Impact des postes centraux de supervision de trafic ferroviaire sur la sécurité

Fabien Belmonte

Thèse

Présentée pour obtenir le grade de Docteur

de

l'Université de Technologie de Compiègne

Spécialité : Technologie de l'Information et des Systèmes

Impact des postes centraux de supervision de trafic ferroviaire sur la sécurité

Fabien Belmonte

Soutenue le 10 septembre 2008 devant le jury composé de Messieurs :

Philippe Bonnifait (utc)	**(Président)**
Erik Hollnagel (ensmp)	**(Rapporteur)**
Christophe Kolski (uvhc)	**(Rapporteur)**
Robert Capel (alstom)	**(Examinateur)**
Walter Schön (utc)	**(Directeur de Thèse)**
Jean-Louis Boulanger (utc)	**(Co-directeur de Thèse)**

RÉSUMÉ

Bien qu'actuellement considérés comme non sécuritaires (les fonctions de sécurité étant assurées par d'autres sous-systèmes) les systèmes de supervision du trafic ferroviaire peuvent contribuer à la sécurité dans certains scénarios de crise où une décision adaptée d'un opérateur de supervision pourrait réduire notablement la gravité des scénarios d'accident. Il est donc de toute première importance d'identifier ce type de scénarios afin d'envisager les systèmes de supervision du futur dans la perspective d'améliorer encore la sécurité des circulations dans un contexte d'augmentation du trafic ferroviaire prévisible et souhaitable dans les années à venir. La supervision impliquant des décisions prises par l'homme, la prise en compte du facteur humain est indispensable, et ce dès la conception des futurs systèmes.

L'étude se focalise sur l'évaluation de l'interaction opérateurs humains – machines et son impact sur la sécurité. Cette démarche nécessite la coopération de spécialistes de l'ingénierie ferroviaire (composante technique), des sciences humaines et sociales (composante humaine et organisationnelle) et de la sûreté de fonctionnement pour la synthèse et l'évaluation de la sécurité. Ces disciplines ont des approches différentes et quelquefois opposées, la thèse vise à établir un pont entre ces différentes disciplines dans un objectif commun de l'évaluation de la sécurité.

Des études spécifiques du facteur humain ont été réalisées sur une plateforme de supervision de trafic ferroviaire. Installée dans les locaux de l'UTC, cette plateforme comprend un système de supervision couplé à un simulateur de trafic permettant de recréer en laboratoire les conditions de travail d'un opérateur de supervision de trafic ferroviaire. L'objectif des expérimentations est d'obtenir des informations sur les processus cognitifs généraux impliqués dans la gestion d'un environnement dynamique de circulation de mobiles et de contribuer ainsi à l'évaluation du système de supervision en situation d'utilisation par des opérateurs confrontés à la gestion d'une situation nominale, normale et dégradée.

La difficulté d'une telle démarche demeure l'intégration des résultats obtenus par l'observation et les techniques de la psychologie ergonomique cognitive dans l'étude de sécurité. Une approche interdisciplinaire s'appuyant sur un référentiel commun aux trois disciplines a été proposée afin de disposer d'un modèle commun entre spécialistes des sciences humaines et sociales et spécialistes de la sûreté de fonctionnement. Ce référentiel a été puisé dans une perspective systémique de l'étude de la sécurité.

ABSTRACT

Title : Impact of the automatic train supervision systems on safety

Currently, railway traffic supervision systems are not considered as safety critical (basic safety constraints being ensured by other sub-systems). By taking a closer look, we can notice that these systems are able to prove their efficiency in safety management by offering critical information to the supervisor confronted with a crisis situation in order to help him to take the right decisions that lead to reduce considerably the impact and the severity of an accident. Taking into account these scenarios in the design in order to contribute to enhance the global safety level is therefore mandatory in a context where the concern of economic efficiency of infrastructures lead to increase traffic. Supervision is tightly related to human decisions ; therefore human factor is to be foremost when designing future supervision systems.

This work focuses on evaluating the human-machine interactions and their impact on safety. In order to complete this study, we required the participation of specialists from three main areas. Firstly railway engineers for the technical aspects, secondly human factors and organisational specialists, and thirdly dependability experts to summarize and evaluate the impact on safety caused by the interactions of the two previous components. These three fields have different approaches that can sometimes be contradictory and this thesis tries to set links between them for the common objective to reach a greater safety level.

The specific studies on the human factor have been conducted on a platform designed to supervise the railway traffic installed in the UTC offices. This platform was composed of an automatic train supervision system coupled with a traffic simulator enabling to re-create the working conditions of a an operator. The objective was to obtain information on the general cognitive processes involved in managing a dynamic traffic environment of trains in order to evaluate the supervising system while in use by operators facing three type of situations : nominal, normal, or degraded.

The difficulty of such study remains the integration of the results from the observation, with the technics of ergonomical cognitive psychology in the safety analysis.

An interdisciplinary approach based on a common referential of these three fields has been proposed in order to get a common model for human ressources and dependability experts. This referential was designed in a systemic perspective of the safety studies.

REMERCIEMENTS

Avant de commencer ce travail de thèse, j'occupais la fonction d'ingénieur de projet en sûreté de fonctionnement auprès d'entreprises de conseil. Ma première expérience en sûreté de fonctionnement m'a été proposée par M. Jean Louis Bon, aujourd'hui Président de l'École Polytech'Lille. Je tiens donc à remercier Jean Louis Bon pour m'avoir mis le pied à l'étrier dans cette activité.

Ma deuxième mission a été effectuée dans le domaine de la sûreté de fonctionnement des logiciels embarqués dans l'industrie automobile. C'est dans ce cadre que j'ai été présenté à M. Jean-Louis Boulanger à l'occasion d'un groupe de travail de l'Institut de Maîtrise Des Risques (IMDR) dirigé par M. Patrice Kahn. Je remercie l'IMDR et M. Kahn pour m'avoir fait rencontrer un des mes futurs encadrants de thèse.

Jean-Louis Boulanger m'a proposé de poursuivre mon expérience par un travail de recherche dans le domaine des transports ferroviaires et dans la thématique des facteurs humains. Dirigé en collaboration avec Walter Schön, je garde le souvenir d'un travail d'équipe passionné. Je veux donc remercier mes deux directeurs de thèse pour la qualité de leur encadrement et de leurs conseils avisés. Je suis tout particulièrement reconnaissant envers Walter Schön pour la relecture rigoureuse qu'il a apportée à mes travaux et à sa disponibilité pour les réunions « *brainstorming* », captivantes, du vendredi matin.

Cette thèse a été développée dans le cadre d'un projet de recherche État-Région Picardie « Hommes, Technologies et Systèmes Complexes ». Je tiens à remercier l'ensemble des membres du projet et plus particulièrement M. Gérard Rigaud de la société Sigma-Conseil pour nous avoir fait découvrir de manière précise et détaillée toute la complexité des systèmes de transport ferroviaire. Les formations qu'il nous a données et les nombreuses réunions de travail que nous avons eues ensemble ont été d'une grande valeur pédagogique. Je veux également remercier les membres de l'équipe ECCHAT de l'université d'Amiens, M. Laurent Heurley et Sylvain Haudegond tous deux spécialistes de la psychologie et de l'ergonomie du travail pour leur précieuse collaboration.

Je veux également adresser mes plus respectueux remerciements aux membres du jury de thèse, MM. Erik Hollnagel, Christophe Kolski, Robert Capel et Philippe Bonnifait.

Enfin, je remercie mes parents et mon épouse pour leur soutien attentionné et constant.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES ACRONYMES

Les principaux acronymes sont présentés et classés par ordre alphabétique dans la liste suivante. Les numéros font références aux pages où ils sont définis et/ou mentionnés.

A

ASTRÉE : Automatisation de Suivi de Trains en temps RÉEl 133
ATC : *Automatic Train Control* 26, 49
ATO : *Automatic Train Operation* 50
ATP : *Automatic Train Protection* 49
ATS : *Automatic Train Supervision* 25, 50

C

CCP : Condition Commune de performance 179
CREAM : *Cognitive Reliability and Error Analysis Model* 97
CS : Commande de Sécurité 192
CSE : *Cognitive Systems Engineering* 177
COCOM : *COntextual COntrol Model* 97

E

EPFH : Étude Probabiliste du Facteur Humain 84
EPS : Étude Probabiliste de Sécurité 83
ERTMS : *European Railway Transportation and Management System* 55
ETTO : *Efficiency Thoroughness Trade Off* 187

F

FRAM : *Functional Resonance Accident Model* 73, 177

H

HILC : *High Integrity Level Control* 56

HRA : *Human Reliability Analysis* 84

I

IPCS : Installation Permanente de Contre Sens 124

L

LAMIH : Laboratoire d'Automatique, de Mécanique, et d'Informatique industrielles et Humaines 133

P

PCC : Poste de Commandement Centralisé 25

S

SIL : *Safety Integrity Level* 26, 82

STAMP : *Systems-Theoretic Accident Model and Processes* 73

T

THERP : *Technique for Human Error Prediction* 93

THR : *Tolerable Hasard Rate* 81

CHAPITRE 1

INTRODUCTION

Résumé

Ce premier chapitre couvre la problématique générale dans laquelle s'inscrit ce mémoire. La première partie décrit le contexte de la thèse. Celui-ci est traité selon deux axes, le contexte industriel des systèmes ferroviaires et le contexte méthodologique relatif à l'évaluation de la sécurité ferroviaire. La deuxième partie présente l'objectif de la thèse et l'organisation du mémoire.

1.1. Contexte

1.1.1. Contexte industriel. — La thèse a pour objet d'étude le transport ferroviaire, plus particulièrement les systèmes de supervision du trafic.

Depuis quelques années, la supervision de trafic ferroviaire a été considérablement transformée. Autrefois bâtie sur l'omniprésence de l'opérateur humain dans les activités ferroviaires depuis le terrain jusqu'au poste de régulation, l'arrivée des systèmes informatisés de surveillance et de commande a réduit considérablement le nombre d'opérateurs ferroviaires et notamment dans la boucle de supervision. En effet, les systèmes modernes de supervision de trafic ferroviaire appelés *Automatic Train Supervision* (ATS) ont tendance à centraliser toute la commande ferroviaire dans un seul poste appelé « Poste Centralisé de Commandement » ou PCC [**14**].

Autrefois garant de la sécurité, l'opérateur de trafic ferroviaire est de plus en plus mis à l'écart au profit de systèmes de sécurité techniques de plus en plus autonomes. Au delà des systèmes d'enclenchements garantissant la sécurité des circulations sur les voies depuis le début du siècle dernier, des systèmes de protection appelés Automatic Train Protection (ATP) ont vu le jour et offrent un niveau de sécurité tel que l'ATS n'est plus considéré comme un acteur majeur de la sécurité [**16, 15**]. Les opérateurs de l'ATS sont confinés à des tâches de surveillance dans la majeure partie de leur activité. De fait, les « surprises de l'automatisation » (voir [**11**]) ne sont pas en reste, puisque l'ATS en raison de sa position centrale dans le système demeure le centre névralgique des opérations lorsque la situation se dégrade ou exige l'exécution de procédures.

La société ALSTOM Transport [1], intervenant majeur de l'industrie ferroviaire internationale produit des systèmes de signalisation et de contrôle automatique de trains appelés *Automatic*

1. http://www.transport.alstom.com

Train Control (ATC). Au sommet du système ATC, le système ATS est intégré dans le PCC et offre de nombreuses fonctionnalités rendues possibles par la généralisation des nouvelles technologies de l'information :

- Contrôle automatique de l'évolution du trafic ;
- Commande des itinéraires de circulation ;
- Communication avec les circulations ;
- Gestion de l'énergie de traction électrique ;
- Gestion des ressources (matériels roulants et personnels) ;
- Contrôle des systèmes auxiliaires (ventilations, escalators, etc.) ;
- Informations aux passagers ;
- Sûreté publique (sécurité malveillance) ;
- etc.

Dans l'objectif de renforcer la sécurité de ses systèmes, ALSTOM Transport a souhaité, dans le cadre d'une démarche de recherche partenariale université-industrie, que puisse être évalué le niveau de sécurité qui pourrait être attribué au système ATS en tenant compte du facteur humain. Le projet SPICA-RAIL, « Supervision Picarde de transport par Rail » financé par l'État et la région Picardie dans le cadre de l'axe mobilisateur « Hommes Technologies et Systèmes Complexes » associe donc ALSTOM Transport, l'Université de Technologie de Compiègne (UTC, référent dans le domaine de la sécurité ferroviaire), l'Université de Picardie Jules Verne [2] (UPJV, référent de l'aspect facteur humain), la société Sigma-Conseil (pour l'expertise en matière d'exploitation ferroviaire) et Bureau Veritas pour l'évaluation indépendante du dossier de sécurité. L'objectif de ce projet consiste à intégrer une évaluation de l'interaction entre opérateurs humains et l'ATS dans les études de sécurité des systèmes ferroviaires. La thèse s'inscrit dans ce projet et vise à synthétiser cette collaboration dans une démarche interdisciplinaire.

1.1.2. Contexte méthodologique. — Le management des risques industriels est devenu une discipline incontournable dans notre société. Née du besoin de contrôler les dangers induits par l'évolution croissante des technologies (notamment à partir de la deuxième moitié du 20e siècle), la maîtrise des risques industriels a d'abord été formalisée dans les années 60 grâce à la théorie mathématique de la fiabilité initiée par Barlow et Proschan [**12**]. Les concepteurs de systèmes à risques ont ensuite intégré ce formalisme aux techniques de l'ingénierie des systèmes [**129**], techniques qui, par la suite, ont été normalisées permettant aux industriels et aux organismes de régulation et de contrôle de la sécurité de disposer d'un référentiel méthodologique commun pour bâtir des systèmes de haut niveau de sécurité. Dans le domaine des systèmes à électronique programmable, la norme IEC 61508 [**74**] établit une procédure d'évaluation et de mise en œuvre de la sûreté de fonctionnement tout au long du cycle de vie du système (réalisation, mise en service, maintenance et démantèlement). La procédure consiste à évaluer la criticité des fonctions exécutées par le système en allouant un niveau d'intégrité de la sécurité (Safety Integrity Level ou SIL) définissant le niveau de risque accepté pour cette fonction. Quatre niveaux de SIL sont définis et ordonnés de façon croissante vis-à-vis du niveau d'intégrité de la sécurité à atteindre. Pour chaque niveau, la norme propose un ensemble de méthodes et de bonnes pratiques permettant de garantir le niveau de sécurité accepté. Les normes sont également contextualisées pour différents domaines industriels, la norme IEC 61508 par exemple est déclinée en trois normes pour les

2. http://www.u-picardie.fr

équipements de contrôle-commande et de signalisation ferroviaire : EN 50126 [**33**], EN 50128 [**34**], EN 50129 [**35**].

La prise en compte des facteurs humains n'a pas été associée à ce mouvement normatif. En effet, les normes présentées ci-avant, auxquelles sont soumis les systèmes ATS, ne font aucune référence directe à une méthodologie de prise en compte des facteurs humains dans les études de sécurité, bien que mentionnant l'importance d'une telle démarche. Les normes fournissent une liste non exhaustive des facteurs humains susceptibles d'avoir un impact sur la sécurité [**33**]. Récemment, des travaux effectués au Health & Safety Executive au Royaume-Uni [**126**] ont identifié les limitations de la norme IEC61508 pour adresser un niveau d'intégrité de la sécurité aux fonctions effectuées par l'opérateur humain en interaction avec un système de supervision. Le rapport de ces travaux propose une démarche visant à pallier ce manque en considérant l'opérateur comme partie intégrante du système et en considérant les fonctions de sécurité exécutées par l'opérateur humain de la même façon que les fonctions de sécurité exécutées par des équipements techniques. Cependant, il existe de nombreuses particularités liées à l'activité humaine de sorte qu'il est impossible d'établir une définition non équivoque du SIL avec un niveau de sécurité de l'opérateur humain. Le concept de SIL est normalement appliqué à un système de protection qui permet de réduire les risques. Or, l'opérateur humain est à la fois source et récupérateur de dangers et de ce fait, les fonctions exécutées par l'opérateur humain ne sont pas couvertes par le concept de réduction de risque considéré par la norme. Cette démarche est encore soumise à discussions et n'a pas été introduite dans la norme.

Le projet SECUGUIDE/NTIC « Impact des nouvelles technologies de l'information et de la communication dans la sécurité des transports urbains guidés » soutenu par le PREDIT [3] vise à définir une position française en matière de sécurité, pour les systèmes de transport urbains guidés. Cette approche tient compte des technologies émergentes qui sont utilisées pour réaliser les fonctions de contrôle - commande du système et intègre les aspects « facteur humain » dans les analyses de sécurité [**5**].

Dans la pratique, les études de sûreté de fonctionnement réalisent des analyses sur le facteur humain sur la base d'un référentiel méthodologique établi au fil des ans et qui comprend des outils spécifiques pour l'évaluation de la fiabilité humaine (Human Reliability Analysis HRA, ou Étude Probabiliste du Facteur Humain en français) et depuis peu pour l'évaluation de l'organisation dans le travail. Les premières méthodes créées dans les années 60 à 80 ont utilisé le cadre formel de la fiabilité en modélisant le fonctionnement de la composante humaine de la même façon qu'un système technique, à savoir par un modèle bimodal (marche ou panne). Cette approche a été fortement critiquée par la communauté scientifique, [**41**] et [**71**] résument ces critiques. Cette première génération de méthodes a également initié un débat sur la nature de l'erreur humaine [**109, 9**]. Une deuxième génération de méthodes est née tenant compte des aspects humains et sociaux de façon plus approfondie grâce à l'apport des sciences humaines et sociales [**71**].

3. Programme de recherche et d'innovation dans les transports terrestres : `http://www.predit.prd.fr`

1.2. Objectifs de la thèse

La thèse consiste à évaluer l'impact des systèmes ATS sur la sécurité. Les composantes technologiques ayant atteint un niveau élevé de sécurité, l'étude doit se focaliser sur l'évaluation de l'interaction opérateurs humains - machines et son impact sur la sécurité. Cette démarche nécessite la coopération de spécialistes de l'ingénierie ferroviaire (composante technique), des sciences humaines et sociales (composante humaine et organisationnelle) et de la sûreté de fonctionnement pour la synthèse et l'évaluation de la sécurité.

Pour ALSTOM Transport, cette démarche apporte un point de vue extérieur et nouveau concernant les ATS. Les études existantes de sûreté de fonctionnement des systèmes ferroviaires utilisent la méthode des arbres de défaillances pour évaluer la probabilité d'occurrence de catastrophes ou d'accidents. La thèse a permis l'élaboration d'une méthode d'évaluation de l'interaction opérateurs humains-ATS permettant d'approfondir l'étude des événements relatifs à l'activité humaine en situation de supervision de trafic ferroviaire.

L'objet de l'étude s'inscrit dans le cadre des systèmes sociotechniques complexes composés d'un niveau technique (les machines et les logiciels), d'un niveau humain (les opérateurs et les concepteurs) et d'un niveau organisationnel (l'ensemble des règles et des interactions qui gouvernent le travail). Chacune de ces composantes est l'objet d'études de différentes disciplines scientifiques. La composante technique est régie par des modèles et des théories issus des sciences de l'ingénieur. La composante humaine au travail est l'objet d'études de la psychologie cognitive et de l'ergonomie cognitive. Enfin, la composante organisationnelle repose sur les sciences sociales. Ces disciplines ont des approches différentes et quelques fois opposées, la thèse vise à établir un pont entre ces différentes disciplines dans un objectif commun de l'évaluation de la sécurité.

Une démarche d'évaluation des risques industriels interdisciplinaire a donc été élaborée. Elle consiste à effectuer une étude approfondie des processus cognitifs généraux impliqués dans la tâche de supervision de trafic ferroviaire sur simulateur et d'appliquer une approche complémentaire permettant d'intégrer les résultats obtenus dans l'étude de sécurité afin d'approfondir l'étude des événements humains et organisationnels insuffisamment traités dans l'approche classique.

Cette approche complémentaire s'appuie sur un référentiel commun aux trois disciplines de modélisation du système. Ce référentiel a été puisé dans une perspective systémique de l'étude de la sécurité. Dans cette perspective, Hollnagel [**68**] a développé une méthode d'étude systémique des accidents appelée *Functional Resonance Accident Model* (FRAM) que nous avons appliquée au cas du système de supervision de trafic ferroviaire et enrichie d'études complémentaires expérimentales dans un environnement simulé. Cet environnement simulé est basé sur un produit d'ALSTOM installé sur le marché international de supervision de trafic ferroviaire.

1.3. Organisation du mémoire

Le premier chapitre présente le contexte industriel. L'objectif de ce premier chapitre est double, il s'agit, d'une part, de présenter le système ferroviaire dans son ensemble en s'arrêtant plus particulièrement sur les principes généraux de la sécurité ferroviaire et, d'autre part, de montrer

les nombreuses évolutions de ce domaine d'activité et notamment l'automatisation des tâches de supervision de trafic ferroviaire.

Le second chapitre introduit la science de l'ingénieur qui s'intéresse aux risques et aux défaillances des systèmes complexes. Appelée sûreté de fonctionnement, cette science de l'ingénieur dispose d'un référentiel méthodologique à la fois mathématique, méthodologique et normatif. L'objectif de ce chapitre 3 est de positionner la problématique de la thèse dans ce référentiel. Le chapitre suivant (numéro 4) est consacré au traitement de la sûreté de fonctionnement des systèmes impliquant l'activité humaine.

Le chapitre 5 est un chapitre introductif de la démarche qui a été appliquée pour évaluer l'impact des facteurs humains profondément modifiés par l'automatisation de la supervision ferroviaire sur la sécurité. Chacune des phases de la démarche constitue un chapitre dans le présent mémoire (chapitres 6, 8 et 9).

Le premier chapitre de la démarche (chap. 6), présente un état de l'art industriel qui a permis de déterminer, grâce à des visites industrielles, les scénarios critiques de la supervision. Un modèle des modes d'exploitation des systèmes industriels sert de support à la présentation du rôle de la supervision pour la sécurité dans différents domaines industriels, dont le transport ferroviaire. Une réflexion sur la nature de l'activité des opérateurs de supervision est proposée, traditionnellement traitée comme faillible dans les études de sûreté de fonctionnement, une nouvelle approche émerge en sûreté de fonctionnement, appelée ingénierie de la résilience et qui consiste à s'intéresser à l'action de l'opérateur humain non seulement comme barrière sécuritaire (acteur résistant aux phénomènes dangereux) mais aussi comme un vecteur de la résilience du système suite à l'apparition d'un phénomène ou un événement ayant dégradé dangereusement le système.

La deuxième contribution de cette thèse représente également l'aboutissement du projet SPICARAIL et est présentée dans le chapitre 7. Ce chapitre est consacré à l'étude du comportement des opérateurs humains en situation de supervision de trafic ferroviaire par une approche psychologique cognitive basée sur des observations sur simulateur. La plateforme de simulation d'un système de supervision de trafic ferroviaire installé à Compiègne est décrite ainsi que les techniques qui ont été mises en œuvres pour configurer l'environnement de simulation et réaliser les expérimentations. Les hypothèses établies pour ces expériences et le protocole expérimental sont ensuite décrits. Enfin, les résultats de ces expériences sont discutés.

Les chapitres 8 et 9 exposent la troisième contribution de la thèse qui consiste à proposer un modèle permettant d'intégrer les résultats issus des observations sur simulateur dans les études de sécurité. Le modèle utilisé est celui de Hollnagel, nommé FRAM, sa caractéristique systémique offre l'avantage de pouvoir associer le référentiel méthodologique issu des sciences sociales (avec lequel ont été conduites les expérimentations) et le référentiel méthodologique de la sûreté de fonctionnement dans lequel se placent les études de sécurité du système de supervision de trafic ferroviaire.

Les chapitres 10 et 11 présentent respectivement les perspectives et les conclusions de ce travail.

Première PARTIE

CONTEXTE INDUSTRIEL ET MÉTHODOLOGIQUE

CHAPITRE 2

LE SYSTÈME FERROVIAIRE

Résumé

Ce chapitre présente le contexte de la thèse : les systèmes de transport ferroviaire. L'objectif est de fournir au lecteur le vocabulaire et les concepts primordiaux du domaine. Le chapitre se focalise notamment sur la sécurité du système en présentant les dangers que génère le transport ferroviaire et les fonctions et objectifs de sécurité qui sont mis en place pour les contenir. Enfin, et c'est l'objet d'étude central de la thèse, la composante de supervision de trafic est décrite au travers d'un bref historique des postes ferroviaires et d'une description de l'architecture des systèmes modernes de contrôle de mouvement des trains. La place de l'homme dans cette structure et son rôle pour la sécurité est discuté. Le chapitre se conclut sur l'avenir et l'harmonisation des systèmes de contrôle des chemins de fer européen.

2.1. Transports terrestres guidés : définitions

La définition normalisée par l'IEC [**75**] présente les transports terrestres guidés de la façon suivante :

Définition 2.1 **(Transport terrestre guidé,** [**75**]**).** — Système de transport comportant des véhicules assujettis à circuler le long d'une voie rigide.

La présente définition comprend tous types de sustentation et de guidage (roulement sur fer, roulement sur pneu, sustentation magnétique, crémaillère, à coussin d'air). Les systèmes suspendus tels que les téléphériques et les systèmes de type escalators et tapis roulant (dit *continus*) ne sont pas inclus.

La suite de ce chapitre utilise un vocabulaire spécifique aux transports guidés terrestres, le sens de chacun de ces termes est donné dans les définitions suivantes.

Définition 2.2 **(Train).** — Engin moteur ou groupe d'engins moteurs pouvant remorquer un ou plusieurs véhicules circulant en suivant une marche tracée, ou en marche indéterminée ou encore selon un régime spécial (trains de travaux, …).

Définition 2.3 **(Manœuvre).** — Déplacement guidé des trains par des signaux spécifiques dits de manœuvres ou par radio.

***Définition 2.4* (Évolution).** — Déplacement d'un train à l'intérieur d'une gare

***Définition 2.5* (Circulation).** — Terme général par lequel sont désignés à la fois les trains, les évolutions et les manœuvres.

***Définition 2.6* (Service de la circulation).** — Le service de la circulation regroupe l'ensemble des opérations permettant d'assurer la sécurité et d'organiser le mouvement des trains ou des manœuvres.

***Définition 2.7* (Acteur circulation).** — Terme générique par lequel sont désignés les agents dont la fonction se rapporte aux circulations (conducteur, responsable sécurité, superviseur, régulateur, etc.)

***Définition 2.8* (Gare).** — Le terme technique employé dans le domaine ferroviaire est différent de celui utilisé dans le langage courant.

Ici, la gare est une installation ouverte au service de la circulation assuré par au moins un acteur circulation responsable de la sécurité. Une gare dispose du minimum d'installation requis pour effectuer les opérations relatives à la circulation. Une gare peut être *permanente* ou *temporaire*.

Cette définition plus large que le sens commun est utilisé par l'organisation du système ferroviaire. La gare est le résultat du découpage géographique du réseau.

***Définition 2.9* (Itinéraire).** — Un itinéraire représente une portion de voie définie par une origine et une destination. L'origine d'un itinéraire est toujours marquée par un signal d'entrée (voir le paragraphe 2.4.2 dédié à la signalisation).

2.1.1. Eléments historiques. — Ce système de transport remonte au début du XVII^e^ siècle et assurait la circulation des chariots de mine (Newcastle Angleterre) sur des rails en bois et tirés par des chevaux. Le développement de l'utilisation de la puissance de la vapeur et l'utilisation de rail en fer permet le transport de tout type de marchandise. Les besoins grandissants de transport continental des marchandises au XIX^e^ siècle sont à l'origine du développement du chemin de fer tel qu'on le connaît aujourd'hui. Les transports de voyageurs sont quant à eux étroitement liés aux concentrations urbaines et ne sont donc devenus prépondérants en Europe qu'à la fin du XX^e^ siècle . L'écartement standard des rails en Europe (1,435m dit IUC pour Union Internationale des Chemins de fer) correspond au choix réalisé au XIX^e^ siècle, en Europe continentale, seuls l'Espagne, le Portugal et l'ex-URSS n'ont pas adopté ce standard. Il existe toutefois, en France, en Espagne ou en Grèce notamment, des voies à écartement métrique.

2.1.2. Dates et repères. —

- 1804 : Première locomotive à vapeur ;
- 1825 : Premier train de voyageurs (ligne Stockton-Darlington) 20 km/h ;
- 1869 : Ouverture de la ligne New-York – San Francisco ;
- 1879 : Premier tramway électrique (Siemens pour l'exposition de Berlin) ;
- 1890 : Premiers métros (Londres, Chicago, Budapest...) ;
- 1891 : Première ligne du métro de Paris (Fulgence Bienvenüe) ;
- 1893 : Invention du moteur Diesel (point commun entre automobile et locomotive) ;

– 1932 : « Michelines » : roulement pneu / rail acier traditionnel ;
– 1950 : Premiers métros sur pneu à Paris (ligne 11) roulement pneu / surface de roulement pneu hors rail ;
– 1964 : Première exploitation commerciale par train à grande vitesse au Japon ;
– 1966 : Prototype expérimental pour grande vitesse à turbine à gaz en France ;
– 1981 : Ouverture tronçon sud de la ligne grande vitesse Paris – Lyon ;
– 1984 : Ouverture de la première ligne du métro automatique de Lille ;
– 1990 : Record du monde de vitesse sur rail (TGV Atlantique) à 515 km/h ;
– 1998 : Mise en service du métro automatique METEOR sur la ligne 14 à Paris ;
– 2007 : Record du monde de vitesse sur rail (TGV Est) à 574,8 km/h.

2.1.3. Principaux types de transports guidés ferroviaires. — Les transports guidés ferroviaires se déclinent selon deux types de réseau correspondant à deux applications distinctes, l'une pour le transport de masse, régulier et à dimension urbaine et l'autre pour le transport de biens ou de personnes de longues distances.

Les grandes agglomérations se sont dotées dès la fin du XIX^e^ siècle de réseaux de transport ferroviaire *fermés* [1] et *spécifiques*, ils comprennent les systèmes métros, tramways et systèmes intermédiaires :

– **Métro** : système de transport pouvant être de petit ou grand gabarit, le roulement est effectué sur fer ou par pneu. Les distances de parcours sont de l'ordre de quelques kilomètres sur un réseau *clos* [2] et *fermé*. L'exploitation n'est pas partagée et n'utilise généralement qu'un seul type de matériel roulant parfois en automatisme intégral, c.-à-d. sans conducteur ;
– **Réseau Express Régional (RER)** : Utilisé dans les très grandes métropoles pour desservir les banlieues, ce système de transport utilise un matériel roulant de grand gabarit à roulement sur fer. Les distances parcourues peuvent atteindre la centaine de kilomètres sur un réseau clos et fermé dans la métropole et pouvant être partagé et ouvert en banlieue ;
– **Tramway** : après leur démantèlement dans les années 1950, profitant de la vague de réaménagement du territoire urbain, ils font leur grand retour dans les villes. Assuré par un roulement sur fer, le tramway transporte sur des distances de quelques kilomètres sur réseau fermé pour la plupart [3]. De la même façon que le métro, les lignes de tramway n'utilisent qu'un seul type de matériel roulant, mais se distinguent parfois par le partage de l'emprise au sol avec la circulation automobile ;
– **Systèmes intermédiaires** : Ce sont des systèmes hybrides entre le bus et le tramway, il en existe différentes sortes à guidage matériel (Nancy, Caen, Clermont-Ferrand) ou immatériel (prévu à Douai).

Le transport sur de longues distances nécessite l'utilisation d'un réseau *ouvert* et *partagé*. En effet, les réseaux de type grandes lignes sont connectés à d'autres réseaux et l'exploitation peut être partagée par plusieurs compagnies avec plusieurs types de matériels :

– **Trains de fret** : mesurant jusqu'à 750 mètres pour 3600 tonnes en France et plus de 10 000 tonnes aux USA ;

1. Fermé : Exploitation propre, pas d'interconnexion avec d'autres réseaux ferroviaires.
2. Clos : Site propre, dédié au système de transport et sans partage de l'emprise au sol.
3. Certains systèmes nommés Tram-Train évoluent en réseau ouvert

– **Trains à Grande Vitesse** : reliant les métropoles urbaines distantes de 300 à 1000 km pour des trajets de 1 à 3 ou 4 heures. La grande vitesse (300 km/h) est atteinte seulement sur des lignes dédiées. En France, les trains à grande vitesse sont soumis au cadencement : le même schéma de dessertes, heures de départ, arrêts en cours de route, heure d'arrivée est répété à intervalles réguliers. Ex : TGV (France), ICE (Allemagne) ou AVE (Espagne) en Europe, Shinkansen au Japon ou encore KTX en Corée ;
– **Trains régionaux et interrégionaux** reliant les villes moyennes distantes de 50 à 300 km pour une durée de parcours de 30 minutes à 4 heures. La fréquence des trains est importante aux périodes de pointes. Ex : Corail, TER ;
– **Trains de « grande banlieue »**, ils apparaissent dans la zone d'attirance des grandes métropoles, l'exploitation est de type Corail, voire TGV sur des distances de 150 à 300 km pour un délai proche de l'heure. Exemples en France dans le grand bassin Parisien à destination de Rouen, Orléans, Le Mans, Tours, etc.

2.2. Système ferroviaire

Le chemin de fer est un système guidé pourvu de roues d'acier roulant sur des rails d'acier basé sur deux caractéristiques :

(1) Déplacement sur une dimension ;
(2) Adhérence et frottement faibles.

Ces deux caractéristiques imposent des contraintes d'exploitation pour le conducteur, les opérateurs de circulation et les installations de changement de voie. Le conducteur ne peut modifier sa route pour éviter une collision et doit disposer d'une distance de freinage supérieure à la vision humaine (à titre d'indication, la distance de freinage d'un train de fret lancé à 100 km/h est de 1 000 mètres et 3 500 mètres pour un TGV à 300 km/h). Le qualificatif « aveugle » s'emploie pour caractériser la conduite d'un train, celle-ci doit être basée sur l'anticipation et non sur la vision directe des événements. Un opérateur de circulation est nécessaire pour ordonnancer les circulations afin que les trains puissent se suivre, il doit prévenir le conducteur suffisamment tôt d'un ordre d'arrêt ou de ralentissement et maintenir devant ce train un espace libre suffisant pour lui permettre d'exécuter l'ordre transmis. La connexion de plusieurs voies est réalisée grâce aux installations de changement de voie, nommées appareils de voie ou encore aiguilles (voir figure 2.1 et la définition 2.10). Ces systèmes ont pour contrainte de conserver le guidage des roues et doivent permettre de prévenir les collisions entre véhicules.

***Définition 2.10* (Aiguille)**. — L'aiguille est un appareil de voie avec rails mobiles appelés « lames » permettant de diriger les trains dans deux directions différentes. La figure 2.2 présente un schéma d'aiguille. Les deux voies vers lesquelles les trains peuvent être dirigés sont sécantes entre elles au niveau du « cœur d'aiguille » (partie 3 sur le schéma). La partie intermédiaire (partie 2 sur le schéma) assure la traversée de la voie. La partie aiguillage (position 1 sur le schéma) comprends les deux lames mobiles. Les deux lames mobiles sont reliées entre elles au moyen d'une tringle d'écartement qui permet de connecter les deux lames : lorsque l'une est ouverte, l'autre est plaquée. Les tringles de manœuvre assurent la transmission du mouvement du moteur ou de la boite de manœuvre aux lames.

FIGURE 2.1. Aiguillage simple en gare d'Épône. *Photo JH. Mora, janvier 2005, GNU Free Dcocumentation License v1.2*

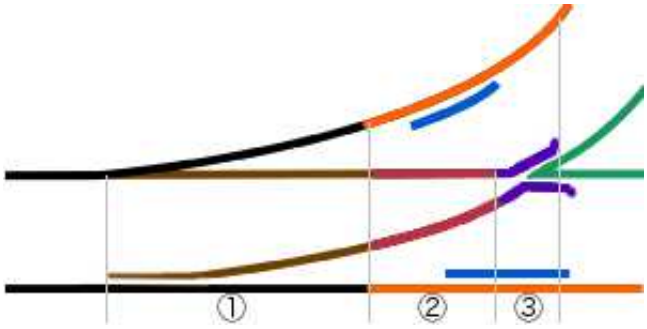


FIGURE 2.2. Schéma d'une aiguille

Du fait des dangers potentiels liés aux circulations (collisions, déraillements, *etc.*), le chemin de fer ne peut donc exister que par la prise en compte de la sécurité dans sa conception, sa réalisation et son exploitation. La prise en compte de la sécurité comme contrainte essentielle a permis de bâtir un système d'un très haut niveau de sécurité où les accidents sont rarissimes.

Comme tout système industriel le système ferroviaire comporte des opérateurs, des outils et des procédures, l'organisation définit les interactions entre ces trois composantes. Les outils et procédures permettent d'exploiter le système ferroviaire, l'opérateur est formé aux procédures et les outils doivent être adaptés aux opérateurs.

La responsabilité du système ferroviaire est partagée entre les gestionnaires d'infrastructures et les entreprises ferroviaires. L'infrastructure représente l'ensemble des installations fixes (voies, caténaires, énergie, *etc.*). L'entreprise ferroviaire dispose des matériels roulants. Les acteurs circulation travaillent pour le gestionnaire d'infrastructure et assurent la mise en condition opérationnelle du réseau. L'exploitation du réseau côté entreprise ferroviaire est réalisée par les

conducteurs et les acteurs sol. En France, le gestionnaire d'infrastructure est la société Réseau Ferré de France (RFF) et la Société Nationale des Chemins de Fer (SNCF) est une entreprise ferroviaire.

La sécurité des circulations concerne les interactions des circulations entre elles et le traitement des modifications inopinées de l'environnement. Elle est maîtrisée par les acteurs circulation, les conducteurs et les acteurs au sol des entreprises ferroviaires.

La sécurité technique assure la conservation des caractéristiques techniques et fonctionnelles permettant à un train de circuler sur l'infrastructure ferroviaire. Elle relève des opérateurs d'entretien et de maintenance du matériel roulant ainsi que des installations fixes.

2.3. Sécurité et transport guidé ferroviaire

L'utilisation d'un guidage repose en grande partie sur un souci de sécurité, car il simplifie la conduite et rend le véhicule moins tributaire d'aléas liés à la conduite dans plusieurs degrés de libertés. En contrepartie le véhicule reste prisonnier de l'infrastructure, le guidage impose une forte adéquation entre infrastructure et mobile tant au niveau technique (outils) que des procédures. Ce choix requiert un dimensionnement fort et robuste de l'exploitation des circulations et donc de l'offre de service, la démarche de sécurité est intrinsèquement liée à la démarche qualité. La réussite du transport ferroviaire repose sur la convergence de l'exploitation, de la qualité et de la sécurité.

Statistiquement, les transports guidés sont de très loin plus sécuritaires que le transport automobile, le nombre de victimes par accident de train est insignifiant par rapport au nombre de victimes d'accidents de la route. À titre d'exemple, l'*European Transport Safety Council* a publié en 2003 une étude statistique comparative de sécurité de différents mode de transport [**79**] pour la période 2001 et 2002. Le nombre de passagers tués par 100 millions de passagers – kilomètres pour les différents modes de transport est présenté dans le tableau 2.1.

Moyen de transport	**Nombre de tués par 100 millions de pass.-Km**
Route	0,95
Ferry	0,25
Aerien	0,035
Rail	0,035

TABLE 2.1. Tableau comparatif d'accidentologie des différents moyens de transport (UE)

Dans un système de transport privé (voiture, moto, vélo, voire piéton), chacun est responsable du niveau de risque qu'il est prêt à prendre et à faire prendre aux autres (consciemment ou inconsciemment). Alors que dans un système de transport public, les clients attendent du prestataire de service une sécurité sans faille. Les passagers sont passifs et de fait intransigeants avec le transporteur représenté par un acteur public ou capitalistique qui doit assumer la sécurité. Ce constat permet d'expliquer la grande différence d'acceptation sociale de l'insécurité entre ces deux modes de transport. Le nombre de victimes sur les routes de France est socialement

accepté alors que tout accident de train conduisant à un ou plusieurs morts est perçu comme inacceptable.

2.3.1. Liste des dangers. — La sécurité et l'exploitation des circulations reposent sur un principe : « La voie est libre et le restera », une assurance : « savoir arrêter et retenir les trains » ainsi qu'un dialogue codifié entre le sol et le véhicule.

Ainsi les principaux événements d'exploitation redoutés sont définis à partir du non respect du principe énoncé ci-dessus. L'itinéraire et/ou le départ vers une voie non libre ainsi que le non maintien de la voie libre (continuité du roulement, trains, manœuvres, obstacles, engagements de gabarit, travaux, passages à niveau, dérives, …) peuvent entraîner les événements redoutés suivants :

- Collision du véhicule avec un autre véhicule ou un obstacle ;
- Déraillement (perte du guidage).

La sécurité des biens et des personnes concerne les événements pouvant causer des dommages sur les biens ou les personnes. Elle peut être engagée dans les cas suivants [**57, 58**] :

- Événements liés à la sécurité des circulations (listés ci-dessus) ;
- Chute depuis le train ou à l'intérieur du train ;
- Sécurité dans les gares et dans les trains (sûreté publique, agressions, attentats) ;
- Asphyxie, Brûlures, (incendie, etc.) ;
- Transport de matières dangereuses (dangers chimiques, explosions, etc.) ;
- Électrocution (spécifique de la traction électrique)

2.3.2. Typologie d'accidents de circulation. —

2.3.2.1. Collisions. — Les collisions entre circulations peuvent être de trois types qui sont également typiques de la circulation automobile : le rattrapage, le nez à nez et la prise en écharpe.

Le rattrapage ainsi que son nom l'indique survient lorsqu'une circulation en percute une autre par l'arrière. Lorsque la circulation est possible dans les deux sens sur une voie (de façon permanente i.e. voie unique ou voie banalisée, ou bien de façon temporaire i.e. circulation à contresens) l'événement collision frontale ou « nez à nez » entre deux mobiles doit être pris en compte.

Enfin, la présence indispensable des appareils de voies permettant de créer plusieurs itinéraires induit des scénarios de collisions particulièrement graves par prise en écharpe, un train en percutant un autre de biais au niveau de l'appareil de voie, voir figure 2.3.

2.3.2.2. Déraillements. — Les scénarios de déraillements peuvent être causés par la survitesse ou une défaillance technique du guidage (roues, essieux, rails et aiguilles).

La survitesse comme scénario envisageable de déraillement, notamment dans les courbes, relève du dépassement du seuil maximal d'effort sur l'infrastructure. Le train quitte alors l'espace à une dimension imposé par le guidage. Le niveau de gravité du déraillement est généralement lié à la collision avec des éléments d'infrastructure ou à un véhicule sur la voie opposée, ainsi que la tenue ou non de l'alignement du train en dehors de son espace de guidage.

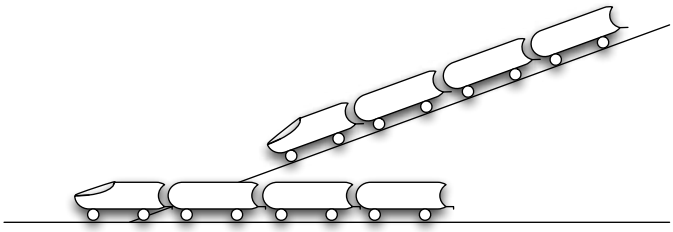


FIGURE 2.3. Collision par prise en écharpe

Les défaillances techniques contribuant aux scénarios de déraillement sont triées par composantes :

- La voie : rail cassé, écrasement de la voie, etc. ;
- Le matériel roulant : rupture d'essieu, casse sur organe de roulement, freins, etc. ;
- L'exploitation : mauvaise utilisation des installations, problème de manœuvres, erreur de composition des trains, mauvais chargement, etc. ;
- Obstacles sur la voie : les obstacles entravant la voie peuvent être d'origine interne au système ferroviaire dans le cas de pertes de marchandises ou d'engagement de gabarit ou d'origine externe notamment sur passage à niveau, chute de rochers, passage d'animaux divaguant etc.
- Le déraillement lié aux mouvements des appareils de voies.

Ce dernier mérite une attention particulière, en effet deux situations peuvent se produire en fonction de la position et de l'immobilité de l'aiguille. Lorsque la lame directionnelle d'une aiguille ne colle pas au rail, l'essieu enfourche l'appareil de voie et sort de la voie en s'immobilisant entre les deux voies, c'est le déraillement par *enfourchement*. Lorsqu'une aiguille bascule avant que le train n'ait totalement dégagé l'appareil de voie, les premiers bogies prennent une direction et les derniers suivent l'autre direction, c'est un déraillement par *bi-voie* voir figure 2.4. L'immobilité absolue et le bon positionnement d'un appareil de voie et des lames d'aiguille lors du passage d'un train sont deux conditions fondamentales.

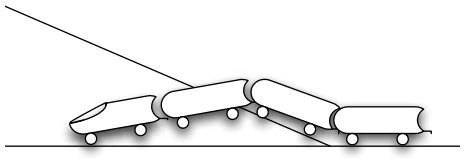


FIGURE 2.4. Déraillement par bi-voie

2.3.3. Fonctions de sécurité. — Les fonctions de sécurité mettent en œuvre les principes de sécurité :

- Itinéraire vers voie libre : Ce principe est assuré par un système de contrôle de libération de la voie, un système d'enclenchement d'itinéraires (verrouille les itinéraires incompatibles), le cantonnement des trains et la signalisation.

– Le maintien de la voie libre : Les systèmes d'enclenchements d'itinéraires et la signalisation assurent ce principe de sécurité.

De plus, des fonctions de sécurité sont mises en place pour contenir chaque type d'accidents de circulation :

Collision :
– le rattrapage est protégé par les fonctions de sécurité freinage, signalisation et cantonnement des trains,
– le nez à nez est protégé par les fonctions des enclenchements et la signalisation,
– la prise en écharpe est protégée par les fonctions de sécurité des aiguillages, des enclenchements et de la signalisation,
– les fonctions de sécurité relatives aux obstacles sur la voie sont assurées par des mécanismes de détection d'obstacles pour la pleine voie et pour les passages à niveau [4] ;

Déraillement :
– par survitesse en courbe : les fonctions de sécurité associées sont la stabilité, le contrôle de la vitesse, la signalisation et le freinage,
– par défaillance technique : la politique de maintenance, la surveillance des circulations (par des agents au bord des voies) et les règles de composition permettent de se prémunir contre les défaillances techniques entraînant des déraillements,
– lié aux appareils de voies : la signalisation, les enclenchements et contrôles de position des lames d'aiguilles permettent de s'en protéger.

Les fonctions de sécurité sont propres à chaque composant technique (matériel roulant, infrastructure) ou en interface technique entre le mobile et le sol comme les aspects mécanique et technique du guidage ou les échanges électriques (traction, signalisation), les échanges de données, etc.

Comme indiqué plus haut, la sécurité repose sur un principe simple qui est assuré par les fonctions de sécurité. A tout instant, la sécurité repose également sur l'assurance de pouvoir arrêter et retenir les trains. Cette assurance est contenue dans les fonctions de sécurité relatives à la prévention des accidents de circulation (signalisation, freinage, contrôle de vigilance, contrôle de vitesse, formation et composition des trains).

Les fonctions de sécurité requièrent une organisation capable de les interpréter et de les mettre en œuvre. Les procédures sont là pour contraindre la sécurité. On distingue les procédures liées à l'exploitation de celles de la conduite des trains et celles de la maintenance du système ferré.

2.4. Les procédures sécurité de l'exploitation

2.4.1. Le canton ferroviaire. — Compte-tenu des contraintes d'exploitation pour les conducteurs de trains, la sécurité ferroviaire repose sur le cantonnement des trains et donc la détection de l'occupation de la voie. Le principe de sécurité sous-jacent est la séparation géographique des trains. Le canton délimite une zone géographique élémentaire dans laquelle il ne peut y avoir qu'un seul train. La longueur du canton est calculée en fonction de la distance de freinage maximale des trains pouvant circuler sur la voie. Les conducteurs sont autorisés à circuler sur

4. Ces fonctions sont relativement rares, matérialisées par des filets au-dessus des ponts ou bien par la détection d'objets métalliques sur les rails faisant shunter les circuits de voies

les cantons libres grâce à un système de dialogue sol – train appelé « signalisation ». Entre deux circulations, il est nécessaire de maintenir un espace suffisant (un canton) pour que le train suiveur puisse freiner, un dispositif de localisation des trains couplé à la signalisation est donc nécessaire pour interdire l'accès du canton occupé et ordonner le freinage au niveau du canton précédent.

Un dispositif de localisation des trains détecte l'occupation d'un canton ferroviaire et est relié à des signaux aux bords des voies à l'entrée des cantons. Plusieurs systèmes sont disponibles, le plus courant est appelé « circuit de voie », son principe est simple et est apparu très tôt dans le développement des systèmes ferroviaires. Il s'agit de mettre en place une isolation électrique entre les cantons ferroviaires et de faire circuler un courant entre les deux files de rails du canton en installant un émetteur et un récepteur électrique aux extrémités du canton. La présence d'un essieu métallique sur le canton court-circuite (*shunte*) ce courant, l'absence de tension sur le récepteur du canton indique l'occupation de celui-ci et modifie l'état du signal d'entrée du canton sur la position fermée (sémaphore rouge) et de celui en amont sur la position avertissement (sémaphore jaune).

Ce système est primordial pour protéger les circulations des collisions. La protection contre les déraillements est également effectué par un dispositif de signalisation. Le paragraphe suivant présente brièvement la procédure d'application de la signalisation et les différents types de signaux.

(a) Signal mécanique fermé, « carré »

(b) Signal lumineux ouvert « voie libre »

FIGURE 2.5. Signalisation SNCF *Autorisation photo Peter Bereczki.*

2.4.2. La signalisation. — L'ouvrage de référence en matière de signalisation ferroviaire est le livre de Roger Rétiveau [**110**] écrit en 1987. À notre connaissance peu de références existent dans ce domaine depuis ce livre.

Les fonctions de sécurité remplies par la signalisation sont efficaces dans la mesure où tout agent, quelles que soient ses fonctions, doit obéissance passive et immédiate aux signaux le

concernant. L'agent est donc formé à la lecture et à l'exécution des informations fournies par la signalétique.

Mis à part le cas des manœuvres, une circulation ferroviaire est « aveugle », car sa distance de freinage et d'arrêt est supérieure à la possibilité de la vision humaine. De fait, tout signal d'exécution est précédé d'un signal à distance l'annonçant et permettant l'exécution de l'ordre donné par la signalétique au point voulu.

La signalisation a pour but d'indiquer au conducteur les conditions de circulation de la voie en aval pour lui permettre de régler la conduite du train. La signalisation comprend les signaux d'arrêt, les signaux d'annonce d'arrêt, les signaux de limitation de vitesse, les signaux à main et détonants, les signaux de manœuvre, les signaux divers et les signaux de traction électrique.

Les signaux peuvent être permanents ou temporaires, fixes ou mobiles, lumineux ou mécaniques. Normalement implantés à gauche ou au-dessus de la voie à laquelle ils s'adressent, ils peuvent toutefois être mis à droite dans les cas prévus par les règlements (installation de contresens par exemple).

2.4.2.1. La signalisation lumineuse. — La signalisation lumineuse a été introduite pour les circulations de nuit. Autrefois la signalisation était mécanique de jour et assurée par des feux la nuit. Les indications de jour se faisaient par cocarde de couleur ou bien par tableau mécanique (voir figure 2.5(a)).

La forme de la cocarde est caractéristique d'un signal et correspond à une couleur permettant d'associer le signal à sa signification. La couleur des feux de nuit est identique à la signalisation lumineuse moderne.

Aujourd'hui la signalisation lumineuse est généralisée sur l'ensemble des réseaux, il subsiste cependant quelques portions de voie en signalisation mécanique.

La signalisation lumineuse est présentée sur des panneaux noirs bordés de blanc portant un ou plusieurs feux (voir figure 2.5(b)).

La position des feux sur les panneaux est toujours à la même place quel que soit le nombre de feux sur le panneau. La couleur des feux et leur positionnement sur le panneau ainsi que la forme du panneau participent à la signification donnée par la signalisation.

Les différents signaux participant à la réglementation ferroviaire sont présentés dans le paragraphe suivant.

2.4.2.2. Types de signalisation. —

– Signalisation d'arrêt : Comme son nom l'indique, la classe des signaux d'arrêt commande l'arrêt des circulations. L'arrêt est commandé pour deux raisons, le maintien de l'espacement entre les trains (cantonnement) et la protection des appareils de voies. Enfin pour permettre la bonne exécution de l'ordre d'arrêt au point géographique voulu, des signaux d'annonce d'arrêt sont présentés aux circulations.

  – Signaux de protection : Appelé Carré en France à la SNCF en raison de sa forme en signalisation mécanique représentant une cocarde carrée à damier rouge et blanc. En signalisation lumineuse, il présente généralement deux feux rouges sur une ligne verticale ou horizontale.

– Signaux de cantonnement (sémaphore) : associé à un système de cantonnement des trains permettant de garantir un espacement minimal entre les trains, ce signal annonce l'occupation des cantons ferroviaires.
– Signaux d'annonce d'arrêt (avertissement) ;
– Signalisation de limitation de vitesse :
– signaux de ralentissement et de rappel de ralentissement,
– signaux de limitation permanente de vitesse,
– signaux de limitation temporaire de vitesse ;
– Signalisation en cabine.

2.4.3. Systèmes d'enclenchement des itinéraires. — La présence d'aiguillages définit plusieurs possibilités d'itinéraires (voir définition 2.9) pour les circulations.

Un itinéraire est « autorisé » lorsqu'il peut être parcouru par un train. Un itinéraire signalisé est autorisé par ouverture de son signal d'origine. Si le signal est fermé, l'itinéraire peut néanmoins être autorisé par délivrance, par le chef de poste, d'une autorisation de franchir un signal fermé (C'est l'une des procédures exceptionnelles voir le paragraphe 2.4.8).

Deux itinéraires sont incompatibles lorsqu'ils ne peuvent pas être parcourus simultanément sans danger par des circulations différentes. Deux catégories d'incompatibilités sont à distinguer :

Incompatibilité par position d'aiguille : les deux itinéraires considérés comportent une aiguille en commun, chacun d'eux correspondant à une position différente de l'appareil, éventuellement deux appareils de voie peuvent être concernés. Ces itinéraires peuvent être convergents, divergents, sécants ou en tiroir (itinéraire en impasse servant à effectuer certaines manœuvres) ;

Incompabilité par sens de circulation : les deux itinéraires considérés ont des sens de circulation contraires et :

(1) soit comportent une partie de voie commune, la ou les aiguilles communes ayant la même position (itinéraires inverses),

(2) soit donnent accès à une même partie de voie (itinéraires nez à nez).

Les enclenchements ont pour objet de rendre impossibles des opérations qui seraient contraires aux règles de sécurité. Dans les postes fonctionnant par itinéraires, les enclenchements interviennent au niveau de la formation et de la destruction des itinéraires et de la commande des aiguilles. On distingue plusieurs types d'enclenchement :

Enclenchement d'incompatibilité : Il s'oppose à la formation de tout itinéraire incompatible par position d'aiguille et par sens de circulation avec un itinéraire déjà formé ;

Enclenchement d'approche : Il s'oppose à la destruction manuelle immédiate d'un itinéraire lorsqu'une partie de voie, située en amont du signal d'origine de l'itinéraire, est engagée par un train. Cette partie de voie, comportant un ou plusieurs circuit de voie, est appelée « zone d'approche » ;

Enclenchement de transit : Il s'oppose à la destruction manuelle immédiate d'un itinéraire tant que la partie de voie comprenant l'ensemble des appareils de voie de l'itinéraire n'est pas dégagée. Cette partie de voie est appelée « zone de transit » ;

Enclenchement de zone d'aiguille : Il s'oppose à la modification de la position d'un appareil de voie lorsqu'une partie de voie, comprenant l'appareil, est engagée par un train. Cette partie de voie, comportant un ou plusieurs circuits de voie, est appelée « zone d'aiguille ».

2.4.4. Les procédures de circulation. — Les procédures de circulation réglementent l'exploitation du système ferroviaire. Elles sont appliquées par les acteurs de la circulation présents dans les différents postes de commandement et sur le terrain.

Avant de décrire les règles générales d'exploitation, il est nécessaire de définir le métier des acteurs de la circulation qui organisent et contrôlent les circulations.

Définition 2.11 **(Régulateur)**. — opérateur humain chargé d'organiser et de suivre la circulation des trains sur certaines lignes. Il a la charge d'exécuter certaines opérations de sécurité.

Définition 2.12 **(Agent circulation)**. — Opérateur humain responsable du service de la circulation sur un ensemble d'installations appelé « secteur circulation ».

Il peut n'y avoir qu'un seul agent circulation par secteur de circulation. Il assume seul la responsabilité de la sécurité sur le secteur de circulation et dispose de l'autorité dans ce domaine sur tout autre agent (même si celui-ci est supérieur dans la hiérarchie).

Il organise la circulation des trains en tenant compte de l'ordre de succession des trains imposé en entrée de la gare et fait respecter la contrainte d'ordre de succession des trains en sortie de sa gare :

- en fonction des informations ou directives reçues du régulateur ;
- en accord avec les agents circulation des gares connexes ;
- d'entente avec les agents circulations des autres secteurs circulation et des dirigeants des chantiers locaux de la gare ;
- en fonction de situations spécifiques : incidents, travaux, etc.

D'une manière générale, une gare constitue un ensemble de voies sous la responsabilité d'agents circulations. Une gare peut contenir plusieurs secteurs circulations, la cohésion entre les agents circulations d'une même gare est assurée par le chef circulation.

Définition 2.13 **(Chef circulation)**. — Il a autorité du point de vue de l'organisation de la circulation sur les autres agents circulations dans les gares importantes, mais chaque agent circulation reste responsable de la sécurité sur son secteur circulation. Il peut de plus exercer tout ou partie des missions de régulateur.

Les règles générales d'exploitation des voies principales reposent sur le principe de protection de la voie. Une circulation ne peut être engagée si la voie est occupée (par une autre circulation, par des travaux ou bien un obstacle).

La voie principale est protégée par les signaux d'arrêt et par la bonne position des appareils de voies.

L'agent circulation a la possibilité de fermer la voie. Pour ce faire, il doit protéger la voie et apposer un dispositif d'attention sur les organes de commande concernés.

L'engagement des voies principales dans une gare que ce soit par une circulation, un stationnement ou une manœuvre ne peut avoir lieu sans l'ordre de l'agent circulation.

2.4.5. Circulation des trains. — Les trains sont désignés par un numéro de marche ou lorsque leur marche est indéterminée par un numéro spécifique. Le respect de l'horaire est primordial, plus en ce qui concerne les avances que les retards. Les trains ne doivent pas circuler avec plus de trois minutes d'avance sauf dans certaines situations dites « sur ordre » en cas de suppression d'arrêt. Les arrêts sont réglementés, il y a les arrêts normaux ou prescrits qui doivent être respectés, les arrêts normaux facultatifs qui ne sont respectés que si la circulation le nécessite et les arrêts fortuits ou accidentels.

Après un arrêt régulier ou prescrit, une procédure de départ réglementée doit être exécutée. Elle consiste à s'assurer que la formation et le service du train sont terminés, que l'heure du départ est atteinte, que rien ne s'oppose au départ du train et que le signal de sortie est ouvert.

Les arrêts fortuits ou incidentels font l'objet d'une procédure de reprise spécifique à chaque système ferroviaire et représente généralement une tâche complexe à mettre en œuvre compte tenu de la nécessaire réorganisation du trafic (la bonne collaboration entre les acteurs de la circulation est primordiale dans une telle situation.)

La réception des trains est spécifique aux types de voies (principales ou voies de services). La déviation de l'itinéraire prévu d'un train implique l'arrêt du train avant le signal précédant la bifurcation afin de pouvoir aviser le conducteur du train du changement d'itinéraire.

2.4.6. Incidents de circulation. — Les acteurs de la circulation (niveau organisationnel ou sur le terrain) sont chargés de surveiller toutes les conditions dangereuses de circulation des trains (boites chaudes [5], frein serré, chargement déplacé, *etc.*). L'agent a la charge d'arrêter ou de faire arrêter le train une fois le danger identifié. Sur les lignes à grande vitesse (LGV), un dispositif automatique de détection de boîte chaude provoque une alarme danger au poste de l'agent circulation. Selon la température atteinte par la boite, le système déclenche la signalisation d'arrêt au train concerné et commande la limitation de vitesse à 80 km/h aux trains croiseurs.

Tout agent qui constate ou ressent un choc et/ou une présomption de danger fait arrêter le train. Le conducteur fait protéger la zone concernée via l'agent circulation et avise un agent sur le terrain par radio ou par téléphone de la gare la plus proche.

Dans les cas de rupture d'attelage, de déraillement ou de partie de train laissée en pleine voie, c'est au conducteur d'assurer autant que possible la mise en protection des voies voisines dans le cas où elles sont engagées.

Lors d'une dérive (train sans moyen de freinage) le conducteur doit aviser les gares pouvant être concernées par la trajectoire du train par radio et/ou par sifflet. Les agents circulation, après avoir identifié le train en dérive, doivent prendre les mesures nécessaires pour arrêter et garer les trains se dirigeant vers la dérive ou pouvant la croiser jusqu'à la fin du danger, et mettre en œuvre par tous les moyens possibles (espace suffisant en avant pour arrêt) l'arrêt du train en dérive et l'immobiliser.

5. Symptôme de chauffe des roulements mécaniques situés dans les essieux du train, causé par le non desserrage d'un frein ou bien la déformation mécanique du roulement.

2.4.7. Danger sur la voie. — En cas de danger sur la voie, présence d'obstacles inopinés par exemple, l'agent circulation dès qu'il est informé doit arrêter et retenir les trains se dirigeant vers l'obstacle. Il doit s'assurer que l'obstacle est protégé après avoir vérifié qu'il n'y a pas de trains entre la gare et l'obstacle ou bien que s'il y en a, ceux-ci sont arrêtés et retenus. Un train peut éventuellement être autorisé à repartir par l'agent circulation après avoir donné par écrit un ordre de marche prudente. La reprise du service normal n'est possible qu'après avis de disparition du danger.

2.4.8. Procédures exceptionnelles. — Lorsque les systèmes de protection ne sont pas disponibles, en situation dégradée ou lors de l'exécution de travaux de maintenance, il existe des procédures papier rigoureuses exécutées en collaboration par l'agent circulation et le conducteur afin de permettre les circulations sous certaines conditions garantissant la sécurité. Par exemple, un signal de protection non franchissable anormalement fermé peut être franchi par un train à condition que l'agent circulation dans le poste se soit assuré par une procédure de type *check-list* que la voie est libre et que les itinéraires incompatibles soient fermés et bloqués.

2.5. La supervision du trafic : les postes

2.5.1. Historique. — Le présent historique a été réalisé à la lecture de l'ouvrage d'Alain Gernigon sur l'histoire de la signalisation ferroviaire française [**51**].

Les premiers signaux étaient manœuvrés à pied d'œuvre, de même que les appareils de voie. Le personnel requis était égal au nombre d'appareils à manœuvrer. La coordination d'une telle équipe dispersée sur la zone engendre inévitablement des erreurs et donc des risques. Pour pallier ces risques, les signaux ont été directement reliés aux aiguilles en fonction d'itinéraires établis. La réalisation du premier système d'enclenchement aiguille - signal a été inventé par Pierre-Auguste Vignier (1811 - 1891) en 1847. Il eut l'idée de rapprocher le signal (mécanique à l'époque) de l'aiguille par une pièce en bois appelée verrou Vignier.

> « Le principe consiste à enclencher deux leviers l'un par l'autre, réalisé à l'aide d'un doigt (verrou) tributaire du premier levier verrouillant (ou libérant), lors de la manœuvre, le second ; l'action de cet enclenchement étant réciproque. » [**51**]

Cette idée fût ensuite reprise pour relier entre eux le mouvement de plusieurs aiguilles et ainsi créer des itinéraires préétablis.

De l'autre côté de la Manche, vers 1843, Stevens (de la compagnie Stevens and Co.) eut l'idée de rapprocher les différents leviers de manœuvre des appareils d'une bifurcation (aiguille et signaux) dans un même lieu (poste ou cabine d'aiguillage) sans pour autant les relier par un enclenchement [(6)]. Ce système fût vite rapidement amélioré en intégrant les enclenchements (en utilisant une technique différente de celle de Vignier), les différents leviers sont raccordés à une table d'enclenchement. Notons aussi les systèmes d'enclenchements Saxby qui ont été installés en grand nombre au début du XX^{e} siècle et qui pour certains ont fonctionné jusqu'en 1987 [(7)].

6. Ce système appelé *Stevens stirrup frame* châssis Stevens à étrier fût mis en service à Kentish Town Junction, GB, en 1844.

7. Notamment, le poste B de Mohon de 1907 à 1987 [**51**].

Ainsi dans un même poste, il est possible de positionner tous les itinéraires et les signaux associés d'une même zone. Le développement jusque dans les années 1930 de nouveaux postes d'aiguillage a apporté son lot d'innovations technologiques telles que les commandes à distance, la motorisation des mouvements d'aiguilles et le Tableau de Contrôle Optique (TCO) permettant de visualiser sur un tableau l'évolution des circulations sur la zone d'enclenchement. Mais les principes restent les mêmes. La figure 2.6 présente un exemple de TCO.

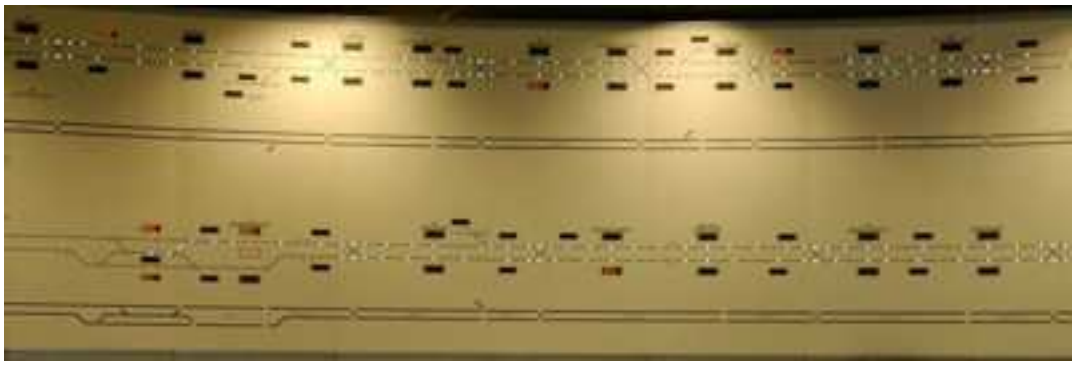


FIGURE 2.6. Exemple de TCO, détail d'une photographie ALSTOM Transport

2.5.2. Les différents types de poste. — Ce paragraphe présente les types de postes ferroviaires en fonction des différentes technologies qui ont été utilisées pour les réaliser.

2.5.2.1. Postes à relais. — Le développement de l'ingénierie électromécanique a remplacé les systèmes mécaniques des enclenchements avec comme principale innovation les postes à leviers d'itinéraires et l'apparition de tableaux de contrôle optique ou TCO. Dans les années 1950 apparaissent les premiers postes réalisant l'enclenchement d'itinéraire par des relais électromécaniques appelés « poste tout relais ». De simples boutons poussoirs remplacent les leviers et de nouvelles fonctionnalités voient le jour et permettent de faciliter l'exploitation de ces postes :

– la destruction automatique des itinéraires : chaque circulation remet au passage du signal le relais d'enclenchement d'itinéraire en position de repos. Le tracé sur le TCO est alors effacé au fur et à mesure de la libération des zones de l'itinéraire ;
– le tracé permanent : le passage d'une circulation ne détruit pas l'itinéraire, la séparation spatiale des trains est assurée par la signalisation de cantonnement ;

Il existe différents postes utilisant cette technologie mais de conceptions différentes :
– PRA : Poste tout Relais à transit souple et à destruction Automatique ;
– PRS : Poste tout Relais à transit Souple ;
– PRG : Poste tout Relais Géographiques, pour l'opérateur, la principale innovation vient de la fusion du TCO et du pupitre de commande : c'est la table de commande et de contrôle.

2.5.2.2. Postes informatisés. — C'est en 1984 que fut exploité en France le premier Poste à Relais à Commande Informatique (PRCI) : le pupitre du PRS est remplacé par un clavier et un moniteur. Pour les postes importants un TCO complète l'équipement. L'intérêt du PRCI est la programmation : l'agent circulation peut programmer des séquences d'itinéraires sur un service complet, ce qui lui permet de se concentrer sur la gestion des conflits de circulations et, entre autres, de gérer un secteur toujours plus important. Enfin, dans les postes entièrement

informatisés PAI ou PIPC (Poste Informatique à technologie PC) toutes les fonctions sont réalisées par l'informatique (y compris les enclenchements) et les relais ont disparu.

2.6. Systèmes modernes de contrôle de mouvement des trains

2.6.1. Automatic Train Control. — Le développement de systèmes d'aide à la conduite (exemple SACEM [**62**]) et par la suite de l'automatisation du mouvement des trains (ex : VAL, MAGGALY [**94**] et SAET-METEOR [**36**]) a été motivé au départ pour des considérations de capacité de transport et de qualité de service. Cette automatisation permet de réduire les intervalles entre chaque train et permet donc de réduire le temps d'attente des voyageurs. Le retour d'expérience sur les lignes équipées montre qu'en effet le trafic s'en trouve fluidifié, les trains sont donc plus ponctuels, ce qui se traduit par en moyenne 98% des trains à l'heure. Par ailleurs, les fonctions sécuritaires de protection du mouvement des trains qui font nécessairement partie d'un système de contrôle automatique des trains sont à même d'intervenir en cas d'erreur humaine pouvant engager la sécurité (franchissement de signaux fermés, *etc.*). A l'extrême dans les systèmes en automatisme intégral, tout risque d'erreur de conduite est écarté. Là encore le retour d'expérience permet d'affirmer que le niveau de sécurité global est amélioré par l'automatisation (à ce jour les seuls cas d'accident sérieux sur métro automatique sont des erreurs humaines lors de travaux sur le système ou à proximité du système). Cette section présente l'architecture typique d'un système de contrôle automatique des trains (ATC) puis détaille les mécanismes qui assurent la mise en sécurité du système.

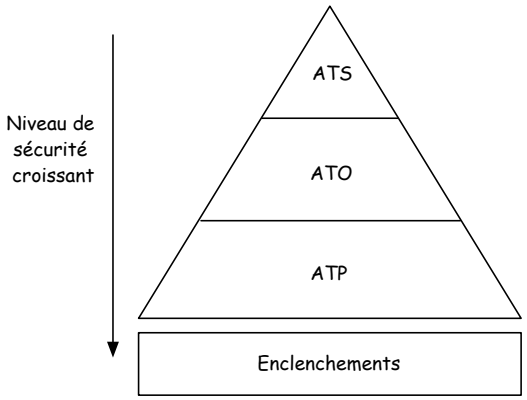


FIGURE 2.7. Systèmes ATC

Le système ATC est composé de trois sous-systèmes (voir figure 2.7) :

- le système ATP : Automatic Train Protection ;
- le système ATO : Automatic Train Operation ;
- le système ATS : Automatic Train Supervision ;

2.6.1.1. Automatic Train Protection. — Le système automatique de protection des trains met en œuvre les fonctions qui assurent la protection des passagers, du personnel et des équipements contre les principaux dangers liés à la circulation ferroviaire (collisions entre trains, survitesses,

déraillements, …). L'espacement entre les trains est assuré par la fonction de gestion d'occupation des cantons. La ligne est découpée en secteurs appelés cantons. Le principe de base de la sécurité ferroviaire consiste, via la signalisation latérale, à n'autoriser la présence que d'un seul train par canton. Dans la plupart des cas, les cantons sont fixes par rapport au sol (cantonnement fixe) et la signalisation latérale est constituée de feux en limites de canton. Pour les systèmes les plus modernes le canton se déplace avec le train et sa longueur évolue avec la vitesse et l'occupation de la voie (canton mobile déformable), ce qui permet une optimisation de la capacité de transport de la ligne. Dans les deux cas le système ATP est en mesure de détecter les vitesses non compatibles avec le respect de l'arrêt en limite de canton occupé et à l'extrême la pénétration sur un canton occupé (et naturellement d'agir en conséquence en freinant le train en urgence si l'un de ces événements se produit). La terminologie usuelle distingue de l'ATP les enclenchements dont la fonction essentielle est d'empêcher les mouvements de trains incompatibles sur les zones d'aiguillage.

2.6.1.2. Automatic Train Operation. — Le système ATO réalise la fonction de pilotage complet ou partiel du train. Il contrôle le mouvement du train en accord avec la table horaire définie quotidiennement pour l'exploitation de la ligne. Il gère les arrêts programmés dans les gares, l'ouverture et la fermeture des portes et le respect du temps d'arrêt dans les gares. Enfin le système redémarre le train après chaque arrêt dans le cas d'un système en automatisme intégral. Dans le cas d'un système automatique partiel, l'ordre de fermeture et d'ouverture des portes ainsi que l'ordre de départ sont effectués par un opérateur à bord du train (conducteur ou « attendant »).

2.6.1.3. Automatic Train Supervision. — L'ATS (voir figure 2.8) assure la surveillance et la régulation de l'ensemble des sous-systèmes qui composent le réseau, du système de suivi des circulations et de l'état des enclenchements aux informations passagers. Les nouvelles technologies de communication ont permis d'intégrer de nombreuses fonctionnalités dans le PCC. L'état de ces systèmes y est représenté sur le TCO servant de panneau de visualisation commun à l'ensemble du personnel.

En guise d'illustration la figure 2.9, présente un exemple de synoptique utilisé dans un TCO afin de superviser les circulations, les signaux et les équipements de voie. Les segments graphiques représentent les circuits de voie qui permettent de détecter l'occupation d'un canton (en rouge). Le code couleur jaune indique que l'itinéraire (succession de cantons) n'est pas tracé alors qu'une succession de cantons en blanc signifie que l'itinéraire est tracé et donc que la circulation est autorisée sur cet itinéraire. Les opérateurs ATS ne peuvent visualiser que la signalisation de manœuvre, c'est-à-dire les signaux qui protègent le mouvement d'appareil de voie. La signalisation de cantonnement n'est pas représentée sur les TCO. Les appareils de voie qui permettent de changer de direction sont représentés par des circuits de voie diagonaux entre les deux voies, les aiguilles sont placées aux extrémités. La position des aiguilles n'est pas représentée sur cet exemple, les opérateurs disposent d'autres vues pour connaître la position des aiguilles.

En effet, les postes de travail opérateur peuvent fournir des vues plus ou moins détaillées et des tableaux ou graphiques de télémesures. L'information présentée peut ainsi être plus ou moins fine selon les contraintes opérationnelles de la ligne. L'ATS permet donc d'appréhender de manière globale l'état d'exploitation de la ligne (par le synoptique en général présenté au TCO

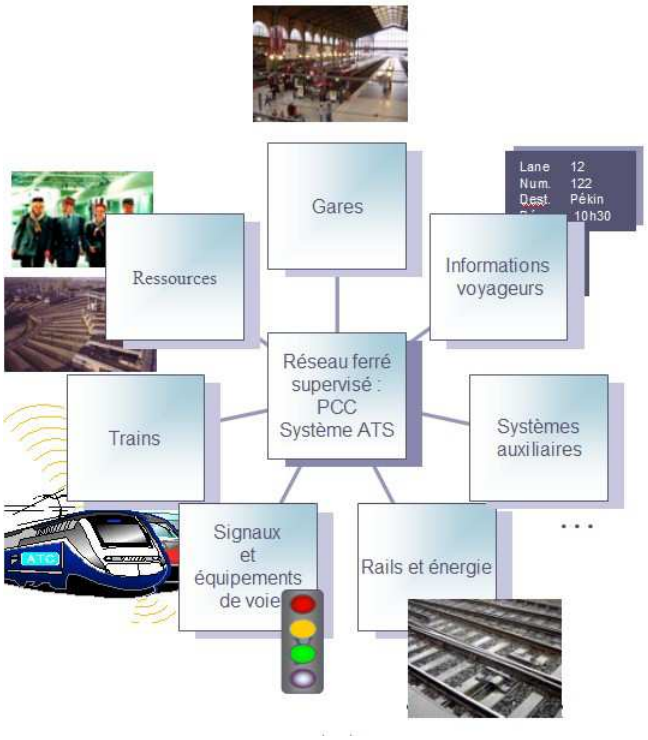


FIGURE 2.8. Description d'un ATS

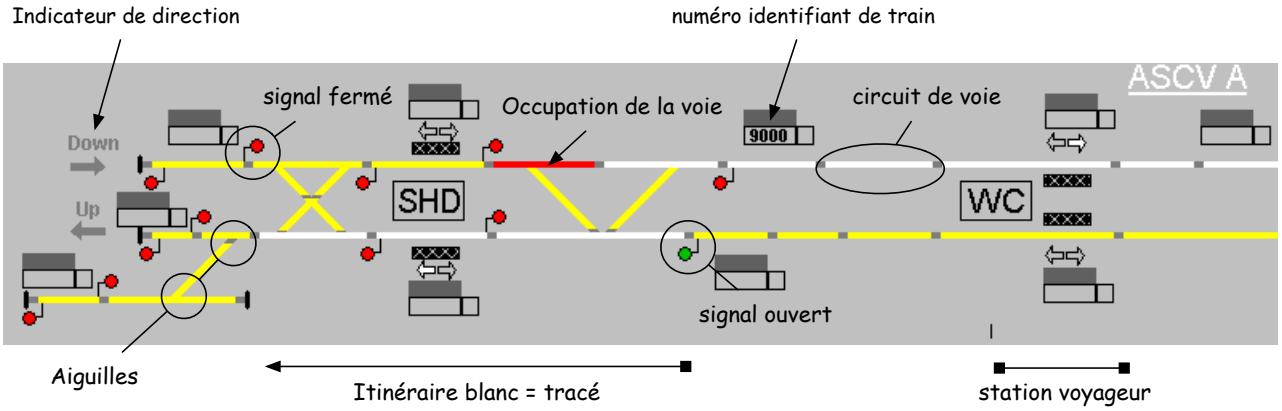


FIGURE 2.9. Exemple de TCO

qui affiche en temps réel des informations comme les cantons occupés, la position des aiguillages, l'état du réseau d'énergie) mais également de focaliser son attention sur un matériel particulier (fixe ou embarqué à bord d'un train) via les télémesures également mises à jour en temps réel, permettant entre autres les remontées d'alarmes sur lesquelles l'opérateur peut alors obtenir des détails. L'ATS présente également les données permettant aux opérateurs PCC d'effectuer la régulation du trafic (en ferroviaire grandes lignes, cette fonction est effectuée par un opérateur particulier appelé régulateur) qui consiste à décider de la politique d'exploitation à adopter en

cas d'incident retardant des trains. Suivant les systèmes, différents types de télécommandes sont possibles depuis les postes ATS, permettant par exemple d'interdire temporairement le départ d'un train ou de lui ordonner une réduction de vitesse pour le reste de son parcours.

2.6.2. Architecture de sécurité. — Comme rappelé ci-avant, les fonctions identifiées de sécurité sont celles de l'ATP et la gestion des enclenchements. Ces deux fonctions font appel désormais à la technologie des systèmes informatisés à très haut niveau de sécurité après avoir historiquement été réalisées par des relais de sécurité et des circuits analogiques en sécurité intrinsèque. Il s'agit toutefois d'une mutation toujours en cours à ce jour : de nombreux ATP analogiques et postes d'aiguillage à relais sont encore en service y compris pour des systèmes en automatisme intégral, mais tout laisse à penser que de par la souplesse et le gain de place qu'ils apportent, les systèmes numériques s'imposeront, qu'il s'agisse de systèmes ATP ou de postes d'aiguillage PAI [**84**] pour la SNCF (en 1997) ou les PIPC (en 1998), les PI-NG en cours d'installation et le PMI (Poste de Manœuvre Informatisé) [**50**] pour la RATP installé fin 2005. Le développement de tels systèmes informatisés de sécurité implique naturellement des méthodes d'une grande rigueur qui sont recommandées par le référentiel CENELEC [**33, 34, 35**]. Cela concerne l'aspect matériel (certains produits étant basés sur des calculateurs sécuritaires développés spécifiquement) ainsi que l'aspect logiciel (l'évitement et l'élimination des fautes des logiciels de sécurité faisant l'objet de techniques spécifiques pouvant aller jusqu'au développement entièrement formel).

Par contre, les fonctions de l'ATO comportent par nature des asservissements complexes et ne sont pour cette raison pas réalisées en sécurité (la sécurité reposant alors sur l'intervention de l'ATP en cas de défaillance de l'ATO pouvant conduire à une situation dangereuse). Ainsi l'approche sécurité de l'ATC considère comme possible une défaillance conduisant l'ATO à émettre un ordre de traction intempestif provoquant une accélération intempestive : la sécurité est dans ce cas assurée par l'ATP effectuant une fonction plus simple (contrôle du respect des limites de vitesse) réalisée en sécurité (pas de défaillances directement dangereuses ou restant latentes non détectées) et donc en mesure de mettre le train en sécurité (par freinage d'urgence) en cas de défaillance de l'ATO considéré comme ne contribuant pas à la sécurité.

Dans l'état de l'art actuel, il en est de même pour l'ATS dans la mesure où il est vrai qu'en mode nominal il n'intervient pas dans la sécurité. De plus pour des raisons économiques et de qualité, les ATS font largement appel à des composants sur étagère (Commercial Off The Shelf : COTS), afin d'éviter de coûteux développements spécifiques. Or, les principes de démonstration de l'intégrité de sécurité des COTS sont peu ou pas définis. L'accès aux données qui permettrait leur analyse est difficile, voire impossible. Il n'en demeure pas moins que comme le montrent clairement les analyses de nombreux accidents ou incidents survenus sur les réseaux ferroviaires, bien que l'origine d'un accident ne soit par définition jamais liée à l'ATS, une bonne décision prise par un opérateur de supervision bien informé aurait pu dans bien des cas contribuer à réduire considérablement la gravité des conséquences par une gestion adaptée de la situation de crise. Cela est notamment le cas pour des scénarios résiduels qui ne peuvent être couverts que par procédure, nécessitant donc une intervention humaine par une personne supposée correctement informée sur l'état du système grâce aux données fournies par l'ATS. Ces scénarios concernent seulement des modes d'exploitation manuelle, dégradée ou en maintenance. C'est aussi dans ces circonstances que se produisent le plus d'accidents. D'une manière générale, plus le mode d'exploitation est dégradé, plus le rôle de l'ATS en sécurité est important. Citons quelques exemples :

– interventions des équipes de maintenance sur les voies ou les équipements de voie : Afin de les protéger du trafic ferroviaire et en fonction de la zone à protéger, les agents circulations (opérateurs de l'ATS) doivent émettre vers les enclenchements des ordres de verrouillage de signaux en position fermée, de verrouillage d'aiguilles dans une position précise, d'interdiction de tracé d'itinéraires, et vers l'ATP des ordres de réduction de vitesse sur les voies adjacentes. Ces opérations de restriction aussi bien que les opérations de levée de restriction requièrent un niveau de sécurité très élevé atteint grâce à des protocoles stricts de passage d'ordres vers les enclenchements et à des vérifications de leur bonne exécution par l'opérateur ATS. Dans de tels cas, l'ergonomie des passages d'ordre et la qualité des informations à vérifier par l'opérateur ATS sont donc essentielles ;
– manœuvres de trains en mode manuel, non protégés par les enclenchements ou l'ATP, en exploitation normale (attelage et dételage de trains en unité multiple, circulation sur les mêmes circuits de voie), en exploitation dégradée (équipements de voie en panne, ou encore après non-respect d'un signal de protection - ce qui fut la cause d'un accident au Brésil) ou en situation de secours (train en panne avec passagers à bord) : Ces manœuvres sont supervisées par les opérateurs ATS qui doivent connaître en permanence la position de tous les trains circulant dans la zone concernée. Des dialogues avec les conducteurs de train permettent de confirmer les informations présentées aux opérateurs ATS, qui sont par nature dégradées et doivent cependant rester pertinentes par rapport à ces situations ;
– situation d'urgence, nécessitant l'arrêt et l'évacuation d'un train (incendie à bord ou en châssis par exemple), ainsi que l'arrêt ou l'éloignement des autres trains proches du train en situation d'urgence : Les opérateurs ATS doivent prendre les décisions appropriées permettant de réduire les conséquences de la situation d'urgence à partir des informations présentées par l'ATS. On peut citer comme situation d'urgence extrême la perte du système de freinage d'urgence du train de banlieue ayant conduit à l'accident de la Gare de Lyon en 1988 [**16, 46**]. C'est en pareilles circonstances que de bonnes décisions prises par des régulateurs ayant les bonnes informations sont déterminantes pour éviter des scénarios catastrophiques, même s'il s'agit bien en l'espèce de l'ultime rempart.

Ces quelques exemples montrent clairement que bien qu'usuellement considéré comme non sécuritaire (la sécurité reposant donc sur les fonctions de l'ATP et les enclenchements), l'ATS n'en demeure pas moins le point névralgique de l'exploitation d'une ligne, celui où les décisions clés sont prises par des opérateurs humains, compte tenu des informations fournies par le système.

Le contexte actuel, sous-tendu par le légitime souci de rentabilité des infrastructures compte tenu de la concurrence du transport routier (qu'il s'agisse d'ailleurs de transport de passagers ou de fret), amène généralement à exploiter les lignes au maximum de leur capacité (au moins dans certaines plages horaires) ce qui a pour conséquence une gestion à flux tendu, nécessitant lorsqu'une intervention d'un opérateur est requise, des délais très courts. De plus l'opérateur humain, s'accoutumant à l'automatisation de certaines tâches qui lui revenaient dans un passé encore récent, est très peu entraîné à agir dans les cas où ces aides ne sont pas disponibles, cas qui sont précisément des situations de crise. Il en résulte au mieux un délai nettement accru avant réaction appropriée, effet qui s'additionne à l'augmentation de trafic mentionnée ci-avant. Dans les pires cas, compte tenu de plus du fait que les consignes n'envisagent généralement pas de manière aussi poussée les scénarios où l'information sur l'état du système est indisponible ou très dégradée, des actions totalement inadaptées de l'opérateur humain (de nature à empirer la situation plus qu'à l'améliorer) peuvent être observées. L'analyse de tels scénarios montre

souvent que l'opérateur, faute d'information complète et fiable sur l'état du système, se forge dans l'urgence un schéma mental cohérent mais erroné sur lequel il base ses décisions, la tension liée à la crise lui faisant passer outre à la recherche d'autres schémas compatibles avec l'information disponible.

2.7. Harmonisation des systèmes européens

En 1994 la commission européenne a lancé un programme visant à relier les grandes villes européennes par des lignes à grandes vitesses [**4**]. Ce projet est d'une difficulté sans précédent, en effet, le rail européen à grande vitesse est une mosaïque de réseaux nationaux qui s'ignorent. Outre l'épineux problème des travaux, la création de liaisons transfrontalières à grandes vitesses rencontre des difficultés de génie civil en raison des obstacles naturels aux frontières (La liaison Lyon - Turin nécessite le creusement d'un tunnel de 53km de long, la liaison Perpignan - Figueras demande le percement d'un tunnel de 8km enfin la liaison Paris - Londres a nécessité la construction du tunnel sous la Manche). Toutefois, une difficulté plus grande doit être surmontée : l'harmonisation des systèmes ferroviaires existants. [**131**] est un travail particulièrement intéressant sur ce sujet, cet article propose un historique des différents systèmes ferroviaires (détection des trains, signalisation, systèmes de freinage, etc.). Au travers de cette vue d'ensemble, il est facile de s'apercevoir des difficultés techniques qu'il faut résoudre pour adapter les réseaux entre eux.

Les problèmes majeurs d'un tel projet sont les suivants (d'après les propos recueillis par Science & Vie de Christophe Cicard, adjoint du chargé des équipements ferroviaires sur la ligne TGV-Est, Science & Vie num. 1079, août 2007) :

– A grande vitesse, le changement de conducteur aux frontières n'est pas rentable (perte de temps), les conducteurs doivent donc pouvoir communiquer avec tous les acteurs circulations et comprendre la signalisation des pays traversés. L'Union Européenne compte 23 systèmes de signalisation différents et presque tous incompatibles. En conséquence, le Thalys doit embarquer sept systèmes de signalisation différents, ce qui augmente les coûts et complexifie les études de sûreté de fonctionnement.
– Les rames de conception différentes (TGV ALSTOM, AVE ALSTOM, ICE Siemens, Eurostar ALSTOM, Thalys ALSTOM) doivent être adaptées aux différentes lignes empruntées. Par exemple, l'Eurostar dispose d'un gabarit plus étroit que toutes les autres rames pour passer le tunnel sous la manche. En Angleterre, certaines zones ne peuvent accueillir les caténaires, en conséquence l'Eurostar est équipé d'un frotteur permettant de capter le courant sur un troisième rail au sol. Autre exemple d'adaptation complexe, l'ICE Allemand qui doit emprunter la LGV-Est a un système de freinage magnétique différent de celui du TGV-Est, or le champ magnétique perturbe le fonctionnement des capteurs de grippage des roues (détection des boîtes chaudes) et est capable d'aimanter des éléments métalliques de certains appareils de voie.

Le projet d'harmonisation des systèmes ferroviaires à grande vitesse passe donc par le développement impératif d'un système de signalisation commun Européen. Les vitesses élevées et la diversité des signalisations européennes imposent une signalisation embarquée dans le train afin de permettre au conducteur de lire les signaux mais aussi d'optimiser la cinématique du

train (courbe de freinage notamment) afin de réduire l'espacement minimal entre deux trains et ainsi augmenter le taux de fréquentation des voies.

L'Union Européenne consciente de ce besoin, a lancé dès 1989 un projet de standardisation : le système européen de gestion du trafic ferroviaire (ERTMS, *European Railway Transportation and Management System*). La première version d'ERTMS a été finalisée en 2002. Ce système est maintenant obligatoire sur toutes nouvelles lignes reliant au moins deux pays de l'Union. ERTMS est un ensemble de spécifications techniques dont il est explicitement demandé de démontrer la conformité pour la mise en place des nouveaux systèmes. Cette conformité sera attestée au travers de certificats de conformité. Les innovations apportées par ERTMS résident dans la généralisation et l'harmonisation de la signalisation en cabine (répétée ou non sur la voie), l'introduction de nouvelles informations telles que le changement de pays. ERTMS propose égalment de nouvelles fonctions comme le contrôle automatique des vitesses.

Grâce à ERTMS, le système de transport va devenir Européen, le nombre de trains et le nombre de types de train vont être augmentés. De nouveaux défis devront être relevés, tel que la langue utilisée pour les communications entre acteurs de nationalités différentes ainsi que l'harmonisation de la réglementation.

2.8. Effets de la centralisation de la commande ferroviaire

2.8.1. L'aspect fonctionnel de la centralisation. — L'impact de la centralisation des postes de trafic ferroviaires s'observe sur les composantes technologiques, humaines et organisationnelles.

La centralisation a été permise grâce à l'informatisation des composants techniques. L'informatisation modifie profondément les techniques de conception des systèmes ainsi que leurs évaluations pour la sécurité. Cette révolution technologique permet également, grâce à la miniaturisation des automates et à la capacité des réseaux d'informations d'intégrer des postes couvrant des lignes ferroviaires plus importantes (distance, interconnexions, bifurcations), il est maintenant possible de centraliser la commande ferroviaire de la totalité d'un réseau national.

Du point de vue de l'opérateur humain, la centralisation du poste a un effet important sur la nature des communications, son activité et les relations humaines. Autrefois restreints à une portion de voie, les postes ferroviaires ont été sous le contrôle d'opérateurs connaissant par cœur le terrain dont ils avaient la responsabilité. Que ce soit par formation, ou bien pour avoir exercé la fonction d'agent à pied d'œuvre, l'opérateur pouvait facilement se représenter mentalement la géographie, la topographie ainsi que toutes les particularités du terrain. Avec la centralisation des postes et l'élargissement des zones contrôlées, il est impossible de former ou de recruter un agent connaissant l'ensemble du réseau.

L'intégration d'automatismes et de systèmes d'informations modifie profondément les métiers du poste ferroviaire. Les postes ferroviaires de générations précédentes nécessitent l'activité de deux métiers qui se partageaient la tâche : l'agent régulateur et l'agent aiguilleur (agent circulation), l'un se chargeant de l'état du trafic et l'autre des directions des trains et des procédures de sécurité.

Au niveau de l'organisation, la centralisation offre de nombreux bénéfices économiques d'abord (réduction de personnel) mais aussi en termes de performance (chaîne de commandement directe sur le trafic, vue globale, centralisation des informations pour les décideurs). Une

organisation centralisée offre l'avantage aux décideurs d'avoir une vue de l'ensemble du réseau à un instant donné.

L'objectif de l'automatisation de la gestion du trafic est une utilisation optimale des voies afin de faire circuler davantage de trains par unité de temps tout en assurant la sécurité [**89**].

Comprendre les habiletés et l'expertise des opérateurs est une nécessité pour réussir l'implémentation des nouveaux systèmes de gestion de trafic et réussir cette collaboration entre l'humain et la machine [**90, 89, 29, 137**].

2.8.2. Conséquences pour la sécurité. — Les fonctions de l'opérateur se limitent à surveiller tous changements anormaux de la situation sur le réseau. Lorsqu'il doit reprendre le contrôle des opérations, l'opérateur ne dispose pratiquement plus d'action directe sur les installations, toutes les commandes sur l'installation sont transmises aux automatismes et filtrées par les barrières de sécurité. Il demeure cependant, et il demeurera toujours des cas où l'opérateur agit directement sur l'installation en contournant les systèmes de protection physiques par l'application de procédures de sécurité. L'installation passe d'un système de protection physique complètement autonome à un système de protection informationnel contrôlé par la performance d'un ou plusieurs opérateurs. Citons quelques exemples de commande directe sur l'installation :

- Mise en place et suppression de restriction de vitesse ;
- Mise en place et suppression de protection de travaux ;
- Blocage et déblocage d'aiguille ;
- Blocage et déblocage d'itinéraire ;
- Blocage de tous les signaux en position fermée ;
- Déblocage de tous les signaux.

Ces cas pratiques reposent sur une procédure informationnelle prévue dans le système de supervision. L'opérateur est guidé dans sa démarche et soumis à des contrôles de l'information échangée avec les actionneurs. Par exemple, les systèmes ALSTOM prévoient pour ces commandes une procédure informatisée nommée HILC pour *High Integrity Level Control*. Cette procédure servira de cas d'étude pour l'application de la démarche proposée dans la thèse dans un chapitre ultérieur.

La procédure HILC est une séquence de communications sécurisées entre le poste informatique ATS et le système de protection. Un code de redondance cyclique CRC permet de protéger l'intégrité des échanges d'informations numériques entre les machines. Un mécanisme de double commande est demandé à l'opérateur pour s'affranchir des commandes non intentionnelles.

La présentation des effets de la centralisation de la commande ferroviaire a fait l'objet de deux communications [**21, 14**].

2.9. Conclusion

Ce chapitre a présenté le domaine des transports ferroviaires dans lequel s'inscrit la thèse. Les principes primordiaux de sécurité auxquels sont soumis les acteurs du système de transport ferroviaire ont été décrits. Les systèmes de transport ferroviaire vivent actuellement deux révolutions, l'une concerne l'intégration des nouvelles technologies de l'information et de la

communication et l'autre relève de l'harmonisation des différents systèmes européens. La thèse se focalise sur les changements de la tâche des acteurs circulation et notamment l'apparition d'un nouveau métier qui consiste à superviser le trafic à l'aide d'outil fortement automatisés. Cette nouvelle activité qu'effectue l'opérateur ATS, est basée sur le métier de l'agent circulation et intègre de nouvelles missions grâce à l'introduction des nouvelles technologies. Il s'agit alors d'étudier la relation du couple formé par le système ATS et l'opérateur humain afin de déterminer l'impact sur la sécurité. Le chapitre suivant présente le référentiel méthodologique actuel qui sert à évaluer la sécurité des grands systèmes complexes tels que celui du transport ferroviaire.

CHAPITRE 3

SÛRETÉ DE FONCTIONNEMENT

Résumé

Ce chapitre présente le cadre général de sûreté de fonctionnement dans lequel se place la thèse. Née du besoin de maîtriser les risques industriels, la sûreté de fonctionnement est une approche interdisciplinaire de l'activité industrielle. On distinguera les risques associés aux matériels de ceux des logiciels et encore de ceux provenant de l'humain. Cette distinction s'explique par les différences de complexité de fonctionnement de ces trois composantes. La notion de système complexe offre un cadre de description des systèmes en vue de l'accomplissement de la sûreté de fonctionnement. Les concepts et méthodes classiques de sûreté de fonctionnement sont présentés ainsi que l'évolution des modèles sous-jacents qui permettent d'évaluer des systèmes de plus en plus complexes et intégrant le facteur humain.

3.1. Introduction

Les risques industriels ont évolué avec les technologies et les besoins des sociétés. La révolution industrielle a apporté son lot de risques dont la portée dépasse la dimension d'un seul homme. Autrefois, les sociétés, les individus et leurs ressources étaient soumis à des dangers de type naturel (sismiques, climatiques, épidémiques), humains (guerres, incendie, etc.). La révolution industrielle au dix-huitième siècle a introduit dans nos sociétés une nouvelle forme de danger provoquée par l'homme. Cette révolution a donné le jour à des machines dont la capacité à produire fut décuplée par rapport à la capacité de production d'un travailleur. Ceci nécessite une quantité considérable d'énergie qui lorsqu'elle n'est plus maîtrisée peut s'avérer très dangereuse.

La maîtrise de ces énergies relève de la sûreté de fonctionnement des systèmes technologiques qui les contrôlent. La définition de technologie qui sera retenue dans ce mémoire est la suivante :

Définition 3.1 **(Technologie)**. — Ensemble de savoirs, de procédés et d'outils qui mettent en œuvre les découvertes et les applications scientifiques les plus récentes (dans un domaine particulier) (anglicisme). Dictionnaire Encarta.

Le développement croissant et rapide de nouvelles technologies après la Deuxième Guerre mondiale marque le départ d'une course effrénée entre développement et assimilation – compréhension des systèmes industriels. La quantité et la complexité de ces nouvelles technologies

permettent d'accéder à de meilleurs objectifs de performance des systèmes, à un niveau de confort plus élevé et à un niveau de contrôle des systèmes plus poussé. La contrepartie de ces avancées (nécessaires) demeure la difficulté de maîtriser convenablement les lois de fonctionnement et l'utilisation de ces technologies.

Bien que les systèmes soient testés dans la majeure partie des cas d'utilisation, il subsiste inévitablement des incertitudes sur le fonctionnement en condition réelle :

- cas d'utilisation non identifiée ;
- défauts de conception ;
- environnement naturel (incertitude naturelle).

Les effets non souhaités sont susceptibles d'engendrer des pertes et/ou des dommages pour la société. Le propre de chaque nouvelle découverte fait que le nombre de composants des systèmes s'accroit (complication des systèmes) de même que leurs interrelations (la complexification des systèmes). La complication a atteint un niveau tel que la seule formulation de toutes les possibilités d'usage et de fonctionnement devient illusoire et rend donc le test exhaustif impossible (sans compter la variabilité de l'environnement extérieur).

L'avènement des grands systèmes industriels, caractérisés par l'intégration de plusieurs technologies couplées, voire entrelacées, ne contribue pas à simplifier les choses. Ainsi imbriquées les technologies sont devenues indispensable les unes aux autres. Pour répondre à l'incertitude issue des défauts des systèmes modernes, les ingénieurs ont développé un arsenal méthodologique basé sur un modèle de représentation du fonctionnement. Ces méthodes proviennent d'études pragmatiques sur des systèmes réels (souvent déjà en service au moment de l'étude) permettant de comprendre et d'analyser les causes et les effets des inévitables défauts afin d'en éviter les effets indésirables. L'intérêt grandissant pour l'étude des dysfonctionnements d'un système et de l'impact sur son environnement repose sur des raisons diverses : économiques, sociales, de sécurité, de santé, etc.

Devenue discipline, que ce soit sous la dénomination de « fiabilité », « maintenabilité », « disponibilité », ou « sécurité » la sûreté de fonctionnement est maintenant indispensable à la conception et au maintien en conditions opérationnelles des systèmes industriels. Ce n'est qu'au début des années 1990 que la dénomination « sûreté de fonctionnement » voit le jour. Cette nouvelle appellation révèle l'engouement nouveau de la société pour les études de risques auxquels elle est parfois confrontée (Accidents de transports, accidents industriels chimiques ou nucléaires, etc.). Toutefois, les grandes industries (présentant des risques majeurs) disposaient déjà de services d'études relatifs à la sûreté de fonctionnement, la nouveauté intervient dans la démocratisation de cette activité pour les petites et moyennes entreprises qui jusque-là étaient les parents pauvres en matière de gestion des risques et pourtant pas moins consommateurs de nouvelles technologies et de matières dangereuses.

La suite de ce chapitre présente cette discipline et plus particulièrement la sûreté de fonctionnement relative aux facteurs humains dans les systèmes complexes. La sûreté de fonctionnement ne s'applique pas de la même façon sur un système simple que sur un système complexe. En effet, les limites des connaissances sur le fonctionnement ne sont pas les mêmes. Aussi, une typologie des systèmes industriels rencontrés en sûreté de fonctionnement est nécessaire, elle permettra de positionner la problématique de la thèse.

3.1.1. Systèmes compliqués et systèmes complexes. — La compréhension du fonctionnement repose sur un modèle de représentation des systèmes. Dans le langage courant et notamment en sûreté de fonctionnement, le terme système est généralement employé sans réelle définition pour représenter l'ensemble des composants organisés en sous-systèmes et délimitant le domaine de l'étude. L'approche « systémique » [**133, 86**] offre un cadre scientifique rigoureux dans lequel est défini le concept de système.

***Définition 3.2* (Système).** — La définition retenue pour la thèse est celle de Joël de Rosnay [**40**] : « Un système est un ensemble d'éléments en interaction dynamique, organisés en fonction d'un but ».

Le système est identifiable par des repères tels que :
- sa frontière avec l'environnement extérieur ;
- ses composants (les éléments qu'il contient) ;
- les liaisons qui relient ses éléments entre eux (interactions).

La nature des éléments peut être abstraite ou bien concrète. Un élément concret est soit un système vivant soit un composant purement matériel, généralement des outils, des moyens de communication ou encore des moyens de stockage de matière, d'énergie ou d'information. D'une manière générale, les éléments abstraits sont sources d'organisation du système : temps, connaissance, formation, procédure, cycle de travail en sont des représentants.

***Définition 3.3* (Systèmes sociotechniques).** — Il est possible de classer les différents systèmes que l'on peut rencontrer en sûreté de fonctionnement de la façon suivante (cf. figure 3.1) :
- Les *systèmes techniques* formés d'éléments abstraits et concrets non vivants, les interactions entre éléments font évoluer le système selon des lois physiques ;
- Les *systèmes vivants* dont la dynamique est régie par la psychologie ;
- Les *systèmes sociaux* formés d'éléments vivants et abstraits dont l'évolution est caractérisée par une organisation ;
- Les *systèmes sociotechniques* constitués d'éléments techniques, psychologiques et sociaux.

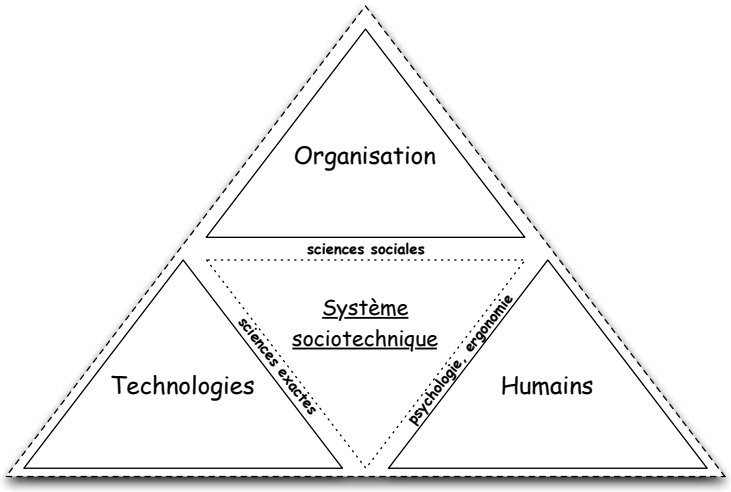


FIGURE 3.1. Systèmes sociotechniques

[**87**] propose une distinction entre un système compliqué et un système complexe sur la base de leur intelligibilité. La simplification d'un système compliqué suffit à découvrir son intelligibilité (explication) alors qu'il est nécessaire de recourir à la modélisation pour un système complexe afin de construire son intelligibilité (compréhension).

Dans le cadre de l'analyse de sûreté de fonctionnement de système industriel, nous opterons pour une définition de la complexité basée sur l'idée d'un niveau de maîtrise du fonctionnement du système au-delà duquel les techniques visant à simplifier et à classer les modes de fonctionnement deviennent insuffisantes.

***Définition 3.4* (Système compliqué)**. — Système qui comporte un nombre de composants suffisamment important pour que cela devienne une difficulté lors de l'étude de son intelligibilité.

Cette définition repose sur la propriété de combinatoire des systèmes et est compatible avec la définition basée sur l'idée de simplification.

La propriété d'un système d'être compliqué ne suffit pas à expliquer la difficulté de la maîtrise du fonctionnement des systèmes.

***Définition 3.5* (Système complexe)**. — Système dont les composants, même les plus élémentaires, ainsi que leurs multiples interactions, rendent difficile leur maîtrise au niveau technique.

La complexité selon cette définition relève de la difficulté de traiter l'analyse de fonctionnement, difficulté qui est expliquée par la nature et le nombre de ses composants et de leurs interactions. Ajoutons à cette définition la présence de comportements émergents qui dépassent le cadre des relations de cause à effet. Ces comportements sont liés à la difficulté d'appréhender les multiples interactions présentes dans le système ainsi que la présence de boucles de rétroactions caractéristiques des effets ayant un impact sur leur propre cause. L'étude de ces systèmes complexes fait l'objet d'études spécifiques et dispose même d'un institut de recherche dédié : « l'Institut de Santa Fe (Santa Fe Institute ou SFI [1]). »

La science de la complexité décrit l'évolution des systèmes complexes en termes d'autonomie, d'interaction et de co-évolution.

La complexité d'un système est une caractéristique qui dépend du niveau d'abstraction que l'on se donne. Vue de l'intérieur d'un système, dans le sens large du terme, la complexité correspond à une mesure du nombre de parties, du nombre et de la nature de leurs interactions. La cardinalité du système ne suffit pas à créer un système complexe. Un système disposant d'un nombre infini de parties n'est pas forcément complexe. Prenons le cas d'un système constitué d'une infinité de composants identiques (l'infinité bien que conceptuelle s'avère une approximation acceptable dans le cas de renouvellement de composants par exemple), la connaissance d'un seul composant et de ses relations avec ses semblables permet de maîtriser le système.

Il ne faut pas confondre la complexité du système avec la complexité de la démonstration de sûreté de fonctionnement. Un système de prime abord simple (quelques composants indépendants) peut s'avérer très complexe selon le niveau de détail nécessaire à la démonstration de

1. `http://www.santafe.edu/`

sûreté de fonctionnement, par exemple, si la confiance dans les services attendus est justifiée par des propriétés physiques subatomiques des composants.

3.2. Théorie de la sûreté de fonctionnement

3.2.1. Modèle de fonctionnement. — L'étude du fonctionnement des systèmes complexes repose sur un modèle de fonctionnement du système et de ses composants représenté par un espace d'états. Un état dans cet espace permet d'indiquer le comportement du système ou de l'élément du système. On note E l'espace d'état du système et E_i l'espace d'état de l'élément i du système. On appelle *fonction de structure* du système l'application qui relie l'ensemble des espaces d'états des éléments du système à l'espace d'état du système. On note ϕ cette application. Dans un système comptant n éléments on a :

$$\phi : E_1 \times \cdots \times E_n \to E \tag{1}$$

La fonction de structure permet de modéliser les interactions entre les éléments du système et leurs impacts sur l'état du système.

On appelle *système binaire* un système dont les espaces d'états ne contiennent que deux valeurs possible : $E = E_i = \{0,1\}$. Par convention, on note :

$$e \in E, e = \begin{cases} 1 : & \text{l'état de bon fonctionnement} \\ 0 : & \text{l'état de panne} \end{cases}$$

Chaque composant i du système est modélisé par une variable booléenne x_i. L'état de tous les composants du système est donné par le vecteur d'état $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Enfin l'état du système est calculé à l'aide de la fonction de structure appliquée au vecteur d'état $\phi(\mathbf{x})$. Dans le cas de systèmes binaires, la fonction de structure est une forme vectorielle booléenne. La donnée de sa formule booléenne la définit complètement.

Les systèmes binaires constituent le paradigme essentiel de la théorie de la fiabilité des systèmes [**92**].

Avec ce formalisme, il est possible de représenter des structures élémentaires qui sont largement employées en fiabilité des systèmes. Ce sont les structures série et parallèle dont la généralisation est la structure k/n. Tout système dont la structure peut être décomposée en systèmes k/n est dit élémentaire, dans le cas contraire le système sera dit à structure complexe. La fonction de structure d'un système élémentaire est obtenue directement en utilisant les fonctions de structures des formes usuelles : série, parallèle et k/n.

3.2.1.1. Système série. — Un système est dit en série si son fonctionnement nécessite le fonctionnement simultané de tous ses composants. La panne d'un seul composant entraîne la panne du système. La fonction de structure d'un tel système est donnée par :

$$\phi(\mathbf{x}) = \min(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i$$

3.2.1.2. Système parallèle. — Le fonctionnement d'un tel système est assuré dès lors qu'un seul de ses composants fonctionne. Le système est en panne si et seulement si tous ses composants sont en panne. Sa fonction de structure est la suivante :

$$\phi(\mathbf{x}) = \max(x_1, \ldots, x_n) = 1 - \prod_{i=1}^{n} (1 - x_i)$$

3.2.1.3. Système k/n. — Le fonctionnement du système dépend du nombre de composants en fonctionnement. Si au moins k composants sur n avec $1 \leq k \leq n$ sont en bon état de marche alors le système est en fonctionnement. Le système sera en panne si $n - k + 1$ composants ou plus sont en panne simultanément. Sa fonction de structure est donnée par :

$$\phi(\mathbf{x}) = \begin{cases} 1 & \text{si } \sum_{i=1}^{n} x_i \geq k \\ 0 & \text{sinon} \end{cases}$$

3.2.1.4. Structure complexe. — Un système qui ne peut pas être décomposé en modules des structures élémentaires précédentes est un système à structure complexe. Leur étude nécessite l'introduction de la notion de coupe et de chemin de la fonction de structure.

Un *chemin* est un sous-ensemble de composants dont le bon fonctionnement simultané assure le bon fonctionnement du système quelque soit l'état des autres composants.

Une *coupe* est un sous-ensemble de composants dont le dysfonctionnement simultané entraîne le dysfonctionnement du système quelque soit l'état des autres composants.

La coupe (resp. le chemin) est *minimale* si la coupe (resp. le chemin) ne contient pas d'autre coupe (resp. chemin) ;

Le système initial est équivalent au système formé par ses coupes minimales (resp. chemins minimaux) en série (resp. en parallèle), où chaque coupe (resp. chemin) est représentée par un système parallèle (resp. série) ayant pour composants les composants de la coupe [**92, 30**].

3.2.1.5. Limites. — Toutefois, avec la complexité croissante des systèmes, cette modélisation devient trop réductrice. Tous les composants ne peuvent se réduire à un modèle de fonctionnement de type interrupteur. Le fonctionnement des systèmes nécessite d'être nuancé. Les systèmes sociotechniques par exemple sont caractérisés par un niveau de performance qui ne peut se réduire à deux états de fonctionnement.

Par opposition au caractère binaire, il est possible d'élargir le domaine de définition de la fonction de structure du système, on parle alors de systèmes *multi-performants*. Il existe deux cas de systèmes multi-performants :

- E est continu, ex : $E = [0, 1]$;
- E est discret, ex : $E = \{e_0, e_1, \ldots, e_n\}$.

Une autre voie d'étude consiste à représenter l'espace d'état par un nombre flou, ce thème permet en outre d'obtenir des résultats sur l'incertitude du modèle, Kim et Bishu [**77**] présentent un état de l'art de ces méthodes appliquées à la modélisation de la fiabilité humaine.

3.2.2. Entrave au fonctionnement. — Le passage d'un mode de fonctionnement à un mode de dysfonctionnement s'explique à l'aide du modèle d'entraves à la sûreté de fonctionnement[**82**]. Ces entraves, appelées défaillances, peuvent être introduites dès la phase de conception du système voire même lors de l'expression du besoin. Un modèle descriptif de cette notion d'entrave à la sûreté de fonctionnement permet de qualifier l'introduction, l'activation et l'expression des défaillances.

***Définition 3.6* (Défaillances [129]).** — Une défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise

La *faute* est associée à l'introduction de l'entrave. L'*erreur* constitue l'activation. L'expression de l'erreur sur les missions du système est une *défaillance*.

Ce modèle rend plus explicite la description de phénomènes inattendus dans le système. A titre d'exemple, la défaillance de la première mission d'Ariane V relève d'une erreur d'interprétation de calcul introduite par une faute liée à réutilisation d'un module de traitement de l'information analogique conçu pour Ariane IV, alors que l'interpréteur Ariane V était conçu pour recevoir des informations numériques (voir le rapport d'enquête [**2**]).

Un indicateur permet de calculer la quantité instantanée de défaillance d'un système. Il s'agit du taux de défaillance défini de la façon suivante :

***Définition 3.7* (Taux de défaillance).** — Le taux de défaillance est égal à la limite, lorsque δt tend vers 0, de la probabilité de défaillance conditionnelle du système sur un intervalle de temps infinitésimal $[t, t + \delta t]$ sachant que le système n'a pas connu de défaillance avant t et divisée par δt. On note $\lambda(t)$ ce nombre. Il s'exprime en défaillances par heures.

Le taux de défaillance est calculé sur la base du retour d'expérience. Statistiquement, il s'interprète comme étant le rapport de défaillance par unité de temps à la date t. Supposons que le système comporte N composants tous en bon état à t. On observe à la date t le nombre de composants encore en fonctionnement. Alors :

$$\lambda(t) = \lim_{\epsilon \to 0} \frac{\text{nb. de composants tombés en panne entre } t \text{ et } t + \delta t}{\epsilon \times N}$$

Les défaillances peuvent être aléatoires ou systématiques [**31**]. La défaillance aléatoire survient de manière non prévisible. Elle peut être causée par un phénomène naturel non maîtrisable, par l'usure (vieillissement) du système, ou encore par la variabilité intrinsèque de la performance du système. La défaillance aléatoire peut être évaluée à l'aide du retour d'expérience et des études sur l'usure ou sur la variabilité de la performance.

La défaillance systématique est un défaut présent dans le système mais latent, c'est-à-dire qui sera activé par un ensemble de conditions tel que l'utilisation d'une fonction particulière par exemple. La faute a été introduite lors de la réalisation (conception, vérifications, maintenance, etc.) du système et ne sera donc éliminée que par une reprise du processus de réalisation. La défaillance systématique n'est pas quantifiable sur le système en exécution, mais peut être évaluée en réalisant une étude approfondie du processus de réalisation.

3.2.3. Évaluation de la sûreté de fonctionnement. — La maîtrise des risques industriels repose sur la connaissance du fonctionnement du système, et de la capacité à le tester **complètement**.

La définition de sûreté de fonctionnement qui a été retenue par la communauté scientifique est celle citée dans [**129, 81, 93**] :

***Définition 3.8* (Sûreté de fonctionnement)**. — La sûreté de fonctionnement (SdF) d'un système est la propriété qui permet de placer une confiance justifiée dans les services attendus de ce système.

La sûreté de fonctionnement est aussi, aujourd'hui, un ensemble de méthodes structurées permettant d'évaluer et d'améliorer cette propriété. Ces méthodes sont maintenant indispensables pour la conception et l'exploitation de systèmes de plus en plus compliqués et complexes.

La sûreté de fonctionnement consiste à rechercher les défaillances potentielles, d'en réduire le nombre et leurs conséquences sur le système. La notion de confiance introduite dans la définition de sûreté de fonctionnement est nécessaire dans la mesure où l'objectif de suppression totale et définitive des défaillances est inaccessible. Une courte explication de cette inaccessibilité se trouve dans l'incapacité de maîtriser les phénomènes naturels. Une autre voie pour comprendre cette inaccessibilité apparaît lors de l'application de modèle faute, erreur, défaillance. En effet, il n'est pas toujours possible de remonter aux causes profondes des défaillances. Ainsi, lorsque l'analyse atteint les limites de la connaissance des phénomènes, la faute ne peut être attribuée qu'à une erreur inexpliquée. Il s'agit alors de prévoir et de contenir les conséquences de ces fautes.

Les industries ne sont pas égales devant les dangers, celles confrontées à des dangers majeurs ne peuvent se soustraire à une démonstration étayée de la maîtrise de la sûreté de fonctionnement, et sont généralement soumises à une autorité de tutelle stricte. Il s'agit de prouver le bon fonctionnement du système, sa capacité de défense face aux risques mais aussi de prévoir les performances de sûreté de fonctionnement compte tenu des limites de l'analyse et des moyens palliatifs.

La première preuve est déterministe, on parle de fiabilité *mécanique*, le bon fonctionnement et la performance défensive sont généralement déterminés à partir des lois physiques ou comportementales des composants du système. Il s'agit d'évaluer le profil de mission du système puis de déterminer les efforts exceptionnels auxquels le système sera soumis (en nombre d'événements maximal par unité de temps) ainsi que l'usure normale ou fatigue du système (en nombre de cycles d'exécution sur la durée de vie du système). Enfin à partir de ces données et des lois de la physique, la modélisation numérique doit démontrer que les contraintes d'utilisation ne dépassent pas la limite d'« élasticité » du système. Ce calcul permet également de surdimensionner le système vis-à-vis des sollicitations exceptionnelles. Il s'agit de surdimensionner le système d'un facteur $k > 1$ par rapport à la dimension limite de tenue aux sollicitations extérieures.

La prévision de sûreté de fonctionnement est quant à elle probabiliste, l'évaluation passe par le calcul d'indicateurs de sûreté de fonctionnement, appelés aussi attributs de la sûreté de fonctionnement : la fiabilité, la maintenabilité, la disponibilité et la sécurité.

Définition 3.9 **(Fiabilité,** [**30, 129**]**).** — La fiabilité d'un système porte sur son aptitude à accomplir sa mission, dans des conditions données de fonctionnement et pour une durée donnée de fonctionnement.

Mathématiquement, la fiabilité est mesurée par la probabilité que le système accomplisse sa mission, dans les conditions données, pendant l'intervalle de temps $[0, t]$ et on note cette probabilité :

$$R(t) = \mathbb{P}\left(\text{Système non défaillant sur } [0, t]\right) \tag{2}$$

Cette définition nécessite un support explicatif de la logique de fonctionnement du système (*i.e.* Quand ne remplit-il pas sa mission ?) La fonction de structure présentée précédemment, fournit un tel support. L'attitude générale consiste alors à utiliser la stratégie de l'antique Sénat Romain « *Divide et impera* ». La stratégie réductionniste permet de décomposer le système en entités plus simples dont le fonctionnement peut être modélisé par une variable booléenne. Cette stratégie fonctionne tant qu'il est possible d'atteindre un niveau de décomposition où toutes les entités sont binaires et tant qu'il est possible de reconstituer la logique de fonctionnement du système global par des opérations logiques sur les états des entités de bases.

Le calcul de la fiabilité du système s'effectue en évaluant la fiabilité de chacun de ses composants, en établissant la fonction de structure du système et en calculant la probabilité :

$$R(t) = \mathbb{P}(\phi(\mathbf{x}) = 1, \text{ sur } [0, t]) \tag{3}$$

L'approche réductionniste en vigueur dans la majeure partie des analyses de fiabilité de systèmes matériels est une approximation qui a fait ses preuves. Toutefois, cette stratégie atteint ses limites lorsque le système comprend des composants compliqués et/ou complexes dont le dysfonctionnement (au sens strict : la mission n'est pas *complètement* remplie) ne suffit pas à expliquer un dysfonctionnement à un niveau plus élevé. Les composants logiciels et la dimension humaine des systèmes rentrent pleinement dans ce cadre.

Définition 3.10 **(Maintenabilité,** [**129**]**).** — La maintenabilité du système représente son aptitude à être rétabli dans un état de fonctionnement qui lui permet d'accomplir sa mission, dans des conditions données de fonctionnement avec des procédures et des moyens prescrits.

Mathématiquement, la maintenabilité est mesurée par la probabilité que la maintenance soit accomplie dans des conditions données avec des procédures et des moyens prescrits à la date t.

On note :

$$M(t) = \mathbb{P}\left(\text{la maintenance est achevée au temps } t\right) \tag{4}$$

Cet attribut ne concerne que les systèmes réparables.

Définition 3.11 **(Disponibilité,** [**129**]**).** — La disponibilité du système mesure son aptitude à être en état d'accomplir sa mission dans des conditions données de fonctionnement à un instant donné.

Mathématiquement, la disponibilité est mesurée par la probabilité que le système soit en état d'accomplir une fonction requise dans des conditions données et à un instant t donné :

On note :

$$A(t) = \mathbb{P}\,(\text{Système non défaillant à l'instant } t) \tag{5}$$

La sécurité, thème principal de ce mémoire revêt une définition particulière. Sa relation à la sûreté de fonctionnement n'est pas exactement la même que celle que peut avoir la fiabilité, la maintenabilité ou la disponibilité.

Définition 3.12 **(Sécurité,** [**129**]**).** — La sécurité est l'aptitude du système considéré à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Lorsqu'elle est quantifiée, la sécurité est généralement mesurée par la probabilité que le système évite de faire apparaître, dans des conditions données, de tels événements.

L'aptitude contraire est appelée « insécurité ».

Toujours selon [**129**], la sécurité est généralement employée de façon subjective, et la prise de décisions relatives à la sécurité des systèmes nécessite le développement de méthodologies de quantification du risque, on parle alors de sécurité probabiliste. La sécurité probabiliste consiste à démontrer *a priori* que la probabilité d'apparition d'une situation dangereuse est inférieure à un seuil défini à l'avance. Poussée à son paroxysme, cette notion implique d'imaginer un système dont le seuil de sécurité probabiliste doit être nul (le risque zéro). Bien que le risque zéro n'existe pas (à cause des défaillances aléatoires de cause naturelle par exemple) cette question permet de définir la notion de sécurité intrinsèque d'un système dès lors que l'assurance est faite que toute défaillance d'un ou plusieurs composants ne peut le faire passer que dans un état plus sécurisé que l'état dans lequel il se trouve au moment de la défaillance. La sécurité intrinsèque se base sur les propriétés physiques des composants, il faut donc connaître à la fois le comportement des composants en cas d'une ou plusieurs fautes ainsi que *toutes* les agressions que le système peut subir. Ceci impose d'une part de n'utiliser que des composants dont la complexité est maîtrisable et d'autre part à admettre que le risque nul n'existe pas.

3.3. Modèle d'accidents

3.3.1. Définitions. —

Définition 3.13 **(Accident – Domaine Ferroviaire** [**35**]**).** — Un accident est un événement ou une série d'événements inattendus conduisant au décès, à des blessures, à la perte d'un système ou d'un service, ou à des dommages sur l'environnement.

La notion d'accident se rapporte à celle d'événement inattendu. Les études de sécurité cherchent à maîtriser ces événements et définissent donc la notion d'événement indésirable ou redouté comme étant les événements qui ne doivent pas se produire ou avec une probabilité restreinte afin de contrôler l'apparition des accidents.

Du point de vue des sciences physiques, il est possible de représenter un accident par la libération non contrôlée d'énergie potentielle (mécanique, de pesanteur, chimique, thermique, électrique, *etc.*).

Une notion similaire à celle de l'accident qui est introduite dans de nombreuses publications et notamment dans les études de retour d'expérience est celle d'incident.

***Définition 3.14* (Incident).** — L'incident est un événement ou une série d'événements inattendus conduisant à des conséquences bénignes.

L'étude des incidents est souvent utilisée comme un indicateur du niveau de performance de la sécurité dans un système. L'analyse des incidents permet d'identifier de nouveaux scénarios accidentels en prolongeant les scénarios des incidents, par l'imagination, avec des contextes moins favorables ou des défaillances multiples.

Une autre notion très importante pour l'étude de la sécurité des systèmes est celle des quasi-accidents.

***Définition 3.15* (Quasi-accident ou presque accident).** — Il n'existe pas de définition normalisée de la notion de quasi-accident, toutefois, l'étude de la littérature converge vers la notion d'évitement de « justesse » des conséquences catastrophiques générées par un événement inattendu.

Par exemple, dans le domaine médical, Vincent et coll. [**130**] définissent le quasi-accident de la façon suivante : « Un quasi-accident est un accident qui a été évité de peu ».

Dans le domaine industriel, Van der Schaff [**114**] propose la définition suivante : « Toute situation au cours de laquelle une séquence d'événements en cours a été empêchée de se développer davantage, empêchant donc l'occurrence de conséquences potentiellement graves ».

Plus récemment, Le Coze et coll. [**85**] proposent une définition du quasi-accident en fonction du nombre de barrières de sécurité franchies, et ce dans le but de mettre en relation la notion de presque accident avec celle d'accident où toutes les barrières de sécurité ont été franchies. La notion de barrière sera présentée un peu plus loin.

Le quasi-accident suit, dans son déroulement, un scénario accidentel dont les conséquences ont pu être évitées. L'étude systématique des scénarios quasi-accidentels est primordiale pour l'élaboration du retour d'expérience, cela permet d'une part, d'obtenir des données sur le déroulement du scénario (état de l'installation avant l'événement, nature de l'événement indésirable, verbalisation des opérateurs, *etc.*), et d'autre part, de collecter les informations sur la réponse du système qui a permis d'éviter l'accident. L'objectif du retour d'expérience consiste à améliorer le système afin d'anticiper plus tôt les événements initiateurs et de mettre en place des mesures de protection plus efficaces appelées barrières de sécurité.

3.3.2. Les différents types de barrières. — La conception des systèmes nécessite la mise en place de barrières visant à éviter les accidents [**122**], quatre types de barrières sont envisagés dans la classification d'Hollnagel [**68**] :

– **Physique :** Ce type de barrière est constitué d'éléments physiques matériels empêchant la réalisation d'action ou d'événement. Ce type de barrière permet également de protéger le système contre les effets d'un événement inattendu par blocage ou dissipation de ces effets. Typiquement, ces barrières sont représentées par des murs, des portes, un guidage, *etc.* L'exemple le plus représentatif dans le domaine nucléaire est celui de l'enceinte de confinement du bâtiment réacteur protégeant l'environnement contre d'éventuelles fuites d'éléments radioactifs. D'un autre côté, l'enceinte de confinement protège également le réacteur d'événements inattendus provenant de l'extérieur du système comme des intempéries par exemple. Dans le domaine ferroviaire, le rail constitue la principale barrière physique qui permet de canaliser l'énergie de mouvement des trains.
– **Fonctionnelle :** Ce type de barrière contraint l'exécution d'une action ou d'un travail par l'entremise de verrouillage logique ou temporel. La barrière fonctionnelle contrôle l'application d'une ou plusieurs conditions préalables avant que l'action ou le travail puisse être exécuté. Ces conditions préalables peuvent être interprétées par un opérateur humain mais le plus souvent, elles sont contrôlées par des systèmes techniques qui offrent une plus grande fiabilité de contrôle et une disponibilité supérieure. L'exemple proposé par Hollnagel est celui d'une serrure nécessitant une clef ou d'un verrou numérique nécessitant un code secret. Dans le cas du transport ferroviaire, l'exemple le plus représentatif est donné par le système d'enclenchement d'itinéraire qui vérifie les conditions préalables d'autorisation de circulation sur l'itinéraire avant de pouvoir le tracer. Historiquement, cette barrière fonctionnelle a d'abord été exécutée par l'opérateur humain, sur le bord des voies, qui s'assurait visuellement que la voie était bien libérée (jusqu'au début du XX^{e} siècle). La mise en œuvre de la barrière a été ensuite téléphonique (*dispatching*) dans les années 1920, où les opérateurs se communiquaient les informations de passage des trains, puis mécanique (table d'enclenchement), électromécanique (PRCI) dans le courant du XX^{e} siècle et aujourd'hui complètement informatisé (PAI).
– **Symbolique :** Ce type de barrière se caractérise par la nécessité d'être interprété par un « agent intelligent » afin d'être mis en œuvre. La barrière est perçue par un opérateur humain (ou tout autre type d'agent intelligent capable de donner du sens à des signes) qui lui donne un sens qui se traduit par une réponse adaptée de son activité ou de son travail. Une barrière symbolique indique généralement une limitation de performance qui doit être respectée. L'exemple le plus représentatif dans le domaine ferroviaire est le système de signalisation auquel le conducteur doit adopter après interprétation les ordres de marche de son train.
– **Immatérielle :** Le dernier type proposé dans cette classification intègre les barrières qui ne reposent sur aucun élément matériel et de fait dépend de la connaissance de son utilisateur. Il s'agit des procédures réglementaires, des principes de sécurité, lois, *etc.* Une barrière immatérielle peut avoir une forme physique du type livre, classeur ou document informatisé hypertexte mais cette forme n'est généralement pas utilisée pendant l'exécution.

Le franchissement de barrières n'explique pas à lui seul l'apparition des accidents. L'analyse doit rechercher les causes et les phénomènes qui les mettent en défaut. Cette démarche rejoint la théorie de la complexité, d'où ont été puisés les modèles permettant de comprendre la dynamique des accidents.

3.3.3. La théorie de l'accident normal. — Plusieurs tentatives d'explication des accidents ont été développées à des niveaux d'abstraction des systèmes technologiques différents. [**127**] présente cette décomposition des systèmes sociotechniques :

- le niveau physique : l'action de l'opérateur humain ;
- le niveau psychologique : l'opérateur humain ;
- le niveau organisationnel : les équipes ;
- le niveau politique : décision générale.

Charles Perrow a publié une théorie [**102**] visant à expliquer les accidents. Il qualifie l'accident de *normal* « parce qu'il est inhérent aux caractéristiques des systèmes hautement couplés et complexes, et qu'il ne peut être évité » [**102**] extrait cité dans [**93**]. Perrow explique l'accident du fait de son caractère intrinsèque aux propriétés techniques du système. Le raisonnement est le suivant [**102**] :

- Les défaillances d'un composant (matériel, humain, organisation) peuvent survenir simultanément avec la défaillance d'une partie complètement différente du système. Cette combinaison imprévisible d'événements peut causer une cascade de défaillances dans d'autres parties ;
- Dans les systèmes complexes les combinaisons potentielles sont illimitées ;
- Les systèmes (de par leur complexité) ont leur propre intelligence : ils disposent de connexions cachées, peuvent neutraliser des redondances, outrepasser des barrières et ainsi exploiter des circonstances fortuites auxquelles aucun ingénieur ne pourrait penser à priori ;
- Les défaillances en cascades accélèrent la perte de contrôle, confondant les opérateurs humains en les empêchant de récupérer la situation.

De fait, la structure organisationnelle du système sociotechnique n'a pas d'influence sur l'occurrence, ni sur la prévention de l'accident normal. Perrow propose deux variables explicatives des systèmes : le niveau de complexité et le degré de couplage. La complexité représente l'ensemble des interactions possibles entre équipements et/ou composants et/ou fonctions. Le niveau de complexité est soit faible, représenté par des interactions linéaires simples, soit élevé lorsque les interactions sont moins évidentes. Les interactions visibles, attendues, et facilement compréhensibles sont qualifiées linéaires simples, par exemple ce sont les interactions prévues dans les phases d'exploitation, de maintenance préventive ou alors les interactions non prévisibles mais facilement reconnaissables et visibles. A l'inverse, les interactions complexes interviennent dans les phases inhabituelles, non planifiées, non visibles et non compréhensibles rapidement. Le degré de couplage est une mesure de la dépendance et de la flexibilité des différents éléments et séquences du système. Perrow fait varier ce degré de fort à lâche. Un degré de couplage fort correspond à l'existence de contraintes temporelles ou d'enchaînements figés et inamovibles. Le degré de couplage lâche caractérise une certaine souplesse dans l'ordre des séquences et dans les délais de réalisation. Cet espace à deux dimensions caractérisant les systèmes est basé sur des échelles subjectives. Perrow fournit les critères permettant de différencier les systèmes dans cet espace [**102**] :

- *Systèmes à interactions complexes* : relations en mode commun, substitutions limitées, informations indirectes, …
- *Systèmes à interaction linéaire* : relations dédiées, substitutions faciles, informations directes, …

– *Systèmes à fort couplage* : délais et ralentissements rarement possibles dans le processus, séquences invariables, « amortisseurs » et redondances préétablis et voulus, faible marge pour les réserves, les équipements, le personnel, …
– *Systèmes à faible couplage* : délais possibles dans les processus, ordre des séquences modifiable, « amortisseurs » et redondances fortuitement disponibles …

Les systèmes à fort couplage et à interactions complexes sont ceux susceptibles de présenter des accidents normaux. En effet, les systèmes à fort couplage requièrent une organisation centralisée pour faire face à une situation dégradée (seule la vision d'ensemble permet d'intégrer les ressources disponibles pour pallier la situation). Or, les systèmes à interactions complexes nécessitent quant à eux une organisation décentralisée pour répondre efficacement aux situations inattendues. L'accident normal découle de ce dilemme, aucune organisation ne peut répondre efficacement au besoin de ce type de système.

L'adjonction d'une troisième variable explicative des accidents permet de relier sa théorie avec la notion de sécurité. En définissant le potentiel de catastrophe, Perrow nuance le caractère inéluctable de sa théorie. Ainsi, bien qu'un système appartienne au domaine de l'accident normal, la réalisation de celui ci n'aboutira pas automatiquement à une catastrophe. La combinaison exacte des événements concourant aux événements indésirables est finalement relativement rare.

La théorie de l'accident normal ouvre un débat sur la question des responsabilités. Cette théorie a permis de nuancer l'approche réductrice présentant l'opérateur de terrain comme source d'infiabilité première [**93**]. L'organisation a sa part de responsabilité dans les accidents. Toujours selon [**93**], cette théorie est aussi politique et contre l'accroissement sauvage des technologies complexes. Le cas d'ajout de système de sauvegarde engendrant une complexité du système protégé supérieure est notamment cité.

3.3.4. Les trois modèles d'Hollnagel. — Trois grands modèles d'accidents ont été élaborés dans le but d'expliquer leurs apparitions [**68, 93**] :

Modèle séquentiel : ce modèle d'analyse se fonde sur la recherche de l'enchaînement logique des événements antérieurs à l'événement indésirable et qui lui sont reliés par un déterminisme causal. L'accident est modélisé par une succession d'événements reliés entre eux par une relation de cause à effet (cette succession a été souvent représentée par la chute de dominos les uns derrières les autres). La fonction de structure d'un tel modèle correspond à la mise en série de plusieurs composants, la chute d'un seul entraîne celle du système. Cela suppose donc que la modélisation causale soit réalisable sans hypothèse réductrice du système. La recherche des lois déterministes du comportement des éléments du système demeurent l'activité principale de l'analyste. Or celle-ci n'existe pas toujours, c'est le cas par exemple des systèmes vivants. De plus un tel modèle suppose qu'une parade ait été pensée à chaque situation où s'est produit un événement inattendu. Les événements initiateurs de la succession de défaillances sont les défaillances matérielles et humaines. Les recommandations pour supprimer les accidents consistent à supprimer l'apparition des événements initiateurs.

Modèle épidémiologique : Le modèle épidémiologique repose sur une analogie biomédicale où le système, tel un organisme vivant, serait attaqué par un agent infectieux parce que ses barrières internes de protection serait affaiblies par un environnement dégradé. L'affaiblissement

des barrières technologiques sont les résultats des défaillances passives, introduites par des conditions latentes dont l'effet n'est pas immédiat mais révélé lors de la sollicitation d'une fonction ou d'un composant du système. Les facteurs contribuant à l'accident sont donc déjà présents avant son apparition : ils se manifestent par des presque accidents ou des comportements suspects. Dans un tel modèle, les recommandations porteront sur la surveillance de ces symptômes et mettent l'accent sur l'aspect organisationnel.

Modèle systémique : En se basant sur la théorie de l'accident normal présenté précédemment, Hollnagel propose un modèle s'affranchissant des relations déterministes causales entre les événements sans toutefois se restreindre aux seules considérations organisationnelles. L'accident émerge des interactions complexes entre composants du système, il est donc contenu dans l'organisation du système. Les conditions anormales ou les facteurs d'influence intrinsèquement négatifs ne sont pas nécessaires pour que l'accident se produise. L'accident est la conséquence de coïncidences d'événements plutôt qu'une succession déterministe d'événements. Le caractère stochastique des événements est mis en avant. L'auteur expose une idée originale de dépendance fonctionnelle entre les composants du système qui permet d'expliquer l'accident. La performance de chaque fonction ou de chaque composant a une variabilité stochastique, la dépendance des fonctions et composants fait que leur variabilité peut entrer en résonance et provoquer le dépassement d'un seuil de performance global du système conduisant à l'apparition d'événements redoutés. Hollnagel a développé une méthode d'analyse fonctionnelle des systèmes basée sur l'idée de résonance stochastique appelée *Functional Resonance Accident Model* (FRAM) [**68**]. Nancy Leveson [**91**] a également développé une méthode d'analyse systémique appelée STAMP (*Systems-Theoretic Accident Model and Processes*) basée sur la théorie du contrôle et la théorie des systèmes.

Ces considérations théoriques étant posées, il est nécessaire de préciser que les analystes de sûreté de fonctionnement n'ont pas encore développé des méthodes d'évaluation et de scénarisation de la dynamique des accidents relatives aux trois modèles présentés. Dans les faits, seuls les deux premiers modèles d'accident forment un cadre méthodologique pour les méthodes employées en sûreté de fonctionnement. Ces méthodes n'ont pas dépassé le cadre de scénarisation déterministe des événements, de relation de cause à effet. Le paragraphe suivant présente ces méthodes, aujourd'hui incontournables dans les études de sûreté de fonctionnement de toutes les industries.

3.4. Les systèmes ultra-sûrs (R. Amalberti)

Selon [**9**] la sécurité des systèmes techniques a atteint un degré très élevé. L'étude des pannes et des défaillances techniques demeure au centre des études de sécurité alors qu'elles ne contribuent pratiquement plus aux accidents. En effet, les principes méthodologiques de sûreté de fonctionnement tel que le « critère de simple défaillance » imposent d'éliminer par conception tous les scénarios conduisant à l'événement redouté par la défaillance d'un seul composant. En d'autres termes cela revient à intégrer des redondances (temps, équipements, missions et/ou diversité) dans le système. Ainsi les systèmes techniques sont capables de se protéger de façon autonome contre toutes les défaillances répertoriées lors de l'analyse de sûreté de fonctionnement en conception. Pour [**9**] les accidents modernes sont le fait d'une lente divergence entre la représentation que se fait l'opérateur humain aux commandes du procédé et la situation

réelle du procédé. La cause de cette divergence résulte d'une erreur humaine qui n'a pas été détectée suffisamment tôt. Il cite pas moins d'une dizaine d'accidents aériens et autant d'autres catastrophes du transport et de l'industrie sur une période allant de 1985 à 1994 pour étayer son propos.

Les systèmes industriels « ultra-fiables » [**8**] ont donc atteint une limite infranchissable de sécurité. La complexité croissante de tels systèmes est née de la volonté d'atteindre un niveau élevé de sécurité mais elle a comme conséquence de réduire la performance des opérateurs. La recherche de la sécurité agit comme une boucle de rétroaction qui limite l'amélioration du niveau de sécurité à un seuil.

3.5. Méthodes de sûreté de fonctionnement

Ce paragraphe présente les méthodes les plus classiques utilisées en sûreté de fonctionnement visant à comprendre l'apparition des accidents en recherchant les dysfonctionnements concourant à des événements indésirables.

Un moyen d'identifier les dysfonctionnements d'un système consiste à en décrire les scénarios d'exécution. Un scénario est déterminé à partir des phases du système et de son environnement extérieur. Deux approches permettent d'identifier les scénarios. La première consiste à se placer dans un environnement et dans une phase d'exécution et de chercher les conséquences des événements jugés importants pour la sûreté de fonctionnement nommés événements initiateurs. Cette démarche est dite « inductive », il s'agit de répondre à des questions du type « que se passe-t-il si … ? » La deuxième approche vise à chercher les causes d'un événement jugé contraire à la sûreté de fonctionnement. La méthode est dite « déductive », cela consiste à répondre à des questions du type « Quelle est la cause de … ? »

La scénarisation est par essence une étude systématique des scénarios possibles et donc des événements qui les génèrent (initiateurs dans le cas inductif et causes dans le cas déductif). Les méthodes présentées ci-après relèvent de cette technique, certaines permettent de construire la fonction de structure du système et ouvrent donc la voie à une quantification des attributs de la sûreté de fonctionnement.

3.5.1. L'analyse fonctionnelle, préliminaire indispensable. — L'analyse fonctionnelle du système a pour objectif de comprendre les mécanismes sous-jacents du système qui lui permettent de remplir sa fonction principale. C'est une méthode qui a pour objet l'identification, l'expression et la caractérisation des fonctions qui modélisent les actions [**53, 54**].

Il s'agit tout d'abord d'identifier cette fonction et de hiérarchiser ses sous fonctions. Plusieurs méthodes se prêtent à cette activité. Les démarches *SADT : Structured Analysis and Design Technique* [**113, 95**] et *FAST : Functional Analysis System Technique* [**132, 142**] proposent toutes les deux un langage graphique et une méthode permettant de décrire le système par ce langage. Cette méthode décompose les fonctions du système de façon hiérarchique et modulaire. Cette technique a été utilisée notamment pour la conception et l'évaluation des systèmes Homme-Machines [**6, 7**] afin de déterminer les modes de fonctionnement et de dysfonctionnement prévisibles du procédé et de son système de commande.

[**80**] propose une comparaison des techniques SADT et FAST pour la conception de système de supervision de procédés complexes.

3.5.2. L'analyse préliminaire des dangers et des risques. — L'Analyse Préliminaire des Dangers et des Risques (APD ou APR) [**129**] est une méthode pouvant être inductive ou déductive. Elle est appliquée dès la phase de conception du système, pour l'identification des dangers inhérents au système étudié. Utilisée aux États-Unis dans les années 60 pour l'analyse de la sécurité des missiles à propergol liquide, l'APR fut ensuite généralisée à l'aéronautique, la chimie et l'industrie nucléaire.

Comme son nom l'indique, cette approche est préliminaire à d'autres études complémentaires, notamment lorsqu'un danger majeur y est mis en évidence. Cette méthode, orientée sécurité, a donc pour objectif l'identification des dangers d'une installation industrielle et de leurs causes, ainsi que l'évaluation de la gravité des conséquences liées aux situations dangereuses et aux accidents potentiels.

L'identification de ces dangers est obtenue grâce aux connaissances acquises dans le domaine, dont le retour d'expérience et le jugement d'expert. La méthode est structurée par des listes guides (*check-lists*) spécifiques à chaque domaine.

De ces réflexions sont déduits des moyens, ainsi que des actions correctrices permettant d'éliminer ou de maîtriser les situations dangereuses et accidents potentiels mis en évidence. Au cours du temps, ces résultats doivent être vérifiés, et l'analyse peut être complétée ou mise à jour, et ceci jusqu'à la fin de vie de l'installation considérée.

Le résultat de cette méthode fournit des éléments permettant d'anticiper les dangers par la mise en place de barrières de sécurité pour chaque danger majeur identifié. En outre, l'APR permet d'évaluer la probabilité d'occurrence des dangers identifiés.

La méthode APR est largement utilisée dans le domaine ferroviaire mais de façon très disparate, chaque industriel disposant de sa propre approche. Dans le cadre du projet SECUGUIDE, une harmonisation de ces approches est en cours, [**55**] propose une formalisation de l'APR pour le ferroviaire utilisant une démarche à la fois inductive et déductive.

3.5.3. Analyse des Modes de Défaillance et de leurs Effets. — L'analyse des Modes de Défaillance et de leurs Effets (AMDE) est une méthode permettant d'identifier les défaillances simples conduisant à des conséquences inacceptables pour la sûreté de fonctionnement (*ie.* événements indésirables). Le raisonnement est inductif, les événements initiateurs sont formés par les modes de défaillances et les fonctions des composants du système. Le scénario consiste à déterminer les effets de chaque initiateur sur le système. La constitution de chaque scénario utilise des données factuelles historiques ainsi que des données prévisionnelles et prospectives.

L'AMDE [**129**] procède en quatre étapes :

– Définition du système, de ses fonctions, de ses composants et des différents contextes d'exécution ;
– Identification des modes de défaillance des composants et de leurs fonctions ainsi que les causes de ces défaillances ;
– Étude des effets des modes de défaillances ;

– Conclusions et recommandations pour l'amélioration du système.

La définition du système est une étape commune à toute étude de sûreté de fonctionnement. Cette étape de l'AMDE doit être couplée avec l'étude de conception du système. En effet, les ingénieurs système réalisent une analyse fonctionnelle du système indispensable à la bonne réalisation de la conception ou de l'amélioration d'un produit. L'analyse fonctionnelle détermine les fonctions principales, les fonctions secondaires et les fonctions contraintes d'un système. Plusieurs outils structurés d'analyse fonctionnelle ont été élaborés et répondent aux besoins de l'AMDE :

– Diagramme de bloc ;
– FAST (Functional Analysis System Technique) [**80**] ;
– SADT (Structured Analysis Design Technique) [**113, 95**] ;

L'analyse fonctionnelle fournit un découpage hiérarchique du système sur lequel va reposer toute l'analyse AMDE. À ceci, il faut ajouter la description du contexte et des conditions d'exécution, à savoir la description de l'environnement extérieur et les phases d'exécution (démarrage, arrêt, transitoires, etc.) dans lequel évoluent ces fonctions.

Cette première étape permet de découper l'analyse de façon à passer en revue chaque fonction et composant du système dans chacune de ses phases.

En plus de la détermination des phases et des fonctions du système, il est également indispensable de définir les limites fonctionnelles du système dans son ensemble ainsi que celles de ses composants. Il en est de même pour les spécifications relatives au fonctionnement du système et de ses composants ainsi que celles relatives à l'environnement dans lequel le système et ses composants sont installés.

La deuxième étape consiste à établir les modes de défaillance des composants et leurs causes. Par définition, un mode de défaillance d'un composant ou d'une fonction est l'effet par lequel une défaillance sur ce composant est observée. C'est donc le caractère perceptible de la défaillance. Il s'agit dans cette étape d'établir une liste exhaustive des modes de défaillance pour chaque fonction et composant du système et ceci pour chaque phase. L'analyste puise ses informations dans le retour d'expérience dans le cas où le composant a déjà été mis en service dans un autre système ou bien sur la base d'étude de fiabilité du composant. Le référentiel normatif présenté dans [**129**] propose des listes guides des modes de défaillances génériques.

La troisième étape consiste à analyser les effets des modes de défaillance sur le système. Les effets doivent être décrits précisément en supposant que le seul composant étudié est défaillant. Le choix du niveau de précision de l'étude aide à la délimitation des effets les plus pertinents à prendre en compte.

Enfin la synthèse et les conclusions des étapes précédentes forment la dernière étape de l'étude. Ses conclusions ont la forme de recommandations sur le système permettant d'améliorer la sûreté de fonctionnement. Les recommandations principales consistent à supprimer les défaillances simples. Une liste des recommandations types fournie par l'AMDE est donnée ci-après (non exhaustive).

– Identification des défaillances simples, proposition de mesures correctives (redondance) ;
– Hiérarchisation des modes de défaillances suivant l'ampleur de leurs effets sur les fonctions du système ;

- Identification de certaines défaillances impliquant plus d'un composant ;
- Établissement pour chaque mode de défaillance de procédures de détection ;
- Établissement pour chaque mode de défaillance de procédures maintenance ;
- Mise en évidence de moyens d'élimination et de minimisation des effets.

La présentation des résultats est synthétisée dans un tableau de dix colonnes :

(1) Phase du système ;

(2) Identification du composant : identification et localisation précise du composant ;

(3) Fonction et états : recenser toutes les fonctions du composant ainsi que ses différents états de fonctionnement ;

(4) Modes de défaillance : ils sont recensés pour chaque composant dans les différents états de fonctionnement envisagés et dans les différentes phases du système ;

(5) Causes possibles de défaillance : regrouper les causes possibles en deux catégories, les causes internes et les causes externes ;

(6) Effets sur le système : inventaire des effets de chaque mode de défaillance ;

(7) Effets externes : inventaire des effets des modes de défaillance sur les systèmes externes en interaction ;

(8) Moyens de détection ;

(9) Fréquence des inspections et des essais ;

(10) Observations.

La présentation des résultats varie en fonction des besoins de l'étude envisagée. Le lecteur intéressé trouvera des exemples d'application dans [**129**].

Une extension de l'AMDE, AMDEC acronyme d'Analyse des Modes de Défaillances de leurs Effets et de leurs Criticités ajoute une analyse quantitative subjective des défaillances. Cette quantification subjective utilise la notion de risque quantifié qui sera présentée dans la suite de ce chapitre. La méthode est identique à celle de l'AMDE à ceci près qu'il faut évaluer sur une échelle subjective la gravité de chaque effet ainsi que la fréquence d'apparition du mode de défaillance. Ce couple détermine un niveau de criticité de l'événement (voir notion de risque 3.16).

[**111**] propose une version spécifique de la méthode AMDE pour l'examen des exigences des informations fournies à l'opérateur de supervision en situation dégradée. L'objectif de cette déclinaison consiste à concevoir le système d'alarme en prenant en compte le facteur humain.

Cette méthode a fait ses preuves dans de nombreuses industries. La validité de la méthode repose sur l'exhaustivité du recensement des défaillances et de leurs effets.

3.5.4. Arbres de défaillances. — La méthode par arbre de défaillances consiste à représenter graphiquement la fonction de structure du système (voir figure 3.2). La méthode est déductive et offre un guide à l'analyste pour construire la logique de fonctionnement du système. Le modèle d'accident sous-jacent est le modèle séquentiel.

La méthode fut développée au début des années 1960 dans les bureaux de Bell Telephone et utilisée pour évaluer et améliorer la fiabilité du système de lancement du missile « Minuteman » [**129**]. Son utilisation obtint un franc succès, depuis son emploi est devenu fréquent dans de

nombreux domaines industriels. C'est aussi la méthode de calcul des attributs de la sûreté de fonctionnement la plus répandue. Utilisée après une AMDE, la méthode par arbre de défaillance la complète par la recherche de défaillances simultanées multiples conduisant à l'événement redouté.

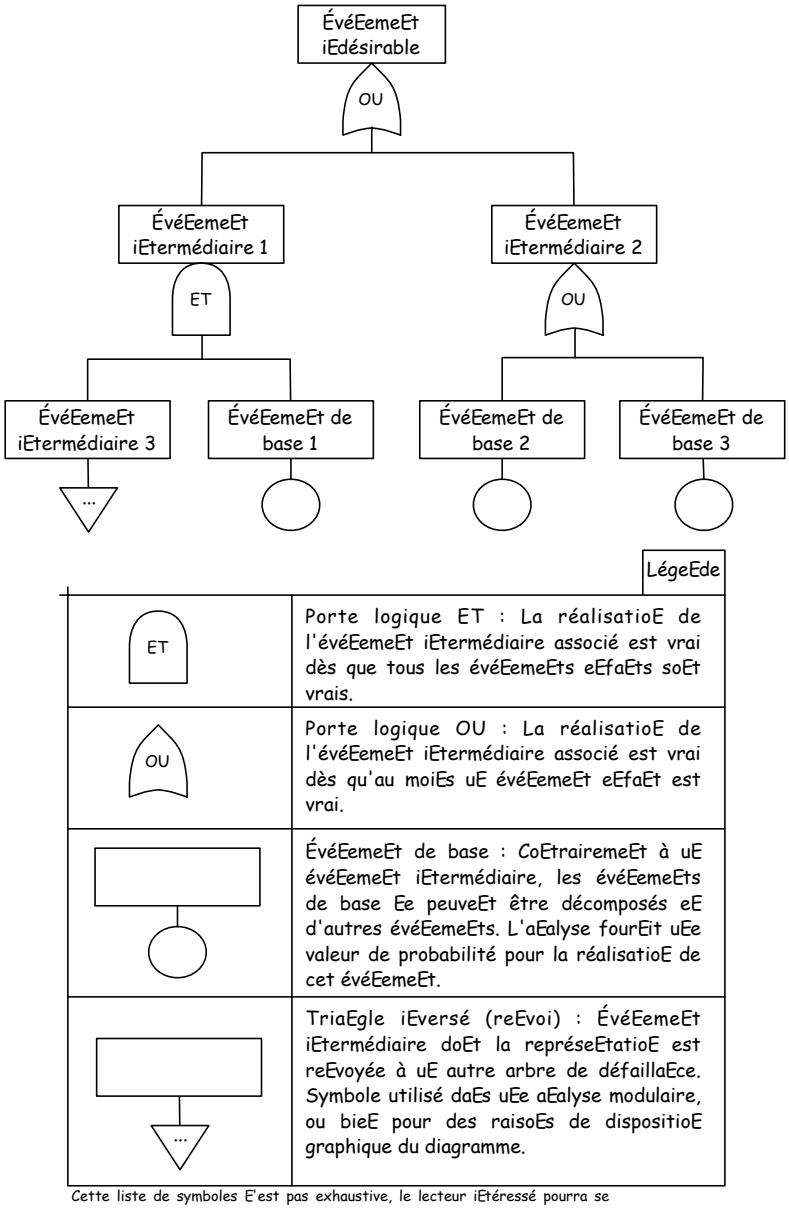


FIGURE 3.2. Exemple d'arbre de défaillance

La particularité de cette méthode est d'être à la fois quantitative en évaluation la probabilité d'apparition de l'événement sommet (probabilité de l'état de panne de la fonction de structure) et qualitative en présentant par le calcul booléen les coupes minimales du système. Il est ainsi possible de juger du nombre de défaillances contribuant à l'événement sommet. La présentation détaillée de cette méthode est donnée dans [**92**].

3.5.5. Arbres d'événements. — Contrairement aux arbres de défaillances la méthode des arbres d'événements [**129**] s'intéresse aux conséquences possibles des défaillances, la méthode est inductive. À partir d'un événement initiateur, l'arbre développe tous les scénarios d'évolutions possibles du système. Le modèle d'accident sous-jacent repose sur le modèle épidémiologique. L'apparition d'un événement initiateur va modifier le comportement du système jusqu'à ce que le dépassement d'une valeur seuil déclenche un processus de sauvegarde du système. Ce processus consiste à prendre des mesures, soit automatiquement, soit par l'intermédiaire d'opérateurs, afin de faire évoluer le système dans un état sécuritaire. Ces mesures peuvent ne pas aboutir pour différentes raisons et, suivant leur succès ou leur échec, le système évoluera de manière différente. Ces mesures de protection sont des événements génériques dont le succès est modélisé par un arbre de défaillance du sous-système de sauvegarde considéré. On représente la réussite ou l'échec de ces mesures à l'aide de branchements dans l'arbre d'événements. Un arbre d'événements se base sur un formalisme graphique. Un arbre d'événements code un ensemble de séquences d'événements. Chaque séquence consiste en un événement initiateur (colonne la plus à gauche) et une succession de défaillances ou de fonctionnements de système de sauvegarde (parade, mission, procédure, *etc.*). Les séquences aboutissent à un état du système (la colonne la plus à droite). Des conséquences que l'on juge acceptables ou inacceptables (événements redoutés) sont associées à ces états.

Chaque branchement dans l'arbre correspond à l'un des deux états possibles du sous-système de sauvegarde. Par convention la branche supérieure correspond au succès et la branche inférieure à l'échec.

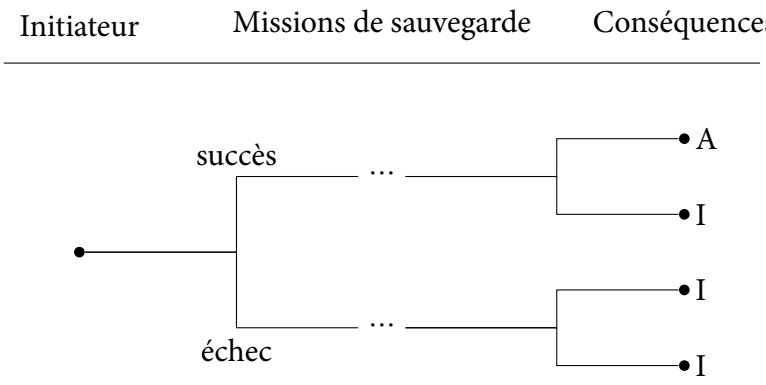


FIGURE 3.3. Exemple d'arbre d'événements

La méthode comporte un aspect temporel et fonctionnel dans la mesure où les sous-systèmes de sauvegarde sont considérés dans l'ordre chronologique de leur intervention et qu'ils peuvent partager des événements de base voire des coupes dans la fonction de structure. La suite de sous-systèmes sollicités dépend du succès ou de l'échec des sous-systèmes de sauvegarde précédents.

3.5.6. Méthodes dynamiques. — La modélisation dynamique consiste à représenter les différents états du système dans le temps, contrairement à l'approche statique employée jusqu'à présent où l'on s'intéressait à l'état du système après une date fixée quel que soit l'ordre d'apparition des pannes. Un processus stochastique permet de représenter l'évolution du système dans le temps. Le lecteur intéressé par l'étude des modèles stochastiques pour la fiabilité pourra se reporter à [**30**] et [**37**].

Il s'agit de recenser et de classer tous les états du système (si le système comprend n composantes, le nombre d'états maximal est de 2^n. Puis il faut identifier toutes les transitions possibles entre ces différents états. Si la probabilité de passer de l'état i à l'état j est $a_{ij}dt$ entre les instants t et $t + dt$ alors a_{ij} est le taux de transition entre ces deux états. Lorsque les taux de transitions sont constants dans le temps, le processus stochastique modélisant l'état du système dans le temps est un processus Markovien homogène [**47**]. L'aspect qualitatif sera représenté par le graphe de Markov associé au processus. Le calcul quantitatif correspond à la probabilité d'entrer dans un état de panne du système avant la durée de mission.

Le calcul Markovien, de nature matricielle, s'avère rapidement couteux en opérations lorsque le nombre de composants du système augmente. C'est l'une des raisons pour lesquelles ces méthodes sont rarement mises en œuvre dans les études globales des systèmes. Elles sont généralement utilisées pour démontrer la fiabilité d'une partie du système de façon spécifique.

Jusqu'à présent, seules les méthodes d'évaluation qualitative et quantitative de la sûreté de fonctionnement ont été présentées. En réalité, un processus de mise en œuvre de la sûreté de fonctionnement permet de guider l'utilisation de ces méthodes et définit les objectifs de sûreté de fonctionnement à atteindre. Ce sont les méthodes analytiques qui proposent une structure globale d'étude et font usage des méthodes présentées dans ce paragraphe.

3.6. Le processus d'évaluation de la sécurité

La sûreté de fonctionnement doit être intégrée dans le processus de conception ou d'amélioration du système. A ce titre les méthodes de sûreté de fonctionnement sont intégrées à celles de l'ingénierie de conception et les complètent. La dernière phase du processus consiste à évaluer la démonstration de la sécurité. Cette phase se nomme « certification de la sécurité ». Le processus d'évaluation et le vocabulaire présentés ci-après est commun aux ingénieurs qui évaluent la sécurité et aux certificateurs. La phase de certification est une étape importante du système, toutes nouvelles méthodes proposées pour évaluer la sécurité doivent être acceptées au niveau de la certification. Se reporter à [**31, 32**] pour plus de précisions sur la phase de certification des applications ferroviaires critiques pour la sécurité.

3.6.1. Évaluation de la sécurité et des risques. — Avant de commencer l'analyse proprement dite, il faut déterminer le niveau de risque acceptable du système étudié. Ce niveau servira d'objectif à atteindre pour l'obtention de la sûreté de fonctionnement. Plusieurs techniques permettent de calculer ce niveau, l'Analyse Préliminaire des Risques (APR) [**129**] est la plus répandue.

***Définition 3.16* (Risque).** — [**129**] *propose la définition suivante :*

« Mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable ou d'une situation dangereuse et une mesure de ses effets ou conséquences. »

Cette définition offre l'avantage d'être suffisamment générale pour pouvoir s'adapter à la plus grande partie des risques naturels ou industriels. Les unités sont données en spécifiant les mesures au système étudié. La spécialisation de cette définition nécessite de donner du sens à

l'association entre les deux mesures effectuées : occurrence et effets. En règle générale, le produit est utilisé.

Pour chaque situation dangereuse, il faut définir une probabilité ou fréquence d'occurrence (objective ou subjective), la norme CENELEC EN 50126 [**33**] définit une échelle dont chaque catégorie est associée à une plage de probabilité ou de fréquence d'occurrence subjective. Une reproduction de cette échelle est présentée dans le tableau 3.1. Dans ce tableau, le terme *souvent* indique que l'événement indésirable ou la situation dangereuse est survenu(e) et surviendra à nouveau.

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

TABLE 3.1. Probabilité d'occurrence ou fréquence d'une situation dangereuse

La définition du risque repose également sur une évaluation des conséquences sur le système de l'apparition de l'événement indésirable appelée niveau de gravité. Cette mesure est généralement subjective mais peut être plus objective (niveau d'accélération des sols dans le cas d'un tremblement de terre par exemple). La table 3.2 présente l'échelle de mesure en vigueur dans les études de sécurité ferroviaire issue de la norme CENELEC EN 50126 [**33**].

Étant donné la diversité des risques et de l'impact qu'ils peuvent avoir sur le système, il est préférable de définir des catégories et d'associer à ces catégories des actions. La table 3.3 propose une telle catégorisation.

Le référentiel normatif recommande la mise en place d'une matrice d'occurrence-gravité permettant d'évaluer les risques. Toujours en utilisant le référentiel en vigueur dans le domaine ferroviaire, la table 3.4 reproduit l'évaluation proposée par [**33**].

Le « risque acceptable » est une valeur d'un risque résultant d'une décision explicite établie de façon objective [**31**]. Ce seuil est noté THR acronyme de *Tolerable Hasard Rate*. Le THR est une probabilité d'occurrence d'une défaillance exprimée en défaillance par heure sous la forme 10^{-x} par heure. Lors de l'identification des situations dangereuses (dans le cadre d'une analyse préliminaire des dangers par exemple voir [**129**] pour une présentation détaillée de cette méthode analytique), il faut associer un THR à chaque événement indésirable recensé.

La maîtrise des risques qui dépassent le seuil d'acceptabilité consiste à :

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

TABLE 3.2. Niveau de gravité des situations dangereuses

Risque	Action à appliquer
Inacceptable	Doit être éliminé
Indésirable	Acceptable uniquement lorsqu'il est impossible de réduire le risque en accord avec l'autorité de tutelle
Acceptable	Acceptable moyennant un contrôle approprié et l'accord de l'exploitant final
Négligeable	Acceptable avec/sans accord de l'exploitant final

TABLE 3.3. Catégorie qualitative des risques

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

TABLE 3.4. Matrice occurrence-gravité

– diminuer la probabilité d'occurrence par des parades préventives qui ont pour but de réduire la vulnérabilité des éléments du système exposés ;
– diminuer la gravité des conséquences par la mise en place de protections.

Ces mesures doivent être prises en compte dans la phase de réalisation ou d'amélioration du système, elles conduisent donc à l'élaboration d'exigences de sécurité pour les éléments concernés.

À partir de la liste des exigences de sécurité et des THR, le référentiel normatif définit un *niveau d'intégrité de la sécurité* noté SIL (*Safety Integrity Level*). Le SIL se décline en 5 valeurs

discrètes permettant de spécifier les prescriptions concernant l'intégrité de la sécurité. La table 3.5 montre le lien qui existe entre SIL et THR.

THR	SIL
$10^{-9} \leq$ THR $\leq 10^{-8}$	4
$10^{-8} \leq$ THR $\leq 10^{-7}$	3
$10^{-7} \leq$ THR $\leq 10^{-6}$	2
$10^{-6} \leq$ THR $\leq 10^{-5}$	1
$10^{-5} \leq$ THR	0

TABLE 3.5. Table des SIL extraite de la norme IEC 61508 [**74**]

Remarque importante : La lecture de ce tableau se fait exclusivement de la gauche vers la droite. Un THR permet de définir un niveau de SIL. Le niveau de SIL correspond à un niveau de confiance à atteindre. Dans de rares exceptions, il est possible de passer d'un niveau de SIL à un THR lors de l'introduction d'un matériel nécessaire à l'obtention d'un niveau de SIL.

Le lecteur intéressé trouvera une présentation détaillée des méthodes d'allocation des THR, SIL et autres objectifs de sécurité dans [**28**].

3.6.2. Quantification prévisionnelle. — L'évaluation du THR est une étape difficile dans le processus d'analyse de sûreté de fonctionnement. En matière de sécurité, le THR sert aussi de moyen de mesure de la sécurité globale d'un système. Dans le domaine nucléaire, les études probabilistes de sécurité ont été mises en place dans l'objectif de démontrer le niveau de risque acceptable d'une installation nucléaire mesuré sur trois niveaux correspondant aux trois grandes barrières d'une centrale nucléaire [**93**] :

– Premier niveau : la gaine combustible, l'étude démontre le THR de la dégradation des éléments combustibles (fusion du réacteur) mesuré par an et par réacteur.
– Deuxième niveau : le circuit primaire, l'étude démontre la tenue de celui-ci suite à une dégradation de la première barrière de façon probabiliste par an et par réacteur.
– Troisième niveau : l'enceinte de confinement, l'étude porte sur les conséquences sur l'environnement et les populations d'une dégradation successive des trois barrières. Cette dernière éventualité n'est généralement pas évaluée du fait des très faibles probabilités manipulées.

De notre point de vue, une telle méthode n'existe pas dans le domaine ferroviaire, les études probabilistes de sécurité dans le domaine nucléaire apportent des éléments de décision sur l'architecture globale du système et les objectifs de sécurité.

La suite de ce paragraphe présente la méthode mise en place pour l'évaluation probabiliste de sécurité de premier niveau.

***Définition 3.17* (EPS, [93]).** — Les Études Probabilistes de Sécurité (EPS [2]) consistent à identifier des accidents ou incidents dits « initiateurs », puis à identifier et modéliser des « missions de sauvegarde » qui visent à récupérer la situation causée par ces initiateurs.

2. A l'origine le sigle EPS a été inventé dans le domaine nucléaire pour Études Probabilistes de Sûreté nucléaire. En effet, la Sûreté nucléaire est une classe particulière de la sécurité relative aux événements indésirables liés à la radioactivité.

On définit alors une *séquence accidentelle* par une suite d'événements formée d'un initiateur et un ou plusieurs échecs de missions de sauvegarde.

L'objectif de l'EPS est de calculer la probabilité d'occurrence de l'ensemble des séquences accidentelles à l'aide du formalisme des arbres d'événements. L'initiateur et les missions de sauvegarde sont modélisés par des arbres de défaillance. Enfin, pour un ensemble de séquences accidentelles, l'EPS fournit la contribution au risque de chacune des composantes modélisées du système.

Conçue pour l'étude de sûreté des centrales nucléaires, la première EPS a été réalisée aux États-Unis en 1975. Les résultats mettaient en évidence trois facteurs déterminants (forte contribution) du risque :

- les transitoires d'exploitation (montée en puissance, arrêts, etc.) ;
- les petites brèches du circuit primaire ;
- et les actions opérateurs.

Les conséquences en cas d'échecs des actions opérateurs étaient envisagées. Exactement quatre ans plus tard, l'accident de Three Miles Island venait confirmer le résultat de l'EPS en révélant l'importance du facteur humain (Voir à propos de l'analyse de cet accident le résumé de [**39**] citant l'analyse de [**38**]).

En effet, les missions de sauvegarde suite à événements initiateurs reposent forcément à un moment ou à un autre sur l'action d'un opérateur. L'évaluation de la fiabilité humaine devient donc un besoin essentiel pour mener à bien l'évaluation globale de la sécurité. Le domaine nucléaire a très tôt développé des méthodes d'évaluation de la fiabilité humaine (*Human Reliability Analysis* HRA ou Étude Probabiliste des Facteurs Humains EPFH [**93**]). Les calculs étaient basés au début sur la notion de Probabilité d'Erreur Humaine (PEH) égale au rapport d'erreurs relevées sur le nombre d'occasions de commettre l'erreur (nombre de cas favorables sur le nombre de cas possibles). Toutefois cette évaluation simpliste a atteint ses limites en raison de la difficulté d'obtenir des données d'une part et de la validité d'un tel modèle d'autre part qui considère l'homme comme un composant matériel du système.

3.7. Conclusion

Le besoin des sociétés modernes impose des choix technologiques complexes, exigeants et parfois risqués. De nouvelles technologies encore peu ou mal assimilées sont de plus en plus rapidement intégrées en produits commercialisables.

Jusqu'à une période relativement récente (fin des années 1950), les concepteurs de systèmes étudiaient de façon limitée les effets des défaillances. Ces études étaient motivées par les réactions des clients et vis-à-vis d'un positionnement sur la concurrence. Les méthodes utilisées s'apparentaient à de la sur-qualité.

La sûreté de fonctionnement est une science appliquée par essence, une science physique cherchant à déterminer les lois de comportement, de fonctionnement, de défaillance ou de réparation des systèmes technologiques.

Les méthodes couramment employées en sûreté de fonctionnement reposent pour la plupart sur l'hypothèse d'exhaustivité d'analyse de l'ingénieur de sûreté de fonctionnement. Hypothèse permettant de prévoir tous les aléas possibles ou bien tous les modes de fonctionnement d'un système. L'ensemble des modes de fonctionnement d'un système est le produit cartésien des ensembles des états du système par l'ensemble des états de l'environnement. Sa dénombrabilité dépend des hypothèses de modélisation. Plus la modélisation du système est fine, plus le support des variables caractéristiques est dense et donc indénombrable voire continu. Inversement, lorsque la modélisation est grossière le support des variables d'états se discrétise formant des ensembles finis. Le niveau de zoom effectué dans les analyses, c'est-à-dire la densité du support des variables d'état, s'interprète comme un indicateur de simplification du modèle.

Jean-Claude Wanner dans son intervention au colloque organisé par l'institut européen de cindyniques [3] (Lettre n°42, Mars 2006) affirme :

« Parmi les événements qui risquent de réduire la sécurité, il faut citer tous ceux que l'on ne peut imaginer au moment de la conception et qui ne se révèlent qu'au cours de l'utilisation. Nous n'avons pas assez d'imagination pour *inventer* les scénarios dangereux et prendre à temps les précautions permettant de les éviter. »

La complexité des systèmes limite l'« imagination » de l'analyste de sûreté de fonctionnement. L'opérateur humain dans le système est l'un des facteurs de complexité sinon le facteur de complexité majeur. Il est possible d'apercevoir cette complexité lorsqu'on cherche à connaître l'impact du facteur humain sur la sécurité par le fait qu'il n'y a pas de réponse sans équivoque à cette question. L'opérateur humain est faillible mais demeure surtout le seul rempart capable d'imaginer, pendant l'exécution, les événements que les concepteurs n'ont pas pu « inventer ». L'opérateur humain ne peut être résumé à sa seule faillibilité, cependant, le référentiel présenté dans le présent chapitre n'offre pas les outils nécessaires à un tel jugement.

Le chapitre suivant présente les méthodes spécifiques au facteur humain qui ont été développées en sûreté de fonctionnement.

3. Le terme cindynique vient du grec *kíndunos* et signifie danger, il désigne aujourd'hui les sciences qui étudient les risques.

CHAPITRE 4

L'ÉTUDE DU FACTEUR HUMAIN

Résumé

Ce chapitre est consacré à la prise en compte du facteur humain dans les études de sûreté de fonctionnement. L'humain en situation de travail est l'objet d'étude d'un ensemble de disciplines des sciences humaines et sociales (psychologie du travail, ergonomie notamment), de fait cette étude ne peut être approchée seulement par les sciences de l'ingénieur qui officient en sûreté de fonctionnement. La difficulté de cette intégration repose en partie sur l'interdisciplinarité de l'étude. Après un bref historique introductif, les modèles majeurs issus de la psychologie et de l'ergonomie du travail sont présentés. La deuxième partie de ce chapitre présente les méthodologies qui permettent d'évaluer le facteur humain dans l'étude sécurité.

4.1. Introduction

Dans le milieu des années 1950, apparaissent les premières études tenant compte de la composante humaine des systèmes. Le besoin d'une telle intégration a été initiée par l'U.S. Air Force, en 1958 deux rapports internes font apparaître la mention « human engineering » dont la meilleure traduction française serait « l'ingénierie des facteurs humains ». Cette nouvelle discipline, issue de la « cybernétique », envisage de comprendre et de modéliser la performance des acteurs humains dans le travail. Elle permet d'inclure dans les études de fiabilité des systèmes une composante essentielle et pourtant jusque-là oubliée de l'ingénierie : l'Homme. Présent dans toutes les phases du cycle de vie d'un système, l'opérateur humain pense, conçoit, crée, fabrique, contrôle, supervise et maintient en condition opérationnelle le système.

Le facteur humain revêt donc une importance capitale dans le sens où un écart significatif de performance lors d'une phase critique de la vie du système pourrait entraîner des conséquences désastreuses.

La première activité de recherche dans ce domaine a consisté à classer les types d'erreurs que l'homme peut produire dans le but de les étudier et de les contrôler. Le modèle sous-jacent relevait alors de la fiabilité classique des systèmes techniques. Les études sur l'erreur humaine ont été élaborées au début dans l'objectif de réduire le nombre d'erreurs par un contrôle du processus de création des erreurs. En parallèle, les premiers modèles de l'activité humaine au

travail apparaissent, (les travaux de Rasmussen sur le modèle SRK notamment [**105**]) avec pour objectif d'expliquer le processus de création des erreurs.

Au début des années 1990, la première approximation de l'homme comme composant technique du système atteint ses limites, Dougherty [**41**] précise le besoin de modèle cognitif dans les études. Ainsi, les travaux se sont portés sur les facteurs d'influence de la performance de l'homme au travail avec pour dessein d'intégrer un modèle de la cognition dynamique en interaction avec un environnement caractérisé par les facteurs d'influence majeurs. L'environnement de travail, physique et psychologique, est épié avec de plus en plus minutie. Le recours à des disciplines relevant des sciences humaines et sociales s'intensifie. L'étude de l'environnement physique entre dans le giron de l'ergonomie du poste de travail, l'environnement psychologique se compose de l'activité individuelle, en équipe et organisationnelle.

L'introduction des sciences cognitives dans l'ingénierie des facteurs humains depuis la fin des années 1990 a nuancé l'objectif premier de tenter de supprimer les erreurs. Amalberti [**9**], notamment, propose un modèle de sécurité écologique mettant en avant le rôle incontournable des erreurs dans le contrôle de processus.

Les techniques de sûreté de fonctionnement relative à la prise en compte des facteurs humains traitent généralement les activités humaines en rapport avec la sécurité d'une manière différente que celle énoncée ici. La distinction des actions humaines de sécurité est généralement donnée en termes d'erreurs humaines. Reason [**109**] propose dans cette optique une classification des erreurs humaines. Il distingue les *ratés* et les *lapsus* qui résultent d'actions non intentionnelles et les *fautes* et les *violations* qui résultent d'actions intentionnelles. Cette classification se base sur le modèle de comportement de l'opérateur humain de Rasmussen [**105**] où il est possible de rattacher les ratés et les lapsus à un comportement basé sur les habiletés et les fautes à un comportement basé sur les règles et les connaissances (voir paragraphe suivant). En ce qui concerne les violations, Reason [**109**] ne les considère pas comme des erreurs, puisqu'il définit l'erreur par la divergence entre le résultat souhaité de l'action et le résultat obtenu. Or, la violation est une action volontaire donc potentiellement conforme au résultat escompté. Amalberti [**9**], juge la violation comme étant le résultat d'un compromis cognitif permettant d'agir et donc potentiellement de réduire les risques tout en préservant une charge de travail utile et nécessaire pour continuer l'activité.

Cette classification de l'erreur humaine s'appuie à la fois sur le comportement de l'opérateur et sur la tâche prescrite. Il est difficile de décrire la tâche prescrite autrement que par l'étude des manuels, de la réglementation de l'activité ou bien par l'observation de l'activité de l'opérateur. L'expérience montre qu'il existe en général une divergence entre ce qui est prescrit par l'organisation et l'observation ; la thèse de Polet [**103**] s'appuie sur ce constat et propose un modèle permettant d'identifier et d'évaluer cette divergence. S'il est possible de modéliser les tâches prescrites par l'organisation du système, il est illusoire de rechercher avec une logique d'exploration systématique les activités réelles de l'opérateur. D'une part, à chaque tâche prescrite correspond une quantité importante et variable d'activité humaine. Par exemple, lorsque la tâche prescrit de surveiller l'état d'un composant technique, l'opérateur humain effectue plusieurs activités et à différents niveaux de traitement cognitifs. D'autre part, d'un opérateur humain à l'autre, il existe une variabilité d'exécution non négligeable. Chacun n'opère pas de la même façon et n'active pas les mêmes niveaux cognitifs au même moment et de la même façon. Dans l'exemple d'une tâche de surveillance, certains seront plus sensibles à la couleur

et d'autres à la forme du signal proposé par l'interface Homme-Machine. De plus, certains opérateurs humains effectueront un traitement cognitif plus évolué (cherchant à interpréter par leur propre raisonnement les signes affichés) alors que d'autres s'appuieront sur le raisonnement préalablement établi dans le règlement.

4.2. Modèles issus de la psychologie et de l'ergonomie du travail

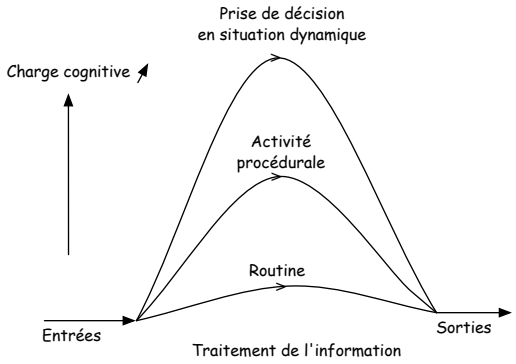


FIGURE 4.1. Les trois niveaux d'abstraction de l'activité cognitive selon Rasmussen [**106**]

4.2.1. Le modèle SRK de Rasmusen. — Le cadre conceptuel de l'analyse des facteurs humains développé par Rasmussen [**106**] définit une décomposition hiérarchique du travail de l'opérateur humain. Cette hiérarchie se décompose en niveaux d'abstraction : Le contrôle cognitif et la cognition humaine se font à plusieurs niveaux d'abstraction (voir figure 4.1). Ces niveaux peuvent être comparés aux différentes couches logicielles d'un système programmé. La couche la plus basse correspond au traitement réflexe de l'information, on parle d'automatisme mental, ou de routine, l'action cognitive est rapide. Les couches plus élevées correspondent à un traitement de l'information de plus en plus complexe. Dans le modèle de Rasmussen, la couche la plus élevée représente la prise de décision en situation dynamique, la charge cognitive étant élevée, les actions en réponse prennent plus de temps. Le modèle décrit les comportements des opérateurs dans un ensemble de trois niveaux ou couches : niveau basé sur les habiletés, niveau basé sur les règles et le niveau basé sur les connaissances. Ceux-ci sont successivement décrits :

4.2.1.1. Comportement basé sur les habiletés. — Un comportement basé sur les habiletés représente un type de comportement qui requiert très peu ou aucun contrôle conscient pour exécuter une action une fois qu'une intention est formée ; connu également sous la dénomination de comportement sensorimoteur. La performance est lisse, automatisée, et consiste en patterns (schèmes) de comportement hautement intégrés dans la plupart des contrôles basés sur les habiletés [**107**]. Par exemple, rouler en vélo est considéré comme un comportement basé sur les habiletés dans lequel peu d'attention est requise pour le contrôle une fois que l'habileté est acquise. Cet automatisme permet aux opérateurs de libérer des ressources cognitives, qui peuvent être utilisées pour des fonctions cognitives de haut niveau comme la résolution de problèmes.

4.2.1.2. Niveau basé sur les règles. — Un comportement basé sur les règles est caractérisé par l'utilisation des règles et de procédures pour sélectionner une séquence d'actions dans une situation de travail familière [**107**]. Les règles peuvent être un ensemble d'instructions acquises par un opérateur par expérience ou données par les superviseurs et les opérateurs formateurs.

Les opérateurs ne sont pas obligés de connaître les principes sous-jacents à un système pour exercer un contrôle basé sur les règles. Par exemple, les hôpitaux ont des réglementations hautement procéduralisées pour les alertes au feu. C'est pourquoi, lorsque quelqu'un voit un feu il peut suivre les étapes nécessaires pour assurer la sécurité sans aucune connaissance de la conduite à adopter en cas de feu.

4.2.1.3. Niveau basé sur les connaissances. — Un comportement basé sur les connaissances représente un niveau plus avancé de raisonnement. Ce type de contrôle doit être employé lorsque la situation est nouvelle et inattendue. Les opérateurs doivent savoir les principes fondamentaux et les lois qui gouvernent le système. Puisque les opérateurs ont besoin d'établir des objectifs explicites (décisions) à partir de leur analyse du système, la charge mentale est typiquement plus élevée que lorsqu'ils activent des comportements basés sur les habiletés ou sur les règles.

4.2.2. Cognitive Work Analysis (Analyse du travail cognitif). — CWA est une méthodologie issue des travaux de l'automatique humaine (plus particulièrement du courant anglophone de ce domaine « human engineering »), spécialement conçue pour l'analyse, la conception et l'évaluation de systèmes sociotechniques complexes. [**128, 108**]. L'intérêt de cette méthodologie repose sur la mise en valeur du caractère dynamique comme facteur essentiel des systèmes sociotechniques complexes. Cette nature dynamique résulte de plusieurs facteurs dont :

- le changement rapide de technologies ;
- l'informatisation du travail ;
- l'accroissement du niveau d'intégration et de couplage à l'intérieur du système.

Ceci explique notamment qu'un changement intervenant dans une activité du système se propage rapidement aux autres activités avec son lot de répercussions.

CWA se base également sur le fait que les systèmes sociotechniques complexes sont fortement automatisés. Ainsi, les conditions de travail stabilisées ou routinières (modes dits normaux et nominaux) sont gérées par les automates. Les opérateurs humains quant à eux sont là pour faire face aux situations imprévues (modes dégradés). Ce sont justement ces situations qui ont un impact important sur la sécurité [**128**]. Amalberti présente à ce propos, le concept de système ultra-sûr [**8**]. La fiabilité des systèmes techniques a atteint un niveau tel qu'ils sont capables de détecter leurs propres défauts et de se replier dans un état sûr de façon autonome. Cet objectif est atteint par la mise en place, lors de la conception, d'une architecture sécuritaire à base de redondances et de mécanismes à sécurité intrinsèque engendrant une forte complexité des systèmes. Pour Amalberti, cet accroissement de la complexité est la cause d'un déséquilibre de la performance des opérateurs et limiterait ainsi l'obtention d'un niveau de sécurité plus haut.

Compte tenu de ces deux caractéristiques et de leurs implications, CWA propose que la conception ainsi que l'amélioration des systèmes sociotechniques complexes (dont les systèmes ultra-sûrs d'Amalberti) ne puissent être basées que sur la seule considération du travail à accomplir ou des objectifs à atteindre pour faire face à des événements anticipés. Au contraire, la conception ou l'amélioration doit apporter des éléments d'adaptations aux changements et à l'apparition

d'événements non anticipés et spécialement celles et ceux qui ne peuvent pas être prédits lors de l'étude de conception ou de renouvellement. Ceci signifie que la conception ou le renouvellement de tels systèmes doit apporter suffisamment de flexibilité de sorte que les opérateurs puissent :

- reconfigurer leurs comportements ;
- modifier leurs activités ;
- construire de nouvelles activités ;
- générer de nouvelles procédures à la demande [**108**].

4.2.3. Le modèle de sécurité écologique. — La psychologie écologique ou la sécurité écologique [**9**] propose un cadre de conception du système automatisé permettant d'obtenir le meilleur équilibre cognitif. Cet équilibre sera d'autant plus juste que l'allocation des tâches entre l'homme et l'automatisme sera judicieuse. Il s'agit de ne pas tout automatiser, en ne laissant que des actions de routines à l'opérateur humain, mais de l'impliquer dans le procédé avec des tâches de plus haut niveau d'abstraction. Autrement dit, le degré de contrôle de la situation « situation awareness » par l'opérateur est un paramètre important pour la sécurité. Les modèles psychologiques en ingénierie des facteurs humains ont pour objectifs de comprendre le travail réel des opérateurs notamment l'activité cognitive, comportementale et physique. Les méthodes et outils de cette discipline servent à comprendre comment l'opérateur gère les risques. L'analyse des erreurs par exemple fournit un indicateur d'évaluation, l'observation naturaliste [1] en est une autre.

La cognition située [**9, 73**] développe l'aspect contextuel de la situation de travail. Deux possibilités permettent l'analyse de la cognition située : (1) l'observation naturaliste (in situ), le travail humain est analysé dans son contexte réel. Ceci n'est pas toujours réalisable compte tenu du biais et de la gêne occasionnée par la présence d'observateurs. (2) L'observation simulée (in vitro) consiste à reproduire le contexte à l'aide de simulations. Cette dernière possibilité offre l'avantage de contrôler pleinement l'analyse, mais il faut se poser la question du réalisme de la simulation. L'évaluation cognitive, outre l'aspect d'évaluation de la prise de risque, permet de concevoir des systèmes hommes-machines performants, en distribuant les tâches en fonction de la compétence de chacun. Du point de vue de la psychologie écologique [**9**], il ne faut pas tenter de supprimer toutes les erreurs humaines, la composante humaine a besoin de faire des erreurs ne serait-ce que pour auto-évaluer son évolution dynamique. L'opérateur doit être capable à tout instant de comprendre la situation du procédé grâce à son interaction avec le système [**9**]. Ainsi la deuxième démarche consiste à fournir à l'opérateur une aide interactive, débrayable, apportant des informations sur la situation de façon à ce qu'il soit un participant et non un attendant. Cette aide doit interagir avec sa logique cognitive.

Dans le domaine ferroviaire, notamment dans la supervision de trafic, on remarque que l'opérateur n'est pas seulement un attendant comme on pourrait le supposer sur la base des observations des évolutions des tâches qui deviennent de moins en moins complexes. En réalité, la tâche augmente de niveau dans la hiérarchie d'abstraction, elle devient de plus en plus cognitive. Le superviseur de trafic ferroviaire doit se forger mentalement un modèle représentatif d'une situation éloignée dont il ne dispose que d'une vision partielle au travers de synoptiques et de

1. C'est une méthode qui vise à étudier un sujet dans son état et/ou dans son environnement naturel. Le chercheur qui effectue ce genre de recherches évite que le sujet remarque qu'il est observé, cela pourrait en effet modifier son comportement.

variables abstraites. Sa seule façon de gérer le risque consiste à comprendre et à s'adapter en temps réel à la situation afin de mieux anticiper tous les changements potentiels. La représentation de la situation repose sur l'information délivrée par l'interface. Cette information présente trois caractéristiques. Premièrement, la fiabilité qui désigne la conformité de l'information avec le terrain. Deuxièmement, l'efficacité de cette information fournie par l'IHM pour la représentation de la situation. Enfin, troisièmement, la qualité de la représentation externe qui représente la capacité de l'information affichée par l'IHM à donner du sens pour permettre d'élaborer des connaissances. La représentation externe est un support à la représentation interne de l'opérateur. En d'autres termes, plus la qualité de la représentation externe de l'information délivrée par l'IHM est bonne, moins l'opérateur doit rechercher de l'information pour réactualiser sa représentation de la situation et plus les actions à entreprendre sont évidentes (routines dans la hiérarchie d'abstraction de Rasmussen). Ces trois propriétés déterminent l'efficacité de l'interface homme-machine.

4.3. Prise en compte du facteur humain dans l'évaluation de la sécurité

Les études probabilistes du facteur humain (EPFH) ont été développées dans les années soixante pour estimer de façon qualitative et quantitative les erreurs humaines dans les postes de travail en interaction avec des opérateurs humains. Les premières méthodes reposaient sur l'évaluation classique de la fiabilité d'un composant matériel (telle que présentée précédemment). L'EPFH est une discipline particulière qui allie l'expérience de plusieurs disciplines : la psychologie, l'ergonomie, l'ingénierie et la sûreté de fonctionnement. La définition de la fiabilité humaine est donnée dans [**98**] :

***Définition 4.1* (Fiabilité humaine).** — C'est la probabilité qu'une tâche ou un travail soit accompli avec succès par une personne dans un temps requis si une exigence temporelle est nécessaire.

L'EPFH est une méthodologie permettant d'évaluer la fiabilité humaine. L'estimation de cette probabilité consiste à l'évaluation statistique ou subjective de la probabilité d'erreur humaine (PEH). Le modèle d'EPFH repose sur un modèle d'accident (présenté au paragraphe 3.3).

L'analyse de facteur humain (Human Reliability Analysis) est un cadre méthodologique plus général regroupant les analyses probabilistes et purement qualitatives de la fiabilité humaine. Certaines proposent une évaluation quantitative de la fiabilité humaine tandis que d'autres proposent une évaluation ergonomique, psychologique ou organisationnelle en fournissant des recommandations pour améliorer le cadre de travail en vue de la sécurité.

Il existe une grande quantité de méthodes d'analyse du facteur humain, autant que de domaines d'application (nucléaire, chimique, trafic aérien, trafic maritime, *etc.*) et que de modèles d'accident[**27, 68**]. Enfin, les niveaux d'application des EPFH ne sont pas les mêmes, certaines méthodes s'appliquent au niveau individuel (action et psychologie), d'autres aux niveaux organisationnel et politique. [**27**] propose une classification des principales méthodes EPFH basée sur le niveau d'application et le modèle d'accident sous-jacent. Pour une revue détaillée des différentes méthodes EPFH, le lecteur intéressé pourra se reporter à [**45**] et [**52**], les auteurs de cette dernière référence ont également synthétisé dans l'ouvrage les tables des valeurs quantifiées par les différentes méthodes.

4.3.1. Modèles issus des sciences de l'ingénieur. —

4.3.1.1. THERP. — La première méthode utilisée appelée THERP (*Technique For Human Error Rate Prediction* [**120**]) est une méthode centrée sur l'opérateur (niveau individuel) dite de première génération en raison du modèle séquentiel d'accident sur lequel il repose. La méthode consiste dans un premier temps à identifier les missions du facteur humain dont la défaillance conduit à l'événement redouté. Cette étape est effectuée à l'aide d'une analyse AMDEC. Il s'agit ensuite de décomposer les tâches de l'opérateur en enchaînement d'actions élémentaires sous la forme d'un arbre d'événements (voir figure 4.2). Chaque nœud de l'arbre représente une action élémentaire pouvant être accomplie avec succès ou bien échouer, générant ainsi deux branches de l'arbre. La probabilité d'échec d'une action élémentaire est fournie par une base de données élaborée par les inventeurs de la méthode THERP [**120**]. La probabilité d'échec d'une action élémentaire est adaptée au contexte à l'aide de facteur correctif appelé facteur de contexte (*Performance Shaping Factor–PSF*). Il est possible d'appliquer un modèle de dépendance au scénario d'actions ainsi modélisé à l'aide de probabilités conditionnelles. Enfin le calcul proprement dit de la fiabilité humaine de la mission considérée est effectué par combinaison des probabilités élémentaires. Cette méthode est particulièrement bien adaptée aux études probabilistes de sécurité car utilise le même modèle mathématique. Cependant ce modèle n'est pas réellement représentatif de la nature de l'action humaine, de plus les données fournies par la méthode sont dépendantes du contexte mais aussi du domaine d'activité (la méthode à été élaborée pour l'industrie nucléaire militaire et civile). Olivier Straëter [**119**] rappelle que les données probabilistes sont encore spéculatives tant qu'aucune étude de validation des valeurs n'aura été réalisée.

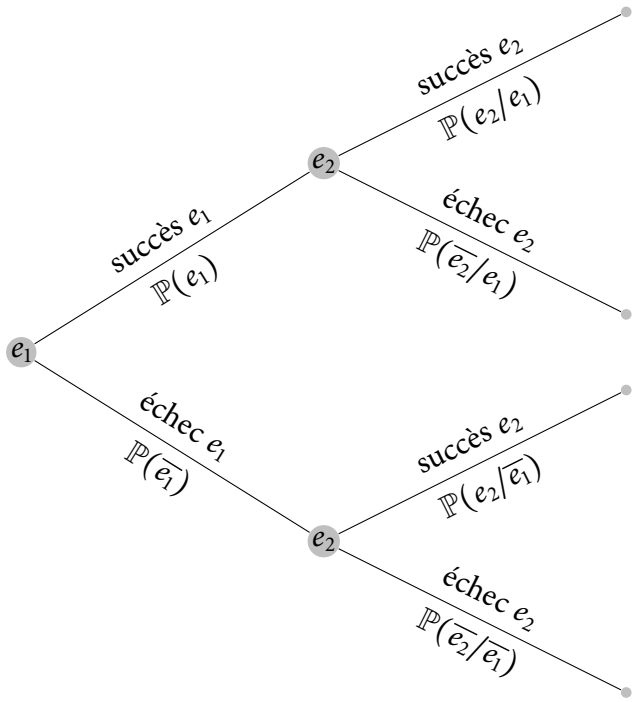


FIGURE 4.2. Arbre THERP

4.3.1.2. Le modèle HCR. — Le modèle *Human Cognition Reliability* (HCR) [**59, 60, 101**] a été conçu pour prévoir la probabilité qu'une équipe en salle de contrôle d'une installation industrielle réponde à un événement majeur dans un temps donné. Le modèle HCR calcule la probabilité de succès (ou d'échec) de l'équipe en fonction du temps et du type de comportement humain requis. Le modèle repose sur l'hypothèse que la probabilité de succès de réaction à un événement dépend essentiellement du temps disponible avant l'accident et du type d'activité cognitive requis. Le modèle peut également intégrer certains facteurs de contextes influençant le temps de réponse des opérateurs. Le modèle SRK de Rasmussen [**107**] est utilisé pour déterminer la probabilité de succès de la mission des opérateurs, selon le type de comportement, basé sur les habiletés, sur les règles ou sur les connaissances, différentes courbes de probabilité sont établies.

4.3.1.3. La méthode ACIH. — La méthode d'analyse de la fiabilité humaine développée par F. Vanderhaegen [**124, 125**] propose une alternative à l'évaluation probabiliste du facteur humain dans les études de sécurité. La méthode se nomme ACIH, acronyme d'« Analyse des Conséquences de l'Infiabilité Humaine ». Elle comprend à la fois une analyse prospective appelée APRECIH et rétrospective appelée APOSCIH. L'objectif d'ACIH est de déterminer les conséquences des scénarios dans lesquels le comportement des opérateurs humains se dégrade.

Cette méthode permet d'évaluer les conséquences de l'infiabilité des opérateurs humains sur les performances du système homme-machine. La méthode ne propose pas de quantification de la fiabilité humaine et s'en écarte volontairement en précisant les limitations d'un tel calcul. La méthode est inductive, elle cherche à déterminer les conséquences d'un ou d'une succession d'événements. La logique de propagation des effets de la dégradation du comportement des opérateurs humains repose sur un modèle cognitif simplifié issu du paradigme « SRK » développé par Rasmussen [**107**]. Ce modèle de la cognition résume l'activité de l'opérateur à trois activités cognitives : L'acquisition de données, le traitement de l'information et l'action. Ainsi, l'échec ou l'omission d'une tâche à réaliser sont imputés à la défaillance de l'une de ces activités.

La méthode d'analyse des conséquences de l'infiabilité humaine étant inductive, sa représentation peut être donnée dans un arbre de conséquences ou arbre d'événements. L'établissement de cet arbre suit trois étapes :

- analyse fonctionnelle du système : permet de définir à partir de l'objectif global, la liste des fonctions permettant de le réaliser. Les fonctions allouées aux opérateurs humains sont appelées procédures. Plusieurs procédures peuvent être mises en œuvre pour réaliser une fonction ;
- analyse des procédures dans leur contexte : chaque procédure étant réalisée différemment selon le contexte dans lequel elle est réalisée, cette étape permet d'une part de collecter l'ensemble des contextes possibles pour chaque procédure et de déterminer l'ensemble des tâches à réaliser pour effectuer chaque procédure dans chaque contexte.

Enfin, l'analyse des conséquences proprement dite consiste à construire l'arbre des conséquences possibles d'une procédure dans un contexte particulier. Le développement de l'arbre suit l'ordre de réalisation des tâches. La racine correspond à la première tâche à réaliser. En fonction de la nature du traitement humain employé pour effectuer la tâche (acquisition, traitement ou action) différentes issues sont envisageables créant autant de nouveaux nœuds au niveau de la tâche suivante. Les issues envisageables sont celles proposées par le modèle cognitif, à savoir la

bonne réalisation de la tâche, la réalisation incorrecte de la tâche ou bien la non-réalisation de la tâche.

4.3.2. Vers une intégration des sciences humaines et sociales. — Les dernières méthodes HRA dite de deuxième génération sont basées sur le modèle systémique d'accident et intègrent un modèle de la cognition permettant de s'affranchir de l'approximation des premiers modèles. La méthode MERMOS développée par EDF [**93**] prend en compte la structure organisationnelle des systèmes sociotechniques, la méthode se fonde sur la longue expérience d'EDF en la matière, notamment sur une base efficace de retour d'expérience. MERMOS est à la fois qualitative et quantitative (intégration des résultats probabilistes dans les EPS). Dans le secteur aérien, la méthode AMSMA [**27**] développé par EUROCONTROL ou encore la méthode CREAM (*Cognitive Reliability and Error Analysis*) [**71**] s'appuie sur un modèle de la performance humaine en interaction avec son environnement. CREAM propose un modèle de la cognition utile à la fois pour réaliser des études rétrospectives et prospectives d'accident. La particularité de CREAM réside dans le fait que les erreurs humaines sont plus conditionnées par le contexte que par un phénomène aléatoire.

À titre d'illustration, la méthode MERMOS et la méthode CREAM sont présentées plus en détail.

4.3.2.1. La méthode MERMOS. — La méthode a été développée par EDF [**83, 93**] pour actualiser la démarche d'évaluation des missions des opérateurs en conduite accidentelle dans les analyses probabilistes de sûreté nucléaire EPS_N. La méthode ne s'applique pas aux événements humains de type initiateur et préinitiateur. L'introduction de procédures informatisées dans les centrales nucléaires du palier N4 a notamment motivé cette actualisation. Les démarches de l'évaluation du facteur humain présenté ci-avant étaient basées sur une activité différente des opérateurs (procédures papiers) dans la salle de conduite.

La défaillance de la mission peut survenir par plusieurs scénarios d'échecs indépendants (qu'il faudra quantifier). L'évaluation probabiliste est donnée par la formule suivante :

$$\mathbb{P}\left(\text{Défaillance Mission FH}\right) = \sum_i \mathbb{P}\left(\text{Scénario}_i\right) + \mathbb{P}_{\text{résiduelle}}$$

où $\mathbb{P}_{\text{résiduelle}}$ est la probabilité des scénarios d'échecs inimaginables par l'analyste. Ceci confine la probabilité de défaillance de la mission FH à une valeur minimale limite. En effet, les limites de la modélisation des scénarios pourraient conduire à évaluer une probabilité optimiste voire nulle.

La première démarche consiste à définir et analyser la séquence accidentelle de l'arbre d'événements de l'EPS considéré. L'analyse fonctionnelle des exigences requises permet de déterminer les missions de sauvegarde à mettre en œuvre par le système pour rétablir les fonctions nécessaires au recouvrement des conséquences inacceptables. Cette analyse qualitative des séquences accidentelles a pour objectif d'identifier **les actions importantes** de l'équipe de conduite durant le déroulement du scénario accidentel. Ces actions importantes sont reformulées en termes d'objectif de conduite par les **missions facteur humain (FH)**. La méthode liste trois catégories possibles de mission FH pour les scénarios accidentels de conduite d'une centrale nucléaire :

– le rétablissement d'une fonction de sécurité ;

– la récupération d'une perte de système ;
– la non-réalisation d'une action inopportune.

Lorsque les missions FH sont identifiées, elles sont définies et analysées en profondeur par l'analyse du requis puis celle de la conduite prescrite et par l'examen du retour d'expérience et des essais sur simulateur. Cette étape est achevée par la rédaction des fiches de mission FH synthétisant les informations relatives à chaque mission identifiée (études physiques des phénomènes engagés, logique de conduite, hypothèses de travail, *etc.*).

L'analyse qualitative et quantitative des missions FH forme la deuxième étape de la méthode. Le modèle de réalisation des missions est systémique. L'idée principale de la méthode considère que la conduite émerge de l'interaction entre le système de conduite et le concept de Configuration Importante de la Conduite Accidentelle (CICA) voir définition 4.2.

Définition 4.2 **(CICA,** [**93**]**).** — « Décrit une inertie temporelle du système déterminant une configuration des ressources et une orientation de la conduite générant les actions adéquates, sélectionnant et priorisant les informations pertinentes à surveiller, et écartant les autres actions non prioritaires ou contraires à l'orientation choisie ainsi que les informations moins pertinentes dans le contexte. »

Le concept de CICA a été introduit pour extraire l'analyse des modèles de relations causales de l'enchaînement des événements dans le scénario qui ont été utilisés intensivement dans les méthodes HRA de première génération (méthode des arbres de défaillance notamment). En lieu et place d'une relation de cause à effet, le concept de CICA fournit « un modèle explicite de rationalité de conduite au niveau du système de conduite » [**93**, page 105].

L'intérêt d'utiliser la méthode MERMOS pour la conduite de scénarios accidentels relatifs aux postes de supervision de trafic ferroviaire n'est pas de prime abord pertinent. Les raisons permettant d'affirmer ce constat sont les suivantes :

– La **dimension temporelle** des scénarios transitoires accidentels est beaucoup plus longue dans le cas de la conduite d'une chaudière nucléaire que dans le cas de la gestion du trafic ferroviaire (45 minutes pour l'accident de Three Miles Island contre quelques minutes pour les accidents majeurs du chemin de fer impliquant le poste de supervision de trafic, Gare de Lyon 1988 : 1min30s et Ladbroke Grove 1999 : 33s, l'agent circulation a entrepris une action de sauvegarde 20s après le moment où la situation accidentelle était visible sur son écran de contrôle) ;
– Il en résulte une **activité cognitive très différente**. La conduite d'une centrale nucléaire requiert des connaissances théoriques en physique (thermodynamique, chimique, neutronique et mécanique) importantes pour maîtriser les procédures de conduite accidentelle d'un réacteur. Les procédures d'urgence d'un poste de supervision de trafic ferroviaire sont plus simples sur le plan théorique mais requièrent une attention particulière. D'autre part les variables représentatives nécessaires à la conduite de la chaudière nucléaire sont continues tandis que les variables surveillées par l'agent circulation sont discrètes (occupation de circuit de voie, état des matériels).
– Dans les deux cas, les opérateurs sont obligés de se forger une représentation distale (indirecte et éloignée) du procédé.

4.3.2.2. La méthode CREAM. — MERMOS est une méthode dédiée à l'activité de conduite accidentelle d'un réacteur nucléaire. La méthode CREAM [**71**] est plus générale, elle permet de couvrir toutes les activités humaines.

CREAM se fonde sur une classification du mode de contrôle de la cognition (*COntextual COntrol Model–*COCOM) [**71**] (voir tableau 4.2) et divers facteurs de contexte liés aux technologies, à l'environnement direct de l'opérateur et de l'organisation. Un questionnaire relatif au facteur de contexte (neuf au total, voir table 4.1 permet d'établir le mode de contrôle associé à la mission. Le mode de contrôle, associé à un type de fonction cognitive permet d'évaluer la probabilité d'erreur sur la base de probabilité *nominale* d'erreur de la fonction cognitive dans un mode de contrôle. Fujita et Hollnagel ont proposé une méthodologie alternative de quantification dans CREAM permettant de calculer un taux moyen d'erreur sans recourir à la notion d'erreur humaine [**48**]. Le lecteur intéressé pourra se reporter à [**78, 77, 96**] pour suivre les développements récents de cette méthode.

	Facteur de Contexte
(1)	Disponibilité des ressources
(2)	Entraînement et expérience
(3)	Qualité des communications
(4)	Qualité des interfaces opérateurs - machines
(5)	Accessibilité et disponibilité des méthodes et des procédures
(6)	Conditions de travail
(7)	Nombre d'objectifs simultanés
(8)	Temps disponible
(9)	Rythme circadien
(10)	Qualité de collaboration en équipe
(11)	Qualité et support de l'organisation

TABLE 4.1. Facteur de contexte CREAM

MERMOS et CREAM reposent sur un modèle cognitif de l'opérateur. Le génie cognitif a été développé par des ingénieurs conjointement avec les spécialistes des sciences humaines pour mieux appréhender la dynamique de l'homme au travail. Le génie cognitif permet de développer des modèles sur lesquels sont basées les études du facteur humain. La tendance actuelle cherche plutôt à tenter d'adapter le contexte de travail à l'homme pour utiliser au mieux sa variabilité de performance et ainsi gagner en sécurité.

4.4. Synthèse

Le tableau 4.3 synthétise les méthodes existantes, les études réalisées et permet de positionner la contribution de la thèse. le modèle SRK de Rasmussen a été fortement utilisé dans les méthodes de premières générations. Le modèle de sécurité écologique d'Amalberti n'a quant à lui pas été traduit en termes de méthode opérationnelle. Pourtant la deuxième génération de méthodes HRA qui vise à prendre en compte plus avant les caractéristiques d'un système vivant (humain ou organisationnel) peut être rapprochée avec le modèle d'Amalberti. Le concept de CICA sert

Mode de contrôle	Description
Mode erratique ou « brouillé » (scrambled)	Ce mode de contrôle correspond pratiquement à la panique de l'opérateur dans la réalisation de sa tâche. L'action de l'opérateur est imprévisible car complexe et se déroulant dans des conditions difficiles (situation d'urgence, manque de formation, *etc.*)
Mode opportuniste	Le mode d'action de l'opérateur est guidé par les caractéristiques les plus visibles du contexte et par les solutions les plus triviales qui lui sont proposées.
Mode tactique	L'action de l'opérateur repose plus ou moins sur une planification elle-même basée autant que possible sur les procédures prescrites.
Mode stratégique	L'opérateur s'appuie sur une planification avancée de la tâche à accomplir et à la prise en compte de ses conséquences.

TABLE 4.2. Modes de contrôle de la cognition COCOM

Méthode	Modèle	Quantification	Commentaire
THERP	SRK	Arbres d'événement	Utilisation d'une base de donnée de valeurs de probabilité pour chaque action de base.
HCR	SRK	Temps avant accident	Une courbe par type de comportement
ACIH	SRK	Méthode qualitative	Analyse qualitative des arbres d'événement
MERMOS	CICA	Jugement d'expert	Adapté à la conduite de transitoires accidentels d'unréacteur nucléaire
CREAM	COCOM	Scaling - possibiliste - crédibiliste	Méthode générique, ne prend pas en compte la dynamique de l'interaction entre l'homme et le système.

TABLE 4.3. Tableau de synthèse

de support au compromis cognitif, qu'Amalberti nomme conscience de la situation dans le domaine de l'aviation.

La démarche méthodologique des travaux qui ont été menés durant ce travail de thèse vise à intégrer plus avant l'étude du facteur humain par la mise en place d'expérimentations spécifiques à l'activité de supervision de trafic ferroviaire [**17**]. Nous ne nous démarquons pas des deux dernières méthodes présentées ci-avant, mais l'accent est mis sur le caractère interdisciplinaire de l'étude de sécurité. La difficulté majeure à relever tient de l'intégration des résultats de l'étude approfondie du facteur humain dans les études de sécurité. La technique proposée dans CREAM semble la plus pertinente, toutefois, il est nécessaire de trouver un référentiel commun aux disciplines des sciences humaines et sociales et celle de la sûreté de fonctionnement. D'autre part, la sûreté de fonctionnement exige une modélisation permettant d'expliquer l'apparition

des accidents. La modélisation utilisée dans cette thèse se démarque des méthodes basées sur les modèles séquentiels et épidémiologiques d'accident et utilise à la place un modèle systémique (voir section 3.3.4 page 72). La démarche est présentée dans le chapitre suivant.

Deuxième PARTIE

CONTRIBUTIONS

CHAPITRE 5

DÉMARCHE MÉTHODOLOGIQUE

Résumé

Ce chapitre présente la démarche méthodologique réalisée pendant cette thèse afin de proposer une méthode d'évaluation des facteurs humains en situation de supervision automatique d'un poste ferroviaire du type ATS.

5.1. Le projet SPICA-RAIL

La thèse s'inscrit dans le projet SPICA-RAIL « Supervision PICArde de transport par RAIL » [**13**] soutenu par la région Picardie et le ministère de la Recherche et de l'Enseignement supérieur. Ce projet a pour but d'évaluer l'impact des nouveaux systèmes de supervision de trafic ferroviaire sur la sécurité. Il a été mené en collaboration avec ALSTOM Transport spécialiste des systèmes de supervision de trafic ferroviaire, la société Sigma-Conseil experte en exploitation de système de transport ferroviaire, la société Bureau-Veritas organisme spécialisé dans les audits de sécurité et agréé pour la certification de sécurité des systèmes ferroviaires, l'Université de Picardie Jules Vernes (UPJV) spécialiste dans la recherche en psychologie et ergonomie cognitive et enfin l'Université de Technologie de Compiègne UTC (pilote du projet) spécialisée dans la recherche en sûreté de fonctionnement des systèmes ferroviaires. Outre l'apport des partenaires industriels qui garantissent le caractère pragmatique du projet, la collaboration de chercheurs en sciences humaines et en ingénierie de sûreté de fonctionnement apporte un point de vue interdisciplinaire dans la recherche d'amélioration des études de sécurité afin de prendre en compte le facteur humain.

Deux travaux importants ont été menés dans ce cadre, l'un concerne l'état de l'art industriel approfondi des systèmes de supervision, transversal à plusieurs domaines industriels et comprenant évidemment la supervision de trafic ferroviaire. La deuxième activité de ce projet a consisté à intégrer une plateforme de supervision de trafic ferroviaire dans un environnement simulé, cette plateforme porte le même nom que le projet qui a permis de la développer : SPICA-RAIL. Toujours dans le cadre de ce projet des expériences sur le comportement des opérateurs humains en situation de supervision de trafic ont été menées. Les scénarios et l'objet de ces expériences ont été élaborés grâce à l'état de l'art industriel approfondi et validés par le collaborateur Sigma-Conseil par son expérience en matière d'exploitation de système ferroviaire.

La démarche de la thèse s'appuie sur ce projet, et inclut ces deux travaux.

5.2. Démarche méthodologique

La démarche est synthétisée dans la figure 5.1.

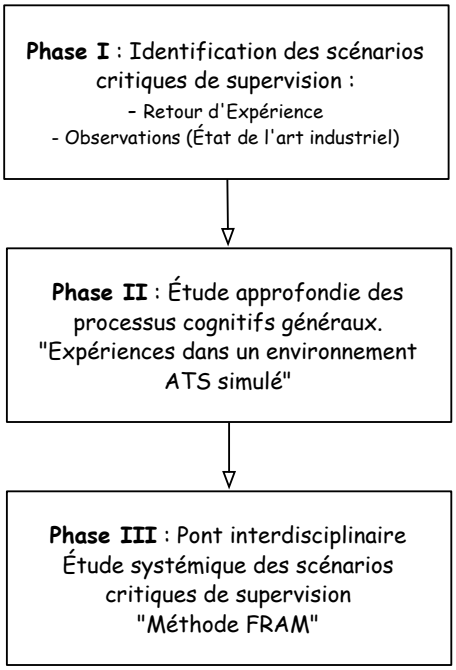


FIGURE 5.1. Démarche méthodologique

L'état de l'art industriel approfondi a permis de comparer l'activité de supervision dans différents domaines industriels avec un regard tout particulier sur ces situations de supervision critiques [**21, 15, 20**]. Le retour d'expérience et l'analyse d'accidents dans le domaine ferroviaire ont également permis d'identifier ces scénarios en focalisant l'étude sur le rôle des opérateurs de supervision de trafic dans l'accident. Reprenant les données de cet état de l'art, la thèse propose un modèle des modes d'exploitation permettant d'identifier les situations critiques de sécurité dans lesquelles l'opérateur de supervision dispose d'un rôle déterminant. Il s'agit de classer les contextes du système, nommés modes d'exploitation, en fonction de la dégradation du niveau de sécurité du système. De sorte, qu'il soit possible d'identifier les scénarios du système susceptibles de transformer l'activité de l'opérateur humain, de superviseur (la plupart du temps passif) en un contrôleur actif ayant une responsabilité directe de la sécurité. Ces scénarios sont appelés « scénarios de supervision critique » et peuvent être classés en deux catégories selon les deux situations suivantes :

– Lorsque le système de supervision permet d'agir directement sur les barrières de sécurité. Le système de supervision devient temporairement un système de contrôle commande du système de protection ;
– Lorsque l'opérateur, bien que normalement pas directement responsable de l'évolution et du contrôle d'une situation dangereuse, a la possibilité de récupérer cette situation. L'ingénierie de la résilience développée par Leveson, Woods et Hollnagel [**70**] ainsi que les travaux d'Amalberti [**9**] offrent un regard nouveau sur ce sujet. Il s'agit de ne plus

considérer l'opérateur humain comme un acteur faillible dans les études de sécurité, mais de prendre en compte sa forte capacité d'anticipation et d'adaptation.

Cet état de l'art a été utilisé pour évaluer le comportement d'opérateurs humains en situation de supervision de trafic ferroviaire, notamment pour le choix et la définition des scénarios. L'accent a été mis sur la détection et l'anticipation d'une situation dangereuse.

D'une manière générale, peu d'études de psychologie ergonomique cognitive ont été appliquées à la gestion de trafic ferroviaire ; Alors que de nombreuses études ont été appliquées dans le domaine des transports [**137**]. Quelques études ont toutefois été réalisées dans le domaine du transport ferroviaire, mais spécifiquement sur les problèmes de vigilance et de perception des signaux chez les conducteurs de trains. Alors que ces dernières études ont permis d'élaborer des modèles de l'opérateur de conduite de train, il n'existe pas à ce jour de modèle spécifique à l'opérateur chargé de la gestion du trafic.

Pourtant, la centralisation de la commande ferroviaire conduit à de profonds bouleversements dans cette activité. L'apparition de nouvelles technologies que l'opérateur doit maîtriser, l'automatisation de nombreuses tâches, apparitions de nouvelles contraintes économiques qui pèsent de plus en plus sur la conception du système ferroviaire nécessitent indéniablement la prise en compte du facteur humain. Ces changements ont pour objectifs d'utiliser de façon optimale l'infrastructure ferroviaire dans un souci de rendement d'exploitation qui s'exprime par le nombre de trains à faire circuler par unité de temps tout en garantissant un niveau de sécurité très élevé [**89**].

Des études spécifiques du facteur humain ont donc été réalisées sur la plateforme SPICA-RAIL [**22, 24, 18**]. Installée dans les locaux de l'UTC. L'objectif des expérimentations est d'obtenir des informations sur les processus cognitifs généraux impliqués dans la gestion d'un environnement dynamique de circulation de mobiles et de contribuer ainsi à l'évaluation du système ATS lorsque les opérateurs sont confrontés à la gestion d'une situation nominale, normale et dégradée. Les résultats forment un ensemble d'hypothèses validées ou invalidées par l'expérience, et une description qualitative de l'activité cognitive au travail préconisant des recommandations sur l'environnement de travail.

La difficulté d'une telle démarche demeure l'intégration des résultats obtenus par l'observation et les techniques de la psychologie ergonomique cognitive dans l'étude de sécurité.

Les techniques classiques de sûreté de fonctionnement telle que la technique des arbres de défaillance ou celle des arbres d'événement réduisent l'activité humaine et organisationnelle à des événements ponctuels avec des modes de défaillances binaires qui ne sont pas représentatifs de la réalité. De plus, les événements humains ou organisationnels sont difficilement mesurables en termes de probabilité d'occurrence avec la validité scientifique de la psychologie cognitive ou des sciences sociales.

Pour pallier ce manque, la thèse propose d'établir un pont interdisciplinaire permettant d'intégrer les résultats d'études spécifiques aux facteurs humains et organisationnels, et cela, grâce à une modélisation systémique des accidents [**19**]. Les scénarios sont représentés dans un modèle commun aux spécialistes de la sûreté de fonctionnement et aux spécialistes de la psychologie cognitive qui sont chargés d'analyser en détail le comportement des opérateurs en situation. La méthode FRAM développée par Hollnagel [**68**] est toute indiquée, elle permet de visualiser sur un même graphique les interactions complexes qui ont lieu à l'intérieur du

système sociotechnique, d'effectuer une étude de la variabilité de performances des fonctions associées au scénario et ainsi de visualiser la propagation d'une mauvaise performance sur l'ensemble de l'activité. En focalisant l'objet de l'étude sur les fonctions du système plutôt que sur sa structure, le modèle FRAM permet de représenter une fonction technique, une activité humaine ou organisationnelle dans un même formalisme. Le raisonnement causal basé sur le principe de résonance fonctionnelle (emprunté à la résonance stochastique en traitement du signal) permet de prendre en compte des modes de défaillances de l'activité adaptés aux opérateurs humains, et aux organisations. L'issue de cette modélisation fournit des hypothèses concernant le comportement des opérateurs de supervision grâce aux modes de défaillances potentiels identifiés.

5.3. Conclusion

La démarche proposée est constituée de trois phases. Le chapitre 6 présente l'état de l'art industriel approfondi constituant la première phase de la démarche. Le chapitre 7 décrit les expériences qui ont été menées sur la plateforme SPICA-RAIL objet de la deuxième phase. Le chapitre 8 décrit le modèle interdisciplinaire s'appuyant sur la méthode FRAM, l'application de ce modèle est illustrée au travers de deux cas d'étude dans le chapitre 9 [**19, 24**].

CHAPITRE 6

ÉTAT DE L'ART INDUSTRIEL APPROFONDI

Résumé

Ce chapitre présente l'état de l'art industriel approfondi constituant la première phase de notre démarche d'évaluation du facteur humain en situation de supervision. En guise d'introduction, une définition de l'activité de supervision est proposée. La section suivante dresse la liste des installations industrielles qui ont été visitées. La présentation des informations collectées est organisée en deux parties. L'approche système fait l'objet de la première partie. Il s'agit de décrire le rôle de la supervision dans l'exploitation des différentes installations. Dans cette perspective, un modèle des modes d'exploitation des installations industrielles a été développé. Il permet de comparer les installations visitées et d'identifier le rôle pris par la supervision lorsque la sécurité se dégrade. La deuxième partie vise à préciser la nature des actions entreprises depuis le poste de supervision. À l'aide d'une définition duale de la sécurité s'appuyant sur les récents travaux de l'ingénierie de la résilience [70], deux types d'actions sont envisagés et illustrés à l'aide des installations visitées. Le chapitre conclut par l'identification des situations de supervision critiques pour la sécurité.

6.1. Introduction : définition de la supervision

La supervision couvre un large éventail d'applications industrielles hétérogènes. Des procédés industriels au contrôle de trafic en passant par les hautes technologies.

À l'origine, le terme supervision décrit la nature de la relation entre un subordonné et son supérieur hiérarchique. Étymologiquement, la supervision représente la « vue d'en haut » : du latin *super* (au-dessus) et *videre*. Les dictionnaires de la langue française définissent la supervision par l'action couplée de surveiller et de contrôler sans entrer dans les détails. La théorie de l'automatique s'intéresse à deux catégories de supervision, l'une relative à un superviseur automatique et l'autre à un superviseur humain.

6.1.1. Théorie du contrôle. — La première catégorie relève de la théorie du contrôle. Celle-ci classe les processus industriels selon l'espace d'état des variables représentatives du processus. Les variables représentatives aussi appelées variables d'état permettent de mesurer l'état physique du processus. Dans le cas où toutes les variables représentatives du processus reposent sur un domaine discret, le processus est dit « discret ». Dans le cas où tous les domaines de définition

des variables sont continus, le processus est dit « continu ». Il existe également une classe de processus hybride représenté par des variables discrètes et continues. Dans le contexte de processus discrets, [**104**] ont élaboré une théorie formelle de la supervision. Le processus est modélisé par un graphe d'états–transitions appelé « automate à états finis » dans lequel les transitions sont étiquetées contrôlables ou non contrôlables. Les actions exercées sur le processus sont modélisées par un autre automate à états finis appelé superviseur qui a la possibilité de neutraliser les actions contrôlables afin de satisfaire les spécifications de fonctionnement. En d'autres termes, le superviseur automatique d'un processus à événements discrets agit sur les transitions contrôlables du processus dans le but de restreindre le comportement du procédé au sous-ensemble des trajectoires possibles autorisées.

6.1.2. Supervision humaine. — La branche de l'automatique qui s'intéresse à cette classe de processus supervisé par des humains est appelée « Automatique Humaine » traduction de *Human Engineering*. Une présentation détaillée et un historique de cette discipline peuvent être trouvés dans les ouvrages de P. Millot [**100**] et T. Sheridan [**115**].

Le modèle introduit par Sheridan [**116**] permet de représenter le travail de l'opérateur humain en situation de supervision (voir figure 6.1). Le procédé est constamment mesuré par des capteurs. L'information mesurée est acheminée vers les automatismes représentés par le système de contrôle commande qui agit de façon autonome sur le procédé et le système d'assistance à la supervision (ou supervision automatique) qui organise et simplifie le travail de l'opérateur de supervision. L'opérateur peut alors préparer des ordres d'actions qu'il transmet via les contrôles du système de supervision automatique aux automates (système de contrôle commande) qui se chargent de faire exécuter la commande par les actionneurs.

Le système de contrôle commande réalise de plus en plus de fonctions (relevant autrefois de la tâche de l'opérateur de supervision). Le système de contrôle commande, d'une manière générale, a permis de remplacer l'opérateur humain de la boucle de contrôle partout où les contraintes technologiques échappent à la performance humaine. Ces contraintes sont les suivantes :

- Capacité physique ;
- Capacité de calcul ;
- Gestion du temps (synchronisation à la micro seconde) ;
- Capacité de mémorisation ;

À ceci s'ajoutent les contraintes visant à améliorer la situation de travail de l'opérateur, principalement la suppression des tâches répétitives, source d'erreur et d'ennui.

D'une manière générale, l'automatisme remplace l'opérateur dans les tâches où la performance humaine atteint ses limites. Si l'on considère l'ensemble des actions qu'il est possible de réaliser et que l'on y retranche celle que l'humain ne peut réaliser à cause des limites physiques et physiologiques, on obtient alors l'ensemble des tâches nécessairement automatisables. Une deuxième classe d'actions relève d'une performance humaine suffisante, mais ayant pour issue une variabilité de performance trop importante pour assurer l'action de façon régulière et/ou stable. Ces tâches sont potentiellement automatisables. Les actions restantes sont les tâches réalisables par l'opérateur humain. La frontière entre tâches potentiellement automatisables et tâches réalisables est à la fois mince et subjective. Cette frontière dépend de la régularité et de la stabilité de la mission à exécuter. Le livre de P. Millot [**99**] propose une démarche d'allocation des tâches entre les automatismes et l'opérateur humain.

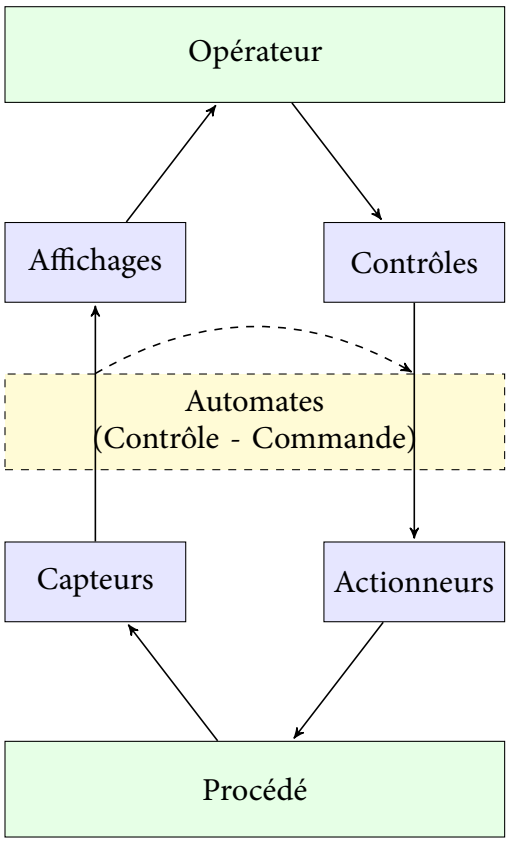


FIGURE 6.1. Aspect général de la supervision (d'après [**116**])

L'activité de supervision est née du besoin de surveiller les tâches nécessairement automatisables, mais représente également une tâche potentiellement automatisable. Ainsi, les systèmes d'assistance à la supervision appelés également systèmes de supervision automatique fournissent une aide à l'opérateur dans la réalisation de sa tâche de supervision. Ce système prépare et organise le travail de l'opérateur en lui proposant d'exécuter des séquences d'actions que l'opérateur choisit ou non de déclencher.

Les outils d'affichage ont un rôle primordial, ils sont la principale source d'information de l'opérateur. Ces outils sont en général des écrans de contrôle, des tableaux de contrôle optiques, et dans une plus large mesure aujourd'hui des postes informatiques individuels.

En ce qui concerne le travail de l'opérateur, [**116**] décrit la tâche de supervision par une séquence de cinq activités régies par trois boucles de contrôle, voir la figure 6.2. Dans un premier temps, le superviseur doit **planifier** son travail. La planification regroupe l'ensemble des principes et méthodes permettant d'établir le programme de l'activité et d'en préparer l'exécution. Il s'agit de répondre à la question suivante : Quelles tâches seront à réaliser et comment les réaliser ? L'activité suivante consiste à **intégrer** le planning dans le système automatisé. La troisième activité de l'opérateur de supervision, celle dans laquelle il passe le plus de temps, consiste à **surveiller** la bonne exécution des tâches conformément au planning. Il s'agit d'observer le procédé, d'analyser les observations afin d'anticiper la conduite à suivre en cas d'écart par rapport au planning. En cas d'apparition d'événements indésirables impliquant un écart trop important dans le planning (non récupérable par les automatismes), le superviseur doit **intervenir** sur

le procédé. L'opérateur doit alors conduire le procédé de façon à le recaler sur le planning et ainsi réactiver le système de contrôle commande. Lorsque cette tâche est impossible, ou bien lorsque la sécurité l'impose, l'opérateur conduit le procédé dans un état de repli où la sécurité est assurée. Cette activité est cruciale pour la sécurité, elle dépend fortement de l'activité précédente et de la capacité à anticiper les événements. De plus, l'entraînement des opérateurs à conduire le procédé en l'absence d'aide automatique est un facteur déterminant. Enfin, la dernière activité consiste à *apprendre* de l'expérience. La capitalisation d'expérience permet de mémoriser les scénarios qui n'ont pas été imaginés lors de la conception du système de supervision.

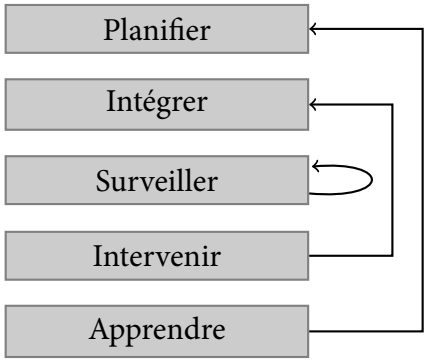


FIGURE 6.2. Les trois boucles d'actions de la supervision (d'après [**116**])

Sheridan complète ces cinq activités par trois boucles de contrôle. La première boucle contrôle l'activité de surveillance. Dans cette boucle, l'opérateur surveille le processus, détecte des événements, les analyse et diagnostique l'état du processus afin d'anticiper (voir table 6.1). Le résultat du diagnostic permet d'anticiper les actions et donc de décider s'il est nécessaire d'intervenir, le cas échéant une deuxième boucle de contrôle lie l'activité d'intervention avec celle d'intégration. Les événements perturbateurs et l'intervention directe de l'opérateur sur le procédé ayant conduit à modifier le planning, l'opérateur doit impérativement recalculer un nouveau planning et l'intégrer dans le système de contrôle commande. L'opérateur humain apprend de son expérience et prendra en compte le résultat de sa conduite face à des événements perturbateurs ou non prévus lors de la prochaine planification, c'est l'objet de la troisième boucle de contrôle.

Un superviseur est un opérateur humain qui surveille un système complexe et exécute par intermittence des actions de contrôle sur le procédé en agissant sur la couche d'automates du système de contrôle commande. L'activité de supervision consiste à recevoir des informations et à commander les automates via un pupitre de commande ou un poste informatique.

L'application du modèle de Sheridan à l'activité ferroviaire a été présentée dans [**15, 20**].

6.2. Liste des installations visitées

La première étape de notre démarche a consisté à réaliser un état de l'art industriel sur le rôle de la supervision industrielle pour la sécurité.

Des visites d'installations industrielles ont été réalisées entre mars 2005 et janvier 2006 dans le cadre du projet SPICA-RAIL afin de visualiser in situ les différents aspects de la supervision. Le détail des installations visitées est présenté dans le tableau 6.2. Un rapport technique a été

Activités	Descriptions
Surveiller	À partir des masses d'informations qui lui parviennent, l'opérateur suit l'évolution du système. Il vérifie notamment que les principaux paramètres sont conformes aux consignes d'exploitation et prend connaissance de tout changement d'état.
Analyser	La surveillance directe de l'état du système ne suffit pas pour garantir de bonnes conditions de sécurité, il faut aussi s'assurer que toute nouvelle situation issue d'un incident banal n'ait pas de conséquences excessives ou non maîtrisables. Grâce à des outils d'analyse ou de leur propre expérience, les opérateurs doivent vérifier qu'ils respectent l'ensemble des règles de sécurité.
Anticiper	Tout événement nouveau doit être intégré pour prévoir les différentes évolutions possibles du système. Dès que l'on s'écarte du programme prévisionnel, les opérateurs doivent apprécier les conséquences éventuelles et préparer les parades associées.

TABLE 6.1. La boucle de surveillance

rédigé pour le projet SPICA-RAIL [**63**], il contient les comptes-rendus des visites et des entretiens qui ont été menés ainsi qu'une synthèse des enseignements. Deux communications [**15**] (en français) et [**23**] (en anglais) présente la synthèse de cet état de l'art industriel.

Les systèmes de supervision visités se divisent en trois catégories :

(1) La supervision de procédés industriels utilisés dans les usines manufacturières, chimiques et de production d'énergie. Les procédés sont caractérisés par la nature des variables qui les représentent que l'on nomme l'espace d'état. Si celui-ci est un ensemble discret alors, le procédé est dit discret (ou batch), les usines manufacturières en sont un exemple. Si l'espace d'état est continu, le procédé est dit continu tel que la production d'énergie où la puissance varie selon une valeur continue ;

(2) La supervision de séquence de lancement de tir est une classe d'application utilisée dans le domaine de la défense ou des hautes technologies. Cela représente la classe des systèmes mono-coup comme le lancement d'une fusée spatiale nécessitant une phase de préparation organisée en séquences ;

(3) La supervision de trafic, le trafic étant un ensemble de mobiles se mouvant en une, deux ou trois dimensions. La supervision de trafic inclut deux notions : la gestion des circulations qui consiste à contrôler les itinéraires empruntés par les mobiles et la gestion de la régulation du trafic des mobiles qui consiste à maîtriser l'ordre, la fréquence ou les horaires des mobiles.

Ent.	Sites visités	Domaine	Procédé supervisé
CEA	LMJ (Laser Mega-Joules)	Haute technologie, défense, LASER, physique nucléaire	Mono-coup : séquence de tir LASER
CFF	PRCI Gare de Lausanne	Ferroviaire grande ligne	Circulations
	CGT	Ferroviaire grande ligne	Régulation de Trafic
DGAC	CRNA-Nord	Aviation civile	Circulations
EDF	CIPN	Centrale nucléaire	chaudière nucléaire et auxiliaires
RATP	PCC Bourdon	Ferroviaire métro	Circulation et régulation de trafic
	PCC RER A	Ferroviaire RER	Circulation et régulation de trafic
	PCC L14	Ferroviaire métro automatique	Circulation et régulation de trafic
	PCC L4	Ferroviaire métro	Circulation et régulation de trafic
SANOFI-AVENTIS	Usine de Vitry	Pharmaceutique	Réacteurs chimiques et auxiliaires
SNCF	PRCI Montparnasse	Ferroviaire grande ligne	Circulations
	PAR LGV Atlantique	Ferroviaire LGV	Circulations
Transpole	PCC Lille	Ferroviaire métro automatique	Circulation et régulation de trafic

TABLE 6.2. Présentation des visites

6.3. Approche système

L'approche système consiste à identifier le rôle de la supervision pour la sécurité. Afin de comparer les différentes installations visitées, un modèle général des modes d'exploitation a été élaboré. Pour chaque domaine industriel rencontré, le travail de veille a consisté à identifier les modes d'exploitation et le rôle du superviseur pour la sécurité dans chacun de ces modes.

6.3.1. Modes d'exploitation. — Quels que soient les dangers encourus, les modes de fonctionnement dans lesquels évoluent les systèmes dynamiques peuvent être classés en cinq catégories : Nominal, Normal, Stressé, Dégradé et Accidentel. Le mode nominal représente le fonctionnement tel que prévu théoriquement dans le planning d'exploitation et en ce sens ne constitue pas un mode d'exploitation, il permet néanmoins d'identifier l'activité théorique du superviseur. Les modes suivants sont quant à eux représentatifs d'une réalité d'exploitation. Le mode *normal* constitue le déroulement réel du planning d'exploitation faisant face à des perturbations *normales* d'exploitation. Nous introduisons un mode intermédiaire entre le nominal et le dégradé nommé *stressé* et rarement prévu dans les spécifications de conception des systèmes. Ce mode représente toutes les phases opérationnelles du système dans lesquelles il atteint les limites de son dimensionnement et de sa performance. Cela peut être un système en fin de vie ou exploité de façon intensive. Ce mode est générateur de *stress* pour les composantes du système techniques, mais aussi humaines. Le mode de fonctionnement *dégradé* inclut les phases de vie du système

subissant des défaillances ou en cours de maintenance et nécessitant une conduite particulière voire exceptionnelle. Le mode de fonctionnement *accidentel* constitue la phase critique où un événement dangereux ou catastrophique apparaît (la sécurité n'a pas été assurée). La dynamique du système contribue à dynamiser ce modèle en transitant d'un mode à l'autre. La sécurité peut être définie par les moyens mis en œuvre afin d'éviter les transitions vers l'état accidentel. La figure 6.3 décrit ce modèle, le mode nominal n'y figure pas car peu représentatif d'une réalité d'exploitation.

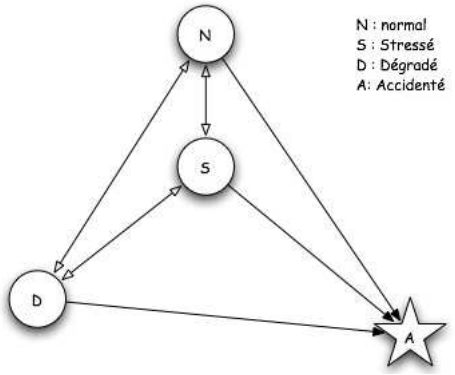


FIGURE 6.3. Modèle des modes d'exploitations

6.3.2. Conduite d'un réacteur nucléaire. — Cette visite a été effectuée au Centre d'Ingénierie du Parc Nucléaire en exploitation (CIPN) d'ÉDF. Cette unité de la Division Ingénierie Nucléaire (DIN) a en charge les études d'ingénierie de maintien en condition opérationnelle des centrales nucléaires des paliers [1] 900 et 1300 MWe selon les exigences de sûreté nucléaire [2], de radioprotection, d'environnement et de prévention sécurité.

Les opérateurs de conduite d'une tranche nucléaire [3] sont clairement identifiés comme responsables de la sûreté nucléaire. La salle de conduite de la tranche nucléaire est divisée en deux types de postes, ceux classés pour la sûreté nucléaire et les postes de supervision non classés pour la sûreté nucléaire.

6.3.2.1. Mode nominal. — Le mode nominal de conduite d'une tranche nucléaire correspond d'une part au planning d'exploitation de la tranche et à la prévision de consommation d'électricité du réseau calculé par EDF. Le planning de maintenance prévoit des arrêts de tranche pour rechargement du réacteur en combustible, des arrêts de maintenance préventive et des arrêts pour effectuer les visites d'inspection.

De fait, les opérateurs de conduite de la tranche ont des activités disparates selon que la tranche est en phase de puissance du réacteur nucléaire, en rechargement de combustible ou en maintenance.

1. Le palier est une classe de réacteur nucléaire.
2. La sûreté nucléaire est le terme utilisé dans le domaine nucléaire en France pour désigner la sécurité industrielle des dangers liés à la radioactivité.[**129, 93**]
3. une tranche correspond à l'ensemble constitué par le réacteur et ses systèmes auxiliaires.

6.3.2.2. Modes normaux. — Le mode normal d'exploitation auquel notre étude de veille s'est particulièrement attachée est celui de l'exploitation en puissance du réacteur. Les activités de l'opérateur sont particulièrement intenses lors des phases transitoires d'exploitation telles que la montée en puissance du réacteur ou l'arrêt du réacteur. La montée en puissance est réalisée en deux étapes. La première étape consiste à amener le réacteur dans les conditions thermodynamiques et chimiques utiles à l'extraction de la puissance nucléaire. La deuxième étape consiste à démarrer la réaction en chaîne de fission nucléaire. La première étape nécessite de contrôler en parallèle plusieurs paramètres de type thermodynamique (pression et température du circuit de refroidissement) et chimique (concentration en éléments neutrophages nécessaires au contrôle de la réaction en chaîne de fission nucléaire). De la même façon l'arrêt d'une tranche nécessite deux étapes, la première pour arrêter la réaction en chaîne et la seconde pour dépressuriser le circuit de refroidissement.

Les phases transitoires sont contrôlées par des systèmes de contrôle automatiques des grandeurs physiques et surveillées par l'opérateur de conduite. Lorsque les seuils de tolérance des équipements sont franchis, la tranche se protège automatiquement en démarrant des systèmes de sauvegardes classés pour la sûreté nucléaire.

Lorsque la tranche produit de l'énergie thermique par puissance nucléaire et lorsque la tranche est couplée au réseau d'électricité national, un système de régulation commande automatiquement la puissance nucléaire, l'opérateur de conduite surveille les paramètres physiques de la tranche à l'aide d'un système de journalisation d'événements et d'alarmes.

6.3.2.3. Modes stressés. — Les modes stressés interviennent notamment dans les phases d'exploitation inhabituelles. Le découplage de la tranche du réseau électrique national (ou îlotage) est une phase particulièrement complexe à conduire. En effet, le réseau n'absorbe plus la puissance fournie par le réacteur, les équipements permettant d'extraire la puissance du réacteur (pompes, condenseurs, *etc.*) sont alors fortement sollicités. Cette situation augmente le niveau d'attention et de stress des opérateurs de conduite.

6.3.2.4. Modes dégradés et accidentels. — La perte d'un équipement non classé pour la sûreté nucléaire est un mode d'exploitation dégradé, selon l'utilité du système perdu, cela peut entraîner l'arrêt du réacteur. La perte d'un équipement classé pour la sûreté nucléaire ou la détérioration d'une barrière de sécurité du système de défense en profondeur est considérée comme un mode d'exploitation accidentel bien que les événements redoutés (fusion du réacteur, libération de matières radioactives dans l'environnement, *etc.*) ne soient pas apparus. Les opérateurs entrent alors dans les procédures de conduite accidentelle du réacteur. Ces procédures suivent une approche par état au lieu d'une approche qui serait fonction de la nature de l'événement contraire à la sûreté nucléaire. L'opérateur est appelé à diagnostiquer les fonctions de sûreté nucléaire de façon itérative à l'aide de diagrammes en forme de logigrammes. Bien que protégée par les systèmes de sauvegardes tels que le système d'arrêt automatique du réacteur, certains modes accidentels nécessitent le maintien des fonctions d'extraction de la puissance nucléaire résiduelle, l'opérateur de conduite a ici, un rôle prépondérant pour la sûreté nucléaire. Une action inadaptée peut conduire à l'événement redouté.

Une défaillance humaine ou organisationnelle dans l'application des procédures de conduite accidentelle de la tranche peut provenir de la méconnaissance de l'état réel des systèmes supervisés comme cela été le cas lors de l'accident de Three Miles Island en 1979 aux États-Unis (voir [**121, 1, 38, 39**] pour une description détaillée de cet accident).

6.3.2.5. Rôle de la supervision automatique. — Un système de supervision automatique nommé Traitement Centralisé des Informations (TCI), a été mis en place dans les salles de conduites des centrales des paliers 900 et 1300 MWe [4]. Ce système est automatique dans le sens où il présente des informations synthétiques et plus significatives que celles fournies par les pupitres de contrôle commande. Les informations fournies sont de nature à éclairer les opérateurs sur une particularité d'un système (physique, état, mesure, *etc.*) sous forme d'images, de courbes ou d'événements. Les informations ne sont pas redondantes avec celles présentées sur les équipements conventionnels de contrôle commande, ce principe de non-redondance d'information est généralisé à l'ensemble des équipements de la salle de conduite afin de se prémunir de toute ambiguïté.

Ce système n'exécute aucune fonction de contrôle commande du réacteur ni de protection. La séparation des fonctions de sauvegarde est clairement délimitée, que ce soit fonctionnellement ou géographiquement. Bien que non critique pour la sûreté nucléaire, ce système est très apprécié par les opérateurs, car il fournit des informations permettant de recouper les analyses réalisées à partir des instruments conventionnels. La fiabilité et la véracité des informations fournies par ce système ne pouvant être démontrées, l'utilisation de celui-ci dans une situation critique pour la sûreté nucléaire est formellement interdite.

6.3.3. Supervision d'un atelier de production chimique. — Le site de production de produits pharmaceutiques de SANOFI-AVENTIS regroupe plusieurs ateliers de production. La plupart des ateliers sont des réacteurs chimiques permettant de synthétiser des molécules. Chaque atelier dispose d'un poste de commande qui centralise la supervision. Toutefois, il peut exister en plus du poste central, un poste de supervision local sur un équipement spécifique. Le traitement des procédés dans un réacteur chimique s'effectue par lots (on parle de procédé par *batchs*). Un même atelier peut servir à la production de plusieurs produits ou de plusieurs constituants d'un produit. De fait, un atelier peut être complètement reconfiguré, ce qui implique la reconfiguration du système de supervision.

La sécurité est un critère de contrôle commande de l'installation. La sécurité est visualisée au travers de grille « causes – effets », ce sont des schémas des actions de sécurité. Les synoptiques de supervision contiennent majoritairement les vues des alarmes. Les alarmes sont classées et il existe une vue dédiée aux alarmes de sécurité.

Les événements redoutés sont de deux ordres. Un relatif à la qualité des produits servant à la fabrication de médicaments et à l'emballement de la réaction chimique pouvant causer des explosions. Et l'autre, aux rejets de matières dangereuses susceptibles de polluer l'environnement (par exemple le rejet d'antibiotiques).

4. Les paliers plus récents sont équipés de salles de conduite complètement informatisées.

6.3.3.1. Mode nominal. — Le mode nominal correspond à la planification et à la configuration des *batchs*. Une mauvaise configuration du mode nominal (configuration de l'atelier et de son système de supervision) peut conduire à des situations accidentelles.

6.3.3.2. Modes normaux. — En exploitation, l'opérateur n'a pas de tâche relative à la sécurité à réaliser. Les alarmes déclenchent automatiquement les actions de sauvegarde. Un opérateur de supervision effectuant par erreur des actions inadéquates ne peut donc pas provoquer un accident.

6.3.3.3. Modes stressés. — Compte tenu du caractère séquentiel du procédé (traitement par *batchs*, le procédé s'arrête lorsque le produit est réalisé), nous n'avons pas identifié de modes stressés particuliers.

6.3.3.4. Modes dégradés. — Les modes dégradés interviennent lorsque des équipements de l'atelier sont défectueux, comme la fuite d'une cuve par exemple ou le non-fonctionnement d'une vanne.

Dans les modes d'exploitation dégradés SANOFI-AVENTIS privilégie le diagnostic humain. L'automatisme demeure une assistance pour l'opérateur de supervision qui est le seul dépositaire de l'état réel de l'installation. L'activité des opérateurs dans ces modes d'exploitation est régie par des procédures.

La supervision en mode dégradé dispose de deux niveaux d'utilisation qui correspondent aux prérogatives de l'opérateur sur l'installation. Plus l'installation est dégradée, plus l'opérateur dispose de prérogatives de contrôle sur l'installation. Le premier niveau autorise l'opérateur à effectuer certaines opérations critiques pour la sécurité, les autres actions étant toujours sous le contrôle du système de contrôle commande. Le deuxième niveau donne complètement le contrôle à l'opérateur qui doit effectuer une conduite procédurale.

Les modes dégradés permettent à l'opérateur d'effectuer des opérations critiques (type bypass) c'est donc seulement dans ce cas que des actions contraires à la sécurité peuvent être effectuées.

6.3.3.5. Modes accidentels. — Lorsqu'un accident se produit, les opérateurs n'ont aucune tâche particulière à effectuer compte tenu du caractère séquentiel du procédé. Les services de secours interviennent pour traiter les conséquences de l'accident.

6.3.4. Supervision du LMJ. — Le LASER MégaJoule (LMJ) est une composante du programme national de défense en matière de « simulation », l'objectif est de permettre aux ingénieurs du Commissariat à l'Énergie Atomique (CEA) de valider le fonctionnement des armes nucléaires de dissuasion en l'absence d'essais (la France ayant ratifié le traité d'interdiction complète des essais nucléaires). Il permettra de valider les modèles physiques sous-jacents aux simulations numériques, grâce aux conditions extrêmes de température et de pression produites par un faisceau de LASER sur les matériaux contenus dans la cible. Le LMJ est à l'heure actuelle en phase de construction.

Ce système d'expérimentation scientifique a la particularité d'être « mono-coup ». Une expérience demande une longue préparation avant la date de tir notée t_0. La séquence de tir qui s'étend d'environ $t_0 - 60$ minutes à $t_0 - 1$ seconde est sous le contrôle des systèmes de supervision et de contrôle commande. La dernière seconde est entièrement gérée par un système

de synchronisation électronique et optique sans intervention humaine, car les contraintes de temps réel sont inférieures à la nanoseconde. Le système de supervision assure également l'acquisition et le stockage des résultats de mesures. Le LMJ dispose de 250 000 points de contrôle, surveillés par environ 500 contrôleurs et supervisés par une vingtaine d'opérateurs grâce à plusieurs centaines de synoptiques réparties sur une trentaine d'écrans.

Les principaux événements redoutés relatifs aux personnels sont liés à la très grande quantité d'énergie manipulée par le système. Les risques proviennent du LASER mais également de la haute tension contenue dans les dispositifs de stockage de l'énergie (grands condensateurs à longue décharge). Lors de tirs de forte énergie sur cible nominale, il faut ajouter le risque nucléaire dû aux neutrons émis pendant la réaction de fusion nucléaire ainsi que les rayonnements résiduels suite à l'activation par les neutrons des matériaux proches de la chambre.

Le principal événement redouté relatif au matériel est l'endommagement des éléments optiques suite à une mauvaise qualité du faisceau lors du tir.

La sécurité est assurée par trois niveaux fonctionnels indépendants :

- Niveau 1 : sécurité intrinsèque des équipements ;
- Niveau 2 : interverrouillages entre les équipements ;
- Niveau 3 : système d'interdiction de tir (le blocage de tir agit sur l'horloge maître de la séquence).

Lorsque l'un de ces niveaux est actionné, le système est mis en sécurité.

Les interventions humaines sont limitées en utilisant dans la mesure du possible une solution technologique adaptée. L'existence même de la notion de barrière utilisateur dans les études préliminaires de sécurité de la future installation montre qu'il existe des scénarios de défaillance dont la couverture sécurité est assurée par une action humaine effectuée par procédure. Les interlocuteurs du CEA n'excluent pas *a priori* l'existence d'actions humaines effectuées au niveau de la supervision qui pourraient être directement contraires à la sécurité. Dans l'état actuel du projet (encore en phase de conception), la réponse apportée est que les études de sécurité devront identifier ces scénarios et définir les procédures adaptées.

6.3.4.1. Mode nominal. — Le mode nominal d'une séquence de tir consiste en trois phases : la préparation, le tir et la phase post-tir. La préparation de tir est planifiée par une séquence chronologique interruptible à tout moment par l'opérateur de supervision sauf dans la dernière seconde où le système de synchronisation prend le relais.

6.3.4.2. Modes stressés. — Il n'y a pas de mode stressé d'exploitation. En effet, la production d'un système expérimental n'est pas sujette à des objectifs stricts de production, seule la qualité des résultats prime, la séquence de préparation avant le tir fait en sorte que chaque tir soit effectué dans les conditions optimales.

6.3.4.3. Modes dégradés. — La dégradation d'un équipement entraîne automatiquement le déclenchement d'un des niveaux de sécurité et entraîne l'arrêt de la séquence de tir.

6.3.4.4. Mode accidentel. — Les accidents du type dégradation du matériel ne peuvent être diagnostiqués qu'*a posteriori*. Compte tenu du temps extrêmement faible de la phase de tir, il n'est pas possible de considérer un mode d'exploitation accidentel.

6.3.5. Contrôle de trafic aérien. — Le Centre en Route de la Navigation Aérienne Nord CRNA/N assure l'extraction des vols à l'arrivée sur les aéroports de Paris. Le CRNA/N effectue une prérégulation des vols dans la zone d'approche des aéroports. Il effectue également l'intégration des vols au départ des aéroports de Paris vers la sortie de la zone d'approche.

Un système d'attente permet de gérer l'arrivée des avions. La programmation peut atteindre 120 à 140 mouvements par heure. Trois modes d'encadrement du trafic sont identifiés :

- En route : concerne les avions progressant en dehors des zones proches des aéroports ;
- En approche : concerne les avions progressant dans les zones proches des aéroports qui sont dans la phase de descente ;
- En tour : concerne les avions en phase d'atterrissage.

La zone de contrôle du CRNA/N est divisée en deux zones géographiques dont le fonctionnement est indépendant. Pour chacune de ces zones, une à trois équipes de contrôleurs aériens opèrent et se partagent l'activité. Une équipe est composée de deux contrôleurs dont le rôle est défini de la façon suivante :

- Le contrôleur *organique* assure les fonctions de régulateur pour les vols arrivant dans le secteur. Il réalise ainsi l'interface avec les secteurs adjacents. Sa deuxième activité consiste à préparer les plans de vol (appelés *STRIP*, bande de papier) pour son équipier « contrôleur radar » ;
- Le contrôleur *radar* assure la communication avec les équipages des avions pour leur donner les consignes de vol du type : changements de cap, changement d'altitude ou encore de vitesse, autorisations d'atterrissage et de décollage, horaires de passage de certains points, *etc.* Son outil de travail est le plan de vol (*STRIP*) où sont imprimés les détails connus du vol : indicatif d'appel en radio téléphonie, route, provenance, destination, type d'aéronef, niveau de vol ou altitude. Sa source d'information concernant le trafic est l'écran radar (voir figure 6.4) qui fournit les altitudes, les caps et les routes suivies par les avions.

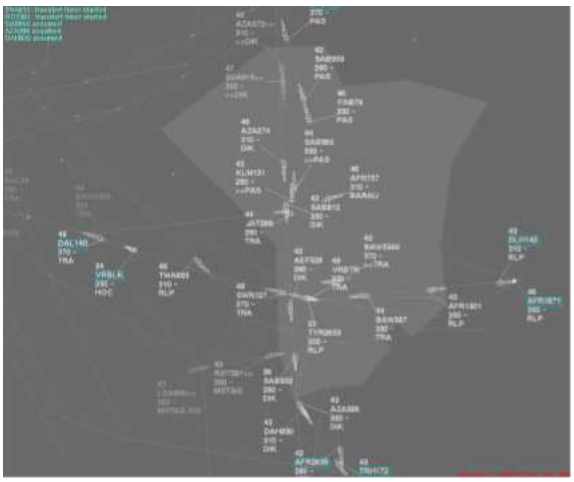


FIGURE 6.4. Écran de radar

Les événements redoutés contraires à la sécurité sont des infractions aux séparations entre les avions et les infractions en altitude.

Les contrôleurs aériens ont en charge la mission de sécurité et en assurent la responsabilité. Ils donnent les directives opérationnelles aux pilotes pour que les conditions de vol se réalisent dans le respect des normes de navigation aérienne.

6.3.5.1. Mode nominal. — Le mode nominal est celui prévu dans le planning des vols qui contient les horaires de passages des vols et leurs routes théoriques.

6.3.5.2. Modes normaux. — L'activité normale du trafic est celle donnée par le mode nominal soumis à de légères perturbations comme l'avance ou le retard des avions sur le planning ou bien les écarts mineurs entre la route réelle des avions et la route théorique. Le travail du contrôleur *organique* consiste à préparer le travail du contrôleur *radar* en fonction de ces perturbations.

6.3.5.3. Modes stressés. — L'accroissement de la densité du trafic est source de tension du système. Ce phénomène a été clairement identifié par les concepteurs du système, de fait, des mesures sont prises pour éviter de rentrer dans le mode d'exploitation stressé. Ces mesures consistent à adapter la couverture géographique des secteurs de contrôle. Lorsque le trafic augmente, il est possible de dégrouper des secteurs, ainsi les binômes contrôleurs couvrent une zone plus restreinte.

6.3.5.4. Modes dégradés. — En situation dégradée, lors de la perte d'équipements conduisant à une capacité de traitement des vols réduite, une analyse est effectuée pour apprécier la capacité du secteur en fonction de la prévision de trafic. Si la capacité n'est pas adaptée à la prévision de trafic, des mesures de régulation sont prises en retardant les avions.

Lorsque les mesures de régulation sur la zone sont insuffisantes, les opérations de régulation globales du trafic sont prises en charge par le centre européen de régulation basé à Bruxelles appelé *Central Flow Management Unit* (CFMU).

6.3.5.5. Modes accidentels. — Le système passe en mode accidentel lorsque les conditions de séparation entre avions et les conditions d'altitudes ne sont pas remplies. La tâche des opérateurs consiste à indiquer aux équipages les directives pour retrouver les conditions de séparation et d'altitude acceptables.

6.3.5.6. Système de supervision automatique. — Un système informatique intègre les éléments issus des informations radars et des plans de vol. Il apporte les informations permettant le suivi des vols et les éléments d'aide à la décision au regard des situations hors-normes possibles, mais ne participe pas directement à la décision de navigation prise par l'opérateur, seul responsable des missions de sécurité.

Depuis les années 80, les ingénieurs du contrôle aérien cherchent à améliorer les outils de contrôle afin de parer à l'augmentation toujours croissante du trafic aérien. Les États-Unis avaient essayé, au début des années 80, de concevoir un système de contrôle aérien complètement automatisé. Une telle entreprise s'est avérée être une chimère compte tenu de la complexité de modélisation d'une part, de la variabilité des tâches à accomplir et de la difficulté d'automatiser des tâches de détection, de diagnostic et surtout d'anticipation dont seul un opérateur humain est capable.

La Direction Générale de l'Aviation Civile (DGAC), qui représente l'autorité française en matière de navigation aérienne, a opté pour un système d'aide à la détection et au diagnostic. Cet

outil n'a été mis en place que très récemment dans le cadre d'une refonte du système informatique de traitement de l'information. Celui-ci vise à réduire la charge mentale des opérateurs et de fait augmente la capacité de traitement des vols tout en garantissant le même niveau de sécurité. Le programme s'appelle *En-Route Air Traffic Organizer* (ERATO).

La solution proposée dans ERATO a été de diminuer la quantité d'informations à évaluer par les contrôleurs. Leur activité mnésique est diminuée grâce à un système d'affichage modulaire qui permet de visualiser et d'anticiper les conflits. Chaque module de l'affichage est paramétrable par l'opérateur en fonction de sa charge et de son besoin. Le système pouvant être totalement débrayé.

6.3.6. Supervision de trafic ferroviaire. —

6.3.6.1. Particularités du trafic urbain. — La supervision de trafic urbain dispose de par ses propriétés spécifiques [5] d'une centralisation de la commande ferroviaire. Chaque ligne est supervisée par un Poste de Commandement Centralisé (PCC) propre. La RATP est allée plus loin dans la centralisation en réunissant les PCC de toutes les lignes (indépendantes fonctionnellement et géographiquement les unes des autres) dans une même salle. Cette salle a été installée dans les années 60 et est basée dans un bâtiment du Boulevard de Bourdon à Paris. À ce jour, la RATP opte pour une politique de décentralisation des PCC, le PCC de la ligne 14 n'a pas été intégré à la salle de Bourdon et le PCC de la ligne 4 a quitté Bourdon lors de son renouvellement. Il en sera de même pour celui de la ligne 1 après son automatisation à l'horizon 2010. Le PCC assure la supervision du trafic sur les lignes, cependant, pour chaque terminus, un poste de manœuvre local assure l'injection et le retrait des trains vers les voies de garage et les différents ateliers. Le PCC de Bourdon est organisé de façon à ce que les opérateurs, affectés chacun à une ligne, puissent s'entraider en cas de perturbation sur une ligne. En effet, les pupitres des opérateurs sont au centre d'une répartition circulaire des Tableaux de Contrôle [6] Optique (TCO) voir schéma de la figure 6.5.

6.3.6.2. Particularités du trafic grande ligne. — La complexité et l'étendue d'un réseau grande ligne par rapport à un réseau urbain nécessite l'installation de plusieurs centres de supervision du trafic. Ainsi, chaque grande gare dispose d'un poste de régulation et d'aiguillage. Par exemple, l'unité de complexité d'un poste de type PRCI est donnée par le nombre d'itinéraires sous sa responsabilité. Les opérateurs disposent d'une station PC spécifique à leur zone géographique de supervision et d'un TCO central donnant une vue générale du réseau couvert par le poste à l'ensemble du personnel.

6.3.6.3. Mode nominal. — Le mode nominal est donné par le planning d'exploitation du réseau. Le planning est construit à l'aide d'une table horaire spécifiant les horaires de passage des trains à des points kilométriques remarquables. Une autre forme de visualisation du planning est fournie par le graphe espace-temps représentant sur un graphique en deux dimensions les successions des circulations. Les abscisses représentent le temps et les ordonnées indiquent l'espace (points kilométriques). Chaque circulation est représentée par une trajectoire dans ce graphe. La pente

5. Réseau fermé, circulation homogène.
6. Les tableaux installés à Bourdon disposent également de commandes.

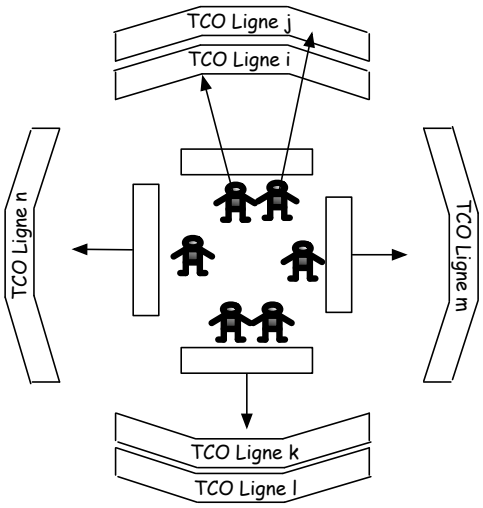


FIGURE 6.5. Schéma de l'organisation du PCC de Bourdon

de la trajectoire décrit la vitesse du train, une pente nulle représente un train à l'arrêt sur la position indiquée en ordonnée voir figure 6.6.

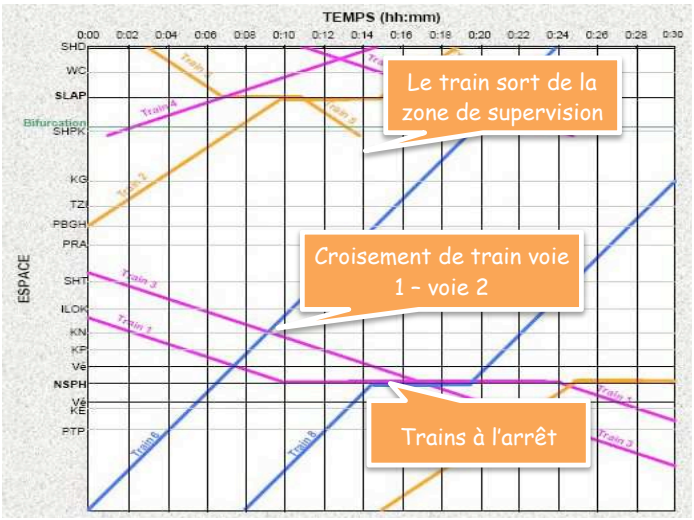


FIGURE 6.6. Graphe espace-temps

Dans un réseau urbain, notamment pour les métros, le mode nominal peut être fourni par la fréquence des trains sur la voie. Un système automatique de régulation assure alors la préservation d'une séparation temporelle entre les trains en retenant plus ou moins les trains dans les stations. D'une façon générale, la régulation d'un réseau urbain est essentiellement temporelle (fréquence entre les trains) et la régulation d'un trafic grande ligne est à la fois spatiale et temporelle.

Dans tous les cas, le mode nominal est intégré dans le système de suivi de train et de tracé automatique des itinéraires. Ainsi, l'opérateur est un superviseur de l'exécution de ce système automatique qui en fonction des informations contenues dans la table horaire et dans le système

de suivi et d'identification des trains, oriente les trains vers leurs destinations de sortie de la zone de couverture du poste en traçant automatiquement les itinéraires (position des aiguilles).

6.3.6.4. Modes normaux. — L'exploitation d'un réseau ferré implique inévitablement de légères perturbations dues à la variabilité de performance des composantes du système ainsi qu'aux interactions entre ces composantes. Les modes d'exploitation normaux requérant l'activité de l'ATS sont ceux liés à la circulation des trains sur la voie dans les conditions prévues dans le planning que ce soit pour le service voyageur, fret ou des opérations de maintenance.

Lorsque ces perturbations sont mineures, le système de tracé automatique des itinéraires ou le système de régulation automatique est capable de gérer les écarts par rapport au nominal.

6.3.6.5. Modes stressés. — À la différence du contrôle aérien, il n'est pas possible de réorganiser les secteurs de supervision compte tenu de l'aspect rigide de l'infrastructure ferroviaire et de ses équipements permettant de contrôler les circulations. C'est le cas, par exemple, lorsque la capacité de trafic maximale est atteinte, comme cela se produit quotidiennement en région Île de France et ce phénomène se généralise compte tenu du souci légitime de rentabilité des infrastructures. Ceci a pour conséquence une gestion à flux tendu, impliquant parfois des écarts trop importants vis-à-vis du planning nominal ayant pour effet de mettre en défaut les systèmes de régulation et de tracé automatique des itinéraires. Dès lors, l'intervention des opérateurs est obligatoire et compte tenu de la densité de trafic, les délais de réactions requis sont de plus en plus courts. L'opérateur a donc le choix de reparamétrer les algorithmes de régulation automatique et de tracé automatique des itinéraires voire de déconnecter ces systèmes pour reprendre le contrôle manuel du graphe espace-temps et de la table horaire. Par exemple, le reparamétrage d'un système de régulation automatique consiste à changer la valeur de fréquence des circulations, ce qui a pour effet de retenir et donc retarder les trains en station afin d'éviter des « bouchons » sur la voie. Le reparamétrage du système automatique de tracé d'itinéraire consiste à réorganiser l'ordre des trains dans le graphe espace-temps et donc dans la table horaire dans le but de fluidifier le trafic.

Lorsque les systèmes de régulation et de tracé automatique des itinéraires sont débranchés, l'opérateur doit alors effectuer toutes les opérations « à la main » via l'interface graphique de l'ATS. Dans le cas d'une régulation en fréquence, l'opérateur dispose d'une commande permettant de retenir les trains en stations, à la RATP il s'agit de la procédure de « départ sur ordre ». Dans le cas d'une régulation spatiale (par tracés d'itinéraires), l'interface de l'ATS propose à l'opérateur des commandes de tracé d'itinéraire qui sont soumises aux systèmes d'enclenchement assurant la sécurité des circulations. Une commande contraire à la sécurité ne sera donc pas exécutée. Toutefois, certaines situations nécessitent l'action directe de l'opérateur sur le système d'enclenchement comme la mise en place ou la suppression de limitation temporaire de vitesse.

Les modes d'exploitation stressés sont générateurs de stress pour le personnel en raison d'une forte augmentation de la charge de travail des opérateurs, qui dans le mode nominal, n'ont que très peu d'actions à effectuer. Il est alors légitime de se demander quelles actions ont un impact direct sur la sécurité, comment les opérateurs les distinguent et les appréhendent.

En effet, la séparation fonctionnelle entre les fonctions de supervision et les fonctions de sécurité est identifiée dans la conception du système de supervision, par la mise en sécurité du protocole de communication lors de la commande de sécurité (voir le paragraphe 2.8.2)

mais l'opérateur n'a pas forcément conscience du niveau de sécurité de son action. La seule distinction entre une commande de supervision et une commande de sécurité est qu'une demande de confirmation est demandée à l'opérateur pour une commande de sécurité.

Le cas de travaux de maintenance préventive peut être traité comme un mode normal d'exploitation puisque prévu dans le planning nominal, mais sera volontairement traité ici comme un des modes stressés ou dégradés en raison des modifications profondes de l'activité de l'opérateur dans de telles situations. L'analyse du retour d'expérience montre que de nombreux incidents, quasi-accidents et accidents sont apparus alors que des travaux étaient en cours, ou bien lors de l'application de procédures particulières en raison de la défaillance ou de la maintenance d'un équipement (voir le paragraphe 6.3.6.8).

6.3.6.6. Modes dégradés. — Les modes dégradés sont consécutifs à la défaillance (nécessitant de la maintenance curative, donc non prévue dans le planning d'exploitation) d'une ou plusieurs installations nécessaires à l'exécution normale de l'exploitation. À la différence des modes stressés, le changement par rapport au mode nominal n'est pas planifié et est source de bouleversement dans l'activité. Cela nécessite des opérations de l'opérateur pour lesquelles il est de moins en moins entraîné.

6.3.6.7. Modes accidentels. — Les modes d'exploitation accidentels sont en général réduits à l'activité de sauvetage puisque une fois l'accident détecté, l'opérateur de supervision de trafic a la possibilité d'arrêter complètement le trafic. La présence et l'activité des opérateurs dans le poste de supervision de trafic sont primordiales, car elles permettent d'organiser le sauvetage.

6.3.6.8. Retour d'expériences. — L'accident qui s'est déroulé en 2003 dans le tunnel de la Biogna (Alpes Maritimes, 06) où deux trains sont entrés en collision en nez à nez sur une voie unique et où deux personnes ont été tuées [7] est représentatif d'un mode d'exploitation dégradé généré par la défaillance chronique d'un équipement et qui a dégénéré en accident.

Les raisons avancées par le Conseil Général des Ponts et Chaussées [**3**] indiquent que l'opérateur du poste de supervision de trafic basé à Breil (Alpes Maritimes, 06) a contourné le système de protection des cantons en raison du dysfonctionnement chronique de l'outil de test du matériel de détection de train. Il s'agissait en l'occurrence d'un détecteur électromagnétique dit « compteur d'essieux » rare sur le réseau français où les trains sont détectés le plus souvent par des circuits de voie qui ne peuvent pas être inhibés. Ce dispositif, mis en place pour cause de canton de très grande longueur génère en cas de dysfonctionnement de fausses alarmes sous forme de fausses informations d'occupation de canton. Cette particularité souvent recherchée par conception dans les systèmes de sécurité (qui consiste à préférer en cas de défaillance une information dite restrictive) a en fait des effets pervers lorsque ces dysfonctionnements sont trop fréquents, ce qui a pour conséquence que l'opérateur s'habitue à ces fausses alarmes qu'il acquitte trop régulièrement. Ce jour-là, l'opérateur trop habitué et peut être préoccupé dans une autre tâche, a omis de vérifier avant la remise à zéro du dispositif qu'il s'agissait bien d'une fausse alarme (ce qu'il pouvait faire grâce à une procédure de suivi manuel des trains qu'il aurait dû effectuer en parallèle, ce qu'il n'a pas fait tout de suite puis oublié peu après), provoquant

7. Les deux conducteurs de l'un des trains, celui du deuxième ayant eu le réflexe de se replier à l'arrière de son train avant le choc.

ainsi l'ouverture d'un itinéraire non autorisé, libérant ainsi la voie à un train vers une voie non libre où circulait un autre train en sens inverse.

Un deuxième accident, récent, survenu en octobre 2006 à Zoufftgen (Moselle, 57) au niveau de la frontière Franco-Luxembourgeoise montre que la mise en place d'une procédure d'exploitation particulière connue sous le nom « Installation Permanente de Contre-Sens » (IPCS) a été un facteur de mise en tension du système. Comme son nom l'indique, cette procédure consiste à utiliser une voie en sens contraire et en voie unique lors de l'indisponibilité de la voie adjacente pour raison de travaux par exemple. Cette procédure est prévue lors de la conception du réseau ferré par l'installation permanente des équipements de voies nécessaires à son exécution (signalisation et équipements de voie en contre-sens). À Zoufftgen, l'IPCS était utilisé en raison des travaux de longue durée sur une voie. Le mode nominal a été modifié sur toute la période des travaux afin de prendre en compte l'exploitation en voie unique d'une partie de la voie. L'enquête de cet accident étant encore en cours, les raisons précises de l'accident ne seront pas présentées, par contre le contexte a été largement présenté par les journaux, les entreprises ferroviaires [8] ainsi que les autorités Françaises et Luxembourgeoises [9].

Le contexte de l'accident est, de notre point de vue, une deuxième mise en tension du mode d'exploitation déjà stressé en raison de l'application du pas d'IPCS (L'utilisation du pas est une procédure relativement rare). En effet, le retard important d'un train de fret a imposé l'arrêt d'un train de voyageurs venant en sens contraire. L'arrêt du train de voyageurs a été imposé par la fermeture du signal d'entrée du pas d'IPCS en raison de la présence du train de fret sur cet itinéraire circulant en sens contraire. Or le conducteur du train de voyageurs, habitué à l'horaire, aurait dû être normalement autorisé à circuler sur l'IPCS à cette heure-ci. Il a donc demandé à l'agent de supervision de trafic les raisons de cette fermeture de signal. Une procédure d'autorisation de franchir le signal fermant l'itinéraire a été délivrée par l'agent de supervision de trafic. L'entrée en mode accidentel est vraisemblablement consécutive à cette demande et pendant la réalisation de la procédure d'autorisation de franchissement d'itinéraire effectuée par l'agent de supervision de trafic qui aurait dû s'assurer que la voie était libre avant de donner l'autorisation.

L'accident survenu à Zoufftgen a été généré par une coïncidence malheureuse d'événements (mise en tension du système) et de caractéristiques particulières de la voie (Interface entre deux réseaux : Français et Luxembourgeois). Le contexte de cet accident est toutefois particulier, il présente l'aspect d'une accumulation de mise en tension du système (Travaux et retard d'un train) qui prise séparément n'aurait sans doute pas conduit à l'accident. L'application du pas d'IPCS bien que prévu dans le mode nominal d'exploitation a, de par son caractère inhabituel, perturbé l'activité des acteurs de la circulation (le manque d'entraînement pourrait être une piste à étayer dans l'analyse de cet accident afin d'étudier les erreurs de l'organisation).

D'autres accidents dont l'accident de la gare de Lyon en 1988 pour le domaine ferroviaire, un accident dans le domaine du contrôle aérien et l'accident de Tchernobyl pour le nucléaire ont été analysés dans [**16**].

8. Communiqué de la SNCF : `http://www.entreprise-sncf.com/communiq/communiq688.html`

9. Communiqué de presse de la préfecture de la Moselle : `http://www.moselle.pref.gouv.fr/Presse/pdf/1777-01.pdf` et le communiqué du gouvernement Luxembourgeois : `http://www.gouvernement.lu/salle_presse/communiques/2006/10/11accident_cfl1/index.html`

6.4. Résilience

6.4.1. Définitions. — Dans ce qui précède, la veille industrielle s'est focalisée sur les conditions d'exploitation permettant d'identifier les modes d'exploitation remarquables du point de vue de la sécurité. Ces modes ont été présentés avec une logique de sécurité décroissante, du mode le plus sécuritaire vers les modes de plus en plus dégradés jusqu'à la perte totale de sécurité. Toutefois, il serait réducteur d'identifier le rôle de l'opérateur de supervision dans cette seule logique. En effet, nombreux sont les accidents ou les incidents qui ont pu être évités par l'action des opérateurs de supervision. Dans cette logique, une approche originale a émergé ces dernières années autour du concept de résilience.

Cette notion de résilience a été empruntée à la physique des matériaux. En physique, la résilience traduit la capacité d'un matériau à résister à des chocs ou à retrouver son intégrité après ces chocs. Ce concept a été transporté dans le domaine de la psychologie et notamment l'étude des traumatismes de l'enfance [**134**]. Cette théorie permet de décrire les phénomènes de reconstruction de la personnalité d'un enfant suite à traumatisme grave. Un autre transfert de cette notion a été effectué dans le domaine de l'écologie [**56**] où la résilience est définie par l'habileté intrinsèque d'un système écologique à résister et à se reconstruire après un traumatisme. Dans ce domaine, la résilience a été associée à la théorie mathématique de la viabilité introduite par Aubin [**10**] dans la thèse de Martin [**97**].

Plus récemment, Hollnagel, Woods et Leveson ont publié un ouvrage [**70**] visant à appliquer cette notion de résilience à l'étude des accidents. L'objet de cet ouvrage est de créer une nouvelle approche dans l'étude des accidents, nommée « ingénierie de la résilience » (traduit de l'anglais *Resilience Engineering*). Cette approche s'inspire des travaux réalisés dans les sciences de la complexité et des systèmes. Cette approche apporte de nouveaux modèles permettant d'intégrer, dans l'analyse de risques, les différentes composantes du système (techniques, humaines et organisationnelles) et leurs interactions. Alors que l'analyse de risque est généralement traitée sous l'angle de la faillibilité, l'ingénierie de la résilience s'intéresse aux mécanismes permettant de contrecarrer les dangers.

Ainsi, pour la composante humaine des systèmes, il s'agit de prendre en considération les activités quotidiennes des opérateurs qui rendent le système sûr et de ne plus considérer uniquement l'opérateur humain comme un acteur faillible dans les études de sécurité, mais de prendre en compte sa forte capacité d'anticipation et d'adaptation.

À ce jour les travaux de l'ingénierie de la résilience sont purement conceptuels, il est donc nécessaire de les rendre plus opérationnels.

Le concept de résilience fait donc appel à deux notions, l'une concernant la capacité de résistance d'un système lui conférant des propriétés à réduire les conséquences d'un traumatisme et l'autre relative à la reconstruction après un traumatisme.

Dans le cadre de la résilience, la sécurité n'est plus considérée comme une propriété du système, mais comme un phénomène émergeant du système [**70**]. La résilience exprime une notion duale [10] de la sécurité. Un système ayant une forte propension à la résilience sera d'autant plus apte à faire émerger la sécurité. En d'autres termes, si l'on considère les deux notions sécurité et résilience comme deux phénomènes caractéristiques du système, la sécurité représente tous

10. Notions duales : Se dit de notions qui se présentent par deux et qui sont réciproques.

les phénomènes contribuant à ne pas générer de pertes et la résilience d'évaluer les mesures mises en place pour résister et se reconstruire suite à un événement contraire à la sécurité.

Alors que l'insécurité est une notion permettant d'évaluer le risque (la gravité et la fréquence) d'une transition vers l'état accidenté, la résilience traduit l'obtention de la sécurité en situation. Dans le but de préciser la notion de résilience qui contient à la fois l'aspect de résistance et de reconstruction, nous proposons les deux définitions suivantes :

***Définition 6.1* (Résistance).** — La résistance d'un système représente les phénomènes, les mécanismes et les activités du système qui lui permettent de ne pas effectuer des transitions vers un mode moins sécuritaire que celui dans lequel il se trouve.

***Définition 6.2* (Résilience).** — La résilience d'un système représente les phénomènes, les mécanismes et les activités du système qui lui permettent de retrouver un mode plus sécuritaire suite à un événement contraire à la sécurité ayant pour effet de réaliser une transition vers un mode dangereux.

La résilience évalue la propension du système à demeurer dans un mode non accidentel ou à recouvrer un mode moins dangereux (transition de dégradé vers stressé ou normal, transition de stressé vers normal).

La figure 6.7 illustre cette représentation. Lorsque le système est soumis à un événement interne ou externe portant atteinte à l'intégrité de la sécurité du système, soit le système peut évoluer vers le mode d'exploitation accidentel, ce qui se traduit par les transitions non sécuritaires (traits continus) soit le système est résistant et demeure dans l'état dans lequel où il se trouvait (traits discontinus). Enfin, l'événement contraire à la sécurité peut générer un mode moins sécuritaire et la capacité du système à se reconstruire implique un retour vers un mode d'exploitation plus sécuritaire (traits pointillés), il s'agit alors de transitions résilientes. Naturellement, une transition résiliente fait suite à une transition préalable vers un mode moins sécuritaire que l'on ne voit pas sur la figure.

***Définition 6.3* (Définition duale de la sécurité).** — La sécurité (S) est un phénomène émergeant des capacités du système à être résistant (R_t) et résilient (R_l).

$$S = R_t + R_l$$

Par extension, il sera possible de parler d'action résistante et respectivement d'action résiliente pour une activité contribuant dans une transition résistante et respectivement résiliente.

L'activité humaine dans le cadre de la supervision de procédé industriel permet de détecter et d'anticiper, dans la mesure du possible, les événements contraires à la sécurité.

6.4.1.1. Caractéristique d'une action résistante. — Une action résistante intervient avant l'arrivée des conséquences d'un événement indésirable. Les conséquences de cet événement risquent de provoquer une transition vers un mode moins sécuritaire et c'est l'action entreprise par l'opérateur qui empêche cette transition. La tâche primordiale de l'opérateur est donc d'**anticiper** la transition.

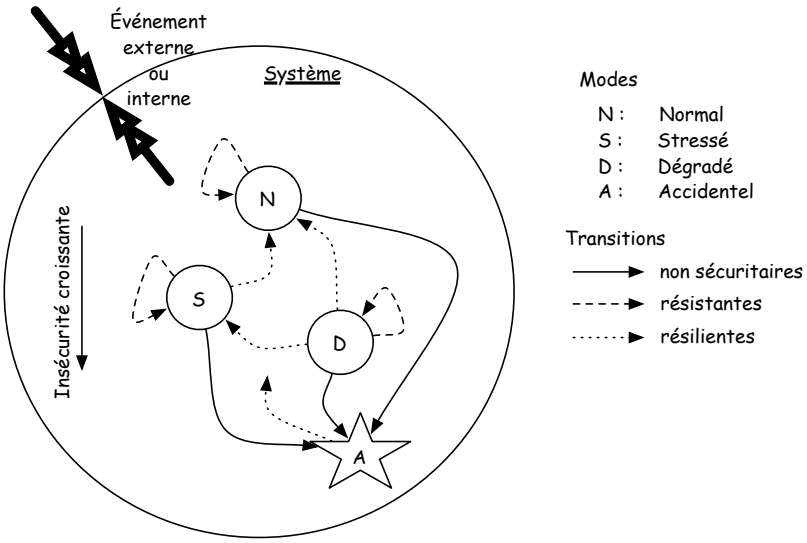


FIGURE 6.7. Transitions de modes d'exploitation suite un événement contraire à la sécurité

6.4.1.2. Caractéristique d'une action résiliente. — Une action résiliente intervient après une dégradation du mode d'exploitation lorsqu'une transition vers un mode moins sécuritaire est en cours ou a déjà eu lieu. Lorsqu'il s'agit d'une transition accidentelle, l'action résiliente n'a de sens que lorsque les conséquences de l'événement n'ont pas encore eu lieu, on parle de quasi-accident. La tâche primordiale de l'opérateur dans le cadre d'actions résilientes est de **détecter** l'événement indésirable ou la transition vers un mode d'exploitation moins sécuritaire.

Ces activités qu'elles soient résistantes ou résilientes recèlent d'une part des caractéristiques propres de l'opérateur humain et d'autre part des caractéristiques propres aux interactions entre l'homme et le système.

6.4.2. Résistance et résilience en supervision industrielle. — L'activité de supervision de procédés industriels participe au phénomène de résilience du système. En effet, quels que soient les procédés supervisés, les opérateurs de supervision disposent d'une vue globale du système. L'objet de leur attention est donc le système dans sa totalité ce qui permet d'appréhender les transitions de modes d'exploitation. Le rôle des interfaces hommes-machine est de transmettre les informations en provenance du procédé qui sont des indicateurs du mode d'exploitation en cours. L'autre rôle primordial des interfaces hommes machines consiste à remonter tous les événements contraires à la sécurité.

Cette nouvelle perspective de la sécurité et du rôle pris par les opérateurs offre un nouveau regard sur la veille industrielle effectuée. Les paragraphes qui suivent présentent les actions résistantes et résilientes dans la supervision des différentes industries rencontrées.

6.4.2.1. Conduite d'un réacteur nucléaire. — L'opérateur de conduite d'une tranche nucléaire doit anticiper les événements contraires à la sécurité. Les phénomènes liés à la résistance sont pour une grande part assurés par les systèmes classés pour la sûreté nucléaire. La tâche de l'opérateur consiste à agir pour la résilience du système puisque son activité dans une procédure

accidentelle consiste à évacuer la puissance résiduelle et à faire en sorte que la tranche retrouve un état sain. Le système est d'autant plus résilient que les opérateurs sont entraînés à conduire un réacteur dans un mode accidentel. De fait, EDF forme et entraîne de façon permanente tous ses opérateurs sur simulateur. De plus, des essais périodiques sont effectués sur l'ensemble des systèmes de sauvegarde classés pour la sûreté nucléaire et assurant les activités de résistance. Pour les opérateurs ces exercices sont importants et contribuent à l'entraînement (capacité accrue de résilience) et à la résistance du système (les essais périodiques permettent de tester la disponibilité des systèmes de protection et de sauvegarde). Le système de Traitement Centralisé des Informations (TCI) offre alors une aide précieuse aux opérateurs pendant ces essais périodiques. En effet, l'apport d'une information synthétique facilement interprétable contribue à l'élaboration du diagnostic et peut être vu comme un élément pédagogique lorsqu'il s'agit d'effectuer des essais périodiques. Cependant, son utilisation systématique peut engendrer une perte d'entraînement et devenir un élément de supervision automatique pernicieux puisque ce système ne doit pas être utilisé en cas de scénarios accidentels compte tenu du manque de fiabilité des informations.

6.4.2.2. Supervision d'un atelier de production chimique. — Dans l'industrie de production de produit pharmaceutique, la phase de reconfiguration des systèmes d'alarme et de contrôle commande est primordiale, car il s'agit de la configuration des mécanismes de résistance du système. L'opérateur qui effectue cette reconfiguration a donc un impact sur la résistance. D'autre part, les phénomènes de résilience sont permis au travers de l'organisation des prérogatives de l'opérateur sur la sécurité. Nous avons vu que SANOFI-AVENTIS a mis en place un système d'allocation des tâches entre le contrôle commande et l'opérateur : plus la situation se dégrade, plus l'opérateur dispose de commandes sur le procédé. Ainsi, il existe un indicateur de mode d'exploitation qui régit l'activité de l'opérateur et l'autorise à entreprendre des actions visant à effectuer des transitions résilientes.

6.4.2.3. Supervision du LMJ. — En ce qui concerne le LMJ, les transitions entre les modes d'exploitation ne sont pas facilement identifiables en raison du caractère expérimental du système, les grandeurs temporelles sont telles que l'opérateur humain n'a que très peu d'occasions pour effectuer des actions de type résistantes ou résilientes. Seules les actions consistant à arrêter la séquence sont significatives. La tâche consiste à effectuer une série de tests avant le déclenchement du tir et à détecter les éventuelles anomalies contraires à la sécurité.

6.4.2.4. Contrôle de trafic aérien. — Le cas du contrôle de trafic aérien est un bon exemple de contribution de l'organisation dans la sécurité. Le caractère adaptatif de l'organisation et la bonne coopération dans le binôme de contrôleurs aériens garantissent à la fois la résistance et la résilience face à une dégradation de la situation. Le programme ERATO contribue à la résistance du système face aux conflits en apportant à l'opérateur radar une aide à leurs détections et à leurs prévisions.

6.4.2.5. Supervision de trafic ferroviaire. — La résistance du système ferroviaire demeure le rôle de la barrière technologique, en effet lors de la conception des systèmes ferroviaires modernes, l'opérateur de supervision de trafic n'est pas identifié comme un acteur de la sécurité dans les modes d'exploitation normaux et stressés. Le superviseur de trafic dispose d'une responsabilité de la sécurité dans les modes dégradés de l'exploitation lorsque la barrière technologique n'est

Événement initiateur conduisant à un mode stressé	Action résiliente
Phénomène d'accumulation du trafic en raison de la densité	L'opérateur de supervision de trafic, dans son rôle de superviseur détecte les prémices d'une accumulation et prend des mesures permettant de fluidifier le trafic (régulation)
Travaux	Rappel aux conducteurs et aux agents de maintenance des procédures de sécurité

Table 6.3. Résilience suite à une mise en tension

Événement initiateur conduisant à un mode dégradé	Action résiliente
Anomalie de signal, raté d'ouverture	Maintenance curative, procédure de franchissement sur autorisation papier
Anomalie d'aiguille	Maintenance curative et choix d'un itinéraire alternatif

Table 6.4. Résilience suite à une dégradation

pas applicable ou indisponible. Cette responsabilité se traduit par l'application de procédures de sécurité et relève d'une part de la qualité de l'organisation du système ferroviaire qui définit ces procédures et la bonne application desdites procédures d'autre part. Le chapitre dédié aux systèmes ferroviaires dans le livre de l'ingénierie de la résilience [**70**] met l'accent sur la vétusté des communications dans les systèmes ferroviaires européens. En effet, l'application des procédures nécessite une bonne communication entre les différents acteurs de la circulation (superviseurs, conducteurs, agents de maintenance) dans le but de garantir la bonne application des procédures. Les auteurs du chapitre n'optent pas en faveur d'un système ferroviaire résilient, mais expliquent le haut niveau de sécurité de ce transport par la culture de sécurité qui a prévalu dans la conception et l'organisation du système ferroviaire. Pourtant, dans une représentation duale de la sécurité adoptée dans cette thèse, la culture de sécurité ne saurait à elle seule, expliquer ce niveau de sécurité.

Bien que non sécuritaire dans les modes normaux et stressés, l'activité de l'opérateur, de par sa vue globale du système, contribue de manière importante à la résilience du système. De nombreux accidents ont pu être évités par les opérateurs de supervision de trafic, de par leur connaissance et leur expérience du trafic. La difficulté réside dans l'évaluation de la résilience qui par essence contribue à la non-apparition d'événements remarquables et donc difficilement identifiables. Les tableaux 6.3, 6.4 et 6.5, fournissent quelques exemples des cas de résilience en situation de supervision de trafic ferroviaire classés en fonction des transitions de modes d'exploitation générés par les événements initiateurs.

Dans tout ce qui précède, il est possible de remarquer la différence d'allocation des tâches de résistance et de résilience entre l'opérateur humain et les systèmes de protection automatique. D'une manière générale, la résistance est allouée au système de protection automatique tandis que la résilience demeure du ressort de l'opérateur de supervision. L'exemple du contrôle aérien nuance ce propos, la résistance s'appuyant sur la qualité de l'organisation du fait de

Événement initiateur conduisant à un mode accidentel	**Action résiliente**
Anomalie de signal, raté de fermeture	Détection et protection des circulations (Blocage des itinéraires convergents, arrêt des circulations convergentes)
Franchissement de signal fermé	Commande de freinage d'urgence, tracé d'itinéraire vers une zone libre, destruction des itinéraires des circulations convergentes, *etc.*

TABLE 6.5. Résilience suite à un quasi-accident

l'impossibilité de recourir à une quelconque barrière technologique permettant de supprimer de manière efficace le potentiel de danger, comme cela est le cas dans le système ferroviaire où il est toujours possible d'arrêter les circulations.

6.5. Situations de supervision critique

Quelle que soit l'activité visitée, la supervision et le contrôle de la sécurité sont généralement bien séparés fonctionnellement. Cependant, cette distinction n'est plus valable du point de vue de l'activité humaine. Un même opérateur peut être amené dans son activité à utiliser le système de supervision et le système de contrôle dédié à la sécurité. Or, ces deux systèmes ne présentent pas le même type d'information, le système de supervision présente des informations de haut niveau (dans le sens où elles ont été traitées par des algorithmes afin de les rendre directement interprétables par l'opérateur) dont l'interprétation est facile, mais dont la fiabilité ne peut pas être démontrée en raison de la complexité du système de supervision. Le système dédié à la sécurité présente des informations de bas niveau, de grande fiabilité, mais dont l'interprétation nécessite une activité cognitive de haut niveau de la part de l'opérateur.

Il est alors possible d'identifier les scénarios du système susceptibles de transformer l'activité de superviseur (la plupart du temps passif) en une activité de contrôleur actif ayant une responsabilité directe de la sécurité, ces scénarios sont appelés scénarios de « supervision critique ». Ils apparaissent dans deux situations :

– Lorsque le système de supervision permet d'agir directement sur les barrières de sécurité. Le système de supervision devient temporairement un système de contrôle commande du système de protection. Dans cette perspective, le rôle de l'opérateur est d'accomplir des actions de type résistantes ou résilientes ;
– Lorsque l'opérateur humain, bien que normalement pas directement responsable de l'évolution et du contrôle d'une situation dangereuse, a la possibilité de récupérer cette situation. Il s'agit là des actions de type résilientes.

L'interface du système de supervision propose deux types de commandes. Les commandes de supervision sont celles qui sont protégées par les barrières fonctionnelles

6.6. Conclusion

Cet état de l'art industriel a permis d'identifier les scénarios critiques de supervision sur lesquels l'étude de sécurité doit se focaliser. Bien que généralement pas identifié comme une réelle barrière de sécurité, le système de supervision offre la possibilité aux opérateurs humains de réaliser des actions résistantes et résilientes. L'étude de ces actions doit être effectuée. La première question qui se pose consiste à déterminer la performance du couple opérateur humain et système de supervision à détecter les transitions d'un mode d'exploitation à un autre. Le chapitre suivant présente la deuxième phase de notre démarche qui consiste à évaluer cette performance sur un réel poste de supervision de trafic ferroviaire couplé à un simulateur de trafic.

CHAPITRE 7

EXPÉRIMENTATIONS

Résumé

Ce chapitre présente l'étude approfondie du comportement des opérateurs ATS à l'aide d'un environnement simulé. Cet environnement est constitué d'un réel produit ATS couplé à un simulateur de trafic ferroviaire, cette plateforme se nomme SPICA-RAIL pour « Supervision PICArde de transport par Rail ». L'objet des expérimentations consiste à évaluer la performance des opérateurs humains dans la tâche de détection d'anomalies constituant une tâche résistante (voir définition 6.1) visant à détecter toutes transitions vers un mode stressé ou dégradé et dans certains cas à anticiper des transitions accidentelles. Trois types d'incidents ont été testés, deux d'entre eux concernent des transitions vers un mode stressé ou dégradé, il s'agit d'événements du type « dysfonctionnement d'aiguille » et « raté d'ouverture d'un signal », le troisième événement testé concerne des transitions vers le mode accidentel, il s'agit de l'événement contraire à la sécurité nommé « raté de fermeture d'un signal ». Les expérimentations ont été menées sur des sujets novices apparentés à des opérateurs en formation, leur performance a été évaluée par le temps de détection d'une transition de mode de fonctionnement. Différentes variables ont été mises en évidence dans l'expérience en vue d'expliquer la performance des opérateurs à détecter ces transitions.

7.1. Introduction

L'évaluation des IHM dans les systèmes complexes ont fait l'objet de travaux réalisés par le Laboratoire d'Automatique, de Mécanique, et d'Informatique industrielles et Humaines [1] (LAMIH) dans le domaine des postes de supervision de trafic ferroviaire. Une démarche d'évaluation de l'IHM a été développée [**7, 6, 43, 44**] et appliquée au projet ASTRÉE « Automatisation de Suivi de Trains en temps RÉEl » de la SNCF. Basé sur une démarche visant à identifier en détail les tâches à effectuer puis à élaborer un modèle *a priori* du comportement probable de l'opérateur humain, il s'agit alors de définir les spécifications fonctionnelles et le besoin informationnel des opérateurs humains pour effectuer leur activité et de générer l'interface. L'expérimentation sur cette interface permet de confronter le modèle *a priori* avec les observations et d'enrichir les spécifications de l'IHM. Ces travaux ont donné des résultats satisfaisants permettant de fournir

1. http;//www.univ-valenciennes.fr/LAMIH/

un jugement sur la qualité des IHM et fournissent des éléments de modélisation de la tâche de l'opérateur [**7, 6, 43, 44**].

Notre objectif demeure l'évaluation de la sécurité, et notamment la perception que se font les opérateurs humains du mode d'exploitation dans lequel le système ferroviaire se situe. Dans cet objectif nous avons mis en place un plan d'expérience en collaboration avec des spécialistes de la psychologie cognitive visant à déterminer l'efficacité de la perception du mode d'exploitation dans lequel se situe le système supervisé. Les résultats de ces observations seront mis à contribution de l'étude interdisciplinaire d'évaluation de la sécurité.

La première partie de ce chapitre est consacrée à la description générale des fonctionnalités de la plateforme SPICA-RAIL. On présente ensuite les modifications qui ont été apportées à la plateforme afin de disposer d'un environnement de simulation généralisable au plus grand nombre d'applications ferroviaires. Enfin, les éléments qui ont permis de déployer la simulation sont explicités.

La deuxième partie est consacrée à la présentation des expériences qui ont eu lieu sur la plateforme SPICA-RAIL. Le protocole expérimental sera présenté ainsi que les résultats de l'expérience.

7.2. Plateforme SPICA-Rail

7.2.1. Description. — Le produit choisi pour l'environnement de simulation est un produit du commerce développé par ALSTOM Transport sous le nom d'ICONIS. Celui-ci appartient à la classe de systèmes nommée *Automatic Train Supervision* ou ATS. Les ATS représentent la nouvelle génération de systèmes intégrés de gestion de trafic ferroviaire. Un rapport technique a été rédigé pour le projet SPICA-RAIL [**25**] et détaille les fonctionnalités de la plateforme.

7.2.2. Analyse fonctionnelle du produit ICONIS. — Les principales fonctions fournies par l'ATS sont :

- gestion des équipements de signalisation ;
- surveillance des équipements ATP et ATS ;
- suivi des trains ;
- identification des trains ;
- routage des trains ;
- gestion des alarmes et événements.

Les opérateurs disposent directement de toutes ces informations via l'IHM (Stations de travail, ou Tableau de Contrôle Optique) et passent leurs commandes via cette IHM.

Les paragraphes suivants présentent brièvement les différents systèmes constituant l'ATS.

7.2.2.1. Gestion des équipements de signalisation (SIG). — Chaque équipement de signalisation est géré comme une classe d'objets. Voici une liste des principaux objets :

- signal : matérialisé par un feu de circulation sur le bord de la voie ;
- Circuit de Voie (CDV) : mécanisme de détection d'occupation d'une partie de voie ;
- aiguille : appareil de voie permettant de connecter deux voies ;
- direction du trafic ;
- cycles : gestion automatique des itinéraires de retournement des trains dans les terminus ;

– bloc de maintenance : ensemble prédéfini d'itinéraires dont la formation automatique ou manuelle est interdite pour raison de travaux sur la voie ;
– signal général d'arrêt d'urgence des circulations ;

L'objet représentatif d'un équipement possède des attributs typés (ex : couleur de signal, état d'un CDV, *etc.*). Ainsi, l'état d'un objet est complètement défini par l'affectation d'une valeur à chacun de ses attributs. Des équations logiques, aussi appelées invariants dans la suite du chapitre, permettent de restreindre l'ensemble des états autorisés. Les invariants sont implémentés lors de la phase de paramétrage (ou configuration) de l'application. Par exemple, un itinéraire est défini par plusieurs attributs : destruction automatique/tracé permanent ; tracé/non tracé ; actif/non actif.

Le système SIG permet de :

– surveiller l'état des équipements de signalisation. Ces états sont utilisés par les autres fonctions de l'ATS notamment : l'interface Homme-Machine pour l'animation des vues, l'« Automatic Route Settings » (ARS) pour le routage des trains et « Train Describers » (TDS) pour le suivi des trains ;
– commander les équipements de signalisation via des commandes classiques ou sécurisées (les commandes sécurisées sont basées sur le protocole HILC) ;
– de vérifier la faisabilité des commandes en fonction des équations logiques d'enclenchement du terrain (reproduites dans l'ATS afin de ne pas solliciter inutilement les systèmes d'enclenchements).

Les commandes de signalisation sont de deux types :
– les commandes classiques (non sécurisées) utilisées pour la gestion des commandes dont l'effet est protégé par des systèmes de protection tels que les enclenchements ;
– les commandes sécurisées (HILC) dotées d'un mécanisme de double commande intégrant une somme de contrôle utilisées pour les commandes sans boucles de rattrapage technologiques : blocage/déblocage de signal, blocage/déblocage d'aiguille, *etc.*

7.2.2.2. Gestion de l'ATC (ATC). — Le système « Automatic Train Control » (ATC) est le système embarqué (à bord des trains et sur la voie) de gestion du mouvement automatique des trains. Il contient les deux composants suivants :

– « Automatic Train Protection » ATP : système sécuritaire permettant de détecter le franchissement des règles d'exploitation (dépassement de vitesse, dépassement de signal fermé et le contrôle des distances de sécurité notamment) ;
– « Automatic Train Operation » ATO : pilotage partiellement ou totalement automatique des trains.

L'ATS communique avec l'ATC afin :
– de réguler les trains sur la ligne ;
– de collecter les informations de maintenance des équipements embarqués et au sol ;
– d'identifier les trains à travers la réception et le traitement des messages du système d'identification des trains (PTI).

De plus, l'opérateur dispose de commandes sécurisées HILC permettant de restreindre la vitesse des trains sur certaines portions de voie. Il s'agit des restrictions temporaires de vitesse.

7.2.2.3. Suivi de train (TDS). — Cette fonction gère le mouvement des trains, leur identification et leur affichage.

Cette fonction permet aux opérateurs de déterminer à tout moment la position et l'identité des trains circulant sur la voie.

Le système TDS détecte les mouvements de trains et leurs arrêts en se basant sur l'état des équipements de signalisation (par exemple l'occupation ou la libération des circuits de voie, la position des aiguilles, …).

En mode dégradé, afin d'éviter de perturber l'opérateur avec des informations erronées, TDS discrimine les vraies occupations de circuit de voie (présence d'un train sur le CDV) des fausses occupations (CDV en panne, encombrement de la voie, *etc.*). L'opérateur est averti par alarme lorsqu'un train reste bloqué entre deux stations.

7.2.2.4. Identification des trains (PTI). — Cette fonction gère la renumérotation des trains. La numérotation des trains peut être :

- manuelle, suite à des commandes opérateurs ;
- automatique en fonction de la table horaire courante ou numérotation par défaut en cas d'erreurs détectées.

La gestion de l'identification des trains permet de suivre tous les trains sur la ligne grâce à l'interface entre l'ATS et le système ATC. L'ATS corrèle l'identification courante du train avec celle reçue par le système d'identification PTI.

7.2.2.5. Routage automatique des trains (ARS). — Tout itinéraire peut être tracé manuellement par l'opérateur ou automatiquement par l'ATS.

En mode automatique (ARS activé), cette fonction détermine les itinéraires à former et demande la formation à l'heure appropriée. L'itinéraire à tracer est généralement déduit de la table horaire, mais il peut être déterminé par la destination du train.

Les requêtes sont déclenchées à l'heure prévue de départ du train ou sur passage en des points particuliers (points d'approche) afin que l'itinéraire soit formé devant le train sans l'obliger à ralentir.

ARS gère également la priorité des trains aux points de jonction et aux cycles en terminus.

Cette fonctionnalité n'a pas été utilisée directement pour l'expérience, le tracé automatique des itinéraires a été implémenté au niveau du simulateur de trafic qui permet de contrôler dynamiquement les itinéraires à l'aide d'un langage de scripts (voir paragraphe 7.2.4).

7.2.2.6. Gestion des alarmes et des événements (A&E). — Cette fonction gère les alarmes et les événements en générant et affichant les alarmes (ex : discordance d'aiguille) et les événements (changement d'état d'occupation d'un CDV) nécessitant l'attention de l'opérateur ATS. De plus, cette fonction permet l'enregistrement des alarmes et des événements dans une base historique afin de permettre des analyses ultérieures.

Cette fonctionnalité a été débranchée pendant l'expérience afin de focaliser l'étude sur la surveillance du TCO.

7.2.3. Fonctionnalités de l'application livrée par ALSTOM Transport. — Le but de cette section est de fournir une description générale des fonctionnalités de l'ATS qui sont mises en œuvre sur la plateforme expérimentale actuellement installée à Compiègne.

7.2.3.1. Architecture. — L'architecture de la plateforme est une restriction de la configuration de la plateforme d'intégration du projet New-Delhi (NWD). L'ATS de NWD gère deux lignes, un métro et un réseau express urbain (RER). Le RER de NWD est constituée de cinq zones de supervision dont un dépôt.

La plateforme SPICA-RAIL est restreinte à « NWD-RER » constitué du dépôt et de trois des quatre zones de supervision (la quatrième est en cours d'installation) :

– un poste central ATS : serveur central contenant une IHM centrale des trois zones de supervision ;
– un poste local ATS : serveur local d'une zone de supervision et IHM des trois locaux ;
– un poste dépôt : serveur dépôt et l'IHM du dépôt ;
– un poste pour le simulateur modulaire : serveur de communication, contient également le serveur du deuxième local ATS ;
– un poste pour le simulateur de trafic : simulation du terrain, c'est le poste d'animation des expérimentations, il contient également le serveur du troisième local ATS.

La figure 7.1 représente l'architecture du réseau de la plateforme.

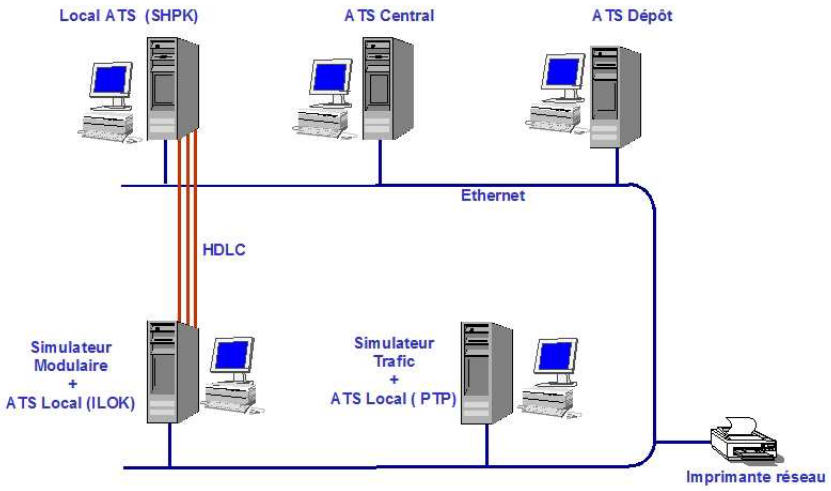


FIGURE 7.1. Réseau plateforme SPICA-RAIL

7.2.3.2. Gestion de la ligne. — La gestion de la ligne RER disponible dans les locaux du laboratoire HEUDIASYC est de type centralisé *i.e.* :

– l'opérateur du poste central possède l'autorité sur l'ensemble de la ligne.
– il est possible de contrôler une zone depuis son poste localisé. Les autorisations de contrôle sont fournies par le poste central grâce au système TAS.

Un tableau de contrôle optique (TCO) est projeté sur un écran en face des opérateurs. La figure 7.2 est une copie d'écran de l'image projetée au TCO. Le TCO représente l'ensemble du trafic et en particulier les points suivants :

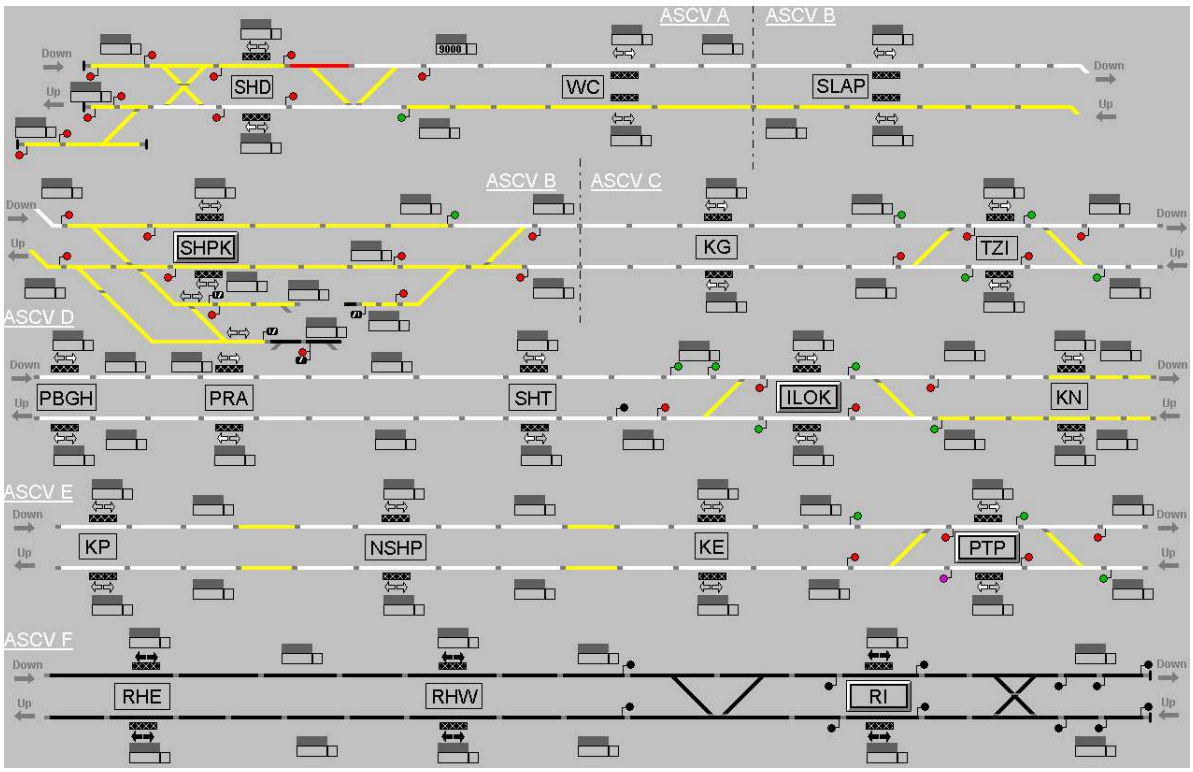


FIGURE 7.2. Tableau de Contrôle Optique

– La topologie du réseau qui est définie dans un espace à une dimension par une succession de circuit de voie (CDV) ;
– Lorsqu'un train est présent sur un CDV, celui-ci prend la couleur rouge. Certains CDV ont à leur proximité un équipement nommé *berth* (trad. affichage de l'index de train) qui permet de donner le numéro d'un train lorsque celui-ci est proche de la zone en question. Par exemple, sur la figure 7.2, nous pouvons remarquer le train 9000 entre les stations SHD et WC ;
– Les élements de signalisation SIG.

Le serveur de communication appelé simulateur modulaire, assure la liaison entre l'ATS et les équipements simulés (ATC, voie, trains, plateforme, *etc.*) par le simulateur de trafic.

7.2.4. Le simulateur de trafic. — Le simulateur de trafic anime l'ATS grâce à un système de création et d'exécution de scénarios. Le langage de création de scénarios est formé de primitives permettant de réaliser les actions de base comme l'injection de trains sur les voies, la formation d'itinéraires, la modification de la vitesse des trains, *etc.*

Le simulateur de trafic dispose d'une interface homme-machine représentant la copie du plan de voie simulé dans l'ATS. Des commandes peuvent être exécutées directement sur cette interface et modifient le comportement des équipements sur l'ATS.

Le simulateur de trafic a été utilisé pour préparer et contrôler le mode nominal d'exploitation. Plusieurs scénarios (scripts) ont été nécessaires, afin de contrôler les itinéraires en tracé permanent, de simuler le système de tracé automatique des itinéraires (itinéraire en destruction

automatique), de simuler les circulations conformément au mode nominal et enfin d'injecter des dysfonctionnements sur les équipements.

Les trains sont considérés comme l'élément principal de l'outil de simulation. Un train est caractérisé par sa position et sa vitesse. Sa position est donnée par le numéro de circuit de voie occupé. La vitesse du train est une variable de type entier naturel, la cinématique des trains n'est pas simulée, le simulateur accélère un train instantanément à une valeur de vitesse qui reste constante. La primitive du langage de script qui permet d'insérer un train consiste à dynamiser l'occupation des circuits de voie en fonction de la vitesse voulue et la longueur des circuits de voie.

Les éléments circuits de voie, aiguilles, signaux, itinéraire, *etc.*, sont contrôlés à partir du simulateur par deux primitives permettant pour l'une d'acquérir la valeur d'une variable de l'ATS et l'autre de modifier cette valeur, ces primitives sont les suivantes :

– *Remote Monitoring* : la primitive *readRM* est utilisée pour lire la valeur d'une variable ATS ;
– *Remote Calling* : la primitive *applyRC* est utilisée pour modifier la valeur d'une variable de l'ATS

Le langage de script dispose également des éléments d'affectation de variables (`varId := val`), des boucles de contrôle de type alternative (`IF ...THEN ...ELSE ...`) et de type répétitif (`EXEC ...UNTIL condition`). Le langage permet également de traiter plusieurs processus en parallèle, cette fonctionnalité est nécessaire pour animer plusieurs trains sur la voie et pour simuler le système de tracé automatique des itinéraires. Le simulateur dispose donc d'une horloge maître qu'il est possible d'utiliser pour gérer l'aspect temporel de la simulation (horaire des trains notamment). Le nombre de processus est toutefois limité à 20. Le système de tracé automatique des itinéraires consomme quatre processus (un pour chaque sens de circulation au niveau de la bifurcation et un au niveau deux au niveau des voies d'évitement), le tracé des itinéraires en mode permanent consomme un processus. Il reste donc 15 processus pour simuler les trains. Cette limitation est imposée par la capacité de traitement du noyau temps réel du simulateur. Le simulateur ne permet pas de créer des procédures et des fonctions, la modularisation est effectuée au niveau des scripts exécutés par le noyau temps réel.

La figure 7.3 présente un script permettant d'ouvrir l'itinéraire `R04B_05B` lorsqu'un train se présente en amont. On place dans une boucle infinie, une primitive permettant de détecter la présence du train — `searchTrain("TC30B", train_num_30B);` — lorsque celui-ci est détecté — `IF (train_num_30B <> -1)` — alors on ouvre l'itinéraire — `THEN applyRC(R04B_05B, "RC") .`

La primitive `searchTrain` utilise dans sa définition une primitive `callRM`.

Deux autres primitives importantes permettent d'insérer un train et de modifier la vitesse d'un train. Il s'agit de la primitive `injectTrain` qui prend comme paramètre le numéro de deux circuits de voies consécutifs permettant de positionner le train et de lui donner la direction du premier circuit de voie vers le second, le dernier paramètre est le numéro du train identifiant le processus dans l'environnement de simulation. La primitive `modifyTrainSpeed`, comme son nom l'indique, modifie la vitesse d'un train, ses paramètres sont le numéro identifiant le processus du train et la valeur de la vitesse désirée (entier naturel).

```
boucle  := FALSE;
EXEC
       PAUSE(2);
       # Recherche d'un train sur TC_30B
       searchTrain("TC30B",train_num_30B);
       # Un train sur TC_30B
       IF (train_num_30B <> -1) THEN applyRC(R04B_05B, "RC");
       ENDIF;
UNTIL boucle ENDEXEC;
```

FIGURE 7.3. Script permettant d'ouvrir un itinéraire

La gestion de la table horaire a été effectuée à l'aide d'un script qui injecte les trains et positionne leur vitesse à différents instants de la simulation. Les trains évoluent ensuite conformément aux règles de circulation imposées par les systèmes d'enclenchements (simulés également par le simulateur de trafic).

Le système de tracé automatique des itinéraires a été implémenté grâce à un processus qui détecte les trains en fonction de leur numéro et de leur instant de passage en des points particuliers de la voie où plusieurs itinéraires sont possibles. Le processus trace l'itinéraire que le train détecté doit suivre dans la planification.

L'injection de dysfonctionnements se fait en temps réel par un expérimentateur manipulant directement les objets sur l'interface homme-machine du simulateur de trafic. Une autre façon de faire, consiste à exécuter au moment voulu (à l'aide de l'horloge de simulation), un script positionnant l'état d'un équipement à la valeur « défaillant » ou en forçant son état à une valeur contraire à la sécurité.

7.2.5. Migration vers une application ferroviaire. — Les fonctionnalités présentées dans la section précédente ont été réalisées dans le cadre de la supervision d'un trafic de type RER. Le trafic ferroviaire grandes lignes dispose de caractéristiques plus générales. Dans une certaine mesure, les applications urbaines (métro ou RER) ou très homogènes (Lignes Grande Vitesse) sont autant de déclinaisons simplifiées du cadre ferroviaire général.

L'obtention de cette généralisation passe par une analyse des spécificités ferroviaires.

7.2.5.1. Analyse des besoins. — Le cadre général ferroviaire est défini par la plus grande complexité d'exploitation et notamment :

- des marches de trains (vitesses) hétérogènes ;
- différents types de circulation aux conditions d'exploitation disparates ;
- des interconnexions avec d'autres réseaux et/ou lignes ;
- un réseau étendu géographiquement.

Ces caractéristiques impliquent l'utilisation d'éléments de topologie de la voie spécifiques présentés dans le document *Éléments pour le schéma d'une ligne ferroviaire* par M. Rigaud (Sigma-Conseil) [**112**].

L'implémentation d'un réseau avec interconnexions est réalisée au moyen de l'élément de topologie *Bifurcation* (voir figure 7.4). Le trafic peut ainsi être connecté à une nouvelle destination supervisée par un autre poste.

L'élément de topologie *Voie d'évitement* (voir figure 7.4) qui permet le dépassement de circulations est un outil de régulation « en espace » et offre ainsi la possibilité de faire circuler des trains aux conditions d'exploitations différentes.

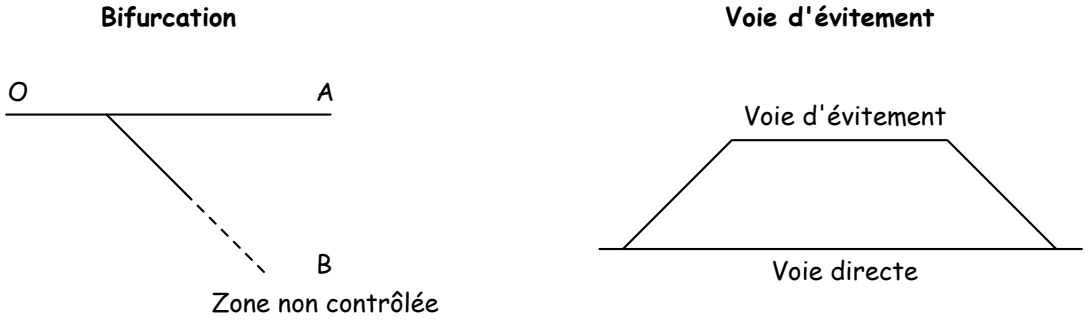


FIGURE 7.4. Bifurcation et voie d'évitement

Un autre aspect lié au ferroviaire est le programme associé à chaque train. Les programmes peuvent se différencier selon les variables suivantes :

- la marche des trains ;
- les itinéraires ;
- les arrêts commerciaux : des trains peuvent parcourir le même itinéraire à la même vitesse mais ne pas s'arrêter aux mêmes stations.

7.2.5.2. Fonctionnalités ferroviaires choisies. — Le mode de fonctionnement de l'ATS adapté est manuel. Nous n'utilisons pas le mode *Constant Headway* car il n'intervient pas dans le contexte ferroviaire.

À partir d'une analyse des fonctionnalités ferroviaires, le plan de voie suivant (voir figure 7.5) a été défini. Il comporte une bifurcation et une voie d'évitement pour chaque sens.

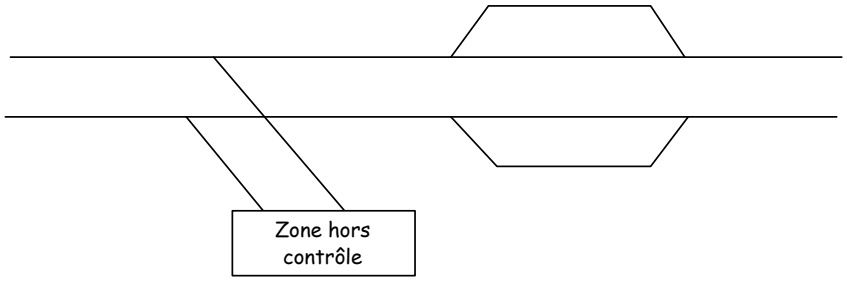


FIGURE 7.5. Plan de voie

Différents programmes pour les trains ont été définis :

- trois types de vitesse : rapide, moyen et lent ;
- différents types d'itinéraires liés à la présence de la bifurcation et la voie d'évitement ;
- différentes missions commerciales (arrêts en station).

7.2.5.3. Modifications réalisées. — Le plan de voie original inclut une bifurcation. Elle permet de garer les trains dans le dépot. Afin de répondre aux exigences ferroviaires, cette bifurcation sera supposée être connectée à un réseau ferré connexe, la gestion du dépôt n'intervient pas dans la simulation.

La réalisation de la voie d'évitement a été plus compliquée. En effet, il a été nécessaire de modifier le plan de la voie de l'ATS et du simulateur. Les modifications consistent à introduire de nouveaux équipements (circuit de voie, itinéraires, signaux, aiguilles, plateforme, *etc.*) et en supprimer.

La figure 7.6 présente de manière détaillée les deux voies d'évitement sur le secteur de supervision modifié.

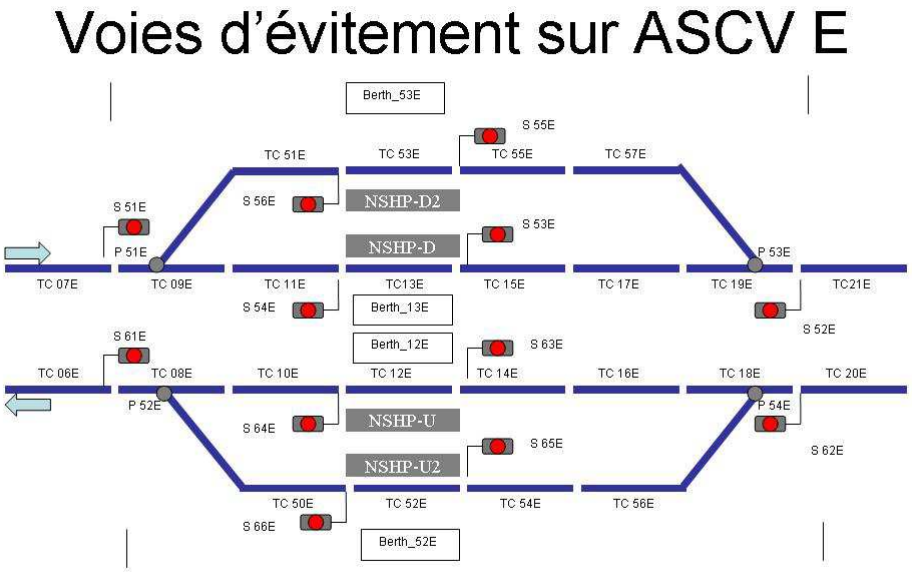


FIGURE 7.6. Voie d'évitement

L'introduction de nouveaux équipements s'accompagne de la définition d'invariants fonctionnels et de sécurité. Ils permettent de restreindre l'espace des états autorisés. Ces invariants sont traduits dans l'ATS et dans le simulateur.

La modification de la spécification a nécessité un travail d'analyse afin d'éviter l'introduction d'incohérences dans le système. C'est un problème sensible. En effet, la modification d'une spécification a des répercussions sur l'ensemble du système. Elle peut introduire des fonctionnalités qui ne sont pas compatibles avec d'autres.

Afin d'éviter les incohérences, la démarche suivie a été la suivante :

– Les nouvelles spécifications ont été traduites dans l'ATS à partir du langage de paramétrage du produit ICONIS d'ALSTOM Transport. Ceci nécessite de compiler à nouveau l'application

ATS relative au secteur modifié. Un compilateur existant a permis de détecter certaines classes d'erreurs par exemple, les redondances ou les erreurs syntaxiques.
– Les nouvelles spécifications ont été traduites dans le simulateur. Les spécifications étant exprimées dans un autre langage, cela rend nécessaire une lecture critique et croisée et ainsi de détecter les erreurs de sémantique *i.e.* de répondre à la question suivante : Est-ce que les spécifications répondent au problème posé ?
– Les deux points précédents relèvent de l'analyse statique. Une fois les spécifications introduites dans le simulateur, il est ensuite possible de les animer afin de réaliser une analyse dynamique et de vérifier la cohérence du système.

La figure 7.7 présente le TCO après les modifications.

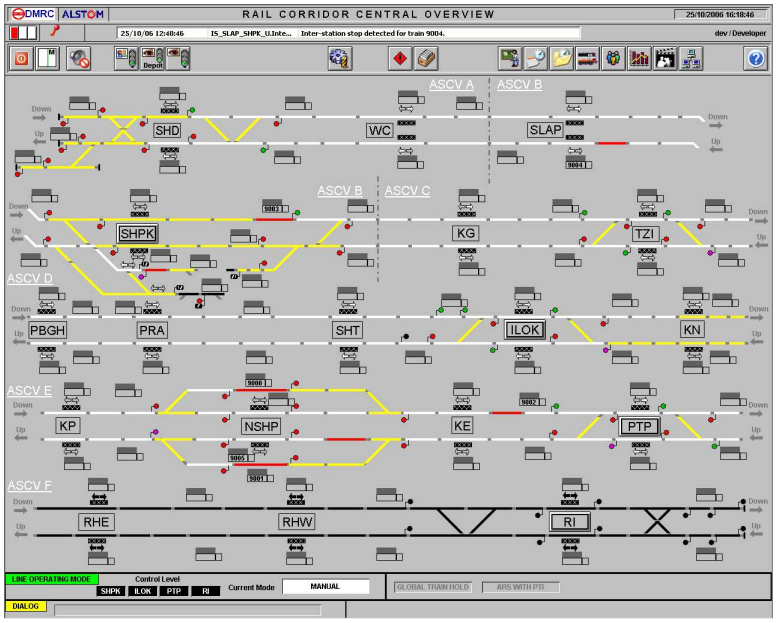


FIGURE 7.7. TCO après modifications

7.3. Procédure expérimentale

Le cadre théorique et la méthodologie utilisés dans cette partie du projet sont ceux de la psychologie cognitive et de la psychologie ergonomique cognitive. La réalisation des procédures expérimentales ainsi que les expériences ont été réalisées en collaboration avec les chercheurs de l'Université de Picardie Jules Verne (UPJV) , membres du laboratoire ECCHAT [(2)] « Efficience Cognitive dans les Conduites Humaines d'Apprentissage et de Travail ».

La procédure expérimentale a fait l'objet de trois communications [**22, 24, 18**].

2. http://www.u-picardie.fr/labo/ecchat/

7.3.1. Préambule. — L'apport de la psychologie cognitive se situe essentiellement sur le plan théorique en fournissant des outils conceptuels permettant de comprendre le fonctionnement cognitif d'un agent de circulation assurant une tâche de supervision et de contrôle de trafic ferroviaire. L'opérateur est ici conçu exclusivement d'un point de vue cognitif, c'est-à-dire comme un système de traitement de l'information à capacité limitée capable d'acquérir, de stocker, d'utiliser des connaissances déclaratives et procédurales dans un environnement de travail.

L'apport de la psychologie ergonomique cognitive se situe quant à lui sur un plan à la fois conceptuel et méthodologique. Sur le plan conceptuel, deux champs d'études qui ont été abondamment abordés par cette discipline sont pertinents dans le cadre de l'évaluation de l'agent circulation : la supervision et le contrôle de processus en situations dynamiques d'une part, et la coopération homme-machine d'autre part.

L'adoption de cette double approche nous conduit, *a priori*, à considérer le couple *homme - machine* comme un système à part entière et non de manière séparée. Ainsi, l'objectif général de l'étude psychologique et ergonomique est de caractériser l'adaptation du système *opérateur - ats* à son environnement et aux tâches qu'il est censé assurer [**66**]. Plus précisément, l'objectif est de déterminer à l'aide d'expérimentations dans un environnement de simulation réalisé à partir d'un ats existant, en l'occurrence la plateforme Spica-rail, dans quelle mesure le système formé par le couple *opérateur - ats* permet d'assurer la supervision et le contrôle efficace et sûr d'une situation de trafic ferroviaire.

La première étape a consisté à effectuer une revue des principaux travaux réalisés en ergonomie sur la gestion du trafic ferroviaire en France et à l'étranger (principalement en Europe) de manière à compléter les données obtenues grâce aux visites de sites effectuées dans le cadre de l'état de l'art industriel de la supervision.

La seconde étape a consisté à utiliser l'ensemble des éléments recueillis et analysés lors de la première étape afin de :

- Poser les problèmes particuliers de la gestion du trafic ferroviaire par un ats ;
- Identifier les principales contraintes (notamment techniques liées à l'intégration d'une plateforme ats d'expérimentation) ;
- Identifier les éléments nécessaires aux simulations et les reproduire en mode simulé sur la plateforme expérimentale ;
- Sélectionner les situations dégradées à simuler et construire les scénarios.

La troisième étape est dédiée aux expérimentations dans l'environnement de simulation. Cette étape comprend trois phases :

- Une phase de formation des sujets au métier d'agent circulation et à l'utilisation de la plateforme ;
- Une phase de réalisation des simulations ;
- Une phase d'analyse des données obtenues lors des expérimentations.

7.3.2. Expérimentation sur des sujets novices. — D'un point de vue cognitif, l'interface de l'ats peut être vue comme un stimulus complexe présentant des éléments statiques (*ex* : les voies, les gares, *etc.*) et des éléments dynamiques (les éléments représentant la position des aiguilles, l'occupation successive des circuits de voies, l'état des signaux, *etc.*). À partir de ce stimulus

(Tableau de Contrôle Optique ou TCO, écran du poste informatique) destiné à représenter une situation distante, l'opérateur (agent de circulation) est censé détecter le plus rapidement possible les anomalies susceptibles de perturber plus ou moins gravement la circulation des trains sur une ligne ferroviaire et d'en affecter la sécurité.

L'expérience qui a été menée sur la plateforme SPICA-RAIL avait pour objectif d'analyser l'effet de la présentation des informations de l'interface de l'ATS sur la vitesse de détection d'anomalies chez des utilisateurs non experts dans le but d'utiliser ultérieurement les résultats de cette analyse pour apporter des améliorations à l'ergonomie de l'interface.

L'étude se focalise plus particulièrement sur le comportement de détection d'anomalies affectant deux types d'installations, les signaux et les aiguilles, compte tenu de l'importance que revêtent ces éléments pour assurer la sécurité des circulations.

L'intérêt de recourir à des sujets non experts se situe au moins à deux niveaux :

– Le premier est que ces sujets, compte tenu de leur inexpérience, peuvent être assimilés dans une certaine mesure à des agents en formation. De fait, les résultats de la présente étude, outre leur intérêt pour l'amélioration de l'interface, fournissent des informations utiles pour la conception de dispositifs de formation de nouveaux agents ;
– Le second est que des sujets non experts peuvent s'avérer plus adaptés pour révéler les insuffisances d'un dispositif d'aide que des sujets ayant une grande expertise. Les premiers sont plus dépendants dudit dispositif tandis que les seconds sont capables de pallier les manques par leur expérience et ainsi occulter involontairement les défauts éventuels.

L'étude s'est déroulée en trois phases :
– Création d'une situation de trafic nominal et élaboration de scénarios comportant des déviations par rapport au nominal (situations dégradées) ;
– Formation de sujets non experts à l'utilisation (*i.e.*, détection d'anomalies) de l'interface de l'ATS de la plateforme expérimentale SPICA-RAIL ;
– Expérimentation et recueil des données.

La constitution du matériel expérimental a nécessité la création d'une ligne ferroviaire simplifiée, la planification d'un trafic théorique (*i.e.*, situation nominale), la création d'un graphe espace - temps, l'implémentation du trafic dans le simulateur et la création de scenarii simulant des situations dégradées (*i.e.*, présentant des anomalies de fonctionnement d'aiguilles ou de signaux).

7.3.3. Création d'une ligne ferroviaire simplifiée. — La ligne ferroviaire simulée dans l'expérience est schématisée dans la figure 7.8. Elle comporte deux voies (1 et 2) ainsi que deux voies d'évitement, deux gares commerciales, un dépôt et une bifurcation. Les flèches indiquent le sens de circulation des trains sur les voies 1 et 2 ainsi que sur la voie menant au dépôt.

La figure 7.9 présente la structure de la ligne telle qu'elle est représentée dans l'interface SPICA-RAIL. Les flèches indiquent le sens de circulation, les parties grisées correspondent aux parties de la ligne qui n'ont pas été implémentées sur la plateforme.

La figure 7.10 présente la vue de l'interface SPICA-RAIL opérationnelle lors des expériences. Les zones non utilisées apparaissent hachurées. Les zones hachurées en rouge correspondent

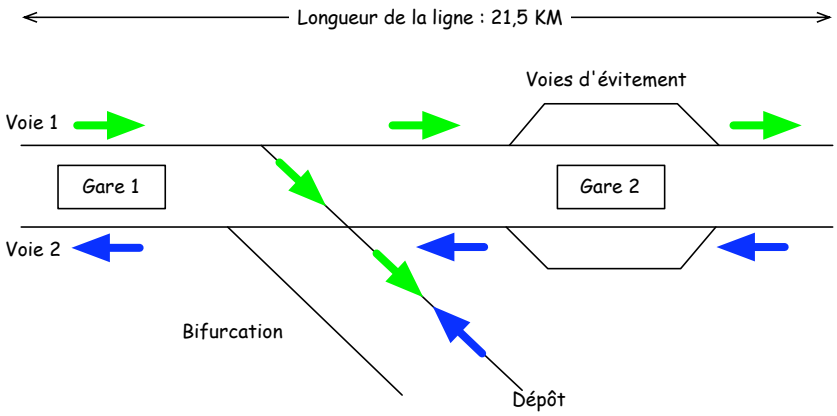


FIGURE 7.8. Ligne ferroviaire simplifiée

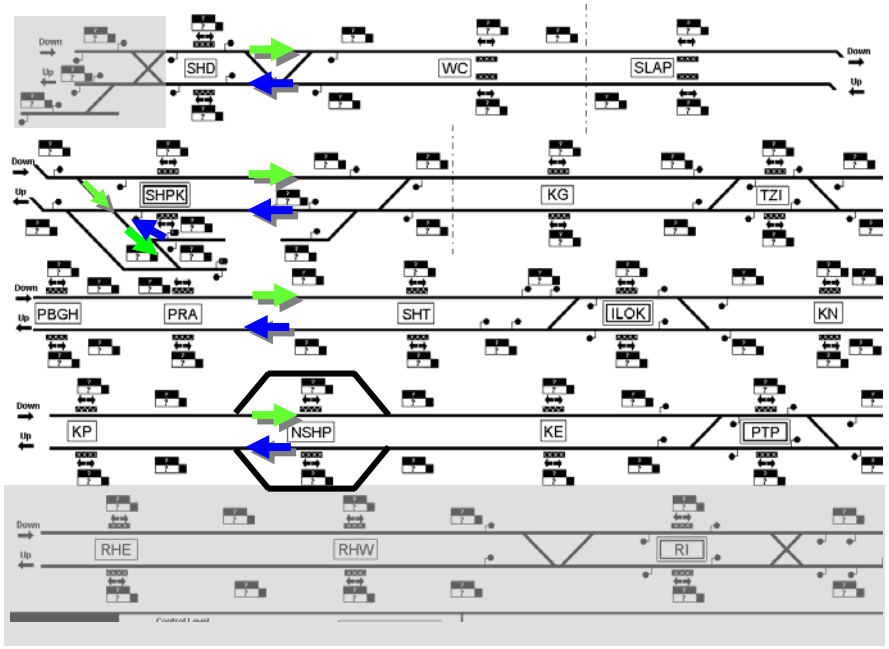


FIGURE 7.9. Structure de la ligne

aux zones non implémentées sur la plateforme, la zone hachurée en bleu correspond à la fenêtre d'alarmes.

7.3.4. Trafic théorique (mode nominal). — Le travail des opérateurs chargés de la planification du trafic ferroviaire, c'est-à-dire de la conception « *off-line* » des tables horaires, nécessite qu'ils anticipent la séquence opérationnelle des événements futurs. Plus précisément, ils doivent se poser les questions suivantes :

- Quel train arrivera, où et quand ?
- Quel va être l'impact des restrictions de voies sur la table horaire ?
- Comment gérer au mieux le flux ?

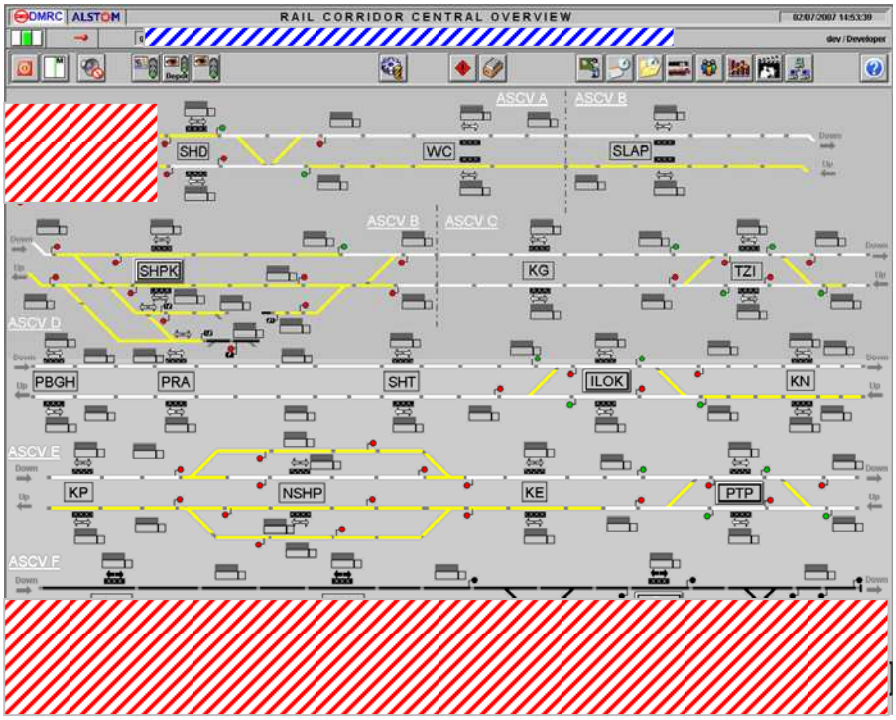
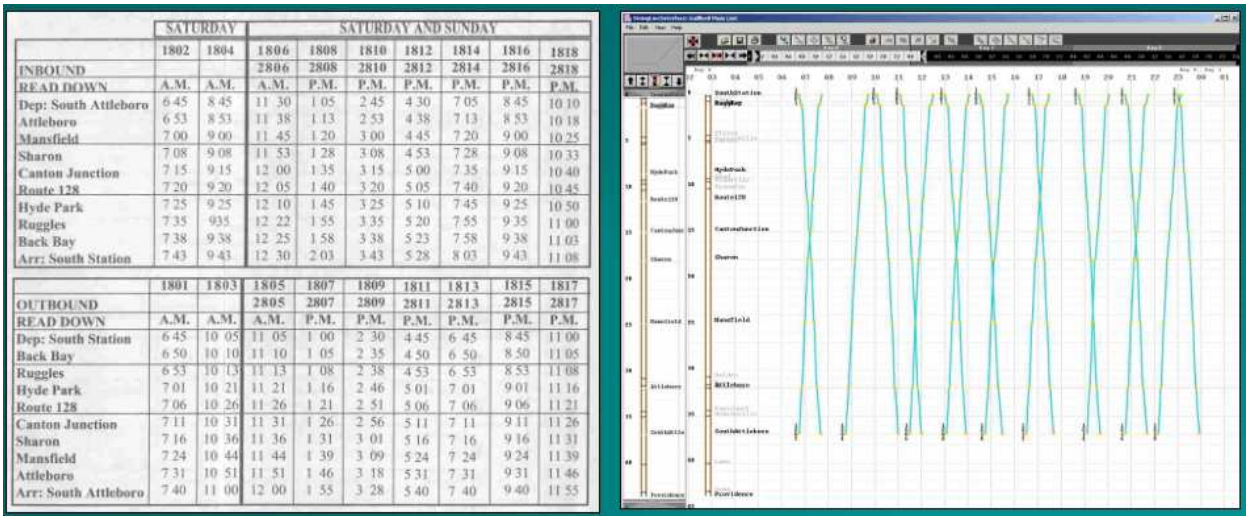


FIGURE 7.10. Vue opérationnelle de la ligne

Pour réaliser cette tâche, la méthode généralement utilisée consiste à construire un graphe espace-temps puis à le traduire en tableaux (table horaire ou tableau de succession des trains). La principale différence entre le graphe espace-temps et la table horaire réside dans le fait que le graphe espace-temps (voir figure 7.12) présente les mouvements des trains sous une forme continue et partiellement analogique tandis que la table horaire représente ces mêmes voyages sous une forme discrète et digitale. Le graphe espace-temps permet de visualiser plus facilement que la table horaire, les risques de conflits entre trains, voir figure 7.11.

Dans les graphes espaces-temps classiques, le temps est représenté sur un axe (généralement l'axe des abscisses) alors que la position (l'espace) est représentée sur l'autre axe. À l'intérieur du graphe le comportement théorique de chacun des trains est représenté par une ligne à laquelle est associé le numéro d'identification du train. La figure 7.12 fournit les indications nécessaires à la lecture d'un graphe espace-temps.

Dans cet exemple fictif, deux trains circulent en sens inverse sur une ligne à double voie. Les droites représentées dans le graphe espace-temps représentent le comportement de chacun des trains (droite rouge = comportement du train 1 ; droite noire = comportement du train 2). Dans cet exemple il existe une correspondance parfaite entre l'état du trafic planifié dans le graphe espace-temps (en bas) et la position que doivent normalement occuper les trains sur les voies si le planning est parfaitement respecté (situation nominale). Conformément à ce qui est prévu les deux trains se croisent à 8H50 au km 125. Il est à noter ici que, comme les deux trains circulent sur des voies différentes, le croisement des deux droites dans le graphe espace-temps ne désigne pas une situation de conflit entre les deux trains.



	SATURDAY		SATURDAY AND SUNDAY						
	1802	1804	1806	1808	1810	1812	1814	1816	1818
INBOUND			2806	2808	2810	2812	2814	2816	2818
READ DOWN	A.M.	A.M.	A.M.	P.M.	P.M.	P.M.	P.M.	P.M.	P.M.
Dep: South Attleboro	6 45	8 45	11 30	1 05	2 45	4 30	7 05	8 45	10 10
Attleboro	6 53	8 53	11 38	1 13	2 53	4 38	7 13	8 53	10 18
Mansfield	7 00	9 00	11 45	1 20	3 00	4 45	7 20	9 00	10 25
Sharon	7 08	9 08	11 53	1 28	3 08	4 53	7 28	9 08	10 33
Canton Junction	7 15	9 15	12 00	1 35	3 15	5 00	7 35	9 15	10 40
Route 128	7 20	9 20	12 05	1 40	3 20	5 05	7 40	9 20	10 45
Hyde Park	7 25	9 25	12 10	1 45	3 25	5 10	7 45	9 25	10 50
Ruggles	7 35	935	12 22	1 55	3 35	5 20	7 55	9 35	11 00
Back Bay	7 38	9 38	12 25	1 58	3 38	5 23	7 58	9 38	11 03
Arr: South Station	7 43	9 43	12 30	2 03	3 43	5 28	8 03	9 43	11 08

	1801	1803	1805	1807	1809	1811	1813	1815	1817
OUTBOUND			2805	2807	2809	2811	2813	2815	2817
READ DOWN	A.M.	A.M.	A.M.	P.M.	P.M.	P.M.	P.M.	P.M.	P.M.
Dep: South Station	6 45	10 05	11 05	1 00	2 30	4 45	6 45	8 45	11 00
Back Bay	6 50	10 10	11 10	1 05	2 35	4 50	6 50	8 50	11 05
Ruggles	6 53	10 13	11 13	1 08	2 38	4 53	6 53	8 53	11 08
Hyde Park	7 01	10 21	11 21	1 16	2 46	5 01	7 01	9 01	11 16
Route 128	7 06	10 26	11 26	1 21	2 51	5 06	7 06	9 06	11 21
Canton Junction	7 11	10 31	11 31	1 26	2 56	5 11	7 11	9 11	11 26
Sharon	7 16	10 36	11 36	1 31	3 01	5 16	7 16	9 16	11 31
Mansfield	7 24	10 44	11 44	1 39	3 09	5 24	7 24	9 24	11 39
Attleboro	7 31	10 51	11 51	1 46	3 18	5 31	7 31	9 31	11 46
Arr: South Attleboro	7 40	11 00	12 00	1 55	3 28	5 40	7 40	9 40	11 55

FIGURE 7.11. Exemple de table horaire et le graphique espace-temps correspondant, [**88**]

Dans le graphe espace-temps classique (espace en ordonnées et temps en abscisse), les variations de comportement des trains sont représentées de manière analogique par les variations de pente des lignes. Ce graphe permet d'obtenir les informations suivantes :

- **Vitesse :** plus la vitesse d'un train est élevée, plus la pente est élevée. Lorsque la pente est nulle (ligne horizontale), cela signifie que le train est arrêté (vitesse nulle). Les ralentissements et les accélérations sont codés par des courbes, les vitesses constantes par des droites ;
- **Identification des trains :** chaque train est identifié par un numéro (la parité est utilisée pour indiquer le sens de circulation des trains) ;
- **Position des trains :** la position des trains est fournie sur l'axe des ordonnées ;
- **heure de passage :** l'heure de passage d'un train est fournie sur l'axe des abscisses ;
- **Sens de circulation :** le sens de circulation est indiqué par le sens de la pente ;
- **Croisement de deux trains sur voies séparées :** le croisement de deux trains est indiqué par le fait que deux lignes ayant un sens de pente différent se croisent dans le cas de circulation des deux trains sur des voies différentes ;
- **Conflits potentiels entre deux trains :**
  - **Prise en écharpe :** la prise en écharpe d'un train par un autre est indiquée par le croisement de deux lignes en un point d'espace particulier correspondant à l'emplacement d'un aiguillage de changement de voie. Le conflit est réel dès lors qu'au moins un train emprunte la voie déviée ;
  - **Nez à nez (collision frontale entre deux trains :** le nez à nez se caractérise sur le graphe espace-temps par le croisement de deux lignes dans le cas d'une circulation sur une voie unique ;
  - **Rattrapage (collision par l'arrière) :** le rattrapage d'un train par un autre est indiqué par le fait que deux lignes ayant le même sens de pente se rejoignent ;

Le graphe espace-temps élaboré pour l'expérience est présenté à la figure 7.13, il représente le mode nominal.

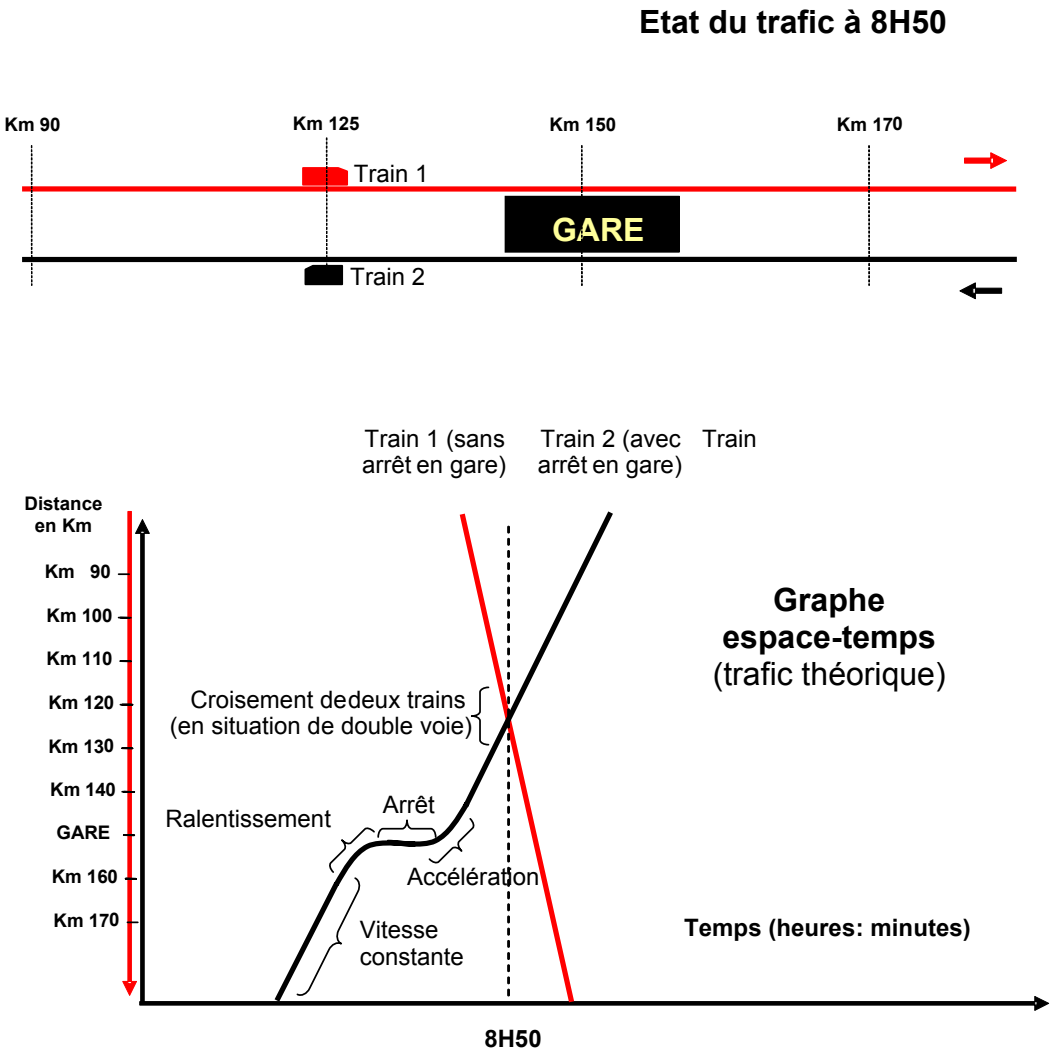


FIGURE 7.12. Lecture d'un graphe espace-temps

La situation nominale est formée d'un trafic théorique comportant 9 trains circulant sur une période de 30 minutes. Pour conserver un degré de validité écologique (c.à-d. proche de la réalité) suffisant, le graphe espace-temps a été élaboré en tenant compte des contraintes suivantes :

- Nécessité que les trains aient des missions différentes (trains avec arrêt en gare, sans arrêt, destinations différentes) ;
- Nécessité que les trains aient des vitesses différentes (trains lents = 54 km/h ; marches moyennes = 108 km/h et trains rapides = 162 km/h) ;
- Intervalle minimal de temps entre deux trains de 3 minutes (correspondant approximativement aux contraintes de cantonnement).

La figure 7.14 présente l'état du trafic tel qu'il apparaît sur l'interface SPICA-RAIL à la sixième minute de la simulation lorsque le trafic est conforme au trafic théorique (c.-à-d. le mode nominal).

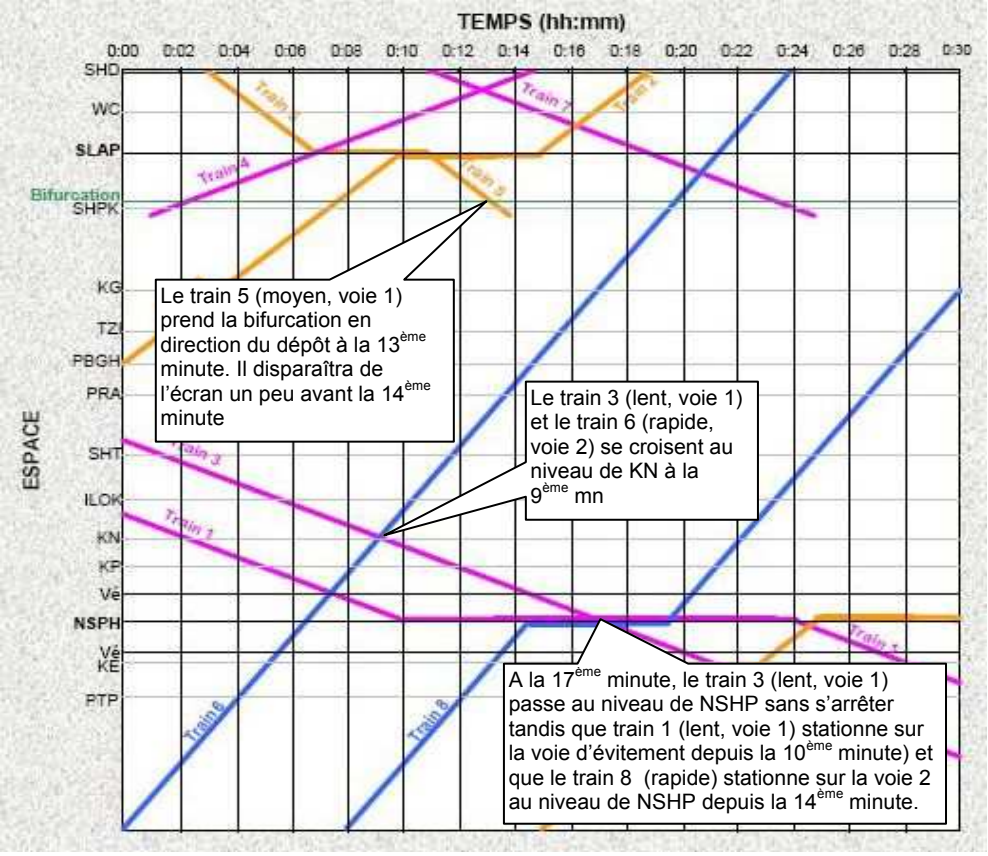


FIGURE 7.13. Graphe espace-temps utilisé dans l'expérience

7.3.5. Création des scénarios comportant des anomalies (modes dégradés). — Afin de tester les hypothèses sur le comportement psychologique des sujets, il a été nécessaire de concevoir et d'implémenter vingt scénarios tests. Chacun de ces scénarios est conçu sur le modèle représenté dans la figure 7.15.

Le temps $t_{\text{début}}$, correspond à la prise de poste de l'opérateur et le début du scénario. Chaque scénario commence par une situation normale de trafic nominal (*i.e.* conforme au trafic présenté dans le graphe espace-temps) d'une durée variable. Toute détection d'une anomalie par le sujet durant cette période est classée en « fausse alarme ». L'expérimentateur injecte un incident à une date différente pour chaque scénario. La date à partir de laquelle l'anomalie apparaît sur le TCO est notée t_0. À partir de cet instant t_0, le sujet dispose de 5 mn pour détecter l'incident et l'identifier. Durant cette période trois types de comportements de l'opérateur sont possibles :

- Détection correcte de l'incident ;
- Détection d'un incident qui n'existe pas — « Fausse alarme » ;
- Non-détection de l'incident, la passation du sujet est automatiquement interrompue par l'expérimentateur au-delà $t_0 + 5mn$ et le délai déclaré « dépassé » (manqué).

Les scénarios ont été élaborés par combinaison de plusieurs variables indépendantes. La notation utilisée affecte une lettre majuscule à la variable indépendante et on indique en indice et

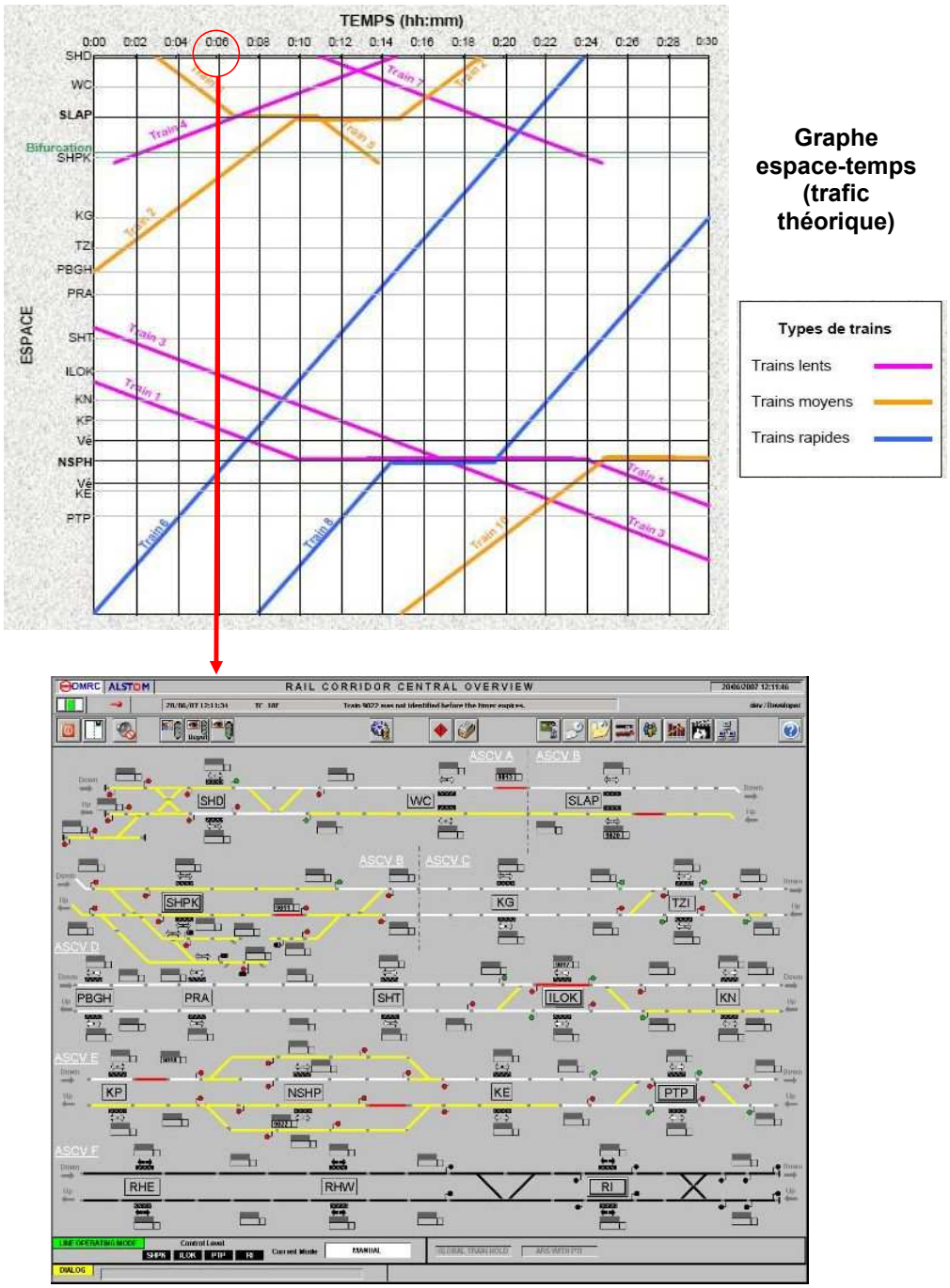


FIGURE 7.14. Graphe espace-temps et vue des installations et du trafic (6 trains) en mode nominal sur le TCO à t = 6 min.

entre accolades, le nombre de modalités de cette variable. Les quatre variables et leurs modalités sont les suivantes :

– $A_{\{2\}}$: le type d'incident { Aiguille en dérangement ; Signal en dérangement } ;

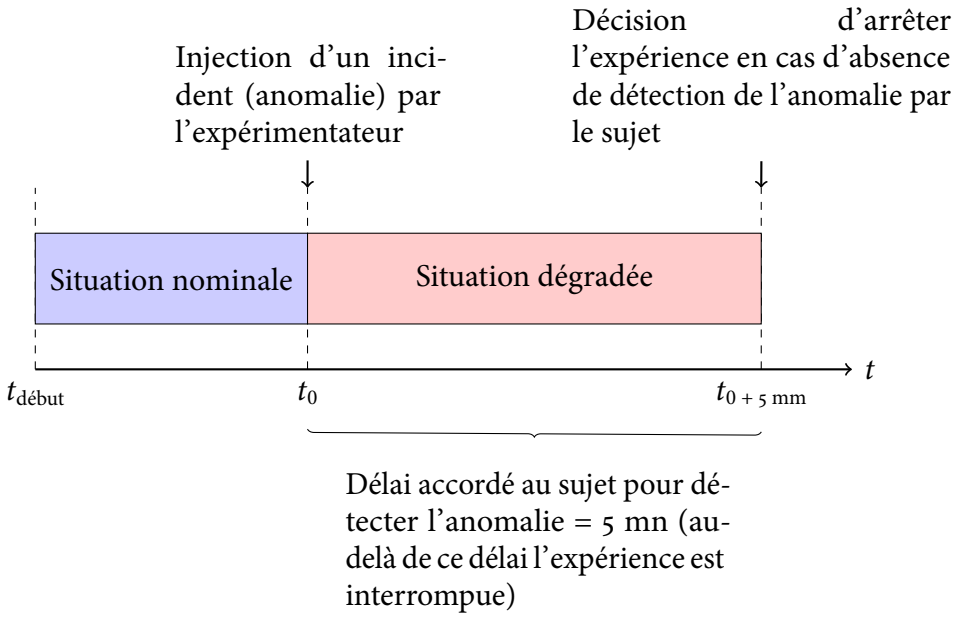


FIGURE 7.15. Structure des scénarios tests.

– $B_{\{2\}}$: le moment de l'incident { Début ; Fin } ;
– $C_{\{3\}}$: le contexte mobile { Sans train à proximité ; Train à proximité sans arrêt ; Train à proximité avec arrêt dû à l'incident } ;
– $D_{\{2\}}$: le contexte statique { Les deux voies en itinéraire permanent ; Au moins une des deux voies en destruction automatique }.

Le croisement de ces quatre variables mutuellement indépendantes forment le plan d'expérience à mesures complètement répétées symbolisé dans l'équation 6 conformément à la notation utilisée en psychologie expérimentale [**118**]. L'opérateur × signifie le croisement total des modalités sur un seul groupe de sujet représenté par $\underline{S}_{\{3\}}$.

$$\underline{S}_{\{3\}} \times A_{\{2\}} \times B_{\{2\}} \times C_{\{3\}} \times D_{\{2\}} \tag{6}$$

Cependant, le simulateur de trafic ne permet pas d'obtenir l'une des mesures : Dérangement d'un signal × Sans train à proximité. En conséquence, quatre des vingt-quatre scénarios initialement prévus n'ont pu être implémentés.

Les conditions expérimentales qui ont pu être simulées sont présentées sur le tableau 7.1.

Tous les scénarios tests font intervenir six trains dans la zone de supervision au moment de l'expérience.

En plus des scénarios tests, dix scénarios distracteurs ont été créés de manière à empêcher les sujets de développer des attentes à propos des variables étudiées et des hypothèses testées. Les scénarios distracteurs sont formés à partir d'une combinaison des variables A, C et D. Ces scénarios se distinguent des scénarios tests par le fait que les incidents étaient injectés à des moments différents de ceux des scénarios tests. Ainsi, la quasi-totalité des incidents survenant

Origine de l'anomalie	Train	DÉBUT	FIN
Dérangement d'AIGUILLE	SANS TRAIN	**Scénario 1 :** (voie 1 = P ; voie 2 = P ; 2RO)	**Scénario 11** (idem scenario 1)
		Scénario 2 : (voie 1 = P ; voie 2 = DA 1 RO)	**Scénario 12** (idem n°2)
	TRAIN SANS ARRET	**Scénario 3 :** (voie 1 = P ; voie 2 = P ; 2RO) le dérangement intervient juste après passage du train)	**Scénario 13** (idem n° 3)
		Scénario 4 : (voie 1 = P ; voie 2 = DA 1RO) le dérangement intervient juste après passage du train)	**Scénario 14** (idem n° 4)
	TRAIN AVEC ARRET	**Scénario 5 :** (voie 1 = P ; voie 2 = P ; 2RO) le dérangement intervient juste avant le passage du train ce qui provoque son arrêt	**Scénario 15** (idem n° 5)
		Scénario 6 : (voie 1 = P ; voie 2 = DA 1RO) le dérangement intervient juste avant le passage du train ce qui provoque son arrêt	**Scénario 16** (idem n° 6)
Dérangement de SIGNAL	SANS TRAIN	Impossible (non simulable)	Impossible (non simulable)
	TRAIN SANS ARRET	**Scénario 7 :** (voie 1 = P ; voie 2 = P ; 1RO) le dérangement intervient juste après passage du train ce qui provoque un RO sur la voie du train mais pas son arrêt	**Scénario 17** (idem n° 7)
		Scénario 8 : (voie 1 = P ; voie 2 = DA ; 1RF) le dérangement du signal sur la voie 2 intervient juste après passage du train le signal reste au vert)	**Scénario 18** (idem n° 8)
	TRAIN AVEC ARRET	**Scénario 9 :** (voie sur laquelle le train circule = DA ; 1RO) le dérangement intervient juste avant le passage du train ce qui provoque son arrêt et le signal ne s'ouvre pas	**Scénario 19** (idem n° 9)
		Scénario 10 (voie sur laquelle le train circule = DA ; 1RO) le dérangement intervient juste avant le passage du train ce qui provoque son arrêt et le signal ne s'ouvre pas	**Scénario 20** (idem n° 10)

Note : P = itinéraire permanent ; DA = itinéraire en destruction automatique ; voie 1 = voie impaire (de SHD vers PTP) ; voie 2 = voie paire (de PTP vers SHD) ; RO = raté d'ouverture d'un signal ; RF = raté de fermeture d'un signal

TABLE 7.1. Répartition des 20 scénarios tests dans les conditions expérimentales

dans les scénarios distracteurs intervient entre la neuvième et la quatorzième minute et sur des équipements (signaux et aiguilles) différents.

Les détails des scénarios tests sont présentés sur le tableau 7.2. Le sigle RO signifie « raté d'ouverture » d'un signal. Le sigle RF signifie « raté de fermeture » d'un signal. Les installations présentant une anomalie sont identifiées par leurs identifiants sur la plateforme SPICA-RAIL. Le type d'anomalie est codé de la façon suivante :

– Aig-xRO : indique une anomalie sur une aiguille impliquant x raté(s) d'ouverture sur le ou les signaux protégeant l'aiguille incriminée ;

– 1RO ou 1RF : indique le type d'anomalie (RO = raté d'ouverture et RF = raté de fermeture) sur un signal.

		DEBUT				FIN			
Nature de l'anomalie	Train	N° du scénario	Installation présentant l'anomalie	Type	Heure d'occurrenc	N° du scénario	Anomalie sur	Type	Heure
Dérangement d'aiguille	SANS TRAIN	1	P01C	Aig-2RO	06:00	11	P01D	Aig-2RO	14:30
		2	P04B	Aig-1RO	09:00	12	P03B	Aig-1RO	14:20
	TRAIN SANS ARRET	3	P01D	Aig-2RO	05:02	13	P04C	Aig-2RO	15:49
		4	P04B	Aig-1RO	05:31	14	P04B	Aig-1RO	18:07
	TRAIN AVEC ARRET	5	P01D	Aig-2RO	04:52	15	P02C	Aig-2RO	15:36
		6	P04B	Aig-1RO	04:50	16	P04B	Aig-1RO	17:30
Dérangement de signal	SANS TRAIN								
	TRAIN SANS ARRET	7	S03D	1RO	06:15	17	S04C	1RO	15:48
		8	S04B	1RF	07:38	18	S02B	1RF	17:45
	TRAIN AVEC ARRET	9	S02B	1RO	04:50	19	S02B	1RO	17:30
		10	S04B	1RO	07:20	20	S01B	1RO	22:44

TABLE 7.2. Détail des 20 scénarios tests en fonction des variables indépendantes A, B et C

De la même façon, les détails des dix scénarios distracteurs sont présentés sur le tableau 7.3

		DISTRACTEURS			
		Scénario	Installation	Type	Heure
Dérangement d'AIGUILLE	SANS TRAIN	21	P02E	Aig-2RO	09:00
		22	P10A	Aig-1RO	20:00
	TRAIN SANS ARRET	23	P10A	Aig-2RO	13:35
		24	P03E	Aig-2RO	12:44
	TRAIN AVEC ARRET	25	P51E	Aig-2RO	13:00
		26	P54E	Aig-1RO	13:15
Dérangement de SIGNAL	SANS TRAIN				
	TRAIN SANS ARRET	27	S04E	1RO	12:44
		28	S01B	1RF	13:12
	TRAIN AVEC ARRET	29	S62E	1RO	13:15
		30	S51E	1RO	13:10

TABLE 7.3. Détail des 10 scénarios distracteurs

7.4. Variables et hypothèses

L'expérimentation a pour objet d'étude l'effet de l'interface SPICA-RAIL sur la vitesse de détection des incidents. En conséquence, la variable dépendante qui a été étudiée est le temps de détection des anomalies contenues dans les scénarios.

Les quatre variables indépendantes qui ont été retenues sont le type d'incident ($A_{\{2\}}$), le moment de l'incident ($B_{\{2\}}$), le contexte mobile ($C_{\{3\}}$) et le contexte statique ($D_{\{2\}}$).

7.4.1. Le type d'incident $A_{\{2\}}$. — L'une des tâches importantes que remplit un opérateur ATS consiste à s'assurer que les aiguilles et les signaux ne sont pas en dérangement. Pour cette raison, la variable $A_{\{2\}}$ « type d'incident » à deux modalités « dérangement d'aiguille » notée A_1 ou « dérangement de signal » notée A_2 a été retenue.

7.4.1.1. Dérangement de signal : A_2. — Un dérangement de signal se manifeste soit par le raté d'ouverture d'un signal soit par un raté de fermeture du signal, voir les définitions suivantes :

***Définition 7.1* (Raté d'ouverture).** — Non-ouverture d'un signal, initialement fermé, suite à une commande d'ouverture. Cet événement n'est pas contraire à la sécurité puisque le signal reste dans une position de sécurité élevée interdisant le mouvement de train à franchir ce signal. Cet événement est contraire à la disponibilité, pouvant causer des retards importants sur le mode normal d'exploitation, il s'agit d'une mise en tension. Voir figure 7.16.

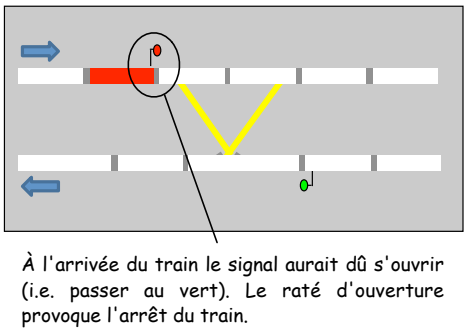


FIGURE 7.16. Raté d'ouverture

***Définition 7.2* (Raté de fermeture).** — Non-fermeture d'un signal, initialement ouvert, suite à la commande de fermeture. Cet événement est contraire à la sécurité, car autorise le mouvement de train à franchir ce signal sur une voie non libre et potentiellement occupée. Il s'agit d'un passage dans le mode dégradé d'exploitation. Voir figure 7.17.

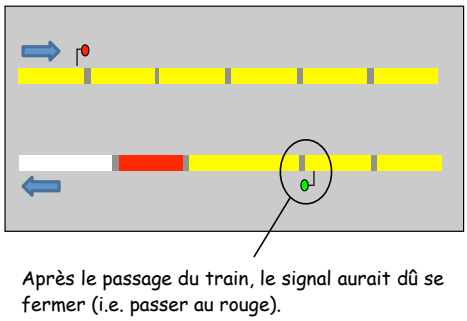
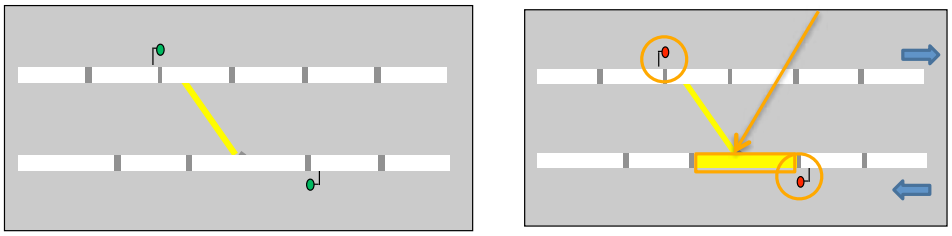


FIGURE 7.17. Raté de fermeture

7.4.1.2. Dérangement d'aiguille : A_1. — Un dérangement d'aiguille se traduit toujours par le raté d'ouverture d'un ou de plusieurs signaux (selon la configuration de la zone où se produit l'incident). Un zoom sur la zone où se produit le dérangement permet d'identifier l'aiguille en dérangement par le fait qu'une alarme le signale en faisant clignoter le symbole de l'aiguille. Un exemple de dérangement d'aiguille est fourni dans la figure 7.18.

D'autres anomalies permettent de déterminer que l'incident est dû à un dérangement d'aiguille et non à un dérangement de signal, voir tableau 7.4



Situation normale : les signaux sont ouverts, les itinéraires sont tracés.

Situation dégradée : les signaux se ferment, l'itinéraire aval de l'aiguille en dérangement se ferme.

FIGURE 7.18. Dérangement d'aiguille

Anomalie(s)	Dérangement d'aiguille	Dérangement de signal (RO ou RF)
Raté d'ouverture du signal	oui	oui (si RO) non (si RF)
Raté de fermeture du signal	non	**oui** (si RF) non (si RO)
Anomalie sur les deux voies	**oui**	non
Arrêt des trains	oui	oui (si RO) non (si RF)
Destruction de l'itinéraire	**oui**	non
Clignotement (alarme)	**oui** (zoom)	non

TABLE 7.4. Tableau récapitulatif des anomalies en cas de dérangement d'aiguille ou de signal.

***Hypothèse 7.3* (Le type d'incident** $(A_{\{2\}})$**).** — *Comme les dérangements d'aiguilles se manifestent généralement par davantage d'indices que les dérangements de signal, nous faisons l'hypothèse que les temps de détection devraient être moins élevés pour les scénarios impliquant un dérangement d'aiguille que pour ceux impliquant un dérangement de signal. En notant* t_{A_1} *le temps de détection d'un dérangement d'aiguille et* t_{A_2} *le temps de détection d'un dérangement de signal, l'hypothèse sur la variable indépendante A est formulée dans l'équation 7.*

$$t_{A_1} < t_{A_2} \tag{7}$$

7.4.2. Le moment de l'incident $B_{\{2\}}$**.** — Dans une situation réelle, un opérateur ATS assure un service sur une durée très longue (environ 6 heures). Pendant cette période, selon les événements qui surviennent ou non, le niveau de vigilance de l'agent peut osciller entre un état d'hypovigilance ou d'hypervigilance. Dans notre expérience la durée maximale d'un scénario est

fixée à 30 minutes. Toutefois, on peut s'attendre à ce que le moment d'apparition d'un accident ait un effet sur la vitesse de détection des anomalies.

Pour tester cette hypothèse nous avons manipulé la variable $B_{\{2\}}$ « moment d'apparition de l'anomalie » à deux modalités : « début de scénario » notée B_1 et « fin de scénario » notée B_2. Dans la moitié des scénarios tests l'incident intervient en début de scénario c.-à-d. entre 4' :50'' et 9' :00'' après le début du scénario ($t_{\text{début}}$). Dans l'autre moitié des scénarios tests l'incident se produit à la fin, c.-à-d. entre 14' :20'' et 22' :44'' après $t_{\text{début}}$.

Hypothèse 7.4 **(Le moment de l'incident** $B_{\{2\}}$**).** — *Si cette hypothèse est correcte, on peut s'attendre à ce que les anomalies soient plus rapidement détectées lorsqu'elles interviennent en début de scénario plutôt qu'à la fin. L'hypothèse est formalisée dans l'équation 8.*

$$t_{B_1} < t_{B_2} \tag{8}$$

7.4.3. Le contexte mobile $C_{\{3\}}$ **(proximité de trains).** — Les scénarios ont été établis de façon à ce que 6 trains soient présents sur le TCO au moment de la survenu des incidents. Ces trains constituent des éléments mobiles qui peuvent se situer à distance ou à proximité des anomalies à détecter. Dans certains cas l'incident peut même modifier le comportement d'un train (ex : un raté d'ouverture de signal ou un dérangement d'aiguille) en l'arrêtant à un moment où il n'est pas prévu qu'il le fasse. En outre, on peut penser que des sujets novices auront tendance à focaliser leur attention sur les installations à proximité des trains en mouvement.

Nous avons donc émis l'hypothèse que les temps de détection des anomalies devraient dépendre de la présence / absence d'un train en mouvement à proximité et de leur effet sur ce train. Pour tester cette hypothèse nous avons créé trois types de scénarios tests qui correspondent aux trois modalités de la variable $C_{\{3\}}$:

- C_1 : sans trains, dans ces scénarios aucun train ne se trouve à proximité de la zone de l'incident ;
- C_2 : présence d'un train sans arrêt, un train quitte la zone où survient l'incident mais son comportement reste conforme au planning nominal ;
- C_3 : présence d'un train avec arrêt, un train arrive sur la zone où survient l'incident ; ce dernier provoque l'arrêt de train.

Hypothèse 7.5 **(Le contexte mobile** $C_{\{3\}}$**).** — *Compte tenu de ces conditions, nous faisons l'hypothèse que le temps de détection des anomalies devrait être moins élevé dans les scénarios où les anomalies surviennent lorsqu'un train se situe à proximité que lorsque les anomalies surviennent dans une zone dans laquelle ne se trouve aucun train. De plus, le temps de détection devrait être moins élevé lorsque l'incident provoque l'arrêt de train que dans le cas où il n'affecte par le comportement de ce dernier. En ce qui concerne cette dernière partie de l'hypothèse, nous considérons que l'arrêt du train constitue une anomalie supplémentaire indiquant la présence d'un incident. L'hypothèse est formalisée dans l'équation 9.*

$$t_{C_3} < t_{C_2} < t_{C_1} \tag{9}$$

7.4.4. Le contexte statique $D_{\{2\}}$ (types d'itinéraires). — Enfin, nous avons décidé de prendre en compte une dernière variable que nous avons désignée par « contexte statique ». En effet, l'exploitation de la ligne ferroviaire simplifiée utilise deux types d'itinéraires :

– les itinéraires permanents (successions de circuit de voie en blanc sur le TCO) qui, comme leur nom l'indique, existent avant l'arrivée d'un train et se reforment automatiquement après le passage d'un train. Ce type d'itinéraire est utilisé sur des zones où les circulations empruntent toujours le même itinéraire (la pleine voie) ;
– les itinéraires en destruction automatique qui se forment au moment où un train arrive et se détruisent au fur et à mesure du passage du train sur l'itinéraire. Ce type d'itinéraire est utilisé sur des zones où les circulations peuvent aller vers plusieurs destinations, c'est le cas notamment au niveau de la bifurcation, les itinéraires en destruction automatique sont tracés par le système de tracé automatique des itinéraires.

Selon qu'un incident survient dans une zone où les deux voies sont en itinéraires permanents ou bien dans une zone où une voie au moins (ou les deux) sont en destruction automatique, les anomalies visibles sur le TCO sont différentes. D'une manière générale, le nombre d'anomalies visibles est plus élevé dans le premier cas que dans le second (principalement lorsqu'il s'agit d'une aiguille en dérangement). Nous avons manipulé cette variable en faisant en sorte que pour la moitié des scénarios, les deux voies soient en itinéraire permanent dans la zone d'incident (modalité D_1) et que pour l'autre moitié des cas au moins une des deux voies soit en itinéraire en destruction automatique (modalité D_2).

***Hypothèse 7.6* (Le contexte statique $D_{\{2\}}$). —** *Les temps de détection devraient être moins élevés lorsque les deux voies sont en itinéraires permanents que lorsqu'au moins une voie est en destruction automatique. L'hypothèse est formalisée dans l'équation 10.*

$$t_{D_1} < t_{D_2} \tag{10}$$

7.4.5. Synthèse. — La synthèse du plan d'expérience et des hypothèses est présentée sur la figure 7.19

7.5. Population et formation

Trois sujets, tous étudiants avancés (niveau bac. +5 ans et bac. +8 ans) à l'Université de Technologie de Compiègne, ont participé volontairement à l'expérience. Les caractéristiques de ces sujets étaient les suivantes :

– Sujet 1 (L) : 22 ans, étudiant en dernière année du cycle ingénieur en informatique ;
– Sujet 2 (S) : 34 ans, docteur en informatique, post-doctorant ;
– Sujet 3 (JM) : 30 ans, docteur en informatique, post-doctorant.

Les 20 scénarios tests et les 10 scénarios distracteurs ont été présentés à chacun des sujets. Au préalable, ceux-ci avaient bénéficié d'une formation accélérée puis avaient subi une évaluation des connaissances acquises durant la formation.

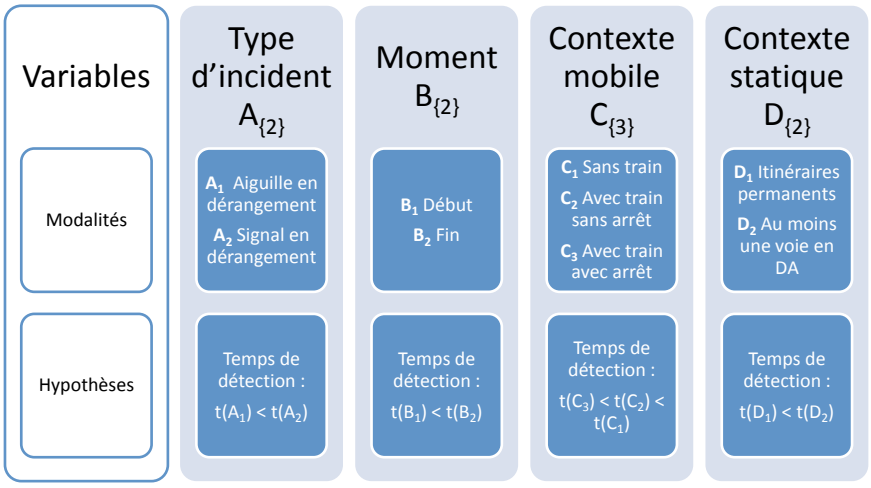


FIGURE 7.19. Plan d'expérience

Chaque sujet a reçu une formation initiale de 6 heures qui étaient distribuée en 3 séances de 2 heures. La première partie de la formation était consacrée à l'explication du rôle de l'agent ATS dans un poste et à la présentation de la situation nominale. La seconde partie portait exclusivement sur la présentation des situations dégradées.

7.5.1. Première partie - Séances 1 & 2 (4 h). — Les deux premières séances étaient consacrées à la présentation des points suivants :

– Rôle et missions de l'opérateur ATS, poste d'aiguillage et outils (TCO, *etc.*) à la disposition de l'opérateur ;
– présentation du réseau et du trafic simulé dans les expérimentations : structure de la ligne (voies, gares commerciales, sens de circulations, *etc.*, types de trains et trajets) ;
– Présentation du graphe espace-temps (trafic théorique) et présentation de la situation nominale sur une période de 30 minutes (fonctionnement des circuits de voie, aiguilles, signaux, progression des trains en mode nominal, *etc.*) ;
– Présentation des installations en mode d'exploitation normal ou en mode dégradé (dérangements d'aiguilles ou de signaux) ;
– Présentation des notions d'itinéraires (permanents et en destruction automatique) et système d'enclenchements.

7.5.2. Seconde partie - Séance 3 (2 h). — La dernière session de formation était entièrement consacrée à la présentation du mode dégradé d'exploitation. Les situations dégradées étaient présentées comme des situations présentant une anomalie de fonctionnement d'une aiguille ou d'un signal. Chaque cas à détecter était illustré à l'aide de vues statiques du TCO ou d'animations.

Le tableau 7.4 page 156 qui synthétise les anomalies relatives aux dérangements d'aiguilles et de signaux était fourni aux sujets. Ce tableau donne des éléments d'aide au diagnostic.

La formation se terminait par la lecture et l'explication de la consigne (voir Annexe A page 223)

7.5.3. Évaluation des connaissances. — À l'issue de la formation, chaque sujet devait répondre à un questionnaire à choix multiples afin de s'assurer qu'il avait bien compris la tâche et qu'il était capable de distinguer aisément les situations comportant une anomalie (c.-à-d. le mode dégradé) des situations présentant un fonctionnement normal (c.-à-d. le mode normal). Ce questionnaire comportait 48 questions à choix multiples conçues pour balayer tous les cas qu'ils seraient amenés à rencontrer ultérieurement pendant la phase de passation. Par exemple pour les cas correspondant aux zones où la voie 1 et la voie 2 sont en itinéraire permanent, un exemple de questions associées est présenté à la figure 7.20.

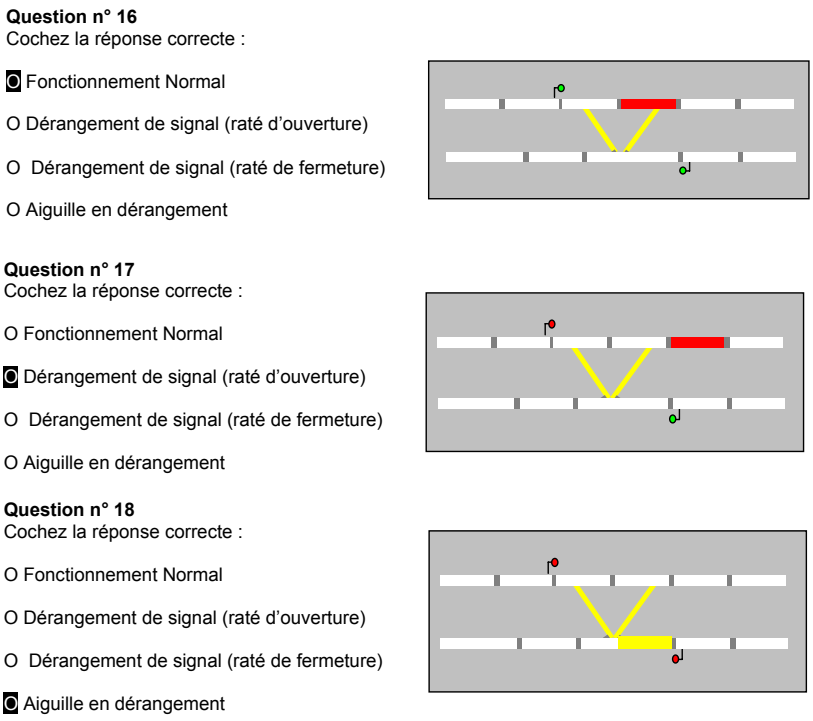


FIGURE 7.20. Exemple de questions

L'analyse des réponses à ce questionnaire a permis d'établir que les trois sujets avaient parfaitement intégré la formation puisque tous ont fourni plus de 99% de réponses correctes au questionnaire.

7.6. Les passations

Les passations se déroulaient dans la salle de l'UTC dédiée à la plateforme SPICA-RAIL, voir photo sur la figure 7.21. Chaque passation étaient individuelle et se déroulait en présence d'un ou de deux expérimentateurs, voir figure 7.22.

Les scénarios (tests et distracteurs) ont été répartis en 5 blocs de 6 scénarios de manière à permettre une passation en 5 séances de 2 heures environ pour chacun des sujets. Chaque bloc comprenait 2 scénarios distracteurs et 4 scénarios tests (voir le tableau 7.5). La répartition des

FIGURE 7.21. Plateforme Spica-Rail

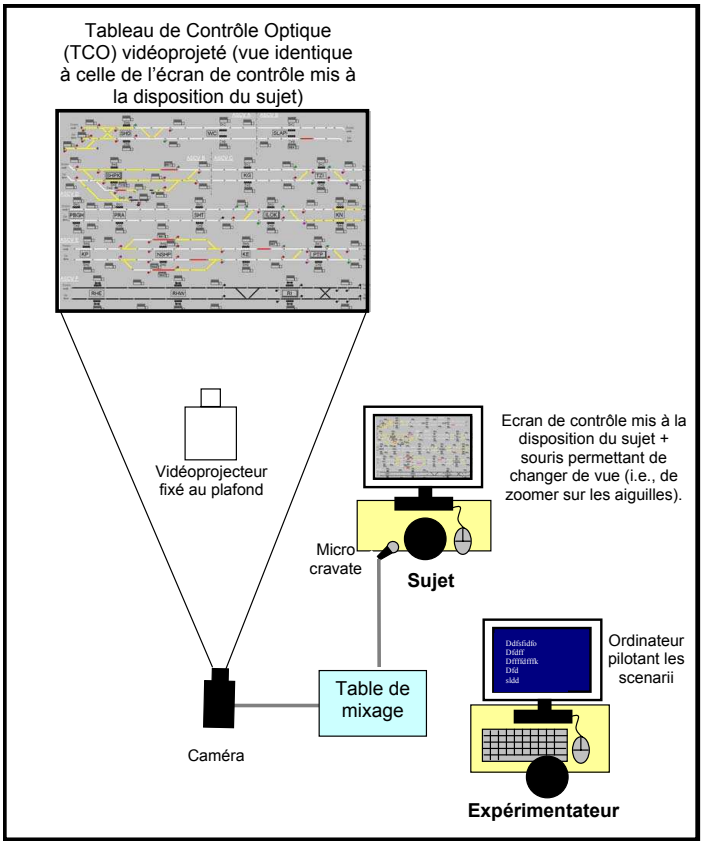


FIGURE 7.22. Dispositif utilisé pour les passations réalisées avec les sujets novices

scénarios tests et distracteurs dans les blocs a été faite de façon aléatoire. Le premier scénario d'un bloc était toujours un scénario distracteur tiré au sort parmi les deux scénarios distracteurs du bloc. L'ordre de présentation des 5 scénarios restant était quant à lui aléatoire. L'ordre de présentation des blocs a été réalisé de manière aléatoire pour les trois sujets (voir le tableau 7.6).

Au début de chaque session, l'expérimentateur lisait la consigne au sujet (voir annexe A). L'accent était mis sur le fait que le sujet devait fournir sa réponse de détection le plus rapidement

Rang	Bloc n°1	Bloc n°2	Bloc n°3	Bloc n°4	Bloc n°5
1	28	21	22	24	23
2	**11**	**18**	**4**	30	**7**
3	**19**	27	**2**	**12**	**15**
4	26	**17**	**9**	**10**	**3**
5	**6**	**8**	**13**	**14**	25
6	**5**	**20**	29	**1**	**16**
Rang	Durée des scénarii (mm:ss)	Durée des scénarii (mm:ss)	Durée des scénarii (mm:ss)	Durée des scénarii (mm:ss)	Durée des scénarii (mm:ss)
1	18:12	14:00	25:00	17:44	18:35
2	19:30	22:45	10:31	18:10	11:15
3	22:30	17:44	14:00	19:20	20:36
4	18:15	20:48	09:50	12:20	10:02
5	09:50	12:38	20:49	23:07	18:00
6	09:52	27:44	18:15	11:00	22:30
	Total : 01:38:09	**Total : 01:55:39**	**Total : 01:38:25**	**Total : 01:41:41**	**Total : 01:40:58**

TABLE 7.5. Tableau de répartition des scénarios tests et des scénarios distracteurs à l'intérieur des blocs

	Séance 1	Séance 2	Séance 3	Séance 4	Séance 5
Sujet 1 (L)	Bloc 3	Bloc 4	Bloc 1	Bloc 2	Bloc 5
Sujet 2 (S)	Bloc 4	Bloc 1	Bloc 5	Bloc 3	Bloc 2
Sujet 3 (J-M)	Bloc 5	Bloc 3	Bloc 1	Bloc 2	Bloc 4

TABLE 7.6. Tableau présentant l'ordre de passation des blocs pour les trois sujets

possible (en disant à voix haute « anomalie détectée ») et qu'il devait s'efforcer de dire à voix haute tout ce à quoi il pensait durant la réalisation de la tâche.

Ce dernier disposait durant toute la réalisation de la tâche du graphe espace-temps de manière à ce qu'il puisse suivre les mouvements des circulations. Pour chaque scénario la procédure suivante était répétée :

– l'expérimentateur lançait la simulation ;
– durant la situation nominale, en cas de fausse alarme, l'expérimentateur indiquait au sujet que sa détection était incorrecte et qu'il devait continuer ;
– l'expérimentateur déclenchait l'incident prévu dans le scénario puis relevait le moment où la première anomalie apparaissait sur le TCO. Ce moment correspond à t_0 ;
– Dès que le sujet détectait correctement l'une des anomalies provoquées par l'incident il devait dire « anomalie détectée » puis indiquer le type d'incident (aiguille ou signal en dérangement) ainsi que le numéro de l'équipement en zoomant sur la zone de l'incident ;
– En cas de non-détection de l'anomalie dans un délai de 5 minutes après t_0, l'expérimentateur interrompait le déroulement du scénario et indiquait « délai dépassé ».

Une fois la passation d'un scénario terminée, l'expérimentateur présentait le scénario suivant au sujet.

À l'issue de chaque séance de passation, l'expérimentateur procédait à un entretien avec le sujet de manière à identifier les stratégies utilisées par ce dernier pour réaliser la tâche.

7.7. Résultats

Les passations ont permis de recueillir environ 10 heures d'enregistrements vidéo par sujet, soit au total une trentaine d'heures pour les trois sujets.

Le dépouillement des données et les résultats des analyses portant sur les temps de détection recueillis pour les scénarios tests sont présentés ci-dessous.

7.7.1. Fausses alarmes et détections correctes. — Dans la quasi-totalité des cas, les anomalies ont été correctement détectées dans un délai de 5 minutes. Le taux d'anomalie non détectée sur l'ensemble des scénarios est très faible et identique pour tous les sujets :

- sujet 1 : 3,3% (1/30) ;
- sujet 2 : 3,3% (1/30) ;
- sujet 3 : 3,3% (1/30).

Le scénario non détecté est différent pour chaque sujet.

Parallèlement, on note très peu de fausses alarmes (c.-à-d. des détections d'anomalies qui n'en sont pas) :

- sujet 1 : 3,3% (1/30) ;
- sujet 2 : 3,3% (1/30) ;
- sujet 3 : 3,3% (1/30).

Ces résultats confirment d'une part que la formation initiale a parfaitement rempli son rôle et indiquent, d'autre part que les anomalies simulées dans la présente expérience sont parfaitement détectables en mode hors alarme par des sujets peu expérimentés.

7.7.2. Analyse des temps de détection. — L'analyse des temps de détection des anomalies a nécessité une numérisation préalable des enregistrements vidéos puis une analyse image par image à l'aide du logiciel Adobe™Premiere®Pro 1.5 pour Windows®. Le calcul du temps de détection par cette technique est illustré sur la figure 7.23.

Pour chaque scénario un temps de détection (en centième de seconde) a été calculé en appliquant la formule 11 :

$$\text{Temps de détection}(T_D) = t_d - t_0 \tag{11}$$

où

T_D **:** Temps de détection ;

t_0 **:** correspond au moment d'apparition de la première anomalie sur l'écran indiquant la survenue d'un incident (ex : changement de couleur d'un signal, d'un circuit de voie *etc.*) ;

t_d **:** correspond au moment ou le sujet commence à produire sa réponse en cas de détection correcte. Si le sujet prononce « anomalie détectée … », t_d correspond au début de la prononciation du « A » de « Anomalie ». Dans le cas où un élément objectif autre que « Anomalie » témoigne d'une détection correcte, t_d correspond à cet élément. Par exemple, si le sujet prononce « Ah ! là …anomalie détectée … », t_d correspond au début de prononciation du « A » de « Ah ».

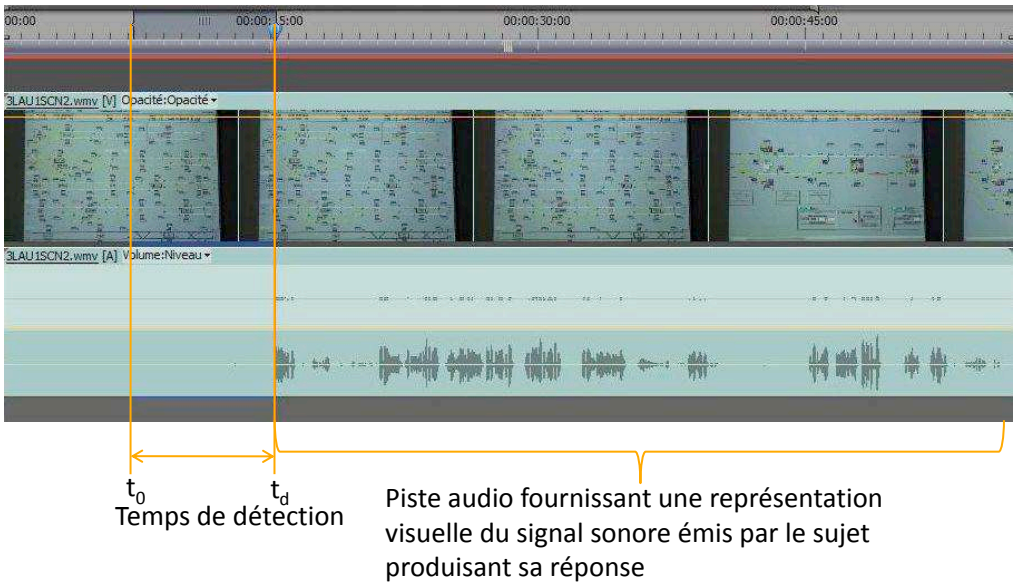


FIGURE 7.23. Le calcul des temps de détection réalisé à partir de la représentation visuelle des signaux sonores de la piste audio du logiciel Adobe™Premiere®Pro 1.5 pour Windows®

Deux cas de délais dépassés (c.-à-d. de non-détection de l'anomalie dans un délai de 5 min) ont été enregistrés en T_D = 300sec. de manière à ne pas réduire la taille des effectifs déjà très réduits pour la réalisation des comparaisons statistiques.

7.7.3. Analyse descriptive des temps de détection T_D. — En raison d'une forte variabilité intra et inter sujets et de l'existence de temps de détection extrêmes, les moyennes et variances ont peu de significativité. En conséquence, les analyses ont été réalisées sur les médianes et les étendues.

Les temps de détections sont présentés dans le tableau 7.7 et les distributions des temps de détection de chaque sujet et pour l'ensemble des sujets sont données dans l'histogramme de la figure 7.24.

Le T_D médian est de 11,96 pour une étendue de 299. L'analyse des temps de détection sur les scénarios tests révèle une forte variabilité entre les sujets. Les temps de détection médians et les étendues pour les 3 sujets sont indiqués dans le tableau 7.8.

Ces premières analyses permettent d'établir que les temps de détection sont relativement élevés si l'on considère que la présente expérience met les sujets dans les conditions les plus favorables pour détecter rapidement les anomalies :

– Les sujets sont informés que chaque scénario comporte une anomalie à détecter (ce qui n'est pas le cas dans un vrai poste ATS) ;
– Les incidents sont réduits à deux types d'incidents, aiguilles et signaux, dans un vrai poste ATS, la nature des incidents peut être beaucoup plus variée ;
– La durée des scénarios est très courte (30 min) comparée à un quart réel de 6 heures dans un poste ATS ;

Sujet 1	Sujet 2	Sujet 3
1,00	3,03	1,04
1,87	3,92	1,14
2,01	5,13	1,23
2,15	11,93	2,09
2,98	12,07	2,84
3,01	12,94	4,10
3,17	13,99	5,97
3,18	17,85	9,05
3,95	20,92	10,98
5,06	20,95	11,21
5,90	23,90	11,93
6,91	24,01	12,95
7,98	24,85	13,11
8,11	27,07	15,06
11,94	34,79	20,93
11,98	40,94	23,88
18,15	47,91	24,03
23,00	49,94	26,20
23,85	51,08	265,09
300,00*	163,93	300,00*

TABLE 7.7. Temps de détection en secondes classés par ordre croissant pour chacun des sujets - * Les valeurs de 300 sec. (5mn) correspondent aux scénarios pour lesquels l'anomalie n'a pas été détectée.

Sujet	T_D médian (sec.)	Étendue
1	5,48	299
2	22,42	160,9
3	11,57	298,96

TABLE 7.8. Temps de détection médians et étendues

– Les sujets n'ont que la tâche de détection à accomplir alors que dans un vrai poste ATS, les opérateurs sont amenés à accomplir plusieurs activités en parallèle ;
– Toute la ligne n'a pas été implémentée sur le TCO. De fait, la zone à superviser est relativement réduite ;

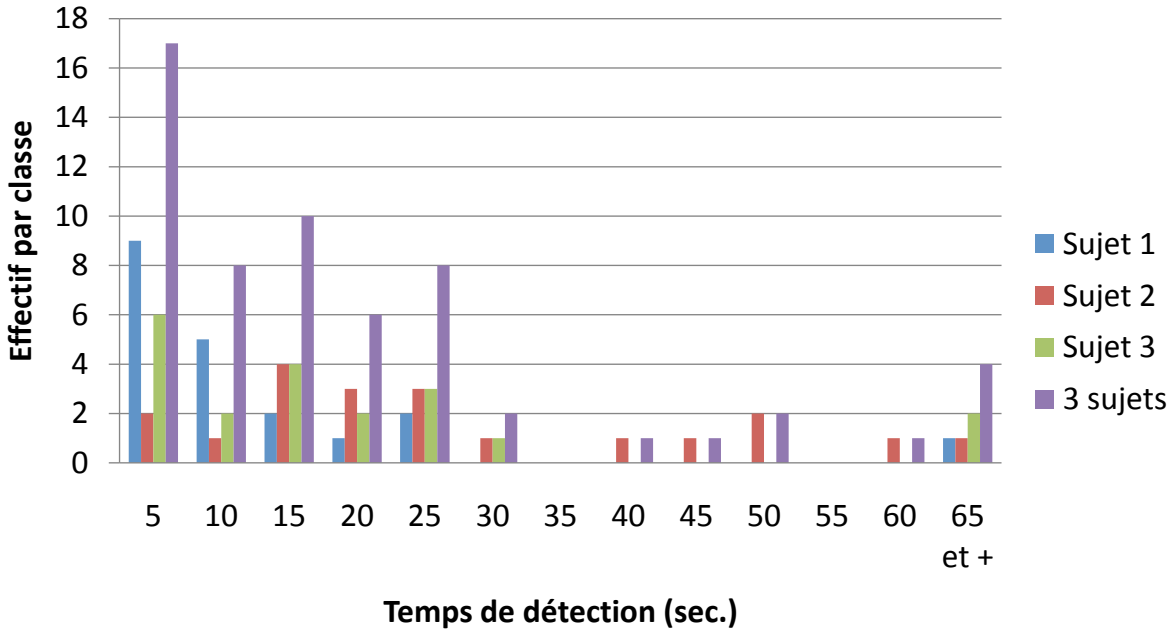


FIGURE 7.24. Distribution des temps de détection (en sec.) pour les 3 sujets

– Enfin, la ligne a été simplifiée, elle ne comporte que deux gares commerciales et une seule bifurcation.

Par ailleurs, on note que le sujet 2 est moins rapide que les autres sujets pour détecter les anomalies. En effet, alors que chez ce sujet 60% des temps de détection sont supérieurs à 20 secondes, ce taux n'est plus que de 20% chez les sujets 1 et 3. Ce résultat suggère que le temps de détection dépend des stratégies employées par les sujets pour explorer le TCO et que les anomalies ne sont pas suffisamment saillantes pour être perçues de la même manière par tous les sujets.

7.7.4. Statistiques non paramétriques. — Une analyse de normalité réalisée sur les données disponibles indique que les distributions ne satisfont pas aux conditions de normalité et d'homogénéité. En conséquence, la significativité statistique des effets pour toutes les comparaisons portant sur des mesures répétées sera testée à l'aide de tests non paramétriques pour échantillons appariés [**117, 118**]. Le seuil de significativité sera fixé *a priori* à 0.05 pour toutes les comparaisons.

7.7.5. Rappel sur les tests statistiques non paramétriques. — L'objectif de notre démarche consiste à comparer de façon non paramétrique deux échantillons. Ces types de tests sont construits à partir d'une statistique linéaire de rang de la forme :

$$S_N = \sum_{i=1}^{N} c_i a_N(R_i) \tag{12}$$

où N est le nombre total des observations $(Z_1, \ldots, Z_N)$, R_i est le rang des Z_i dans l'échantillon ordonné, les $a_N(i), 1 \leq i \leq N$, sont des scores construits en général à partir d'une fonction définie sur $]0,1[$, les c_i sont des constantes dites constantes de régression.

Dans notre étude, l'échantillon Z est formé de deux échantillons X et Y de même taille (n) que nous voulons comparer :

$$Z = (X_1, \ldots, X_n, Y_1, \ldots, Y_n) \tag{13}$$

Pour comparer les performances des sujets deux à deux, nous utiliserons le test de Mann et Witney [**118**] qui représente le nombre de fois où une observation de X est plus grande qu'une observation de Y. La statistique de Mann et Witney est la suivante :

$$U_N = \sum_{i=1}^{n} R_i - \frac{n(n+1)}{2} \tag{14}$$

U_N varie donc de 0 à n^2.

On obtient après transformation sur les rangs :

$$U_N = \sum_{i=1}^{n} \sum_{j=1}^{n} 1_{\mathbb{R}^+}(X_i - Y_j) \tag{15}$$

On teste alors l'hypothèse H_0 « X=Y » et on calcule la probabilité de rejeter à tort l'hypothèse H_0 notée p à partir de la valeur de U_N observée, de la taille des échantillons n, du seuil de significativité $\alpha = 0.05$ et de la valeur de la loi exacte de U_N lue dans une table. Si $p < \alpha$ on rejette H_0 et si $p > \alpha$ on accepte H_0.

Pour tester l'effet des variables, nous utiliserons le test de Wilcoxon [**118**] pour échantillons appariés qui consiste à sommer les rangs signés des différences entre paires d'observations de chaque échantillon. Ce test utilise une statistique linéaire de rang, dans ce test les rangs sont ceux des différences entre paires d'observations, la statistique est de la forme :

$$T_N = \sum_{i=1}^{n} R_i \tag{16}$$

Ce type de test est utile lorsque l'on veut établir si deux traitements sont différents ou si un traitement est « meilleur » qu'un autre. Dans tous les cas, le groupe qui a subi le traitement est comparé à celui qui n'en a pas subi, ou qui a subi un traitement différent. Ce cas se présente, par exemple, quand on compare deux méthodes de mesure en soumettant à ces deux méthodes les mêmes individus, choisis dans une population donnée. Ici nous avons soumis plusieurs scénarios avec la même modalité d'une variable à plusieurs sujets et un nombre identique de scénarios avec l'autre modalité. Nos hypothèses à tester consistent à vérifier si une modalité donne des temps de détection plus grands ou plus petits que l'autre modalité.

La procédure consiste à calculer la différence entre chaque n paire d'observations :

(17) $$d_i = X_i - Y_i, 1 \leq i \leq n$$

L'étape suivante consiste à ordonner les valeurs absolues des d_i. Les R_i correspondent aux rangs des $|d_i|$ ainsi ordonnés auxquels on rajoute le signe de d_i.

Si les traitements X et Y sont équivalents, donc si H_0 est vraie, la somme des rangs ayant un signe positif et celle des rangs ayant un signe négatif devraient être à peu près égales. Mais si la somme des rangs de signes positifs est très différente de celle des rangs de signes négatifs, nous en déduirons que le traitement X diffère du traitement B, et nous rejetterons l'hypothèse nulle. Donc, il y a rejet d'H_0 que si la somme des rangs de signe négatif ou que celle des rangs de signe positif est faible.

Il est possible que les deux scores d'une quelconque paire soient égaux. Il n'y a pas de différence observée entre les deux traitements pour cette paire ($d = 0$). De telles paires sont abandonnées. n est alors égal au nombre de paires dont la différence entre les traitements n'est pas nulle.

On somme alors les rangs de même signe, on obtient T^+ pour la somme des rangs positifs et T^- pour la somme des rangs négatifs, enfin la valeur de la statistique T de Wilcoxon pour échantillons appariés est donnée par la valeur de la somme des rangs du signe observée le moins fréquent. L'hypothèse H_0 « X=Y » est testée contre H_1 « $X \neq Y$ » (test unilatéral) ou bien « $X > Y$ », « $X < Y$ » (tests bilatéraux).

La loi de la statistique de Wilcoxon donne les valeurs critiques de T en fonction de N, du seuil de significativité et du type de l'hypothèse alternative pour les tests bilatéraux.

Si le T observé est égal ou inférieur à la valeur donnée dans la table pour un niveau de signification et pour le nombre de différences non nulles n, l'hypothèse nulle peut être rejetée à ce niveau de signification.

Tous les tests statistiques effectués pour l'expérience ont été traités par deux logiciels : Microsoft Excel et le logiciel de statistique R.

7.7.6. Comparaisons des données des trois sujets. — La comparaison des temps de détections des sujets a été effectuée par paires avec le test de Mann et Witney. Chaque sujet a effectué $n = 20$ scénarios tests. Les valeurs de p sont données dans le tableau 7.9.

Paire	p	H_0 « X=Y »
Sujet 1 - Sujet 2	0,00041	Rejeté
Sujet 1 - Sujet 3	0,21	Accepté
Sujet 2 - Sujet 3	0,03	Rejeté

TABLE 7.9. Comparaisons des données des trois sujets. Test de Mann et Witney, $\alpha = 0.05$

Ce résultat confirme le résultat des statistiques descriptives, les analyses indiquent que les temps de détections du sujet 2 diffèrent significativement de ceux du sujet 1 ($U = 74$ et $p < 0,05$) et de ceux du sujet 3 ($U = 120$ et $p < 0.05$).

7.7.7. Effet des variables. — Les résultats sont détaillés pour l'analyse de la variable $B_{\{2\}}$ « moment de l'incident » afin de présenter le raisonnement employé. Les analyses des autres variables sont données dans des tableaux synthétiques.

L'analyse de l'effet du moment de l'incident sur l'ensemble des sujets fournit les résultats suivants :

L'hypothèse était $t_{B_1} < t_{B_2}$, ce qui se traduit dans le test de Wilcoxon par le fait que la somme des rangs de signe positif (noté T^+) soit plus grande que la somme des rangs de signe négatif (noté T^-) lorsqu'on effectue la différence des observations de la modalité A_2 à celle de la modalité A_1 dans chaque paire. Or, les résultats donnent, pour $n = 30$ paires :

$$T = 224$$
$$T^+ = 241$$
$$T^- = 224$$

Le sens observé est donc conforme à celui attendu. Pour $N = 30$ la valeur critique de T est égale à 152, or le calcul de T donne 224, ce qui est supérieur au T critique, l'effet n'est pas significatif.

Le tableau 7.10 synthétise les résultats des analyses de la variable « moment de l'incident » pour chacun des sujets.

Sujet	n	Hypothèse $t_{B_1} < t_{B_2}$	Effet significatif ?
1	10	contraire à celle prédite	non
2	10	conforme	non
3	10	conforme	non

TABLE 7.10. Effet de la variable $B_{\{2\}}$ « moment de l'incident », résultats pour chaque sujet.

L'analyse de la variable $A_{\{2\}}$ est présentée dans le tableau 7.11, celle de la variable $C_{\{3\}}$ dans les tableaux 7.12, 7.13 et 7.14 et enfin l'analyse de la variable $D_{\{2\}}$ dans le tableau 7.15.

Sujet	n	Hypothèse $t_{A_1} < t_{A_2}$	Effet significatif ?
Tous	30	contraire à celle prédite	non
1	10	contraire à celle prédite	non
2	10	contraire à celle prédire	non
3	10	contraire à celle prédite	non

TABLE 7.11. Effet de la variable $A_{\{2\}}$ « Type d'incident »

Les résultats ne sont pas significatifs, il est donc impossible d'inférer des conclusions concernant l'effet des variables sur la base des tests statistiques non paramétriques. La taille des échantillons est sans doute responsable du manque de significativité de ces résultats. Pourtant, les tests non paramétriques de rang signé pour échantillons appariés tels que le test de Wilcoxon

Sujet	n	Hypothèse $t_{C_3} < t_{C_2}$	Effet significatif ?
Tous	24	conforme	non
1	8	conforme	non
2	8	conforme	non
3	8	contraire à celle prédite	non

TABLE 7.12. Effet de la variable $C_{\{3\}}$ « Contexte mobile », arrêt du train vs. non arrêt du train à proximité de l'incident

Sujet	n	Hypothèse $t_{C_2} < t_{C_1}$	Effet significatif ?
Tous	24	conforme	non

TABLE 7.13. Effet de la variable $C_{\{3\}}$ « Contexte mobile », arrêt du train vs. sans train à proximité de l'incident

Sujet	n	Hypothèse $t_{C_3} < t_{C_1}$	Effet significatif ?
Tous	24	contraire à celle prédite	oui ($p = 0,0461$)

TABLE 7.14. Effet de la variable $C_{\{3\}}$ « Contexte mobile », non arrêt du train vs. sans train à proximité de l'incident

Sujet	n	Hypothèse $t_{D_1} < t_{D_2}$	Effet significatif ?
Tous	30	conforme	non
1	10	conforme	non ($p = 0,0527$)
2	10	conforme	non
3	10	conforme	non

TABLE 7.15. Effet de la variable $D_{\{2\}}$ « Contexte statique »

sont tout à fait applicables à notre expérience. Le nombre de paires $n > 8$ pour chaque tests est suffisant, en effet, l'étude des rangs signés donne des résultats pour des valeurs de n petites [**117, 118**]. Pour $n > 30$ nous aurions pu utiliser l'approximation normale puisque la statistique de Wilcoxon converge vers la loi normale lorsque $n \to \infty$.

Seul l'effet de la variable « Contexte mobile » a fourni un résultat significatif, concernant l'hypothèse que le temps de détection est plus grand lorsque l'incident se produit dans une zone avec un train qui n'est pas arrêté par l'incident que lorsque l'incident se produit sur une zone sans train à proximité. Et ce, contrairement à ce qui avait été prédit. Ce résultat semble surprenant, en effet, il paraissait raisonnable de supposer que la stratégie du sujet pour balayer le TCO soit sensible à la présence d'une circulation et que celui-ci s'attache à poser son regard périodiquement sur les circuits de voies occupés. Or, l'analyse statistique montre que cette supposition n'est pas valable. La performance des sujets ne dépend vraisemblablement pas d'une telle stratégie.

L'ensemble des résultats statistiques indique qu'il serait souhaitable de prolonger l'analyse sur la stratégie de balayage du TCO par l'opérateur. Nous avons constaté des différences significatives d'un sujet par rapport aux deux autres. Cet écart pourrait donc provenir de la stratégie utilisée par les sujets pour balayer le TCO, toutefois il faudrait néanmoins vérifier que cette différence n'est pas liée à la variabilité normale inter-sujets, chose que nous n'avons pu analyser dans notre expérience, il aurait fallu un nombre plus important de sujets pour conclure sur la variabilité inter-sujets. De même, la contradiction avec l'hypothèse qui a été émise concernant le contexte mobile de l'incident est un indice supplémentaire pour continuer les recherches dans cette voie. S'il s'avérait possible d'identifier plusieurs stratégies de surveillance et de les classer par ordre de performance, il serait alors possible de proposer des spécifications pour l'amélioration des interfaces Hommes-Machines qui orienteraient l'opérateur dans sa tâche de surveillance.

7.8. Conclusion

La plateforme SPICA-RAIL a permis d'étudier les temps de détection d'incidents contraires ou non à la sécurité par des opérateurs novices. L'incident de type « raté de fermeture » d'un signal est contraire à la sécurité, replacé dans le modèle des modes d'exploitation du chapitre précédent, il constitue une transition accidentelle. L'incident « raté d'ouverture » d'un signal ainsi que le dérangement d'une aiguille sont des transitions vers un mode d'exploitation dégradé. La détection de ces transitions a été étudiée au travers de quatre variables explicatives qui avaient pour objectif de valider ou bien d'invalider des hypothèses sur les processus généraux impliqués dans cette tâche de détection.

Il ressort des expériences une certaine variabilité inter-sujets qui doit être confirmée par de nouvelles expériences. Les temps de détections sont relativement élevés compte tenu de l'environnement favorable dans lequel étaient placés les sujets. Ce résultat montre que l'IHM de supervision est faiblement efficace dans sa mission d'aide à la détection. La perception directe de l'apparition d'un incident sur les éléments graphiques symbolisant les équipements ferroviaires est une propriété importante que l'IHM doit proposer à l'opérateur humain. De notre point de vue, cette propriété assure une « continuité » de l'activité cognitive de l'opérateur. Dans cette perspective nous envisageons de préparer de nouvelles expériences qui porteront sur l'identification de cette « continuité » de l'activité par la mise en place d'un dispositif permettant de détecter la stratégie de surveillance de l'IHM par l'opérateur humain. Les travaux effectués par le LAMIH dans ce domaine utilisent un dispositif appelé « oculomètre » qui permet d'enregistrer les mouvements oculaires l'opérateur humain sur l'écran [**7, 6, 43, 44**].

Le chapitre suivant présente la troisième phase de notre démarche, il s'agit de proposer un processus de modélisation de l'activité de supervision de trafic ferroviaire dans une perspective interdisciplinaire alliant l'évaluation de la sécurité et l'étude spécifique du facteur humain.

CHAPITRE 8

ÉVALUATION INTERDISCIPLINAIRE DE LA SÉCURITÉ D'UN SYSTÈME SOCIOTECHNIQUE COMPLEXE

Résumé

Ce chapitre constitue la troisième phase de la démarche de la thèse. Nous proposons d'utiliser la méthode FRAM comme méthode de modélisation de l'activité. Après avoir présenté les motivations de ce choix, la première partie du chapitre présente les propriétés liées à l'interdisciplinarité de l'étude de l'impact des systèmes de supervision automatique sur la sécurité. La deuxième partie du chapitre est consacré à la description de la méthode FRAM et à son application dans le cadre de l'évaluation de la sécurité.

8.1. Motivations

La thèse traite des systèmes sociotechniques complexes composés d'un niveau technique (les machines, les logiciels), d'un niveau humain (les opérateurs, les concepteurs) et d'un niveau organisationnel (l'ensemble des règles et des interactions qui gouvernent le travail accompli par le système). Chacune de ces composantes correspond à une discipline scientifique.

Dans ce chapitre, nous proposons une démarche d'évaluation des risques industriels tenant compte de ces trois disciplines. L'idée consiste à appliquer une approche complémentaire à l'analyse de risque classique permettant d'approfondir les niveaux humain et organisationnel insuffisamment traités dans l'approche classique de la sûreté de fonctionnement.

Cette approche complémentaire doit disposer d'un référentiel commun aux trois disciplines impliquées dans les systèmes sociotechniques complexes. Dans une première partie, nous présenterons les différences entre les démarches de l'ingénierie et celle des sciences humaines et sociales. La méthode FRAM développée par Hollnagel [**68**] pour analyser les accidents utilise une approche dans laquelle les trois composantes (technique, humaine et organisationnelle) cohabitent et sont en interactions mutuelles. La méthode est présentée au paragraphe 8.4 et nous introduisons une démarche guidée pour le développement de cette méthode dans le cadre d'une analyse de risque interdisciplinaire (paragraphe 8.5). Utilisée en complément de l'approche de sûreté de fonctionnement classique, la méthode FRAM permet de « zoomer » sur les événements humains et organisationnels afin d'affiner le résultat qualitatif de l'étude. L'aspect interdisciplinaire de notre approche a été présenté dans [**19**].

8.2. Des démarches scientifiques différentes

La composante technique des systèmes sociotechniques est régie par des modèles et des théories issus des sciences exactes. L'analyse de la composante humaine au travail est l'objet d'étude de la psychologie cognitive [**26, 9**] et de la psychologie ergonomique cognitive [**39, 65, 128**]. Enfin, la composante organisationnelle repose sur les sciences sociales. Ces trois disciplines n'ont pas les mêmes fondements. Les démarches, les techniques de représentation et de modélisation utilisées sont différentes et quelquefois opposées.

Le statut de la modélisation est différent pour chaque discipline scientifique. Les sciences dites « exactes » (mathématiques, physiques notamment) donnent une position dominante aux modèles mathématiques structurés entièrement formalisés. Les sciences de l'ingénieur privilégient ce type de modèle, mais n'excluent pas les modèles semi-formalisés associant une structure formelle à un langage graphique. Ces deux types de modélisation sont validés en priorité par la logique et l'expérimentation.

Les sciences du vivant ainsi que les sciences sociales n'ont généralement pas la possibilité de valider de tels modèles par l'expérimentation. L'observation permettrait de contourner cette difficulté si ce n'est que l'observateur introduit un biais dans le système. Le psychologue ou le sociologue doit alors recourir à la modélisation à partir des informations qu'il a pu recueillir sur le terrain ou dans la littérature.

8.2.1. L'approche de l'ingénierie. — Le management des risques industriels s'appuie sur les techniques de sûreté de fonctionnement, reprenant le formalisme mathématique de la fiabilité et de la maintenabilité développé par Barlow et Proschan [**12**]. Ce formalisme contient un modèle de fonctionnement des composantes du système bimodal dans lequel le composant n'a que deux états possibles : le bon fonctionnement ou bien la panne. Le système est alors caractérisé par le vecteur d'état de tous ses composants. La démarche consiste a déterminer l'état du système en fonction de ce vecteur caractéristique. L'analyste utilise un raisonnement rigoureux construit par une logique déductive ou inductive pour arriver à cette fin. La méthode de travail repose sur une logique d'exploration systématique des événements ou des composants potentiellement dangereux.

Les méthodes développées par les ingénieurs de sûreté de fonctionnement apportent les outils nécessaires au raisonnement permettant d'expliquer l'apparition des défaillances à différents niveaux du système jusqu'à l'apparition des accidents. (Voir le chapitre 3 page 59).

8.2.2. L'approche des sciences humaines et sociales. — Le cadre théorique et la méthodologie utilisés pour l'évaluation des facteurs humains sont ceux de la psychologie cognitive et de la psychologie ergonomique cognitive. L'apport de la psychologie cognitive se situe essentiellement sur le plan théorique en fournissant des outils conceptuels permettant de comprendre le fonctionnement cognitif d'un opérateur effectuant un travail. Le point de vue de cette discipline conçoit l'opérateur comme un système cognitif, c'est-à-dire comme un système de traitement de l'information à capacité limitée capable d'acquérir, de stocker, d'utiliser des connaissances déclaratives et procédurales dans un environnement de travail.

L'apport de la psychologie ergonomique cognitive est à la fois conceptuel et méthodologique. Sur le plan conceptuel deux champs d'étude qui ont été abondamment abordés par cette discipline sont pertinents dans le cadre du management des risques des grands systèmes industriels complexes [**64, 9, 65, 107, 128**] : la supervision et le contrôle de processus de situations dynamiques d'une part, et la coopération opérateur humain – machine d'autre part. Ces études ont débouché sur l'élaboration de concepts et de modèles permettant d'améliorer les conditions de travail des opérateurs et ainsi de garantir indirectement plus de sécurité.

Contrairement à l'ingénierie de sûreté de fonctionnement, la psychologie cognitive et la psychologie ergonomique cognitive s'appuient largement sur le raisonnement empirique (basé sur des expériences) et sont parfois amenées à utiliser un raisonnement flou et discriminant basé sur une logique d'abduction notamment pour supprimer les solutions improbables (l'abduction s'oppose à une logique d'exploration systématique très largement utilisée en sûreté de fonctionnement).

La psychologie cognitive est l'étude empirique des processus de traitement de l'information qui interviennent dans les conduites humaines (et animales). Basées sur l'observation d'événements sur le terrain ou dans un environnement simulé, les méthodes de la psychologie cognitive visent à établir, par des techniques statistiques, des hypothèses qui permettent de prédire des événements dans des situations analogues. Les méthodes statistiques utilisées sont aussi bien descriptives qu'inférentielles. Citons, parmi les plus utilisées, l'analyse de la variance, les tests statistiques paramétriques et non paramétriques, l'analyse factorielle, *etc.* Les modèles utilisés sont des modèles de dépendance entre variables expérimentales.

Les résultats de l'étude de psychologie cognitive forment un ensemble d'hypothèses validées ou invalidées par l'expérience, ainsi qu'une description qualitative de l'activité cognitive au travail préconisant des recommandations sur l'environnement de travail.

8.3. Théories et modèles d'accidents

La démarche analytique en sûreté de fonctionnement représente les accidents comme une succession d'événements dans laquelle la sécurité apparaît comme une propriété des systèmes. L'ingénierie de la résilience [**70**], dans un cadre systémique, définit la sécurité comme un phénomène émergeant du système plutôt que comme une propriété.

8.3.1. Modèles d'accident. — Comme nous l'avons vu dans le chapitre 3 section 3.3.4, Hollnagel [**68**] classe les modèles d'accidents en trois catégories : séquentiel, épidémiologique et systémique.

Dans le modèle séquentiel, l'accident est expliqué par une succession d'événements reliés entre eux par une relation de cause à effet. Dans le modèle épidémiologique élaboré par Reason [**109**], l'accident est le résultat des défaillances passives, introduites par des conditions latentes dont l'effet n'est pas immédiat, mais révélées lors de la sollicitation d'une fonction ou d'un composant du système. Enfin, le modèle systémique, introduit par Woods, Leveson et Hollnagel [**140, 91, 68**] décrit l'accident par l'émergence d'interactions complexes entre les différentes composantes du système. L'accident est la conséquence de coïncidences d'événements plutôt qu'une succession déterministe d'événements [**68**].

8.3.2. Référentiel méthodologique. — La sûreté de fonctionnement n'a pas encore développé des méthodes d'évaluations et de scénarisation de la dynamique des accidents relatives aux trois modèles présentés. Dans les faits, seuls les deux premiers modèles d'accident forment un cadre méthodologique en sûreté de fonctionnement. Les principales méthodes ont été présentées dans le chapitre 3 section 3.5 :

– la technique des arbres de défaillance ;
– celle des arbres d'événements ;
– ou encore l'Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticités (AMDEC).

Elles sont largement employées dans l'industrie et préconisées par les référentiels normatifs.

Elles établissent une base de représentation du système à partir de l'état de ses composants. Que ce soit la méthode des arbres de défaillances, celle des arbres d'événements ou bien l'AMDEC, l'état des composants est bimodal : fonctionnement et non-fonctionnement ou multimodal. Ces méthodes permettent d'inférer l'état du système à partir du vecteur des variables binaires ou multimodales des composants du système et l'on peut suivre l'évolution de l'état du système sur un graphe d'état. À titre d'illustration, la figure 8.1 représente un système formé de deux composants aux états binaires, cela forme quatre états possibles pour le système, la trajectoire dessinée sur la figure décrit un scénario d'évolution de l'état du système en quatre temps.

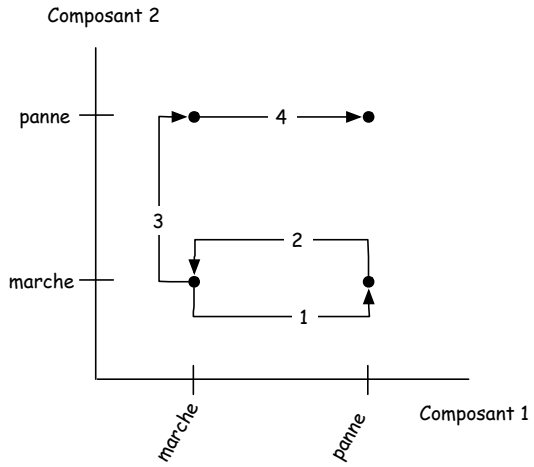


FIGURE 8.1. Représentation séquentielle de la dynamique du système

Cette représentation des accidents répond entièrement au besoin des systèmes techniques dont la sécurité est basée sur un ensemble de scénarios préétablis contre lesquels le système doit se prémunir. Toutefois, elle s'avère trop réductrice lorsqu'il s'agit de traiter les événements impliquant les humains et les organisations. L'assimilation des opérateurs humains à un système bimodal va à l'encontre des modèles de la psychologie cognitive. Pour s'affranchir de cette simplification, les modèles systémiques transfèrent l'étude des composants à l'étude des fonctions du système. L'objectif étant de pouvoir représenter la dynamique du système sociotechnique dans un continuum basé sur des mesures des fonctions exercées par le système. La figure 8.2 présente une trajectoire continue de l'évolution d'un système effectuant trois fonctions. La difficulté réside dans la recherche d'une mesure efficace des fonctions.

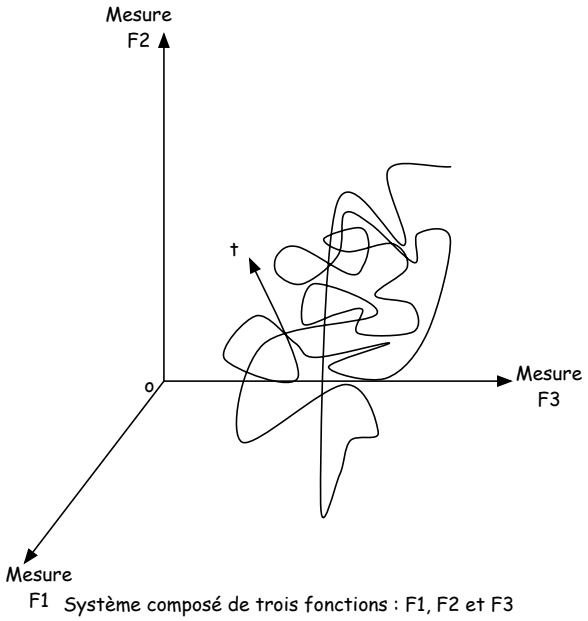


FIGURE 8.2. Représentation de la dynamique du système dans un continuum

8.3.3. Un référentiel commun : la systémique. — L'avantage immédiat de l'approche systémique est une meilleure intégration des études orientées facteurs humains avec celles de la sécurité, notamment en corrigeant le référentiel de l'étude. Dans la perspective de Woods et d'Hollnagel [**141, 139, 67**], les systèmes sociotechniques sont des systèmes cognitifs, ils les nomment *Joint Cognitive Systems*. Les auteurs ont développé une nouvelle branche de l'ingénierie des interactions hommes-machines appelée *Cognitive Systems Engineering* (CSE) [**69, 76**]. Les systèmes hommes – machines ont traditionnellement été analysés séparément et à cela venait s'ajouter l'étude des interactions. Pour les fondateurs de CSE cette décomposition est insuffisante, une représentation du système dans son ensemble est requise unissant les opérateurs et les machines. Le dénominateur commun est donné par la dimension cognitive du système ainsi réuni.

Toutefois, une représentation essentiellement globale du système ne permettra pas de réaliser l'amélioration de la sécurité. En effet, les relations à l'intérieur du système n'ont pas toutes la même intensité et les mêmes conséquences pour la sécurité. [**27**] énonce un bilan mitigé des représentations systémiques dans les études de sécurité. L'auteur conclut sur le nécessaire rapprochement des spécialistes de l'ingénierie de la sûreté de fonctionnement et des spécialistes des sciences humaines et sociales. La réalisation d'études de sécurité à l'aide d'une méthode systémique demeure, à notre point de vue une démarche complémentaire aux analyses de sûreté de fonctionnement existantes.

8.4. La méthode FRAM

Le cadre de la systémique propose aux spécialistes des sciences sociales et de l'ingénierie un référentiel commun pour modéliser les systèmes complexes, il est nécessaire de proposer une méthode basée sur ce référentiel afin de réaliser les études de sécurité ou d'étude de risque.

La méthode FRAM développée par Hollnagel [**68**] permet de décrire le système sociotechnique par ses fonctions et ses activités plutôt que par sa structure. L'objectif de FRAM est de représenter la dynamique du système par la modélisation des dépendances non linéaires qu'elle contient et par une représentation originale de la performance des fonctions et des activités. Le modèle de dépendance repose sur le concept de résonance fonctionnelle emprunté à la physique ondulatoire, métaphore de la résonance stochastique. Le principe de résonance stochastique consiste à la surimposition d'un signal non linéaire (bruit) sur un signal périodique de faible amplitude difficilement détectable. L'addition du bruit permet alors d'établir une résonance avec le signal de faible amplitude et de le rendre ainsi détectable.

8.4.1. La résonance fonctionnelle. — Normalement utilisée pour expliquer l'émergence d'ordre dans un système, Hollnagel l'applique ici pour expliquer l'apparition des accidents. Il réalise ce transfert vers l'étude de sécurité en s'appuyant sur la variabilité de performance des fonctions ou des activités d'un système sociotechnique.

Selon [**68**], la variabilité de performance dans les systèmes techniques est relative aux imperfections en conception et en production, aux spécifications non exhaustives des conditions de travail (effets de l'environnement et des entrées non prévues). La variabilité de performance des humains et des organisations vient de leur capacité à s'adapter aux conditions de travail et à l'absence de régularité dans les activités (perception, cognition, action, communication).

Le parallèle avec la résonance stochastique s'explique par le caractère stochastique de la variabilité de performance des fonctions et des activités du système assimilés à des signaux non linéaires. D'autre part, Hollnagel utilise la superposition des signaux comme modèle de dépendance fonctionnelle entre les fonctions et les activités du système.

Le signal faible correspond à la variabilité de performance de chaque fonction exercée par les différents sous-systèmes. Cette variabilité de performance est faible dans le sens où les écarts de performance des fonctions n'ont pas ou peu d'impact sur la performance du système et sur la sécurité. Le signal non linéaire permettant d'établir la résonance correspond à la variabilité de performance du reste du système lorsqu'on considère une fonction ou une activité prise à part. Le signal faible peut être la variabilité de performance de n'importe quelle fonction ou activité du système et le bruit correspond à l'agrégation des variabilités de performance du reste du système (environnement compris). Hollnagel appelle ce phénomène la « résonance fonctionnelle. »

L'étude des potentialités d'accident avec la méthode FRAM se résume en quatre étapes appliquées à l'étude d'une activité ou d'une fonction du système qu'il faudra préciser :

(1) Identifier et caractériser les fonctions essentielles. L'étude fonctionnelle des activités et des fonctions est basée sur une représentation hexagonale munie de six connecteurs ;

(2) Déterminer le potentiel de variabilité à l'aide d'une *check-list* ;

(3) Appliquer le principe de résonance fonctionnelle sur les dépendances entre les activités et les fonctions ;

(4) Identifier les barrières contre la variabilité et spécifier les nécessaires mesures de surveillance de la performance.

8.4.2. Analyse de l'activité. — La première étape récrit l'analyse fonctionnelle ou l'analyse de la tâche dans un formalisme constitué de tâches ou de fonctions élémentaires auxquelles sont attachés six attributs (voir figure 8.3). Ces attributs servent de connecteurs entre les fonctions ou activités élémentaires :

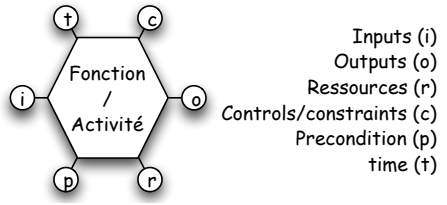


FIGURE 8.3. Codage des fonctions dans FRAM (Hollnagel, 2004 [**68**])

Inputs (i) : La ou les entrées de la fonction ;

Outputs (o) : La ou les sorties de la fonction ;

Ressource (r) : La ou les ressources nécessaires au traitement de la fonction ;

Time (t) : Le temps nécessaire à la réalisation de la fonction ;

Control (c) : Représente le ou les contrôles et contraintes qui gouvernent l'exécution de la fonction (boucle de rattrapage, procédures, méthodes, *etc.*) ;

Precondition (p) : Les préconditions représentent les éléments qui doivent nécessairement être satisfaits pour que la fonction soit opérationnelle.

8.4.3. Variabilité de performance. — La deuxième étape consiste à déterminer la variabilité de performance du contexte général de l'activité dans lequel s'exécutent toutes les fonctions. La variabilité de performance du contexte général est déterminée par onze Conditions Communes de Performance (CCP). Toutes les fonctions ne sont pas affectées de la même façon par les CCP. FRAM classe les fonctions en trois catégories : humaines (H), techniques (T) ou organisationnelle (O) selon les acteurs exécutant les fonctions. De plus, chaque CPP ne s'applique que sur une catégorie de fonction. Le tableau 8.1 présente les onze CCP proposées par Hollnagel [**72**] et la catégorie de fonction à laquelle elles s'appliquent.

Les conditions communes de performance utilisées dans FRAM sont issues de la méthode d'étude de la fiabilité humaine d'Hollnagel CREAM *Cognitive Reliability and Error Analysis Method* se reporter à [**71**] pour une présentation détaillée.

L'action des CCP peut être positive ou négative sur la performance des fonctions, cependant, l'étude de sécurité se place toujours dans le contexte le moins favorable, c'est pourquoi seul l'effet négatif est considéré dans la méthode.

La qualité des CCP est appréciée par trois valeurs possibles : (c_1) stable ou variable mais adapté ; (c_2) stable ou variable mais inadapté ; (c_3) imprévisible. Il s'agit de déterminer pour chaque scénario d'étude la qualité des onze CCP. Hollnagel [**72**] (page 193) établit une relation entre la qualité d'une condition de performance et la variabilité de performance. Si une condition de performance est stable ou variable, mais adaptée alors la variabilité de performance associée à la fonction est faible. Dans le cas stable ou variable, mais inadapté, la variabilité de performance est élevée. Enfin, si une condition de performance est imprévisible, la variabilité associée est très

Numéro	Conditions de performance	Catégorie
C_1	Disponibilité des ressources	H - T
C_2	Entraînement et expérience	H
C_3	Qualité des communications	H - T
C_4	Qualité des interfaces opérateurs - machines	H
C_5	Accessibilité et disponibilité des méthodes et des procédures	H
C_6	Conditions de travail	H - T
C_7	Nombre d'objectifs simultanés	H - O
C_8	Temps disponible	H
C_9	Rythme circadien	H
C_{10}	Qualité de collaboration en équipe	H
C_{11}	Qualité et support de l'organisation	O

TABLE 8.1. Nomenclature des conditions communes de performance

élevée. On notera pour la suite, v_1 le niveau de variabilité faible, v_2 le niveau de variabilité élevé et v_3 le niveau de variabilité très élevé d'une fonction.

Les CCP déterminent donc la contrainte de variabilité commune à toutes les fonctions de l'activité. L'évaluation des effets des CCP sur les fonctions sera précisé au paragraphe suivant.

8.4.4. Dépendance fonctionnelle. — La troisième étape établit les dépendances entre les fonctions ou activités. Ceci est effectué par la mise en correspondance des attributs assignés à la première étape. Graphiquement cela revient à connecter les entrées et les sorties des fonctions représentées par leur hexagone, la figure 8.4 fournit un exemple de réseau FRAM appliqué à la procédure de blocage d'une aiguille pour protéger une équipe de maintenance en activité sur les voies. Cet exemple sera discuté de façon détaillée dans le chapitre suivant. Le réseau ainsi créé permet de visualiser le flux des informations et des matières lors de l'exécution normale de l'activité étudiée. Les mentions H, T ou O dans l'en-tête des fonctions indique la catégorie des entités participant à la fonction. Il s'agit alors de rechercher les résonances fonctionnelles négatives issues de la variabilité de performance des fonctions et propagées par les interrelations complexes entre les fonctions.

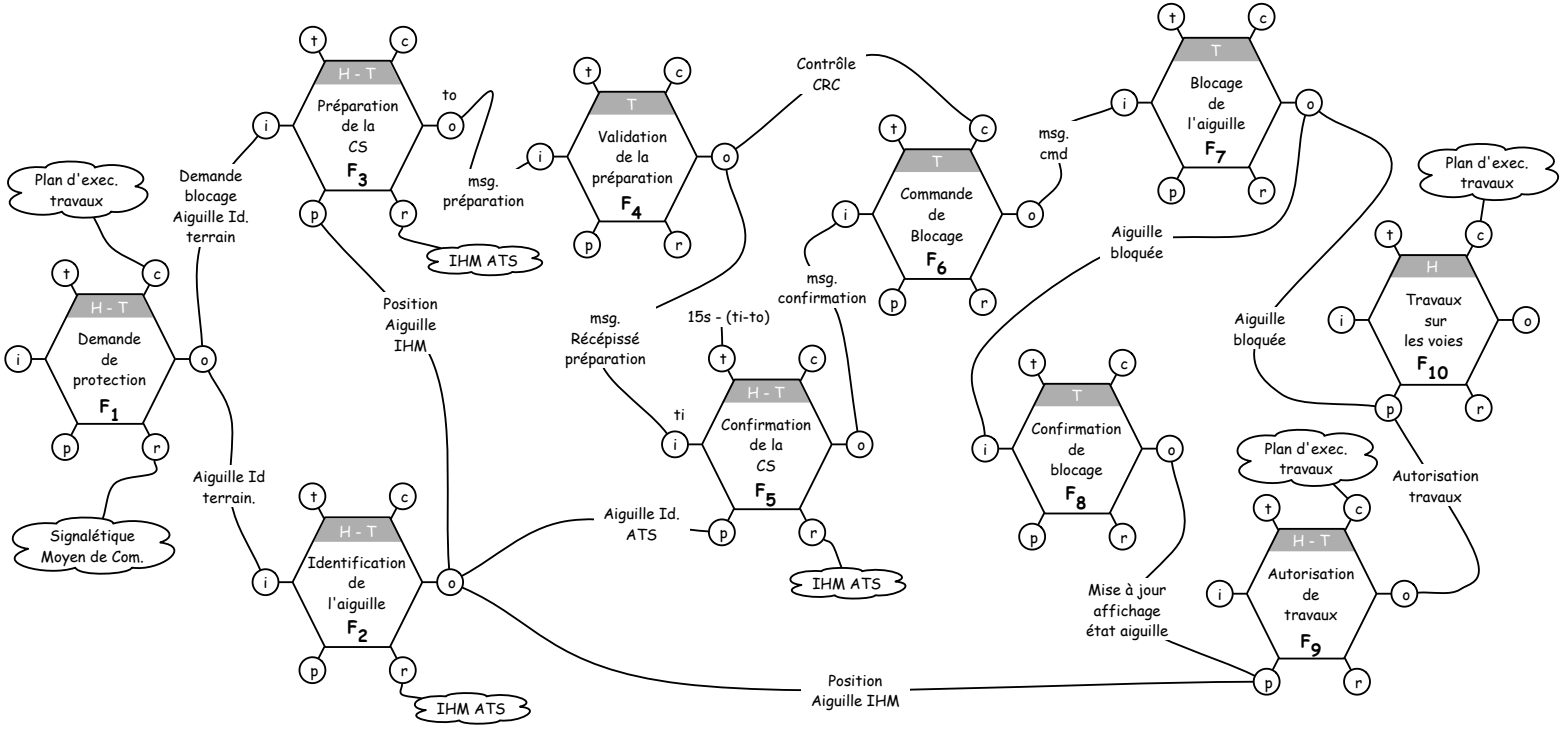


FIGURE 8.4. Réseau FRAM

8.5. Proposition d'une méthode dirigée

8.5.1. Étude de l'activité. — La première étape consiste à comprendre l'activité afin d'en déduire ses caractéristiques ainsi que ses attributs de modélisation. La description de l'activité passe par la décomposition en actions ou fonctions élémentaires auxquelles il faudra préciser la nature des acteurs impliqués : Humain, Technologique, Organisationnel, une association de deux ou des trois types d'acteurs. Pour chaque fonction élémentaire, un dictionnaire des attributs doit être établi. Il s'agit de rechercher un identifiant unique et représentatif pour chacun des attributs (*input, time, control, ressource, precondition, output*) de la fonction. Il peut y avoir plusieurs attributs du même type, seul l'attribut *output* est obligatoire pour chaque fonction, toutefois, le modèle gagnera en précision dès lors que le maximum d'attributs sera indiqué.

L'élaboration du dictionnaire des attributs doit être normalisée. En effet, des choix de modélisation sont toujours possibles, à savoir, un attribut *control* peut être assimilé à un attribut *precondition* et vice-versa, de même qu'un attribut *input* peut être confondu avec une précondition.

Dans la liste d'attributs proposée par Hollnagel, nous distinguons trois catégories. Les attributs *precondition* et *control* agissent comme des barrières sur l'exécution de la fonction. Les attributs *time* et *ressource* représentent ce qui est consommé par l'activité (leur absence totale interdit la réalisation de la fonction). Enfin les attributs *input* et *output* traduisent la transformation effectuée par la fonction.

Des confusions sont possibles entre les attributs *input, precondition* et *control* du fait que ces attributs établissent une contrainte de précédence sur la fonction. Les attributs *time* et *ressource* traduisent tous les deux une ressource de la fonction, toutefois les sources de confusions sont faibles, car l'attribut *time* représente une ressource temporelle.

Les règles suivantes visent à proposer des règles de décision dans les choix de modélisation.

8.5.1.1. Input. — L'attribut *input* correspond à ce qui va être traité et transformé par la fonction. Son absence bloque la réalisation de la fonction. Il s'agit d'un flux de matière ou d'information qui sera transformé via un plan en un autre flux de matière ou d'information. Par exemple, un flux d'information du type « numéro d'identifiant » qui sera transformé par la fonction en une « position de commande » sur un synoptique de commande. Un flux de matière tel qu'une molécule chimique qui sera transformé par la fonction en un médicament est un autre exemple. Un flux de matière respectivement d'information n'est pas exclusivement transformé en un autre flux de matière ou d'information. En reprenant l'exemple d'une molécule chimique, la fonction peut être amenée à transformer ce flux de matière en un flux d'information tel que la formule chimique de la molécule. Inversement, par la donnée d'une formule chimique, la fonction peut être amenée à produire la molécule.

8.5.1.2. Precondition. — On reconnaîtra un attribut *precondition* par le fait que ce flux de matière ou d'information précède l'exécution de la fonction et n'est pas utilisé pendant l'exécution. L'exemple le plus représentatif est celui d'une autorisation d'exécution de la fonction. Dans le domaine ferroviaire, l'autorisation de circuler sur une voie est donnée par l'état d'une barrière symbolique (la signalisation) interprétée par le conducteur. Le flux d'information « voie libre » (feu vert) fourni par le système de signalisation est un attribut *precondition* pour la fonction

du train de circuler sur la voie. Ce flux n'est pas nécessairement informationnel, au début du transport ferroviaire, l'autorisation de circuler sur une voie était donnée au conducteur dès lors qu'il possédait le « bâton pilote » associé à la voie.

L'absence ou l'irrégularité d'un attribut *precondition* peut ne pas empêcher l'exécution d'une action. Généralement, il s'agit d'une barrière franchissable.

La différence entre les attributs *input* et *precondition* est illustrée dans la figure 8.5

8.5.1.3. Control. — Un attribut *control* contrairement à l'attribut *precondition* agit pendant l'exécution de la fonction. Ce flux d'information ou de matière représente généralement une barrière fonctionnelle ou immatérielle qui contrôle l'exécution de la fonction.

Le rôle de l'attribut *control* est illustré sur la figure 8.5.

Une procédure est un flux d'information permanent pendant l'exécution de la fonction qui illustre un attribut de type *control*. Il peut exister des boucles de rétroactions entre l'état de la fonction et l'état de l'attribut *control*, c'est le cas dans une procédure qui s'adapte à l'état de la fonction. Toutes autres barrières de sécurité (voir section 3.3.2 page 69) peuvent être considérées comme un attribut de type *control* sauf dans le cas où l'étude modélise l'activité d'une barrière auquel cas l'étude approfondie des mécanismes de la barrière est effectuée.

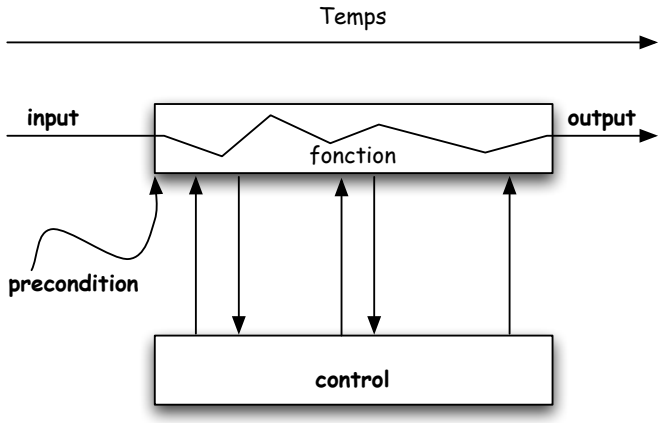


FIGURE 8.5. Différence entre *input*, *precondition* et *control*

8.5.1.4. Ressource. — L'attribut *ressource* représente ce qui est consommé ou utilisé par la fonction pour transformer le flux entrant (*ie. input*). Il peut être permanent à l'exécution de la fonction ou utilisé ponctuellement à n'importe quel moment de l'exécution de la fonction. Une interface homme-machine est un exemple de ressource permettant à un opérateur humain de réaliser une fonction de type contrôle ou commande sur un procédé, le flux entrant à ce type de fonction est un ordre de contrôle ou de commande.

8.5.1.5. Time. — L'attribut *time* peut être un flux d'information indiquant le temps disponible pour réaliser la fonction. Il peut s'agir également d'une représentation de la pression temporelle qui contraint l'exécution de la fonction. D'une manière générale, l'attribut *time* sera différencié des autres attributs par le caractère temporel d'un contrôle, d'une ressource ou d'une contrainte.

Nom	Nature	Attributs
Id1	H,T,O	– Id *input 1* – … – Id *input* n_i – Id *precondition 1* – … – Id *precondition* n_p – Id *time 1* – … – Id *time* n_t – Id *control 1* – … – Id *control* n_c – Id *ressource 1* – … – Id *ressource* n_r – Id *output 1* – … – Id *output* n_o

TABLE 8.2. Tableau descriptif d'une fonction élémentaire

8.5.1.6. Formalisation des fonctions. — Le résultat de cette phase est constitué d'une liste d'attributs pour chaque fonction. Le tableau 8.2 constitué de 3 colonnes pour le nom de chaque fonction, la nature de la fonction, la liste des attributs est un exemple de présentation d'une liste d'attribut pour une fonction. On note n_i, n_p, n_t, n_c, n_r et n_o respectivement le nombre d'attributs du type *input, precondition, time, control, ressource* et *output*.

8.5.2. Variabilité de performance. — La technique proposée par Hollnagel [**72**] (page 193), consiste à présent à déterminer pour chaque fonction, les CCP qui sont susceptibles de l'affecter. Par exemple, une fonction de catégorie H (pour « Humaine ») est potentiellement affectée par toutes les CCP incluant la catégorie H, or, de par la réalité de la fonction, toutes les CCP incluant la catégorie H ne sont pas forcément applicables, seule une expertise permet de déterminer la liste des CCP dont relève la fonction. Le résultat de cette étape fournit la liste de CCP dont dépend l'activité.

Cependant, une activité peut impliquer plusieurs acteurs à différents endroits du système. Il est donc nécessaire d'affiner cette allocation par le dédoublement des CCP lorsque cela est nécessaire. Prenons l'exemple d'une activité ayant recours à deux agents ayant un niveau d'expérience différent, la CCP C_2 « Entraînement et expérience » ne peut être appliquée à ces deux agents, il est alors nécessaire d'introduire une CCP C_2 pour chaque agent.

L'étape suivante consiste à évaluer la qualité des conditions de performance afin de déterminer le potentiel de variabilité de chaque fonction. Chaque évaluation de l'ensemble des conditions de performance de l'activité définit un contexte d'exécution, autrement dit, un scénario de mode d'exploitation. On parlera de grille d'évaluation des conditions de performance pour chaque évaluation de l'ensemble des conditions de performance.

L'évaluation de la qualité des conditions de performance doit être effectuée par des experts de chaque domaine dont dépendent les CCP. Par exemple, la CCP C_1 « Disponibilité des ressources »

a un impact sur les fonctions de type H « Humaine » et T « Technologique », de fait, l'évaluation doit être effectuée en collaboration par des psychologues ou ergonomes et des ingénieurs.

Une grille d'évaluation est formalisée dans un tableau indiquant la valeur obtenue pour chaque CCP, le tableau 8.3 donne un exemple d'évaluation pour une activité dont les fonctions dépendent des onze CCP sans que ne soient ajoutées de nouvelles conditions de performance liée à la réalité de l'activité.

CCP	Variabilité	Catégorie
C_1	v_1	H - T
C_2	$\mathbf{v_2}$	H
C_3	v_1	H - T
C_4	v_1	H
C_5	$\mathbf{v_3}$	H
C_6	v_1	H - T
C_7	v_1	H - O
C_8	$\mathbf{v_2}$	H
C_9	v_1	H
C_{10}	v_1	H
C_{11}	v_1	O

TABLE 8.3. Exemple d'évaluation des CCP

Les fonctions affectées par des CCP de forte variabilité sont considérées au cas par cas pour déterminer l'impact sur la variabilité de performance de la fonction.

Nous proposons que soit associé à chaque évaluation du potentiel de variabilité d'une fonction, un mode de fonctionnement basé sur le modèle des modes d'exploitation présenté au chapitre 6. La définition de la fonction passe donc par la description de chacun des modes, normaux, stressés et dégradés. Il alors nécessaire de présenter les conditions d'application d'un mode à une fonction. Par exemple, lorsque toutes les CCP sont adéquates à la réalisation de la fonction, le mode de la fonction est normal.

Enfin, les fonctions n'ont pas le même niveau de variabilité de performance selon que le mode est normal, stressé ou dégradé. Ceci nous amène à déterminer les niveaux de performance associés à chaque mode, et ce, pour toutes les fonctions. En effet, il est impossible d'adresser de manière générale des règles d'allocation de niveau de variabilité, seule l'analyse au cas par cas des fonctions permettra de déterminer les conséquences de la variabilité de performance du contexte sur la variabilité de performance de la fonction. On voit, ici, une difficulté majeure de la méthode qui en fait toute sa richesse. FRAM nécessite une étude minutieuse et approfondie de chaque fonction. L'identification des conditions de performance et la caractérisation de l'effet de leur variabilité sur l'exécution de la fonction est au cœur de la démarche. La difficulté réside dans la définition, **pour chaque fonction**, d'un raisonnement causal, permettant d'inférer la variabilité de performance du produit de la fonction (attribut *output*) à partir de l'évaluation du contexte d'exécution (c.-à-d. les CCP).

8.5.3. Un raisonnement causal pour chaque fonction. — Un modèle causal est un modèle abstrait qui utilise la logique de cause à effet pour décrire le comportement d'un système. L'identification des interrelations complexes lors de l'élaboration du diagramme de FRAM est un exemple de modèle causal permettant de décrire les relations de causes à effets entre les fonctions. Comme nous venons de le voir, il est nécessaire d'appliquer un modèle causal à chacune des fonctions afin de déterminer sa variabilité de performance en fonction de la variabilité de performance de son contexte (les CCP et ses attributs).

Le raisonnement causal d'une fonction dans FRAM est à 3 volets. Le premier concerne l'identification du mode de fonctionnement à partir des CCP. Le deuxième doit permettre de déterminer les changements générés par le mode sur la configuration de la fonction. Le troisième permet d'identifier la variabilité de performance du produit de la fonction à partir du changement de configuration de la fonction.

Prenons le cas d'une fonction opérée par un opérateur humain de supervision de trafic ferroviaire consistant à diagnostiquer une anomalie sur le TCO. Supposons que cette fonction dépend des deux conditions de performances « temps disponible » et « entraînement et expérience ». Supposons de plus qu'il n'existe aucune connexion sur les attributs d'entrée de cette fonction. Le premier raisonnement causal consiste à déterminer le mode de la fonction de diagnostic. Le mode normal relève de la bonne adéquation de ces deux conditions de performance. Le mode stressé, décrit au chapitre 6 comme représentant « toutes les phases opérationnelles de la fonction dans lesquelles elle atteint les limites de son dimensionnement et de sa performance ». Traduit en terme d'action humaine, le mode stressé correspond à un niveau de performance limite où l'opérateur humain dispose à peine des facultés nécessaires à son accomplissement. Dans notre exemple, ce mode est atteint lorsque l'opérateur dispose de l'entraînement et de l'expérience suffisante pour accomplir cette tâche, mais que le temps disponible restreint sa performance. Le mode dégradé traduit une incapacité à traiter la fonction, elle apparaît notamment lorsque l'opérateur humain n'est pas suffisamment entraîné ou ne dispose pas de l'expérience suffisante pour accomplir cette tâche.

Le deuxième raisonnement causal consiste à déterminer le changement de configuration de la fonction dans chaque mode. Dans le mode normal, la fonction est effectuée conformément à ce qui est attendu, c'est-à-dire que l'opérateur humain réalise un diagnostic correct dans la majorité des cas. En mode stressé, le raisonnement de l'opérateur humain sera perturbé par la contrainte temporelle, bien que suffisamment entraîné, il risque d'être amené à faire des raccourcis cognitifs pouvant impliquer des erreurs de diagnostic qu'il ne commettrait pas en mode normal. Enfin, en mode dégradé, l'opérateur ne dispose pas des schémas mentaux lui permettant de réaliser la tâche de diagnostic, la fonction peut être alors considérée comme quasiment aléatoire.

Le dernier raisonnement causal sert à déterminer la variabilité de performance produite par la fonction. Dans le mode normal, on s'attend à ce que l'opérateur ait une performance faiblement variable, c'est-à-dire qu'il ne se trompe que très rarement, et ce, pour des cas d'anomalies ambiguës et complexes. Dans le mode stressé, la variabilité de performance de l'opérateur humain devient plus variable au sens ou les risques liés aux raccourcis cognitifs sont plus grands. En d'autres termes, la confiance que l'on peut donner aux résultats du diagnostic est plus faible. Enfin, le mode stressé, de par son caractère quasi aléatoire, génère une variabilité de performance très élevée, aucune confiance ne peut être apportée au produit de la fonction.

Les modes de fonctionnement présenté dans cet exemple sur une action humaine sont à rapprocher avec le modèle COCOM d'Hollnagel [**71**] présenté dans le chapitre 4 page 97 et notamment le tableau 4.2. Dans COCOM, les modes de contrôle stratégiques et tactiques correspondent au mode normal de l'activité de l'opérateur humain, le mode de contrôle opportuniste est à rapprocher du mode stressé et enfin le mode de contrôle erratique au mode dégradé. Le vocabulaire et les définitions présentés dans le modèle basé sur les modes normaux, stressés et dégradés présentent l'avantage de pouvoir s'appliquer sur une fonction de type Humaine, Technique ou Organisationnelle.

Dans FRAM, Hollnagel [**68**] propose d'appliquer un raisonnement spécifiques aux fonctions relatives aux opérateurs humain. Ce raisonnement est basé sur le modèle *Efficiency Thoroughness Trade Off* (ETTO) (traduit par « compromis efficacité minutie »). Les nombreux résultats obtenus au siècle dernier à partir d'études expérimentales de la performance humaine sur des tâches simples, montre que généralement, les sujets font plus d'erreurs lorsqu'ils répondent plus rapidement et inversement, ils en réalisent moins lorsqu'ils prennent plus de temps. Il s'agit du compromis « rapidité précision » : Il est impossible de remplir les deux critères en même temps sur une longue période. Hollnagel généralise ce modèle à des tâches plus complexes par le compromis efficacité minutie. La minutie représente l'application des opérateurs humains à effectuer la bonne activité de la meilleure façon possible. L'efficacité traduit le rendement d'une activité. Le compromis consiste pour les opérateurs humains à être minutieux sans perdre trop d'effort pour remplir la demande générée par la situation et sans se soucier si cette demande est imposée par une source extérieure ou provenant de leur propre activité. Ce compromis est proche de l'idée du compromis cognitif [**9**] développée par Amalberti sur le cadre de la sécurité écologique. Tandis que le modèle d'Hollnagel s'applique à une tâche dans son ensemble (outils et environnement compris), le compromis cognitif d'Amalberti se situe au niveau de la cognition. Il permet de décrire l'utilisation d'heuristiques de décisions et de raccourcis mentaux. L'opérateur humain réalise un écart vis-à-vis de la tâche prescrite (un raccourci) dans le seul but de garantir au mieux la sécurité tout en préservant des ressources cognitives. Les ressources cognitives servent à anticiper les événements à venir et à ne pas perdre la conscience de la situation.

Au niveau de la tâche, Hollnagel dérive le modèle ETTO par un certain nombre de règles qui visent à expliquer la réalité de la performance humaine. Ces règles présentent le type de raisonnement possible d'un opérateur vis-à-vis d'une situation de travail contrainte (temps ou ressources par exemple), la liste des règles est présentée ci-après :

– « Tout semble OK. » L'opérateur réalise un jugement rapide basé sur sa propre expérience ;
– « Pas vraiment important. » Le niveau de gravité est temporairement relevé, l'opérateur pense que les symptômes ne sont pas suffisamment sérieux pour nécessiter une action de sa part ;
– « Normalement OK, pas besoin de vérifier maintenant. » L'opérateur supprime une vérification sur la base de l'habitude afin de remplir ses objectifs de production ;
– « Quelqu'un d'autre le vérifiera plus tard. » L'opérateur s'appuie sur l'hypothèse que quelqu'un d'autre fera cette vérification plus tard ;
– « Quelqu'un l'a déjà vérifié. » L'opérateur s'appuie sur l'hypothèse que quelqu'un a déjà effectué cette vérification ;

– « Je ne me souviens plus comment on fait. » Le manque d'expérience et de support de l'organisation empêche l'opérateur de réaliser la tâche ;
– « Pas le temps ni les ressources nécessaires, sera fait plus tard. » L'opérateur reporte la tâche car elle n'est pas jugée essentielle et s'applique à effectuer une autre activité ;
– « Cela marchait la dernière fois. » L'opérateur remplace une vérification en s'appuyant sur une référence anecdotique ;
– « Pas de souci, c'est parfaitement sécurisé, rien ne va se passer. » Quelqu'un se voit inculquer un mauvais principe de sécurité sur la base d'une autorité ou d'une expérience plutôt que sur les faits. Cette dernière règle s'applique également au cas d'**homéostasie du risque** [**135, 136**]. L'homéostasie du risque traduit une tendance qu'auraient les individus à fonctionner « à un niveau de risque *perçu* constant ». En d'autres termes, se sentant protégé par une barrière de sécurité, l'opérateur a tendance à compenser en adoptant une attitude plus risquée. Il s'agit également d'une surconfiance que l'opérateur place dans les équipements de sécurité.

D'autres modèles issus de l'ergonomie sont applicables. Dans le domaine de la sécurité routière, plusieurs modèles du comportement humain soumis à des risques ont été élaborés. Par exemple, le modèle de l'évitement de la menace élaboré par Fuller [**49**] représente le comportement d'un opérateur humain par des réponses conditionnées et intègre la notion d'anticipation. L'opérateur associe, par expérience, des stimuli à des situations dangereuses. L'expérience contient alors un répertoire des stimuli. La détection ou la veille des stimuli indique une menace et déclenche le comportement d'évitement associé à la situation dangereuse. La réponse dépend également de la probabilité subjective d'apparition du danger, du coût de l'évitement et du bénéfice sur le rendement de la prise de risque. Un autre exemple adapté au modèle de conduite automobile est celui du modèle hiérarchique du risque de Van der Molen & Bötticher [**123**] qui définit trois niveaux d'activité et trois niveaux de risque associés à ces activités. Dans le domaine du pilotage d'avion, le modèle du compromis cognitif d'Amalberti [**9**] présenté précédemment, définit le travail cognitif par deux activités : ajuster sa représentation et garder la connaissance de la situation. La variation du niveau d'exigence et la métaconnaissance de la performance imposent à l'opérateur un compromis entre la réussite et la compréhension.

Dans le domaine ferroviaire, peu de modèles de la tâche et de la cognition d'un opérateur ATS sont disponibles, les expériences menées sur la plateforme SPICA-RAIL ont été envisagées dans cet objectif. Le premier cas d'étude présenté dans le chapitre suivant utilise les résultats des expériences pour déterminer le modèle causal de certaines fonctions humaines.

8.5.4. Dépendance fonctionnelle. — Lorsque le dictionnaire des attributs a été correctement établi, les interrelations entre les fonctions doivent apparaître. Si l'identifiant d'un attribut *output* apparaît dans un attribut d'une autre fonction, un lien est tracé entre les deux fonctions. Le résultat de cette étape permet de concevoir le réseau FRAM de l'activité. Ce réseau présente l'exécution normale de l'activité, en ce sens, il est à rapprocher du mode normal d'exploitation présenté au chapitre précédent.

8.5.5. Résonance fonctionnelle et instanciation du modèle. — Le terme instanciation est issu de l'informatique, il indique le remplacement d'une variable par une constante. En programmation orientée objet, on appelle instance d'une classe un objet avec un comportement et un état, tous deux définis par la classe. Dans ce contexte, instance est un anglicisme, qui signifie

« cas », « exemple ». Ce terme a été utilisé dans FRAM par [**138**] et reflète bien l'utilisation qui est faite du modèle. En effet, le modèle initial permet de visualiser le comportement normal d'une activité et offre ainsi une approche complémentaire aux techniques classiques de sûreté de fonctionnement (arbres de défaillance ou arbres d'événement) qui représentent seulement la vue des défaillances du système. La vue « défaillante » de l'activité dans FRAM est donnée par l'instanciation du modèle.

L'instanciation du modèle FRAM consiste à initialiser les fonctions à partir d'une grille d'évaluation des conditions de performance, puis à déterminer à partir des raisonnements causaux de chaque fonction la propagation de la variabilité de performance au travers du modèle et à identifier les accidents potentiels lorsque la variabilité de performance d'une ou plusieurs fonctions atteint le seuil critique d'accident du système.

Cette dernière étape consiste à propager les effets des conditions de performance sur le produit des fonctions dans le réseau de dépendance fonctionnelle. L'application de la résonance fonctionnelle permet de visualiser sur le réseau FRAM les modes d'exploitation stressés, dégradés, voire accidentels de l'activité globale.

Cette étape dépend fortement du contexte de l'étude. Toutes les connaissances disponibles doivent être mises à contribution. Par exemple, les ingénieurs déterminent la sûreté de fonctionnement des composants techniques et sont donc à même de déterminer l'effet d'un contexte particulier sur l'exécution d'une fonction technologique. Les ergonomes et psychologues de la cognition apportent respectivement de l'expérience et des modèles de la cognition qui permettent d'évaluer les effets de la variabilité du contexte sur la variabilité des fonctions humaines. Pour l'aspect organisationnel, peu développé dans cette thèse, les spécialistes des sciences sociales doivent fournir les éléments d'application de la résonance fonctionnelle pour les fonctions organisationnelles.

8.5.6. Proposition de mesures correctives. — L'objectif de la démarche FRAM est de mettre en évidence des scénarios accidentels en utilisant le modèle systémique d'accident. L'issu de cette démarche doit permettre de proposer des moyens de prévention contre les scénarios identifiés.

8.6. Conclusion

La technique FRAM permet de représenter l'exécution d'une activité dans tous ses modes d'exploitation et notamment le mode normal. En effet, contrairement aux techniques usuelles de sûreté de fonctionnement qui représentent essentiellement les modes dégradés du système, la technique FRAM s'appuie sur l'aspect fonctionnel détaillé de l'activité et offre l'avantage de modéliser plusieurs scénarios (stressés, dégradés, voire accidentels) sur un schéma commun.

Ce ne sont pas tant les résultats de la méthode qui sont enrichissants, mais comme toute modélisation systémique, la construction du modèle apporte des éléments de connaissance du système dans son fonctionnement et notamment en ce qui concerne les interrelations complexes qu'il renferme. En effet, l'analyse systémique requiert de nombreuses informations et nécessite de comprendre en détail les différents contextes d'exécution des fonctions et leurs effets sur l'activité. Cette démarche constructive propose à l'ingénieur de sécurité une méthode dirigée

qui lui permet de comprendre les phénomènes complexes intervenant dans le système avec un regard interdisciplinaire nécessaire.

Le besoin d'une expertise interdisciplinaire approfondie de chaque fonction afin de déterminer son modèle causal demeure la principale difficulté de cette approche. Cependant, c'est le coût nécessaire à investir pour dépasser les limitations des modèles basés sur un modèle causal plus simple tel que les arbres d'événements. Les systèmes ferroviaires ont atteint un niveau élevé de complexité, le rapport entre activité humaine et sécurité ayant évolué avec l'introduction de systèmes fortement automatisés, il est donc important de prendre en compte cette nouvelle relation, plus complexe, avec les outils méthodologiques adaptés à cette complexité.

Le chapitre suivant présente deux cas d'application de la technique FRAM. Un cas d'étude est étudié pour chaque type de situation de supervision critique identifiée lors de l'état de l'art industriel approfondi, voir section 6.5 page 130.

CHAPITRE 9

CAS D'ÉTUDE

Résumé

La méthode FRAM est appliquée à deux cas de situation critique de supervision. Le premier exemple traite une procédure de protection d'une équipe de maintenance et constitue une situation de supervision critique du type « action directe sur les barrières de sécurité ». Le deuxième s'intéresse au deuxième type de supervision critique identifié au chapitre 6, lorsque l'opérateur humain, bien que normalement pas directement responsable de l'évolution et du contrôle d'une situation dangereuse, a la possibilité de récupérer cette situation.

9.1. Introduction

L'objectif de notre démarche consiste à évaluer l'impact des systèmes ATS sur la sécurité. Les composantes technologiques ayant atteint un niveau élevé de sécurité, l'étude doit se focaliser sur l'évaluation de l'interaction opérateurs humains – machines et son impact sur la sécurité. Cette démarche nécessite la coopération de spécialistes de l'ingénierie ferroviaire (composante technique), des sciences humaines et sociales (composante humaine et organisationnelle) et de la sûreté de fonctionnement pour la synthèse et l'évaluation de la sécurité.

Afin de présenter l'intérêt d'une approche systémique dans cette démarche interdisciplinaire, la méthode FRAM a été appliquée en complément des études de sécurité classiques au cas du blocage d'un appareil de voie en vue de la protection d'une équipe de maintenance. Le processus de modélisation est présenté de façon détaillée. Dans cet exemple, les interactions opérateurs humains - opérateurs humains et opérateurs humains - machines ont un impact sur la sécurité. Il s'agit d'une situation de supervision critique du type « action directe sur les barrières de sécurité ». Un deuxième cas d'étude dont la modélisation sera présentée de façon plus concise traite une situation de supervision critique du deuxième type « récupération d'une situation dangereuse » et adaptée de la tâche qui a été évaluée sur simulateur. La modélisation avec FRAM de ce cas d'étude utilise des résultats issus des expérimentations dans l'élaboration des modèles causaux des fonctions.

9.2. Protection de travaux par procédure de blocage d'aiguille

La protection des équipes de travaux nécessite le blocage des appareils de voies (aiguilles) convergeant vers la zone de travaux. La défaillance du blocage des aiguillages peut s'avérer fatale pour les membres des équipes de maintenance en activité sur les voies.

L'opération est menée en collaboration entre le chef de l'équipe de maintenance et l'opérateur ATS. Elle nécessite la commande directe des enclenchements « ultra » sécuritaires par l'opérateur ATS et est en cela réellement atypique puisque la majeure partie des opérations exécutables depuis le PCC sont normalement « filtrées » par ces mêmes systèmes d'enclenchements et l'ATP. Ici, la commande est directement passée sur le système de contrôle commande des protections. Les ingénieurs et les spécialistes de la sécurité ont toutefois prévu une procédure sécurisée que nous appellerons « Commande de Sécurité » (CS).

Cette procédure est une séquence de communication sécurisée entre le poste informatique ATS et le système de protection. Un Code de Redondance Cyclique (CRC) permet de protéger l'intégrité des échanges d'informations numériques entre les machines. Un mécanisme de double commande est demandé à l'opérateur pour s'affranchir des commandes non intentionnelles. La séquence de CS de demande de blocage d'une aiguille pour protection de travaux se déroule de la façon suivante (voir figure 9.1) :

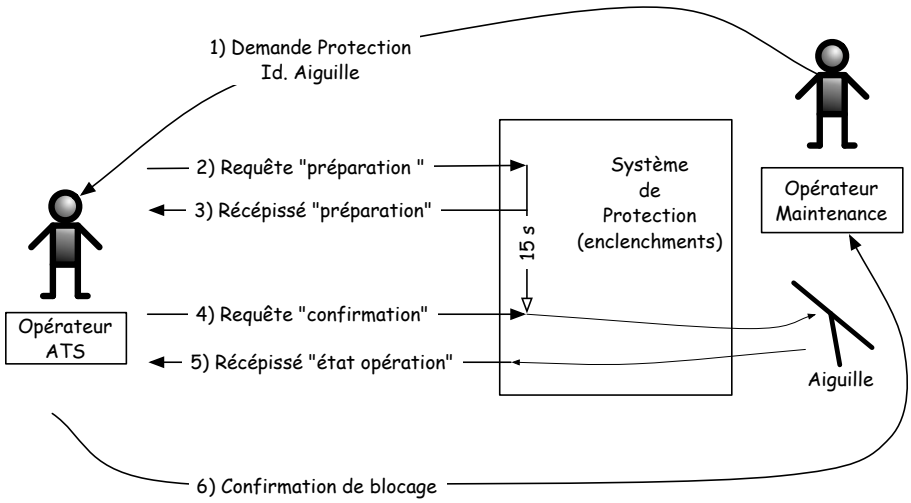


FIGURE 9.1. Procédure CS

(1) L'opérateur de maintenance recherche le numéro de l'aiguille à bloquer et demande la protection à l'opérateur ATS ;

(2) L'opérateur ATS envoie une requête de préparation au système de protection ;

(3) Le système de contrôle commande des enclenchements prépare et envoie un récépissé de la préparation de commande de l'opérateur.

(4) L'opérateur ATS valide sa commande en s'assurant que le récépissé est conforme à sa commande et envoie une requête de confirmation ;

(5) Le système de contrôle commande des enclenchements s'assure de la validité du message en contrôlant la cohérence du CRC des deux messages reçus par l'ATS, puis réalise le blocage de l'aiguille considérée et envoie un récépissé à l'ATS indiquant le statut de l'opération sur l'aiguille ;

(6) Enfin, l'opérateur ATS s'assure du blocage de l'aiguille sur son interface et confirme à l'opérateur de maintenance le blocage de l'aiguille.

Le contexte de l'application de cette procédure est présenté sur la figure 9.2 qui présente une copie de l'écran de supervision de la zone nécessitant une protection par blocage d'aiguille pour la réalisation de travaux sur la voie.

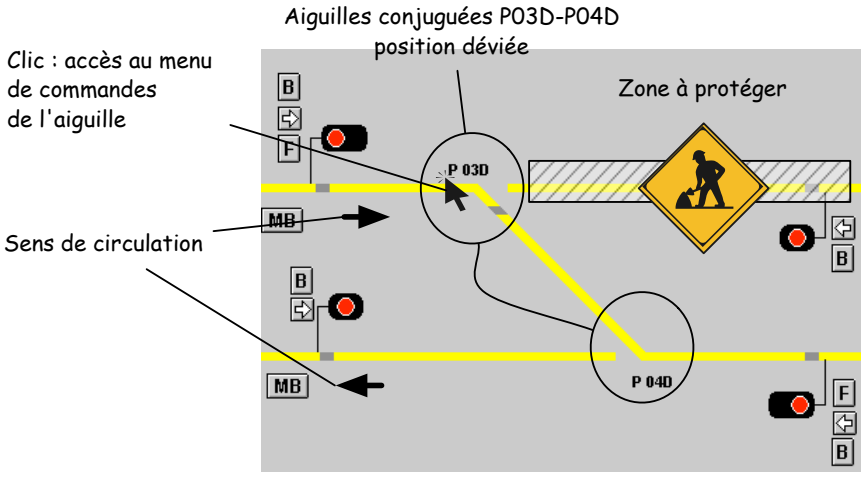


FIGURE 9.2. Écran de supervision : protection de travaux

La zone est constituée de deux voies banalisées (pouvant être empruntées dans les deux sens) et de deux aiguilles permettant aux circulations de changer de voie. Ces deux aiguilles sont actionnées en même temps, elles sont dites « conjuguées » de telle sorte que deux positions soient possibles : la position normale (pas de changement de voie) et la position déviée qui permet aux circulations de changer de voie. Sur la figure 9.2, la position des aiguilles conjuguées est déviée, cela se caractérise par la continuité des segments vers la voie opposée. Sur la voie du haut, la circulation se fait de la gauche vers la droite et inversement sur la voie du bas. La zone à protéger se situe sur la voie du haut à droite de l'aiguille conjuguée. La position déviée de l'aiguille assure la protection des opérateurs de maintenance, en interdisant les circulations sur la zone de travail. Pour les besoins de l'étude, nous faisons l'hypothèse que les aiguilles sont déjà en position déviée avant la demande de protection, la commande de position d'une aiguille n'est pas une action sécuritaire et n'est donc pas soumise au protocole CS car protégée par la barrière fonctionnelle du système d'enclenchement. La procédure de protection des opérateurs de maintenance requiert le blocage de cette aiguille pour éviter tout mouvement *a posteriori* qui pourrait être commandé par un autre opérateur ATS ou bien par les algorithmes de tracé automatique des itinéraires. De plus, certains trains spéciaux, notamment des trains de travaux, ne sont pas détectables par les circuits de voie, ces trains circulent la nuit lorsque le service normal est arrêté, le blocage des aiguilles par l'opérateur ATS garantit l'impossibilité pour ces trains de rentrer dans la zone

protégée. Le blocage interdit également tout changement de position des aiguilles depuis la commande locale sur le terrain.

L'opérateur accède au menu de commande des aiguilles conjuguées en « cliquant » sur l'un ou l'autre identifiant des deux aiguilles conjuguées. La fenêtre représentée sur la figure 9.3 apparaît.

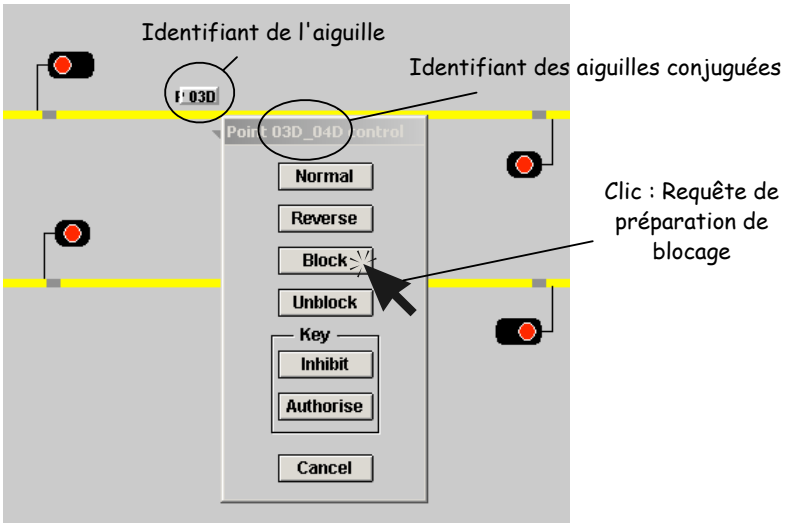


FIGURE 9.3. Menu de commande d'aiguille

Six boutons sont disponibles, les deux premiers permettent de positionner les aiguilles conjuguées. Le bouton *block* permet d'envoyer une requête de préparation de blocage des aiguilles. Inversement, le bouton *unblock* permet d'envoyer une requête de préparation de déblocage des aiguilles. Les deux boutons suivants ne servent pas au cas d'étude présent, le dernier bouton permet de fermer cette fenêtre sans effectuer de commande.

Le récépissé envoyé par le système de contrôle commande des enclenchements est présenté à la figure 9.4. L'opérateur contrôle l'identifiant des aiguilles conjuguées et confirme sa commande en « cliquant » sur le bouton de confirmation.

Lorsque le blocage des aiguilles est effectué, le système de contrôle commande des enclenchements met à jour l'affichage de l'ATS, l'écran de supervision de la figure 9.5 présente l'aspect des symboles ajoutés aux aiguilles spécifiant leurs blocages (ronds rouges sur les aiguilles).

9.2.1. Approche analytique classique. — La probabilité d'un accident potentiel est liée au temps que l'opérateur ATS met pour détecter une CS non réalisée ou erronée. Sur la base des analyses fonctionnelles, les ingénieurs de sûreté de fonctionnement conçoivent les arbres de défaillances des accidents potentiels après identification au préalable des dangers potentiels. Cette technique, analytique repose sur un modèle d'accident linéaire dans un espace d'état du système discrétisé. L'arbre de défaillances d'un accident potentiel sur défaillance du blocage d'aiguille est présenté dans la figure 9.6. Les rectangles représentent les événements « défaillances des fonctions ». Les portes logiques indiquent la conjonction ou la disjonction de défaillances des fonctions filles générant la défaillance de la fonction mère. Les cercles signifient que l'événement n'est pas décomposable et qu'il dispose d'une valeur de probabilité propre. Les triangles inversés,

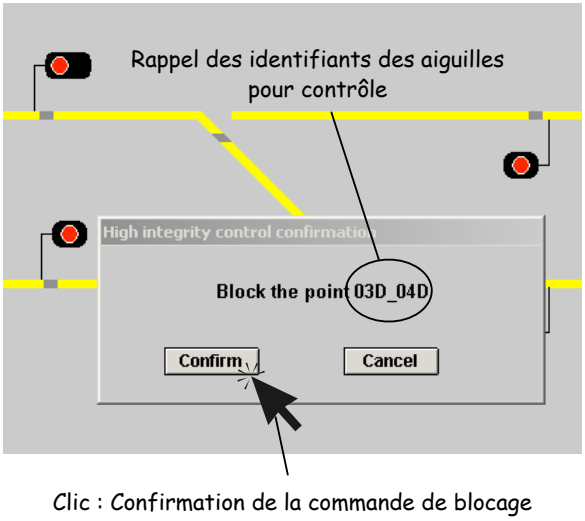


FIGURE 9.4. Fenêtre de confirmation de la commande de blocage

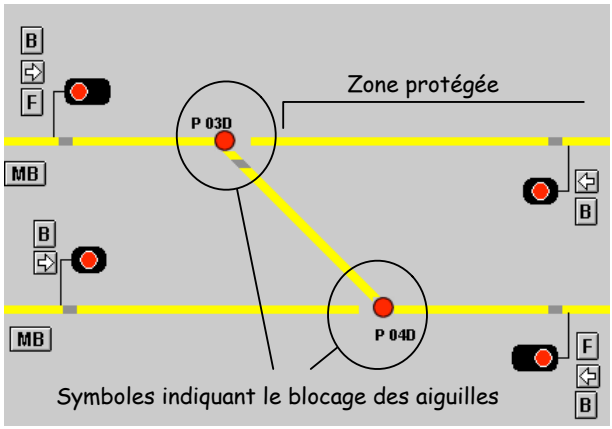


FIGURE 9.5. Aiguilles bloquées

à l'inverse des cercles, indiquent que l'événement se décompose en d'autres événements de base représentés dans un autre arbre de défaillance. Pour une meilleure lisibilité, un symbole « FH » est accolé sur les événements de type humain.

Les valeurs de probabilité des équipements techniques sont calibrées sur la base d'études spécifiques du comportement des composants, sur le retour d'expérience et les données du fournisseur. Les probabilités de défaillance des actions des opérateurs sont généralement issues de la littérature dans le domaine de la fiabilité humaine, les travaux de Swain et Rasmussen [**120, 105**] sont mis à contribution. Par exemple, la probabilité qu'une procédure ne soit pas respectée par un opérateur dépend de facteurs de contexte tels que l'expérience ou l'entraînement. Ainsi, pour un opérateur suffisamment entraîné et pour une procédure habituelle dans l'activité, on considère une probabilité de défaillance de 10^{-3}.

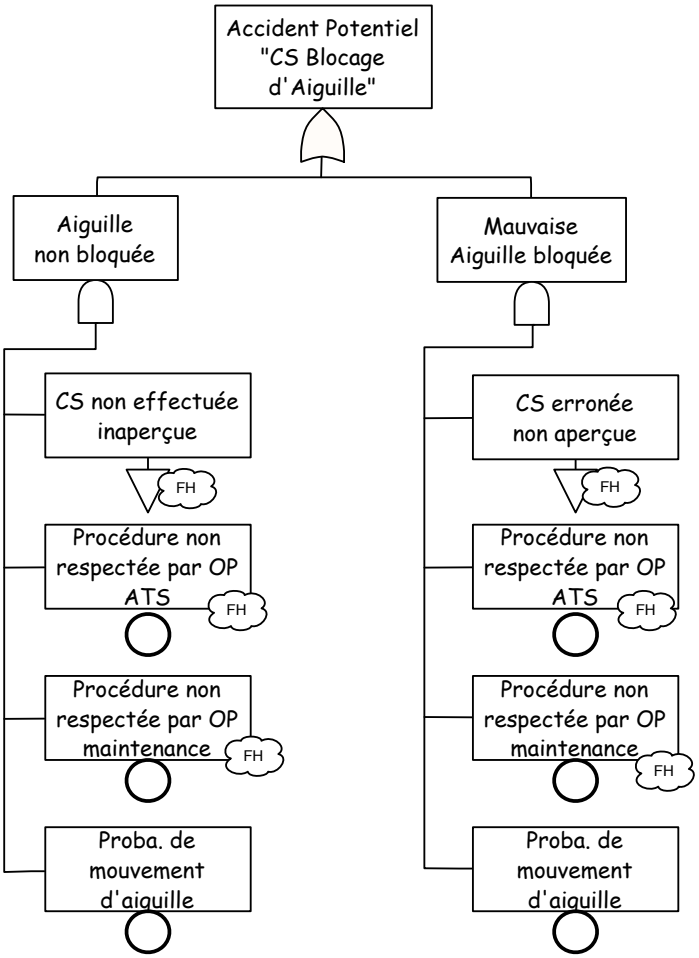


FIGURE 9.6. Arbre de défaillances « Accident sur Blocage d'Aiguille »

Le résultat de cette méthode appliquée au cas d'une CS de blocage d'aiguille pour protection de travaux montre qu'un accident potentiel peut être généré par la défaillance coordonnée d'au moins quatre fonctions dont les valeurs de probabilité sont inférieures à 10^{-3} chacune.

9.2.2. Approche complémentaire avec FRAM. — Cette activité est à présent étudiée avec la méthode FRAM. Pour ce premier cas d'étude, la démarche guidée proposée au chapitre précédent est présentée en détail.

9.2.2.1. Étude de l'activité. — L'étude de l'activité nécessite un approfondissement de l'activité des systèmes techniques et humains mis en jeu dans cette procédure. Le tableau 9.1 synthétise les fonctions mises en jeu pour le blocage d'une aiguille afin de protéger des travaux, une description des fonctions est fournie ainsi que la catégorie des acteurs de la fonction (H code pour opérateur humain et T pour système technique).

Le dictionnaire des attributs des fonctions est donné de façon synthétique dans le tableau 9.2.

9.2.2.2. Potentiel de variabilité. — L'objet de cette étape consiste à sélectionner la liste des conditions communes de performance CPP.

Id.	Nom	Description	Catégorie
F_1	Demande de protection	Fonction réalisée par un opérateur humain à l'aide du système de communication. Identification de l'aiguille sur le terrain, et demande de protection à l'ATS.	H – T
F_2	Identification de l'aiguille.	Fonction réalisée par l'opérateur ATS, initiée par une communication avec un humain et exécutée à l'aide d'un poste informatisé comprenant une IHM de l'ATS. L'opérateur mémorise l'identifiant de l'aiguille et trouve sa position sur l'IHM	H – T
F_3	Préparation de la CS	Fonction réalisée par l'opérateur ATS, initiée par une communication avec l'opérateur de maintenance et exécutée à l'aide d'un poste informatisé ATS. L'opérateur clique sur la position de l'aiguille identifiée puis sur une demande de blocage de celle-ci, un message de préparation est envoyé au système d'enclenchement.	H – T
F_4	Validation de la préparation	Fonction réalisée par le système d'enclenchement qui reçoit un message de préparation par un réseau de communication informatique. Le système doit générer le message de contrôle CRC et envoyer un message de récépissé à l'IHM ATS	T
F_5	Confirmation de la CS	Fonction exécutée par l'opérateur ATS à l'aide de l'IHM ATS. Initiée par la communication du message de récépissé du système d'enclenchement. Il s'agit d'une demande de validation dans une fenêtre de l'IHM ATS. L'opérateur doit contrôler le récépissé avec l'identifiant de l'aiguille à bloquer.	H –T
F_6	Commande de blocage	Fonction exécutée par le système d'enclenchement. Initiée par une communication de l'humain vers la machine. Le système d'enclenchement doit s'assurer de la validité du message par le contrôle CRC, puis envoyer l'ordre de commande à l'aiguille.	T
F_7	Blocage de l'aiguille	Fonction réalisée par un système technique automatique qui actionne l'aiguille, initiée par la réception d'un message de commande en provenance du système d'enclenchement.	T
F_8	Confirmation de blocage	Fonction réalisée par le système d'enclenchement et initiée par le blocage effectif de l'aiguille. Le système d'enclenchement met à jour l'affichage de l'ATS. La fonction traduit l'information provenant du mécanisme de blocage de l'aiguille sur l'affichage de l'ATS	T
F_9	Autorisation de travaux	Fonction réalisée par l'opérateur ATS, de son initiative personnelle suite à la mise à jour de l'état de l'équipement sur l'IHM à l'emplacement de la position de l'aiguille. L'opérateur communique l'autorisation à l'opérateur de maintenance via le système de communication.	H– T
F_{10}	Travailler sur les voies.	Fonction exécutée par un opérateur humain de sa propre initiative suite à la protection de la zone de travail par le blocage d'une aiguille et sous couvert d'une autorisation communiquée par l'opérateur ATS.	H

TABLE 9.1. Fonctions de la procédure CS de blocage d'une aiguille

	input	*precondition*	*ressource*	*control*	*time*	*output*
F_1			1- Signalétique aiguille 2- Moyen de communication	1- Plan d'exécution des travaux (Barrière immatérielle)		1- Demande de blocage 2- Identifiant de l'aiguille
F_2	1- Identifiant de l'aiguille		1- IHM ATS			1- Position de l'aiguille sur l'IHM 2- Identifiant de l'aiguille
F_3	1- Demande de blocage	1- Position de l'aiguille sur l'IHM	1- IHM ATS			1- Message de préparation de CS (t_0)
F_4	1- Message de préparation de CS			1- Procédurel CS (Barrière fonctionnelle)	1- Minuteur	1- Contrôle CRC 2- Message de récépissé de préparation
F_5	1- Message de récépissé de préparation (t_i)	1- Identifiant de l'aiguille	1- IHM ATS		1- 15'' - $t_i - t_o$	1- Message de confirmation de CS
F_6	1- Message de confirmation de CS			1- Contrôle CRC (Barrière fonctionnelle)		1- Message de commande
F_7	1- Message de commande					1- Aiguille bloquée
F_8	1- Aiguille bloquée					1- Mise à jour affichage état aiguille
F_9		1- Mise à jour affichage état aiguille 2- Position de l'aiguille sur l'IHM ATS		1- Plan d'exécution des travaux (Barrière immatérielle)		1- Autorisation de travaux
F_{10}		1- Aiguille bloquée 2- Autorisation de travaux		1- Plan d'exécution des travaux (Barrière immatérielle)		

TABLE 9.2. Dictionnaire des attributs

9.2.2.2.1. CCP applicables. — Le tableau 8.1 page 180 du chapitre précédent présente la nomenclature des onze conditions de performances proposées par Hollnagel et le tableau 9.3 indique la liste des conditions de performance applicables à chaque fonction du présent cas d'étude.

Fonctions	**CCP**
F_1	$C_1 - C_2 - C_3$
F_2	$C_2 - C_4 - C_7 - C_8$
F_3	$C_2 - C_4 - C_7 - C_8$
F_4	C_3
F_5	$C_2 - C_4 - C_7$
F_6	C_3
F_7	C_6
F_8	C_3
F_9	$C_2 - C_3 - C_7 - C_8$
F_{10}	$C_2 - C_6 - C_{10}$

TABLE 9.3. Conditions de performance applicables à chaque fonction

9.2.2.2.2. Contextualisation des CCP. — Pour chaque fonction, il s'agit de contextualiser les CCP identifiées à l'étape précédente.

À titre d'exemple, la contextualisation détaillée des CCP de la fonction F_1 « Demande de protection » est présentée au paragraphe suivant. La contextualisation de toutes les fonctions est synthétisée dans le tableau 9.4.

9.2.2.2.3. Contextualisation des CCP de F_1. — La fonction F_1 dépend de la CCP C_1 « Disponibilité des ressources », deux ressources ont d'ores et déjà été identifiées dans le dictionnaire des attributs, on introduit donc les deux conditions de performance suivantes :

- C_1^1 : Disponibilité de la signalétique de l'aiguille sur le terrain ;
- C_1^2 : Disponibilité des moyens de communication entre le terrain et le poste ATS.

Cette fonction dépend également de C_2 « Entraînement et expérience » appliqué à l'acteur de la fonction F_1, l'opérateur de maintenance, cela donne la condition de performance C_2^1 « Entraînement et expérience de l'agent de maintenance »

Enfin, la fonction F_1 dépend de la « qualité des communications » C_3, or la communication utilisée pour cette fonction est le moyen de communication entre le terrain et le poste ATS. La condition de performance C_3^1 « Qualité des communication entre le terrain et le poste ATS » est ajoutée à la liste.

9.2.2.2.4. Tableau de synthèse. — Le tableau 9.4 présente les conditions de performance ajoutées dans le but de contextualiser les performances requises pour chaque fonction de l'activité de blocage d'une aiguille pour protection de travaux. La notation utilisée indique en indice le type de CCP auquel appartient la condition de performance et en exposant son numéro

d'identification. Les conditions entre parenthèses indiquent que la condition de performance a déjà été mentionnée et qu'elle est donc partagée avec une autre fonction.

Fonction	CCP	Conditions de performance ajoutées
F_1	C_1	C_1^1 : Disponibilité de la signalétique de l'aiguille
		C_1^2 : Disponibilité du moyen de communication entre le terrain et le poste ATS
	C_2	C_2^1 : Entraînement et expérience de l'agent de maintenance
	C_3	C_3^1 : Qualité de la communication terrain - poste ATS
F_2	C_2	C_2^2 Entraînement et expérience de l'agent ATS
	C_4	C_4^1 : Qualité de l'IHM ATS
	C_7	C_7^1 : Nombres d'objectifs simultanés de l'opérateur ATS
	C_8	C_8^1 : Temps disponible pour la mise en protection
F_3		$(C_2^2 ; C_4^1 ; C_7^1 ; C_8^1)$
F_4	C_3	C_3^2 : Qualité de la communication ATS - Enclenchements
F_5		$(C_2^2; C_4^1; C_7^1)$
F_6		(C_3^2)
F_7	C_6	C_6^1 : Condition de travail du système de blocage de l'aiguille
F_8		(C_3^2)
F_9		$(C_2^2; C_3^1; C_7^1; C_8^1)$
F_{10}		(C_2^1)
	C_6	C_6^2 : Conditions de travail sur le terrain (météo, nuit)
	C_{10}	C_{10}^1 : Qualité de la collaboration de l'équipe de maintenance

TABLE 9.4. Conditions de performance contextualisées

9.2.2.3. Évaluation interdisciplinaire des conditions de performances. — Il s'agit alors d'évaluer pour l'ensemble de l'activité la variabilité des conditions de performance ajoutées par une expertise effectuée en collaboration entre les différents spécialistes de chaque domaine (psychologie, ergonomie, sciences sociales et ingénierie).

Chaque condition de performance est appréciée par trois niveaux de variabilité :

– v_1 : Variabilité faible associée à une condition de performance stable ou variable, mais adaptée à l'exécution de la fonction ;
– v_2 : Variabilité élevée associée à une condition de performance stable ou variable mais inadaptée à l'exécution de la fonction ;
– v_3 : Variabilité très élevée associée à une condition de performance imprévisible.

À titre d'exemple, une grille d'évaluation des conditions de performance pour le cas d'étude est fournie dans le tableau 9.5. On se place dans un cas favorable, pour lequel toutes les conditions de performance sont stables sauf l'urgence de la situation qui se traduit par un nombre d'objectifs

simultanés élevé pour l'agent ATS (condition $C_7^1 = v_3$) et le temps disponible pour l'exécution de la procédure très faible ($C_8^1 = v_3$). Ce contexte est caractéristique d'un scénario d'urgence dans lequel l'agent de maintenance s'aperçoit qu'il n'est pas protégé et demande à l'opérateur ATS d'exécuter la procédure alors que celui-ci est en train d'effectuer d'autres tâches. Cette grille d'évaluation traduit un mode d'exploitation stressé du système, en effet, les barrières fonctionnelles sont disponibles, car les conditions de performance des systèmes techniques ont une variabilité faible, les barrières immatérielles sont elles aussi bien évaluées, la disponibilité des ressources a une faible variabilité de même que l'entraînement et l'expérience des opérateurs. Seul le contexte relatif au nombre de tâches à effectuer et le temps disponible pour exécuter la mise en protection ont une forte variabilité et impliquent une mise en tension du système.

L'étape suivante consiste à visualiser sur le réseau de fonction FRAM l'effet de cette mise en tension du système au travers des interrelations complexes entre les fonctions du système.

Condition de performance	**Valeur**	**Fonctions impactées**
C_1^1 : Disponibilité de la signalétique de l'aiguille	v_1 Faible	F_1
C_1^2 : Disponibilité du moyen de communication entre le terrain et le poste ATS	v_1 Faible	F_1; F_{10}
C_2^1 : Entraînement et expérience de l'agent de maintenance	v_1 Faible	F_1; F_{10}
C_2^2 : Entraînement et expérience de l'agent ATS	v_1 Faible	F_2; F_3; F_5; F_9
C_3^1 : Qualité de la communication terrain - poste ATS	v_1 Faible	F_1; F_9
C_3^2 : Qualité de la communication ATS - Enclenchements	v_1 Faible	F_4; F_6; F_8
C_4^1 : Qualité de l'IHM ATS	v_1 Faible	F_2; F_3; F_5
C_6^1 : Condition de travail du système de blocage de l'aiguille	v_1 Faible	F_7
C_6^2 : Condition de travail sur le terrain (météo, nuit)	v_1 Faible	F_{10}
C_7^1 : Nombre d'objectifs simultanés de l'opérateur ATS	$\mathbf{v_3}$ Très élevé	F_2; F_3; F_5; F_9
C_8^1 : Temps disponible pour la mise en protection	$\mathbf{v_3}$ Très élevé	F_2; F_3; F_9
C_{10}^1 : Qualité de la collaboration de l'équipe de maintenance	v_1 Faible	F_{10}

TABLE 9.5. Exemple de grille d'évaluation des conditions de performance

9.2.2.4. Dépendance fonctionnelle. — La mise en relation des attributs identifiés dans le dictionnaire des attributs permet de tracer le diagramme FRAM présenté sur la figure 9.7. Ce réseau de dépendance fonctionnelle présente l'activité de protection d'une équipe de travaux par une CS de blocage d'une aiguille dans le mode normal d'exploitation.

La procédure est initiée par l'opérateur de maintenance qui réalise une demande de protection de sa zone de travaux. Deux informations découlent de cette activité, une demande de blocage et l'identifiant de l'aiguille à bloquer. Ces deux informations sont envoyées à l'opérateur ATS. Sur le schéma, cela se traduit par deux relations de dépendance fonctionnelle entre l'activité de l'opérateur de maintenance et l'activité de l'opérateur ATS qui consiste à identifier l'aiguille sur l'interface de l'ATS d'une part et l'activité de l'opérateur ATS qui consiste à préparer la CS de protection demandée d'autre part.

Cette représentation du mode d'exploitation normal de l'activité fournit des informations importantes sur l'activité. On peut remarquer le nombre important de redondances informationnelles traduisant de nombreuses possibilités de vérifier la véracité des flux d'informations échangés dans cette activité.

La procédure requiert en grande partie l'action d'opérateurs humains. Sur cette base il est possible de visualiser un grand nombre de scénarios en appliquant différentes grilles d'évaluation des conditions de performance identifiées à l'étape précédente.

9.2.2.5. Résonance fonctionnelle et instanciation du modèle. — Considérons la mise en tension identifiée par la grille d'évaluation présentée précédemment dans le tableau 9.4. L'application de ce contexte sur le réseau de fonction FRAM de la figure 9.7 ainsi que l'application de la résonance fonctionnelle implique les modifications présentées sur le réseau FRAM de la figure 9.8. Cette figure présente l'activité de protection d'une équipe de travaux par CS de blocage d'une aiguille dans un mode d'exploitation stressé.

Le niveau très élevé des conditions de performance C_7^1 et C_8^1 se traduit sur le diagramme par une pression temporelle sur les fonctions exécutées par l'opérateur ATS. Sur le diagramme cette pression temporelle est symbolisée par le signe (») [(1)] sur les attributs *time* des fonctions F_2, F_3, F_5 et F_9. Pour la fonction F_2, cette pression temporelle implique une forte variabilité d'exécution de l'identification de la position de l'aiguille sur l'IHM de l'ATS et donc d'une mauvaise utilisation des ressources. Ce faisant, l'opérateur, dans l'urgence peut être amené à confondre la position de l'aiguille. La fonction F_3 dépend de la fonction F_2 par l'attribut *precondition*. Le nombre d'objectifs simultanés et le manque de temps peut impliquer la non-vérification de la position de l'aiguille sur l'IHM et ainsi préparer la CS sur une autre aiguille que celle permettant de protéger les travaux. La croix sur les attributs indique le caractère erroné du flux d'information. Les flèches en pointillés illustrent l'effet de la pression temporelle sur l'utilisation des ressources ou la vérification des préconditions.

La fonction F_5 est une vérification redondante des informations de la CS préparée. Or l'identification de l'aiguille sur l'IHM est erronée. Le manque de temps est amplifié par la connaissance du minuteur qui contraint davantage le travail de l'opérateur (mal nécessaire permettant d'éviter les CS intempestives). En conséquence, la résonance fonctionnelle implique la non-vérification du numéro de l'aiguille sur la fenêtre de confirmation. Cette étape aurait pu

1. Notation utilisée par Hollnagel dans [**68**].

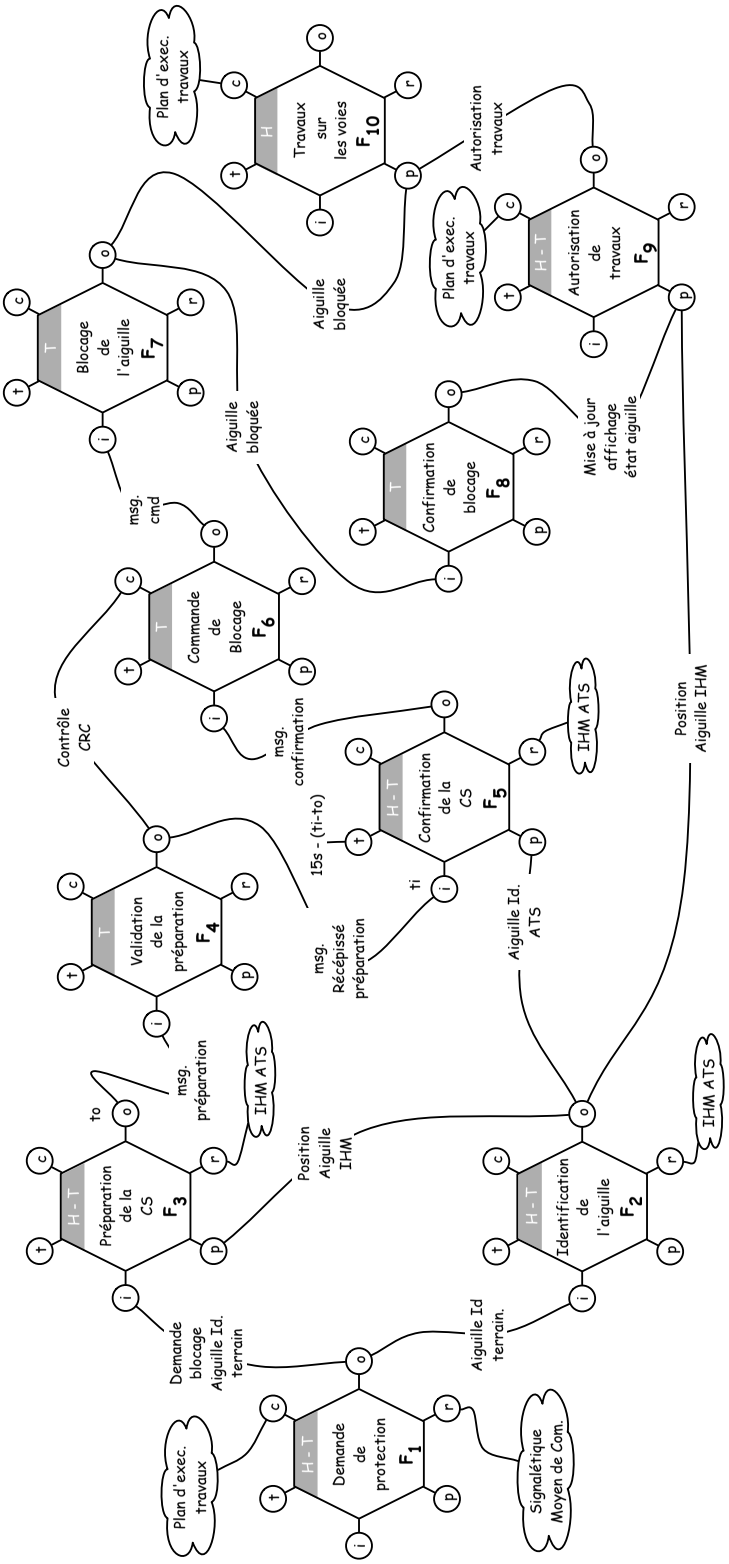


FIGURE 9.7. Réseau FRAM : Activité en mode d'exploitation normal

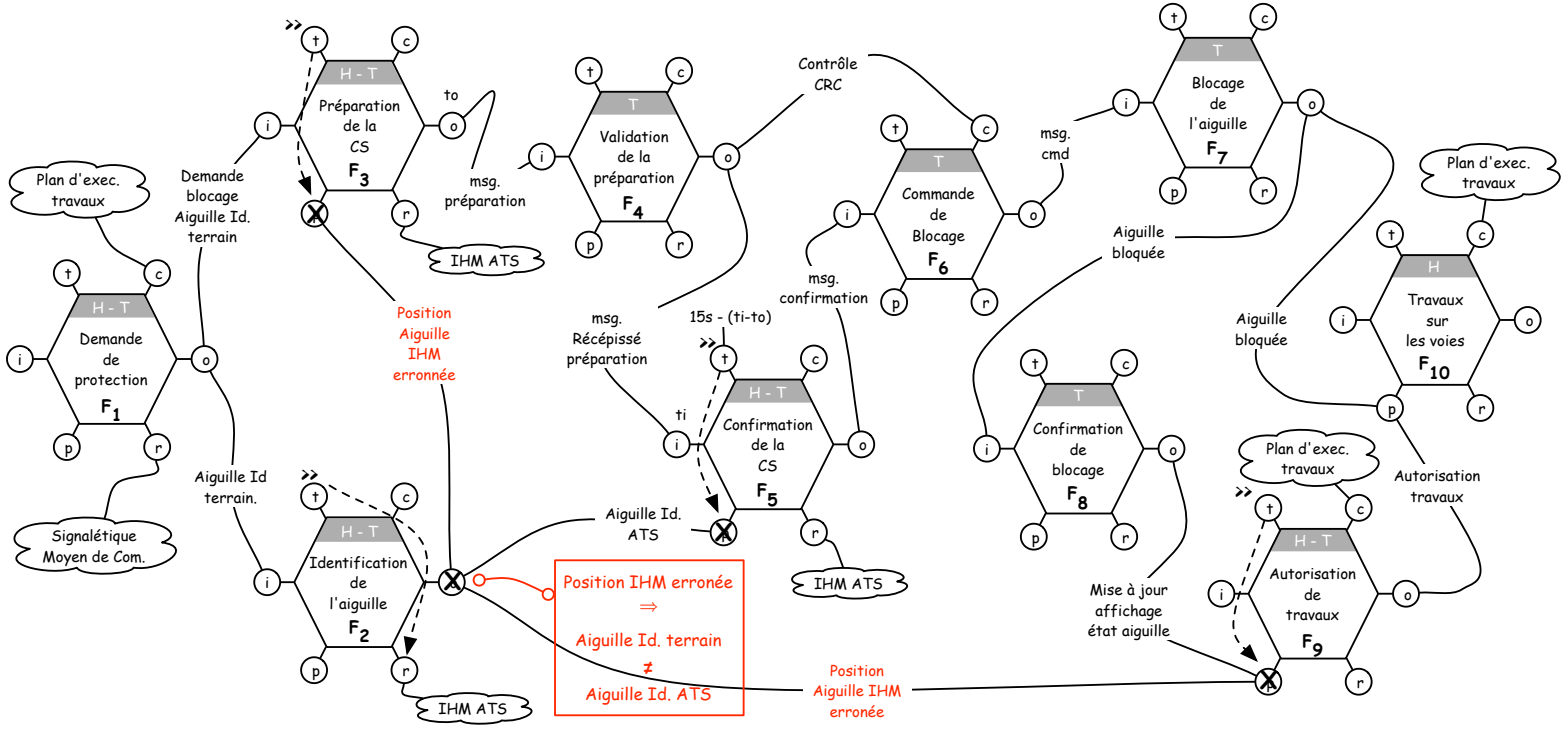


FIGURE 9.8. Réseau FRAM : Activité en mode d'exploitation stressé

être l'occasion de détecter l'erreur commise précédemment et d'effectuer une action résiliente visant à redemander le numéro de l'aiguille à l'agent de maintenance. Mais la situation d'urgence, en application du modèle du compromis cognitif d'Amalberti ou bien du modèle ETTO, agit de sorte à court-circuiter cette vérification. Les règles ETTO applicables dans ce cas sont « Pas le temps ni les ressources nécessaire » et « Pas de souci, c'est parfaitement sécurisé ». Pour cette dernière règle, l'homéostasie du risque peut être provoquée par la confiance que fournit la sécurisation du protocole de communication de la CS.

Enfin, le même phénomène s'applique à la fonction F_9 où l'opérateur ATS détecte le blocage d'une aiguille, mais ne s'assure pas que c'est bien celle qui va protéger les équipes de travaux par la vérification de l'attribut *precondition* et autorise l'agent de maintenance à travailler sur les voies non protégées.

9.2.3. Conclusion du cas d'étude. — Cet exemple a permis d'identifier un scénario accidentel complexe impliquant plusieurs événements qui n'ont pas été identifiés dans les arbres de défaillance de l'étude de sûreté de fonctionnement. Une erreur de positionnement d'un élément graphique sur l'IHM et deux absences de vérifications ont été expliqués par le contexte d'urgence de l'activité et conduisent à la non-protection de l'équipe de maintenance sur les voies. Ce cas d'étude a été présenté dans [**19**].

Le type de supervision critique « action directe sur les barrières de sécurité » qui vient d'être étudié est une activité procédurale fortement guidée. Ainsi, les fonctions et les flux d'informations échangés sont définis par la procédure CS et facilement identifiables par une analyse de la procédure. Le cas d'étude suivant est un type de supervision critique qui intervient lorsque l'opérateur a la possibilité de récupérer une situation dangereuse. Il n'existe pas de procédure pour cette activité. L'analyse de la tâche est donc nécessaire, à cette fin, le cas d'étude suivant utilise l'état de l'art industriel et les expérimentations qui ont été menées sur la plateforme SPICA-RAIL.

9.3. Détection d'incidents

La détection d'incidents a été étudiée lors de la deuxième phase de la démarche de la thèse au chapitre 7. L'application de la méthode FRAM est présentée de façon moins détaillée que le cas d'étude précédent. L'accent est mis sur l'utilisation des résultats des expériences menées en collaboration avec les spécialistes de la psychologie cognitive pour l'élaboration du modèle.

9.3.1. Modélisation. — Le cas d'étude reprend l'activité des opérateurs de supervision de trafic ferroviaire qui a été expérimentée sur la plateforme SPICA-RAIL à savoir la surveillance du TCO et la détection d'incident. Cette activité précède et conditionne la mise en place de mesures correctives suite à un incident. Le modèle élaboré est synthétisé sur la figure 9.9.

Six fonctions ont été identifiées. La première fonction a été identifiée grâce à l'expérimentation sur SPICA-RAIL. En effet, les résultats des expériences suggèrent que la stratégie de surveillance du TCO influe sur le temps de détection des anomalies. Le choix de cette stratégie constitue la première fonction du modèle. Elle dépend uniquement de la condition de performance relative à l'entraînement et l'expérience de l'opérateur. Dans le cas où cette condition de performance

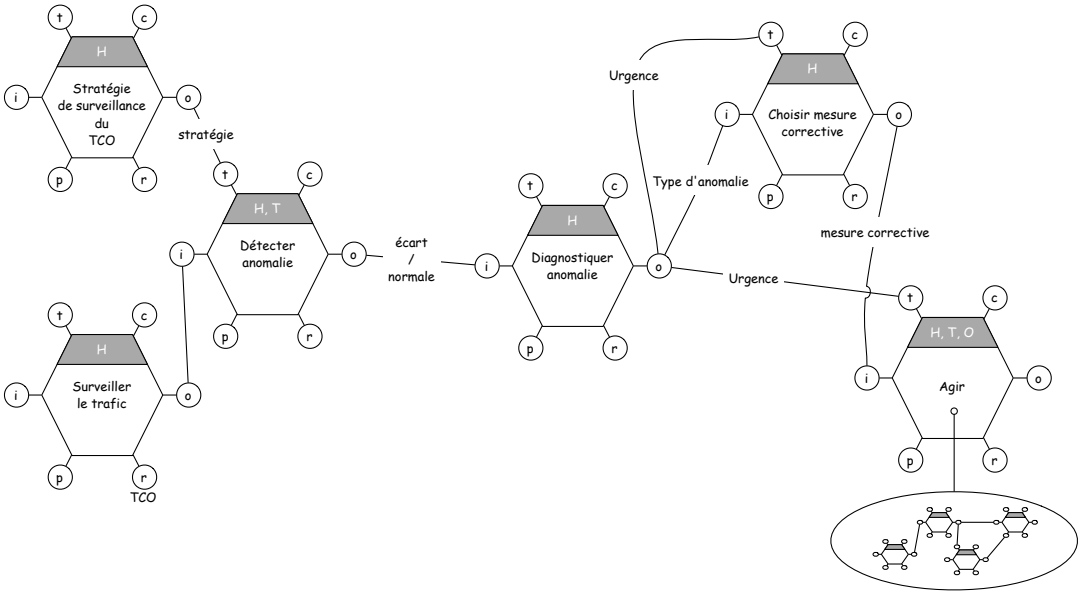


FIGURE 9.9. Modèle de l'activité de surveillance du trafic

est évaluée adaptée et donc dans le cas d'un opérateur expérimenté, on peut considérer que la stratégie choisie a une faible variabilité de performance. Dans le cas où cette condition de performance est jugée stable ou variable, mais inadaptée, ceci se traduit pour notre exemple par un opérateur novice qui a suivi une formation initiale, mais qui ne dispose pas d'expérience. En conséquence, nous considérerons que la variabilité de performance de la stratégie choisie est élevée. Enfin, un opérateur inexpérimenté (la condition de performance est jugée « imprévisible ») produit des heuristiques de surveillance aléatoires, de fait, la variabilité de performance de la stratégie choisie est très élevée.

La deuxième fonction consiste à surveiller le trafic, elle est exécutée par le couple opérateur humain - système ATS. Cette fonction utilise comme ressource le TCO et l'IHM du poste de supervision. Les conditions de performance de cette fonction sont : la qualité des communications entre le terrain et l'ATS, la qualité de l'IHM et le nombre d'objectifs simultanés suivis par l'opérateur humain. La qualité des communications est jugée à partir de l'étude de sûreté de fonctionnement, et notamment par la disponibilité et la fiabilité du système de communication entre le terrain et l'ATS, nous considérons pour cet exemple que celui-ci a été développé avec un haut niveau de fiabilité et de disponibilité. La qualité de l'IHM peut être appréciée grâce aux expériences menées sur la plateforme SPICA-RAIL. L'expérimentation sur SPICA-RAIL montre que les taux de fausses alarmes et de non-détection sont faibles, ceci nous amène à juger la qualité de l'IHM adaptée à la tâche de surveillance et de détection, en conséquence la fonction de surveillance du trafic n'est vraisemblablement pas soumise à la variabilité de performance de l'IHM. Par contre, le nombre d'objectifs simultanés suivis par l'opérateur n'a pas été testé lors des expériences. Si ce nombre est adapté à l'activité, l'opérateur dispose du temps nécessaire pour suivre l'évolution du trafic et donc la variabilité de performance du produit de la fonction de surveillance reste stable et peu élevée. Par contre, si le nombre d'objectifs suivis par l'opérateur humain est trop élevé, ce dernier peut être amené à ne pas suivre l'évolution du trafic et donc la variabilité de performance de la fonction est très élevée.

La troisième fonction est relative à l'activité de détection d'une anomalie. Elle est assurée par le couple opérateur humain – système ATS. Le temps de détection dépend de la stratégie de détection qui a été choisie par l'opérateur. Il s'agit pour l'opérateur de détecter un écart par rapport à la situation normale. Cette fonction dépend des conditions de performance relatives à l'entraînement et l'expérience des opérateurs, de la qualité de l'IHM et de la qualité des communications entre le terrain et l'ATS. Ces deux dernières ont été traitées dans la deuxième fonction. Les expériences ont montré que dans un environnement favorable et pour des sujets novices formés, ceux-ci avaient une variabilité de réponse assez élevée. En conséquence, si l'entraînement et l'expérience sont jugés inadaptés (opérateur novice manquant d'expérience) la variabilité de performance de la détection d'un écart par rapport à la normale est élevée. Nous considérons que cette variabilité se stabilise lorsque l'entraînement et l'expérience sont jugés adaptés (opérateur expérimenté), cette hypothèse doit être confirmée par l'expérience. La variabilité de performance sera très élevée lorsque l'opérateur n'a pas été formé à ce métier. Les expériences ont également émis l'hypothèse que la tâche de détection dépendait de la stratégie de surveillance du TCO (variabilité inter sujets) et qu'elle influait sur le temps de détection. Nous supposons que si la variabilité de performance de la stratégie utilisée par l'opérateur est faible, alors le temps de détection est faible. Inversement, plus la variabilité de performance de la stratégie utilisée est élevée, plus le temps de détection sera long.

La quatrième fonction identifiée représente la tâche de diagnostic. L'opérateur ayant détecté un écart de fonctionnement, il doit alors déterminer la nature du dysfonctionnement. Deux éléments sont produits par cette fonction. Le résultat du diagnostic révèle le type d'anomalie et l'urgence avec laquelle la situation doit être traitée. Cette fonction dépend des deux conditions de performance : « entraînement et expérience » ainsi que « temps disponible ». La variabilité de performance de la fonction est d'autant plus faible que ces deux conditions de performance sont adaptées.

La cinquième fonction consiste pour l'opérateur à choisir la mesure corrective adaptée. Elle dépend du type d'anomalie et est contrainte dans le temps par l'urgence de la situation. De la même façon que la fonction précédente, le choix de la mesure corrective dépend des deux conditions de performance : « entraînement et expérience » et « temps disponible ». Cette dernière condition dépend du résultat du diagnostic, en effet le diagnostic permet d'établir le niveau d'urgence de la situation et induit nécessairement une contrainte temporelle sur la tâche du choix de la mesure corrective. Une forte variabilité dans les résultats du diagnostic peut provoquer une erreur de diagnostic et/ou une erreur d'appréciation du niveau d'urgence de la situation. En conséquence, une forte variabilité de performance au niveau de la tâche de diagnostic implique nécessairement une variabilité de performance imprévisible au niveau du choix de la mesure corrective. Le cas où la variabilité de performance du diagnostic est faible n'est pas non plus sans conséquence sur cette fonction. Un diagnostic correct peut conduire à un type d'anomalie nécessitant un traitement d'urgence, dans ce cas le choix de la mesure corrective est contraint par la pression temporelle relative à l'urgence de la situation.

La sixième fonction, nommée « agir » consiste à mette en œuvre les mesures correctives. Cette fonction est initiée par l'opérateur de supervision de trafic, puis exécutée par un système technique (dans le cas d'une commande) ou bien par une organisation (dans le cas d'intervention d'une équipe de maintenance). Cette fonction peut se décliner en plusieurs sous fonctions et donc constituer un autre modèle FRAM.

9.3.2. Instanciation du modèle. — Une instance possible, parmi de nombreuses autres, consiste à supposer que l'opérateur est novice, qu'il n'effectue que la tâche de surveillance (nombre d'objectifs simultanés compatible) et qu'un incident de type « raté de fermeture » apparaît sur la ligne ferroviaire. L'instance du modèle est présentée sur la figure 9.10.

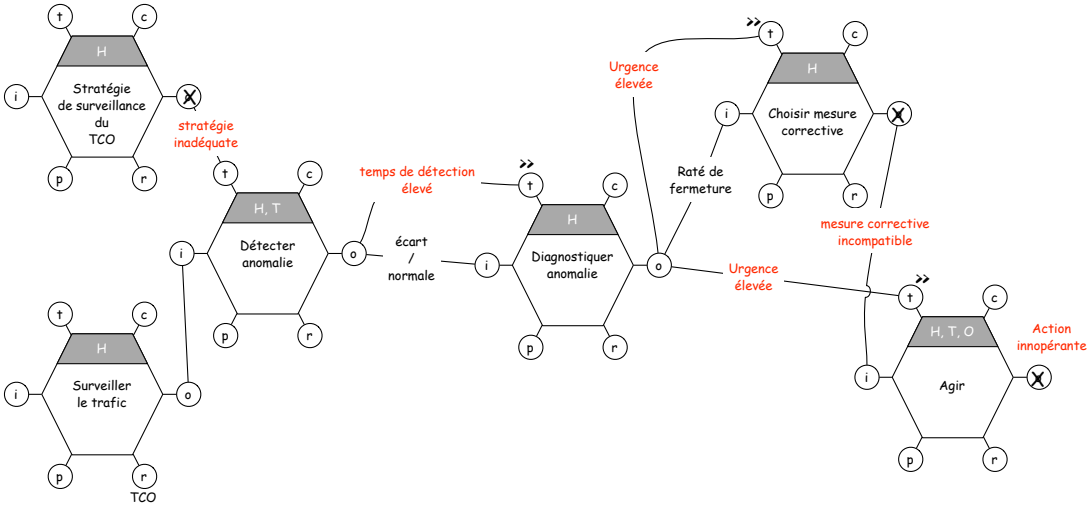


FIGURE 9.10. Instance du modèle

Le manque d'expérience de l'opérateur le conduit à utiliser une stratégie de surveillance inadaptée, une croix sur l'attribut *output* de la fonction symbolise cette forte variabilité de performance. En conséquence, lorsque l'anomalie apparaît sur l'IHM l'opérateur ATS la détecte tardivement. De fait, il ne lui reste que peu de temps pour accomplir le diagnostic, choisir la mesure corrective et agir. La pression temporelle est symbolisée sur le modèle par la mention (») sur l'attribut *time* de la fonction. L'écart par rapport à la normale est suffisamment explicite pour diagnostiquer un raté de fermeture et inférer un niveau d'urgence de la situation très élevé. Le choix de la mesure corrective contraint par le temps précipite la décision de l'opérateur (novice) et le conduit à faire un mauvais choix qui l'amène à exécuter une mesure incompatible avec la situation « raté de fermeture » et donc inopérante. La conséquence immédiate d'une telle instanciation est un accident par collision de deux trains lorsque le raté de fermeture intervient en présence de mobiles à l'abord du signal défaillant.

9.3.3. Conclusion du cas d'étude. — Ce deuxième exemple appliqué à un cas de supervision critique mal représenté dans les études de sûreté de fonctionnement puisque l'ATS n'est pas considéré comme une barrière de sécurité permet d'élaborer de nouveaux scénarios accidentels par instanciations successives du modèle FRAM. Les relations causales offertes dans le formalisme FRAM permettent d'intégrer les travaux de diverses spécialités qui ont pour objet d'étude les systèmes sociotechniques complexes dans un objectif commun d'évaluer les risques et la sécurité. Cet exemple a fait l'objet d'illustration de notre démarche dans [**24**].

9.4. Discussion

D'autres scénarios peuvent être décrits sur un même modèle. Ce modèle est un de support commun entre les spécialistes de la sûreté de fonctionnement et les chercheurs en sciences humaines et sociales spécialistes de la psychologie cognitive. D'une part, le modèle FRAM permet aux expérimentateurs de formuler des hypothèses sur les conditions de performance des opérateurs et leurs répercussions sur la sécurité et, d'autre part, de synthétiser leurs résultats dans un scénario utilisable par les études de sûreté de fonctionnement classique.

La technique FRAM permet d'analyser de manière plus approfondie les événements de l'arbre de défaillances. L'exemple qui a été présenté a permis d'approfondir l'étude des causes humaines de la porte « Mauvaise aiguille bloquée » de l'arbre de défaillances (figure 3.2). Le deuxième cas d'étude n'est pas traité dans les arbres de défaillances développés par ALSTOM pour l'étude de sécurité des systèmes ATS. Pourtant, la récupération d'une situation potentiellement accidentelle représente une activité majeure de l'opérateur ATS. Le modèle élaboré sur cet exemple permet trivialement de construire un arbre de défaillance dont les événements de base sont les fonctions du modèle FRAM. Toutefois, cette restriction est trop réductrice. En effet, les événements de base de l'arbre de défaillances n'ont que deux modalités possibles (espace d'état binaire) alors qu'une fonction dans FRAM dispose d'un espace d'état aussi large que l'analyste le veut. Pour lever cette restriction, l'utilisation d'arbres de défaillances multimodaux (où les événements de base dispose d'un espace d'état multimodal) présenté brièvement au chapitre 3 [**92**] est une perspective à explorer.

La méthode FRAM reste toutefois limitée à une approche qualitative de la sécurité. C'est pourquoi, elle demeure une approche complémentaire de l'étude de sécurité classique par arbres de défaillances ou d'événements. L'apport de cette méthode permet d'identifier de nouveaux événements de base pour les arbres de défaillances et d'événements à partir de l'instanciation du modèle FRAM. Subsiste cependant, l'épineux problème de leur quantification. De nouvelles expériences sont nécessaires pour pallier ce manque, l'objectif de quantifier ces événements nécessite de nombreuses passations sur le scénario identifié dans l'instance du modèle FRAM afin d'obtenir un échantillon inter-sujet suffisamment représentatif pour obtenir des statistiques paramétriques fiables.

Un outil nommé FRAMVISUALIZER a été développé par l'université de Linköpings (Suède) et est disponible à l'adresse *web* `http://code.google.com/p/framvisualizer/`. Cet outil permet de guider l'utilisateur dans l'élaboration du modèle FRAM. Pour chaque fonction, l'utilisateur dispose de tables permettant de définir les attributs et les CCP. L'outil génère automatiquement le schéma du modèle. L'outil est en version de développement et est limité à la seule visualisation du réseau de dépendance fonctionnelle. Il ne permet pas de visualiser les instanciations du modèle. La difficulté à surmonter pour permettre de visualiser les instanciations du modèle consiste à informatiser les raisonnements causaux de chaque fonction.

Enfin, l'étude de sécurité ferroviaire doit être soumise à une phase de certification qui évalue la démonstration de sécurité. L'apport de FRAM dans cette perspective réside dans la dernière étape de la méthode (non traitée dans la thèse) qui consiste à proposer des mesures préventives de la variabilité de performance. Ces mesures doivent être soumises au jugement du certificateur qui en évaluera l'efficacité.

Dans le chapitre suivant, les perspectives relatives à la démarche proposée dans la thèse sont présentées. La question de la quantification du modèle FRAM est discutée et un modèle probabiliste du formalisme FRAM est proposé.

Troisième PARTIE

PERSPECTIVES ET CONCLUSIONS

CHAPITRE 10

PERSPECTIVES

10.1. Introduction

L'étude d'impact de l'automatisation de la tâche de supervision sur la sécurité du transport ferroviaire est une activité en constante évolution. En effet, l'automatisation de la supervision est rendue possible grâce à l'intégration des nouvelles technologies de l'information dont la vitesse d'évolution technologique est grande. Les expériences qui ont été présentées dans le chapitre 7 contribuent à l'étude des effets de la modification de la tâche du contrôleur de trafic ferroviaire sur la sécurité. Il s'agissait d'évaluer la relation duale entre la performance d'opérateurs novices (apparentés à des agents en formation) à détecter un ensemble d'anomalies sur les IHM de supervision et l'efficacité de ces IHM à permettre une telle détection. La première partie de ce chapitre présente les futures pistes qui devraient être explorées à l'aide de l'environnement simulé constitué par la plateforme SPICA-RAIL. L'élaboration de nouvelles expériences passe par l'étude interdisciplinaire de l'évaluation de la sécurité. Les résultats apportés par la méthode FRAM fournissent des hypothèses qui doivent être confrontées à l'observation.

L'absence de quantification prévisionnelle de la sécurité est la principale limitation de la démarche interdisciplinaire qui a été élaborée, aussi ce chapitre propose une perspective de recherche afin d'intégrer cette quantification. L'idée repose sur l'ajout d'un modèle probabiliste à la méthode FRAM.

10.2. Expérimentations

Les résultats qui sont pour l'instant limités au niveau de la représentativité statistique montrent que d'autres expériences sont nécessaires pour obtenir des résultats quantitatifs à partir de statistiques paramétriques. Les résultats des expériences qui ont été menées sur SPICA-RAIL sont de deux ordres :

– La variabilité inter-sujets semble importante, il est donc nécessaire d'approfondir cette étude de manière quantitative afin de déterminer si cette variabilité correspond à une variabilité « normale » (naturelle) entre les sujets ;
– Dans le cas contraire, la stratégie exploratoire des IHM de supervision du trafic pourrait être une raison de cette forte variabilité. Un protocole expérimental spécifique doit être mis en place pour vérifier cette hypothèse.

10.2.1. Variabilité inter-sujets. — Une telle étude requiert de nombreux volontaires, en effet les tests de normalité convergent de la même façon que la loi des grands nombres, c'est-à-dire que l'on pourrait établir une répartition représentative des sujets à partir d'un échantillon de trente individus. Si la répartition de ces observations revêtait la forme d'une courbe Gaussienne (concentration des observations autour de la moyenne), il serait possible de conclure à une variabilité inter-sujets liée à l'aléa. Dans le cas contraire, plusieurs cas se présentent.

La principale difficulté d'une telle entreprise relève de la taille du plan d'expérience. Le plan d'expérience à mesures complètement répétées a nécessité une dizaine d'heures de passation pour chaque sujet. Évaluer trente sujets sur ce même plan d'expérience revient à enregistrer 300 heures d'information vidéo soit 37 jours ouvrés à temps plein.

10.2.2. Stratégie exploratoire des IHM. — Une étude spécifique de la stratégie exploratoire des IHM par les opérateurs humains nécessite la mise en place d'un protocole expérimental spécifique. Les expériences qui ont été menées par le LAMIH [**43**] sur le projet ASTREE de la SNCF utilise un dispositif appelé oculomètre permettant d'enregistrer la position du regard du sujet sur un écran. Ce système est couramment employé dans les études expérimentales d'Interaction Hommain–Machine [**42, 43**] et notamment pour identifier la stratégie adoptée par le sujet durant sa tâche. Il permet d'identifier les zones d'intérêt de l'IHM et les séquences successives d'observations que réalise le sujet de l'expérience [**43**].

10.2.3. Diagnostic et action de l'opérateur. — Le modèle FRAM appliqué à la détection au diagnostic et à la récupération d'incidents doit être continué. En effet, seule la première fonction a été évaluée sur simulateur, la tâche de diagnostic et l'action de l'opérateur sont les deux prochaines séries d'expériences qui doivent être menées.

10.3. Quantification d'un modèle FRAM

Une des limitations de notre démarche d'évaluation interdisciplinaire de la sécurité demeure l'évaluation quantitative de la sécurité. Ce paragraphe propose deux perspectives de travail pour réaliser des évaluations quantitatives dans la méthode FRAM. La première perspective décrit une modélisation déterministe et a pour objectif de traduire le modèle FRAM par un réseau de neurones artificiel afin d'évaluer le niveau de performance des fonctions. La deuxième perspective est probabiliste, l'objectif est de calculer la probabilité de franchissement d'un seuil critique de performance d'une fonction.

10.3.1. Vers un réseau de neurones artificiel. — L'objet d'étude de la méthode FRAM est la variabilité de performance. La méthode FRAM repose sur l'hypothèse que la variabilité de performance des fonctions est un signal non linéaire. Supposons maintenant l'existence d'un mode de fonctionnement du système parfait (que nous avons nommé mode d'exploitation nominal dans le modèle présenté au chapitre 6) où le niveau de performance est uniformément stable. À un instant t fixé, il est possible de définir le niveau de performance d'une fonction F_i noté x_t^i avec $\forall\, i \in I, x_t^i \in [0,1]$ où I représente l'ensemble des indices des fonctions.

Ce niveau de performance dépend des contraintes exercées par les différents CCP de la fonction et les niveaux de performance des fonctions connectées aux entrées *input, control, time,*

precondition et *ressource* de la fonction considérée. On modélise le niveau de contrainte exercées par les CCP à l'instant t par un seul nombre noté $c_t \in [0,1]$ et on note $\mathbf{x}_t^{\mathcal{E}_i}$ le vecteur constitué des niveaux de performance des fonctions en entrée de la fonction F_i avec $\mathcal{E}_i = \{k \in I, F_k \to F_i\}$.

Un modèle de dépendance possible est présenté dans l'équation 18 :

$$x_t^i = \varphi\left(c_t; \mathbf{x}_t^{\mathcal{E}_i}\right) \tag{18}$$

Où φ est une fonction complexe qui sert à modéliser le raisonnement causal de la fonction.

Cette équation présente des similitudes avec la fonction de transfert d'un neurone dans un réseau de neurones artificiel. Les réseaux de neurones constituent un champ disciplinaire très largement étudié, de nombreux ouvrages existent dans ce domaine, voir par exemple [**61**] pour une présentation de cette technique.

Le modèle mathématique d'un neurone artificiel est illustré à la figure 10.1. Un neurone est constitué d'un intégrateur qui effectue la moyenne pondérée de ses entrées. Le résultat n_i de cette somme est ensuite transformé par une fonction de transfert qui produit la sortie x_t^i du neurone.

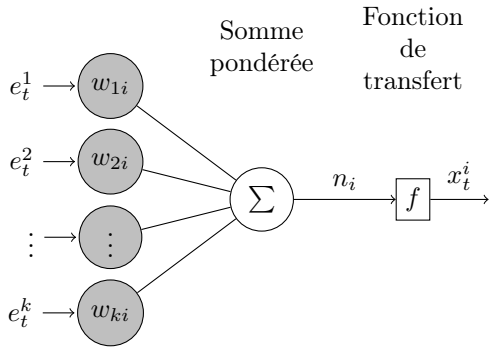


FIGURE 10.1. Modèle mathématique d'un neurone artificiel

La sortie n_i de l'intégrateur du neurone i est donnée par l'équation 19 :

$$n_i = \sum_{j=1}^{k} w_{ji} e_t^j \tag{19}$$

La valeur de sortie du neurone i est donnée par l'équation 20.

$$x_t^i = f(n_i) = f(\sum_{j=1}^{k} w_{ji} e_t^j) \tag{20}$$

La fonction de transfert f est généralement non linéaire, la fonction seuil est la plus couramment employée, d'autres fonctions peuvent être utilisées du type sigmoïde, tangente hyperbolique *etc.*

Le réseau de neurones artificiel est construit en appliquant la sortie d'un neurone à l'une des entrées d'un autre neurone.

Revenons à l'équation 18, il est possible d'appliquer la technique des réseaux de neurones artificiels au réseau FRAM en posant $\varphi = f\left(\sum\right)$.

Dans cette perspective une fonction dans FRAM, F_i sera modélisée par un neurone dont les entrées sont ses attributs et les CCP. Chaque CCP doit faire l'objet d'une évaluation quantitative par l'expertise et représente une entrée du réseau de neurones global. Pour chaque fonction, il est nécessaire d'identifier les poids w_{ij} à affecter aux attributs et aux CCP. Enfin, une fonction de transfert f_i associée à une fonction FRAM doit être modélisée.

Afin de préserver la cohérence de notre modèle, il est nécessaire d'imposer les deux conditions suivantes :

$$f : [0,1] \to [0,1] \tag{21}$$

et,

$$\sum_{j=1}^{k} w_{ij} = 1 \tag{22}$$

L'utilisation de réseau de neurones artificiel pour modéliser le niveau de performance des fonctions dans FRAM implique nécessairement que le temps soit discret et que les changements de niveau de performance des fonctions soient synchronisés.

10.3.2. Modèle probabiliste. — Un espace de probabilité doit être associé à chaque fonction.

Soit X_i, le niveau de performance associé à la fonction F_i mesuré dans l'intervalle $[0,1]$. $X_i = 0$ indique une performance nulle, les objectifs de la fonctions ne peuvent être remplies. $X_i = 1$ représente l'exécution optimale de la fonction, dans le modèle des modes d'exploitation ce niveau de performance correspond au mode nominal.

On se donne alors le modèle probabiliste suivant :

$$X_i : \Omega \to [0,1] \tag{23}$$

avec Ω représentant l'univers des possibles (les différentes exécutions possibles de la fonction) et X_i et une variable aléatoire réelle positive et bornée entre 0 et 1. On suppose l'existence d'une densité g_i pour chaque X_i, on a alors :

$$\forall i \in I, \int_0^1 g_i(x)dx = 1$$

Comme $\forall i, X_i(\omega) \in [0,1]$ (*i.e* les variables aléatoires sont bornées), l'espérance et la variance de ces variables aléatoires existent. On note respectivement $\mathbb{E}(X_i)$ et $\mathbb{V}(X_i)$ l'espérance et la variance de la variable aléatoire X_i, voir équations 24 et 25.

$$\mathbb{E}(X_i) = \int_0^1 x g_i(x) dx \tag{24}$$

$$\mathbb{V}(X_i) = \mathbb{E}\left(X_i^2\right) - \mathbb{E}(X_i)^2 \tag{25}$$

La variance est une mesure de l'incertitude de l'expérience aléatoire, elle détermine la dispersion des valeurs de la variable aléatoire. Appliquée au niveau de performance, la variance de X_i permet de modéliser la variabilité de performance de la fonction F_i. Ce n'est plus la variabilité de performance dans le temps, mais l'incertitude liée au niveau de performance à l'instant t qui est modélisé.

Il s'agit alors d'appliquer ce modèle au réseau de neurones développé précédemment. Les entrées du neurone artificiel sont notées E_i, ce sont les variables aléatoires représentant le niveau de performance des fonctions en entrée de F_i (cet ensemble est noté $F_{\mathcal{E}_i}$) et celles modélisant le niveau d'adéquation des CCP.

Ainsi, la variable aléatoire de sortie de notre modèle est donnée par l'équation 26 :

$$X_i = f(\sum_{j=1}^{k} w_{ji} E_j) \tag{26}$$

L'initialisation du réseau de neurones artificiel traduit du réseau de dépendance fonctionnelle de FRAM est effectuée par le tirage des variables aléatoires représentant les CCP.

Bien entendu, les variables X_i ne sont pas indépendantes. Il s'agit alors de calculer la variance de la variable de sortie du neurone artificiel. La méthode analytique consiste à calculer $\mathbb{V}\left[f\left(\sum_{j=1}^{k} w_{ji} E_j\right)\right]$ avec les E_i non indépendants. Cette méthode nécessite de calculer les covariances de tous les couples possibles des E_i.

Une autre méthode consiste à effectuer des simulations de Monte-Carlo. Il s'agit de programmer informatiquement le réseau et de calculer de proche en proche, N fois, la valeur de probabilité du niveau de performance de chaque fonction. La variance peut alors être approchée statistiquement à partir de la variance des échantillons issues des N simulations.

La modélisation de la variabilité de performance d'une fonction FRAM F_i **dans le temps** revient à étudier la variance du processus stochastique formé par la suite de variables $X_i(t)$ où t représente le temps.

10.4. Conclusion

Les perspectives de ce travail sont de deux ordres, premièrement il est nécessaire d'approfondir l'étude des situations de supervision critique par l'expérimentation et d'intégrer les résultats dans le modèle FRAM. Enfin, dans le but de proposer une évaluation quantifiée des risques, nous avons proposé une perspective de modélisation basée sur les réseaux de neurones artificiels.

CHAPITRE 11

CONCLUSION

L'objectif de ce travail était d'évaluer l'impact des postes centraux de supervision de trafic ferroviaire sur la sécurité dans une perspective interdisciplinaire.

Le premier chapitre a présenté le système ferroviaire et ses principes de sécurité. Il a notamment été constaté que l'évolution des systèmes de contrôle du trafic ferroviaire vit une mutation sans précédent. L'automatisation de la tâche de supervision de trafic ferroviaire est révélatrice de ce constat, en effet, la forte culture de sécurité des acteurs humains du trafic, avec laquelle le transport ferroviaire s'est développé, se reporte aujourd'hui vers le développement de systèmes ayant atteint un très haut niveau de sécurité, reléguant le rôle de l'opérateur humain pour la sécurité au second plan. Au travers de cette thèse, une réflexion sur la prise en compte des facteurs humains dans les études de sécurité a été fournie.

Le contexte méthodologique des études de sécurité ferroviaire est fondé sur les techniques de sûreté de fonctionnement. Ce champ disciplinaire doit faire face à la complexité croissante des systèmes sociotechniques. L'approche réductionniste ne suffit plus à modéliser les systèmes sociotechniques complexes. La démarche d'évaluation de la sécurité s'inscrit dans un processus parallèle aux différents cycles de vie du système (conception, mise en service, maintenance et démantèlement). À chaque cycle, une démarche de certification évalue la démonstration de sécurité. Il est primordial de proposer des méthodes d'évaluation de la sécurité présentant de façon non équivoque les arguments de la démonstration de sécurité au certificateur. Ces arguments traduisent la démarche de sécurité comme l'étude du dimensionnement, la mise en œuvre de la diversité et/ou des redondances des systèmes et l'élaboration des barrières.

L'étude du facteur humain dans l'analyse de sûreté de fonctionnement repose sur des modèles de la tâche et de la cognition. Un grand nombre de méthodes a été proposé dans ce domaine. Ces méthodes ont été développées pour chaque domaine industriel. Il est possible de classer chronologiquement ces méthodes en deux générations. La première génération s'appuie sur le modèle de la cognition développé par Rasmussen [**105**] et les outils classiques de sûreté de fonctionnement. La deuxième génération a été enrichie de modèles de la tâche et de la cognition plus élaborés prenant en compte de manière plus approfondie le modèle mental que se forgent les opérateurs humains, l'environnement et le contexte de la tâche. De récents travaux visent à améliorer les modèles liés à l'activité humaine et organisationnelle. Le concept de la sécurité écologique d'Amalberti [**9**] et l'ingénierie de la Résilience [**70**] offrent un regard nouveau sur l'activité des opérateurs humains et l'organisation des systèmes sociotechniques. Il s'agit de dépasser la vision faillible généralement utilisée pour évaluer les attributs de la sûreté

de fonctionnement et de proposer une définition duale de la sécurité qui tient compte de la performance réelle des opérateurs humains et des organisations. Cette performance relève de l'anticipation, de la reconnaissance des modes d'exploitation dans lesquels se situe le système et de la capacité à récupérer leurs propres erreurs et les situations dangereuses non prévues lors de la conception du système.

À notre connaissance, dans le domaine ferroviaire, l'étude du facteur humain est insuffisamment étudiée. Le rapport du projet de recherche SECUGUIDE [**5**] présente un état de l'art des travaux effectués par les industriels ferroviaire pour évaluer le facteur humain. Il ressort que les études effectuées par les industriels sont très hétérogènes, la plupart des entreprises contactées travaillent sur la base du retour d'expérience, les études visent à améliorer l'« exploitabilité » des systèmes. Certaines entreprises évaluent la probabilité de défaillance des opérateurs humains à partir de valeurs mentionnées dans la littérature.

Nous avons proposé une démarche méthodologique pour évaluer le facteur humain dans les études de sécurité. À notre point de vue, il est impératif de faire collaborer les spécialistes de l'activité humaine au travail, les ingénieurs de sécurité et les certificateurs. Le retour d'expérience, l'observation sur le terrain et l'observation dans un environnement simulé constituent les données d'entrée de l'analyse de l'activité humaine au travail. Un état de l'art industriel approfondi de la sécurité a permis d'identifier les situations de supervision critiques qui doivent être étudiées. La synthèse de cet état de l'art industriel a été présentée grâce à un modèle des modes d'exploitation commun à l'ensemble des installations visitées.

Une première situation de supervision critique a été identifiée grâce à ce modèle, il s'agit des actions de l'opérateur de supervision généralement effectuées en mode dégradé qui consistent à agir directement sur les barrières de sécurité. De plus, le concept de résilience a été traduit pour chaque installation visitée. Cette conception duale de la sécurité a permis d'identifier une deuxième situation de supervision critique relative à la détection de transitions vers un mode moins sécurisé d'exploitation et aux actions résilientes ou résistantes (selon que les dommages soient apparus ou non) que l'opérateur humain doit entreprendre.

Cette dernière situation a été étudiée dans un environnement ATS simulé en collaboration avec des spécialistes des sciences humaines. Une plateforme constituée d'un réel système ATS a été intégrée en collaboration avec les ingénieurs de développement d'ATS d'ALSTOM. Un transfert des connaissances industrielles vers l'UTC a été réalisé afin de développer les scénarios du protocole expérimental. Une technique de développement de scénarios de supervision a été développée par l'informatique en réutilisant les outils de tests d'ALSTOM à des fins de simulation de situation trafic ferroviaire normal et dégradé.

L'objectif des expériences était d'évaluer les processus cognitifs généraux des sujets impliqués dans la détection d'une transition de mode d'exploitation du type « mise en tension » ou « dégradation ». Trois sujets novices ont été formés à la tâche de détection de trois types d'incidents, dont deux « mises en tension » du système et un incident contraire à la sécurité. La performance des sujets a été évaluée par leur temps de détection de ces incidents. Les résultats ont montré que les temps de détection étaient relativement élevés compte tenu de l'environnement favorable dans lequel ils étaient placés. Ceci démontre la faiblesse de l'ergonomie de l'IHM à favoriser la perception directe des incidents. La forte dispersion des temps de détection inter-sujets est une piste de réflexion qui doit être étudiée de manière plus approfondie, notamment en ce qui concerne la stratégie de surveillance de l'IHM utilisée par les sujets.

L'intégration des résultats de l'étude spécifique de la performance des opérateurs humains dans l'étude de sécurité a été réalisée grâce à la méthode FRAM développée par Hollnagel[**68**]. Le modèle d'accident systémique que propose cette méthode est basé sur le concept de résonance fonctionnelle. Il offre un référentiel commun favorisant l'interdisciplinarité de l'étude de sécurité. Cette démarche a été illustrée grâce à deux cas d'étude, un pour chaque type de situation de supervision critique identifié par l'état de l'art industriel approfondi. Le premier enseignement qu'apportent ces deux cas d'étude montre que la méthode peut être aussi bien appliquée à des activités procédurales que non procédurales. Les résultats de l'instanciation du modèle FRAM contribuent à l'identification de scénarios accidentels qui tiennent compte de la complexité des systèmes sociotechniques.

Les principales difficultés rencontrées lors de ce travail portent sur la mise en place d'un protocole expérimental. D'une part, l'approche consistant à évaluer des sujets novices apparentés à des opérateurs humains en formation atteint ses limites lorsqu'il s'agit d'évaluer la tâche de diagnostic, choix des mesures correctives à entreprendre et de leurs réalisations. En effet, les entreprises ferroviaires ne laissent bien évidemment jamais un opérateur novice seul face aux systèmes de supervision de trafic, il est toujours accompagné par un agent expérimenté. De plus, les agents de supervision de trafic sont généralement recrutés en interne et disposent d'une grande expérience du terrain.

Ce constat a été effectué lors de nos visites des postes de supervision de trafic de réseaux urbain et grandes lignes en France et en Suisse. Toutefois, la libéralisation du transport ferroviaire européen va certainement modifier cette façon de procéder. Les entreprises ferroviaires ne sont d'ores et déjà plus propriétaires des infrastructures, l'arrivée de nouvelles entreprises ferroviaires accompagnée d'une augmentation du trafic nécessitera dans un futur proche la formation de nombreux agents responsables de la supervision de trafic. En France, un mastère professionnel vient d'être créé dans cet objectif, motivé par la Fédération des Industries Ferroviaires (FIF) et coordonnée par l'École Nationale des Ponts et Chaussées (ENPC), cette formation débutera en septembre 2008. Plusieurs industriels et universités, dont l'UTC assureront les formations. La plateforme SPICA-RAIL sera mise à contribution pour la formation des étudiants pour le module de signalisation ferroviaire et de supervision de trafic.

L'objectif de l'évaluation quantifiée de la sécurité demeure la perspective majeure de ce travail. Les travaux restants à effectuer au moment de conclure ce mémoire visent à explorer la perspective d'évaluation probabiliste d'une instanciation des réseaux FRAM en exploitant une analogie des diagrammes FRAM avec les réseaux de neurones artificiels. Par ailleurs, l'étude spécialisée du comportement humain sur la plateforme SPICA-RAIL doit être poursuivie afin d'alimenter la modélisation par la méthode FRAM des activités de supervision critiques du trafic ferroviaire.

Nous souhaitons que ce travail ait permis de rapprocher deux disciplines indispensables que sont les sciences humaines et sociales et la sûreté de fonctionnement dans le but de relever les prochains défis de la maîtrise des risques des systèmes sociotechniques industriels complexes.

ANNEXE A

CONSIGNE FOURNIE AUX SUJETS POUR L'EXPÉRIENCE

Une reproduction de la consigne fournie aux sujets au début de chaque session est donnée à la figure A.1 de la page suivante.

CONSIGNE

Nous allons vous présenter des scénarii simulant des situations de trafic ferroviaire. Chaque scénario aura une durée maximale de 30 mn. Chaque scénario comportera une anomalie (déviation par rapport au nominal) qui pourra apparaître à tout moment.

Trois types d'anomalies sont susceptibles de survenir :
- aiguille en dérangement (cf. présentation des cas possibles pendant la formation) ;
- raté de fermeture d'un signal (cf. présentation des cas possibles pendant la formation) ;
- raté d'ouverture d'un signal (cf. présentation des cas possibles pendant la formation).

Pour chaque scé` ario, votre tâche co` sistera à surveiller le plus atte` tiveme` t possible le fo` ctio` ` eme` t des i` stallatio` s (sig` aux et aiguilles) afi` de détecter et d'ide` tifier l'a` omalie susceptible d'être prése` te da` s le scé` ario.

En cas de détection d'une anomalie nous vous demandons de respecter la procédure suivante :
- signalez sans délai (i.e., le plus rapidement possible) l'anomalie en disant le plus distinctement possible « anomalie détectée » tout en pointant l'anomalie sur l'écran avec la souris ; en cas d'anomalie concernant une aiguille vous pourrez zoomer sur la partie de l'écran qui vous permettra de vérifier si votre détection est correcte ;
- parallèlement, indiquez à voix haute le type d'anomalie en utilisant la nomenclature suivante : « aiguille en dérangement », « raté de fermeture de signal » ou « raté d'ouverture de signal »
- Précisez le plus explicitement possible les raisons pour lesquelles vous en arrivez à ce diagnostic.

En cas de détection correcte, votre tâche sera terminée et le scénario s'arrêtera. En cas de détection incorrecte l'expérimentateur vous indiquera « fausse alarme » et vous devrez poursuivre votre tâche de surveillance.

En cas d'anomalie non détectée, l'expérimentateur vous indiquera « délai dépassé » après un certain délai et interrompra le déroulement du scénario. Vous serez informée sur le type d'anomalie après chaque essai.

Verbalisatio` s :
Pendant toute la durée de la tâche, et principalement en cas de détection d'une anomalie, je vous demande de dire à voix haute, le plus distinctement possible, tout ce à quoi vous pensez même si cela vous paraît être sans intérêt. Le recueil de vos verbalisations est destiné à nous permettre de reconstituer le cheminement de votre raisonnement durant la réalisation de la tâche qui vous est demandée.

Vous ne devez jamais vous retourner pendant la réalisation de la tâche (notamment pour communiquer avec l'expérimentateur) de manière à ne pas interrompre votre activité de surveillance.
Pouvez-vous me résumer ce que nous vous demandons de faire ?

FIGURE A.1. Consigne

BIBLIOGRAPHIE

[1] « Report on the president's commision on the accident at three mile island » – Report 2003-0022-01, Pergamon Press, avril 1979.

[2] « Rapport de la commission d'enquête Ariane 501 – Échec du vol 501 » – Tech. report, Centre National d'Études Spatiales, 1996.

[3] « Rapport de la mission administrative d'enquête technique sur l'accident survenu le 27 janvier 2003 dans le tunnel de la biogna » – Rapport d'enquête, Conseil général des Ponts et Chaussées, 2003.

[4] « ERTMS pour un trafic ferroviaire fluide sûr » – Tech. report, Commission Européenne – DG Énergie et Transport, 2006.

[5] « SECUGUIDE/NTIC impact des nouvelles technologies de l'information et de la communication dans la sécurité des transports Lot 2 : État de l'art concernant la sécurité des facteurs humains » – Rapport de projet PREDIT, Laboratoire d'automatique, de mécanique et d'informatique industrielles et humaines (LAMIH) et le Laboratoire Heuristique, diagnostic et systèmes complexes HEUDIASYC, 2007.

[6] M. Abed & H. Ezzedine – « Vers une démarche intégrée de conception-évaluation des systèmes homme-machine », *Journal of Decision Systems* **7** (1998), p. 147–175.

[7] M. Abed, H. Ezzedine & J.-C. Angué – « Méthodologie d'analyse et description de tâches d'interaction homme-machine avec des outils de spécifications », *Revue européenne. Diagnostic et sûreté de fonctionnement* **5** (1995), no. 2, p. 159–180.

[8] R. Amalberti – « Sécurité et cognition », ch. Chap. 9 : Dysfonctionnements des systèmes et dysfonctionnements de la cognition. Contribution à la compréhension de la sécurité des systèmes ultra-sûrs, p. 185–201, Hermès, 1999.

[9] ———, *La conduite des systèmes à risque*, Paris : PUF, 2001.

[10] J.-P. Aubin – *Viability theory*, Birkhäuser, 1991.

[11] L. Bainbridge – « Ironies of automation », *Automatica* **vol. 19** (1983), p. 775–779.

[12] R. E. Barlow & F. Proschan – *Mathematical theory of reliability*, Wiley, New York, 1965.

[13] F. Belmonte, K. Berkani, J. Boulanger & W. Schön – « Supervision et sécurité ferroviaire », *2nde Conférence internationale des sciences et technique de l'automatisme.* (Sousse (Tunisie)), 17-19 décembre 2005.

[14] _____, « Safety enhancement of railway traffic by modern supervision systems », *Seventh World Congress on Railway Research.* (Montreal (Canada)) (WCRR, éd.), 4-8 June 2006.

[15] _____, « Supervision et sécurité : Le projet spica-rail », *Lambda-Mu, 15e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement* (Lille, France), IMDR-Sdf, 9-13 octobre 2006.

[16] _____, « Taking into account human factors in railway supervision », *Ninth International Symposium of the ISSA Research Section : Design process and human factors integration : optimising compagny performance.* (Nice (France)) (I. S. S. A. (ISSA), éd.), 1-3 March 2006.

[17] F. Belmonte, J. Boulanger & W. Schön – « Human reliability analysis for automatic train supervision », *10th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine systems* (Seoul, Korea) (IFAC, éd.), 4-6 septembre 2007.

[18] _____, « Dispatcher reliability analysis : SPICA-RAIL experiment », *COMPRAIL, 11th International Conference On Computer System Design and Operation in the Railway and other Transit System.* (Toledo, Spain), septembre 2008.

[19] _____, « Utilisation d'un modèle d'accident systémique comme référentiel commun à une analysede risque interdisciplinaire », *Conférence Internationale Francophone d'Automatique* (Bucarest, Roumanie), novembre 2008.

[20] F. Belmonte, J. Boulanger, W. Schön & K. Berkani – « Automatic supervision survey for SPICA-RAIL program », *EAM'06 European Annual Conference on Human Decision-Making and Manual Control* (Valenciennes, France), 27-29 septembre 2006.

[21] _____, « Role of supervision systems in railway safety », *COMPRAIL, Tenth International Conference On Computer System Design and Operation in the Railway and other Transit System.* (Pragues (Czech Republic)) (W. I. Technology, éd.), 10-12 July 2006.

[22] F. Belmonte, W. Schön & J. Boulanger – « Facteur humain et évaluation du risque : Procédure expérimentale spica-rail », *Workshop international : Logique et Transport* (Sousse, Tunisie), IEEE System Man and Cybernetics Society, 18-20 novembre 2007.

[23] F. Belmonte, W. Schön, J. Boulanger & K. Berkani – « Railway traffic supervision research program : Spica rail platform », *EURNEX-ZEL, 14th international symposium "Toward the competitive rail systems in europe"* (Zilina, Rep. Slovaque (EU)), 30-31 mai 2006.

[24] F. Belmonte, W. Schön, J. Boulanger & R. Capel – « Évaluation du facteur humain dans le domaine de la supervision de trafic ferroviaire : le projet SPICA-RAIL », *Lambda-Mu, 16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement* (Avignon, France), octobre 2008.

[25] K. Berkani & F. Belmonte – « Rapport spica-rail lot 3 : Mise en place de la plateforme ats », Tech. report, UTC - HTSC, 2006.

[26] A. Bertrand & P.-H. Garnier – *Psychologie cognitive*, Studyrama, 2005.

[27] C. Bieder – *Les facteurs humains dans la gestion des risques, évolution de la pensée et des outils*, Hermes, 2006.

[28] A. Blas & J. Boulanger – « Comment améliorer les méthodes d'analyse de risques et d'allocation des THR, SIL et autres objectifs de sécurité », *Lambda-Mu, 16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, à paraître* (Avignon), octobre 2008.

[29] C. Blatter – « La charge de travail mentale dans le transport ferroviaire : revue des notions, méthodes et analyses appliquées aux postes d'aiguillage », *Direction de la recherche et de la technologie. SNCF. Projet PREDIT* (2004).

[30] J.-L. Bon – *Fiabilité des systèmes, méthodes mathématiques*, Paris, Masson, 1994.

[31] J. Boulanger – « Expression et validation des propriétés de sécurité logique et physique pour les systèmes informatiques critiques », Thèse, Université de Technologie de Compiègne, 2006.

[32] J. Boulanger & W. Schön – « Assessment of safety railway application », *ESREL, Safety and Reliability Conference* (Stavanger, Norway), june 2007.

[33] CENELEC – « EN-50126 : Application ferroviaires - spécification et démonstration de fiabilité, disponibilité, maintenabilité et sécurité (fmds) », Norme, CENELEC, 1999.

[34] _____, « EN-50128 : Applications ferroviaires - système de signalisation, de télécommunication et de traitement - logiciels pour systèmes de commande et de protection ferroviaire », Norme, CENELEC, 2001.

[35] _____, « EN-50129 : Application ferroviaires - système de signalisation, de télécommunication et de traitement - systèmes électroniques relatifs à la sécurité pour la signalisation », Norme, CENELEC, 2001.

[36] A. Chaumette & L. Le Fèvre – « Système d'automatisation de l'exploitation des trains de la ligne meteor », *REE* **8**, p. 53.

[37] C. Cocozza-Thivent – *Processus stochastique et fiabilité des systèmes*, Springer, 1997.

[38] F. Daniellou – *L'opérateur, la vanne, l'ecran. l'ergonomie des salles de contrôles*, ANACT Montrouge, 1986.

[39] F. Darses & M. De Montmollin – *L'ergonomie*, La découverte, 2006.

[40] J. De Rosnay – *Le macroscope*, Edition Le Seuil, coll. Points, Paris, 1975.

[41] E. M. Dougherty – « Human reliability analysis - where shouldst thou turn ? », *Reliability Engineering & System Safety* **29** (1990), no. 3, p. 283–299.

[42] A. T. Duchowski – *Eye tracking methodology : theory and practice*, Springer, 2003.

[43] H. Ezzedine & C. Kolski – « Démarche d'évaluation d'IHM dans les systèmes complexes, application à un poste de supervision de trafic ferroviaire », *Revue d'Interaction Homme Machine* **5** (2004), no. 2, p. 91–120.

[44] _____, « Modeling of cognitive activity during normal and abnormal situations using object petri nets, application to a supervision system », *Cognition, Technology and Work* **7** (2007), p. 167–181.

[45] E. Fadier – *L'état de l'art dans le domaine de la fiabilité humaine*, OCTARES Editions, 1994.

[46] FENVAC – « Mémoire sur l'accident de la gare de lyon 1988 », Report, Fédération Nationale des Victimes d'Accidents Collectifs, 1988.

[47] D. Foata & A. Fuchs – *Processus stochastiques : Processus de poisson, chaîne de markov et martingales*, Dunod, 2004.

[48] Y. Fujita & E. Hollnagel – « Failures without errors : quantification of context in HRA », *Reliability Engineering & System Safety* **83** (2004), no. 2, p. 145–151.

[49] R. Fuller – « Conceptualisation of driving behaviour as threat avoidance », *Ergonomics* **27** (1984), p. 1139–1155.

[50] M. Gallardo – « Poste de manœuvre à enclenchement informatique (PMI) », *Revue générale des chemins de fer* (2007), no. 3, p. 29–38.

[51] A. Gernigon – *Histoire de la signalisation ferroviaire française*, Éditions la vie du rail, Paris, 1998.

[52] D. I. Gertman & H. S. Blackman – *Human reliability & safety analysis data handbook*, John Wiley & Sons, 1994.

[53] J. O. Grady – « Functional analysis », System Requirements Analysis, Academic Press, Burlington, 2006, p. 105–117.

[54] _____, « Functional analysis alternatives », System Requirements Analysis, Academic Press, Burlington, 2006, p. 200–230.

[55] F. Guenab, J. Boulanger & W. Schön – « Impact des NTIC sur les systèmes de contrôle-commande et signalisation ferroviaire », *Conférence Internationale Francophone d'Automatique, à paraître* (Bucarest, Roumanie), 2008.

[56] L.-H. Gunderson & L. Pritchard – *Resilience and the behavior of large scale ecosystems*, SCOPE volume. Island Press, Washington, DC, 2002.

[57] H. Hadj-Mabrouk – « La maîtrise des risques dans le domaine des automatismes des systèmes de transport guidés : le problème de l'évaluation des analyses préliminaires de risque », *Revue recherche et transports* **49** (1995), p. 101–112.

[58] H. Hadj-Mabrouk, A. Stuparu & D. Bied-Charreton – « Exemple de typologie d'accidents dans le domaine des transports guidés », *Revue générale des chemins de fer* (1998), no. 3, p. 17–27.

[59] G. W. Hannaman, A. J. Spurgin & Y. D. Lukic – « Human cognitive reliability model for pra analysis (epri rp 2170-3) », Tech. report, Electric Power Research Institute, Palo Alto, CA, USA, 1984.

[60] _____, « A model for assessing human cognitive reliability in pra studies », *IEEE Third Conference on Human Factors and Power Plants* (Monterey, CA, USA), 1985.

[61] S. Haykin – *Neural networks : A comprehensive foundation*, IEEE Press, 1994.

[62] C. Hennebert & G. Guiho – « Sacem : A fault tolerant system for train speed control », *FTCS-23, 23rd Int l Symp. on Fault-Tolerant Computing* (Toulouse, France), 1993, p. 624–628.

[63] L. Heurley, S. Haudegond, K. Berkani, F. Belmonte, J. Boulanger & W. Schön – « Rapport spica-rail lot 1 : Etat de l'art industriel approfondi », Tech. report, Université de Technologie de Compiègne – Université de Picardie Jules Verne, 2006.

[64] J.-M. Hoc – *Supervision et contrôle de processus : la cognition en situation dynamique*, Grenoble : Presses Universitaires de Grenoble, 1996.

[65] _____, *La gestion de situation dynamique*, Paris : PUF, 2004.

[66] J.-M. Hoc, R. Amalberti, J.-M. Cellier & V. Grosjean – « Psychologie ergonomique : tendances actuelles », ch. Adaptation et gestion des risques en situation dynamique, p. 15–48, Paris : PUF, 2004.

[67] E. Hollnagel – « Dependability of joint human-computer systems », *SAFECOMP '02 : Proceedings of the 21st International Conference on Computer Safety, Reliability and Security* (London, UK), Springer-Verlag, 2002, p. 4–9.

[68] _____, *Barrier analysis and accident prevention*, Aldershot, UK : Ashgate, 2004.

[69] E. Hollnagel & D. Woods – *Joint cognitive systems : Foundations of cognitive systems engineering*, CRC Press, 2005.

[70] E. Hollnagel, D. Woods & L. N. – *Resilience engineering*, Ashgate, 2006.

[71] E. Hollnagel – *Cognitive reliability and error analysis method*, Oxford : Elsevier Science Ltd, 1998.

[72] J. Holy – « Some insights from recent applications of hra methods in psa effort and plant operation feedback in czech republic », *Reliability Engineering & System Safety* **83** (2004), no. 2, p. 169–177.

[73] E. Hutchins – *Cognition in the wild*, Cambridge, MA, MIT Press, 1996.

[74] IEC – *61508 :1998 and 2000, part 1 to 7. functional safety of electrical, electronic and programmable electronic systems.*, 2000.

[75] _____, *Iec 62267 railway application – automated urban guided transport (augt) safety requirements*, 2005.

[76] B. Johansson – « Joint control in dynamic situations », Thèse, Linköpings universitet, Institute of Technoloy, 2005.

[77] M. C. Kim, P. H. Seong & E. Hollnagel – « A probabilistic approach for determining the control mode in cream », *Reliability Engineering & System Safety* **91** (2006), no. 2, p. 191–199.

[78] M. Konstandinidou, Z. Nivolianitou, C. Kiranoudis & N. Markatos – « A fuzzy modeling application of cream methodology for human reliability analysis », *Reliability Engineering & System Safety* **91** (2006), no. 6, p. 706–716.

[79] M. C. Koornstra – « Transport safety performance in the eu. a statictical overview », Tech. report, European Transport Safety Council, 2003.

[80] M. Lambert, B. Riera & G. Martel – « Application of functional analysis techniques to supervisory systems », *Reliability Engineering and System Safety* **64** (1999), p. 209–224.

[81] J.-C. Laprie (éd.) – *Guide de la sûreté de fonctionnement*, Cépaduès, 1995.

[82] J.-C. Laprie, A. Avizienis & H. Kopetz (éds.) – *Dependability : Basic concpets and terminology, volume 5 of dependanble computing and fault-tolerant system.*, Springer Verlag, Wien New York, 1992.

[83] P. Le Bot – « Human reliability data, human error and accident models–illustration through the three mile island accident analysis », *Reliability Engineering & System Safety* **83** (2004), no. 2, p. 153–167.

[84] P. Le Bouar, Y. Peterschmiidtt & J. Bomo – « La mise en service du poste d'aiguillage informatique de la gare de Strasbourg », *Revue générale des chemins de fer* (2008), p. 7–21.

[85] J.-C. Le Coze, S. Lim & N. Dechy – « Gestion des presque accidents et accidents majeurs : premier bilan d'un enquête sur des sites seveso », *Lambda-Mu, 15e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement* (Lille, France), IMDR-Sdf, 9-13 octobre 2006.

[86] J.-L. Le Moigne – *La théorie du système général, théorie de la modélisation*, Presse Universitaire de France, 1977.

[87] _____, *La modélisation des systèmes complexes*, Dunod, 1990.

[88] M. T. Lee – « Visualizing railroad operations : A tool for traffic planners and dispatchers », *Railroad dispatching operations : Putting research into practice* (Scottsdale), 2004.

[89] D. Lenior, W. Janssen, M. Neerincx & K. Schreibers – « Human-factors engineering for smart transport : Decision support for car drivers en train traffic controllers », *Applied Ergonomics* **37** (2006), p. 479 – 490.

[90] T. M. J. Lenior – « Analyses of cognitive processes in train traffic control », *Ergonomics* **36** (1993), p. 1361 – 1368.

[91] N. Leveson – « A new accident model for engineering safer systems », *Safety Science* **42** (2004), no. 4.

[92] N. Limnios – *Arbres de défaillances, deuxième édition revue et augmentée*, Hermès, Lavoisier, 2005.

[93] L. Magne & D. Vasseur – *Risques industriels - complexité, incertitudes et décision : une approche interdisciplinaire*, Lavoisier, 2006.

[94] A. Maire – « Présentation du système MAGGALY », *Symposium international sur l'innovation technologique dans les transports guidés, ITIG'93* (Lille, France), septembre 1993.

[95] D. Marca & C. McGowan – *Sadt : structured analysis and design technique*, New York : McGraw-Hill Book Co., 1988.

[96] M. Marseguerra, E. Zio & M. Librizzi – « Quantitative developments in the cognitive reliability and error analysis method (cream) for the assessment of human performance », *Annals of Nuclear Energy* **33** (2006), no. 10, p. 894–910.

[97] S. Martin – « La résilience dans les modèles de systèmes écologiques et sociaux », Thèse, École Normale Supérieure de Cachan, 2005.

[98] D. Meister – « Reliability handbook », ch. Human factors in reliability, section 12, McGrow-Hill, New York, 1966.

[99] P. Millot – *Supervision des procédés automatisés et ergonomie*, Hermès, 1988, Traité des nouvelles technologies, série automatique.

[100] _____, « Systèmes homme-machine et automatique », *Journée doctorales d'automatique JDA'99, conférence plénière* (Nancy, France), 21-23 septembre 1999.

[101] P. Moieni, A. J. Spurgin & A. Singh – « Advances in human reliability analysis methodology. part i : frameworks, models and data », *Reliability Engineering & System Safety* **44** (1994), no. 1, p. 27–55.

[102] C. Perrow – *Normal accidents, living with high-risk technologies*, Basic Books, 1984.

[103] P. Polet – « Modélisation des franchissements de barrières pour l'analyse des risques des systèmes homme-machine », Thèse, Université de Valenciennes et du Haut-Cambrésis, 2002.

[104] P. Ramadge & W. W. – « Supervisory control of a class of discrete event process », *SIAM Jounal on Control and Optimization* **25** (1987), no. 1, p. 206–230.

[105] J. Rasmussen – « Skills, rules, knowledge ; signals, signs, and symbols, and other distinctions in human performance models », *IEEE Transactions on Systems, Man and Cybernetics* **13** (1983), p. 257–266.

[106] _____, *Information processing and human-machine interaction : An approach to cognitive engineering*, New-York : North-Holland, 1986.

[107] _____, « Mental models and the control of action in complex environments », ch. 1, p. 41–46, North-Holland : Elsevier Science Publishers, 1990.

[108] J. Rasmussen, A. M. Pejtersen & L. P. Goodstein – *Cognitive systems engineering*, John Wiley & Sons, Inc., New York, NY, USA, 1994.

[109] J. Reason – *Human error*, Cambridge University Press, 1990.

[110] R. Rétiveau – *La signalisation ferroviaire*, Presses de l'école Nationale des Ponts et Chaussées, 1987.

[111] B. Riera, B. Vilain & P. Millot – « A proposal to define and to treat alarms in supervision room », *Proceedings of the Sixth IFAC Congress of Analysis, Desing an Evaluation of Man-Machine Systems.* (Cambridge, MA), MIT, 1995.

[112] G. Rigaud – « Éléments pour le schéma d'une ligne ferroviaire, projet spica-rail », Tech. report, Sigma-conseil, 2006.

[113] D. Ross – « Structured Analysis (SA) : a language for communicating ideas », *IEEE Transactions on Software engineering* **3**, no. 1, p. 16.

[114] T. Van der Schaaf – « Near miss reporting in the chemical process industry », Thèse, Eindhoven university of technology, 1992.

[115] T. B. Sheridan – « Forty-five years of man-machine systems : History and trends », *2nd IFAC Conference Analysis, Design and Evaluation of Man-Machine Systems* (Varese, Italy), 1985.

[116] _____, *Telerobotics, automation, and human supervisory control.*, Cambridge, MA :MIT Press, 1992.

[117] S. Siegel – *Nonparametric statistics for the behavioral sciences*, McGraw-Hill, New York, 1956.

[118] S. Siegel & N. Castellan – *Nonparametric statistics for the behavioral sciences*, McGraw-Hill, New York, 1988.

[119] O. Strater – « Considerations on the elements of quantifying human reliability », *Reliability Engineering & System Safety* **83** (2004), no. 2, p. 255–264.

[120] A.-D. Swain & G. H-E. – « Handbook on human reliability analysis with emphasis on nuclear power plant application », Tech. Report NUREG/CR-1278, USNRC, 1983.

[121] P. Tanguy – « L'accident d'harrisburg. scénario et bilan. », *Revue Générale Nucléaire* **n °5** (1979), p. pp. 524–531.

[122] J. Valancogne – « La défense en profondeur », *Revue RATP–Savoir faire* (2002).

[123] H. H. Van Der Molen & A. M. T. Böttticher – « A hierarchical risk model for traffic participants », *Ergonomics* **31** (1988), no. 4, p. 537–555.

[124] F. Vanderhaegen – « Aprecih : a human unreliability analysis method - application to railway system », *Control Engineering Practice* **7** (1999), no. 11, p. 1395–1403.

[125] _____, « A non-probabilistic prospective and retrospective human reliability analysis method – application to railway system », *Reliability Engineering & System Safety* **71** (2001), no. 1, p. 1–13.

[126] A. Vectra – « Proposed framework for adressing human factors in iec-61508 », Tech. report, Health & Safety Executive, 2001.

[127] K. J. Vicente – *The human factor*, Routledge, 2004.

[128] K. Vicente – *Cognitive work analysis : Toward safe, productive, and healthy computer-based work*, Mahwah, NJ : Lawrence Erlbaum Associates, 1999.

[129] A. Villemeur – *Sûreté de fonctionnement des systèmes industriels : fiabilité, facteur humain, informatisation.*, Eyrolles, 1988.

[130] C. Vincent, M. Ennis & R. Audley – *Medical accidents*, Oxford University Press, 1993.

[131] B. Vincze & G. Tarnai – « Evolution of train control system », *EURNEX Zel : 14th International Symposium, Towards the competitive Rail Systems in Europe*, vol. 1, May 2006, p. 69–76.

[132] R. Vogin – « Présentation de l'analyse fonctionnelle : C'est quoi ? et pourquoi l'utiliser ? », *« Publication CETIM », Conférence sur l'analyse fonctionnelle au service de la qualité*, 1995.

[133] L. Von Bertalanffy – *General system theory : Foundations, development, applications*, george braziller, Mai 2000.

[134] E. E. Werner – « Vulnerable but invincible : high-risk children from birth to adulthood. », *Acta Paediatr Suppl* **422** (1997), p. 103–105.

[135] G. Wilde – « Risk homeostasis theory and traffic accidents : propositions, deductions and discussion of dissension in recent reactions », *Ergonomics* **31** (1988), no. 4, p. 441–468.

[136] _____, *Target risk*, PDE Publication, 1994.

[137] J. Wilson & B. J. Norris – « Rail human factors : Past, present and future », *Applied Ergonomics* **36** (2005), p. 649 – 660.

[138] R. Woltjer & E. Hollnagel – « Modelling and evaluation of air traffic management automation using the functional resonance analysis method », *Proceedings of the 8th International Symposium of the Australian Aviation Psychology Association*, April 2008.

[139] D. Woods & E. Hollnagel – *Joint cognitive systems*, CRC Press, Inc., Boca Raton, FL, USA, 2006.

[140] D. D. Woods – « On taking human performance seriously in risk analysis : Comments on dougherty », *Reliability Engineering & System Safety* **29** (1990), no. 3, p. 375–381.

[141] D. D. Woods, E. M. Roth & K. B. Bennett – « Explorations in joint human-machine cognitive systems », Cognition, computing, and cooperation, Ablex Publishing Corp., Norwood, NJ, USA, 1990, p. 123–158.

[142] G. Zwingelstein – *Diagnostic des défaillances – théorie pratique pour les systèmes industriels*, Hermès, Paris, 1995.