exprimée selon une échelle à préciser (nombre de voyageurs exposés, coût des dégâts matériels par exemple). *La fréquence d'exposition* et la *durée d'exposition* sont des paramètres quantitatifs qui peuvent être éventuellement connus selon la situation d'exploitation analysée.

b) La classe « zone dangereuse »

Elle concerne une zone, définie par un *nom*, dans laquelle une personne est exposée à un risque. Cette zone peut se rapporter à une *section de voie*, munie d'*infrastructures* particulières.

c) La classe « contexte »

Elle représente l'ensemble des éléments de l'environnement qui entourent ou influent sur une situation d'exploitation. Ceux-ci sont exprimés dans une *description*.

d) La classe « activité »

Elle se rattache aux éléments de régulation des trains pour une situation d'exploitation particulière. Ces éléments concernent la *provenance*, la *destination* et le *planning* des trains dont la *fréquentation* par les voyageurs est plus ou moins élevée.

e) La classe « équipe d'opérateurs »

Elle se rapporte aux différents opérateurs intervenant dans une situation d'exploitation. Une équipe d'opérateurs, définie par un *nom*, est constituée d'un *nombre* donné d'opérateurs ayant une *tâche* à remplir selon des *conditions de travail* particulières.

f) La classe « mode d'exploitation »

Les différents modes d'exploitation que peut comporter un système de transport guidé sont traduits par cette classe. Un mode donné, caractérisé par un *nom*, fait appel à des *procédures* définies.

g) La classe « fonction de sécurité »

Elle concerne les différentes fonctions de sécurité du système de transport intervenant dans la situation d'exploitation. Une fonction de sécurité élémentaire est définie par un *nom*, un *niveau d'intégrité*, un *rôle* et se trouve dans un *état* de fonctionnement ou de panne pour la situation d'exploitation examinée.

h) La classe « sous-système »

Elle comprend les différents éléments techniques envisagés dans la conception du système de transport guidé et elle est associée aux différentes fonctions de sécurité à réaliser. Ces éléments ont un *nom*, une *catégorie*, ils peuvent comporter des *interfaces avec les opérateurs*, ils se rapportent à une *technologie* donnée et possèdent des paramètres opérationnels dépendant du contexte.

i) La classe « événement dangereux »

Elle représente les événements physiques et organisationnels, de *nature* interne ou externe au système de transport. Ces événements, ayant un *nom*, peuvent survenir dans une situation d'exploitation à un *instant d'occurrence* aléatoire, et ont une *durée* qui dépend du contexte

d'exploitation. Ces événements proviennent de zones dangereuses, de sous-systèmes, de l'environnement, ou d'opérateurs.

Intérêt de l'utilisation du modèle générique

Le modèle générique d'une situation d'exploitation contribue à la modélisation d'un système complexe de transport guidé existant ou d'un système en phase de conception grâce à la décomposition du système selon les attributs relatifs aux différentes classes du modèle. En outre, le modèle fait ressortir les différentes actions de sécurité prévues dans le système face aux situations dangereuses pouvant exister, en d'autres termes différents profils de risque du système sont suggérés et peuvent être a priori explicités. Ainsi la complexité du système est appréhendée en mettant en évidence la structure causale des fonctions de sécurité préconisées pour réduire le risque. De plus, pour tenir compte de l'évolution dynamique du système liée au déplacement des trains dans leur environnement et aux changements d'état du système, ce modèle peut être intégré à une démarche de discrétisation de l'exploitation du système modélisant l'évolution des situations d'exploitation. L'exploitation du système comprend notamment des séquences d'événements dangereux qui peuvent potentiellement mener à des accidents et que la démarche détaillée ci-dessous modélise dans un but ultérieur d'évaluation du risque.

3.3.4 Démarche de discrétisation pour la modélisation de l'évolution dynamique du système

La démarche modélisant l'évolution des situations d'exploitation s'appuie sur la discrétisation du temps de mission du système en plusieurs intervalles égaux. La taille du pas de discrétisation est définie de manière à considérer l'invariance des états des fonctions du système sur chaque intervalle. Une situation d'exploitation notée $\mathbf{O_i}$ est alors comprise sur l'intervalle **i**, les attributs des différents objets du modèle de situation d'exploitation, en particulier les attributs états des objets *fonction de sécurité*, n'évoluant pas sur une situation d'exploitation. A noter que, même si les attributs sont invariants sur $\mathbf{O_i}$, le système continue à évoluer. Par exemple, en considérant que l'attribut « paramètres opérationnels » de l'objet « sous-système train » correspond à la vitesse du train, si ce paramètre est affecté d'une valeur non nulle, le train se déplace selon cette vitesse.

A partir de l'évolution des attributs d'une situation d'exploitation à une autre, la *dynamique* du système est ainsi construite, notamment l'évolution des événements dangereux menant à la

manifestation d'un accident. En effet, la transition d'une situation $\mathbf{O_i}$ à une situation $\mathbf{O_{i+1}}$ est caractérisée par l'apparition ou au contraire l'élimination de dangers liée à l'occurrence d'événements, tels les changements d'état des fonctions de sécurité relatifs à une activation normale ou anormale des systèmes de sécurité, ou la modification du contexte opérationnel avec, par exemple, la présence d'un obstacle sur la voie.

La Figure 3.6 illustre cette discrétisation du fonctionnement du système en plusieurs situations d'exploitation pour rendre compte de l'évolution des événements dangereux. Dans cette figure, les différents intervalles échantillonnés sont représentés sur la flèche associée au temps de mission du système. L'évolution du système, sans changement des attributs de la situation d'exploitation sur l'intervalle **i**, est assimilée à une succession d'événements discrets $\mathbf{e_{ij}}$, où $\mathbf{j=\{1,..,J\}}$ est le nombre d'événements apparaissant conditionnellement aux états des fonctions de sécurité durant l'$\mathbf{O_i}$ (par exemple, l'arrivée en station d'un train fait partie de la même situation d'exploitation, les attributs de cette situation n'ayant pas évolué dans le cas où il n'y a pas eu de défaillance, et commence par les événements de décélération du train jusqu'à l'arrêt, l'ouverture des portes, l'entrée des voyageurs dans le train).

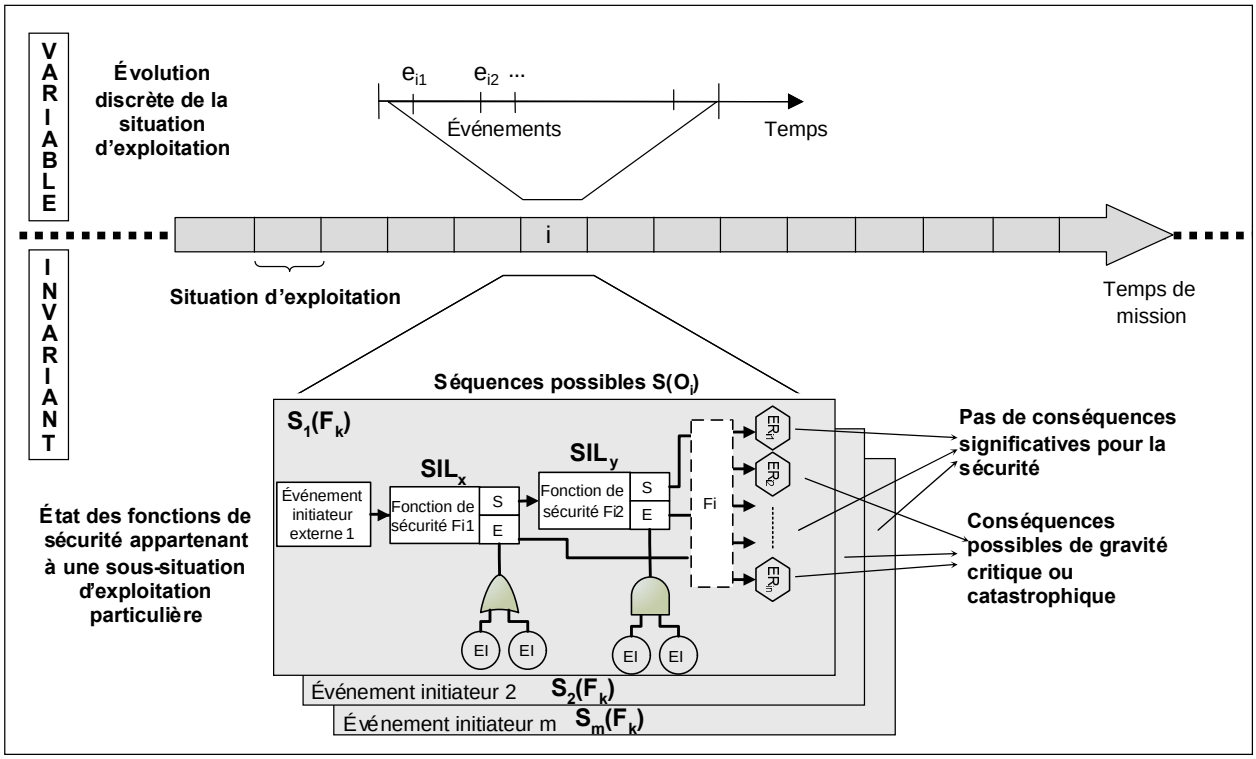


Figure 3.6 Différentes séquences d'événements dangereux apparaissant sur une situation d'exploitation

Pour décrire la présence de fonctions dupliquées qui sont liées à l'étendue du système et qui mènent à des actions de sécurité identiques sur différents domaines de la ligne de transport, plusieurs sous-ensembles de situations d'exploitation, appelés sous-situations d'exploitation, peuvent être identifiés. Une situation d'exploitation se compose d'un ensemble d'objets dont certains peuvent avoir des attributs identiques ; une sous-situation d'exploitation se restreint aux objets distincts. En notant $\mathbf{S(O_i)}$ les séquences d'événements dangereux sur $\mathbf{O_i}$, les séquences d'événements dangereux propres aux sous-situations d'exploitation (séquences $\mathbf{S_m}$ dont l'événement initiateur est **m**, **M** étant l'ensemble des événements initiateurs) recouvrent[7] l'ensemble $\mathbf{S(O_i)}$ comme l'illustre la Figure 3.6.

Compte tenu qu'une fonction non dupliquée peut intervenir dans plusieurs séquences d'événements dangereux contenues dans $\mathbf{S(O_i)}$, le recouvrement[7] des séquences peut alors se résumer à l'équation (3.4). Dans cette équation, une fonction de sécurité est désignée par la notation $\mathbf{F_k}$, **k** étant la k^{ième} fonction parmi **K** fonctions.

Pour $S_m(F_{k(k\in K)})_{(m\in M)} \subset S(O_{i(i\in I)})$:

$$\forall k \in K,\ \forall m \in M,\ S(O_i) = \bigcup_{m\in M} S_m(F_k) \quad \text{et} \quad \forall k \in K,\ \exists n \in M, \bigcap_{n\in M} S_n(F_k) \neq \varnothing \qquad (3.4)$$

La quatrième partie de ce chapitre présente une méthode de simulation définissant la manière dont des expérimentations peuvent être menées sur le modèle du système de transport guidé selon les principes de la démarche de modélisation venant d'être décrite.

3.4 Méthode de simulation pour l'obtention de scénarios de risque

3.4.1 Présentation de la méthode dédiée à la simulation de l'évolution des situations d'exploitation

La méthode de simulation proposée à la Figure 3.7 est une approche par événements qui cherche à reproduire les conditions d'exploitation d'une ligne de transport. Ces conditions d'exploitation tiennent compte du contexte environnemental source de dangers et du fonctionnement du système également à l'origine de dangers.

[7] Un recouvrement d'un ensemble X est un ensemble Y de sous-ensembles non vides de X tel que l'union de ces sous-ensembles soit égale à Y.

Le modèle simulé est basé sur les attributs du modèle de situation d'exploitation se rapportant au système de transport guidé. Les fonctions de sécurité et les événements dangereux ont notamment été mis en évidence par l'emploi de ce modèle.

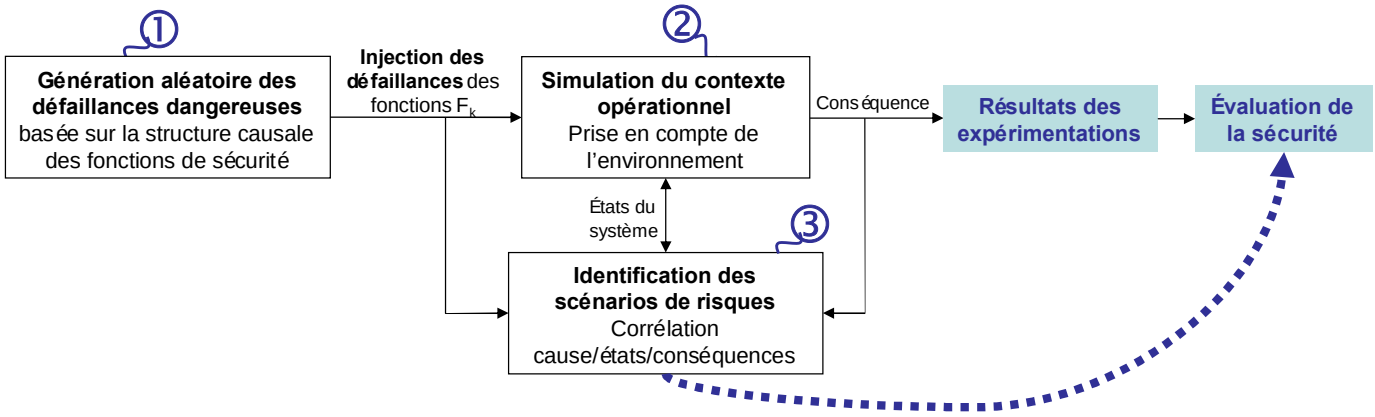


Figure 3.7 Méthode dédiée à la simulation de l'évolution des situations d'exploitation

La méthode génère aléatoirement des instants d'occurrence d'événements dangereux internes au système, c'est-à-dire les événements dangereux relatifs aux défaillances des fonctions de sécurité (point ① de la Figure 3.7).

Ces événements sont ensuite injectés dans la simulation du contexte opérationnel où l'évolution des variables continues, telles les variables de vitesse ou de distance par exemple, sont considérées dans le temps selon une succession d'événements discrets (point ② de la Figure 3.7).

Enfin, compte tenu des défaillances dangereuses et des comportements à risque observés lors de la simulation du contexte opérationnel, les scénarios de risque peuvent être identifiés puis évalués (point ③ de la Figure 3.7).

Les paragraphes suivants détaillent la génération aléatoire des défaillances dangereuses, la technique d'injection de ces défaillances dans la simulation du contexte opérationnel et l'étape d'identification des scénarios de risque.

3.4.2 Génération aléatoire de défaillances dangereuses

Dans la démarche de modélisation basée sur le concept de situation d'exploitation, les séquences de défaillances dangereuses consistent en des séquences d'événements dont l'instant d'occurrence a été échantillonné selon des lois de probabilité relatives au succès ou à l'échec des fonctions de sécurité. L'approche par simulation de Monte Carlo biaisée présentée au paragraphe 3.2.3.2 est intéressante pour cette étape car, avant d'entreprendre des statistiques sur les séquences d'événements menant à des événements redoutés, elle génère en premier lieu, sur une échelle de temps, une succession d'événements d'occurrence aléatoire (histoire) incluant potentiellement les séquences d'accident à comptabiliser. L'occurrence des événements rares étant biaisée, des défaillances dangereuses se produisent assurément sur le temps de mission du système.

Ces événements surviennent sur les intervalles de temps $\mathbf{\Delta t}$, suite à une combinaison de défaillances issues du système menant à la défaillance des fonctions de sécurité. La *fonction de structure* employée pour coder les combinaisons menant à la défaillance de chacune des fonctions de sécurité est notée $\mathbf{SF(F_k,t)}$ ($\mathbf{F_k}$ représentant la fonction de sécurité **k** et **t** un instant analysé). Elle permet de tenir compte des dépendances fonctionnelles entre les fonctions de sécurité du système de transport guidé. La fonction $\mathbf{SF(F_k,t)}$ apparaît plus exactement comme un vecteur dont chaque coordonnée est associée à l'état des différentes fonctions de sécurité.

3.4.3 Technique d'injection de défaillances dangereuses

Les séquences de défaillances dangereuses générées aléatoirement sont injectées dans la simulation du contexte opérationnel sous forme de variables discrètes. Ces événements surviennent sur le temps de mission du système, et influent alors sur la simulation du contexte opérationnel par SED (simulation par événements discrets) jusqu'à éventuellement déclencher un incident, c'est-à-dire un événement qui modifie le comportement attendu et normal du système, ou un accident, c'est-à-dire un événement redouté. Les séquences particulières de défaillances dangereuses menant à ces événements peuvent alors être identifiées.

3.4.4 Identification des scénarios de risque

Cette étape repose sur l'identification des scénarios de risque, c'est-à-dire les séquences de défaillances dangereuses ayant mené à un événement redouté lors de la simulation du contexte opérationnel.

Les scénarios sont identifiés selon l'analyse des séquences aboutissant à un accident de gravité élevée, tels les collisions ou déraillements susceptibles d'entraîner de nombreuses victimes et de lourds dégâts matériels. L'emploi de diagrammes de causes-conséquences donne lieu à une description adaptée de ces scénarios de risque par la mise en évidence à la fois des séquences de défaillances de fonctions de sécurité menant aux événements redoutés et des causes de défaillance de ces fonctions.

3.4.5 La simulation en tant que moyen de validation de la sécurité du système

La méthode de simulation apporte le moyen de tester la robustesse de l'ensemble du système de transport face aux différents risques existants. En effet, d'une part, cette méthode cherche, à vérifier que les scénarios de risque obtenus dans les expérimentations impliquent les différentes fonctions de sécurité envisagées lors de la démarche de modélisation précédente, c'est-à-dire que la méthode vise à démontrer la nécessité d'implanter une ou plusieurs fonctions de sécurité prévue en conception. D'autre part, l'exhaustivité des scénarios obtenus est recherchée, la simulation pouvant mettre en exergue des scénarios de risque non prévus lors de la conception du système.

Dès lors, l'évaluation de ces scénarios peut être effectuée selon les méthodes de quantification des profils de risque faisant l'objet de la deuxième partie de ce chapitre. Au final, la probabilité des événements redoutés ayant été déterminée, elle pourra être comparée aux principes d'acceptation du risque adoptés.

3.5 Conclusion

Dans ce troisième chapitre, nous avons proposé une nouvelle approche probabiliste et systémique pour l'évaluation de la sécurité d'un système complexe de transport guidé. Cette approche a pour but ultime de vérifier si les exigences de sécurité établies par l'autorité de transport permettent d'atteindre un niveau de sécurité acceptable.

La première partie de ce chapitre s'est d'abord attachée à définir clairement la manière dont les exigences quantitatives de sécurité sont établies dans les spécifications des systèmes de transport guidé. Elles sont liées à l'usage de niveaux d'intégrité de sécurité (les SILs) qui doivent être alloués aux fonctions de sécurité conformément aux normes de sécurité fonctionnelle.

La deuxième partie a présenté deux méthodes de quantification de profils de risque ayant pour paramètres les SILs, plus précisément elles s'appuient sur la combinaison de plusieurs fonctions de sécurité dépendantes ayant chacune un SIL alloué *a priori* :

- une méthode dite d'« algèbre des SILs » et,
- une méthode basée sur une simulation de Monte Carlo biaisée cherchant à surmonter la faible occurrence des événements de sécurité qualifiés d'événements rares.

La deuxième méthode, plus complexe à mettre en œuvre, s'est révélée plus intéressante car elle s'adapte adéquatement à l'étude de combinaison des SILs pour des structures fonctionnelles complexes des fonctions de sécurité.

La partie suivante a exposé une démarche systémique de modélisation du système de transport guidé s'appuyant sur le concept original de situation d'exploitation. Ce dernier fournit un support à la modélisation du système dans son environnement, et permet de mettre en évidence la structure causale des fonctions de sécurité et les événements dangereux pouvant perturber le fonctionnement du système et altérer sa sécurité. La modélisation permet de prendre en compte l'évolution dynamique du système par l'évolution des situations d'exploitation dans le temps. Ainsi un cadre à la génération de séquences circonstancielles de combinaisons d'événements pouvant mener à des événements redoutés est constitué.

La dernière partie de ce chapitre a envisagé une méthode de simulation permettant de simuler le contexte opérationnel du système de transport guidé intégrant les séquences d'événements dangereux évoquées dans la démarche de modélisation du système. L'analyse des séquences d'événements qui auront mené à un accident fournit les profils de risque qui pourront être évalués.

Le chapitre suivant se propose de valider l'approche sur un système de transport guidé donné. Les conditions de sécurité préalablement établies par modélisation sont ensuite testées et évaluées selon la simulation du contexte opérationnel.

Chapitre 4. Simulation d'un système de transport guidé pour la validation de l'approche proposée

Sommaire

INTRODUCTION 100

4.1 PRESENTATION DU SYSTEME DE TRANSPORT GUIDE 100

4.1.1 Cartographie du réseau 100

4.1.2 Les fonctionnalités liées au cantonnement 101

4.1.3 Les fonctionnalités liées aux enclenchements d'itinéraires 102

4.1.4 La transmission des données du sous-système sol au sous-système bord 104

4.2 MODELISATION DU SYSTEME SELON LE CONCEPT DE SITUATION D'EXPLOITATION ET DEVELOPPEMENT DE LA MAQUETTE LOGICIELLE DU SYSTEME 105

4.2.1 L'instanciation des classes du modèle de situation d'exploitation 105

4.2.2 La génération dans le temps de défaillances dangereuses du système par simulation de Monte Carlo biaisée 109

4.2.2.1 La prise en compte des dépendances des fonctions de sécurité 109

4.2.2.2 La prise en compte de la duplication des fonctions de sécurité 110

4.2.2.3 Mise en œuvre de la simulation de Monte Carlo biaisée 111

4.2.3 La simulation du contexte opérationnel intégrant des événements dangereux 112

4.2.3.1 Présentation de la maquette logicielle reproduisant le fonctionnement du système 112

4.2.3.2 L'influence des défaillances dangereuses sur la simulation de la maquette logicielle 113

4.3 IDENTIFICATION ET EVALUATION DES SCENARIOS OBTENUS PAR SIMULATION 113

4.3.1 Les profils de risque établis a priori 113

4.3.2 Evaluation préalable : analyse quantitative sans prise en compte du contexte opérationnel 117

4.3.3 Analyse qualitative des situations d'exploitation 121

4.3.4 Analyse quantitative des situations d'exploitation 123

4.3.4.1 Optimisation nécessaire du temps d'exécution des simulations 123

4.3.4.2 Résultats de l'évaluation pour les deux cas d'étude retenus 124

4.3.5 Discussion 126

4.4 CONCLUSION 127

Chapitre 4. Simulation d'un système de transport guidé pour la validation de l'approche proposée

Introduction

Ce chapitre a pour objectif d'illustrer et de valider l'approche d'évaluation de la sécurité d'un système complexe de transport guidé proposée au chapitre précédent, cette approche permettant en particulier d'étudier la robustesse du système de transport face aux risques existants. Pour cela, un système constitué de trains se déplaçant sur un réseau ferré dont le tracé est fictif est considéré dans ce chapitre, au travers d'une maquette logicielle que nous avons développée.

La première partie du chapitre s'attache d'abord à décrire les fonctionnalités considérées dans un hypothétique cahier des charges du système.

La seconde partie présente la modélisation du système d'après la démarche de modélisation reposant sur le concept de situation d'exploitation, celui-ci permettant la prise en compte des différentes caractéristiques de sécurité du système de transport guidé.

L'évolution dynamique du système modélisé est alors possible grâce à la méthode de simulation exposée au troisième chapitre. La manière dont cette méthode de simulation est mise en œuvre sur la maquette logicielle est présentée.

Les résultats concernant l'identification et l'évaluation des scénarios de risque obtenus par simulation sont exposés en dernière partie.

4.1 Présentation du système de transport guidé

4.1.1 Cartographie du réseau

La ligne de transport guidé considérée est constituée de quatre stations dénommées A, B, C, et D, ayant chacune deux quais pour desservir chaque station dans un sens de circulation comme

dans l'autre. La ligne comporte un embranchement après la station B où les trains, à cette bifurcation, sont alternativement envoyés vers les stations C ou D. Ces dernières sont ainsi desservies de manière égale.

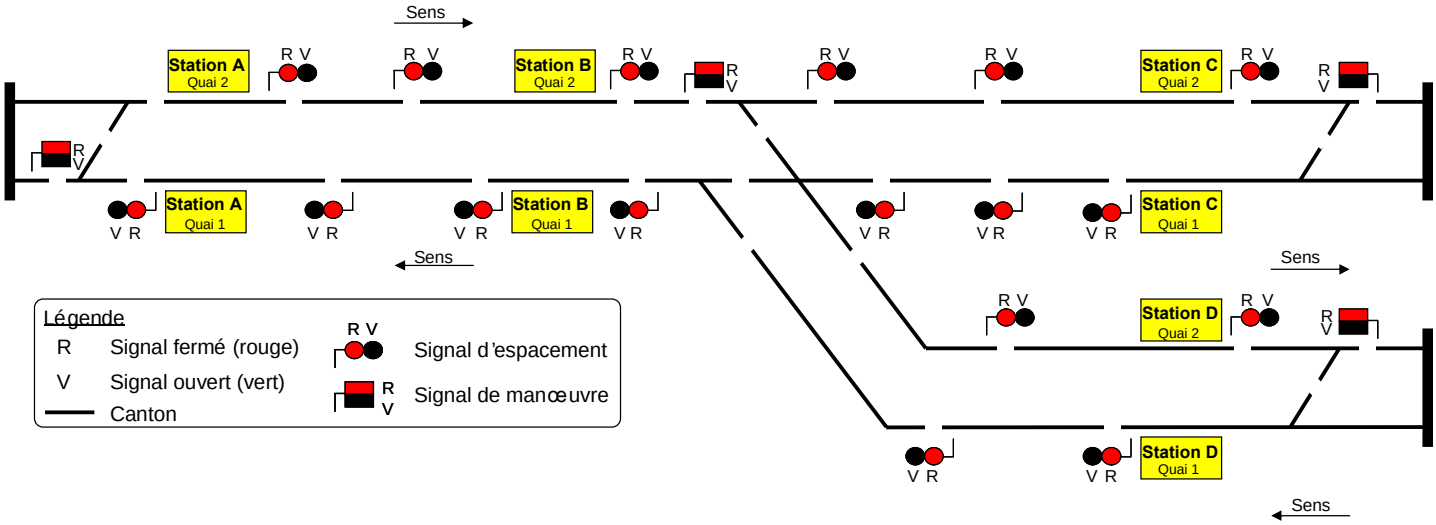


Figure 4.1 La cartographie du réseau du système de transport guidé étudié

Les paragraphes suivants détaillent les fonctionnalités du système étudié, celles-ci étant inspirées des spécifications fonctionnelles présentées dans le projet UGTMS [UGTMS D9 2004]. Le système se rapporte à un système qualifié d'ATC (*Automatic Train Control*, commande automatique des trains). Ces fonctionnalités sont réalisées par différents sous-systèmes de signalisation qui assurent la sécurité de la circulation des trains.

4.1.2 Les fonctionnalités liées au cantonnement

Comme indiqué au deuxième chapitre, le cantonnement permet d'éviter les collisions par rattrapage en imposant un et un seul train sur une section de voie appelée canton. Dans le système étudié, la ligne est divisée en cantons de longueur fixe. Chaque canton occupé est protégé par un block automatique lumineux composé d'un circuit de voie et d'un signal. Le système de transport guidé est considéré comme étant en milieu urbain, ce qui implique une faible longueur de cantons pour permettre la circulation d'un nombre important de trains sur la ligne, face à la forte densité de voyageurs.

Les signaux représentent la partie visuelle, sur voie, de la signalisation des transports guidés. Ceux-ci se déclinent en de nombreux aspects et formes qui sont différents selon les pays ou les modes de transport guidé. Ces différents aspects et formes sont associés à des procédures spécifiques que les conducteurs des trains doivent respecter. Le signal le plus simple

comporte deux aspects : *rouge* pour interdire le franchissement du signal par le train, il implique donc l'arrêt du train avant le signal par le conducteur, et *vert* pour donner la permission au conducteur de franchir le signal. Ces principes seront retenus pour notre système.

Le principe du cantonnement utilisé est illustré à la Figure 4.2. Cette figure montre clairement le fonctionnement des blocks automatiques lumineux suivant l'occupation des cantons par les trains qui évoluent de la situation 1 à la situation 3.

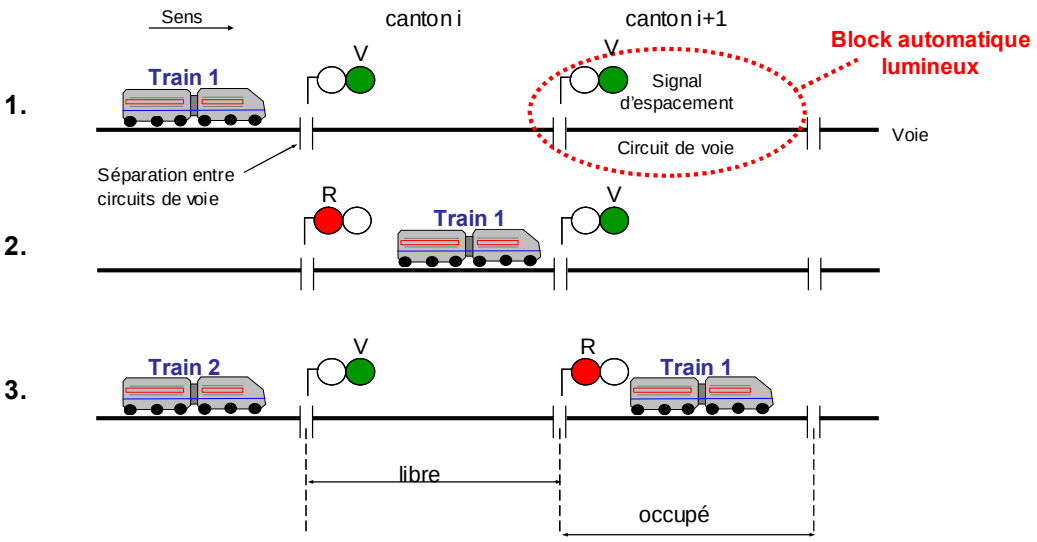


Figure 4.2 Principe du cantonnement

Dans certaines situations, un signal est placé plusieurs mètres en amont du canton qu'il protège pour assurer l'arrêt du train à la fin du canton, dans le cas où le signal montrant une indication d'arrêt aurait été franchi. La zone protégée selon ce principe est appelée section tampon ou zone de chevauchement. Elle existe notamment au niveau de la plupart des croisements ou bifurcations. Le paragraphe suivant fait référence à ces zones de chevauchement dans l'exposé des fonctionnalités du processus d'enclenchement d'itinéraires qui sécurise les sections comportant des voies sécantes.

4.1.3 Les fonctionnalités liées aux enclenchements d'itinéraires

L'enclenchement d'itinéraires est un processus gérant les itinéraires conflictuels des trains. Un itinéraire est formé d'un ensemble de sections de voie que doit emprunter le train pour atteindre la prochaine station prévue dans son parcours. Deux itinéraires sont conflictuels s'ils ont une section commune, lieu de collision potentielle. Dans le système étudié, cette situation

peut être rencontrée en différents endroits de la ligne: au niveau des changements de voie, et sur la zone mise en évidence à la Figure 1.1 représentant une ressource partagée par les trains.

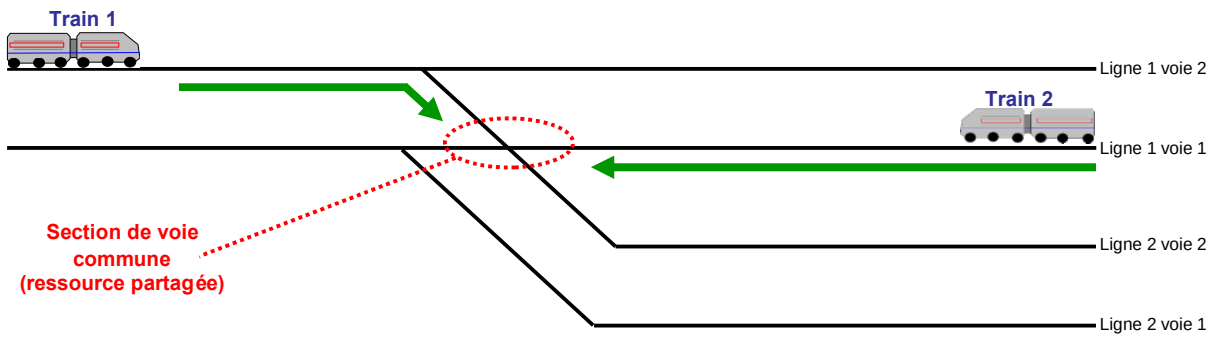


Figure 4.3 Itinéraires possédant une ressource partagée

Le processus d'enclenchement possède les différentes fonctions présentées ci-dessous, permettant la réservation et la libération d'un itinéraire:

- La commande de l'itinéraire de manière automatique ou de manière manuelle, étant donné l'action d'un aiguilleur sur une interface homme-machine (si un itinéraire sécant à celui-ci est déjà établi, l'itinéraire commandé est alors enregistré),
- La formation de l'itinéraire qui implique : la manœuvre des aiguilles aux intersections selon l'itinéraire prévu pour le train, le verrouillage des aiguilles pour éviter tout déraillement, et l'assurance que le positionnement de ces aiguilles est compatible avec l'itinéraire commandé,
- L'établissement de l'itinéraire qui autorise le franchissement de l'intersection par une ouverture du signal débutant l'itinéraire, si l'ensemble des conditions précédentes est réuni,
- La destruction de l'itinéraire qui provoque la fermeture du signal, une fois l'itinéraire parcouru, et supprime la formation de cet itinéraire.

De cette manière, un signal fermé protégeant le passage d'un train sur une intersection ne peut pas être ouvert pour le passage d'un autre train sur cette même intersection.

La Figure 4.4 illustre l'itinéraire commandé pour le train 1 et met en évidence les sections de voie sur lesquelles interviennent les fonctions de sécurité du système d'enclenchement gérant le processus d'enclenchement. Ces fonctions empêchent le train 2, en approche de l'intersection, d'emprunter la ressource partagée réservée au train 1.

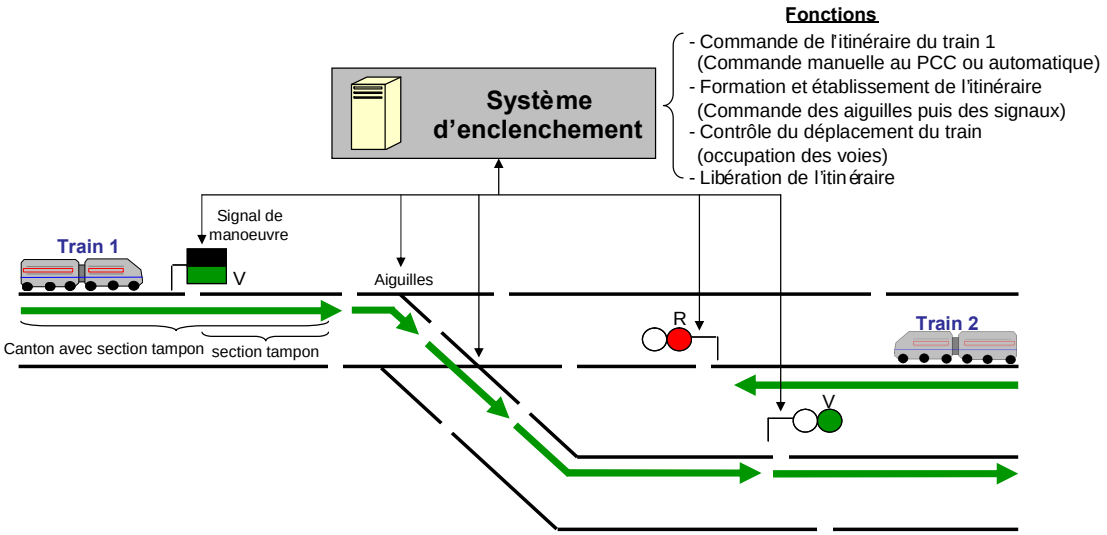


Figure 4.4 Gestion des conflits d'itinéraire par le système d'enclenchement

Le calcul du profil de vitesse jusqu'au prochain point d'arrêt du train est ici effectué par le sous-système bord qui tient compte des données d'autorisation de mouvement qui lui sont transmises. Le mode de transmission des données pris en compte dans le système étudié, depuis le sous-système sol jusqu'au sous-système bord, est détaillé dans le paragraphe suivant.

4.1.4 La transmission des données du sous-système sol au sous-système bord

Les circuits de voies, ayant pour fonction la détection des trains, permettent également la transmission continue aux trains (par modulation de fréquence) d'informations relatives à la voie. Ces informations englobent les commandes de restriction de vitesse, l'état du prochain signal lumineux (informations relatives aux autorisations de mouvement) et les données caractérisant la voie (courbures, déclivité, etc.). Les commandes de vitesse sont calculées par le sous-système sol selon la position des autres trains. Les données de vitesse émises par les circuits de voie sont reçues et décodées par les équipements des trains. Ceux-ci suivent et contrôlent la vitesse de consigne envoyée selon les caractéristiques propres du train (dimension, performances, etc.) et les données cinématiques calculées et mesurées (position relative du train, vitesse courante instantanée).

La Figure 4.5 illustre ces différentes fonctionnalités. Le calculateur bord (dénommé PES pour *Programmable Electronic System*) est considéré comme étant redondant. La gestion de l'ouverture et de la fermeture des portes se rapporte également à la sécurité des trains mais n'est pas modélisée par la suite, tout comme le système de diagnostic, les fonctionnalités

considérées étant déjà nombreuses. Ces deux dernières fonctionnalités sont toutefois représentées sur la Figure 4.5.

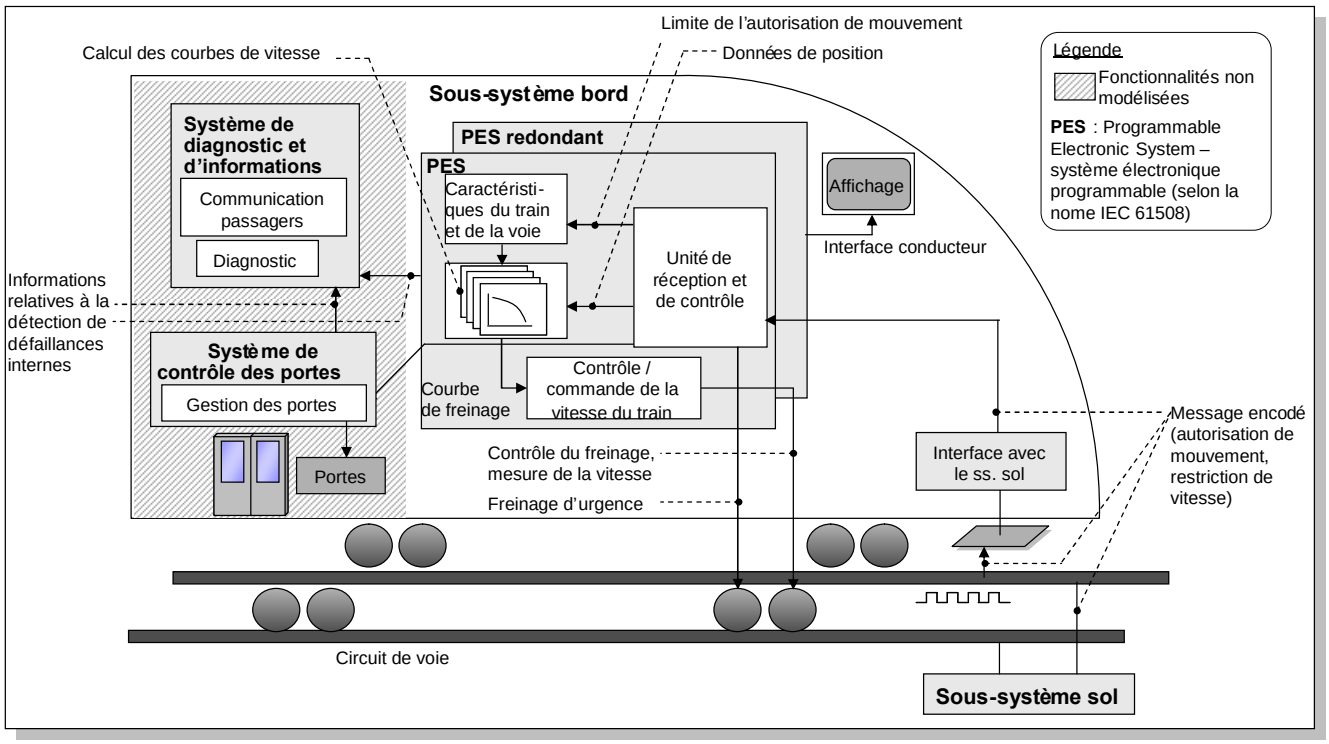


Figure 4.5 La transmission des données du sous-système sol ou sous-système bord

La deuxième partie de ce chapitre se consacre à la modélisation de ce système selon la démarche de modélisation basée sur le concept de situation d'exploitation, et détaille comment a été développée la maquette logicielle permettant la simulation de l'évolution dynamique du système modélisé.

4.2 Modélisation du système selon le concept de situation d'exploitation et développement de la maquette logicielle du système

4.2.1 L'instanciation des classes du modèle de situation d'exploitation

Comme exposé au troisième chapitre, la modélisation consiste au préalable en l'identification des différents objets constituant une situation d'exploitation du système de transport guidé analysé. Elle suppose à ce niveau une prise de vue statique du système dans son environnement c'est-à-dire que l'ensemble du système est considéré dans un état donné et figé sur le domaine d'exploitation qu'est la ligne de transport.

Le système de transport guidé possède plusieurs fonctionnalités identiques en raison de la présence de plusieurs éléments dupliqués à la fois dans le sous-système bord (les trains), et

dans le sous-système sol (les systèmes d'enclenchement contrôlant un sous-ensemble de l'ensemble des ressources partagées, les stations, les signaux). Pour éviter l'accumulation d'informations redondantes liées à la duplication des fonctions et donc pour ne pas alourdir la présentation des instances du modèle, le domaine d'exploitation peut être divisé en plusieurs sous-domaines, à l'intérieur desquels les fonctions sont non dupliquées. Cette division mène à la considération de situations d'exploitation sur lesquelles ne sont considérées que les fonctions ayant des rôles distincts et permet de simplifier l'analyse. Celles-ci sont appelées sous-situations d'exploitation. Les classes du modèle générique de situation d'exploitation peuvent alors être instanciées compte tenu de la prise en compte uniquement des sous-situations d'exploitation.

A l'aide de cette modélisation, les fonctions de sécurité à mettre en place pour minimiser les risques encourus sont mises en évidence. A noter que les opérateurs de conduite du système ne sont pas pris en compte dans le développement de la maquette logicielle, les classes *activités*, *équipe d'opérateurs* et *mode d'exploitation* ne seront instanciées qu'au travers d'exemples présentés en annexe D.

La classe « risque »

La classe risque précise les différents événements redoutés qui peuvent être rencontrés selon le contexte dépeint par la classe *contexte*, et selon les événements dangereux mis en évidence par la classe *événement dangereux*. Ils se rapportent aux événements redoutés exposés au deuxième chapitre, ces événements étant ici inscrits dans une situation d'exploitation donnée. Ceux-ci ayant été présentés au deuxième chapitre, ils ne sont pas rappelés ici.

La classe « zone dangereuse »

Toutes les zones sur lesquelles circulent les trains sont dangereuses *a priori*. Cette classe permet de lister ces différentes zones pour faciliter la recherche des événements dangereux. La Figure 4.6 liste les différentes zones identifiées dans le système étudié.

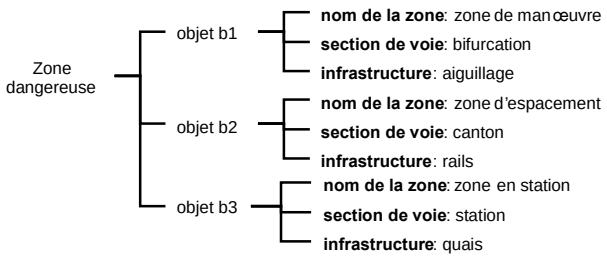


Figure 4.6 Instanciation de la classe « zone dangereuse »

La classe « contexte »

Différents contextes existent sur une situation d'exploitation du système. Ceux-ci sont répertoriés à l'aide de l'instanciation de la classe contexte, comme le montre l'exemple de la Figure 4.7.

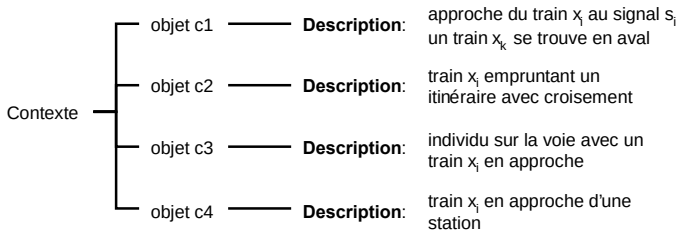


Figure 4.7 Exemple d'instanciation de la classe « contexte »

La classe « fonction de sécurité »

Les différentes fonctionnalités présentées dans la première partie de ce chapitre peuvent être résumées selon le Tableau 1.1 qui met en avant les fonctions de sécurité réalisées par les différents sous-systèmes considérés. La classe « fonction de sécurité » du modèle de situation d'exploitation est alors instanciée selon les objets décrits à la Figure 4.8.

Nom de la fonction de sécurité	Sous-système réalisant la fonction	Nom de la fonction de sécurité	Sous-système réalisant la fonction
F1 : Fonction d'enclenchement	(Dépend des sous-systèmes de F2, F3, et F4)	F8 : Calcul de la limite de vitesse du train	PES* bord 1 et 2 (sous-système redondant)
F2 : Détection et localisation du train	Circuit de voie	F9 : Contrôle du déplacement du train	(Dépend des sous-systèmes de F10, et F11)
F3 : Attribution et détermination de l'autorisation de mouvement	PES* sol	F10 : Contrôle de la vitesse du train	PES* bord 1 et 2 (sous-système redondant)
F4 : Formation et établissement de l'itinéraire	Signaux et aiguillages	F11 : Contrôle de la position du train	PES* bord 1 et 2 (sous-système redondant)
F5 : Gestion de l'autorisation de mouvement par le train	Antenne de réception	F12 : Commande du freinage d'urgence	Équipement du train
F6 : Commande de la vitesse du train bord	(Dépend des sous-systèmes de F5, F7, et F8)	F13 : Déclenchement du freinage d'urgence	Équipement du train
F7 : Commande de la vitesse du train sol	(Dépend des sous-systèmes de F2 et F3)	F14 : Freinage de service	Équipement du train
		F15 : Freinage d'urgence	(Dépend des sous-systèmes de F12 et F13)

*Programmable Electronic System (système programmable électronique)

Tableau 4.1 Relations d'association entre les fonctions de sécurité et les sous-systèmes employés

Certaines de ces fonctions de sécurité (F1, F6, F7, F9, F15) ne sont opérationnelles que si les fonctions de sécurité dont elles dépendent le sont également. Leur SIL dépend donc de la combinaison de ces autres fonctions de sécurité. A noter que les SILs des différentes fonctions ont été fixés *a priori* par comparaison des SILs fixés dans le projet UGTMS [UGTMS D6 2003].

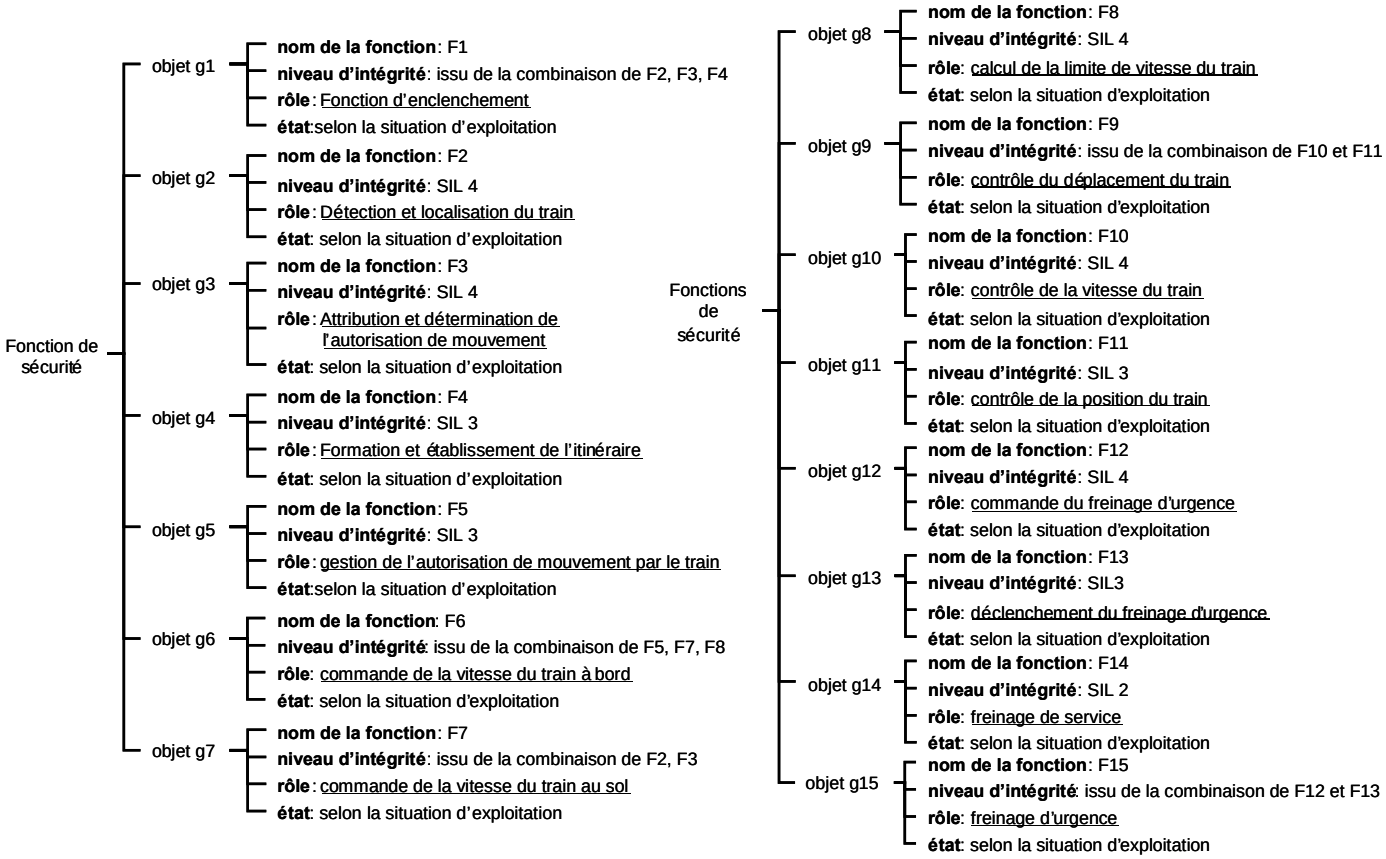


Figure 4.8 Instanciation de la classe « fonction de sécurité »

La classe « sous-système »

Les relations d'association qui existent entre les objets « fonctions de sécurité » et les objets « sous-systèmes » apparaissent dans le Tableau 1.1. Le détail de ces objets appartenant à la classe « sous-système » est présenté à la Figure 4.9. Cette classe met ainsi en évidence les choix de conception retenus ou envisagés pour assurer la sécurité.

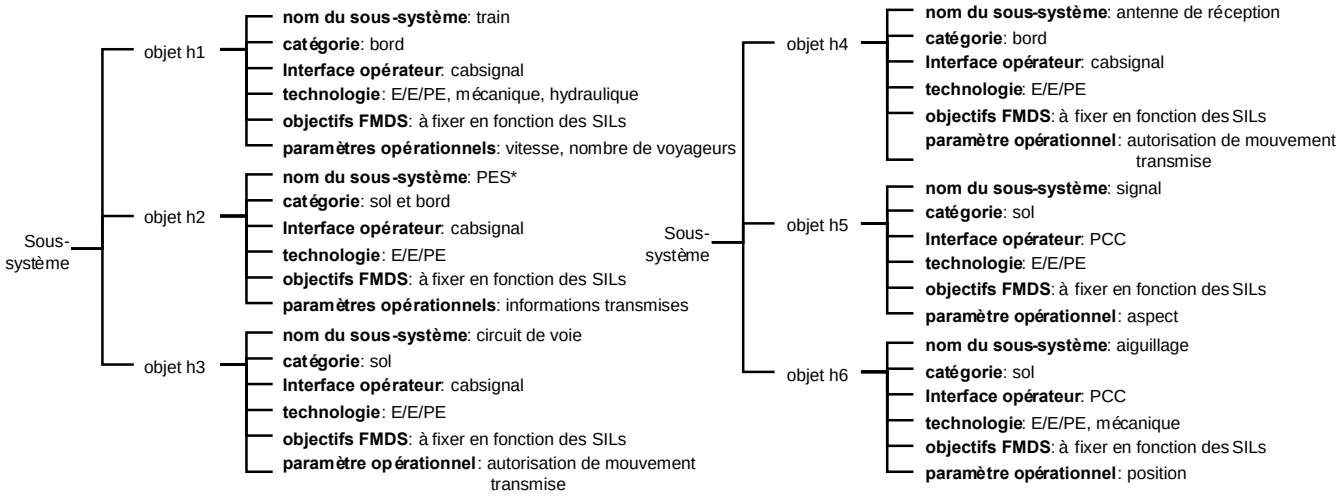


Figure 4.9 Instanciation de la classe « sous-système »

La classe « événement dangereux »

Les différents objets relatifs à cette classe intègrent des événements dangereux issus des classes *zone dangereuse*, *sous-système*, *opérateur*, et *contexte*, classes en association avec la classe *événement dangereux*. La Figure 4.10 illustre différents événements dangereux originaires de ces quatre classes. Ces événements dangereux sont de nature externe au système, tels les événements provenant d'une zone dangereuse particulière ou de l'environnement en général, ou de nature interne, tels les événements provenant des défaillances des différents sous-systèmes réalisant les fonctions de sécurité.

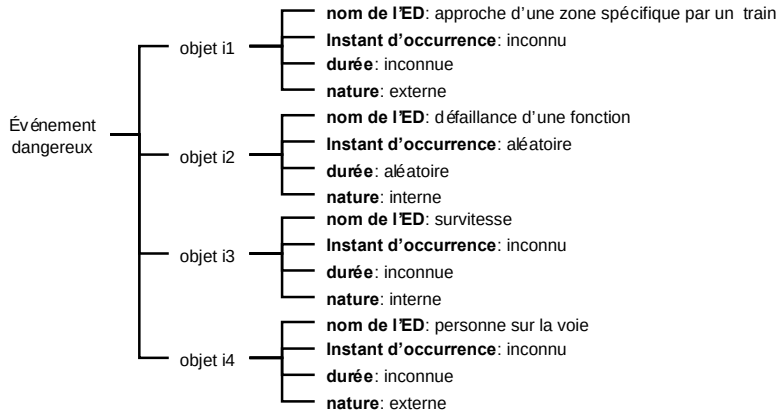


Figure 4.10 Exemple d'instanciation de la classe « événement dangereux »

Les attributs de type « durée » dont la valeur est « inconnue » se rapportent à des valeurs pouvant être mesurées lors des expérimentations effectuées sur le modèle. Ceux dont la valeur est « aléatoire » se rapportent aux événements de défaillances des fonctions de sécurité générés aléatoirement par l'approche de simulation de Monte Carlo dont la mise en œuvre est détaillée ci-dessous.

4.2.2 La génération dans le temps de défaillances dangereuses du système par simulation de Monte Carlo biaisée

4.2.2.1 La prise en compte des dépendances des fonctions de sécurité

Les dépendances entre les fonctions de sécurité mises en évidence lors de la définition des objets *fonctions de sécurité* et *sous-systèmes* peuvent s'exprimer selon les conditions logiques de la Figure 4.11 soulignant les fonctions de sécurité du sous-système bord et les fonctions de sécurité du sous-système sol. Chaque condition représente la structure d'une fonction de sécurité selon la combinaison logique d'autres fonctions de sécurité.

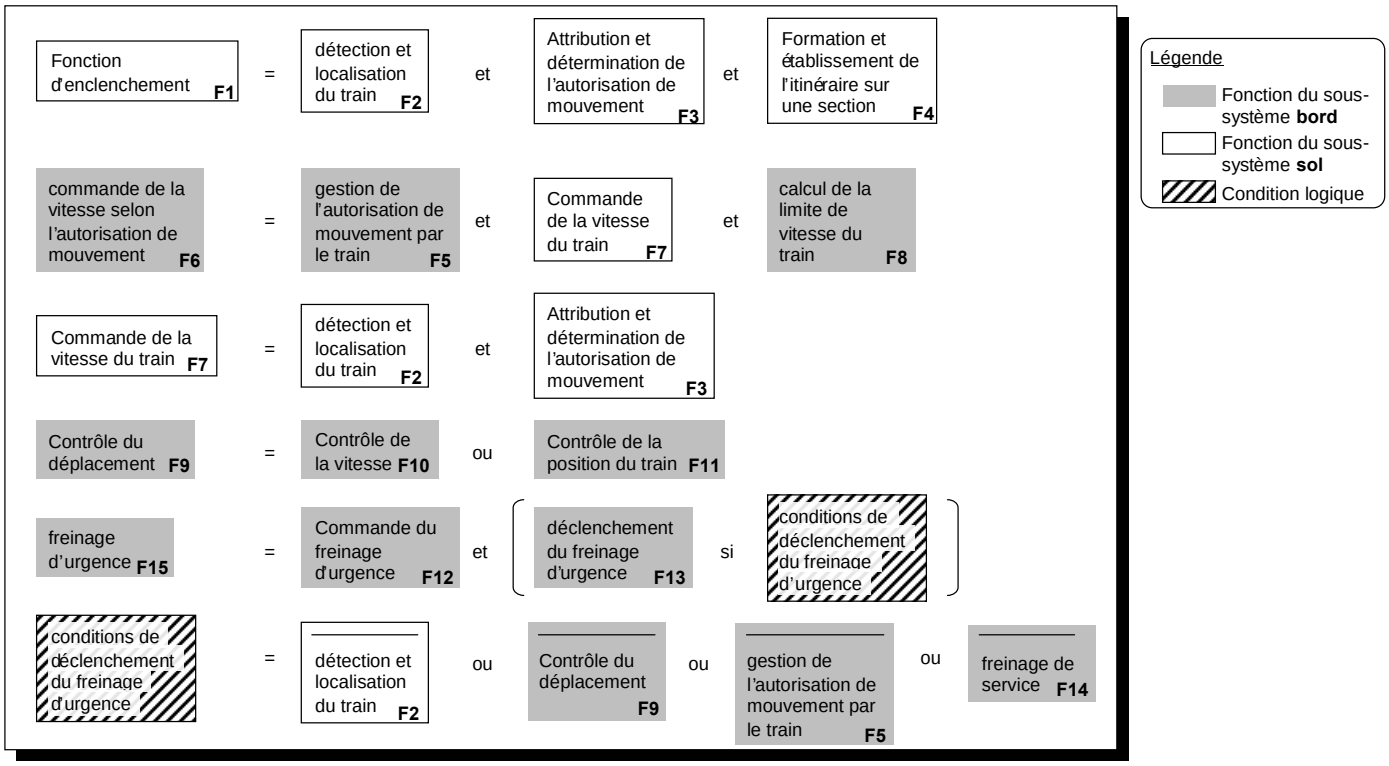


Figure 4.11 Dépendances entre les fonctions de sécurité

La fonction de structure du système, ou plus exactement le vecteur de fonctions de structure du système, peut alors s'exprimer selon l'équation (4.1).

$$\begin{pmatrix} F1 \\ F6 \\ F7 \\ F9 \\ F15 \end{pmatrix} = \begin{pmatrix} F2.F3.F4 \\ F5.F7.F8 \\ F2.F3 \\ F10 \text{ ou } F11 \\ F12.(F13 \text{ si conditions}) \end{pmatrix} = \begin{pmatrix} F7.F4 \\ F5.F7.F8 \\ F2.F3 \\ F10 \text{ ou } F11 \\ F12.(F13 \text{ si conditions}) \end{pmatrix} \tag{4.1}$$

avec : $conditions = \overline{F2} \text{ ou } \overline{F9} \text{ ou } \overline{F5} \text{ ou } \overline{F14}$

La présence de plusieurs fonctionnalités identiques dans le système, liée à la présence de plusieurs sous-systèmes bord (les trains) et de plusieurs sous-systèmes sol contrôlant différentes sections de voie, implique la duplication de chaque fonction de sécurité du vecteur (4.1). Le paragraphe suivant détaille comment cette duplication est prise en compte.

4.2.2.2 La prise en compte de la duplication des fonctions de sécurité

Les fonctions du *sous-système bord* sont dupliquées selon le nombre de trains intervenant dans le système. Six trains circulent ici sur la ligne de transport.

Les fonctions du *sous-système sol* sont dupliquées selon le nombre de sections existantes. Une section se rapporte à la zone formée par l'ensemble des itinéraires possibles passant par une et une seule ressource partagée. Le découpage en sections permet une gestion séparée des ressources grâce à plusieurs systèmes d'enclenchement, chacun d'entre eux commandant les signaux et les aiguilles d'une unique section. Dans le système étudié, quatre sections sont considérées en raison de la présence de quatre ressources partagées : les trois intersections de changement de voie, et l'intersection précédemment évoquée à la Figure 1.1.

Certaines fonctions dépendant à la fois du sous-système bord et du sous-système sol sont dupliquées selon le nombre de trains multiplié par le nombre de sections telles les fonctions F2, F6, et F7. L'ensemble des fonctions existantes, ainsi que leurs dépendances codées selon l'équation de structure (4.1), sont présentées en **Annexe E**.

4.2.2.3 Mise en œuvre de la simulation de Monte Carlo biaisée

La simulation de Monte Carlo (SMC) biaisée utilisée est développée en langage C selon l'algorithme fourni en annexe A. L'occurrence d'un événement dangereux coïncidant avec la défaillance d'une fonction de sécurité est liée au SIL de la fonction, plus précisément au paramètre quantitatif du SIL. Ce dernier correspond à un intervalle de taux de danger tolérables THR (Tolerable Hazard Rates). Les bornes de l'intervalle de THR de chaque fonction sont uniquement prises en compte dans l'exécution de l'algorithme. Elles représentent des taux de valeurs extrêmement faibles qui vont faire l'objet du biaisage. La remise en état de chacune des fonctions après défaillance est prise en compte avec un taux de réparation de 1/24 h^{-1} (en considérant qu'une réparation prend en moyenne une journée).

L'algorithme de SMC, dédié à l'évaluation statistique d'événements redoutés, génère plusieurs histoires dans lesquelles apparaissent des événements dangereux à des instants donnés, ces histoires étant ici retranscrites sous forme de fichiers de données. Une histoire correspond à un fichier dans lequel sont enregistrés uniquement les instants de défaillances de chacune des fonctions de sécurité sur l'intervalle de temps [0 h , 350640 h] (40 ans, temps moyen d'exploitation en transport guidé). La simulation du contexte opérationnel intégrant ces données va maintenant être détaillée.

4.2.3 La simulation du contexte opérationnel intégrant des événements dangereux

4.2.3.1 Présentation de la maquette logicielle reproduisant le fonctionnement du système

La maquette logicielle a été développée au moyen du progiciel de simulation par événements discrets (SED) *Arena 8*. La construction du modèle du système de transport guidé dans ce progiciel a consisté en premier lieu à modéliser le fonctionnement du système. Pour cela, le réseau de transport guidé a été créé selon les dimensions présentées à la Figure 4.12. Les sections comportant une et une seule ressource partagée y figurent également. Ensuite la gestion du mouvement des trains, fonction : du trajet de chaque train vers la station C ou la station D, de la vitesse (vitesse moyenne à 70 km), de l'accélération et de la décélération des trains ; et la gestion des signaux, fonction : de l'occupation des voies et des arrêts en station, a été développée dans différents sous-modèles selon la programmation par blocs d'Arena.

La modélisation des dysfonctionnements du système menant à des situations dangereuses, plus précisément la modélisation du comportement du système lors de l'occurrence de défaillances dangereuses des fonctions de sécurité (aux temps indiqués dans les fichiers issus de la simulation de Monte Carlo), fait l'objet du paragraphe suivant.

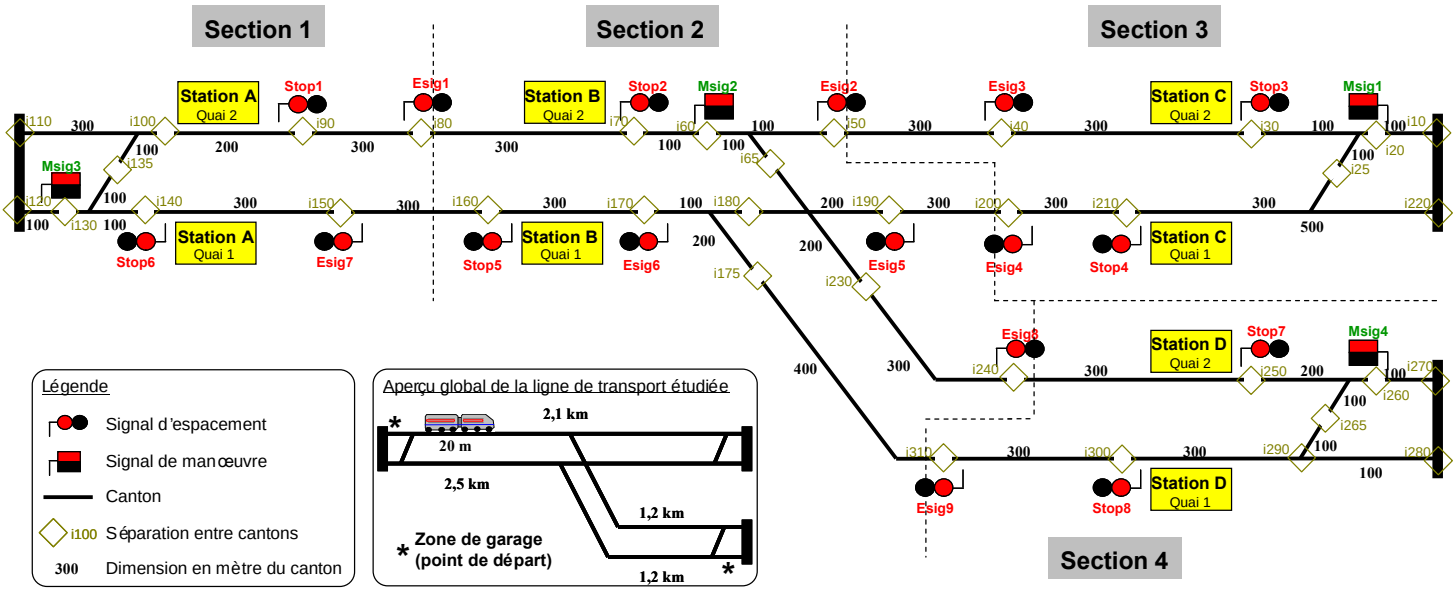


Figure 4.12 Maquette logicielle du système

4.2.3.2 L'influence des défaillances dangereuses sur la simulation de la maquette logicielle

Le modèle du système simulé par SED est conçu pour réagir aux défaillances des fonctions de sécurité, événements dangereux du modèle de situation d'exploitation de nature interne. Le système simulé ne se comportera pas de la même manière selon par exemple, l'occurrence de la défaillance de la fonction d'enclenchement, de la fonction de commande de la vitesse à bord ou de la fonction du freinage d'urgence.

Dans le premier cas, la défaillance de la fonction d'enclenchement mène à l'événement dangereux correspondant à la création de deux itinéraires qui peuvent être conflictuels.

Dans le deuxième cas, la défaillance de la fonction de commande de la vitesse à bord mène à la modification de la vitesse du train. Cette modification change la vitesse normale du train en une vitesse qui peut être potentiellement dangereuse lorsque cette vitesse est supérieure à la vitesse autorisée, l'arrêt des trains aux signaux fermés n'étant alors plus garanti.

Dans le troisième cas relatif à la défaillance de la fonction de freinage d'urgence, la simulation doit vérifier au préalable que cette fonction ait été déclenchée selon les conditions exposées au paragraphe 4.2.2.1. Si elle a été déclenchée, le train a normalement changé immédiatement sa vitesse en une vitesse nulle. Si elle a été déclenchée en étant défaillante, aucune modification de vitesse n'est effectuée.

La partie suivante de ce chapitre présente les résultats des expérimentations effectuées sur la maquette logicielle du système de transport guidé étudié et les conclusions quant à la sécurité de ce système.

4.3 Identification et évaluation des scénarios obtenus par simulation

4.3.1 Les profils de risque établis a priori

Selon les fonctions de sécurité considérées, différents profils de risque peuvent être établis *a priori*. En effet, les fonctions de sécurité ont été conçues dans un but donné qui suppose la prise en compte préalable de différents scénarios de risque pouvant se produire. Ces différents profils de risque selon la représentation du diagramme de causes-conséquences sont illustrés dans les Figures 4.13, 4.14 et 4.15. Dans ces figures, les événements initiateurs extérieurs sont notés EIX, et se déclinent selon les événements initiateurs EIX_i suivants:

- EIX_1 : approche d'un signal d'espacement par un train.
- EIX_2 : approche d'un signal d'espacement par un train, un autre train se trouve en aval.
- EIX_3 : approche, par un train, du signal de manoeuvre précédant une intersection.
- EIX_4 : approche, par un train, du signal de manoeuvre précédant une intersection, un autre train se trouve en aval.
- EIX_5 : arrivée d'un train en station (dans ce cas, le train est annoncé et les voyageurs en station doivent se reculer des bords des quais).

Les scénarios envisagés à la Figure 4.13 se rapportent aux fonctions de sécurité employées lors de la gestion de l'espacement entre trains. Ces scénarios peuvent être initiés par EIX_1, EIX_2 ou EIX_5.

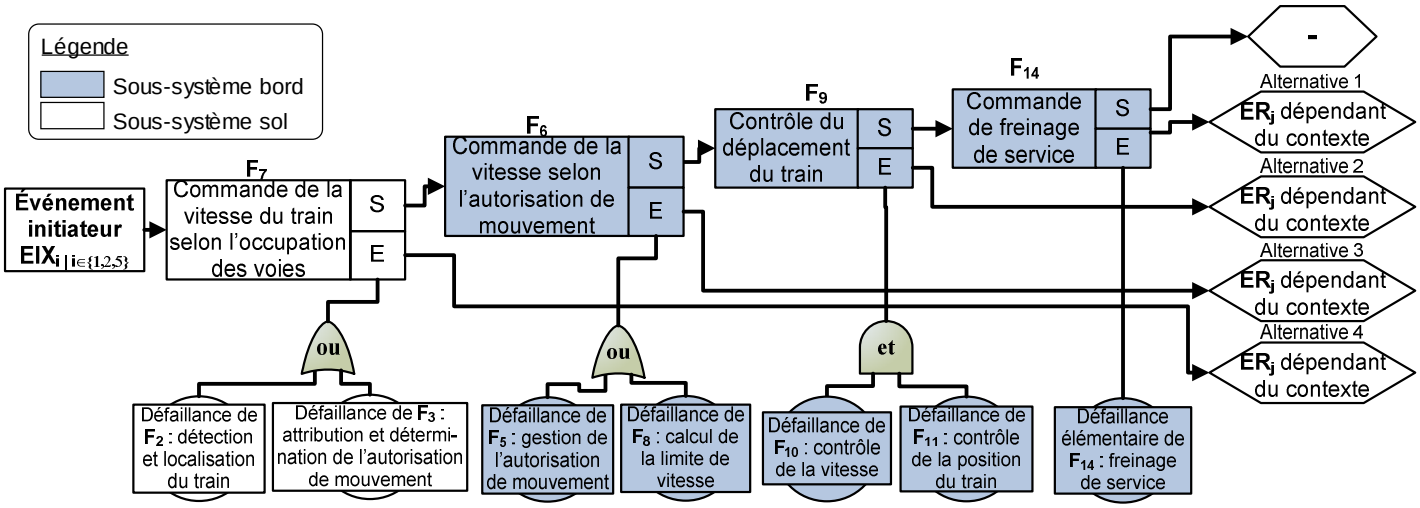


Figure 4.13 Profils de risque relatifs à l'espacement entre train

La Figure 4.14 représente, de manière séparée par rapport aux autres scénarios, la prise en compte du freinage d'urgence, celui-ci n'étant déclenché que sous certaines conditions de défaillance des fonctions de sécurité (conditions rappelées dans la figure). L'ensemble des événements initiateurs $EIX_{i \mid i=\{1..5\}}$ peuvent être suivis d'un freinage d'urgence.

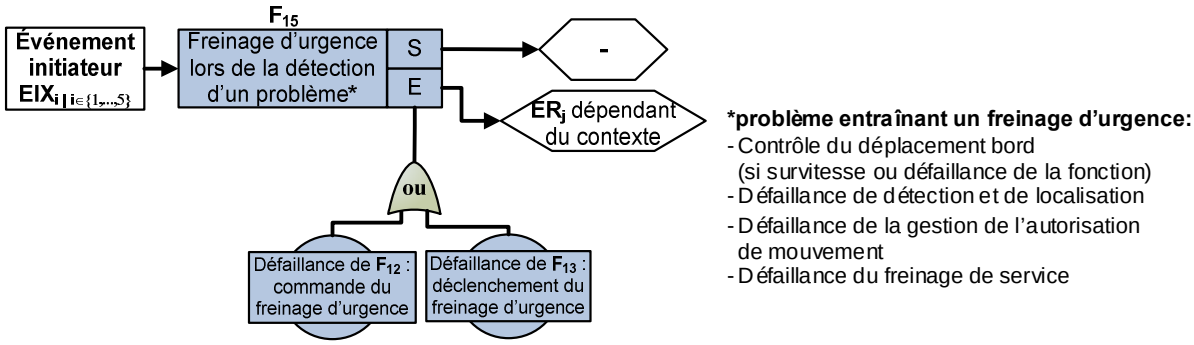


Figure 4.14 Profils de risque relatifs à l'activation du freinage d'urgence

Les scénarios envisagés à la Figure 4.15 se rapportent aux fonctions de sécurité employées lors de la gestion de l'accès aux intersections compte tenu des itinéraires affectés aux différents trains. Ces scénarios peuvent être initiés par EIX_3 ou EIX_4.

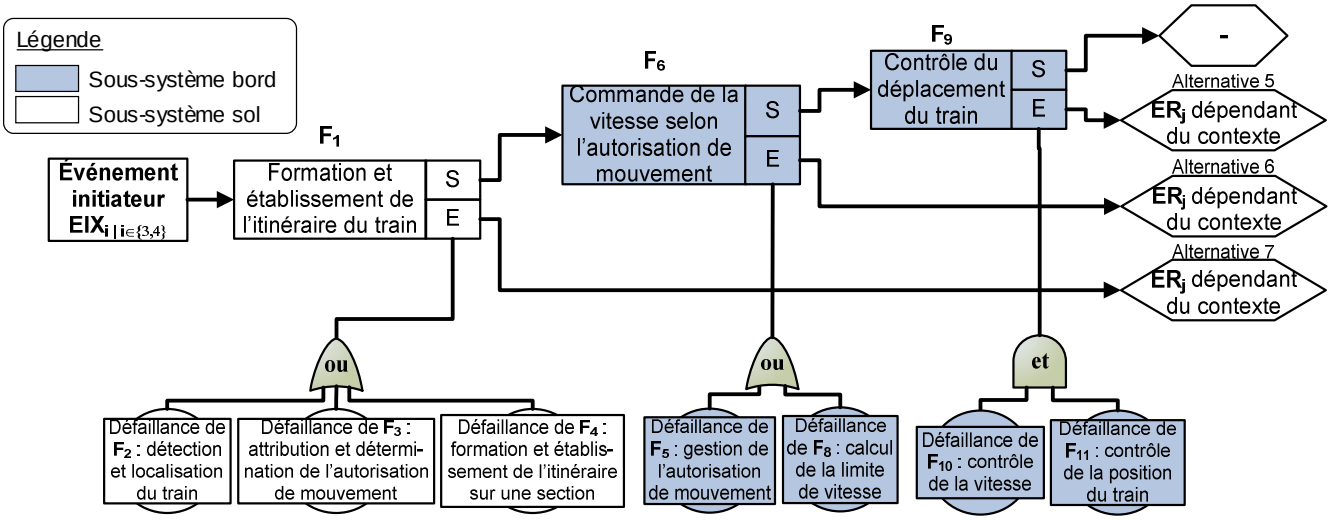


Figure 4.15 Profils de risque relatifs à l'accès d'une intersection

Les événements initiateurs peuvent évoluer selon différentes alternatives vers des événements redoutés notés ER_j. Un ER lié à une alternative donnée n'est pas précisé dans les figures précédentes. En effet, la séquence d'événements formant l'alternative peut ne pas aboutir au même ER selon la configuration spatiale dans laquelle se trouve le système (position des trains sur une section donnée) et la valeur des paramètres opérationnels du système (telle la vitesse des trains).

Selon la Figure 4.13 et la Figure 4.15, ces alternatives sont au nombre de sept. Les événements de la Figure 4.14 ne sont pas inclus dans des alternatives distinctes car leur occurrence est liée aux événements des sept alternatives mentionnées.

Les ER_j potentiels pouvant être identifiés *a priori*, sont présentés au Tableau 4.2. Ces ER_j ($j \in \{1,\ldots,7\}$) dépendent des paramètres opérationnels de position et de vitesse des différents trains présents dans le système. Les alternatives 1 à 4 peuvent s'achever par $ER_{j \mid j \in \{1,2,3,4,5\}}$ et les alternatives 5 à 7 peuvent s'achever par $ER_{j \mid j \in \{1,3,6,7\}}$.

Événement initiateur	Freinage d'urgence activé	Vitesse faible du train en approche du signal	Vitesse élevée du train en approche du signal	Vitesse élevée du train en approche de la station
EIX_1: Approche d'un signal d'espacement par un train	—	ER_1: Franchissement du signal	ER_1: Franchissement du signal	ER_2: Franchissement du signal, dommages humains en station
EIX_2: Approche d'un signal d'espacement par un train, un autre train se trouve en aval	—	ER_3: Franchissement du signal, collision vitesse réduite	ER_4: Franchissement du signal, collision avec nombreux dommages matériels	ER_5: Franchissement du signal, dommages matériels et humains en station (quelle que soit la vitesse)
EIX_3: Approche par un train du signal de manoeuvre précédant une intersection	—	ER_1: Franchissement du signal	ER_6: Franchissement du signal, déraillement	
EIX_4: Approche par un train du signal de manoeuvre précédant une intersection, un autre train se trouve en aval	—	ER_3: Franchissement du signal, collision vitesse réduite	ER_7: Franchissement du signal, déraillement avec nombreux dommages matériels	
EIX_5: Arrivée d'un train en station	—			ER_2: dommages humains en station

Tableau 4.2 Événements redoutés pouvant se produire selon l'occurrence d'un événement initiateur donné

A noter que les dépendances entre événements se retrouvent dans ces différentes alternatives. Par exemple, la défaillance de certaines fonctions de sécurité va aboutir à l'activation du freinage d'urgence du train concerné, ou encore, une fonction de sécurité peut intervenir dans plusieurs profils de risque.

Les expérimentations menées et détaillées ci-dessous portent d'abord sur l'analyse probabiliste à l'aide de la SMC biaisée de chacun des profils de risque mis en avant ci-dessus, sans la prise en compte du contexte opérationnel (10000 simulations sont effectuées). Cette étape permet d'envisager quelles valeurs probabilistes relatives aux exigences de SIL peuvent être intéressantes à analyser lors de la considération du contexte opérationnel.

Ensuite, plusieurs simulations du contexte opérationnel (au nombre de 500), celles-ci intégrant les événements contenus dans les histoires générées par la SMC biaisée, sont effectuées. Chaque simulation conduit ou non à différents événements redoutés dont les conditions d'occurrence sont analysées qualitativement pour identifier les scénarios survenus et les comparer aux alternatives présentées ci-dessus. L'analyse quantitative de ces événements redoutés conduit ensuite à l'évaluation probabiliste de la sécurité du système de transport guidé.

4.3.2 Evaluation préalable : analyse quantitative sans prise en compte du contexte opérationnel

Cette première évaluation consiste à déterminer uniquement, à l'aide de la SMC biaisée, l'évolution de la probabilité sur 40 ans de chacune des alternatives présentées ci-dessus. Le nombre d'histoires simulées est fixé à 10000.

A ce niveau, les résultats fournis permettent de donner, de manière rapide, un aperçu sur les grandeurs probabilistes concernant la sécurité, grandeurs réévaluées par la suite en tenant compte du contexte opérationnel. Ces évaluations ultérieures étant beaucoup plus longues à mettre en œuvre (cf. 4.3.4.1), cette étape initiale permet également de cibler les configurations d'exigences de SIL intéressantes à prendre en compte pour l'évaluation globale de sécurité.

L'évaluation des différentes alternatives est établie sans la prise en compte de la duplication des fonctions de sécurité, et en utilisant les exigences de SIL suivantes:

- cas 1 : configuration avec les exigences de SIL initialement considérées (cf. Figure 4.8 établissant les SILs des différentes fonctions par comparaison avec l'allocation des SILs utilisée dans le projet UGTMS [UGTMS D6 2003]), la borne minimale des THR étant considérée,
- cas 2 : configuration avec les exigences de SIL initialement considérées, la borne maximale des THR étant considérée,
- cas 3 : configuration avec des exigences de SIL d'un niveau immédiatement inférieur aux exigences de SIL initialement considérées (par exemple, les fonctions de SIL 4 sont analysées comme ayant un SIL3), la borne minimale des THR étant considérée,
- cas 4 : configuration avec des exigences de SIL d'un niveau immédiatement inférieur aux exigences de SIL initialement considérées, la borne maximale des THR étant considérée.

Les cas 2 et 3 sont identiques étant donné que les valeurs de THR minimales d'un niveau de SIL donné, correspondent aux valeurs maximales du niveau de SIL suivant (exemple : $THR_{min\ SIL3} = THR_{max\ SIL4}$).

Plusieurs points sont d'abord à souligner sur l'obtention des résultats statistiques fournissant les courbes de probabilité pour chaque alternative par simulation de Monte Carlo biaisée (la Figure 4.16 prend en exemple l'alternative 6 du cas 4) :

- Les courbes présentent une variance mauvaise caractérisée par une très grande étendue des valeurs visible par l'emploi d'une échelle logarithmique (Figure 4.16.b), celle-ci comportant des puissances de 10 négatives (les puissances négatives les plus élevées étant très peu représentatives car équivalentes à 0). En fait, les configurations de défaillances favorisées par l'algorithme de biaisage sont associées à un poids statistique plus petit que 1 et qui tend vers 0 au fur et à mesure du déroulement de la simulation, contrairement aux configurations défavorisées pouvant avoir un poids plus grand que 1. Ces poids détériorent les résultats statistiques.

- La variance peut difficilement être réduite car l'algorithme de biaisage est fortement dépendant de plusieurs paramètres dont la valeur est délicate à fixer. Un premier paramètre concerne le pas de discrétisation. Lorsque ce dernier est trop large, il ne permet pas de considérer tous les changements d'états et donc certaines occurrences qui pourraient contribuer aux statistiques ne sont pas prises en compte. Lorsqu'il est trop petit il pénalise fortement la durée de simulation (un pas de 2h a ici été considéré). Un second type de paramètre concerne les paramètres directement liés au biaisage. Lorsque le biaisage est trop prononcé, les poids statistiques distordent trop l'information recherchée, lorsqu'il est peu prononcé, pas assez d'événements se produisent.

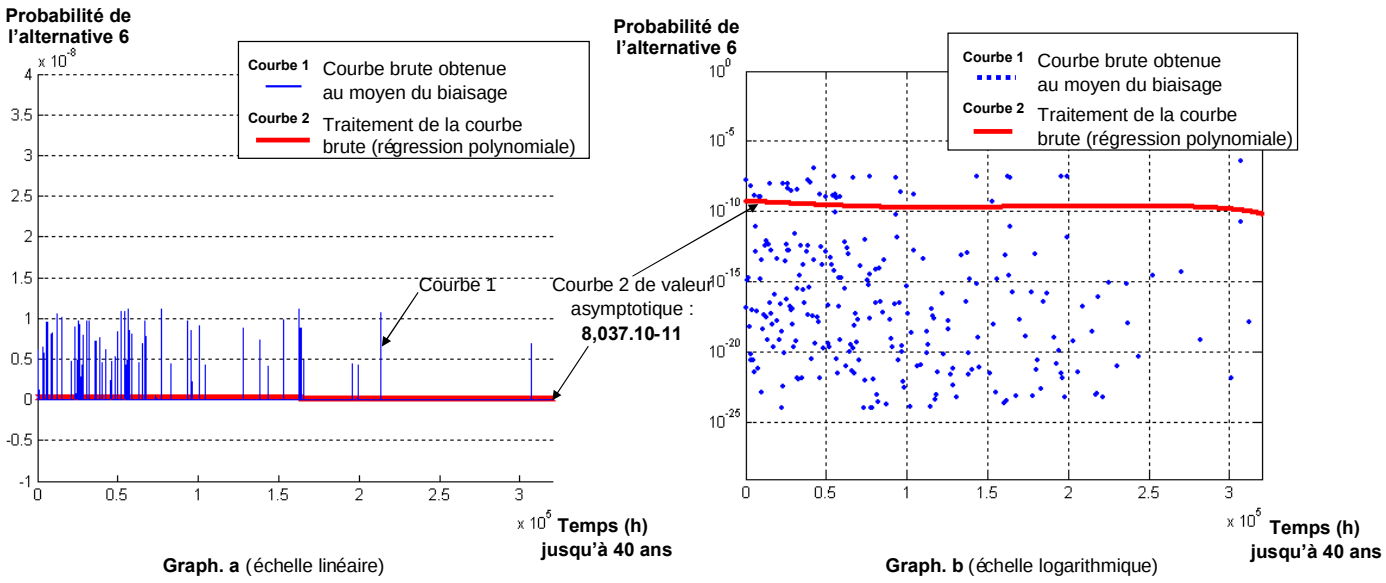


Figure 4.16 Probabilité obtenue pour l'alternative 6 (cas 4)

- Cette mauvaise variance ne permet pas d'obtenir immédiatement l'information recherchée. Différents tests ont été effectués sur les courbes obtenues par SMC biaisée pour des configurations de fonctions des sécurité plus simples (2 et 3 fonctions en association), dont les calculs de probabilité ont pu être effectués analytiquement et dont les grandeurs de fiabilité sont identiques aux cas étudiés (taux de défaillance très faibles liés aux SILs, et taux de réparation élevés de 1/24 h^{-1}, amenant immédiatement à des probabilités asymptotiques sans période de transition). Les techniques de régression polynomiale appliquées sur les courbes obtenues pour les configurations simples concordent avec les résultats analytiques. Ces techniques ont donc été employées ici pour les configurations plus complexes. L'information contenue dans les courbes peut ainsi être mise en avant comme le monte la Figure 4.16.

Compte tenu de ces remarques, le Tableau 4.3 présente les différents résultats obtenus concernant la valeur asymptotique des courbes pour chaque alternative de chacun des cas considérés.

Alternative	**n° 1** $F_7.F_6.F_9.\overline{F_{14}}.\overline{F_{15}}$	**n° 2** $F_7.F_6.\overline{F_9}.\overline{F_{15}}$	**n° 3** $F_7.\overline{F_6}.\overline{F_{15}}$	**n° 4** $\overline{F_7}.\overline{F_{15}}$	**n° 5** $F_1.F_6.\overline{F_9}.\overline{F_{15}}$	**n° 6** $F_1.\overline{F_6}.\overline{F_{15}}$	**n° 7** $F_1.\overline{F_{15}}$
cas 1	$3.984*10^{-13}$	–	$1.923*10^{-13}$	$5.27*10^{-15}$	–	$1.923*10^{-13}$	$5.27*10^{-15}$
cas 2,3	$4.908*10^{-11}$	–	$3.167*10^{-11}$	$1.262*10^{-12}$	–	$3.167*10^{-11}$	$1.262*10^{-12}$
cas 4	$1.994*10^{-9}$	–	$8.037*10^{-11}$	$7.777*10^{-12}$	–	$8.037*10^{-11}$	$7.736*10^{-12}$

Tableau 4.3 Evaluation préalable sans prise en compte du contexte opérationnel

La simulation de Monte Carlo même biaisée ne fournit aucun résultat pour les alternatives 2 et 5. Celles-ci ont en commun la défaillance de la fonction F9 (contrôle du déplacement du train) qui est issue de l'association de deux fonctions bord : F10 (contrôle de la vitesse) et F11 (contrôle de position). Ces deux fonctions possèdent chacune une redondance liée à la redondance du calculateur bord. La redondance de ces fonctions ayant un taux de défaillance très faible, implique une faible occurrence de défaillance de la fonction F9 par rapport aux autres fonctions de sécurité, d'où une évaluation qui n'aboutit pas à un résultat exploitable.

Pour pouvoir apprécier ces résultats, il est nécessaire de définir un critère d'acceptation du risque avec lequel les évaluations de sécurité pourront être comparées. Au second chapitre, plusieurs principes d'acceptation du risque dans le domaine des transports guidés ont été présentés. Le principe MEM (*Mortalité Endogène Minimale*) délivre en particulier un critère probabiliste explicite d'acceptation du risque. Celui-ci se réfère, pour un nombre de victimes

de une à une centaine de personnes, à une occurrence acceptable de 10^{-5} accidents par an, soit $1{,}15.10^{-9}$ accidents par heure. Afin de définir, dans cette étude, un critère d'acceptation du risque du même ordre, la disponibilité d'une fonction de sécurité de SIL 4 (THR $\in[10^{-9}$; $10^{-8}[$) est adoptée comme critère, cette disponibilité étant comprise entre les valeurs de probabilité $2{,}4.10^{-8}$ et $2{,}4.10^{-7}$ pour un taux de réparation de $1/24\,h^{-1}$, en utilisant la distribution exponentielle. L'intervalle $[2{,}4.10^{-8}$; $2{,}4.10^{-7}]$ représente donc l'intervalle de probabilité dans lequel la valeur de la probabilité d'un événement redouté, pour un instant donné, doit se situer. La borne supérieure $2{,}4.10^{-7}$ peut, en fait, uniquement être considérée en tant que critère d'acceptation du risque, les valeurs de probabilité des événements redoutés qui lui sont inférieures étant acceptables.

Les valeurs de probabilité du Tableau 4.3 sont toutes inférieures au critère d'acceptation du risque venant d'être défini, même pour la configuration du cas 4 prenant en compte la borne maximale des exigences de SIL d'un niveau immédiatement inférieur aux exigences de SIL initialement considérées dans le début du chapitre. Cependant, ces valeurs concernent la probabilité qu'une alternative donnée se produise et non la probabilité qu'un événement redouté issu de ces alternatives se produise, sachant que, comme analysé précédemment, plusieurs alternatives différentes peuvent aboutir au même type d'événement redouté.

En conclusion, la combinaison des 15 fonctions de sécurité formant une structure complexe de par leurs interactions et menant à différentes alternatives de risques, conduit à un risque acceptable en ne tenant pas compte de l'environnement d'exploitation du système. Cette conclusion est valable pour les exigences de SILs considérées dans les quatre cas présentés ci-dessus.

L'évaluation de sécurité qui suit, se rapporte à la prise en compte, dans les simulations, du contexte opérationnel dans lequel évolue le système de transport guidé. Elle analyse le système selon les exigences de SIL du cas 2-3 (les cas 2 et 3 étant identiques), et du cas 4 pour délivrer des probabilités d'accident différenciées selon les événements redoutés qui se produisent. Le cas 1 se rapportant aux exigences de SIL initialement prévues avec les bornes minimales des THR associés au SIL, n'est pas considéré à se stade puisque le cas 2 associé aux bornes maximales des THR pour ces mêmes exigences, délivre déjà une sécurité satisfaisante. Le cas 4 s'est avéré intéressant à étudier d'après les résultats corrects de sécurité obtenus, même si les niveaux de SIL sont moins exigeants que dans la modélisation initiale.

La mise en œuvre des simulations mène préalablement à une analyse qualitative intéressante pour l'identification des scénarios de risque.

4.3.3 Analyse qualitative des situations d'exploitation

Cette analyse qualitative a pour but de décrire la manière dont peuvent être identifiés les différents scénarios de risques ayant conduit à un événement redouté. Pour cela un exemple de situation d'exploitation obtenue lors de l'occurrence d'un événement redouté donné est présenté. Pour ce cas précis, le scénario recherché a mené à l'événement redouté ER_5 selon les circonstances présentées à la Figure 4.17.

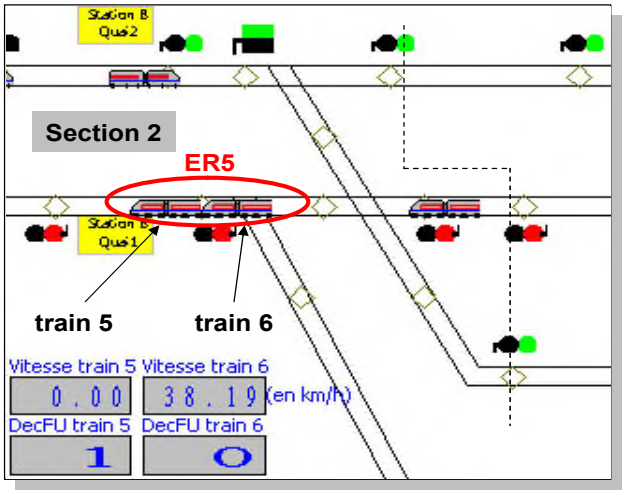


Figure 4.17 Exemple d'événement redouté généré par une simulation du contexte opérationnel

Selon cette figure, le train 6 roulant à faible vitesse est entré en collision avec le train 5 à l'arrêt, à l'entrée d'une station, suite au franchissement d'un signal fermé. A l'instant de cet accident, les états des différentes fonctions de sécurité sont présentés dans le Tableau 4.4. Dans ce tableau, seuls les états des fonctions relatives aux trains 5 et 6 et à la section 2 (lieu de l'accident) sont détaillés.

L'analyse de ces états, sachant que les valeurs 1 et 0 correspondent respectivement au fonctionnement et au dysfonctionnement d'une fonction de sécurité, permettent de comprendre la cause de l'accident et de reconstruire le scénario qui s'est produit. Ici l'événement initiateur est EIX_2 (Approche d'un signal d'espacement par un train, un autre train se trouve en aval), et le scénario s'apparente à l'alternative 3 présentée au paragraphe 4.3.1. Plus précisément, le train 5 est à l'arrêt à l'entrée d'une station suite au déclenchement de son freinage d'urgence, et le train 6 n'a pas respecté le signal fermé, suite à une mauvaise

interprétation par le système bord d'une commande de vitesse envoyée par le système sol, celle-ci tenant compte de l'arrêt du train 5.

Fonction de sécurité	Désignation	Etat des fonctions lors de l'accident	Fonction de sécurité	Désignation	État des fonctions lors de l'accident
F1	Enclench(section2)	0	F9	ControleDeplac(train5) ControleDeplac(train6)	1 1
F2	Detection(train5,section2) Detection(train6,section2)	1 1	F10	ControleVitesse(train5) ControleVitesse(train6)	1 1
F3	AutorisMouv(section2)	1	F11	ControlePosition(train5) ControlePosition(train6)	1 1
F4	FomationEtabliss(section2)	1	F12	CommandeFU(train5) CommandeFU(train6)	1 1
F5	GestionAutorisMouv(train5) GestionAutorisMouv(train6)	0 1	F13	DeclenchFU(train5) DeclenchFU(train6)	1 1
F6	CommandeVitesseBord(train5,section2) CommandeVitesseBord(train6,section2)	0 0	F14	Fservice(train5) Fservice(train6)	0 1
F7	CommandeVitesseSol(train5,section2) CommandeVitesseSol(train6,section2)	1 1	F15	FU(train5) FU(train6)	1 1
F8	CalcLimiteVitesse(train5) CalcLimiteVitesse(train6)	1 0	freinage d'urgence déclenché pour le train 5		

Tableau 4.4 Détail de l'état des fonctions dans l'exemple de situation d'exploitation

Pour améliorer la robustesse du système face aux risques, un sous-système de sécurité au sol détectant le signal franchi aurait pu être implanté juste aux abords de ce signal, mais selon les conditions présentées, ce sous-système n'aurait pas changé la situation finale, la commande au sol étant mal interprétée et le train en aval étant trop proche.

De manière générale, d'une part, l'analyse sur une histoire simulée de chaque état des différentes fonctions de sécurité lors de l'occurrence d'un événement redouté permet d'identifier le scénario de risque qui s'est produit, scénario pouvant être envisagé *a priori* ou non (selon l'analyse de différents cas, aucun scénario non prévu n'a été décelé mais ce point demande l'analyse de chaque jour appartenant aux 500 histoires simulées pour éventuellement rencontrer un cas non prévu). D'autre part, cette analyse permet, à l'aide de la visualisation et de la connaissance des paramètres de situation d'exploitation, d'établir des conclusions sur la robustesse des différents systèmes de sécurité conjointement utilisés au sein du système de transport, face aux situations à risque rencontrées. Dans la situation étudiée, un exemple de telles conclusions a été présenté (cf. paragraphe précédent). L'analyse qui suit concerne l'évaluation probabiliste des événements redoutés.

4.3.4 Analyse quantitative des situations d'exploitation

4.3.4.1 Optimisation nécessaire du temps d'exécution des simulations

Les simulations du contexte opérationnel consomment énormément de temps et ont nécessité l'emploi de trois procédés d'optimisation, qu'il convient de présenter pour détailler la manière dont les résultats ci-après ont été obtenus. Ces procédés optimisent la durée de simulation d'une histoire. Dès lors, la simulation d'un maximum d'histoires (ici 500) peut être réalisée afin d'affiner l'analyse statistique des événements redoutés apparus en exploitation.

Le premier procédé a porté sur l'enregistrement des instants de défaillances « intéressants » dans les fichiers de données associés à chaque histoire. Ces instants se rapportent aux conditions d'exploitation pour lesquelles, selon les sous-systèmes de sécurité utilisés dans cette étude, un événement redouté peut se produire. Ces conditions sont les suivantes :

- pour un train donné, les conditions de freinage d'urgence sont réunies mais la fonction de freinage d'urgence est défaillante, ou
- le freinage d'urgence d'un train donné n'est pas déclenché même si certaines de ses fonctions de sécurité (fonctions bord) sont défaillantes, ou
- une ou plusieurs fonctions de sécurité d'une section donnée (fonctions sol) sont défaillantes et différents trains y circulent.

Le deuxième procédé d'optimisation a consisté à considérer la période d'exploitation du système par journées de 24h. La simulation d'une histoire, alors effectuée journée par journée, est moins longue à effectuer si les journées de 24h sur lesquelles aucun événement dangereux ne se produit, ne sont pas analysées. Pour cela, le système de transport guidé est supposé revenir dans sa position initiale toutes les 24h, ce qui s'apparente à un retour quotidien des trains dans leur dépôt. De plus, lors d'un accident sur une journée, la simulation passe directement à la journée suivante en considérant que le système est réinitialisé et l'accident déblayé.

Le troisième et dernier procédé qui a été envisagé s'appuie sur une constatation faite lors de l'observation de l'enchaînement des événements de défaillance dans une histoire. En raison du biaisage utilisé dans la simulation de Monte Carlo, l'enchaînement des défaillances sur une journée de 24 heures peut être exactement le même sur les journées qui suivent. Sur ces journées, la simulation peut alors ne pas être effectuée en considérant que le système réagira

de la même manière que sur la journée donnée (journée de référence). Cette considération est possible dans le sens où le système est réinitialisé chaque 24h. Cependant, le caractère aléatoire lié à l'aspect de modélisation présenté au paragraphe 4.2.3.2 (concernant le changement de la vitesse normale du train en une autre vitesse lors d'une défaillance) ne pourra pas être maintenu ; les valeurs des paramètres de vitesse sur ces journées ayant le même enchaînement d'événements de défaillance seront les mêmes. Ce point concerne le contexte opérationnel et ne modifie en rien le caractère stochastique des défaillances. L'évaluation résultante des événements redoutés du Tableau 4.2 ne pourra donc pas distinguer les ER_3 et ER_4 succédant l'événement initiateur EIX_2, et les ER_3 et ER_7 succédant l'événement initiateur EIX_4.

Les cas d'étude relatifs au cas 2-3 et au cas 4 sont maintenant présentés compte tenu de la prise en compte du contexte opérationnel (le cas 1 n'a pas été considéré à ce stade comme expliqué précédemment au paragraphe 4.3.2).

4.3.4.2 Résultats de l'évaluation pour les deux cas d'étude retenus

L'évaluation probabiliste par l'analyse statistique des événements redoutés obtenus lors des 500 simulations reproduisant l'exploitation du système, ces simulations reprenant les données de défaillances de 500 histoires générées par simulation de Monte Carlo, a initialement été menée sur une période de 40 ans. Cependant, avec l'emploi d'un biaisage forçant les changements d'états sur une histoire, il s'est avéré que les événements se déroulant de 15 ans à 40 ans sur les 500 histoires avaient un poids statistique proche de 0. Ces événements n'apportent donc de ce fait aucune information aux statistiques. Sur certaines histoires, des changements d'états peuvent apparaître sur cette période de 15 à 40 ans avec un poids non nul, notamment lorsque davantage d'histoires sont simulées. Sur les 10000 histoires effectuées sans la prise en compte du contexte opérationnel, certaines histoires possèdent des événements intéressants entre 15 et 40 ans. Dans le cas présent, la durée de simulation tenant compte du contexte opérationnel étant longue (plusieurs heures), seules 500 histoires ont été examinées, histoires dans lesquelles les événements de poids non nuls se situent uniquement sur la période de 0 à 15 ans. L'évaluation statistique n'a donc été menée que jusqu'à cette durée de 15 ans.

Sur les 500 histoires, seule une partie est analysée, étant donné l'application des principes du premier procédé d'optimisation (par exemple pour le cas 4, seules 424 histoires sont analysées car ces histoires contiennent des événements pouvant potentiellement mener à un accident).

Également, les histoires analysées n'aboutissent pas toutes à un événement redouté, ce qui pénalise les statistiques présentées aux Figures 4.18 et 4.19 et rend difficilement visible l'information recherchée dans les différentes distributions de probabilité. De plus, en raison des poids statistiques, la variance reste très mauvaise.

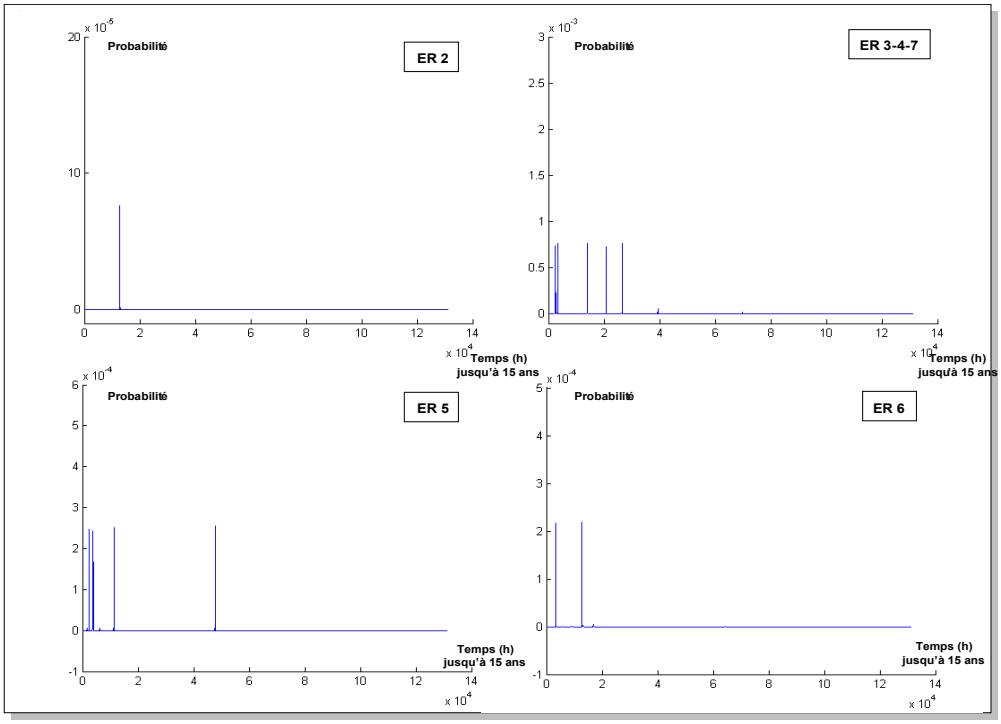


Figure 4.18 1er cas d'étude (cas 4)

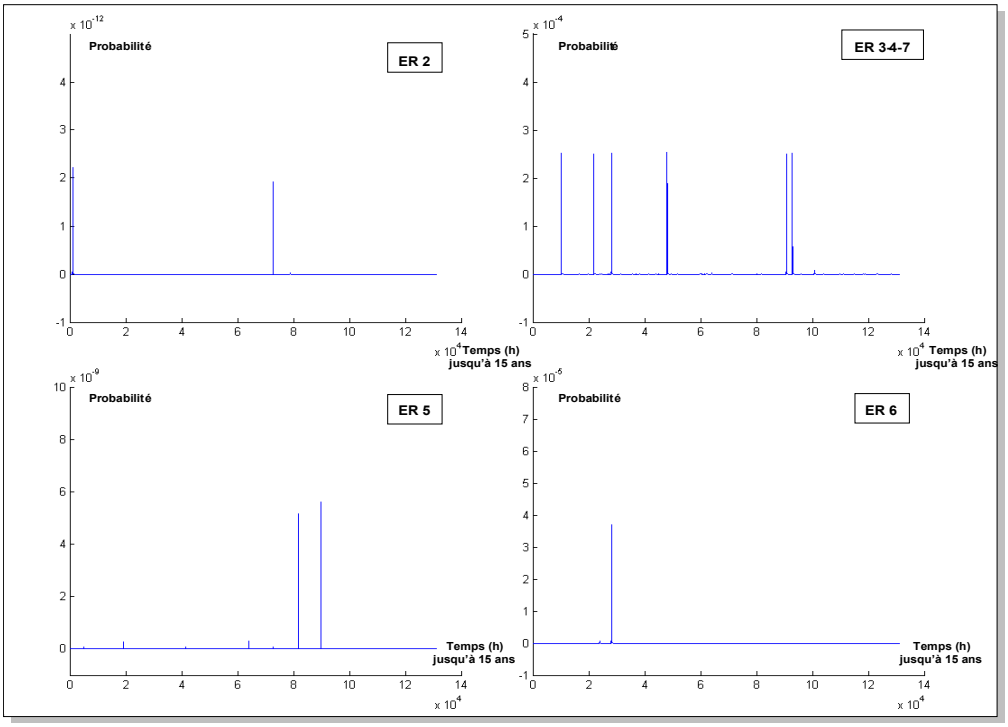


Figure 4.19 2ème cas d'étude (cas 2-3)

Le Tableau 4.5 présente l'information contenue dans chacune de ces courbes, selon le même principe appliqué au 4.3.2, pour pouvoir discuter de ces résultats par rapport au critère d'acceptation du risque retenu. A noter que la distribution de probabilité relative à l'ER1 n'a pas été représentée, cet ER ne conduisant pas à des conséquences à caractère catastrophique.

Evénement redouté	Nombre d'histoires retenues sur les 500 après l'exécution de la SMC biaisée	Nombre d'histoires contribuant à l'obtention des statistiques	ER 2	ER 3 – ER4 – ER7	ER5	ER6
Cas 4	424	314	$1.644*10^{-6}$	$1.555*10^{-5}$	$5.183*10^{-6}$	$4.69*10^{-6}$
Cas 2-3	468	193	$4.639*10^{-14}$	$5.089*10^{-6}$	$1.147*10^{-10}$	$7.725*10^{-7}$

Tableau 4.5 Principales informations contenues dans les résultats

Ces résultats sont maintenant discutés.

4.3.5 Discussion

Les exigences des fonctions de sécurité considérées au cas 4 (cas où les exigences sont moins contraignantes qu'initialement prévu lors de la modélisation du système de transport guidé), ne permettent pas d'obtenir une sécurité du système suffisante selon le critère d'acceptation du risque retenu basé sur le SIL 4. En effet toutes les probabilités d'ER sont supérieures à $2{,}4.10^{-7}$. Le niveau de sécurité évalué précédemment sans la prise en compte du contexte opérationnel devient insatisfaisant lors de la présente étude, d'où la nécessité de la mettre en œuvre.

Concernant le cas 2-3 (cas se rapportant aux valeurs maximales des niveaux de SIL initialement alloués lors de la modélisation du système de transport guidé) dont les conditions de sécurité sont plus exigeantes que le cas 4, la probabilité associée aux ER 2 et 5 concordent avec le principe d'acceptation du risque choisi. Cependant la probabilité associée au groupement des ER 3, 4 et 7 (la probabilité de ces ER ne peut être distinguée comme expliqué précédemment) et la probabilité associée à l'ER 6 sont supérieures à ce critère d'acceptation du risque. Ceci conduit à la conclusion que la sécurité du système de transport ayant les exigences de SIL du cas 2-3 est également insuffisante. Un critère basé sur le SIL 3 (risque de probabilité $< 2{,}4.10^{-6}$) aurait mené à une conclusion moins critique si les probabilités distinctes des ER 3, 4 et 7, nécessairement moins élevées que la probabilité de l'ensemble, avaient été connues.

Suite à ces constatations, le cas 1 se rapportant aux valeurs minimales des niveaux de SIL initialement alloués lors de la modélisation du système, a été examiné. Cependant celui-ci n'a pas pu être apprécié car le nombre d'histoires contribuant à l'obtention des statistiques était insuffisant après l'application du premier procédé d'optimisation.

Ces remarques mettent en évidence la nécessité d'étudier la sécurité du système en exploitation, mais il est difficile de garantir le niveau de sécurité global car la pertinence des résultats est limitée due principalement :

- au biaisage des lois relatives au changement d'état des fonctions de sécurité, délicat à paramétrer de manière optimale, notamment pour l'obtention de cas de défaillance intéressants se rapportant à la défaillance de deux ou plusieurs fonctions de sécurité (celles-ci étant de surcroît très rapidement remises en état de marche). L'approche indirecte de la simulation de Monte Carlo a été utilisée, d'autres possibilités de biaisage par l'approche directe sont à tenter.
- à une mise en œuvre des simulations qui de par leur durée d'exécution importante (plusieurs heures même avec l'automatisation de l'enchaînement des simulations et l'utilisation des modes de simulation accélérée), pénalise l'obtention des statistiques issues de ces simulations. Cependant, l'analyse qualitative s'est avérée riche d'informations et ne nécessite pas *a priori* autant de simulations.

4.4 Conclusion

Ce quatrième chapitre a permis de mettre en œuvre, sur un système de transport guidé donné, l'approche probabiliste et systémique d'évaluation de la sécurité proposée dans ce mémoire.

Les fonctionnalités considérées pour le système étudié ont été décrites dans la première partie de ce chapitre. Ces fonctionnalités sont basées sur plusieurs moyens de réductions des risques existant actuellement dans les transports guidés, et qui ont été présentés au deuxième chapitre.

La deuxième partie s'est concentrée sur la modélisation du système selon le concept de situation d'exploitation. D'après les caractéristiques des fonctions de sécurité mises en évidence dans la modélisation (SIL des fonctions, duplications des fonctions sur l'ensemble du réseau de transport et dépendances entre les fonctions), la mise en œuvre de la simulation de Monte Carlo biaisée générant les séquences d'événements liés à la sécurité, a été décrite.

Ces événements interviennent dans la simulation de l'évolution dynamique du système, simulation permise grâce à une maquette logicielle qui a été développée pour reproduire le contexte opérationnel dans lequel évolue le système. Cette maquette et son fonctionnement ont également été détaillés dans cette partie.

La dernière partie du chapitre a consisté en l'évaluation du système de transport guidé sur plusieurs « histoires » du système (simulations du système sur une durée d'exploitation), afin de certifier ou non que les exigences de sécurité considérées permettent d'atteindre un niveau de sécurité acceptable. Cette évaluation a d'abord été réalisée sans la prise compte du contexte opérationnel pour retenir des configurations d'exigences de sécurité intéressantes lors de la prise en compte de ce contexte opérationnel. La considération de l'environnement d'exploitation a d'abord mené à une analyse qualitative du système permettant d'identifier des scénarios de risque qui aboutissent en particulier à des conclusions sur la robustesse du système de transport guidé face aux risques existants. Une analyse quantitative a ensuite permis de conclure quant à un niveau de sécurité insuffisant du système par rapport au critère d'acceptation du risque choisi. Ces résultats restent à être améliorés compte tenu des techniques de biaisage pouvant encore être explorées et des procédés d'optimisation pouvant être utilisés en supplément afin de permettre une diminution des durées de simulation qui pénalisent l'obtention d'expérimentations multiples, et réduisent la qualité des statistiques.

Chapitre 5. Perspectives

Sommaire

INTRODUCTION **130**
5.1 L'UTILISATION QUANTITATIVE DES SILS **131**
5.1.1 Intégration de facteurs liés au diagnostic dans le calcul des SILs *131*
5.1.2 Le SIL vu comme un paramètre incertain *132*
5.2 DEFINITION DE VARIABLES D'INFLUENCE SUPPORT D'AIDE A LA DECISION **133**
5.2.1 Mise en évidence de critères opérationnels *133*
5.2.2 La prise en compte de la composante de coût dans la décision d'acceptation du risque *134*
5.3 PRISE EN COMPTE DES FACTEURS HUMAINS DANS L'EVALUATION DE LA SECURITE GLOBALE **135**
5.3.1 Spécificités des facteurs humains dans le domaine des transports guidés *135*
5.3.2 Une approche basée sur la méthode Safe-SADT pour la quantification de l'erreur humaine associée à une tâche donnée *137*
5.3.2.1 Intérêts de la méthode Safe-SADT 137
5.3.2.2 Esquisse d'une méthode Safe-SADT^{+} tenant compte des facteurs humains 137
5.4 CONCLUSION **139**

Chapitre 5. Perspectives

Introduction

Le chapitre précédent s'est concentré sur la validation de l'approche d'évaluation de la sécurité d'un système de transport guidé compte tenu des différents dispositifs de sécurité prévus lors de la phase de conception d'un tel système. Dans cette approche, les exigences de sécurité ont été considérées en termes de SILs (Safety Integrity Levels), lesquelles ont été employées selon les hypothèses décrites au troisième chapitre.

L'utilisation de ces exigences de SILs, abordées quantitativement, ne tient pas compte des facteurs de tests de diagnostic présentés dans la norme de sécurité IEC 61508, point sur lequel la méthode peut encore être approfondie. Il en est de même pour la considération de l'ensemble de l'intervalle lié à un SIL. Pour ce point, une analogie entre le paramètre quantitatif lié à un SIL et un paramètre entaché d'une incertitude peut être envisagée. Ces différentes perspectives relatives aux SILs sont détaillées dans la première partie du chapitre.

La deuxième partie du chapitre présente des perspectives d'amélioration de l'approche d'évaluation de la sécurité des transports guidés proposée dans ce mémoire. Elles concernent l'utilisation de variables d'influence, basées sur des critères opérationnels spécifiques et sur des critères de coût, pour la caractérisation de l'aspect gravité des conséquences d'un profil de risque.

La dernière partie se concentre sur la prise en compte des facteurs humains dans l'analyse de sécurité. En effet, même si la mise au point des dispositifs de sécurité dans les transports guidés fait l'objet de nombreux efforts depuis ces dernières années, aux vues de l'analyse *a posteriori* des accidents survenant lors de l'exploitation des systèmes de transport guidé, les erreurs humaines restent à l'origine d'un nombre significatif de ces accidents [Andersen 1999]. Une piste de recherche est donnée par l'emploi de la méthode Safe-SADT [Benard 2004] [Cauffriez, Benard et al. 2006] élargie aux facteurs humains.

5.1 L'utilisation quantitative des SILs

5.1.1 Intégration de facteurs liés au diagnostic dans le calcul des SILs

Le paramètre quantitatif lié au SIL d'un système de sécurité peut être estimé en tenant compte de la possible détectabilité des défaillances du système par des tests de diagnostic. La norme IEC 61508 fait référence à des tests de diagnostic caractérisés par un facteur de taux de couverture, et à des tests périodiques caractérisés par un intervalle dont la longueur conduit à des tests beaucoup plus espacés que les tests de diagnostic (cf. Annexe C). La norme emploie ces facteurs pour déterminer le SIL associé à des architectures redondantes de type MooN (M out of N : M sur N composants, c'est-à-dire que le système constitué de N composants nécessite le fonctionnement d'au moins M composants sur les N pour fonctionner sachant M<N). Le calcul du paramètre quantitatif lié au SIL est effectué en fonction des modes de fonctionnement à faible et à forte sollicitation de la fonction de sécurité (cf. l'équation (5.1) exprimant la probabilité moyenne de défaillance à la demande et l'équation (5.2) exprimant la probabilité de défaillance dangereuse par heure).

$$PFD_{avg} = F(\lambda_{DD}, \lambda_{DU}, t_{CE}, t_{GE}, MTTR, \beta) \tag{5.1}$$

$$PFH = F(\lambda_{DD}, \lambda_{DU}, t_{CE}, \beta) \tag{5.2}$$

avec
- $F()$: fonction de ( )
- λ_{DD} et λ_{DU} : taux de défaillance dangereuse détectée et non détectée
- t_{CE} et t_{GE} : temps moyen d'indisponibilité équivalent au niveau sous-système et système
- $MTTR$: temps moyen de réparation
- β : proportion de défaillances de cause commune

Cependant, la norme ne définit pas la procédure à suivre pour obtenir le SIL de la combinaison de différents sous-systèmes de sécurité ayant différents SILs, l'architecture finale du système de sécurité étant plus complexe.

L'approche basée sur la simulation de Monte Carlo présentée au troisième chapitre a apporté une solution à ce problème. Cette approche intègre uniquement des taux de réparation. Elle pourrait être modifiée par l'utilisation de distributions tenant compte de tests de diagnostics (tels que ceux présentés par la norme IEC 61508) pour échantillonner les changements d'état.

5.1.2 Le SIL vu comme un paramètre incertain

Le SIL, représentant un objectif quantitatif à atteindre exprimé sous la forme d'un *intervalle de valeurs* probabilistes, peut être assimilé à un paramètre incertain. En effet, un tel paramètre est caractérisé par une valeur quantitative qui est définie le plus souvent sur un intervalle borné dans lequel les valeurs sont réparties ou distribuées selon une loi de probabilité donnée. Un SIL peut donc être assimilé à un paramètre incertain pour permettre la prise en compte de l'ensemble des valeurs au sein de l'intervalle pour un SIL donné, les bornes minimale et maximale ayant seulement été considérées jusqu'alors.

Ainsi pour la quantification de profils de risque exposée au troisième chapitre, un intervalle de THR (Tolerable Hazard Rate) correspondant à un SIL donné peut être attribué, en tant que paramètre incertain, aux différentes fonctions de sécurité dont les actions forment les événements des profils de risque. La combinaison ou la propagation des paramètres incertains au travers de la structure causale de ces profils correspond alors à une analyse d'incertitude [Kumamoto et Henley 1996] (cf. Figure 5.1).

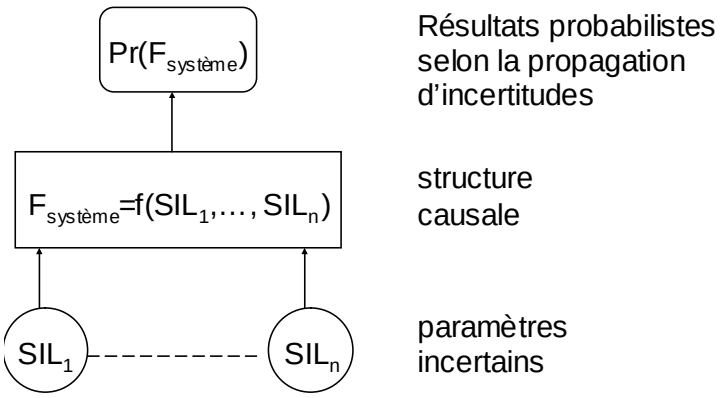


Figure 5.1 Analyse d'incertitudes pour la combinaison des SILs

Cette analyse d'incertitude est qualifiée de paramétrique puisque les incertitudes concernent les paramètres probabilistes associés aux événements intervenant dans les profils de risque. Les incertitudes peuvent également être relatives à la complétude des analyses (par exemple, tous les modes de défaillances des composants ont-ils été identifiés ?) et à la modélisation du système (les hypothèses de modélisation reflètent-elles correctement le système réel ? les circonstances particulières d'utilisation du système sont-elles envisagées ?). Ces sources d'incertitudes se rapportent aux incertitudes de modélisation et sont considérées comme étant limitées par une analyse rigoureuse du système.

Suite à la propagation des incertitudes dans la structure causale des profils de risque, les résultats probabilistes peuvent être obtenus à l'aide de méthodes analytiques, comme la méthode des moments, ou de méthodes numériques avec l'emploi de l'algèbre des probabilités discrètes, ou l'emploi de la simulation de Monte Carlo [Bedford et Cooke 2001] [Kumamoto et Henley 1996].

L'algorithme de simulation de Monte Carlo utilisé dans le troisième chapitre peut intégrer l'incertitude liée aux SILs par un second échantillonnage de valeurs dans l'intervalle du THR lié à chaque fonction de sécurité. Ce double échantillonnage se rapporte à une simulation de Monte Carlo du second ordre qui implique que chaque histoire générée est déjà le résultat d'une SMC [Ferson et Ginzburg 1996]. L'échantillonnage supplémentaire augmente le temps d'exécution de la SMC mais est nécessaire à l'analyse d'incertitude. L'amplitude des intervalles liés au THR est très différente d'un niveau de SIL à l'autre en raison de l'échelle basée sur les puissances décimales utilisée dans la définition des SILs (voir le second chapitre). De ce fait, l'intervalle correspondant au THR d'une fonction peut-être assimilé à une distribution log-uniforme permettant d'échantillonner de manière équiprobable toutes les valeurs comprises dans l'intervalle (le logarithme de l'intervalle respectant une loi uniforme).

Les deux parties suivantes se focalisent sur plusieurs points permettant d'approfondir l'approche de sécurité globale. La première est dédiée à la définition de variables d'influence sur la gravité des conséquences d'un profil de risque. Ces variables fournissent alors un support d'aide à la décision face aux risques présents. La suivante est dédiée à l'intégration des erreurs humaines dans l'analyse de sécurité des transports guidés.

5.2 Définition de variables d'influence support d'aide à la décision

5.2.1 Mise en évidence de critères opérationnels

Les conditions circonstancielles dans lesquelles survient un événement redouté permettent de caractériser la gravité d'un tel événement. Au quatrième chapitre, les expérimentations ont tenu compte de critères opérationnels comme la vitesse des trains mis en causes dans un accident et la position de ces trains lors de l'accident (proximité d'autres trains, proximité d'infrastructures particulières telles les stations, les intersections…).

Outre ces critères de vitesse et de position, des critères d'occupation des quais par un certain nombre de personnes ou d'occupation des trains pourraient être pris en compte. En effet,

selon les périodes d'heures creuses ou d'heures de pointe, la fréquentation des lignes de transport ne sera pas la même donc la gravité des conséquences d'un accident potentiel ne sera pas la même. La modélisation de cette fréquentation est envisageable selon des modèles de déplacements de personnes sur les réseaux soit par des méthodes de recherche opérationnelle établissant les chemins optimaux des déplacements sur le réseau de transport, soit par des modèles de flux de passagers basés par exemple sur des réseaux de Petri [Castelain et Mesghouni 2003].

Ces critères opérationnels peuvent alors être traduits au travers de variables d'influence (les variable V1 à V3 de la Figure 5.2 prenant leur valeur entre 0 et 1 par exemple), sur lesquelles les décisions prises concernant l'acceptation du risque pourraient s'appuyer en comparaison d'une référence d'acceptation basée sur la même échelle.

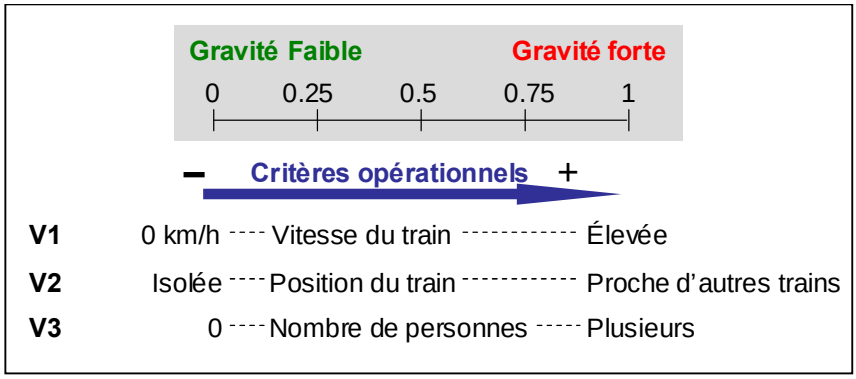


Figure 5.2 Définition de variables d'influence caractérisant la gravité d'événements redoutés

A ces critères peut s'ajouter un critère de coût lié aux dommages qu'occasionne un accident sur l'environnement, sur le système, et sur ses utilisateurs.

5.2.2 La prise en compte de la composante de coût dans la décision d'acceptation du risque

Les coûts relatifs à un accident sont directement liés à la perte financière associée aux dégâts subis par le système et l'environnement, et peuvent inclure une estimation monétaire du nombre de victimes, pratique qui est commune au Royaume-Uni [Sharpe 2004] dans le cadre d'approches économiques décisionnelles, même si l'estimation d'une vie est un point de vue très subjectif pouvant être sujet à controverses. Ces coûts intègrent également des pertes financières indirectes liées aux conséquences de l'accident sur l'exploitation du système de transport (généralement un arrêt d'exploitation), et aux procédures administratives pouvant être déclenchées (cf. Tableau 2.1).

Coûts directs		Coûts indirects
Coûts relatifs aux dégâts	**Coûts relatifs aux victimes**	
- dommages causés aux matériels roulants et aux infrastructures - remise en état après accident (extinction incendie, déblayage, reconstruction…) - impact sur l'environnement	- aide médicale - perte humaine (passagers, employés)	- perte d'exploitation - coûts administratifs (enquête judiciaire, expertise, assurance…) - dommages et intérêts aux victimes et familles

Tableau 5.1 Coûts liés à un accident

Selon les résultats des expérimentations menées dans le cadre de l'approche de sécurité proposée, ces coûts pourraient être estimés à l'issue des simulations, et traduits au moyen d'une *fonction de coût* dépendant des pertes financières liées aux dégâts, au nombre de victimes, et à la perte d'exploitation estimée. Cette fonction correspond alors à une fonction décisionnelle.

Il est à noter que les coûts de nouvelles fonctionnalités envisagées pour améliorer la sécurité peuvent être comparés aux coûts estimés de l'accident qui peut se produire en l'absence de telles fonctionnalités. Cette comparaison oriente alors les choix et décisions de conception. L'analyse pourrait, en outre, se tourner vers une optimisation combinatoire des conditions de sécurité (dont les SILs) sous contrainte de coût.

La partie suivante se consacre à la possibilité d'intégrer les facteurs humains dans l'évaluation de la sécurité globale.

5.3 Prise en compte des facteurs humains dans l'évaluation de la sécurité globale

5.3.1 Spécificités des facteurs humains dans le domaine des transports guidés

L'aspect procédural des transports guidés impliquant des règles de trafic, de régulation et de sécurité, occupe une part importante dans la gestion de la circulation des trains. Un apprentissage de ces règles par les opérateurs humains (détaillant les tâches prescrites) est nécessaire pour répondre par une ou des actions appropriées à la procédure requise dans une situation donnée (tâches effectives). La fiabilité des opérateurs, en particulier la fiabilité des conducteurs des trains, repose sur un ensemble d'actions correctes étant donné un contexte variant et un certain nombre de tâches à accomplir. Comme détaillé au deuxième chapitre, les

risques liés à un opérateur se rapportent aux erreurs qu'il peut commettre lors de l'exploitation du système et de la maintenance des infrastructures ou du matériel roulant, ces erreurs menant à une situation dangereuse immédiate ou à un accident. Certaines situations telles le respect d'un signal ou d'une vitesse indiquée, l'établissement d'itinéraires non conflictuels à un poste d'aiguillage, exigent une grande fiabilité humaine.

L'opérateur intervient également sur le système pour en surveiller le bon fonctionnement, et agir rapidement en cas de dérives pour éviter tout problème ou apporter des actions de correction ou de reconfiguration. C'est notamment le cas dans les situations où le système est configuré pour fonctionner dans un mode dégradé prévu en conception, dans ce cas l'opérateur assure la continuité de fonctionnement du système de transport.

Le comportement d'un opérateur humain est analysable et quantifiable lors d'expérimentations concrètes menées par différents sujets sur la même situation observée. Cependant, ces expérimentations concrètes sont difficiles à mettre en œuvre dans des simulations qui reproduisent le contexte d'exploitation d'un système de transport et qui sont effectuées sur toute la durée de vie du système, critères de l'approche présentée au troisième chapitre. Cette approche intègre certes les facteurs humains par l'instanciation des classes « activité », « équipe d'opérateurs » et « mode d'exploitation » du modèle de situation d'exploitation, mais ce point de modélisation reste descriptif et n'est pas pris en compte dans la méthode de simulation évaluant les scénarios de risque.

Le paragraphe suivant propose d'employer une approche « fiabiliste » basée sur la méthode Safe-SADT pour identifier les distributions de probabilité liées au succès et à l'échec de chacune des tâches prescrites qui auront été décrites qualitativement par le modèle de situation d'exploitation. Même si la genèse d'une erreur est difficilement quantifiable objectivement en raison de facteurs cognitifs tels l'acquisition des connaissances, la manière dont sont effectués les raisonnements, la perception de la situation par l'opérateur, la prise de décision (bases des approches « cognitivistes » s'opposant aux approches « fiabilistes ») [Millot 1999], l'emploi de critères probabilistes fournit un moyen d'évaluation et d'aide à la décision en regard des risques existants. L'emploi de tels critères est particulièrement intéressant dans les études de sécurité, puisque celles-ci comportent des profils de risque où certaines tâches prescrites, liées à la mise en sécurité du système, ont peu de chance d'être réalisées car rarement demandées ; une approche fiabiliste telle que présentée ci-dessous permet alors de les prendre en compte.

5.3.2 Une approche basée sur la méthode Safe-SADT pour la quantification de l'erreur humaine associée à une tâche donnée

5.3.2.1 Intérêts de la méthode Safe-SADT

La méthode Safe-SADT est une approche développée au LAMIH [Benard 2004] [Cauffriez, Benard et al. 2006] dans le but d'évaluer les paramètres de sûreté de fonctionnement des systèmes complexes, compte tenu de l'évolution de ces systèmes dans le temps. Dans cette méthode, une analyse multi-niveaux du système est effectuée selon, dans un premier temps, une démarche descendante but/moyen détaillant les objectifs, les fonctions puis les composants, et dans un second temps, selon une démarche ascendante reposant sur une agrégation partie/tout permettant d'intégrer différents services. Ces points sont intéressants pour l'adaptation de la méthode à la quantification de l'erreur humaine liée à une tâche prescrite décrite. En effet, une tâche, définie comme un but à atteindre connaissant la situation actuelle d'exploitation, est décomposable en sous-tâches correspondant à des sous-buts [Polet 2002]. La notion de tâche peut alors être intégrée à la méthode Safe-SADT mettant ainsi en relation les éléments techniques et humains pour l'estimation des distributions recherchées. Les tâches élémentaires restent à être déterminées et quantifiées en terme d'erreurs dues à l'homme, par des méthodes de fiabilité humaine comme THERP par exemple (Technique for Human Error Rate Prediction) [Swain et Guttmann 1983], par des méthodes de jugements d'experts, ou selon des historiques de données issus de retours d'expériences.

De plus, la méthode Safe-SADT permet de prendre en compte la configuration du système lors de modes dégradés. Les tâches devant être réalisées par les opérateurs lors de configurations particulières du système peuvent ainsi être considérées.

5.3.2.2 Esquisse d'une méthode Safe-SADT^{+} tenant compte des facteurs humains

La méthode Safe-SADT a pour but premier de définir l'*architecture opérationnelle* d'un système réalisant des services requis et répondant aux objectifs spécifiés dans un cahier des charges (objectifs liés aux tâches prescrites et objectifs de sûreté de fonctionnement FMDS – Fiabilité, Maintenabilité, Disponibilité, Sécurité– la sécurité pouvant être définie au travers d'exigences de SIL). Pour cela, l'architecture opérationnelle est obtenue à partir de la projection d'une architecture fonctionnelle sur un ensemble de ressources, et est évaluée en fonction des différentes contraintes et caractéristiques des ressources du système.

Compte tenu des remarques faites au paragraphe précédent sur l'intérêt de la méthode Safe-SADT pour la quantification des tâches réalisées par les opérateurs humains, une esquisse de cette méthode adaptée aux facteurs humains est envisagée. Cette évolution de la méthode Safe-SADT initiale en une version Safe-SADT$^+$ est présentée à la Figure 5.3. Celle-ci détaille un bloc Safe-SADT$^+$ représentant un niveau de hiérarchie spécifique dans l'analyse du système. Ce bloc possède des paramètres de contrôle (au dessus du bloc) qui modélisent les conditions régissant la fonction ou le sous-système analysé. Les *événements contrôlables* concernent les actions de type correctif ou compensateur permettant de garder le système dans un mode de fonctionnement nominal ou dégradé. Les *événements incontrôlables* indiquent les perturbations possibles du système (événements de défaillances, événements favorisant l'erreur humaine) qui doivent être contrôlés à un niveau immédiatement supérieur. Les *contraintes* désignent des conditions liées à la performance du système, aux procédures à respecter, et à l'affectation des fonctions sur les supports d'exécution logiciels et matériels. Les *critères d'acceptation du risque* apparaissent comme des critères de décisions. En dessous du bloc sont modélisées les ressources du système, celles-ci se divisant en ressources matérielles et en ressources humaines. Sur ces ressources sont projetés les *services à exécuter* (fonctions et tâches) –situés en entrée– pour délivrer en sortie l'ensemble des *services exécutés* avec la quantification de leurs paramètres FMDS.

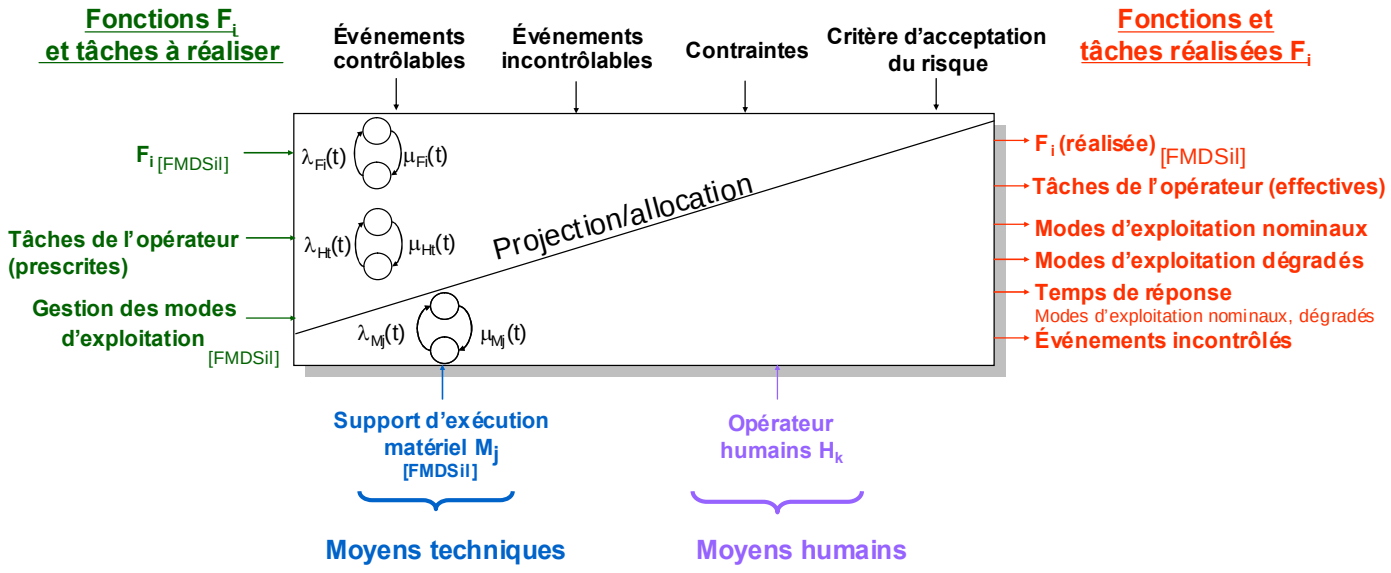


Figure 5.3 Description d'un diagramme Safe-SADT$^+$ d'un système tenant compte des facteurs humains

Une analyse approfondie du comportement des opérateurs doit conduire à la quantification des erreurs humaines pour chacune des tâches effectives pouvant être répertoriées en trois classes : les tâches de perception, les tâches de décision ou les actions. Il est alors possible d'aboutir à des taux de défaillance de l'opérateur pour chacune des tâches effectives et en déduire éventuellement un taux de défaillance global de l'opérateur en fonction de certains paramètres tels que fatigue, stress, surcharge de travail. La notion de taux de réparation concerne l'aptitude de l'opérateur à faire une reprise sur erreur détectée.

L'utilisation de la méthode Safe-SADT, telle qu'elle vient d'être présentée, pourrait ainsi fournir les caractéristiques liées aux opérateurs humains pour l'approche d'évaluation de la sécurité d'un système de transport guidé proposée dans ce mémoire.

5.4 Conclusion

Ce chapitre a mis en évidence différentes perspectives pouvant découler des travaux de recherche présentés dans ce mémoire. Dans la première partie du chapitre, celles-ci se sont d'abord concentrées sur la possibilité d'approfondir l'emploi des exigences de SILs selon des facteurs de tests de diagnostic tels que présentés dans la norme de sécurité IEC 61508. Compte tenu des caractéristiques quantitatives liées au concept de SIL, la possibilité d'assimiler un SIL à un paramètre incertain a également été envisagée. Cette analogie permettrait d'appliquer les méthodes relatives aux analyses d'incertitude sur les études de sécurité des systèmes complexes comprenant plusieurs fonctions de SIL donné.

La deuxième partie a été consacrée à la proposition d'une amélioration directe de l'approche d'évaluation de la sécurité des transports guidés développée dans cette thèse. Cette amélioration a été orientée sur la caractérisation de la gravité des conséquences d'un profil de risque par la proposition de différentes variables d'influence sur la gravité d'un accident, celles-ci tenant compte de critères opérationnels et de coût. La prise de décision face aux risques décrits, tâche sensible de la gestion des risques, pourrait ainsi s'appuyer, outre sur l'évaluation de la sécurité, sur l'analyse de ces variables classées en catégorie d'importance selon la gravité du risque.

Enfin, la dernière partie s'est focalisée sur un sujet ouvrant un large champ de recherches sur le thème de l'évaluation de la sécurité des transports guidés : l'intégration dans les études, des facteurs humains, ces facteurs ayant un impact important sur le niveau de sécurité exigé. Une

évolution de la méthode Safe-SADT a été envisagée pour l'obtention des caractéristiques liées aux facteurs humains, celles-ci pouvant alors être intégrées dans l'évaluation de la sécurité globale.

Conclusion générale

La mission d'un système de transport guidé consiste à assurer le déplacement de passagers ou de marchandises d'un lieu donné à un autre, selon un temps de parcours établi et selon des conditions de sécurité optimales. Garantir les conditions de sécurité lors de l'exploitation d'un tel système est la préoccupation majeure des autorités de transport, notamment de l'Union Européenne qui a inscrit cet objectif dans sa politique globale sur les transports, au travers la publication du Livre Blanc de septembre 2001 [Livre Blanc 2001] (document contenant un ensemble de propositions d'actions communautaires dans le domaine des transports). Cependant, pour répondre aux nouvelles contraintes de rapidité de transport, d'intensification des flux et d'échanges d'informations, ceci dans un contexte d'interopérabilité des réseaux et des matériels roulants, le développement des systèmes de transport guidé tend vers la mise au point de systèmes de plus en plus complexes. Ces systèmes aux technologies avancées et aux fonctionnalités nouvelles, doivent être analysés pour justifier que leur niveau de sécurité est suffisant vis-à-vis des critères sévères d'acceptation du risque fixés par les directives nationales. Si ce niveau est démontré comme insuffisant, des moyens réduisant les différents risques qui pénalisent la sécurité, doivent être mis en œuvre.

Les travaux de recherche présentés dans ce mémoire de thèse ont pris pour défi de proposer une approche d'évaluation de la sécurité des systèmes de transport guidé compte tenu du besoin de méthodes pour entreprendre cette tâche qui apparaît délicate en raison de la complexité évoquée. Cette complexité a orienté les études vers une approche systémique se focalisant sur l'ensemble d'un système (le sous-système bord embarqué dans chaque train, et le sous-système sol déployé tout le long des lignes) pour tenir compte à la fois des différentes interactions fonctionnelles et de l'évolution dynamique du système dans son environnement. Cette approche se veut également probabiliste pour permettre la considération des exigences de sécurité quantitatives définies dans les récentes normes de sécurité par le biais du concept de SIL (Safety Integrity Level).

Dans le premier chapitre, la notion de complexité et les différents aspects de la systémique, lesquels apportent un cadre théorique et méthodologique à la modélisation des systèmes

complexes, ont été introduits. Citons les aspects d'analyse globale, d'interactions, de comportement, d'organisation, de téléologie (finalité d'un système) et d'émergence de propriétés. L'analyse de la sûreté de fonctionnement d'un système complexe, dans le contexte de l'analyse systémique, a ensuite été présentée en distinguant les concepts, les moyens, et les analyses qualitatives et quantitatives utilisés dans cette discipline. La maîtrise des risques, employant les connaissances issues des analyses de sûreté de fonctionnement, a enfin été exposée. Cette discipline est dédiée plus spécifiquement à l'appréciation des moyens de prévention et de protection à mettre en œuvre pour éliminer ou réduire l'occurrence et les conséquences des dangers, le but étant, au final, d'assurer la sécurité.

Le deuxième chapitre a mis en évidence, dans une première partie, les différents risques pouvant exister lors de l'exploitation d'un système de transport guidé et, dans une deuxième partie, les diverses caractéristiques des sous-systèmes de sécurité actuellement employés pour éviter tout accident, ou de manière générale pour éviter tout événement redouté. Ces deux parties représentent les activités d'identification et d'analyse des moyens de réduction des risques, celles-ci étant nécessaires à la conduite d'un processus de gestion des risques aboutissant à la maîtrise des risques résiduels. Néanmoins, les autres activités *d'évaluation du risque résiduel* et de *prise de décision* en regard du niveau de sécurité souhaité restent problématiques face à la complexité grandissante des sous-systèmes de sécurité décrits. La partie suivante s'est focalisée sur la présentation des SILs, exigences de sécurité qui ont été introduites par les normes de sécurité fonctionnelle pour tenter de répondre à cette problématique. Ces exigences sont allouées aux fonctions de sécurité selon différentes méthodes, dans le but de réduire le risque jusqu'à un niveau acceptable. Cependant, ces méthodes, en analysant séparément chacune des fonctions de sécurité, ne permettent pas une réelle évaluation de sécurité globale d'un système de transport guidé, la sécurité y étant assurée par l'action conjointe de plusieurs de ces fonctions. Il est alors apparu nécessaire d'employer une approche systémique qui tient compte des dépendances fonctionnelles.

Cette considération a été prise en compte dans le troisième chapitre pour proposer, en premier lieu, des méthodes de quantification de profils de risque basées sur la combinaison des fonctions de sécurité. Un profil de risque se rapporte aux causes et aux conséquences des différentes alternatives de risques menant à un événement redouté. Il peut être décrit sous la forme d'une structure causale des différentes actions de sécurité possibles, celles-ci correspondant à un enchaînement successif d'événements dépendants qui coïncident avec le

succès ou l'échec des fonctions de sécurité. Cette structure causale est la base de deux méthodes de quantification proposées. L'une s'appuie sur des règles de combinaison des SILs appelée « algèbre des SILs ». L'autre s'appuie sur une approche de simulation de Monte Carlo biaisée qui, en fonction des SILs des fonctions de sécurité, génère aléatoirement et de manière forcée l'échec d'une ou plusieurs de ces fonctions, afin d'analyser statistiquement la conséquence de ces échecs. Cette dernière méthode s'est avérée plus pertinente car mieux adaptée aux structures causales complexes. A noter qu'une attention particulière a été portée sur la manière dont les propriétés quantitatives du SIL ont été employées étant donné l'existence de différentes interprétations à ce sujet liées au sens équivoque de la définition du SIL présentée dans les normes de sécurité.

Pour effectuer l'analyse globale du système de transport guidé, au regard des aspects de complexité qui le caractérisent, le troisième chapitre a ensuite présenté une démarche de modélisation basée sur le concept original de « situation d'exploitation ». Ce dernier concourt à l'identification des profils de risque par la mise en évidence des conditions de sécurité du système selon le contexte opérationnel dans lequel il évolue. Cette évolution dynamique du système dans son environnement est envisagée par l'emploi d'une méthode de simulation. Celle-ci a pour but de mener aux séquences accidentelles d'événements, les scénarios de risque, qui pourront ensuite être analysées et évaluées. La simulation comprend l'occurrence d'événements de défaillances des fonctions de sécurité qui sont générés par l'approche de simulation de Monte Carlo précédente.

Le quatrième chapitre a appliqué la démarche de modélisation proposée à un système de transport guidé dont les fonctionnalités envisagées en conception ont été exposées. Basée sur les différentes caractéristiques de sécurité mises en évidence par la modélisation des situations d'exploitation, une maquette logicielle a été développée pour réaliser des expérimentations reproduisant l'évolution dynamique du système durant la phase d'exploitation, y compris les défaillances concernant les différents systèmes de sécurité présents. Les simulations effectuées sur la maquette, selon le procédé décrit au troisième chapitre, ont permis d'examiner la robustesse du système en situations risquées par une analyse qualitative de scénarios identifiés. Leur étude quantitative a conclu à un niveau de sécurité du système qui est insuffisant par rapport au critère d'acceptation du risque choisi. Cependant, la durée importante des simulations et le biaisage de l'occurrence des événements dangereux difficilement paramétrable de manière optimale, ont pénalisé la qualité de ces statistiques.

Enfin, le dernier chapitre a présenté des perspectives de recherche intéressantes quant à la suite de ces travaux. Elles ont d'abord envisagé la considération de contraintes de diagnostics dans l'emploi des exigences de SILs, contraintes que définit la norme de sécurité fonctionnelle IEC 61508 dans les modalités d'applications des SILs. D'autre part, une analogie entre les études de sécurité basées sur les exigences de SIL et les études employant des techniques d'analyse d'incertitudes a été considérée pour une quantification de profils de risque plus axée sur les intervalles de valeurs probabilistes associées aux SILs. Pour une évaluation de la sécurité plus approfondie, des variables d'influence sur le risque ont ensuite été analysées compte tenu de paramètres opérationnels et de paramètres de coûts. Les perspectives s'orientent à long terme sur la possibilité d'intégrer l'erreur humaine dans l'approche de sécurité par l'emploi d'une démarche de quantification de l'erreur humaine.

Références bibliographiques

[Abrial 1996] Abrial J.-R. (1996). *The B book: assigning programs to meanings.* Cambridge, England, Cambridge University Press. ISBN 0-521-49619-5.

[Andersen 1999] Andersen T. (1999). *Human Reliability and Railway Safety*. 16th ESReDA seminar - European Safety, Reliability & Data Association, Oslo, Norvège. ISBN 92-828-9143-7.

[Andrews et Moss 1993] Andrews J. D. et Moss T. R. (1993). *Reliability and Risk Assessment.* Essex, England, Longman Scientific & Technical. ISBN 0-582-09615-4.

[Becker et Naïm 1999] Becker A. et Naïm P. (1999). *Les réseaux bayésiens, modèles graphiques de connaissance*. Paris, France, Eyrolles. ISBN 2-212-09065-X.

[Bedford et Cooke 2001] Bedford T. et Cooke R. M. (2001). *Probabilistic risk analysis: foundations and methods*. Cambridge, England, Cambridge University Press. ISBN 0521773202.

[Benard 2004] Benard V. (2004). *Evaluation de la sûreté de fonctionnement des systèmes complexes, basée sur un modèle fonctionnel dynamique: la méthode Safe-SADT.* Thèse de doctorat. LAMIH (Laboratoire d'Automatique, de Mécanique et d'Informatique Industrielles et Humaines). UVHC (Université de Valenciennes et du Hainaut-Cambrésis).

[Berbineau 2001] Berbineau M. (2001). *Les systèmes de télécommunication existants ou émergents et leur utilisation dans le domaine des transports guidés*. Les collections de l'INRETS, n°40. Institut National de Recherche sur les Transports et leur Sécurité. ISBN 2-85782-562-5.

[Beugin 2003] Beugin J. (2003). *Report of the UVAL Training 7-11 July 2003 carried out in RATP (Régie Autonome des Transports Parisiens)*. Document interne du LAMIH, Valenciennes, France.

[Beugin, Renaux et al. 2005a] Beugin J., Renaux D. et Cauffriez L. (2005a). *A SIL quantification approach to complex systems for guided transportation*. ESREL 2005 - European safety and reliability conference, Gdansk, Poland. In Kołowrocki (eds), pp 197-204, Taylor & Francis Group, London. ISBN 0-415-38340-4.

[Beugin, Renaux et al. 2005b] Beugin J., Renaux D. et Cauffriez L. (2005b). *A Safety Assessment Method for Guided Transportation Systems: A Dynamic Approach Using Monte Carlo and Discrete Event Simulation*. 17th IMACS World Congress - Scientific Computation, Applied Mathematics and Simulation, Paris, France. In Borne, Benrejeb, Dangoumau and Lorimier (eds). ISBN 2-915913-02-1.

[Beugin, Renaux et al. 2007] Beugin J., Renaux D. et Cauffriez L. (2007). *A SIL Quantification Approach based on an Operating Situation Model for Safety Evaluation in Complex Guided Transportation Systems*. Reliability Engineering & System Safety. (Acceptée le 22 septembre 2006).

[Bied-Charreton 1998] Bied-Charreton D. (1998). *Sécurité intrinsèque et sécurité probabiliste dans les transports terrestres*. Les collections de l'INRETS, n°31. Institut National de Recherche sur les Transports et leur Sécurité.

[Blaise, Lhoste et al. 2003] Blaise J. C., Lhoste P. et Ciccotelli J. (2003). *Formalisation of normative knowledge for safe design*. Safety Science 41(2-3): pp 241-261.

[Booch 1994] Booch G. (1994). *Analyse et conception orientées objets*. Paris, Addison-Wesley France. ISBN 2-87908-069-X.

[Braband 1999] Braband J. (1999). *Allocation of safety integrity requirements for railway signalling applications*. ESREL '99 - European safety and reliability conference, Munich-Garching, Germany. In Schüller and Kafka (eds), pp 1237-1242.

[Bukowski, Rouvroye et al. 2002] Bukowski J. V., Rouvroye J. L. et Goble W. M. (2002). *What is PFDavg?* Sellersville, USA, Exida library.

[Castelain et Mesghouni 2003] Castelain E. et Mesghouni K. (2003). *Modélisation d'un réseau de transport urbain avec des réseaux de Petri de haut niveau: prise en compte des flux de passagers*, Travaux de recherche du GRRT - Groupement Régional Nord-Pas-De-Calais pour la Recherche dans les Transports.

[Cau 2003] Cau G. (2003). *The new diagnostic system of the ETR 500 Italian high speed trains fleet*. WCRR 2003 - World Congress on Railway Research, Edimbourg, Ecosse, Royaume-Uni.

[Cauffriez 2005] Cauffriez L. (2005). *Méthodes et Modèles pour l'Évaluation 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.* Habilitation à diriger des recherches. LAMIH (Laboratoire d'Automatique, de Mécanique et d'Informatique Industrielles et Humaines). UVHC (Université de Valenciennes et du Hainaut-Cambrésis).

[Cauffriez, Benard et al. 2006] Cauffriez L., Benard V. et Renaux D. (2006). *A new formalism for designing and specifying RAMS parameters for safe complex distributed control systems: the Safe-SADT formalism*. IEEE Transactions on Reliability.

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

[CENELEC 1998] CENELEC, prEN 50128, (1998). *Applications ferroviaires: logiciels pour systèmes de commande et de protection ferroviaire*. CENELEC, Comité Européen de Normalisation Electrotechnique. Fontenay-aux-Roses, France, UTE, Union Technique de l'Electricité et de la communication.

[CENELEC 1999] CENELEC, prEN 50129, (1999). *Applications ferroviaires: systèmes électroniques de sécurité pour la signalisation*. CENELEC, Comité Européen de Normalisation Electrotechnique. Fontenay-aux-Roses, France, UTE, Union Technique de l'Electricité et de la communication.

[Charpentier 2002] Charpentier P. (2002). *Architecture d'automatisme en sécurité des machines: études des conditions de conception liées aux défaillances de mode commun.* INRS (Institut National de Recherche et de Sécurité). Institut National Polytechnique de Lorraine.

[Chevreau, Wybo et al. 2005] Chevreau F. R., Wybo J. L. et Cauchois D. (2005). *Organizing learning processes on risks by using the bow-tie representation*. Journal of Hazardous Materials 130(3): pp 276-283.

[Chittaro, Guida et al. 1993] Chittaro L., Guida G., Tasso C. et Toppano E. (1993). *Functional and Teleological Knowledge in the Multimodeling Approach for Reasoning about Physical Systems: A case Study in Diagnosis*. IEEE Transactions on Systems, Man, and Cybernetics 23(6): pp 1718-1751.

[Ciccotelli 1999] Ciccotelli J. (1999). *Des systèmes compliqués aux systèmes complexes. Eléments de réflexion pour l'ingénierie de prévention.* Cahier de notes documentaires - Hygiène et sécurité du travail 177(4ème trim.): pp 125-133.

[De Dianous et Fiévez 2005] De Dianous V. et Fiévez C. (2005). *ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance*. Journal of Hazardous Materials 230(3): pp 220-233.

[De Rosnay 1975] De Rosnay J. (1975). *Le Macroscope, vers une vision globale*. Paris, France, Le Seuil. ISBN 2-02-004567-2.

[Delcroix, Piechowiak et al. 2003] Delcroix V., Piechowiak S. et Maalej M.-A. (2003). *Calcul des diagnostics les plus probables a posteriori*. Revue d'intelligence artificielle (RIA) 17(4): pp 627-654.

[Desroches 1995] Desroches A. (1995). *Concepts et méthodes probabilistes de base de la sécurité.* Paris, France, Lavoisier - Tec & Doc. ISBN 2-7430-0030-9.

[Desroches, Leroy et al. 2003] Desroches A., Leroy A. et Vallée F. (2003). *La gestion des risques, principes et pratiques*. Paris, France, Hermès Sciences Publications - Lavoisier. ISBN 2-7462-0640-4.

[Directive 49/CE 2004] Directive 49/CE, Parlement et Conseil Européens (2004). *Directive 2004/49/CE sur la sécurité des chemins de fer communautaires*. Journal Officiel de l'Union Européenne. http://europa.eu.int/eur-lex/pri/fr/oj/dat/2004/l_164/l_16420040430fr00440113.pdf.

[Directive 50/CE 2004] Directive 50/CE, Parlement et Conseil Européens (2004). *Directive 2004/50/CE modifiant la directive 96/48/CE du Conseil relative à l'interopérabilité du système ferroviaire transeuropéen à grande vitesse et la directive 2001/16/CE du Parlement et du Conseil relative à l'interopérabilité du système ferroviaire transeuropéen conventionnel*. Journal Officiel de l'Union Européenne.
http://europa.eu.int/eur-lex/pri/fr/oj/dat/2004/l_164/l_16420040430fr01140163.pdf.

[Dowell 1998] Dowell A. M. (1998). *Layer of protection analysis for determining safety integrity level*. ISA (The Instrumentation, Systems and Automation Society) Transactions 37(3): pp 155-165.

[Dubi 2000] Dubi A. (2000). *Monte Carlo applications in systems engineering*. Chichester, West Sussex, England; New York, USA, Wiley. ISBN 0471981729.

[Duquenne 2003] Duquenne N. (2003). *The safety management in an interoperability project like ERTMS. The French application*. WCRR 2003 - World Congress on Railway Research, Edimbourg, Ecosse, Royaume-Uni.

[Dutuit, Châtelet et al. 1997] Dutuit Y., Châtelet E., Signoret J.-P. et Thomas P. (1997). *Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases.* Reliability Engineering & System Safety 55(2): pp 117-124.

[Embrey 1992] Embrey D. E. (1992). *Incorporating management and organisational factors into probabilistic safety assessment*. Reliability Engineering & System Safety 38(1-2): pp 199-208.

[Everett, Keene et al. 1998] Everett W., Keene J. et Nikora A. (1998). *Applying software reliability engineering in the 1990s*. IEEE Transactions on Reliability 47(Septembre): pp 372-378.

[Ferson et Ginzburg 1996] Ferson S. et Ginzburg L. R. (1996). *Different methods are needed to propagate ignorance and variability*. Reliability Engineering & System Safety 54(2-3): pp 133-144.

[Fishman 1996] Fishman G. S. (1996). *Monte Carlo concepts, algorithms, and applications*. Springer series in operations research. New York, USA; Berlin, Allemagne, Springer. ISBN 0-387-94527-X.

[Fransson 2001] Fransson M. (2001). *InterFlow, a low cost communication based signalling system.* WCRR 2001 - World Congress on Railway Research, Cologne, Allemagne.

[Fremaux et Noé 2002] Fremaux F. et Noé A. (2002). *Le système de sécurité "TGV" de la SNCF.* Revue générale des chemins de fer - Février: pp 13-21.

[Goble 1998] Goble W. M. (1998). *Control systems safety evaluation and reliability (2nd ed.)*. Research Triangle Park (NC), ISA (The Instrumentation, Systems, and Automation Society).

[Habrias 2001] Habrias H. (2001). *Spécification formelle avec B*. Paris, France, Lavoisier. ISBN 2-7462-0302-2.

[Hadj-Mabrouk, Hadj-Mabrouk et al. 2001] Hadj-Mabrouk H., Hadj-Mabrouk A. et Dogui M. (2001). *Sécurité ferroviaire et facteurs humains, apport de la chronobiologie de la vigilance*. Les collections de l'INRETS, n°38. Institut National de Recherche sur les Transports et leur Sécurité. ISBN 285782-558-7.

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

[Hasan 2002] Hasan R. (2002). *Contribution à l'amélioration des performances des systèmes complexes par la prise en compte des aspects socio-techniques dès la conception. Proposition d'un modèle original de situation de travail pour une nouvelle approche de conception.* Thèse de doctorat. Institut National de Recherche et de Sécurité. Université Henri Poincaré Nancy 1.

[Hasan, Bernard et al. 2003] Hasan R., Bernard A., Ciccotelli J. et Martin P. (2003). *Integrating safety into the design process: elements and concepts relative to the working situation.* Safety Science 41(2-3): pp 155-179.

[Hoegberg 1998] Hoegberg L. (1998). *Risk perception, safety goals and regulatory decision-making.* Reliability Engineering & System Safety 59(1): pp 135-139.

[Hofer, Kloos et al. 2002] Hofer E., Kloos M., Krzykaz-Hausmann B., Peschke J. et Sonnenkalb M. (2002). *Dynamic Event Trees for Probabilistic Safety Analysis*. EUROSAFE, Berlin, Allemagne, IRSN (Institut de Radioprotection et de Sûreté Nucléaire), GRS (Gesellschaft für Anlagen - und Reaktorsicherheit).

[IEC 60050-821 1998] IEC 60050-821 (1998). *Vocabulaire électronique international. Partie 821: Signalisation et appareils de sécurité pour chemin de fer*. Geneva, Switzerland, IEC, International Electrotechnical Commission.

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

[IEC 61508 2000] IEC 61508 (2000). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. IEC 61508-1 to 7. Geneva, Switzerland, IEC, International Electrotechnical Commission.

[IEC 61511 2003] IEC 61511 (2003). *Functional safety - Safety instrumented systems for the process industry sector*. Geneva, Switzerland, IEC, International Electrotechnical Commission.

[IEC 62061/Ed.1 2005] IEC 62061/Ed.1 (2005). *Safety of machinery - Functional safety of electrical, electronic and programmable control systems for machinery (Project)*. Geneva, Switzerland, IEC, International Electrotechnical Commission.

[Kosmowski et Sliwinski 2005] Kosmowski K. T. et Sliwinski M. (2005). *Methodology for functional safety assessment*. ESREL 2005 - European safety and reliability conference, Gdansk, Poland. In Kołowrocki (eds), pp 1173-1180, Taylor & Francis Group, London. ISBN 0-415-38340-4.

[Kumamoto et Henley 1996] Kumamoto H. et Henley E. J. (1996). *Probabilistic risk assessment and management for engineers and scientists*. New York, IEEE Press. ISBN 0780310047.

[Labeau 2000] Labeau P.-E. (2000). *Partially unbiased estimators for reliability and availability calculations*. Progress in Nuclear Energy 36(2): pp 131-187.

[Labeau, Smidts et al. 2000] Labeau P. E., Smidts C. et Swaminathan S. (2000). *Dynamic reliability: towards an integrated platform for probabilistic risk assessment*. Reliability Engineering & System Safety 68: pp 219-254.

[Labeau et Zio 2001] Labeau P. E. et Zio E. (2001). *Biaising schemes in component-based and system-based Monte Carlo algorithms in system engineering*. ESREL 2001 - European safety and reliability conference, Torino, Italy. In Zio, Demichela and Piccinini (eds), pp 903-910, Politecnico di Torino.

[Labeau et Zio 2002] Labeau P. E. et Zio E. (2002). *Procedures of Monte Carlo transport simulation for applications in system engineering*. Reliability Engineering & System Safety 77(3): pp 217-228.

[Lamy 2002] Lamy P. (2002). *Probabilité de défaillance dangereuse d'un système: explications et exemple de calcul*. INRS (Institut National de Recherche et de Sécurité) Note scientifique et Technique n°225.

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

[Le Moigne 1990] Le Moigne J.-L. (1990). *La modélisation des systèmes complexes*. Afcet Systèmes. Paris, France, Dunod. ISBN 2-04-019704-4.

[Le Moigne 1994] Le Moigne J.-L. (1994). *La théorie du système général, théorie de la modélisation (4ème éd.)*. Paris, Presses universitaires de France. ISBN 2-13-046515-3.

[Lind 1994] Lind M. (1994). *Modeling goals and functions of complex industrial plants*. Applied Artificial Intelligence 8(2): pp 259-283.

[Livre Blanc 2001] Livre Blanc, Commission des Communautés Européennes (2001). *La politique européenne des transports à l'horizon 2010: l'heure des choix*. Bruxelles, Belgique, http://ec.europa.eu/comm/off/white/index_fr.htm.

[Lyonnet 2000] Lyonnet P. (2000). *La maintenance mathématiques et méthodes*. Londres, Paris, New York, Tec et doc. ISBN 2-7430-0419-3.

[Maalej, Delcroix et al. 2003] Maalej M.-A., Delcroix V. et Piechowiak S. (2003). *Les réseaux bayésiens pour la recherche des diagnostics*. PENTOM 2003 - Performances et Nouvelles Technologies en Maintenance, Valenciennes, France, pp 315-327, Presses Universitaires de Valenciennes. ISBN 2-905725-51-6.

[Marseguerra et Zio 2002] Marseguerra M. et Zio E. (2002). *Basics of the Monte Carlo Method with Application to System Reliability.* Hagen, Germany, LiLoLe Verlag. ISBN 3-934447-06-6.

[Melchers 2001] Melchers R. E. (2001). *On the ALARP approach to risk management.* Reliability Engineering & System Safety 71(2): pp 201-208.

[Millot 1999] Millot P. (1999). *Systèmes Homme-Machine et Automatique*. JDA'99 - Journées Doctorales d'Automatique, conférence plénière, Nancy, France.

[Monin 2000] Monin J.-F. (2000). *Introduction aux méthodes formelles (2nd ed.)*. Collection technique et scientifique des télécommunications. Paris, France, Hermès Science Publications. ISBN 2-7462-0140-2.

[Morin 1990] Morin E. (1990). *Introduction à la pensée complexe*. Collection: Communication et complexité. Paris, France, Éditions Sociales Françaises. ISBN 2-7101-0800-3.

[Musa 1998] Musa J. (1998). *Software Reliability Engineering: more reliable software, faster development and testing*. New-York, USA, McGraw-Hill. ISBN 0-07-913271-5.

[Narbonne 2005] Narbonne Y. (2005). *Complexité et systémique*. Paris, France, Hermès Sciences Publications. ISBN 2-7462-1110-6.

[Pagès 1980] Pagès A. (1980). *Fiabilité des systèmes.* Collection de la Direction des études et recherches d'Electricité de France. Paris, Eyrolles.

[Pasquet 1999] Pasquet S. (1999). *Analyse de sûreté de fonctionnement de systèmes dynamiques à l'aide de diagrammes de flux et réseaux de neurones.* Thèse de doctorat. LM2S (Laboratoire de Modélisation et Sûreté des Systèmes). Université Technologique de Troyes.

[Peled 2001] Peled D. A. (2001). *Software Reliability Methods*. New York, USA; Berlin, Allemagne, Springer-Verlag. ISBN 0-387-95106-7.

[Planchette 2002] Planchette G. (2002). *Et si les risques m'étaient comptés!* Toulouse, Octares. ISBN 2-906769-82-7.

[Polet 2002] Polet P. (2002). *Modélisation des Franchissements de Barrières pour l'Analyse des Risques des Systèmes Homme-Machine.* Thèse de doctorat. LAMIH (Laboratoire d'Automatique, de Mécanique et d'Informatique Industrielles et Humaines). UVHC (Université de Valenciennes et du Hainaut-Cambrésis).

[Procaccia et Suhner 2003] Procaccia H. et Suhner M.-C. (2003). *Démarche bayésienne et applications à la sûreté de fonctionnement*. Paris, France, Lavoisier. ISBN 2-7462-0600-5.

[Rausand et Høyland 2004] Rausand M. et Høyland A. (2004). *System Reliability Theory: Models, Statistical Methods and Applications (2nd ed.)*. Wiley series in probability and statistics. Hoboken, New Jersey, John Wiley & Sons, Inc. ISBN 0-471-47144-X.

[Renpenning et Braband 2002] Renpenning F. et Braband J. (2002). *Risk assessment of a novel railway signalling concept*. Lambda-Mu - ESREL 2002 - European Conference, Lyon, france, pp 251-257.

[Rodriguez 2004] Rodriguez J. (2004). *Gestion et optimisation des réseaux de transport (Projet 6)*. Février 2004, Séminaire du pôle ST2 - Sciences et Technologies pour la Sécurité dans les Transports.

[Rouvroye 2001] Rouvroye J. L. (2001). *Enhanced Markov Analysis as a method to assess safety in the process industry.* Beta Research School for Operations Management and Logistics. Technische Universiteit Eindhoven, The Netherlands.

[Rubinstein 1981] Rubinstein R. Y. (1981). *Simulation and the Monte Carlo Method*. Wiley series in probability and mathematical statistics. New York, USA; Chichester, England, John Wiley & Sons, Inc. ISBN 0-471-08917-6.

[SAMRAIL 2004] SAMRAIL, Wigger P., Schäbe H. et Schmitz D. (2004). *Standards and best practice, Report D.2.7.1 of the SAMRAIL project*. 5ème programme cadre européen. SAMRAIL (Safety Management in Railways).

[Schäbe 2001] Schäbe H. (2001). *Different approaches for determination of tolerable hazard rates*. ESREL 2001 - European safety and reliability conference, Torino, Italy. In Zio, Demichela and Piccinini (eds), pp 435-442, Politecnico di Torino.

[Schäbe 2002] Schäbe H. (2002). *The Safety Philosophy behind the CENELEC Railway Standards*. ESREL 2002 - European safety and reliability conference, Lyon, France.

[Schäbe 2003] Schäbe H. (2003). *Apportionment of safety integrity levels in complex electronically controlled systems*. ESREL 2003 - European safety and reliability conference, Maastricht, The Netherlands. In Bedford and v. Gelder (eds), pp 1395-1400, Swets & Zeitlinger. ISBN 90-5809-551 7.

[Schäbe et Wigger 2000] Schäbe H. et Wigger P. (2000). *Experience with SIL allocation in Railway Applications*. 4th International Symposium Programmable Electronic Systems in Safety Related Applications, Köln, Germany.

[Sharpe 2004] Sharpe A. (2004). *Safety Decision Making for the Railway*. Practical Elements of Safety: Proceedings of the Twelfth Safety-critical Systems Symposium. In F. Redmill and T. Anderson (eds), Springer Verlag London, UK.

[Signoret et Chabot 2002] Signoret J.-P. et Chabot J.-L. (2002). *Comment cacher un réseau de Petri derrière un bloc diagramme de fiabilité*. ESREL 2002 - European safety and reliability conference, Lyon, France, pp 319-324.

[Smith et Simpson 2004] Smith D. J. et Simpson K. G. L. (2004). *Functional safety: a straightforward guide to IEC 61508 and related standards*. Boston, Elsevier. ISBN 0750662697.

[Sourisse et Boudillon 1996] Sourisse C. et Boudillon L. (1996). *La sécurité des machines automatisées. Tome 1: notions de base, règlementation, normes, techniques de prévention*. Cergy-Pontoise, France, Institut Schneider Formation. ISBN 2-907314-29-7.

[Stavrianidis et Bhimavarapu 2000] Stavrianidis P. et Bhimavarapu K. (2000). *Performance-based standards: safety instrumented functions and safety integrity levels*. Journal of Hazardous Materials 71(1-3): pp 449-465.

[Summers 1998] Summers A. E. (1998). *Techniques for assigning a target safety integrity level*. ISA (The Instrumentation, Systems and Automation Society) Transactions 37(2): pp 95-104.

[Summers 2003] Summers A. E. (2003). *Introduction to layers of protection analysis*. Journal of Hazardous Materials 104(1-3): pp 163-168.

[Swain et Guttmann 1983] Swain A. D. et Guttmann H. E. (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications*. NUREG/CR-1278.

[Tyrell 2001] Tyrell D. (2001). *Overview of Full-Scale Rail Vehicle Impact Tests in the USA*. WCRR 2001 - World Congress on Railway Research, Cologne, Allemagne.

[UGTMS D6 2003] UGTMS D6, Cassir C.,Schütte J., Cauffriez L., Beugin J., Renaux D., Millot P., Cacciabue P.C. et Evans A. (2003). *Safety conceptual approach and guidelines. Deliverable D6 of the UGTMS project.* 5ème programme cadre européen. UGTMS (Urban Guided Transport Management System).

[UGTMS D9 2004] UGTMS D9 (2004). *UGTMS functions and architecture. Deliverable D9 of the UGTMS project.* 5ème programme cadre européen. UGTMS (Urban Guided Transport Management System).

[Vallée 2003] Vallée F. (2003). *Sécurité informatique pour la gestion des risques*. Techniques de l'Ingénieur SE2500 (dossier Sécurité et Gestion de l'Environnement).

[Vanderhaegen 2003] Vanderhaegen F. (2003). *Analyse et contrôle de l'erreur humaine*. Paris, France, Lavoisier. ISBN 2-7462-0722-2.

[Villemeur 1988] Villemeur A. (1988). *Sûreté de fonctionnement des systèmes industriels fiabilité, facteurs humains, informatisation*. Collection de la Direction des études et recherches d'Electricité de France. Paris, Eyrolles.

[Weber, Cerisier et al. 2005] Weber P., Cerisier L. et Jouffe L. (2005). *Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN)*. Reliability Engineering & System Safety, in press.

[Zhang, Long et al. 2003] Zhang T., Long W. et Sato Y. (2003). *Availability of systems with self-diagnostic components - applying Markov model to IEC 61508-6.* Reliability Engineering & System Safety 80(2): pp 133-141.

[Zwingelstein 1995] Zwingelstein G. (1995). *Diagnostic des défaillances.* Paris, France, Hermès. ISBN 2-86601-463-4.

[Zwingelstein 1999] Zwingelstein G. (1999). *Sûreté de fonctionnement des systèmes industriels complexes*. Techniques de l'Ingénieur S8250 (dossier Informatique Industrielle).

Annexes

Sommaire

ANNEXE A. THEORIE DU TRANSPORT DE PARTICULES APPLIQUEE A LA DYNAMIQUE DES SYSTEMES – EVALUATION PAR SIMULATION DE MONTE CARLO 154
A.1 Théorie du transport de particules appliquée à la dynamique des systèmes 154
A.2 Algorithme d'évaluation par simulation de Monte Carlo biaisée 158
ANNEXE B. FONCTIONS REALISEES PAR LES PRINCIPAUX SYSTEMES DE TRANSPORT GUIDE EXISTANTS 159
ANNEXE C. TERMINOLOGIE RELATIVE A L'ETUDE DES DEFAILLANCES DANGEREUSES D'UN SYSTEME DE SECURITE 165
C.1 La typologie des défaillances 165
C.2 Les tests périodiques 165
C.3 Les tests de diagnostic 166
C.4 Le taux de couverture des tests de diagnostic 166
C.5 La proportion de défaillances en sécurité 167
ANNEXE D. EXEMPLE D'INSTANCIATION DES CLASSES DU MODELE DE SITUATION D'EXPLOITATION RELATIVES A L'OPERATEUR HUMAIN 168
D.1 La classe « activité » 168
D.2 La classe « équipe d'opérateurs » 168
D.3 La classe « mode d'exploitation » 169
ANNEXE E. FONCTION DE STRUCTURE DU SYSTEME ETUDIE 170
E.1 Caractéristiques des fonctions de sécurité du système 170
E.2 Désignation des fonctions de sécurité dupliquées 171
E.3 Fonction de structure 172

Annexe A. Théorie du transport de particules appliquée à la dynamique des systèmes – évaluation par simulation de Monte Carlo

A.1 Théorie du transport de particules appliquée à la dynamique des systèmes

L'estimation de la fiabilité dynamique par une simulation de Monte Carlo repose sur la théorie du transport de particules neutres avec collision et sans fission [Labeau 2000], c'est-à-dire qu'une particule émise depuis une source se déplace en ligne droite jusqu'à ce qu'elle subisse une collision qui l'envoie dans une autre direction sans la production de plusieurs autres particules. La densité de collision $\psi(P)$ en P est exprimée par l'équation (A.1), où $Q(P')T(P' \to P)$ est la densité d'émission de particules depuis une source P' jusqu'en P sans collision, et $\psi(P'')C(P'' \to P')T(P',P)$ est la densité d'entrée en collision d'une particule à P'' repartant avec la coordonnée P' jusqu'en P sans collision. Une particule peut être absorbée lors d'une collision, mettant ainsi fin à son transport.¨

$$\psi(P) = \int Q(P').T(P' \to P).dP' + \iint \psi(P'').T(P' \to P).C(P'' \to P').dP'.dP'' \qquad \text{(A.1)}$$

<u>Paramètres de l'équation (A.1)</u>

- P Coordonnées (vitesse et position) d'une particule
- $Q(P)$ Densité de source
- $T(P' \to P)$ Noyau de transition ou noyau de libre parcours d'une particule de P' vers P
- $C(P' \to P)$ Noyau de collision d'une particule en P' repartant en P

L'évolution temporelle d'un système complexe est analogue au processus de transport de particules dans le sens où les changements d'états du système ou transitions sont assimilables à des collisions de particules, et les états de pannes, pour l'évaluation de la fiabilité, sont assimilables à des états absorbants. De plus, la formulation –ci après– de l'équation de densité de transition d'un système composé de *n* états démontre cette équivalence.

La densité de transition, ou densité d'événement, est le nombre d'entrées du système dans l'état *k*, notée $\psi_k(t)$ et énoncée dans l'équation (A.2) [Dubi 2000]. Le nombre d'entrées du système dans l'état k' à τ, dans l'intervalle de temps infinitésimal $d\tau$, correspond à la probabilité $\psi_{k'}(\tau).d\tau$. Ajouté le fait que le système reste dans *k'* jusqu'à l'instant $t > \tau$, la probabilité s'écrit $\psi_{k'}(\tau).R_{k'}(t-\tau).d\tau$, où $R_{k'}(t-\tau) = 1 - F_{k'}(t-\tau)$ (« fiabilité de l'état ») est la probabilité de rester dans l'état *k'* jusqu'à l'instant *t*. La probabilité par unité de temps que le système entre ensuite dans l'état *k* à *t* s'écrit finalement $\psi_{k'}(\tau).R_{k'}(t-\tau).z_{k'\to k}(t-\tau).d\tau$ où le facteur $z_{k'\to k}(t-\tau)$ est explicité ci dessous. En intégrant sur l'espace de temps (continu) et d'état (discret), il vient le second terme de l'équation (A.2). Le terme source $\psi_k^0(t) = P_{k_0}.\delta(t-t_0)$ représente la probabilité d'entrée du système dans l'état k_0 à l'instant t_0 (sachant $\delta(0) = 1$ $\delta(t-t_0 \mid t \neq t_0) = 0$).

$$\begin{aligned}
\psi_k(t) &= \psi_k^0(t) + \sum_{k'} \int_0^t \psi_{k'}(\tau).R_{k'}(t-\tau).z_{k'\to k}(t-\tau).d\tau \\
&= \psi_k^0(t) + \sum_{k'} \int_0^t \psi_{k'}(\tau).\frac{z_{k'\to k}(t-\tau)}{z_{k'}(t-\tau)}.z_{k'}(t-\tau).R_{k'}(t-\tau).d\tau \qquad \text{(A.2)} \\
&= \psi_k^0(t) + \sum_{k'} \int_0^t \psi_{k'}(\tau).C(t,k'\to k).T(k',\tau\to t).d\tau
\end{aligned}$$

<u>Paramètres de l'équation (A.2)</u>

- $z_k(t) = \dfrac{f_k(t)}{1-F_k(t)}$ fonction de taux ou fonction de hasard (probabilité par unité de temps qu'un événement arrive à *t* en partant de l'état *k*) impliquant $F_k(t) = 1 - e^{-\int_0^t z_k(x)dx}$ et $f_k(t) = \dfrac{dF_k(t)}{dt} = z_k(t)e^{-\int_0^t z_k(x)dx}$
- $z_{k'\to k}(t-\tau)$ fonction de hasard partielle pour le passage d'un état *k'* entré à τ vers un état *k* à l'instant *t* la fonction de hasard totale est $z_k(t-\tau) = \sum_{j=1}^{n} z_{j\to k}(t-\tau)$

  d'où $f_k(t-\tau) = \left(\sum_{j=1}^{n} z_{j\to k}(t-\tau)\right) e^{-\int_\tau^t z_k(x)dx}$
- $R_k(t-\tau) = e^{-\int_\tau^t z_k(x)dx}$ est la probabilité que le système ne sorte pas de l'état *k* avant *t* sachant qu'il y est entré à $\tau < t$.

- $T(k',\tau \to t) = z_{k'}(t-\tau).R_{k'}(t-\tau) = z_{k'}(t-\tau).e^{-\int_\tau^t z_{k'}(x)dx}$ est le noyau de transition ou noyau de libre parcours (densité de changement d'état à *t* sachant que le système était dans l'état *k'* à τ)
- $C(t,k' \to k) = \dfrac{z_{k'\to k}(t-\tau)}{z_{k'}(t-\tau)}$ est le noyau de collision (densité de transition vers l'état *k* hors de l'état *k'*)

L'équation (A.2) est clairement analogue à l'équation de transport de particule (A.1) présentée précédemment, d'où son nom d'équation de transport du système définie sur l'espace de temps et d'état de ce système.

<u>Notion de taux de réaction :</u>

Dans le domaine du transport des particules, une problématique est l'évaluation du taux de réaction *G* représenté dans l'équation (A.3) [Labeau 2000]. Ce taux peut être estimé par simulation de Monte Carlo.

$$G = \int \psi(P).f(P).dP = \sum_{i=0}^{\infty} \int \psi_i(P).f(P).dP \tag{A.3}$$

Le calcul de l'estimation consiste, à partir de *N* réalisations de la variable *P* distribuée selon $\psi(P)$, à calculer la moyenne des valeurs prises par *f(P)*, *G* est alors approché par $\tilde{G}$ (cf. l'équation (A.4)) et *f(P)* désigne un estimateur sans biais de *G*.

$$\tilde{G} = \frac{1}{N}\sum_{i=1}^{N} f(P) \tag{A.4}$$

La forme équivalente de l'équation (A.3) dans le domaine de la dynamique des systèmes est représentée par l'équation (A.5). $G(t)$ est l'expression générale, à l'instant *t*, de la probabilité associée aux critères de sûreté (fiabilité, disponibilité, maintenabilité).

$$G(t) = \sum_k \int_0^t \psi_k(\tau).R_k(t-\tau).d\tau \tag{A.5}$$

Du fait de l'analogie des deux domaines, G est également évaluable par simulation de Monte Carlo à partir de l'échantillonnage dans le temps et l'espace de $\psi_k(t)$, et de l'utilisation de compteurs associés à $R_k(t-\tau)$ sur les *N* scénarios (histoires) du système générés.

Notion de fonction de structure associée à l'état du système :

Alors que la trajectoire d'une particule P est déterminée par l'évolution de ses coordonnées, un système évolue selon le couple *(k,t)* où le facteur k correspond à l'état du système à l'instant t. Cet état est obtenu selon la configuration et les états propres des N_C composants constituant le système. Pour modéliser cette configuration de nature déterministe, une fonction de structure S telle que $k = S(j_1,...,j_i,...,j_{N_C})$ est employée. j_i désigne l'état courant associé à chacun des composants i possédant N_S^i états. La fonction S permet de coder les dépendances entre composants, et l'influence de leurs modes de défaillance et de réparation sur chacun d'entre-eux. Ainsi l'état du système est échantillonné à partir des transitions aléatoires associées à ses composants, et pour chaque transition d'un composant d'un état à un autre, la fonction de structure est réévaluée pour fournir le nouvel état du système.

A.2 Algorithme d'évaluation par simulation de Monte Carlo biaisée

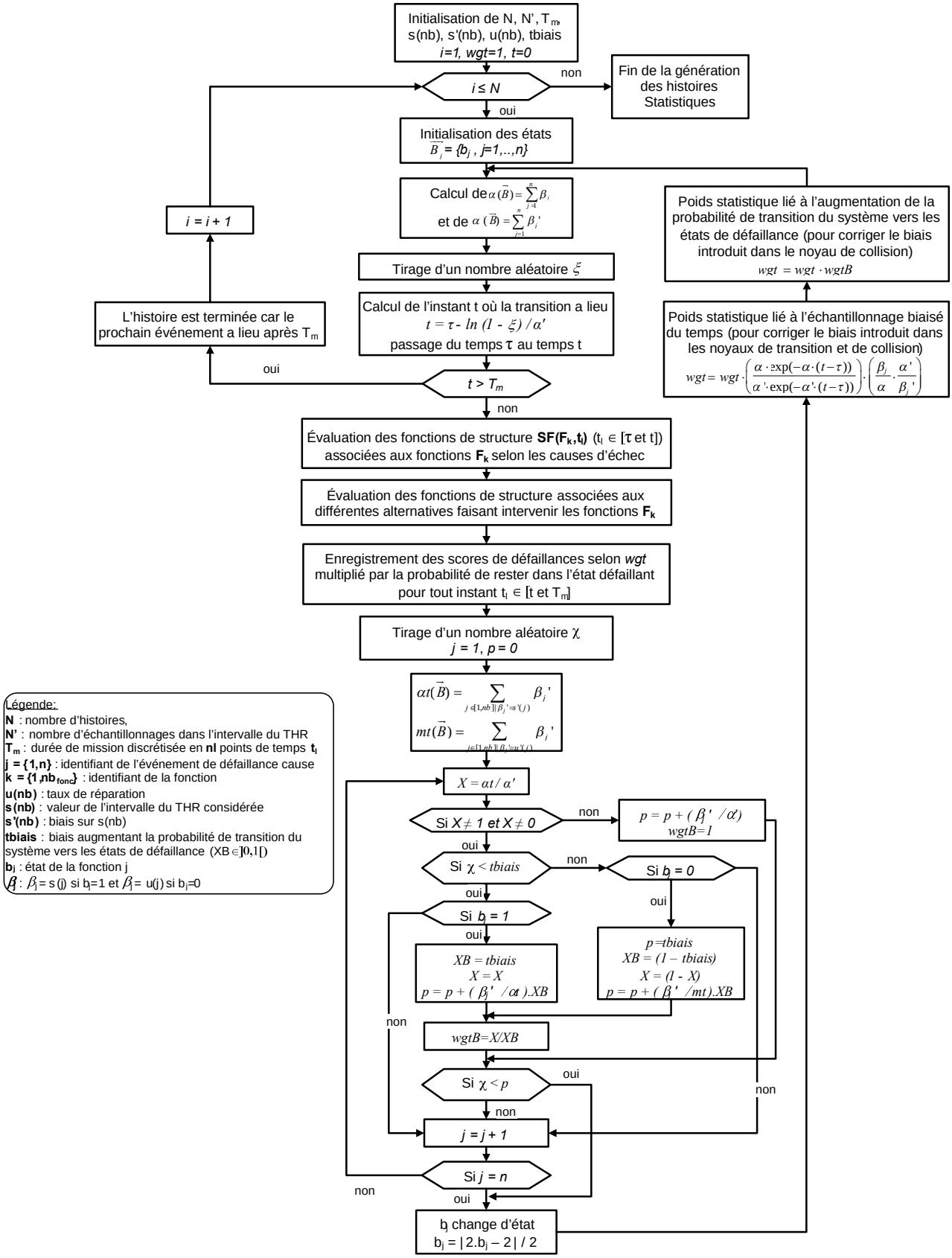


Figure A.1 Algorithme de la simulation de Monte Carlo biaisée utilisé pour l'évaluation de scénarios de risque

Annexe B. Fonctions réalisées par les principaux systèmes de transport guidé existants

Tableau B.1 Récents systèmes de signalisation pour les réseaux conventionnels ou grande vitesse

Systèmes de signalisation pour les réseaux conventionnels ou grande vitesse						
Type d'équipement / Syst. de signalisation	**Fonctions du système de signalisation bord**		**Fonctions du système de signalisation sol**			
	Fonctions du calculateur bord (système ATP bord)	Fonctions de l'affichage en cabine dédié à l'opérateur de conduite (interface homme/machine)	Fonctions du système d'enclenchement (partie du système ATP sol)	Fonctions des balises (avec présence éventuelle de boucles de détection) (partie du système ATP sol)	Fonctions des circuits de voie (avec éventuellement d'autres systèmes de détection tels les compteurs d'essieux)	Fonctions des signaux lumineux
ERTMS / ETCS niveau 1 (système adapté aux systèmes conventionnels basés sur les cantons fixes et les signaux)	- Enregistrement de l'autorisation de mouvement selon les informations issues des balises - Calcul du profil de vitesse jusqu'au prochain point cible - Contrôle en continu de la vitesse maximum autorisée selon l'autorisation de mouvement reçue, les caractéristiques du tronçon de voie reçues et les caractéristiques du matériel roulant préprogrammées dans le système bord - Déclenchement du système de freinage si le contrôle détecte une survitesse ou si un point d'arrêt est franchi	- Traduction de l'autorisation de mouvement par l'affichage de la vitesse courante, de la limite de vitesse, de la prochaine limite de vitesse, et de la distance restante où s'effectue ce prochain changement de vitesse - Indications sur le statut du système	- Protection des itinéraires (position correcte des aiguilles et signaux lumineux affichés pour éviter les itinéraires conflictuels) calculés selon l'occupation des voies et selon les caractéristiques des voies - Transfert de l'autorisation de mouvement, c'est-à-dire des informations issues de l'enclenchement (état des aiguilles et signaux) grâce aux balises	-Localisation des trains et transfert des données de localisation au système d'enclenchement qui calcule les autorisations de mouvement de chaque train -Transfert de l'autorisation de mouvement et des caractéristiques du tronçon de voie (paramètres locaux de restriction de vitesse, de pente…) au système bord - Transfert de l'état des signaux au système bord	- Détection et localisation des trains permettant la confirmation de l'intégrité du train	Protection d'un circuit de voie occupé
ERTMS / ETCS niv. 2	- Calcul de la position du train transférée ensuite numériquement par radio à l'antenne	- Traduction de l'autorisation de	- Réception par le centre radio (RBC) de la	- Transfert vers le train d'une référence de localisation	- Détection et localisation des trains permettant la	NU*

ERTMS / ETCS **niveau 2** (suite)	GSM-R pour la mise à jour dynamique du mouvement par le centre radio (RBC) - Enregistrement de l'autorisation de mouvement selon les informations reçues par l'antenne radio - Calcul du profil de vitesse jusqu'au prochain point d'arrêt - Contrôle en continu de la vitesse maximum autorisée selon l'autorisation de mouvement reçue, les caractéristiques du tronçon de voie préprogrammées dans le système bord et les caractéristiques du matériel roulant préprogrammées dans le système bord - Déclenchement du système de freinage si le contrôle détecte une survitesse ou si un point d'arrêt est franchi	mouvement par l'affichage de la vitesse courante, de la limite de vitesse, de la prochaine limite de vitesse, et de la distance restante où s'effectue ce prochain changement de vitesse - Indications sur le statut du système	localisation des trains - Protection des itinéraires (position correcte des aiguilles) calculés selon l'occupation des voies et les caractéristiques des voies - Transfert au système bord de l'autorisation de mouvement, c'est-à-dire des informations issues de l'enclenchement (état des aiguilles) grâce au centre radio (RBC) puis à l'antenne GSM-R	permettant la correction d'éventuelles erreurs de mesure faites dans par le système bord dans le calcul de la localisation	confirmation de l'intégrité du train	
ERTMS/ ETCS **niveau 3**	- Calcul de la position du train transférée ensuite numériquement par radio à l'antenne GSM-R pour la mise à jour dynamique du mouvement par le centre radio (RBC) - Enregistrement de l'autorisation de mouvement selon les informations reçue par l'antenne radio - Calcul du profil de vitesse jusqu'au prochain point cible - Contrôle en continu de la vitesse maximum autorisée selon l'autorisation de mouvement reçue, les caractéristiques du tronçon de voie préprogrammées dans le système bord et les caractéristiques du matériel roulant préprogrammées dans le système bord - Déclenchement du système de freinage si le contrôle détecte une survitesse ou si un point d'arrêt est franchi	- Traduction de l'autorisation de mouvement par l'affichage de la vitesse courante, de la limite de vitesse, de la prochaine limite de vitesse, et de la distance restante où s'effectue ce prochain changement de vitesse - Indications sur le statut du système	- Réception par le centre radio (RBC) de la localisation des trains - Protection des itinéraires (position correcte des aiguilles) calculés selon l'occupation des voies et les caractéristiques des voies - Transfert au système bord de l'autorisation de mouvement, basées sur le principe des cantons mobiles, grâce au centre radio (RBC) puis à l'antenne GSM-R	- Transfert vers le train d'une référence de localisation permettant la correction d'éventuelles erreurs de mesure faites par le système bord dans le calcul de la localisation	NU*	NU*

TVM 430 (système numérique)	- Enregistrement de l'autorisation de mouvement selon les informations issues des circuits de voie - Calcul du profil de vitesse jusqu'au prochain point cible - Contrôle en continu de la vitesse maximum autorisée selon l'autorisation de mouvement reçue, les caractéristiques du tronçon de voie reçues et les caractéristiques du matériel roulant préprogrammées dans le système bord - Déclenchement du système de freinage si le contrôle détecte une survitesse ou si un point d'arrêt est franchi	- Traduction de l'autorisation de mouvement par l'affichage de la vitesse courante, de la limite de vitesse, de la prochaine limite de vitesse, et de la distance restante où s'effectue ce prochain changement de vitesse - Indications sur le statut du système	- Protection des itinéraires (position correcte des aiguilles et signaux lumineux affichés pour éviter les itinéraires conflictuels) calculés selon l'occupation des voies et les données relatives aux voies - Transfert au système bord de l'autorisation de mouvement, c'est-à-dire des informations issues de l'enclenchement (état des aiguilles et signaux) et grâce aux rails	NU*	- Détection et localisation des trains - Transfert des restrictions de vitesse et des caractéristiques du tronçon de voie (paramètres locaux de restriction de vitesse, de pente…) au système bord - Transfert de l'autorisation de mouvement au système bord	NU* (des repères sont utilisés pour délimiter les cantons)
KVB (système analogique)	- Enregistrement de l'autorisation de mouvement selon les informations issues des balises - Calcul du profil de vitesse jusqu'au prochain point cible - Contrôle en continu de la vitesse maximum autorisée selon l'autorisation de mouvement reçue, les caractéristiques du tronçon de voie reçues, la vitesse limite indiquée par les balises et les caractéristiques du matériel roulant préprogrammées dans le système bord - Déclenchement du système de freinage si le contrôle détecte une survitesse ou si un point d'arrêt est franchi	- Traduction de l'autorisation de mouvement par l'affichage de la vitesse courante, de la limite de vitesse, de la prochaine limite de vitesse, et de la distance restante où s'effectue ce prochain changement de vitesse - Indications sur le statut du système	- Protection des itinéraires (position correcte des aiguilles et signaux lumineux affichés pour éviter les itinéraires conflictuels) calculés selon l'occupation des voies et les données relatives aux voies - Transfert au système bord de l'autorisation de mouvement, c'est-à-dire des informations issues de l'enclenchement (état des aiguilles et signaux) grâce aux balises	-Transfert de la vitesse limite à la hauteur de la balise - Transfert de l'autorisation de mouvement et des caractéristiques du tronçon de voie au système bord - Transfert de l'état des signaux au système bord	(système KVBP : possible transmission électrique continue d'informations codées par les rails)	NU*

* Non utilisé

Tableau B.2 Récents systèmes de signalisation pour les réseaux urbains [Beugin 2003]

Système de signalisation pour les réseaux urbains								
Type d'équipement / Syst. de signalisation	**Fonctions du système de signalisation bord**			**Fonctions du système de signalisation sol**				
	Fonctions du calculateur bord (système ATP bord)	Fonctions de l'ATO	Fonctions de l'affichage en cabine dédié à l'opérateur de conduite (interface homme/machine)	Fonctions du système d'enclenchement (partie du système ATP sol)	Fonctions des balises (avec présence éventuelle de boucles de détection) (partie du système ATP sol)	Fonctions des circuits de voie	Fonctions du tapis de transmission	Fonctions des signaux lumineux
PA (mode de conduite disponible dans tous les métros exploités par la RATP)	- Contrôle de la vitesse limite transmise par le sol (tapis), définie selon le type de train ayant les plus basses performances	- Commande de l'accélération, du freinage, de l'arrêt en station en fonction des caractéristiques de la voie et du matériel roulant - Gestion du temps d'arrêt en station - Gestion des ordres de la régulation - Gestion de l'allure pour le confort des voyageurs	NU* (Pupitre de commande standard)	- Protection des itinéraires (vérification de l'état des signaux lumineux affichés pour éviter les itinéraires conflictuels) calculés selon l'occupation des voies et les données relatives aux voies	Mesure la vitesse des trains	- Détection et localisation des trains	- Transmission des informations de vitesse selon les caractéristiques de la voie préprogrammées dans le tapis et selon l'occupation des cantons (choix de 2 programmes de marche paramétrés dans le tapis : un pour la marche normale, un pour l'arrêt) aussi bien pour les métros sur pneus que les métros sur rails	Bloc automatique lumineux dont l'état est fonction de l'occupation des circuits de voie

SACEM (système utilisé sur la partie centrale de la ligne RER A du réseau RATP)	- Enregistrement de l'autorisation de mouvement selon les informations issues des circuits de voie - Calcul du profil de vitesse jusqu'au prochain point cible - Contrôle en continu de la vitesse maximum autorisée (comparée aux informations de vitesse issues d'une roue phonique) selon l'autorisation de mouvement reçue, les caractéristiques du tronçon de voie reçues et les caractéristiques du matériel roulant préprogrammées dans le système bord - Déclenchement du système de freinage si le contrôle détecte une survitesse ou si un point d'arrêt est franchi	- Gestion de l'arrêt en station en fonction des caractéristiques de la voie et du matériel roulant -Gestion des ordres de la régulation - Gestion de l'allure pour le confort des voyageurs	- Traduction de l'autorisation de mouvement par l'affichage de la vitesse courante, de la limite de vitesse, de la prochaine limite de vitesse, et d'informations sur l'espacement entre les trains	- Protection des itinéraires (position correcte des aiguilles et signaux lumineux affichés pour éviter les itinéraires conflictuels) calculés selon l'occupation des voies et les données relatives aux voies - Transfert au système bord de l'autorisation de mouvement, c'est-à-dire des informations issues de l'enclenchement (état des aiguilles et signaux) et grâce aux rails - Annulation de la signalisation latérale au fur et à mesure de l'avancement des trains (extinction des signaux lumineux et affichage d'une croix de saint André caractéristique du SACEM)	- Vérification que le train passant la balise est bien équipé de SACEM pour permettre l'annulation des signaux - Localisation des trains et transfert des données de localisation au système d'enclenchement qui calcule les autorisations de mouvement de chaque train -Transfert de l'autorisation de mouvement et des caractéristiques du tronçon de voie (paramètres locaux de restriction de vitesse, de pente…) au système bord	- Découpage optimisé des cantons de signalisation en gare - Détection et localisation des trains - Transfert des restrictions de vitesse et des caractéristiques du tronçon de voie (paramètres locaux de restriction de vitesse, de pente…) au système bord - Transfert de l'autorisation de mouvement au système bord	NU*	Signaux utilisés uniquement en cas de panne du système
SAET (système de la ligne de métro 14 du réseau RATP entièrement automatisé)	- Enregistrement de l'autorisation de mouvement (comparée aux informations de vitesse issues d'une roue phonique) selon les informations issues du tapis de transmission - Calcul du profil de	- Commande de l'accélération, du freinage, de l'arrêt en station en fonction des caractéristiques de la voie et du matériel roulant	NU* (Pas de conducteur)	- Protection des itinéraires calculés selon l'occupation des voies et les données relatives aux voies - Transfert au système bord de l'autorisation de mouvement, c'est-à-dire des informations issues	- Transfert vers le train d'une référence de localisation permettant la correction d'éventuelles erreurs de mesure faites par le système bord dans le calcul de la	- Détection et localisation des trains	- Transmission des informations de vitesse selon les caractéristiques de la voie préprogrammées dans le tapis et selon l'occupation	Signaux simplifiés utilisés uniquement en cas de panne du système

SAET (système de la ligne de métro 14 du réseau RATP entièrement automatisé) (suite)	vitesse jusqu'au prochain point cible - Contrôle en continu de la vitesse maximum autorisée selon l'autorisation de mouvement reçue, les caractéristiques du tronçon de voie reçues et les caractéristiques du matériel roulant préprogrammées dans le système bord - Déclenchement du système de freinage si le contrôle détecte une survitesse ou si un point d'arrêt est franchi - Vérification que les portes sont bien fermées	- Gestion du temps d'arrêt en station et de l'ouverture et de la fermeture des portes du trains et des portes palières -Gestion des ordres de la régulation - Gestion de l'allure pour le confort des voyageurs		de l'enclenchement (état des aiguilles et signaux) et grâce aux rails	localisation		des cantons (choix de 2 programmes de marche paramétrés dans le tapis : un pour la marche normale, un pour l'arrêt)	

* Non utilisé

Quelques références Internet pour les systèmes de signalisation pour les réseaux conventionnels ou grande vitesse:

http://www.ertms.com

http://www.railway-technical.com

Quelques références Internet pour les systèmes de signalisation pour les réseaux urbains:

http://www.metro-pole.net/expl/sacem

http://www.navily.net/regulrera.php

Annexe C. Terminologie relative à l'étude des défaillances dangereuses d'un système de sécurité

C.1 La typologie des défaillances

Les SIL sont attribués aux systèmes de sécurité sur la base de l'étude de leurs défaillances dangereuses, sous ensemble des défaillances (cf. Figure C.1).

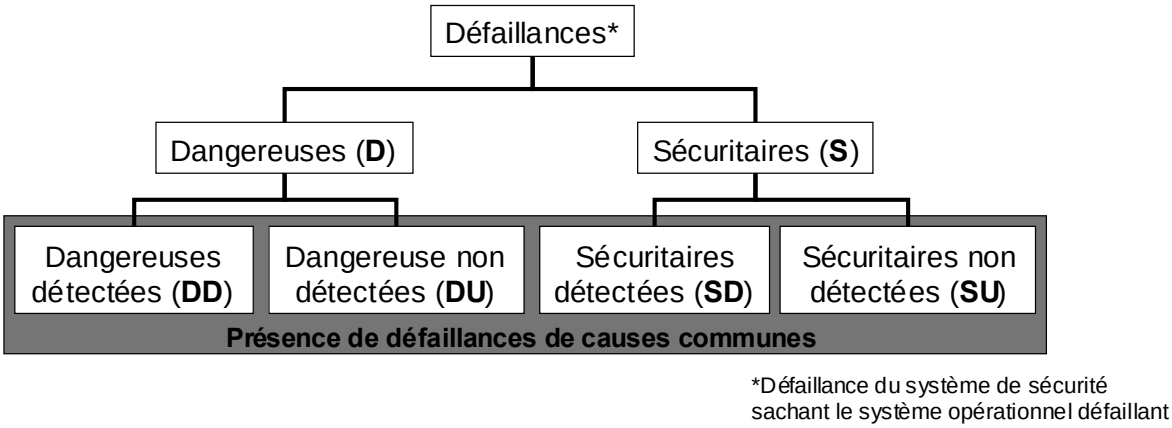


Figure C.1 Classification des défaillances

Les défaillances dangereuses peuvent également être analysées selon leur détection possible par des tests périodiques ou par des tests de diagnostic. Un système de sécurité faiblement sollicité peut en effet être inopérant, lors d'une demande d'action par le système opérationnel, car il peut se trouver dans un état défaillant non identifié, donc non résolu avant son activation.

C.2 Les tests périodiques

Les tests périodiques (*proof tests*) sont des tests hors ligne destinés à détecter les défaillances d'un *système* relatif à la sécurité de telle sorte que le système puisse être réparé afin de revenir dans un état équivalent à son état initial.

C.3 Les tests de diagnostic

Les tests de diagnostic (*autotests*) sont des tests automatiques en ligne (watchdog –chien de garde–, checksum –test de mémoire–) effectués périodiquement pour détecter des défauts de *composants*. Ces tests peuvent être compensés par des tests périodiques, de période plus allongée, pour révéler des défaillances d'ordre plus global, au niveau du système. L'intervalle de temps entre tests doit nécessairement être plus petit que l'intervalle de demande du système de sécurité faiblement sollicité.

C.4 Le taux de couverture des tests de diagnostic

La norme [IEC 61508 2000] (partie 2) définit un taux de couverture des tests de diagnostic DC (*Diagnostic Coverage*) désignant la probabilité qu'une panne soit détectée par un test de diagnostic et s'exprime selon l'équation (C.1). Intervenant notamment dans le cadre de la tolérance aux fautes logicielles, ce taux est généralement classé en quatre catégories : faible (<60%), moyen (60%≤DC<90%), élevé (90%≤DC<99%), très élevé (≥99%), et est le plus souvent déterminé par un travail d'expertise.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \tag{C.1}$$

avec $\lambda_D = \lambda_{DD} + \lambda_{DU} \rightarrow$ Taux de défaillances dangereuses

$\lambda_{DD} \rightarrow$ Taux de défaillances dangereuses détectées par un test de diagnostic

Pour les composants complexes où il n'est pas possible d'effectuer une analyse détaillée de chaque type de défaillance, une répartition équiprobable des défaillances est effectuée permettant d'obtenir λ_D et λ_{DD} pour un composant (cf. équation (C.2)).

$$\lambda_{DD} = \lambda_D \times DC = 0,5 \times \lambda \times DC \tag{C.2}$$

avec $\lambda \rightarrow$ Taux de défaillances du composant

A noter que la couverture de diagnostic n'inclut pas les fautes détectées par les tests périodiques et peut exister pour l'ensemble ou une partie du système de sécurité (éléments capteurs et/ou système logique et/ou les éléments finaux, par exemple).

C.5 La proportion de défaillances en sécurité

La proportion de défaillances en sécurité SFF (*Safe Failure Fraction*), ressemblant au taux de couverture, est également introduite dans la norme [IEC 61508 2000] (partie 2) (cf. équation (C.3)).

$$SFF = \frac{\sum \lambda_{DD} + \sum \lambda_S}{\sum \lambda_D + \sum \lambda_S} \tag{C.3}$$

avec $\lambda_S \rightarrow$ Taux de défaillances en sécurité

Elle est utilisée, en association avec un critère de tolérance aux anomalies matérielles, pour spécifier des contraintes architecturales concernant un système qui réalise une fonction de sécurité et qui est composé de plusieurs sous-systèmes (cf. Tableau C.1 et Tableau C.2). L'analyse d'une architecture existante peut également être estimée en terme de SIL. La tolérance aux anomalies matérielles correspond au nombre de redondances dans le système de sécurité : N + 1 anomalies peuvent provoquer la perte de la fonction de sécurité en présence de N redondances (par exemple N=1 pour le système redondant 1oo2 –1 out of 2– nécessitant le fonctionnement d'au moins 1 composant sur les 2 pour fonctionner).

Proportion de défaillances en sécurité	**Tolérance aux anomalies matérielles des systèmes de faible complexité** (dits de Type A [IEC 61508 2000])		
	0	**1**	**2**
<60%	SIL 1	SIL 2	SIL 3
60%≤SFF<90%	SIL 2	SIL 3	SIL 4
90%≤SFF<99%	SIL 3	SIL 4	SIL 4
SFF≥99%	SIL 3	SIL 4	SIL 4

Tableau C.1 Contraintes architecturales sur les sous-systèmes de faible complexité relatifs à la sécurité

Proportion de défaillances en sécurité	**Tolérance aux anomalies matérielles des systèmes complexes** (dits de Type B [IEC 61508 2000])		
	0	**1**	**2**
<60%	non autorisé	SIL 1	SIL 2
60%≤SFF<90%	SIL 1	SIL 2	SIL 3
90%≤SFF<99%	SIL 2	SIL 3	SIL 4
SFF≥99%	SIL 3	SIL 4	SIL 4

Tableau C.2 Contraintes architecturales sur les sous-systèmes complexes relatifs à la sécurité

Annexe D. Exemple d'instanciation des classes du modèle de situation d'exploitation relatives à l'opérateur humain

D.1 La classe « activité »

Elle traduit les paramètres mis à jour de la table d'horaires associée au système de transport guidé. La régulation n'étant pas simulée par la suite, la Figure D.1 illustre un exemple d'instanciation de la classe *activité*.

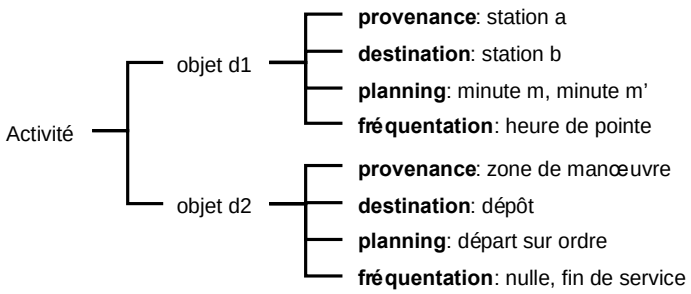


Figure D.1 Exemple d'instanciation de la classe « activité »

D.2 La classe « équipe d'opérateurs »

Les opérateurs peuvent être la source d'événements dangereux. Cette classe permet de lister les différentes conditions de travail pouvant mener les opérateurs à commettre une erreur, comme le montre l'exemple de la Figure D.2.

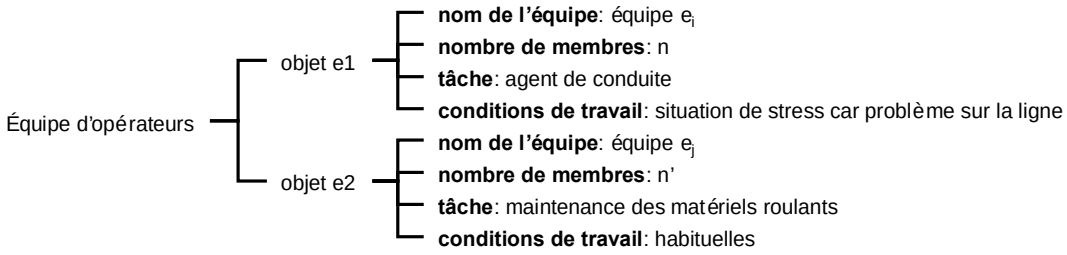


Figure D.2 Exemple d'instanciation de la classe « équipe d'opérateurs »

D.3 La classe « mode d'exploitation »

Selon le mode d'exploitation, les opérateurs n'auront pas les mêmes procédures à suivre et leur conditions de travail ne seront donc pas les mêmes. La Figure D.3 illustre un exemple d'instanciation de la classe *mode d'exploitation*.

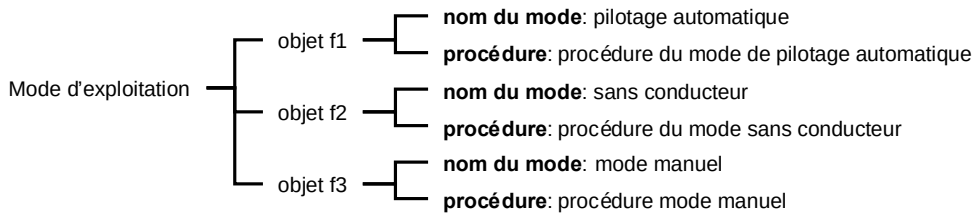


Figure D.3 Exemple d'instanciation de la classe « mode d'exploitation »

Annexe E. Fonction de structure du système étudié

E.1 Caractéristiques des fonctions de sécurité du système

Les fonctions de sécurité utilisées au chapitre 4 sont présentées au Tableau E.1 ainsi que leur SIL, leur désignation et le nombre de fois que chacune des fonctions est dupliquée (suivant le nombre de trains et de zones considérées).

Nom de la fonction de sécurité	**SIL de la fonction de sécurité**	**Désignation de la fonction de sécurité**	**Nombre de fois selon lequel est dupliquée la fonction**
Fonction d'enclenchement	Dépend d'autres fonctions	`Enclench`	nombre de sections
Détection et localisation du train	SIL 4	`Detection`	nombre de sections * nombre de trains
Attribution et détermination de l'autorisation de mouvement	SIL 4	`AutorisMouv`	nombre de sections
Formation et établissement de l'itinéraire	SIL 3	`FomationEtabliss`	nombre de sections
Gestion de l'autorisation de mouvement par le train	SIL 3	`GestionAutorisMouv`	nombre de trains
Commande de la vitesse du train bord	Dépend d'autres fonctions	`CommandeVitesseBord`	nombre de sections * nombre de trains
Commande de la vitesse du train sol	Dépend d'autres fonctions	`CommandeVitesseSol`	nombre de sections * nombre de trains
Calcul de la limite de vitesse du train	SIL 4	`CalcLimiteVitesse`	nombre de trains
Contrôle du déplacement du train	Dépend d'autres fonctions	`ControleDeplac`	nombre de trains
Contrôle de la vitesse du train	SIL 4	`ControleVitesse`	nombre de trains
Contrôle de la position du train	SIL 3	`ControlePosition`	nombre de trains
Commande du Freinage d'urgence	SIL 4	`CommandeFU`	nombre de trains
Déclenchement du freinage d'urgence	SIL 3	`DeclenchFU`	nombre de trains
Freinage de service	SIL 2	`Fservice`	nombre de trains
Freinage d'urgence	Dépend d'autres fonctions	`FU`	nombre de trains

Tableau E.1 Caractéristiques des fonctions de sécurité

E.2 Désignation des fonctions de sécurité dupliquées

Le Tableau E.2 associe à chaque fonction de sécurité dupliquée une désignation unique qui est employée dans la fonction de structure ci-dessous, celle-ci détaillant les dépendances entre les fonctions de sécurité.

Id.	Désignation de la fonction de sécurité dupliquée	Id.	Désignation de la fonction de sécurité dupliquée
1a	Enclench(section1)	18a	CommandeVitesseBord(train2,section3)
2a	Enclench(section2)	19a	CommandeVitesseBord(train3,section3)
3a	Enclench(section3)	20a	CommandeVitesseBord(train4,section3)
4a	Enclench(section4)	21a	CommandeVitesseBord(train5,section3)
5a	CommandeVitesseBord(train1,section1)	22a	CommandeVitesseBord(train6,section3)
6a	CommandeVitesseBord(train2,section1)	23a	CommandeVitesseBord(train1,section4)
7a	CommandeVitesseBord(train3,section1)	24a	CommandeVitesseBord(train2,section4)
8a	CommandeVitesseBord(train4,section1)	25a	CommandeVitesseBord(train3,section4)
9a	CommandeVitesseBord(train5,section1)	26a	CommandeVitesseBord(train4,section4)
10a	CommandeVitesseBord(train6,section1)	27a	CommandeVitesseBord(train5,section4)
11a	CommandeVitesseBord(train1,section2)	28a	CommandeVitesseBord(train6,section4)
12a	CommandeVitesseBord(train2,section2)	29a	FU(train1)
13a	CommandeVitesseBord(train3,section2)	30a	FU(train2)
14a	CommandeVitesseBord(train4,section2)	31a	FU(train3)
15a	CommandeVitesseBord(train5,section2)	32a	FU(train4)
16a	CommandeVitesseBord(train6,section2)	33a	FU(train5)
17a	CommandeVitesseBord(train1,section3)	34a	FU(train6)
1A	CommandeVitesseSol(train1,section1)	16A	CommandeVitesseSol(train4,section3)
2A	CommandeVitesseSol(train2,section1)	17A	CommandeVitesseSol(train5,section3)
3A	CommandeVitesseSol(train3,section1)	18A	CommandeVitesseSol(train6,section3)
4A	CommandeVitesseSol(train4,section1)	19A	CommandeVitesseSol(train1,section4)
5A	CommandeVitesseSol(train5,section1)	20A	CommandeVitesseSol(train2,section4)
6A	CommandeVitesseSol(train6,section1)	21A	CommandeVitesseSol(train3,section4)
7A	CommandeVitesseSol(train1,section2)	22A	CommandeVitesseSol(train4,section4)
8A	CommandeVitesseSol(train2,section2)	23A	CommandeVitesseSol(train5,section4)
9A	CommandeVitesseSol(train3,section2)	24A	CommandeVitesseSol(train6,section4)
10A	CommandeVitesseSol(train4,section2)	25A	ControleDeplac(train1)
11A	CommandeVitesseSol(train5,section2)	26A	ControleDeplac(train2)
12A	CommandeVitesseSol(train6,section2)	27A	ControleDeplac(train3)
13A	CommandeVitesseSol(train1,section3)	28A	ControleDeplac(train4)
14A	CommandeVitesseSol(train2,section3)	29A	ControleDeplac(train5)
15A	CommandeVitesseSol(train3,section3)	30A	ControleDeplac(train6)
1b	Detection(train1,section1)	44b	CalcLimiteVitesse(train6)
2b	Detection(train2,section1)	45b	ControleVitesse1(train1)
3b	Detection(train3,section1)	46b	ControleVitesse1(train2)
4b	Detection(train4,section1)	47b	ControleVitesse1(train3)
5b	Detection(train5,section1)	48b	ControleVitesse1(train4)
6b	Detection(train6,section1)	49b	ControleVitesse1(train5)
7b	Detection(train1,section2)	50b	ControleVitesse1(train6)
8b	Detection(train2,section2)	51b	ControleVitesse2(train1)
9b	Detection(train3,section2)	52b	ControleVitesse2(train2)
10b	Detection(train4,section2)	53b	ControleVitesse2(train3)
11b	Detection(train5,section2)	54b	ControleVitesse2(train4)
12b	Detection(train6,section2)	55b	ControleVitesse2(train5)
13b	Detection(train1,section3)	56b	ControleVitesse2(train6)
14b	Detection(train2,section3)	57b	ControlePosition1(train1)
15b	Detection(train3,section3)	58b	ControlePosition1(train2)
16b	Detection(train4,section3)	59b	ControlePosition1(train3)
17b	Detection(train5,section3)	60b	ControlePosition1(train4)

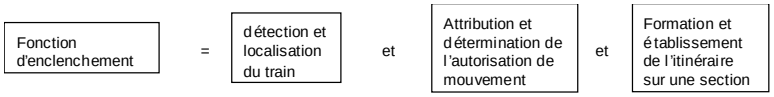
Id.	Désignation de la fonction de sécurité dupliquée	Id.	Désignation de la fonction de sécurité dupliquée
18b	Detection(train6,section3)	61b	ControlePosition1(train5)
19b	Detection(train1,section4)	62b	ControlePosition1(train6)
20b	Detection(train2,section4)	63b	ControlePosition2(train1)
21b	Detection(train3,section4)	64b	ControlePosition2(train2)
22b	Detection(train4,section4)	65b	ControlePosition2(train3)
23b	Detection(train5,section4)	66b	ControlePosition2(train4)
24b	Detection(train6,section4)	67b	ControlePosition2(train5)
25b	AutorisMouv(section1)	68b	ControlePosition2(train6)
26b	AutorisMouv(section2)	69b	CommandeFU(train1)
27b	AutorisMouv(section3)	70b	CommandeFU(train2)
28b	AutorisMouv(section4)	71b	CommandeFU(train3)
29b	FomationEtabliss(section1)	72b	CommandeFU(train4)
30b	FomationEtabliss(section2)	73b	CommandeFU(train5)
31b	FomationEtabliss(section3)	74b	CommandeFU(train6)
32b	FomationEtabliss(section4)	75b	DeclenchFU(train1)
33b	GestionAutorisMouv(train1)	76b	DeclenchFU(train2)
34b	GestionAutorisMouv(train2)	77b	DeclenchFU(train3)
35b	GestionAutorisMouv(train3)	78b	DeclenchFU(train4)
36b	GestionAutorisMouv(train4)	79b	DeclenchFU(train5)
37b	GestionAutorisMouv(train5)	80b	DeclenchFU(train6)
38b	GestionAutorisMouv(train6)	81b	Fservice(train1)
39b	CalcLimiteVitesse(train1)	82b	Fservice(train2)
40b	CalcLimiteVitesse(train2)	83b	Fservice(train3)
41b	CalcLimiteVitesse(train3)	84b	Fservice(train4)
42b	CalcLimiteVitesse(train4)	85b	Fservice(train5)
43b	CalcLimiteVitesse(train5)	86b	Fservice(train6)
1B	Detection(section1)	6B	Detection(train2)
2B	Detection(section2)	7B	Detection(train3)
3B	Detection(section3)	8B	Detection(train4)
4B	Detection(section4)	9B	Detection(train5)
5B	Detection(train1)	10B	Detection(train6)
1R	ControleVitesse(train1)	7R	ControlePosition(train1)
2R	ControleVitesse(train2)	8R	ControlePosition(train2)
3R	ControleVitesse(train3)	9R	ControlePosition(train3)
4R	ControleVitesse(train4)	10R	ControlePosition(train4)
5R	ControleVitesse(train5)	11R	ControlePosition(train5)
6R	ControleVitesse(train6)	12R	ControlePosition(train6)

Tableau E.2 Désignation des fonctions de sécurité

E.3 Fonction de structure

Chaque condition de la Figure 4.11 du chapitre 4 est détaillée en tenant compte de la duplication des fonctions de sécurité (la variable représentant une fonction est à 1 si la fonction est opérationnelle ou à 0 sinon).

Fonction d'enclenchement




```
Enclench(section1) = Detection(section1) * AutorisMouv(section1) *
                     FomationEtabliss(section1)
Enclench(section2) = Detection(section2) * AutorisMouv(section2) *
                     FomationEtabliss(section2)
Enclench(section3) = Detection(section3) * AutorisMouv(section3) *
                     FomationEtabliss(section3)
Enclench(section4) = Detection(section4) * AutorisMouv(section4) *
                     FomationEtabliss(section4)
```

Explication : Chaque section possède sa propre fonction d'enclenchement.

Détail de la fonction Détection et Localisation du train selon les sections

détection et localisation du train

```
Detection(section1) = Detection(train1,section1) * Detection(train2,section1) *
                      Detection(train3,section1) * Detection(train4,section1) *
                      Detection(train5,section1) * Detection(train6,section1)
Detection(section2) = Detection(train1,section2) * Detection(train2,section2) *
                      Detection(train3,section2) * Detection(train4,section2) *
                      Detection(train5,section2) * Detection(train6,section2)
Detection(section3) = Detection(train1,section3) * Detection(train2,section3) *
                      Detection(train3,section3) * Detection(train4,section3) *
                      Detection(train5,section3) * Detection(train6,section3)
Detection(section4) = Detection(train1,section4) * Detection(train2,section4) *
                      Detection(train3,section4) * Detection(train4,section4) *
                      Detection(train5,section4) * Detection(train6,section4)
```

Explication : La détection et la localisation des trains sur une section ne sont possibles que si chaque train présent sur la section est détecté correctement. En effet, la mauvaise détection d'un train influence la gestion de la position des autres trains par le sous-système sol.

Fonction Commande de la vitesse de chaque train à bord

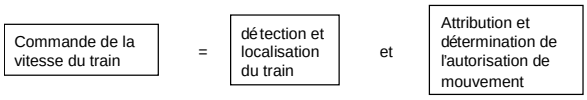
commande de la vitesse selon l'autorisation de mouvement = gestion de l'autorisation de mouvement par le train et Commande de la vitesse du train et calcul de la limite de vitesse du train

```
CommandeVitesseBord(train1,section1) = GestionAutorisMouv(train1) *
                      CommandeVitesseSol(train1,section1) * CalcLimiteVitesse(train1)
CommandeVitesseBord(train2,section1) = GestionAutorisMouv(train2) *
                      CommandeVitesseSol(train2,section1) * CalcLimiteVitesse(train2)
CommandeVitesseBord(train3,section1) = GestionAutorisMouv(train3) *
                      CommandeVitesseSol(train3,section1) * CalcLimiteVitesse(train3)
CommandeVitesseBord(train4,section1) = GestionAutorisMouv(train4) *
                      CommandeVitesseSol(train4,section1) * CalcLimiteVitesse(train4)
CommandeVitesseBord(train5,section1) = GestionAutorisMouv(train5) *
                      CommandeVitesseSol(train5,section1) * CalcLimiteVitesse(train5)
CommandeVitesseBord(train6,section1) = GestionAutorisMouv(train6) *
                      CommandeVitesseSol(train6,section1) * CalcLimiteVitesse(train6)
CommandeVitesseBord(train1,section2) = GestionAutorisMouv(train1) *
                      CommandeVitesseSol(train1,section2) * CalcLimiteVitesse(train1)
CommandeVitesseBord(train2,section2) = GestionAutorisMouv(train2) *
                      CommandeVitesseSol(train2,section2) * CalcLimiteVitesse(train2)
CommandeVitesseBord(train3,section2) = GestionAutorisMouv(train3) *
                      CommandeVitesseSol(train3,section2) * CalcLimiteVitesse(train3)
CommandeVitesseBord(train4,section2) = GestionAutorisMouv(train4) *
                      CommandeVitesseSol(train4,section2) * CalcLimiteVitesse(train4)
CommandeVitesseBord(train5,section2) = GestionAutorisMouv(train5) *
                      CommandeVitesseSol(train5,section2) * CalcLimiteVitesse(train5)
CommandeVitesseBord(train6,section2) = GestionAutorisMouv(train6) *
                      CommandeVitesseSol(train6,section2) * CalcLimiteVitesse(train6)
CommandeVitesseBord(train1,section3) = GestionAutorisMouv(train1) *
                      CommandeVitesseSol(train1,section3) * CalcLimiteVitesse(train1)
CommandeVitesseBord(train2,section3) = GestionAutorisMouv(train2) *
                      CommandeVitesseSol(train2,section3) * CalcLimiteVitesse(train2)
CommandeVitesseBord(train3,section3) = GestionAutorisMouv(train3) *
                      CommandeVitesseSol(train3,section3) * CalcLimiteVitesse(train3)
CommandeVitesseBord(train4,section3) = GestionAutorisMouv(train4) *
                      CommandeVitesseSol(train4,section3) * CalcLimiteVitesse(train4)
CommandeVitesseBord(train5,section3) = GestionAutorisMouv(train5) *
                      CommandeVitesseSol(train5,section3) * CalcLimiteVitesse(train5)
CommandeVitesseBord(train6,section3) = GestionAutorisMouv(train6) *
                      CommandeVitesseSol(train6,section3) * CalcLimiteVitesse(train6)
CommandeVitesseBord(train1,section4) = GestionAutorisMouv(train1) *
                      CommandeVitesseSol(train1,section4) * CalcLimiteVitesse(train1)
CommandeVitesseBord(train2,section4) = GestionAutorisMouv(train2) *
                      CommandeVitesseSol(train2,section4) * CalcLimiteVitesse(train2)
CommandeVitesseBord(train3,section4) = GestionAutorisMouv(train3) *
                      CommandeVitesseSol(train3,section4) * CalcLimiteVitesse(train3)
```

```
CommandeVitesseBord(train4,section4) = GestionAutorisMouv(train4) *
                        CommandeVitesseSol(train4,section4) * CalcLimiteVitesse(train4)
CommandeVitesseBord(train5,section4) = GestionAutorisMouv(train5) *
                        CommandeVitesseSol(train5,section4) * CalcLimiteVitesse(train5)
CommandeVitesseBord(train6,section4) = GestionAutorisMouv(train6) *
                        CommandeVitesseSol(train6,section4) * CalcLimiteVitesse(train6)
```

Explications : La vitesse d'un train est commandée à l'aide des fonctions bord selon les informations reçues des fonctions sol de la section sur laquelle le train se trouve.

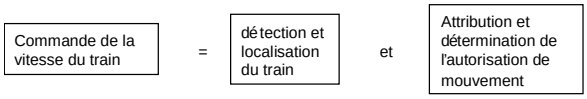
Fonction Commande de la vitesse de chaque train




```
CommandeVitesseSol(train1,section1) = Detection(train1,section1) * AutorisMouv(section1)
CommandeVitesseSol(train2,section1) = Detection(train2,section1) * AutorisMouv(section1)
CommandeVitesseSol(train3,section1) = Detection(train3,section1) * AutorisMouv(section1)
CommandeVitesseSol(train4,section1) = Detection(train4,section1) * AutorisMouv(section1)
CommandeVitesseSol(train5,section1) = Detection(train4,section1) * AutorisMouv(section1)
CommandeVitesseSol(train6,section1) = Detection(train5,section1) * AutorisMouv(section1)
CommandeVitesseSol(train1,section2) = Detection(train1,section2) * AutorisMouv(section2)
CommandeVitesseSol(train2,section2) = Detection(train2,section2) * AutorisMouv(section2)
CommandeVitesseSol(train3,section2) = Detection(train3,section2) * AutorisMouv(section2)
CommandeVitesseSol(train4,section2) = Detection(train4,section2) * AutorisMouv(section2)
CommandeVitesseSol(train5,section2) = Detection(train5,section2) * AutorisMouv(section2)
CommandeVitesseSol(train6,section2) = Detection(train6,section2) * AutorisMouv(section2)
CommandeVitesseSol(train1,section3) = Detection(train1,section3) * AutorisMouv(section3)
CommandeVitesseSol(train2,section3) = Detection(train2,section3) * AutorisMouv(section3)
CommandeVitesseSol(train3,section3) = Detection(train3,section3) * AutorisMouv(section3)
CommandeVitesseSol(train4,section3) = Detection(train4,section3) * AutorisMouv(section3)
CommandeVitesseSol(train5,section3) = Detection(train5,section3) * AutorisMouv(section3)
CommandeVitesseSol(train6,section3) = Detection(train6,section3) * AutorisMouv(section3)
CommandeVitesseSol(train1,section4) = Detection(train1,section4) * AutorisMouv(section4)
CommandeVitesseSol(train2,section4) = Detection(train2,section4) * AutorisMouv(section4)
CommandeVitesseSol(train3,section4) = Detection(train3,section4) * AutorisMouv(section4)
CommandeVitesseSol(train4,section4) = Detection(train4,section4) * AutorisMouv(section4)
CommandeVitesseSol(train5,section4) = Detection(train5,section4) * AutorisMouv(section4)
CommandeVitesseSol(train6,section4) = Detection(train6,section4) * AutorisMouv(section4)
```

Explications : Le sous-système sol d'une section donnée établit la vitesse des trains se trouvant sur cette section selon une autorisation de mouvement qui est calculée par ce sous-système et selon la détection et la localisation des trains sur cette section.

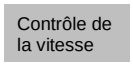
Fonction Contrôle du déplacement de chaque train




```
ControleDeplac(train1) = ControleVitesse(train1) + ControlePosition(train1)
ControleDeplac(train2) = ControleVitesse(train2) + ControlePosition(train2)
ControleDeplac(train3) = ControleVitesse(train3) + ControlePosition(train3)
ControleDeplac(train4) = ControleVitesse(train4) + ControlePosition(train4)
ControleDeplac(train5) = ControleVitesse(train5) + ControlePosition(train5)
ControleDeplac(train6) = ControleVitesse(train6) + ControlePosition(train6)
```

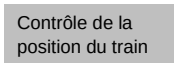
Explications : Chaque train contrôle son déplacement à l'aide des fonctions de contrôle de vitesse et de position.

Redondances de la fonction Contrôle de la vitesse



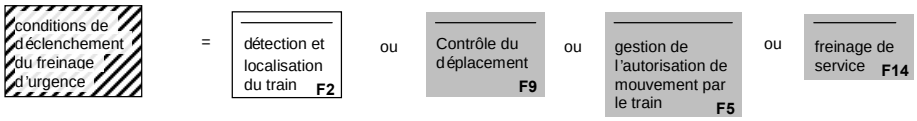

```
ControleVitesse(train1) = ControleVitesse1(train1) + ControleVitesse2(train1)
ControleVitesse(train2) = ControleVitesse1(train2) + ControleVitesse2(train2)
ControleVitesse(train3) = ControleVitesse1(train3) + ControleVitesse2(train3)
ControleVitesse(train4) = ControleVitesse1(train4) + ControleVitesse2(train4)
ControleVitesse(train5) = ControleVitesse1(train5) + ControleVitesse2(train5)
ControleVitesse(train6) = ControleVitesse1(train6) + ControleVitesse2(train6)
```

Redondances de la fonction Contrôle de la position du train




```
ControlePosition(train1)= ControlePosition(train1) + ControlePosition(train1)
ControlePosition(train1)= ControlePosition(train1) + ControlePosition(train1)
ControlePosition(train1)= ControlePosition(train1) + ControlePosition(train1)
ControlePosition(train1)= ControlePosition(train1) + ControlePosition(train1)
ControlePosition(train1)= ControlePosition(train1) + ControlePosition(train1)
ControlePosition(train1)= ControlePosition(train1) + ControlePosition(train1)
```

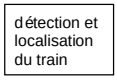
Conditions de déclenchement du freinage d'urgence




```
CondDeclenchFU(train1) = 1 - Detection(train1) * ControleDeplac(train1) *
                       GestionAutorisMouv(train1) * Fservice(train1)
CondDeclenchFU(train2) = 1 - Detection(train2) * ControleDeplac(train2)) *
                       GestionAutorisMouv(train2) * Fservice(train2)
CondDeclenchFU(train3) = 1 - Detection(train3) * ControleDeplac(train3)) *
                       GestionAutorisMouv(train3) * Fservice(train3)
CondDeclenchFU(train4) = 1 - Detection(train4) * ControleDeplac(train4)) *
                       GestionAutorisMouv(train4) * Fservice(train4)
CondDeclenchFU(train5) = 1 - Detection(train5) * ControleDeplac(train5)) *
                       GestionAutorisMouv(train5) * Fservice(train5)
CondDeclenchFU(train6) = 1 - Detection(train6) * ControleDeplac(train6)) *
                       GestionAutorisMouv(train6) * Fservice(train6)
```

Explications : Le freinage d'urgence d'un train donné est déclenché, si le train ne reçoit aucun signal du circuit de voie sur lequel il se trouve (il n'est alors plus détectable), si la fonction bord contrôlant son déplacement est défaillante, si le train ne reçoit pas d'autorisation de mouvement, ou si le freinage de service est défaillant.

Détail de la fonction détection et localisation pour un train donné




```
Detection(train1) = Detection(train1,section1) * Detection(train1,section2) *
                    Detection(train1,section3) * Detection(train1,section4)
Detection(train2) = Detection(train2,section1)* Detection(train2,section2) *
                    Detection(train2,section3) * Detection(train2,section4)
Detection(train3) = Detection(train3,section1)* Detection(train3,section2) *
                    Detection(train3,section3) * Detection(train3,section4)
Detection(train4) = Detection(train4,section1)* Detection(train4,section2) *
                    Detection(train4,section3) * Detection(train4,section4)
Detection(train5) = Detection(train5,section1) * Detection(train5,section2) *
                    Detection(train5,section3) * Detection(train5,section4)
Detection(train6) = Detection(train6,section1) * Detection(train6,section2) *
                    Detection(train6,section3) * Detection(train6,section4)
```

Explications : Un train est détecté et localisé s'il est détecté sur l'une des sections de voie considérées.

Fonction Freinage d'urgence

```
FU(train1) = CommandeFU(train1) * DeclenchFU(train1)
FU(train2) = CommandeFU(train2) * DeclenchFU(train2)
FU(train3) = CommandeFU(train3) * DeclenchFU(train3)
FU(train4) = CommandeFU(train4) * DeclenchFU(train4)
FU(train5) = CommandeFU(train5) * DeclenchFU(train5)
FU(train6) = CommandeFU(train6) * DeclenchFU(train6)
```

Explications : Le freinage d'urgence d'un train donné est opérationnel si un signal de déclenchement du freinage d'urgence est bien envoyé lorsque la condition de déclenchement du freinage d'urgence est vraie, et si la commande qui s'ensuit active ce freinage.

Index des figures

Figure 1.1 Les concepts de la sûreté de fonctionnement [Desroches, Leroy et al. 2003]..... 21
Figure 1.2 Exemple de réseau bayésien 26
Figure 1.3 Équivalence entre quelques méthodes de sûreté de fonctionnement et les réseaux bayésiens..... 30
Figure 1.4 Modèle du « nœud papillon » [Chevreau, Wibo et al. 2005][De Dianous et Fiévez 2005]..... 33
Figure 1.5 Modèle du diagramme causes-conséquences [Villemeur 1988] 33
Figure 1.6 Modèle générique de Embrey classifiant les causes d'un accident [Embrey 1992]..... 34
Figure 1.7 Processus de gestion des risques..... 37
Figure 1.8 Diagrammes illustrant des principes d'acceptation du risque..... 38
Figure 1.9 Différents niveaux de sûreté des installations automatisées [Cauffriez 2005]..... 40
Figure 2.1 Classification des événements redoutés existant dans le domaine des transports guidés, adaptée de [Hadj-Mabrouk, Stuparu et al. 1998] 46
Figure 2.2 Architecture générale d'un système de signalisation..... 51
Figure 2.3 Critères d'acceptation du risque ALARP et MEM d'après [CENELEC 2000] 59
Figure 2.4 Gestion des risques dans le domaine des transports guidés, dérivée de [Braband 1999]..... 62
Figure 2.5 Réduction du risque par l'utilisation d'une fonction de sécurité faiblement sollicitée 65
Figure 2.6 Réduction du risque par l'utilisation d'une fonction de sécurité fortement sollicitée..... 66
Figure 2.7 Exemple de graphe de risque..... 67
Figure 2.8 Exemple de matrice de gravité des événements dangereux 68
Figure 3.1 Exemple de représentation des profils de risque selon un diagramme causes-conséquences 78
Figure 3.2 Les dépendances existant dans l'enchaînement des événements dangereux 79
Figure 3.3 Résultats des probabilités d'échec obtenues par l'application de l'approche de SMC 83
Figure 3.4 Macro vue du modèle de situation d'exploitation..... 87
Figure 3.5 Le modèle générique d'une situation d'exploitation représenté sous la forme d'un diagramme de classes issu du formalisme UML 89
Figure 3.6 Différentes séquences d'événements dangereux apparaissant sur une situation d'exploitation 92
Figure 3.7 Méthode dédiée à la simulation de l'évolution des situations d'exploitation 94
Figure 4.1 La cartographie du réseau du système de transport guidé étudié..... 101
Figure 4.2 Principe du cantonnement..... 102
Figure 4.3 Itinéraires possédant une ressource partagée 103
Figure 4.4 Gestion des conflits d'itinéraire par le système d'enclenchement..... 104
Figure 4.5 La transmission des données du sous-système sol ou sous-système bord 105
Figure 4.6 Instanciation de la classe « zone dangereuse »..... 106
Figure 4.7 Exemple d'instanciation de la classe « contexte »..... 107
Figure 4.8 Instanciation de la classe « fonction de sécurité » 108
Figure 4.9 Instanciation de la classe « sous-système » 108
Figure 4.10 Exemple d'instanciation de la classe « événement dangereux »..... 109
Figure 4.11 Dépendances entre les fonctions de sécurité..... 110
Figure 4.12 Maquette logicielle du système..... 112
Figure 4.13 Profils de risque relatifs à l'espacement entre train 114
Figure 4.14 Profils de risque relatifs à l'activation du freinage d'urgence 114
Figure 4.15 Profils de risque relatifs à l'accès d'une intersection..... 115
Figure 4.16 Probabilité obtenue pour l'alternative 6 (cas 4)..... 118
Figure 4.17 Exemple d'événement redouté généré par une simulation du contexte opérationnel 121
Figure 4.18 1er cas d'étude (cas 4) 125
Figure 4.19 2ème cas d'étude (cas 2-3)..... 125
Figure 5.1 Analyse d'incertitudes pour la combinaison des SILs 132
Figure 5.2 Définition de variables d'influence caractérisant la gravité d'événements redoutés 134
Figure 5.3 Description d'un diagramme Safe-SADT+ d'un système tenant compte des facteurs humains..... 138
Figure A.1 Algorithme de la simulation de Monte Carlo biaisée utilisé pour l'évaluation de scénarios de risque 158
Figure C.1 Classification des défaillances 165
Figure D.1 Exemple d'instanciation de la classe « activité »..... 168
Figure D.2 Exemple d'instanciation de la classe « équipe d'opérateurs » 168
Figure D.3 Exemple d'instanciation de la classe « mode d'exploitation » 169

Index des tableaux

Tableau 1.1 Principales méthodes de sûreté de fonctionnement d'après [IEC 60300-3-1 2003] 25
Tableau 1.2 Classification des termes employés autour de la notion de danger 32
Tableau 2.1 Tableau de SILs selon le mode de fonctionnement des fonctions ou systèmes de sécurité..... 61
Tableau 2.2 Exemple de matrice de risques ou tableau de criticité..... 64
Tableau 3.1 Différents indicateurs quantitatifs associés à la faible sollicitation du système de sécurité 74
Tableau 3.2 Différents indicateurs quantitatifs associés à la forte sollicitation du système de sécurité..... 75
Tableau 3.3 Exemple d'application des règles de combinaison des SILs selon l'exemple présenté en Figure 3.182
Tableau 4.1 Relations d'association entre les fonctions de sécurité et les sous-systèmes employés 107
Tableau 4.2 Événements redoutés pouvant se produire selon l'occurrence d'un événement initiateur donné.... 116
Tableau 4.3 Evaluation préalable sans prise en compte du contexte opérationnel..... 119
Tableau 4.4 Détail de l'état des fonctions dans l'exemple de situation d'exploitation 122
Tableau 4.5 Principales informations contenues dans les résultats..... 126
Tableau 5.1 Coûts liés à un accident..... 135
Tableau B.1 Récents systèmes de signalisation pour les réseaux conventionnels ou grande vitesse 159
Tableau B.2 Récents systèmes de signalisation pour les réseaux urbains [Beugin 2003]..... 162
Tableau C.1 Contraintes architecturales sur les sous-systèmes de faible complexité relatifs à la sécurité..... 167
Tableau C.2 Contraintes architecturales sur les sous-systèmes complexes relatifs à la sécurité..... 167
Tableau E.1 Caractéristiques des fonctions de sécurité..... 170
Tableau E.2 Désignation des fonctions de sécurité 172

CONTRIBUTION A L'EVALUATION DE LA SECURITE DES SYSTEMES COMPLEXES DE TRANSPORT GUIDE

Résumé :

Un système de transport guidé est un système complexe qui intègre de nombreux sous-systèmes en interaction pour garantir un déplacement en toute sécurité. Répartis sur l'ensemble du système en tant que sous-systèmes bord et sol, de tels moyens de sécurité consistent à éviter toute situation à risque pouvant mener à des conséquences graves. La sécurité nécessite d'être évaluée afin de justifier que l'ensemble des moyens mis en œuvre pour maîtriser les risques est suffisant. Cependant en raison de la complexité de ces systèmes, l'évaluation globale de la sécurité apparaît problématique.

Ces travaux de recherche se sont consacrés à l'élaboration d'une approche d'évaluation de la sécurité focalisant sur l'ensemble du système et tenant compte des SILs (Safety Integrity Levels). Les niveaux d'intégrité de sécurité sont des exigences introduites par les normes de sécurité fonctionnelle pour fixer des objectifs à atteindre par les fonctions de sécurité selon un référentiel commun. Une quantification des profils de risque tenant compte des dépendances et des SILs de ces fonctions a d'abord été proposée, notamment par l'emploi de techniques de simulation de Monte Carlo biaisée surmontant la faible occurrence des événements de sécurité. Ensuite un exemple de système de transport guidé a été modélisé selon le concept original de situation d'exploitation développé pour considérer les différentes conditions de sécurité dont le contexte opérationnel du système, et permettre de formaliser différents profils de risque. Grâce à une maquette logicielle s'appuyant sur la modélisation précédente, plusieurs simulations du système ont été réalisées et ont mené une évaluation de la sécurité.

Mots clés : Gestion des risques, Transports guidés, Sécurité fonctionnelle, Niveau d'intégrité de sécurité, Simulation de Monte Carlo biaisée, Situation d'exploitation

CONTRIBUTION TO SAFETY EVALUATION OF COMPLEX GUIDED TRANSPORTATION SYSTEMS

Abstract :

A guided transportation system is a complex system, which integrates multiple interacting subsystems that ensure a safe transfer of passengers. Such safety means are distributed throughout the onboard and trackside subsystems, in order to avoid risky situations and potentially catastrophic accidents. The level of safety must be assessed to prove that all these safety means are sufficient. This implies evaluating the safety of the overall system. However, faced with the complexity of such systems, assessing the safety of guided transportation systems is a thorny question.

In this research, an approach to risk evaluation of the entire system is proposed using the probabilistic Safety Integrity Level (SIL) requirements. The standardized SIL concept allows the safety requirements of each safety subsystem to be specified. Our approach is based both on the operating situation concept and on biased Monte Carlo simulation (MCS) allowing the complexity of the dependencies between rare failure events to be taken into consideration. The proposed operating situation concept is developed to deal with the complexity of guided transportation systems and to analyze the evolution of the system. MCS make it possible to perform risk profile evaluation based on the formalization of the system safety conditions according to the operating situation model. The sample implementation is presented and examined in term of the safety results.

Keywords : Risk management, Guided transportation systems, Functional Safety, Safety Integrity Level, biased Monte Carlo simulation, Operating situation