Acquisition et évaluation des connaissances de sécurité des systèmes industriels. Application au domaine de la certification des systèmes de transport ferroviaires guidés

Habib Hadj-Mabrouk

Mémoire

Présenté à l'Université de Technologie de Compiègne

Pour l'obtention de

L'Habilitation à Diriger des Recherches (HDR)

Par

Habib HADJ-MABROUK

Docteur en automatique industrielle et humaine
Chargé de recherche à l'INRETS

ACQUISITION ET ÉVALUATION DES CONNAISSANCES DE SÉCURITÉ DES SYSTÈMES INDUSTRIELS.

Application au domaine de la certification d'automatismes des systèmes de transport ferroviaires guidés

Soutenu le 25 février 1998 devant la commission d'examen :

COUVREUR Gérard	Directeur d'unité de recherche, INRETS-ESTAS	(Examinateur)
DAVID Yves	Consultant, (ex. Directeur régional du centre de Lille-INRETS)	(Examinateur)
DUBUISSON Bernard	Professeur, Université de Technologie de Compiègne	(Rapporteur)
FALSON Pierre	Professeur, CNAM	(Rapporteur)
GANASCIA Jean-Gabriel	Professeur, Université Pierre et Marie Curie - Paris VI	(Examinateur)
PERRIN Jean-Paul	Conseiller scientifique et technique, RATP	(Examinateur)
SIDAHMED Menad	Professeur, Université de Technologie de Compiègne	(Examinateur)
ZWINGELSTEIN Gilles	Professeur, Université Paris VIII	(Rapporteur)

Sommaire

INTRODUCTION GÉNÉRALE

Ce rapport présente, dans le cadre de ma demande d'obtention de l'Habilitation à Diriger des Recherches, mes activités scientifiques, d'expertises, d'enseignement et d'encadrement de la recherche effectuée depuis septembre 1989. D'abord au LAMIH de l'Université de Valenciennes et particulièrement dans l'équipe Informatique Industrielle et Communication Homme-Machine dirigée par le professeur Patrick MILLOT. Ensuite, dans le cadre de ma fonction de Chargé de Recherche à l'INRETS, depuis Janvier 1993, et plus précisément au sein de l'unité de recherche ESTAS (Evaluation des Systèmes de Transport Automatisés et de leur Sécurité) dirigée par Monsieur Gérard COUVREUR.

L'objet de ce mémoire est de présenter les travaux réalisés par mes soins ou sous ma responsabilité par des doctorants, des DEA, des DESS et des Ingénieurs, dans le cadre du groupe de recherche que j'ai constitué au sein de l'INRETS-ESTAS sur le thème acquisition, capitalisation et validation des connaissances de sécurité. Ces travaux sont actuellement regroupés dans l'axe de recherche « AVIS » (Acquisition et Validation des connaissances de Sécurité) qui est l'une des composantes du programme de recherche de l'INRETS (Axe 3.13 - Volet 1). Ils s'exercent principalement dans le cadre du programme interministériel de recherche sur les transports PREDIT/ASCOT. Ils sont soutenus notamment par la direction des transports terrestres (DTT) du Ministère des transports et le Groupement Régional de recherche sur les transports du Nord-Pas-de-Calais (GRRT).

Le domaine d'application de ces travaux concerne essentiellement la certification d'automatismes des systèmes de transport terrestres guidés. L'originalité de ces travaux réside notamment dans l'utilisation conjointe des méthodes cogniticiennes d'acquisition du savoir-faire des experts du domaine, des méthodes plus formelles d'apprentissage symbolique automatique et des approches d'évaluation de la connaissance (en termes de complétude, de cohérence et de traçabilité). Ces recherches se basent donc sur des concepts et méthodes issus du génie logiciel, des sciences cognitives et de l'intelligence artificielle.

Une présentation détaillée des différents thèmes, activités et perspectives de recherche est faite dans la suite de ce mémoire. Le premier chapitre présente ces activités de façon synthétique et fait apparaître mon implication au sein de l'INRETS-ESTAS tant du point de vue expertise et assistance technique que du point de vue administratif, enseignement et recherche (encadrement de thèses et de projets, collaborations,...).

Le deuxième chapitre est consacré au contexte de la recherche. Après une présentation rapide de l'INRETS et des principales activités du département ESTAS, il aborde successivement le cadre de notre recherche, le processus de développement, de validation, d'homologation et de certification d'un système, le processus de mise en sécurité des automatismes d'un système de transport guidé, les principales motivations de nos travaux de recherche, les techniques et méthodes mises en œuvres pour atteindre ces objectifs, les organismes demandeurs qui financent nos travaux, les moyens humains et enfin les principales composantes de l'axe de recherche « AVIS » (Acquisition et Validation des connaissances de Sécurité).

Le troisième chapitre détaille mes activités de recherche qui se sont déroulées au sein de l'unité de recherche ESTAS de l'INRETS. Ces contributions résultent du travail de l'équipe que j'ai constituée pour le développement de l'axe de recherche « AVIS » qui s'articule autour de sept projets complémentaires détaillés tout au long de ce chapitre. Pour chacun de ces projets, on indique le contexte général de l'étude, la problématique scientifique, les motivations, les techniques et méthodes mises en œuvre, l'application réalisée et les résultats obtenus.

Enfin, le dernier chapitre précise les perspectives envisagées pour les projets évoqués tout au long de ce mémoire ainsi que les nouveaux projets récemment mis en place.

PREMIÈRE PARTIE

NOTICE INDIVIDUELLE

1. CURRICULUM VITAE

1.1. État civil

Prénom NOM Habib HADJ-MABROUK

Né le

Nationalité Française

Adresse professionnelle Institut National de Recherche sur les Transports et leur Sécurité
2 av. du Général Malleret-Joinville, 94114 Arcueil Cedex - France
Tél. : 01 47 40 73 52 - Fax : 01 45 47 56 06

1.2. Diplômes

Juillet 1989 : Diplôme d'Etudes Approfondies (D.E.A.), *Major de la promotion*
Spécialité : automatique industrielle et humaine
Laboratoire d'Automatique Industrielle et Humaine de l'Université de Valenciennes
Titre : « Méthodes d'apprentissage symbolique automatique pour l'élaboration de la base de connaissances d'un système expert. Application à la maintenance préventive »

Décembre 1992 : Thèse de doctorat en Automatique Industrielle et Humaine
Laboratoire d'Automatique Industrielle et Humaine de l'Université de Valenciennes
Équipe Informatique Industrielle et Communication Homme-Machine.
Mention : très honorable
Titre : « Apprentissage automatique et acquisition des connaissances : deux approches complémentaires pour les systèmes à base de connaissances. Application au système ACASYA d'aide à la certification des systèmes de transport automatisés ».

Composition du Jury :

Président :	- J-G. GANASCIA	Professeur, Université de Paris VI Jussieu, LAFORIA
Examinateurs :	- M. STAROSWIECKI	Professeur, Université de Lille I
	- J. DEFRENNE	Professeur, Université de Valenciennes
	- B. HOURIEZ	Professeur, Université de Valenciennes
	- B. LE TRUNG	Directeur de Recherche, INRETS Paris
	- P. MILLOT	Professeur, Université de Valenciennes (Directeur de thèse)

1.3. Situation professionnelle actuelle

Chargé de Recherche depuis le 1er janvier 1993
à l'Institut National de Recherche sur les Transports et leur Sécurité (INRETS)
Affectation : Unité de Recherche ESTAS (Évaluation des Systèmes de Transport Automatisés et de leur Sécurité)

1.4. Actions professionnelles

Janvier 1993 : Chargé de recherche à l'INRETS.

Février 1993 : Participation à l'expertise du système de transmission voie-machine TVM 430 TGV Nord.

Mai 1993 : Constitution d'une base de scénarios d'accidents.

Mai 1993 : Chef du projet n° 60 du programme de recherche INRETS "Sécurité des systèmes de transport guidés. Nouvelles méthodes d'évaluation".

Juin 1993 : Participation à l'expertise du projet ANTARES de signalisation, de contrôle de vitesse et d'aide à la conduite du RER-ligne C-Paris.

Avril 1994 : Validation et amélioration du système à base de connaissances ACASYA pour l'aide à la capitalisation, à la classification et à l'évaluation des scénarios d'accidents.

Avril 1994 : Proposition d'un projet de recherche dans le cadre du programme Interministériel PREDIT/ASCOT/Fiche INRETS 17, intitulé "Introduction des techniques d'intelligence artificielle dans le processus de certification des systèmes de transport guidés".

Juin 1994 : Création d'un projet de recherche SAPRISTI dont l'objectif est le développement d'un système à base de connaissances pour l'aide à l'élaboration et à l'évaluation des analyses préliminaires de risques. En octobre 1994, ce projet a permis de démarrer la thèse de Gilles CHOPARD-GUILLAUMOT (Bourse MESR fléchée INRETS) et d'établir une convention de recherche avec le LAFORIA (Equipe ACASA du Professeur J-G GANACIA). Ce projet s'inscrit actuellement dans le cadre du programme de recherche du groupement régional de recherche sur les transports du Nord-Pas-de-Calais (GRRT)

Octobre 1994 : Responsable scientifique d'un axe de recherche AVIS (Acquisition, capitalisation et validation des connaissances de sécurité) que j'ai élaboré fin 1993. Cet axe s'inscrit dans le cadre du programme de recherche de l'INRETS (Axe 3.13-volet 1).

Février 1995 : Création d'un projet de recherche FACTHUS dont l'objectif et le développement d'une méthode d'intégration des facteurs humains dans les activités d'analyse de sécurité et de développement des systèmes de transport guidés.

Septembre 1995 : Développement d'une maquette de faisabilité d'un système basé sur le raisonnement à partir de cas pour l'aide à la capitalisation et à l'évaluation des analyses des effets des erreurs de logiciel (AEEL) - projet SAUTREL. Cette étude a fait l'objet d'un mémoire de DEA, d'un stage de fin d'étude d'ingénieur et d'un stage de DESS que j'ai encadrés à l'INRETS.

Octobre 1995 : Le projet FACTHUS a reçu le soutien de la Direction des Transports terrestres (DTT) du Ministère des Transports. Un contrat de recherche DTT/INRETS a été établi. En novembre 1995, ce projet a permis de lancer la thèse de Bertrand TELLE (Bourse INRETS/Région).
En mars 1996, une convention de recherche avec le LAMIH de l'Université de Valenciennes a été établie (équipe IICHM du Professeur Patrick MILLOT). Ce projet est également développé en collaboration avec le département facteur humain de la SNCF (équipe de M. Pierre VIGNES), l'Institut de Psychologie de l'Université René Descartes Paris V (équipe du Professeur J-C. SPERANDIO), l'Institut Polytechnique de Sévenans (Professeur MAZOUET) et le laboratoire Heudiasyc de l'Université de Technologie de Compiègne (Professeurs P. MORIZET-MAHOUDEAUX et M. SIDAHMED).
En outre, ce projet s'inscrit dans le programme de recherche du GRRT.

Décembre 1995 : Elaboration d'une démarche d'aide à la génération des scénarios d'accident basé sur des techniques d'apprentissage automatique. Ces travaux ont fait l'objet de la thèse de Lassaâd MEJRI soutenue le 12 décembre 1995 à l'Université de Valenciennes. J'ai encadré cette thèse conjointement avec le Professeur Bernard HOURIEZ (équipe IICHM du Professeur Patrick MILLOT). Plusieurs étudiants en DEA ont contribué à la réalisation de cette étude.

Décembre 1995 : Création d'un projet de recherche SPECIALS qui consiste à étudier l'apport du génie cognitif au génie logiciel dans le cadre de l'évaluation des logiciels critiques de sécurité. Ce projet a permis de lancer la thèse de Myriam DARRICAU (Bourse MESR fléchée INRETS) en collaboration avec le LIP6 (ex LAFORIA) de Paris VI. L'encadrement de cette thèse est assuré conjointement par le Professeur Jean-Gabriel GANASCIA et moi -même.

Janvier 1996 : Constitution d'une base de connaissances pour l'aide aux AMDEC des équipements matériels des systèmes de transport guidés - Projet SASEM. Ce travail a été réalisé en partie par deux stagiaires de l'Ecole Polytechnique Féminine de Sceaux encadrées par mes soins.

Avril 1996 : Elaboration d'une convention de recherche avec le laboratoire d'informatique et de mathématiques Appliquées (LIMAV) de l'Université de Valenciennes (équipe du Professeur Arnaud FREVILLE). La recherche porte sur l'étude de faisabilité d'une démarche méthodologique pour l'aide à la validation des connaissances de sécurité.

Avril 1996 : Elaboration d'une convention d'étude avec l'Institut Polytechnique de SEVENANS. Cette étude a porté sur l'analyse de quelques exemples de prise en compte des facteurs humains à la SNCF et à EDF.

Mai 1996 : Elaboration d'une convention de recherche avec le Laboratoire d'Analyse et Modélisation de systèmes pour l'aide à la décision (LAMSADE) de l'Université de Paris IX Dauphine. L'objet de cette convention consiste à étudier la faisabilité d'engendrer des critères d'évaluation d'une analyse de sécurité des logiciels (AEEL) à l'aide d'un système d'apprentissage de règles CHARADE (J-G GANASCIA). Dans le cadre de cette recherche j'ai encadré un étudiant en DESS d'ingénierie de l'aide à la décision.

Mai 1996 : Rédaction d'un rapport comportant plusieurs éléments permettant l'élaboration de conventions de recherche. Ce rapport précise également quelques règles de confidentialité et un ensemble d'obligations exigées des stagiaires et Doctorants.

Août 1996 : Participation à l'élaboration des statuts de la nouvelle agence de certification ferroviaire (CERTIFER).

Septembre 1996 : Collaboration avec la société CETIM (M. S. BOUAZDI) pour la mise en oeuvre d'une méthode d'analyse de risques.

Septembre 1996 : Développement d'une interface d'un logiciel d'élaboration des analyses préliminaires de risque. Ce travail a été effectué dans le cadre d'un stage d'ingénieur de l'IIE-CNAM dont j'ai assuré la responsabilité scientifique.

Février 1997 : Enseignement à l'Université de Versailles Saint-Quentin-en-Yvelines.
DESS Sécurité des Transports.
Intitulé du cours dispensé : application de l'intelligence artificielle à l'analyse de la sécurité

Mai 1997 : Collaboration avec le Laboratoire Heudisyc de l'Université de Technologie de Compiègne (Professeurs P. MORIZET-MAHOUDEAX et M. SIDAHMED) en vue d'étudier les principes d'intégration des facteurs humains dans le développement et l'analyse de sécurité des transports guidés.

Septembre 1997 : Collaboration avec l'Institut des Transports et de planification de l'Ecole Polytechnique Fédérale de Lausanne.
Objet : jusqu'où l'automatisation de la fonction de conduite pourra-t-elle être menée pour le réseau ferroviaire européen classique ?

Octobre 1997 : Proposition d'un programme de recherche à partenaires multiples (RATP, SNCF, SLTC, INRETS, ...) en vue de développer une base de scénarios d'accidents (ou de quasi-accidents) à partir du retour d'expérience.

Nov. Déc.1997 : Enseignement à l'école Nationale des Ponts et Chaussées.
Master "Systèmes intelligents de transports"
Intitulé du cours dispensé : analyse et évaluation du risque dans les transports

Jav. Fév.1998 : Enseignement à l'école Nationale des Ponts et Chaussées.
Master "Systèmes intelligents de transports"
Intitulé du cours dispensé : modèles de développement des systèmes et logiciels

Février 1998 : Enseignement à l'Université de Versailles Saint-Quentin-en-Yvelines.
DESS Sécurité des Transports.
Intitulé du cours : processus de construction de la sécurité des systèmes de transport guidés

1.5. Bilan quantitatif des travaux, ouvrages, articles et réalisations

Mes travaux de recherche et d'expertise ont débouché sur la production des travaux suivants :

LISTE DES TRAVAUX	Travaux réalisés	Travaux en cours
Participation à l'encadrement de thèses	**1**	(+3 en cours)
Encadrement d'étudiants (DEA, DESS, Ingénieur)	**11**	
Enseignement	**4** interventions dans deux établissements	
Expertise et assistance technique	**2** interventions (TGV Nord, ANTARES)	
Liste des contrats gérés avec un intérêt pour l'industrie	**4**	(+1 en cours)
Revues	**13**	
Congrès internationaux	**15**	(+1 propositions)
Congrès nationaux	**10**	(+1 propositions)
Rapports de conventions/contrats	**21**	(+1 en cours)
Rapports d'expertises	**7**	
Rapports de recherche (intermédiaires ou d'étape)	**7**	
Conférences sur invitation	**8**	

2. ACTIVITÉS DE RECHERCHE

2.1. Thèmes de la recherche

Mes activités de recherche consistent à étudier l'apport des techniques d'intelligence artificielle et des facteurs humains au domaine de la sécurité d'automatismes des systèmes de transport guidés. Elles visent le développement des méthodes et outils logiciels à base de connaissances en vue de faciliter les missions d'expertise et d'assistance technique menées par l'INRETS en matière d'analyse de sécurité et de certification des systèmes de transports guidés. Ces activités de recherche portent plus précisément sur les thèmes suivants :

- modélisation, capitalisation et validation des connaissances ;
- méthodes et stratégies d'évaluation des études de sécurité au niveau système, matériel et logiciel,
- intégration des facteurs humains et de l'ergonomie dans le processus d'analyse de sécurité et de développement des systèmes de transports guidés.

L'ensemble de ces thèmes est actuellement regroupé dans un axe de recherche baptisé « AVIS » (Acquisition et Validation des connaissances de Sécurité) qui comporte sept projets de recherche complémentaires :

1. Projet SAPRISTI : système à base de connaissance pour l'aide à l'élaboration et à l'évaluation des analyses préliminaires de risques (APR),
2. Projet ACASYA : sysème d'apprentissage automatique pour l'aide à la capitalisation, à la classification à l'évaluation et à la génération des scénarios d'accidents,
3. Projet SAUTREL : système d'aide aux analyses des effets des erreurs de logiciels (AEEL) de sécurité basé sur le raisonnement à partir de cas,
4. Projet SASEM : système à base de connaissances pour l'aide à l'analyse des modes de défaillance, de leurs effets et de leur criticité des équipements matériels,
5. Projet FACTHUS : méthode d'intégration des facteurs humains dans les activités d'analyse de sécurité et de développement des systèmes,
6. Projet SPECIALS : apport du génie cognitif au génie logiciel dans le cadre de l'évaluation des logiciels critiques de sécurité,
7. Projet VALIDE : méthode de validation des connaissances de sécurité.

2.2. Contexte de la recherche et collaborations scientifiques

Ces activités de recherche s'exercent principalement dans le cadre du Programme inter-ministériel de recherche sur les transports (PREDIT-ASCOT : Programme de Recherche et Développement pour l'Innovation et la Technologie des Transports Terrestres - Automatismes de sécurité et Systèmes de Contrôle-commande dans les Transports guidés). Elles sont soutenues par la Direction des transports terrestres (DTT) du Ministère des transports et le Groupement régional de recherche sur les transports du Nord-Pas-de-Calais (GRRT).

2.3. Secteurs d'application des recherches

Transports, Industries à risques

2.4. Disciplines, domaines de recherche

Sécurité, Automatique, Intelligence artificielle, Facteurs Humains

2.5. Mots clés

Systèmes de transport terrestre guidés, Sûreté de fonctionnement des systèmes, Sécurité des automatismes, Analyse des risques, Certification des systèmes de transports guidés, Acquisition des connaissances, Modélisation et capitalisation des connaissances, Validation des connaissances, Systèmes à base de connaissances, Apprentissage symbolique automatique, Facteurs Humains, Méthode de spécification des logiciels, Évaluation des logiciels critiques.

2.6. Activités d'encadrement de recherche

Mon encadrement a principalement consisté à :

- définir les sujets et les problématiques de recherche,
- effectuer les démarches administratives en vue d'obtenir les moyens financiers et logistiques nécessaires,
- transmettre les connaissances relatives au problème posé (fourniture de documents, exposés, inscription à des séminaires,
- orientation et validation des travaux,
- correction des mémoires.

2.6.1. Participation à l'encadrement de thèses

Thèse soutenue :

- Lassaâd MEJRI. « Une démarche basée sur l'apprentissage automatique pour l'aide à l'évaluation et à la génération de scénarios d'accidents. Application à l'analyse de sécurité des systèmes de transport automatisés ». Thèse de doctorat, Université de Valenciennes, 6 décembre 1995, 210p.

Thèses en cours :

- Gilles CHOPARD-GUILLAUMOT. « Un système à base de connaissances d'aide à l'analyse préliminaire de risques et aux analyses de sécurité fonctionnelle des systèmes de transports guidés ». Université de Paris VI, LAFORIA. Thèse démarrée en octobre 1994.

- Myriam DARRICAU. « Apport du génie cognitif au génie logiciel dans le cadre de l'évaluation des logiciels de sécurité. Application au domaine de la certification des logiciels dans les transports guidés". Université de Paris VI, LAFORIA. Thèse démarrée en décembre 1995.

Thèse pour laquelle je n'assure que la validation des travaux au regard de leur intérêt pour la sécurité

- Bertrand TELLE. « Intégration de la fiabilité humaine dans les systèmes de transports guidés ». Université de Valenciennes. Thèse démarrée en novembre 1995.

2.6.2. Encadrement d'étudiants (D.E.A., D.E.S.S., Ingénieur)

- DARRICAU M. « Maquette de faisabilité d'un outil basé sur le raisonnement à partir de cas pour l'aide à la capitalisation et à l'analyse des erreurs de logiciels. Application à la sécurité des logiciels dans les transports guidés ». Mémoire de DEA IARFA (Intelligence Artificielle, Reconnaissance des Formes et Applications), Université Paris 6 - Jussieu. INRETS, Arcueil, septembre 1995, 22 p.

- DARRICAU M. « Apport du raisonnement à partir de cas à l'analyse des effets des erreurs de logiciels. Application à la sécurité des logiciels critiques dans les transports guidés ». Rapport de fin d'études d'ingénieur de l'École Polytechnique Féminine. INRETS, Arcueil, juin 1995, 106 p.

- DAUFES S., CAUDRON C. « Base de connaissances d'analyse des modes de défaillances, de leurs effets et de leur criticité. Application à la sécurité des équipements matériels des systèmes de transport guidés ». Rapport de projet industriel de l'École Polytechnique Féminine. INRETS, Arcueil, janvier 1996, 113 p.

- DERENTY V. « Réalisation d'une interface Homme-Machine pour l'exploitation de deux mécanismes d'apprentissage symbolique-numérique : CLASCA et EVALSCA ». Rapport de stage de DESS-ICHM. Laboratoire d'Automatique Industrielle et Humaine de l'Université de Valenciennes, mars 1992.

- GABER K. « Contribution à la réalisation et à l'évaluation d'un système d'apprentissage inductif par classification ». Mémoire de DEA en automatique industrielle et humaine, Université de Valenciennes, Juin 1992.

- KAUTZMANN J. « Exemples d'intégration des facteurs humains dans le développement des projets industriels ». Mémoire de stage de D.E.S.S. d'Ergonomie de l'institut de psychologie de l'université de Paris V. INRETS, Arcueil, juillet 1996, 59 p.

- KAUTZMANN J. « Apports et limites des méthodes de prise en compte des facteurs humains au domaine des systèmes de transport guidés ». Mémoire de stage de fin d'études d'ingénieur de l'institut polytechnique de Sevenans. INRETS, Arcueil, octobre 1996.

- MEJRI L. « Réalisation d'une maquette de faisabilité d'un système d'apprentissage de descriptions de classes d'objets ». Rapport de stage de fin d'études d'Ingénieur en informatique de l'ENSI de Tunis. LAIH de l'Université de Valenciennes, janvier 1991.

- MEJRI L. « Apport des méthodes d'apprentissage automatique au domaine de la certification des systèmes de transport automatisés ». Mémoire de DEA en automatique industrielle et humaine. Université de Valenciennes, Juin 1991.

- NDIAYE A. « Aide à l'évaluation des analyses des effets des erreurs du logiciel. Application à la sécurité des systèmes de transports guidés. ». Mémoire de stage de D.E.S.S. d'Ingénierie de l'aide à la décision, Université Paris IX Dauphine. INRETS, Arcueil, septembre 1996, 40 p.

- RAÎS F. « Analyse et conception de l'interface d'un logiciel d'élaboration des analyses préliminaires de risques ». Rapport de stage de fin de 2ème année d'école d'ingénieur - Institut d'informatique d'entreprise (CNAM-IIE). INRETS, Arcueil, septembre 1996, 30 p.

2.7. Recherches effectuées pour des tiers (contrats)

Intitulé : Introduction des techniques d'intelligence artificielle dans le processus de certification des systèmes de transport terrestres guidés.

Organisme concerné : PREDIT-ASCOT - Programme de Recherche et Développement pour l'Innovation et la Technologie des Transports Terrestres - Automatismes de sécurité et Systèmes de Contrôle-commande dans les Transports guidés.

Date : 1994 - 1998.

Intitulé : Méthode d'intégration des facteurs humains dans les activités de développement et d'analyse de sécurité des systèmes de transport guidés.

Organismes concernés : - DTT - Direction des transports terrestres du Ministère des transports,
- SNCF - Département facteurs humains.

Date : 1995 - 1998

Intitulé : Système à base de connaissances d'aide à l'analyse préliminaire de risques.

Organismes concernés: - Programme de Recherche PREDIT-ASCOT
- GRRT : Groupement régional de recherche sur les transports du Nord-Pas-de-Calais,

Date : 1995 - 1998

Intitulé : Mise en oeuvre et validation d'une méthode d'analyse des risques dans les domaines des ascenseurs et des industries mécaniques.

Organismes concernés : - CETIM : Centre technique des industries mécaniques. Établissement de SENLIS. Service commandes électroniques industrielles,
- OTIS : Département méthodes de conception des ascenseurs electriques.

Date : (en cours de négociation)

3. ACTIVITÉS D'EXPERTISE ET D'ASSISTANCE TECHNIQUE DANS LE DOMAINE DE LA SÉCURITÉ D'AUTOMATISMES DES SYSTÈMES DE TRANSPORT GUIDÉS

Le développement et l'exploitation d'un système de transport guidé font intervenir trois principaux acteurs : le maître d'œuvre développe et valide son système, le maître d'ouvrage homologue le système et l'État ou la collectivité territoriale veille au respect des exigences techniques de sécurité par l'ensemble des intervenants. Il délivre les autorisations de mise en service et peut retirer ces autorisations en cas de non respect des exigences de sécurité que doit satisfaire le système lors de sa conception, de sa réalisation et de son exploitation. Cette autorisation est accordée au vu d'un dossier d'homologation conçu par le Maître d'ouvrage et d'un rapport d'évaluation (ou de certification) élaboré par l'INRETS. L'INRETS-ESTAS assure donc une mission d'assistance technique auprès de la DTT (Direction de Transports Terrestre) pour la certification des automatismes de protection des usagers dans les systèmes de transport guidés en France. A la demande d'industriels ou de collectivités locales, ESTAS mène également certaines actions d'expertise ou d'audit. Cette position d'expert de L'INRETS-ESTAS résulte des connaissances acquises dans ses travaux de recherches dans le domaine du logiciel et de celui de la sécurité des systèmes.

Ma participation a porté principalement sur les missions suivantes :

Système TVM 430 de Transmission Voie-Machine du TGV Nord

Les travaux confiés à L'INRETS consistant à évaluer les moyens, méthodes et techniques mis en œuvre par le maître d'ouvrage SNCF et le maître d'œuvre CSEE-Transport, ont abouti à un rapport final permettant à la Direction de Transports Terrestre d'autoriser l'exploitation du TGV-Nord entre Paris et Lille à partir de Mai 1993. Ma contribution dans le cadre de ce projet a porté essentiellement sur l'examen de la traçabilité des études de sécurité [Bied-Charreton et al. 93].

Système ANTARES de signalisation, de contrôle de vitesse et d'aide à la conduite du RER-Ligne C-Paris

Cette mission, commencée en juin 93, s'attache à examiner l'adéquation, la consistance, l'exhaustivité, la cohérence et la traçabilité des méthodes de développement, de validation et d'homologation mises en œuvre par le maître d'ouvrage SNCF et le maître d'œuvre MATRA-Transport. Ma contribution dans le cadre de ce projet a porté principalement sur l'analyse et l'examen de plusieurs documents d'analyse de sécurité au niveau système et plus particulièrement l'évaluation du dossier d'Analyse préliminaire de risques. Cette étude a permis d'élaborer plusieurs rapports qui ont débouché sur un ensemble de remarques et questions adressées à la SNCF et à la Direction de Transports Terrestre du ministère des transports [Hadj-Mabrouk et Bied-Charreton 94a, 94b, 94c, 94d, 95].

4. ACTIVITÉS D'ENSEIGNEMENT

- **Nom de l'École :** D.E.S.S. Sécurité des transports

- **Lieu (établissement) :** Université de Versailles Saint-Quentin-en-Yvelines. 78280 GUYANCOURT.

- **Intitulé du cours dispensé :** Application des techniques d'intelligence artificielle à l'analyse et à l'évaluation de la sécurité d'automatismes des systèmes de transport guidés.

- **Thèmes développés :**

1. Sécurité et certification des systèmes de transport guidés,
2. Méthodes d'analyse de la sécurité,
3. Techniques d'intelligence artificielle,
4. Application de l'intelligence artificielle à l'analyse et à l'évaluation de la sécurité.

- **Année :** 1997
- **Durée :** 14 heures

- **Nom de l'École :** MASTER « Systèmes Intelligents de Transports »
- **Lieu (établissement) :** Ecole Nationale des Ponts et Chaussées. 77455 Marne la Vallée
- **Intitulé du cours dispensé :** Analyse et évaluation du risque dans les transports

- **Thèmes développés :**

1. Les accidents dans les transports,
2. Concepts relatifs à la sécurité (dommage, accident, quasi-accident, accident potentiel, danger, risque, ...),
3. Evaluation et moyen de réduction du risque,
4. Sûreté de fonctionnement des systèmes (fiabilité, maintenabilité, disponibilité, sécurité),
5. Différentes techniques de sécurité (intrinsèque, probabiliste, contrôlée)
6. Processus de mise en sécurité d'un système (construire la sécurité, administrer la sécurité, valider la sécurité)

- **Année :** 1997
- **Durée :** 12 heures

- **Nom de l'École :** MASTER « Systèmes Intelligents de Transports »
- **Lieu (établissement) :** Ecole Nationale des Ponts et Chaussées. 77455 Marne la Vallée
- **Intitulé du cours dispensé :** Modèles de développement des systèmes et logiciels

- **Thèmes développés :**

1. Différents modèles de développement (modèle en V, modèle en spirale, modèle en cascade, ...)
2. Exemples de méthodologies de développement de systèmes de transport guidés (Tvm430-TGV, Maggaly, ...)
3. Intégration des études de sécurité dans le cycle de développement d'un système

- **Année :** 1998
- **Durée :** 12 heures

- **Nom de l'École :** D.E.S.S. Sécurité des transports
- **Lieu (établissement) :** Université de Versailles Saint-Quentin-en-Yvelines. 78280 GUYANCOURT
- **Intitulé du cours dispensé :** Processus de construction de la sécurité des automatismes des systèmes de transport guidés.

- **Thèmes développés :**

1. Méthodes de construction de la sécurité au niveau système : APR, ASF
2. Méthodes de construction de la sécurité au niveau logiciel : AEEL, Projet SPECIALS, ...
3. Méthodes de construction de la sécurité au niveau matériel : MAC, AMDEC, MCPR

- **Année :** 1998
- **Durée :** 14 heures

5. ACTIVITÉS ADMINISTRATIVES

- Depuis 1994 : Responsable scientifique de l'axe de recherche « AVIS » (Acquisition et Validation des connaissances de Sécurité). Dans le cadre de cet axe, j'ai été amené à gérer plusieurs contrats et conventions de recherche, à mettre en œuvre un certain nombre de collaborations scientifiques avec des organismes et des laboratoires universitaires, à définir une problématique scientifique adéquate et à assurer le suivi administratif et scientifique de ces collaborations industrielles et universitaires.

- En 1995 : Chef de projet à l'INRETS. Projet n°60 intitulé « Sécurité des systèmes de transport guidés. Nouvelles méthodes d'évaluation ». Dans le cadre de ce projet, j'ai proposé un programme de recherche dont j'ai assuré le suivi, en collaboration avec deux autres chargés de recherche et un ingénieur de recherche. Dans ce contexte, j'ai encadré deux thésards.

- Depuis 1995 : Membre des jurys des pré-soutenances de thèse au Laboratoire d'Informatique de Paris 6 (LIP6). Université Pierre et Marie curie.

- En 1996 : membre du groupe 5 de l'association A.E.O.C.F. (Association pour l'étude d'un organisme français de certification ferroviaire) dont la mission est d'élaborer les statuts de la nouvelle *Agence de Certification Ferroviaire* Française (CERTIFER). La création de cette agence répond aux exigences de la directive n°96/48 du 23 juillet 96 du Conseil de l'Union européenne relative à l'interopérabilité du réseau européen de trains à grande vitesse qui spécifie, à l'article 20, qu'il doit être fait appel à des organismes, notifiés par un Etat membre, pour effectuer toute attestation de conformité. Afin d'éviter d'avoir à faire appel à des organismes étrangers, la fédération des industries ferroviaires (FIF), la SNCF, la RATP et l'INRETS ont décidé de créer en février 1997 CERTIFER.

- En 1996 : dans le cadre du groupe « Industrialisation et commercialisation de certains produits ou activités de l'INRETS », j'ai contribué à l'élaboration d'un rapport intitulé « Éléments pour l'élaboration de conventions de recherche ». Seule une protection efficace et systématique de la production intellectuelle de l'Inrets peut en garantir la valorisation. La mise en œuvre d'une telle protection suppose que soient rédigées des conventions entre l'Inrets et ses partenaires (universités, industriels…) ou ses personnels non permanents. Confrontés au besoin d'organiser nos relations avec d'autres laboratoires, nous avons été amenés à étudier puis élaborer plusieurs conventions. Ce rapport comporte trois éléments : un exemple de convention de recherche, un avenant à une convention de stage qui précise quelques règles de confidentialité, ainsi qu'un ensemble d'obligations imposées à nos stagiaires.

6. APPARTENANCE A DES GROUPES DE RECHERCHE ET COLLABORATIONS

Les travaux de recherche et d'expertise, précédemment cités, m'ont naturellement incité non seulement à collaborer avec des laboratoires universitaires mais aussi à m'impliquer dans plusieurs groupes de recherche, en vue de suivre l'évolution des domaines de la sécurité et de l'intelligence artificielle. L'objectif visé est la recherche des méthodes, techniques et outils les plus adéquats pour appréhender le domaine d'analyse de sécurité et de certification des transports guidés.

6.1. Appartenance à des groupes de recherche

- Groupe 5 de l'association A.E.O.C.F. dont la mission est d'élaborer les statuts de la nouvelle Agence de Certification Ferroviaire Française « CERTIFER ».
- Groupe « GRACQ » : Groupe de Recherche en Acquisition et modélisation des Connaissances, affilié à l'AFCET et à l'AFIA.
- Groupe « transports guidés et logique floue » coordonné par l'association CRIN (Coordination Recherche Industriel).
- Groupe « Logiciel zéro-défaut » de l'AFCET.
- Groupe « Pôle Intelligence Artificielle » de l'INRETS.
- Groupe « Industrialisation et commercialisation de certains produits ou activités de l'INRETS ».

6.2. Collaborations scientifiques

Cette recherche est effectuée en collaboration avec les laboratoires et organismes suivants :

- Laboratoire d'Informatique de Paris 6 LIP6 (ex LAFORIA) de l'Université de Pierre et Marie Curie de Paris 6-Jussieu (équipe ACASA du Professeur Jean-Gabriel GANASCIA),
- Laboratoire HEUristique et DIAgnostic des SYstèmes Complexe (HEUDISYC) de l'Université de Technologie de Compiègne (Professeurs B. DUBUISSON, P. MORIZET-MAHOUDEAUX, M. SIDAHMED),
- Laboratoire d'Informatique et de Mathématiques Appliquées (LIMAV) de l'Université de Valenciennes (Professeur Arnaud FREVILLE et Jalel TABKA - Maître de conférence),
- Laboratoire d'Automatique et de Mécanique industrielle et Humaine (LAMIH) de l'Université de Valenciennes (équipe Informatique Industrielle et Communication Homme-Machine du Professeur Patrick MILLOT),
- École Polytechnique Féminine de Sceaux (EPF),
- Laboratoire d'Analyse et Modélisation de Systèmes pour l'Aide à la Décision (LAMSADE) de l'Université de Paris IX Dauphine (M. Daniel VANDERPOOTEN - Maître de conférence et Mme Camille SABROUX - Maître de conférence),
- Institut Polytechnique de Sévenans (Professeur MAZOUET),
- Institut de Psychologie de l'Université René Descartes Paris V (Professeur J-C. SPERANDIO),
- Laboratoire LIRMM de l'Université de Montpellier II (Professeurs Michel HABIB et Michel CHEIN),
- Direction des Transports Terrestres du Ministère des transports (Mme Jacqueline GAUDOT),
- Institut d'Informatique d'Entreprise d'Évry (IIE-CNAM),
- Institut des Transports et de Planification de l'Ecole Polytechnique Fédérale de Lausanne (Professeur R-E. RIVIER, M. D. EMERY et J-D. BURI),
- SNCF : Société National des Chemins de Fer Français :
  - M. Pierre VIGNES, M. Blatter et Mme P. JOST, Département facteur humain
  - Mme Michel BÉRRIEAU,
  - M. Patrick OZELLO, Direction de la recherche
- RATP : Régie Autonome des Transports Parisiens (M. Jacques VALANCOGNE),
- SLTC : Société Lyonnaise de Transports en Commun (M. Alain QUÉRÉ).

7. LISTE DES TRAVAUX, OUVRAGES, ARTICLES ET RÉALISATIONS

7.1. REVUES AVEC COMITÉ DE LECTURE

CHOPARD-GUILLAUMOT G., HADJ-MABROUK H., GANASCIA J-G. (1996).
« Contribution à une meilleure définition de l'analyse préliminaire de risques pour les systèmes de transport guidés ». *Journal Européen des Systèmes Automatisés (RAIRO-APII-JESA),* Paris, vol. 30, n° 1, pp 121-143, Avril 1996.

CHOPARD-GUILLAUMOT G., HADJ-MABROUK H. (1996).
« Définition des principaux concepts relatifs à la notion de sécurité dans les transports guidés ». *Revue Générale des Chemins de Fer*, Paris, n° 2, Éditions Dunod, pp 23-36, Février 1996.

DARRICAU M., HADJ-MABROUK H., GANASCIA J-G. (1997).
« Une approche pour la réutilisation des spécifications de logiciels. Application au domaine de la sécurité des systèmes de transport guidés ». *Revue Génie Logiciel*, Édition EC2 & Développement, Paris, n° 45, septembre 1997, pp 2-8.

DARRICAU M., HADJ-MABROUK H.(1996).
« L'analyse des effets des erreurs de logiciel basée sur le raisonnement à partir de cas ». *Lettre de la sûreté de fonctionnement*, Édition EC2 & Développement, Paris, n° 42/43, mai-juillet 1996, pp 12-22.

HADJ-MABROUK H., STUPARU A., BIED-CHARRETON D. (1998).
« Exemple de typologie d'accidents dans le domaine des transports guidés ». *Revue Générale des Chemins de Fer*, Éditions Dunod, Paris, mars 1998 (A paraître).

HADJ-MABROUK H. (1997).
« L'acquisition des connaissances pour l'élaboration d'une base de scénarios d'accidents ». *Lettre de la sûreté de fonctionnement*, n° 50, Édition EC2 & Développement, Paris, septembre 1997, pp 3-16.

HADJ-MABROUK H. (1997).
« CLASCA, EVALSCA et GENESCA : trois mécanismes d'apprentissage dédiés respectivement à la classification, à l'évaluation et à la génération des scénarios d'accidents ». *La lettre de l'intelligence artificielle*, n° 126/127, Édition EC2 & Développement, Paris, septembre/octobre 1997, pp 9-15.

HADJ-MABROUK H. (1996).
« Méthodes et outils d'aide aux analyses de sécurité dans le domaine des transports terrestres guidés ». *Revue Routes et Transports*, Montréal-Québec, vol. 26, n° 2, pp 22-32, Été 1996.

HADJ-MABROUK H. (1996).
« Capitalisation et évaluation des analyses de sécurité des automatismes des systèmes de transport guidés ». *Revue Transport Environnement Circulation*, Paris, TEC n° 134, pp 22-29, Janvier-février 1996.

HADJ-MABROUK H. (1995).
« La maîtrise des risques dans le domaine des automatismes des systèmes de transport guidés : Le problème de l'évaluation des analyses préliminaires de risques ». *Revue Recherche-Transport-Sécurité*, numéro 49, pp 101-112, France, Décembre 1995.

HADJ-MABROUK H. (1994).
« ACASYA : a learning system for functional safety analysis ». *Revue Recherche Transports Sécurité*, n° 10, pp 9-21, France, Septembre 1994.

HADJ-MABROUK H. (1993).
« Apport des techniques d'intelligence artificielle à l'analyse de la sécurité des systèmes de transport guidés », *Revue Recherche Transports Sécurité*, n° 40, pp 3-16, France, Septembre 1993.

HADJ-MABROUK H., HOURIEZ B., EL KOURSI M., LE TRUNG B. (1992).
« Méthodologie d'analyse et d'évaluation de la sécurité basée sur les techniques d'intelligence artificielle ». *Revue européenne de diagnostic et sûreté de fonctionnement*, Éditions Hermès 1992, France, volume 2 - n° 1/1992, pp 5-35, juin 1992.

7.2. CONGRÈS INTERNATIONAUX AVEC ACTES ET COMITÉ DE LECTURE

CHOPARD-GUILLAUMOT G., HADJ-MABROUK H., GANASCIA J-G. (1996).
« Towards a computer aided assessment of railway system preliminary hazard analyses ». Comprail 96*, 5e Conférence internationale sur la conception, la construction et l'exploitation assistées par ordinateur dans les systèmes de transport ferroviaires*, Berlin, pp 493-502, 21-23 août 1996.

DARRICAU M., HADJ-MABROUK H., GANASCIA J-G. (1998).
« Amodel for reusing specifications of safety-critical software in the field of automated people movers ». *Congrès IEEE, Computational engineering in systems applications.* Nabeul-Hammamet, Tunisia, April 1-4, 1998. (A paraître).

DARRICAU M., HADJ-MABROUK H., GANASCIA J-G. (1997).
« Acquisition and structuration of knowledge of safety critical software specifications ». *8th IFAC Symposium on Transportation Systems*, Chania, Greece, Volume 3, pp 1227-1231, 16-18 june 1997.

DARRICAU M., HADJ-MABROUK H. (1996).
« Applying case-based reasoning to the storing and assessment of software error-effect analysis in railway systems ». Comprail 96, *5e Conférence internationale sur la conception, la construction et l'exploitation assistées par ordinateur dans les systèmes de transport ferroviaires*, Berlin, pp 483-492, 21-23 août 1996.

DARRICAU M., HADJ-MABROUK H. (1995).
« Étude de faisabilité d'un outil d'aide aux analyses des effets des erreurs des logiciels, basé sur le raisonnement à partir de cas. Application à la sécurité des systèmes de transport guidé ». *Huitièmes journées internationales du génie logiciel et de ses applications*. Paris-La-Défense, 15-17 novembre 1995, pp 677-689.

HADJ-MABROUK H., MEJRI L. (1998).
« ACASYA : a knowledge-based system for aid in the storage, classification, assessment and generation of accident scenarios ». ». *Congrès IEEE, Computational engineering in systems applications.* Nabeul-Hammamet, Tunisia, April 1-4, 1998. (A paraître).

HADJ-MABROUK H., STUPARU A. (1998).
« What is the human driver's place in the automatic guided transportation ? ». Comprail 98*, Sixth Intrnational Conference on Computer Aided Design, Manufacture and Operation in the Railway and other advanced Mass Transit Systems*, Lisbon, Portugal, 2-4 September 1998 (proposition).

HADJ-MABROUK H., CHOPARD-GUILLAUMOT G., DARRICAU M. (1996).
« Tools for providing aid for modelling, storing and assessing safety analyses in the area of terrestrial guided transport ». 29th Isata, *29e Symposium international sur les technologies de l'automobile et de l'automatique*, Florence-Italie, pp 357-364, 3-6 juin 1996.

HADJ-MABROUK H. (1994).
« Introduction des techniques d'apprentissage automatique et d'acquisition des connaissances dans l'analyse de sécurité des transports guidés ». *Troisième conférence maghrébine en génie logiciel et intelligence artificielle*. Rabat, Maroc, 11-14 Avril 1994, p 331-340.

HADJ-MABROUK H., MEJRI L., EL KOURSI M., HOURIEZ B. (1992).
« Méthodologie d'aide à l'évaluation de la sécurité des systèmes de transport automatisés, basée sur l'apprentissage automatique ». *Forum de la SCGM (Sté Canadienne de Génie Mécanique), TRANSPORT 1992+,* Université Concordia (session : Sécurité dans les transports), Montréal, Québec, Canada 1-4 Juin 1992, volume III, p 957-964.

HADJ-MABROUK H., MEJRI L., EL KOURSI M., HOURIEZ B (1992).
« Système expert à apprentissage pour l'aide à l'analyse de sécurité. Application à la certification des systèmes de transport automatisés ». *12èmes Journées Internationales d'Avignon 92*. Conférence Intelligence Artificielle, Défense et Sécurité civile. Avignon 2-3 Juin 1992, France, volume 2, p 97-112.

HADJ-MABROUK H., HOURIEZ B. (1992).
« Acquisition de connaissances et apprentissage automatique pour l'élaboration d'une base de connaissances ». *7èmes Journées Francophones d'Apprentissage et d'Explicitation des Connaissances (JFAEC).* AFIA-AFCET, PRC GRECO IA, Dourdan, 15-17 Avril 1992, France, p 29-46.

LE TRUNG, M. EL KOURSI B., HOURIEZ B., HADJ-MABROUK H. (1992).
« Knowledge base for safety analysis in unmanned metro system ». *COMPRAIL 92*, 18-20 August 1992, WASHINGTON DC, USA.

MEJRI L., HADJ MABROUK H., EL KOURSI M., HOURIEZ B. (1993).
« Un système expert d'aide à la génération des scénarios d'accidents basé sur l'apprentissage automatique ». ITTG 93, *Symposium International sur l'innovation technologique dans les transports guidés*. Lille, 28-30 septembre 1993, p 627-638.

MEJRI L., HADJ MABROUK H., EL KOURSI M., HOURIEZ B. (1993).
« Deux approches contextuelles et hors contexte basées sur l'apprentissage pour l'aide à la génération d'exemples. Application à la certification des systèmes de transport automatisés ». *Huitièmes Journées Francophones sur l'Apprentissage (JFA*). Saint-Raphaël, France, 29 Mars-2 Avril 1993.

MEJRI L., HADJ MABROUK H., EL KOURSI M., HOURIEZ B. (1992).
« Learning based assistance tool for the generation of scenarios for automated transport systems certification ». *11th European Annual Conference on Human decision making and manual control*. Valenciennes, France, 17-19 november 1992, 14p.

7.3. CONGRÈS NATIONAUX AVEC ACTES ET COMITÉ DE LECTURE

CHOPARD-GUILLAUMOT G., HADJ-MABROUK H., GANASCIA J.-G. (1996).
« Aide aux analyses préliminaires de risques des systèmes de transport guidés ». λμ 10, *10e Colloque national de fiabilité et maintenabilité*, France, Saint-Malo, tome 1, pp 378-386, 1-3 octobre 1996.

DAVID Y., LE TRUNG B., HADJ-MABROUK H. (1994).
« L'erreur humaine dans les systèmes de transport guidés ». *Journée spécialisée INRETS - L'erreur humaine : question de points de vue ?* Centre Reille, Paris 17 novembre 1994, 10p.

EL KOURSI M., LE TRUNG B., HADJ-MABROUK H., HOURIEZ B. (1992).
« Base de connaissances pour l'aide à l'analyse de sécurité des systèmes de transports terrestres automatisés ». *8ème colloque de fiabilité et de maintenabilité*, Grenoble 6-8 Octobre 1992, France.

HADJ-MABROUK H. (1998).
« Une méthode originale d'analyse préliminaire de risques ». λμ 11, *11e Colloque national de fiabilité et maintenabilité*, France, Arcachon, 29 septembre au 1er octobre 1998. (proposition)

HADJ-MABROUK H. (1996).
« La nécessité de prendre en compte l'erreur humaine dans l'analyse de sécurité et le développement des systèmes de transport guidés ». *OCTARES Éditions*, collection colloques, l'erreur humaine : question de points de vue ? France, pp 85-98, 1996.

HADJ-MABROUK H., DARRICAU M. (1996).
« SAUTREL : outil d'aide aux analyses des effets des erreurs de logiciels de sécurité dans les transports guidés ». λμ 10, *10e Colloque national de fiabilité et maintenabilité*, France, Saint-Malo, tome 2, pp 790-797, 1-3 octobre 1996.

HADJ-MABROUK H. (1995).
« L'apprentissage automatique : principes et exemple d'application au domaine de la sécurité ». JE'95*, Journées électronique et informatique pour la sûreté*, Commissariat à l'Énergie Atomique. Gif-sur-Yvette, 7-9 février 1995, pp 187-197.

HADJ-MABROUK H. (1994).
« CLASCA, un système d'apprentissage automatique dédié à la classification des scénarios d'accidents ». *9ème colloque international de fiabilité & maintenabilité*. La Baule, France, 30 Mai-3 Juin 1994, p 1183 - 1188.

HADJ-MABROUK H., MEJRI L., HOURIEZ B. (1992).
« Complémentarité des deux mécanismes d'apprentissage : CLASCA et CHARADE pour le développement d'un système à base de connaissances ». *3èmes Journées symbolique-numérique*. SFC-AFCET-AFIA, Paris 14-15 Mai 1992, France, p 157-170.

HADJ-MABROUK H., EL KOURSI M., HOURIEZ B., MILLOT P. (1991).
« Approche méthodologique d'aide à la certification des systèmes de transport automatisés basée sur l'apprentissage ». *5èmes Journées Acquisition de Connaissances*. Sète 17 Mai 1991, France.

HADJ-MABROUK H., DUPAS R., MILLOT P. (1989).
« Outil d'aide à la maintenance préventive par apprentissage ». *Forum Intelligence Artificielle et Systèmes Experts*, Paris 13-15 Décembre 1989.

7.4. RAPPORTS DE CONVENTIONS/CONTRATS

CHOPARD-GUILLAUMOT G., HADJ-MABROUK H., GANASCIA J-G. (1996).
« Un système d'aide aux analyses préliminaires de risques ». Convention INRETS/LAFORIA, rapport n° ESTAS/A-96-37, diffusion restreinte, 15 p, Arcueil, juin 1996.

CHOPARD-GUILLAUMOT G., HADJ-MABROUK H., GANASCIA J-G. (1995).
« Proposition d'un modèle générique d'analyses préliminaires de risques pour les transports guidés ». Rapport ESTAS/A-95-03, convention INRETS/LAFORIA, Arcueil, juin 1995, 45 p.

DARRICAU M., HADJ-MABROUK H., GANASCIA J-G. (1997).
« Acquisition et représentation des connaissances impliquées dans les spécifications des logiciels de sécurité. Application au système de pilotage automatique ». Convention INRETS/LAFORIA, rapport n° ESTAS/A-97-29, diffusion restreinte, 40 p, Arcueil, 10 juin 1997.

DARRICAU M., HADJ-MABROUK H., GANASCIA J-G. (1996).
« Méthodes contribuant à l'évaluation des logiciels de sécurité. Étude bibliographique ». Convention INRETS/LAFORIA, rapport n° ESTAS/A-96-62, diffusion restreinte, 44 p, Arcueil, novembre 1996.

HADJ-MABROUK H., JÉZÉQUEL R. (1997).
« Description générale du programme interministériel de recherche sur les transports PREDIT/ASCOT. Description de la fiche INRETS 17 ». Convention INRETS/ASCOT, rapport provisoire n° ESTAS/A-97-53, diffusion restreinte, Arcueil, 26 septembre 1997.

HADJ-MABROUK H. (1996).
« Projet FACTHUS : prise en compte des facteurs humains dans le développement des projets industriels ». Convention INRETS/DTT, rapport n° ESTAS/A-96-65, diffusion restreinte, 73 p, Arcueil, décembre 1996.

HADJ-MABROUK H., TABKA J. (1996).
« Projet VALIDE : méthode d'évaluation de la sécurité des transports guidés. Étape n° 1 : identification du problème ». Convention INRETS/LIMAV, rapport n° ESTAS/A-96-61, diffusion restreinte, Arcueil, mai 1996.

HADJ-MABROUK H. (1995).
« Le besoin d'introduire les facteurs humains dans le développement et l'analyse de sécurité des systèmes de transport guidés ». Rapport ESTAS/A-95-30, convention INRETS/DTT, Arcueil, juillet 1995, 55 p.

HADJ MABROUK H. (1994).
« Formalisme de représentation et d'acquisition des Analyses Préliminaires des Risques ». Rapport d'avancement des travaux de recherche dans le cadre du programme PREDIT-ASCOT-NOYAU N1-FICHE INRETS 17-SUJET 1-ETAPE 1. Arcueil, CR/A-94-46, 30 Juin 1994, 48 p.

HADJ MABROUK H., MEJRI L., EL KOURSI M., BIED-CHARRETON D., LE TRUNG B., HOURIEZ B. (1994).
« Base de scénarios d'accidents ». Convention Région Nord-Pas de Calais/INRETS-CRESTA /LAIH-UVHC. Dossier technique INRETS-CRESTA, Indice E, CR/A-94-16, Arcueil 21 Mars 1994, 213p.

HADJ MABROUK H. (1994).
« Bilan sur les connaissances acquises pour le développement d'un système d'aide à l'examen de la sécurité des transports guidés ». Résultat des sessions de recueil de connaissances du 15/02/90 au 22/02/94. Rapport de convention Région Nord-Pas de Calais/INRETS-CRESTA/LAIH-UVHC. CR/A-94-28, Arcueil 22 Avril 1994, 34p.

HADJ MABROUK H., BIED-CHARRETON D. (1993).
« Mise à jour de la BCHS : Base de Connaissances Historiques des Scénarios d'accidents potentiels ». Convention Région Nord-Pas de Calais/INRETS-CRESTA/LAIH-UVHC. Dossier technique INRETS-CRESTA, Indice C, CR/A-93-36, Arcueil Mai 1993.

HADJ MABROUK H., HOURIEZ B., MILLOT P. (1992).
« CLASCA et EVALSCA deux mécanismes d'apprentissage Symbolique-Numérique pour le développement d'un système à base de connaissances d'aide à la certification des systèmes de transport automatisés ». Rapport de fin de contrat de la convention Région Nord-Pas de Calais/INRETS n°89 0882 et du contrat VALUVAL-LAIH/INRETS-CRESTA du 15/01/91 n°90090065. LAIH, Université de Valenciennes, Juin 1992.

HADJ MABROUK H., HOURIEZ B., MILLOT P. (1991).
« Étude de faisabilité d'un système à base de connaissances pour l'aide à la certification des systèmes de transport automatisés ». Rapport de fin de contrat de la convention Région Nord-Pas de Calais/INRETS n°89 0882 et du contrat VALUVAL-LAIH/INRETS-CRESTA du 15/01/91 n°90090065. Laboratoire d'Automatique Industrielle et Humaine, Université de Valenciennes, Juin 1991.

HADJ MABROUK H., HOURIEZ B., MILLOT P. (1990).
« Développement d'un système d'aide à la certification des systèmes de transport automatisés ». Convention Région Nord-Pas de Calais/INRETS n°89 0882. Laboratoire d'Automatique Industrielle et Humaine, Université de Valenciennes. Deux rapports d'activité, Octobre 1990 et Juin 1991.

KAUTZMANN J., HADJ-MABROUK H. (1996).
« Étude bibliographique sur la prise en compte des facteurs humains ». Convention INRETS/COSINUS, rapport n° ESTAS/A-96-35, diffusion restreinte, 23 p, Arcueil, juin 1996.

KAUTZMANN J., HADJ-MABROUK H. (1996).
« Exemples de prise en compte des facteurs humains à la SNCF et à EDF ». Convention INRETS/COSINUS, rapport n° ESTAS/A-96-50, diffusion restreinte, 17 p, Arcueil, août 1996.

MEJRI L., HADJ-MABROUK H., HOURIEZ B., MILLOT P. (1995).
« Un système d'aide à la génération de scénarios contraires à la sécurité ». Rapport de fin de contrat, convention INRETS/LAMIH, Université de Valenciennes, janvier 1995, 31 p.

MEJRI L., HADJ MABROUK H., HOURIEZ B., BIED-CHARRETON D., BARANOWSKI F., MILLOT P. (1994).
« Validation de la maquette du système d'aide à la génération de scénarios contraires à la sécurité. Etape n°1 : validation de l'approche statique ». Rapport sur convention LAMIH-UVHC/INRETS-ESTAS. Université de Valenciennes, novembre 1994, 40p.

NDIAYE A., HADJ-MABROUK H. (1996).
« Apports et limites d'un outil d'aide aux analyses des effets des erreurs des logiciels ». Convention INRETS/LAMSADE, rapport n° ESTAS/A-96-36, diffusion restreinte, 17 p, Arcueil, juin 1996.

NDIAYE A., HADJ-MABROUK H. (1996).
« Identification de critères d'évaluation des A.E.E.L. à l'aide d'un système d'apprentissage : une étude de faisabilité ». Convention INRETS/LAMSADE, rapport n° ESTAS/A-96-52, rapport confidentiel, 24 p, Arcueil, septembre 1996.

7.5. RAPPORTS D'EXPERTISES ET D'ASSISTANCE TECHNIQUE

BIED-CHARRETON D., STUPARU A., HADJ MABROUK H. (1993).
« Conclusions de l'examen des méthodes de validation et d'homologation de la TVM 430 (Transmission Voie-Machine) du TGV Nord ». Rapport INRETS CR/A-93-32, Arcueil, Avril 1993, 64p.

HADJ-MABROUK H., BIED-CHARRETON D. (1995).
« Avis de l'INRETS sur le document Analyse Préliminaire des Risques (APR) du système KVBP/KVIM du projet ANTARES ». Rapport ESTAS/A-95-15, Arcueil, 16 mars 1995, 38 p.

HADJ MABROUK H. (1994).
« Examen du dossier Analyse Préliminaire des Risques (APR) du système KVBP/KVIM du projet ANTARES ». Rapport INRETS-ESTAS CR/A-94-64, Arcueil, 2 Décembre 1994, 35p.

HADJ MABROUK H., BIED-CHARRETON D. (1994).
« Évaluation des méthodes de développement, de validation et d'homologation du système ANTARES de signalisation, de contrôle de vitesse et d'aide à la conduite du RER-Ligne C-Paris. Étape 1 : Identification du problème ». Rapport INRETS CR/A-94-01, 3ème Édition, Arcueil, Avril 1994, 91p.

HADJ MABROUK, H. BIED-CHARRETON D. (1994).
« Évaluation des méthodes de développement, de validation et d'homologation du système ANTARES de signalisation, de contrôle de vitesse et d'aide à la conduite du RER-Ligne C-Paris. Étape 2.1. : Macro analyse au niveau système ». Rapport INRETS CR/A-94-10, Arcueil, Mai 1994, 79p.

HADJ MABROUK H., BIED-CHARRETON D. (1994).
« Examen des documents généraux (PDP, PSP) et de définitions (SBU, DSE) du système KVBP/KVIM du projet ANTARES. Bilan des remarques et questions ». Rapport INRETS CR/A-94-15, 2ème Édition, Arcueil, 11 Mars 1994, 25p.

HADJ MABROUK H., BIED-CHARRETON D., LE TRUNG B. (1993).
« Lien Fixe Transmanche : Expression formelle du choix de la vitesse du train et évaluation ». Rapport confidentiel, 1ère Édition, INRETS-CRESTA, CR/A-93-34, Arcueil, Mars 1993.

7.6. RAPPORTS DE RECHERCHE (INTERMÉDIAIRES OU D'ÉTAPE)

DARRICAU M., HADJ-MABROUK H. (1995).
« Le raisonnement à partir de cas : une étude bibliographique ». Rapport ESTAS/A-95-28, Arcueil, juin 1995, 20p.

HADJ-MABROUK H. (1997).
« Projet SAPRISTI : proposition d'une méthode et d'une maquette d'aide à l'élaboration et à la capitalisation des analyses préliminaires de risques ». Rapport n° ESTAS/A-97-66, 17p, Arcueil, 19 novembre 1997.

HADJ-MABROUK H., STUPARU A., JÉZÉQUEL R. (1997).
« Proposition d'un programme de recherche sur le retour d'expérience dans le domaine de la sécurité des systèmes de transports guidés ». Rapport n° ESTAS/A-97-67, 27p, Arcueil, 20 novembre 1997.

HADJ-MABROUK H. *avec la collaboration de STUPARU A.* (1997).
« Exemple de typologie d'accidents dans le domaine de la sécurité des systèmes de transport guidés ». Rapport n° ESTAS/A-97-47, 18 p, Arcueil, août 1997.

HADJ-MABROUK H. (1996).
« Exemples de systèmes de contrôle de vitesse dans les transports terrestres : principes de fonctionnement ». Rapport n° ESTAS/A-96-01, 16 p, Arcueil, janvier 1996.

HADJ MABROUK H. (1993).
« La théorie des sous-ensembles flous : concepts, principes de base et applications ». Étude bibliographique, Rapport INRETS-CRESTA, CR/A-93-60, Arcueil, Septembre 1993, 90 p.

HADJ MABROUK H., LE TRUNG B., BIED-CHARRETON D. (1993).
« Rôle de l'INRETS-CRESTA dans le processus de développement et d'exploitation d'un système de transport guidé ». INRETS-CRESTA, CR/A-93-54, Édition provisoire, Arcueil, Août 1993.

7.7. AUTRES RAPPORTS (NOTE D'INFORMATION)

HADJ-MABROUK H. (1995).
« Projet AVIS : acquisition et validation des connaissances de sécurité ». Bulletin de l'AFIA, n° 22, juillet 1995.

HADJ-MABROUK H., CHOPARD-GUILLAUMOT G. (1996).
« Éléments pour l'élaboration de conventions de recherche ». Rapport n° ESTAS/A-96-32, 16p, Arcueil, mai 1996.

7.8. CONFÉRENCES SUR INVITATION (SÉMINAIRES)

HADJ-MABROUK H., STUPARU A., BARANOWSKI F. (1997).
« Jusqu'où l'automatisation de la fonction de conduite pourra-t-elle être menée pour le réseau ferroviaire européen classique ? ». Institut des Transports et de Planification de l'Ecole Polytechnique Fédérale de Lausanne. INRETS-Arcueil, 3 septembre 1997, 60 p.

HADJ-MABROUK H. (1996).
« L'axe de recherche AVIS : des méthodes et des outils d'aide à l'élaboration et à l'évaluation des analyses de sécurité ». Journée cellule ASCOT, programme PREDIT, Villeneuve d'Ascq, 14 mai 1996, 29 p.

CHOPARD-GUILLAUMOT G., HADJ-MABROUK H. (1995).
« Le projet SAPRISTI : présentation et état d'avancement ». Exposé, Conseil scientifique du GRRT, Villeneuve d'Ascq, 14 juin 1995, 27 p.

HADJ-MABROUK H. (1995).
« Introduction des techniques d'intelligence artificielle dans le processus de construction de la sécurité ». Exposé, Conseil scientifique du GRRT, Villeneuve d'Ascq, 15 février 1995, 25 p.

HADJ-MABROUK H. (1994).
« Techniques d'apprentissage automatique pour l'aide à la classification et à l'évaluation des scénarios d'accidents. Application au domaine de la sécurité des transports guidés ». Pôle Intelligence Artificielle, INRETS-Arcueil, 18 novembre 1994.

HADJ-MABROUK H. (1994).
« L'analyse préliminaire des risques dans le domaine de la sécurité des transports guidés ». LAFORIA , Université de Paris VI, 21 septembre 1994.

HADJ-MABROUK H. (1992).
« ACASYA : Aide à la Certification par Apprentissage des SYstèmes de transport Automatisé ». GRRT, Lille, 20 octobre 1992

HADJ-MABROUK H. (1991).
« Apport des techniques d'apprentissage pour l'aide à la certification des systèmes de transport automatisés ». LAFORIA, Université de Paris VI, 6 Juin 1991.

DEUXIÈME PARTIE

CADRE ET MOTIVATIONS DE LA RECHERCHE

INTRODUCTION

Après une présentation des principales actions de recherche et d'expertise effectuées par l'unité de recherche ESTAS de l'INRETS en matière de sécurité et de certification des systèmes de transport, le présent chapitre détaille successivement le cadre, les motivations de ma recherche (PREDIT-ASCOT et CERTIFER), les principales composantes de l'axe de recherche « AVIS » (Acquisition et Validation des connaissances de Sécurité) et enfin les méthodes et techniques mises en œuvre pour développer cet axe de recherche.

1. PRESENTATION GÉNÉRALE DE L'INRETS-ESTAS

1.1. Présentation de l'INRETS

L'INRETS regroupe 400 personnes dont 200 chercheurs. Elle est placée sous la double tutelle du Ministère de la recherche et du Ministère des transports. Les missions publiques confiées à L'INRETS sont les suivantes :

- Effectuer, faire effectuer et évaluer des recherches pour l'amélioration des systèmes et moyens de transport et de circulation du point de vue technique, économique et social.
- Mener dans ces domaines des travaux d'expertise et de conseil.

L'INRETS est composé de 17 unités de recherche réparties sur 4 sites :

7 unités à Arcueil :
MAIA : Département Mathématiques Appliquées et Intelligence Artificielle
LTN : Laboratoire des Technologies Nouvelles
LPC : Laboratoire de Psychologie de la Conduite
DEST : Département Economique et Sociologie des Transports
DERA : Département Evaluation et Recherche en Accidentologie
DART : Département Analyse et Régulation du Trafic
CIR : Centre Informatique Recherche

5 unités à Lyon/Rhône-Alpes
LCB : Laboratoire des Chocs et de Biomécanique
LEN : Laboratoire Energie-Nuisances
LESCO : Laboratoire Ergonomie Santé Confort
LICIT : Laboratoire d'Ingénierie Circulation Transport
MMA : Département Modélisation Mécanique et Acoustique

1 unité à Salon de Provence : MA - Département Mécanismes d'Accidents

1 unité à Marseille : LBA - Laboratoire de Biomécanique Appliquée

3 unités à Villeneuve d'Ascq :
LEOST : Laboratoire Electronique, Ondes et Signaux pour les Transports
TRACES : Centre de Socio-Economie des Transports et de l'Aménagement
ESTAS : Evaluation des Systèmes de Transport Automatisés et de leur Sécurité (DUR : Gérard COUVREUR)

1.2. Présentation du département «ESTAS»

Répartie sur les sites de Villeneuve d'Ascq et d'Arcueil, ESTAS dispose d'un effectif de 15 personnes dont 11 chargés de recherche et Ingénieurs. La principale originalité du département ESTAS réside dans sa double compétence en matière de recherche et d'expertise. En matière d'expertise, ESTAS est sollicité depuis plusieurs années par les autorités publiques pour donner un avis sur la sécurité d'automatismes des systèmes de transports guidés tels que le VAL de Lille, MAGGALY de Lyon, le TVM 430 du TGV Nord, le Tunnel sous la Manche. Diverses évaluations technico-économiques de systèmes de métro et de transports intermédiaires (métro léger, bus en site propre) en France et à l'étranger ont également été réalisées à la demande des ministères. ESTAS apporte également aux constructeurs une aide technique et un soutien pour l'exportation, y compris hors Europe (USA, Egypte, Amérique du Sud).

Les activités de recherche du département ESTAS s'articulent autour de deux directions : la sécurité et l'exploitation des systèmes de transport automatisés. Dans le domaine de la sécurité, les recherches portent sur plusieurs thèmes : l'intelligence artificielle, les facteurs humains, les objectifs de sécurité et leurs répartitions sur les sous-systèmes, les architectures numériques réparties (aspect matériel), les méthodes formelles de conception et d'évaluation des logiciels, etc. Dans le domaine de l'exploitation, ESTAS conduit plusieurs recherches portant notamment sur le développement d'outils de simulation (comportement d'une ligne, d'un réseau,...), le développement des méthodes de régulation de trafic basées sur la logique floue et les réseaux de neurones, le développement des dispositifs pour améliorer la qualité de l'offre (améliorer l'accès des personnes à mobilité réduite aux transports en commun), le développement des systèmes d'aide au diagnostic des dispositifs électroniques d'un métro automatique ou d'un système de signalisation des lignes à grande vitesse. ESTAS participe également aux projets européens sur la sécurité des transports ESPRI, DRIVE....

2. DÉVELOPPEMENT, VALIDATION, HOMOLOGATION ET CERTIFICATION D'UN SYSTÈME

Le développement et l'exploitation d'un système de transport terrestre guidé font intervenir trois principaux acteurs (Figure 1) [Hadj-Mabrouk et al. 93] et [Hadj-Mabrouk 95b] :

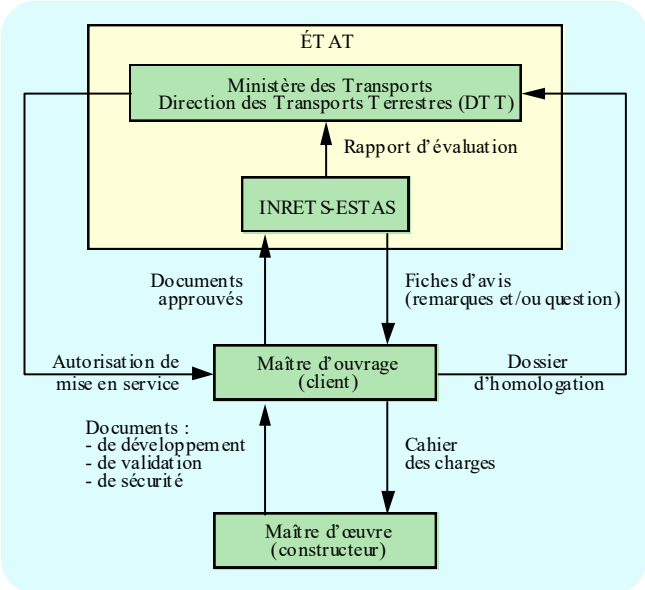

Figure 1 : principaux acteurs impliqués dans le développement d'un système de transport guidé [Hadj-Mabrouk et al. 93] et [Hadj-Mabrouk 95b]

- Le maître d'œuvre (ou le constructeur) développe et valide son système. Ceci consiste à apporter les preuves (démonstrations, calculs, résultats d'essais, …) que le système est conforme aux spécifications y compris celles relatives à la sécurité.
- Le maître d'ouvrage (ou le client) homologue le système. L'homologation est prononcée par le client au vu des résultats de la validation réalisée par le constructeur, du dossier de sécurité et des essais et vérifications qu'il juge utile de réaliser lui même par ailleurs.
- L'État ou la collectivité territoriale veille au respect des exigences techniques de sécurité par l'ensemble des intervenants. Il délivre les autorisations de mise en service et peut retirer ces autorisations en cas de non respect des exigences de sécurité que doit satisfaire le système lors de sa conception, de sa réalisation et de son exploitation. Cette autorisation est accordée au vu d'un dossier d'homologation conçu par le Maître d'ouvrage et d'un rapport d'évaluation (ou de certification) élaboré par l'INRETS-ESTAS.

Les chercheurs et experts de l'INRETS-ESTAS sont chargés du contrôle du système essentiellement sur le plan de la sécurité et ont accès à l'ensemble des documents techniques ainsi qu'aux différentes installations d'essais. Le paragraphe suivant présente les principales actions d'assistance technique et d'expertise confiées à l'INRETS-ESTAS.

3. PRINCIPALES ACTIONS D'EXPERTISE ET D'ASSISTANCE TECHNIQUE CONFIÉES A L'INRETS-ESTAS PAR LES AUTORITÉS PUBLIQUES

l'INRETS-ESTAS a rempli plusieurs missions d'assistance technique et d'expertise dans le domaine de la sécurité des transports guidés et plus précisément dans la sécurité des systèmes de contrôle/commande. On peut citer notamment : VAL-Lille, VAL-Toulouse, VAL-Orly, MAGGALY-Lyon, POMA-2000-Laon, ARAMIS, METEOR-Paris, TVM430-TGV-Nord, LIEN-FIXE-TRANSMANCHE. La nature des travaux confiés à l'INRETS, par les services compétents de l'Etat, diffère d'une mission à l'autre. L'INRETS se donne comme objectif principal l'examen des méthodes de développement, de validation et d'homologation des équipements matériels et logiciels assurant des fonctions de sécurité. Les avis émis par l'INRETS, pour aider l'Etat à fonder une appréciation sur le respect des exigences de sécurité, portent notamment sur [Hadj-Mabrouk et al. 93] et [Hadj-Mabrouk et al. 96]:

- l'adéquation, la complétude, la cohérence et la traçabilité des méthodes et techniques utilisées par le maître d'oeuvre pour *construire la sécurité* (au niveau système, logiciels et matériels) ;
- l'organisation et les méthodes de travail des différentes équipes mises en place par le constructeur et le client pour *administrer et valider la sécurité*, au regard notamment de l'indépendance entre les équipes "développement" et les équipes "sécurité" ;
- la bonne application des principales normes suivies pour la réalisation du projet ;
- l'acceptabilité des objectifs de sécurité recherchés par le maître d'ouvrage ainsi que sur les allocations de sécurité effectuées à différents niveaux ;
- la qualité de la documentation fournie par le constructeur et le client au regard de la clarté et de l'exhaustivité ;
- les moyens mis en oeuvre pour développer, valider et homologuer les équipements matériels et logiciels de sécurité.

Les travaux présentés dans ce mémoire, s'inscrivent dans le cadre de la phase d'évaluation de la complétude et de la cohérence des méthodes de *construction de la sécurité*. Le paragraphe suivant présente les principales activités de construction de la sécurité mises en œuvre par le constructeur.

4. PROCESSUS DE MISE EN SECURITE D'UN SYSTÈME DE TRANSPORT GUIDÉ

Généralement, le processus de construction de la sécurité d'un système (figure 2) comporte plusieurs analyses complémentaires hiérarchisées [Hadj-Mabrouk 92, 93, 94a, 95a, 96a] : L'analyse préliminaire de risques, l'analyse fonctionnelle de la sécurité, et l'analyse de la sécurité du produit réalisé.

L'analyse préliminaire de risques (APR) a pour but d'identifier essentiellement les accidents potentiels liés au système et à ses interfaces afin de les évaluer et de proposer des solutions pour les supprimer, les réduire ou les contrôler. Les résultats de cette analyse permettent de définir les exigences et critères de sécurité (de haut niveau) du système, d'établir le cadre de la démonstration de la sécurité ainsi que les grandes lignes des analyses de sécurité situées en aval (analyse de la sécurité fonctionnelle, analyse de la sécurité des logiciels, analyse de la sécurité des matériels).

L'analyse fonctionnelle de la sécurité (AFS) a comme objectif de justifier que l'architecture de conception du système est sécuritaire vis à vis des accidents potentiels identifiés par l'analyse préliminaire de risques et par conséquent de s'assurer que toutes les dispositions de sécurité sont prises en compte pour couvrir les dangers ou les accidents potentiels. Ces analyses fournissent des critères de sécurité (de bas niveau) pour la conception du système et la réalisation des équipements matériels et logiciels de sécurité. Elles imposent aussi des critères de sécurité liés au dimensionnement, à l'exploitation et à la maintenance du système. Les AFS peuvent mettre en évidence des scénarios contraires à la sécurité qui nécessitent une reprise de la spécification [Hadj-Mabrouk 93, 94b].

L'analyse de la sécurité du produit réalisé concerne l'analyse de la sécurité des logiciels (ASL) et l'analyse de la sécurité des matériels (ASM). L'ASL est généralement basée sur la méthode d'analyse des effets des erreurs du logiciel (AEEL) ainsi que sur les lectures critiques de code. L'ASM porte notamment sur les cartes électroniques et les interfaces définies comme étant de sécurité. Cette analyse met en œuvre deux types d'analyses :

1. une analyse de type « inductif » par analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) complétée par une méthode des combinaisons de pannes résumées (MCPR) ;
2. une analyse de type « déductif » par recherche de scénarios contraires à la sécurité [Hadj-Mabrouk 94c, 94d] mettant en défaut le respect des critères de sécurité issus de l'analyse fonctionnelle de la sécurité. Cette analyse déductive nécessite généralement le recours à la méthode de l'arbre des causes (MAC).

En effet, l'ensemble de ces méthodes d'analyse de sécurité repose sur deux démarches fondamentales, l'une de type « inductive » et l'autre de type « déductive » [Lievens 76], [Villemeur 88] : Dans la démarche inductive, le raisonnement va du plus particulier au plus général, ce qui conduit à une étude détaillée des effets d'une défaillance sur le système et son environnement. Autrement dit, les méthodes inductives partent des événements élémentaires, soit pour rechercher directement les conséquences, soit pour identifier les combinaisons d'événements qui peuvent avoir des conséquences autres que mineures. L'APR, L'AMDE, l'AEEL et la MCPR sont des exemples de méthodes inductives. Dans la démarche déductive, le raisonnement va du plus général au plus particulier de telle façon que, face au système défaillant, on déduit les causes de la défaillance. La principale méthode déductive est la méthode de l'arbre des causes (MAC). Généralement, l'analyse de sécurité d'un système complexe nécessite de la part des experts du domaine la mise en oeuvre d'un processus de construction de la sécurité itératif faisant intervenir à la fois des méthodes inductives et déductives.

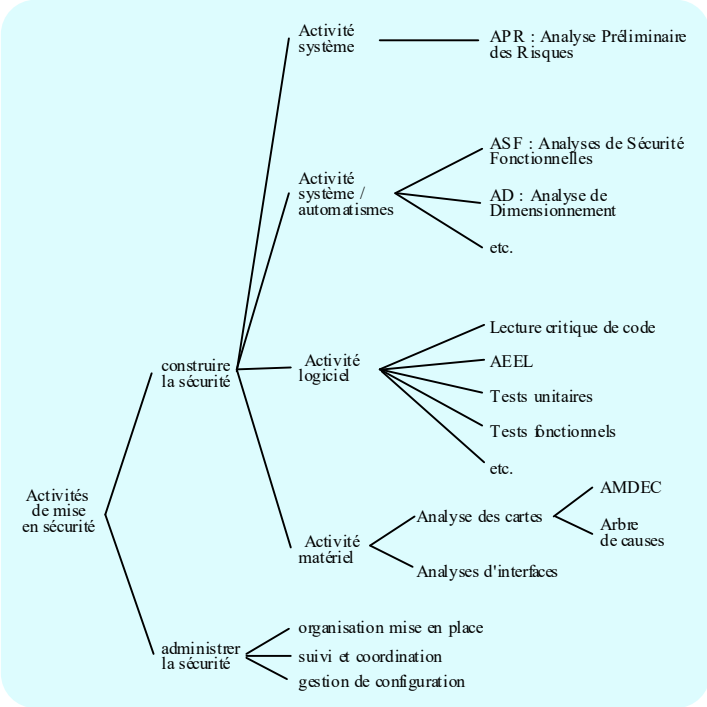

Figure 2 : processus de mise en sécurité des automatismes d'un systèmes de transport guidé [Hadj-Mabrouk 95a]

Dans ce processus de construction de la sécurité, l'une des difficultés consiste à s'assurer de l'exhaustivité et de la cohérence des différentes analyses (APR, ASF, ASL, ASM) par la recherche des risques et scénarios contraires à la sécurité non pris en compte lors de l'élaboration du dossier de sécurité. L'étude présentée dans ce mémoire vise le développement des outils logiciels à base de connaissance pour l'aide à l'évaluation de la complétude et de la cohérence de ces analyses de sécurité.

5. CADRE DE LA RECHERCHE

L'étude s'inscrit principalement dans le cadre du Programme de Recherche et Développement pour l'Innovation et la Technologie des Transports Terrestres PREDIT-ASCOT. Elle a pour principal objectif d'aider les organismes de certification dans leur mission d'analyse et d'examen des études de sécurité. Les deux paragraphes suivants présentent successivement une description du programme interministériel de recherche sur les transports PREDIT-ASCOT et de la nouvelle agence de certification ferroviaire CERTIFER dans laquelle je me suis impliqué en participant à l'élaboration des statuts.

5.1. Programme inter-ministériel de recherche sur les transports PREDIT-ASCOT

L'organisation générale du programme PREDIT-ASCOT et l'articulation des différents thèmes de recherches impliqués sont illustrées par la figure 3 présentée ci-après [Hadj-Mabrouk, Jézéquel 97]. Ce programme fait intervenir plusieurs thèmes d'études : transports guidés, technologies des véhicules routiers, transports de marchandises, etc. Le thème « Transports guidés », dans lequel s'inscrivent mes activités de recherche, est structuré en quatre sous-thèmes : grandes vitesses, nouveaux matériels et composants technologiques, systèmes de contrôle-commande des circulations et nouveaux systèmes urbains et suburbains.

En 1990, dans le cadre du sous-thème "systèmes de contrôle-commande des circulations", les ministères concernés ont demandé, pour pouvoir mettre en place un financement, de préparer la définition d'un grand programme baptisé ASCOT (Automatismes de Sécurité et Systèmes de Contrôle-commande dans les Transports guidés). Début 1994, le programme ASCOT a été accepté par le Ministère et les travaux sont en cours de développement. Le déroulement de ce programme ASCOT, présidé par Monsieur Jean-Paul PERRIN, est planifié sur une durée de 5 ans à partir de 94.

Depuis quelques années, la part "contrôle-commande des circulations des transports guidés" n'a cessé d'augmenter et représente aujourd'hui un pourcentage non négligeable du coût global (vis-à-vis du génie civil et du matériel roulant). Ceci est dû à plusieurs facteurs liés notamment à la sécurité, à la qualité du service, à l'évolutivité, au confort et aux performances exigées. Dans ce contexte, il est donc nécessaire de développer et mettre à la disposition des concepteurs des systèmes de contrôle-commande des outils adaptables, maintenables, réutilisables et meilleur marché.

Compte tenu de l'ampleur du problème et en vue d'assurer une cohérence globale tout en minimisant les frais de recherche, GEC-ALSTHOM, MATRA TRANSPORT, CSEE TRANSPORT, la RATP, la SNCF et l'INRETS ont décidé d'unir leurs efforts. L'objectif final du programme ASCOT consiste à mettre à la disposition des services techniques des différents intervenants de la profession (sociétés exploitantes, industriels et organismes de certification) les moyens d'accès à un atelier système de référence, à des outils pour la conception formelle des logiciels, à des architectures de traitement et d'échange, etc. L'objectif de l'atelier système de référence de mieux maîtriser les systèmes de transport guidés et notamment la partie concernant le contrôle-commande. Il permettra en particulier : de mieux maîtriser la qualité de conception, de la réalisation et de la validation, de mieux répondre aux besoins des voyageurs, des exploitants et des "mainteneurs" et enfin de respecter les objectifs en matière de sécurité, de disponibilité, de performance et d'adaptabilité.

L'objectif est de disposer de méthodes, d'outils et de standards d'échange qui puissent donner à l'ensemble de la profession du transport guidé un langage commun et une capacité tout au long des principales phases de vie du système de commande et de contrôle : rédaction du cahier des charges, spécification du système, conception du système, etc. L'ensemble de ces études se répartit en deux fiches associées chacune à un sujet :

- Sujet 10 SNCF : définition de l'atelier système ;
- Sujet 17 INRETS (proposé par mes soins) : Introduction des techniques d'Intelligence Artificielle dans le processus d'analyse de sécurité et de certification des systèmes de transport guidés.

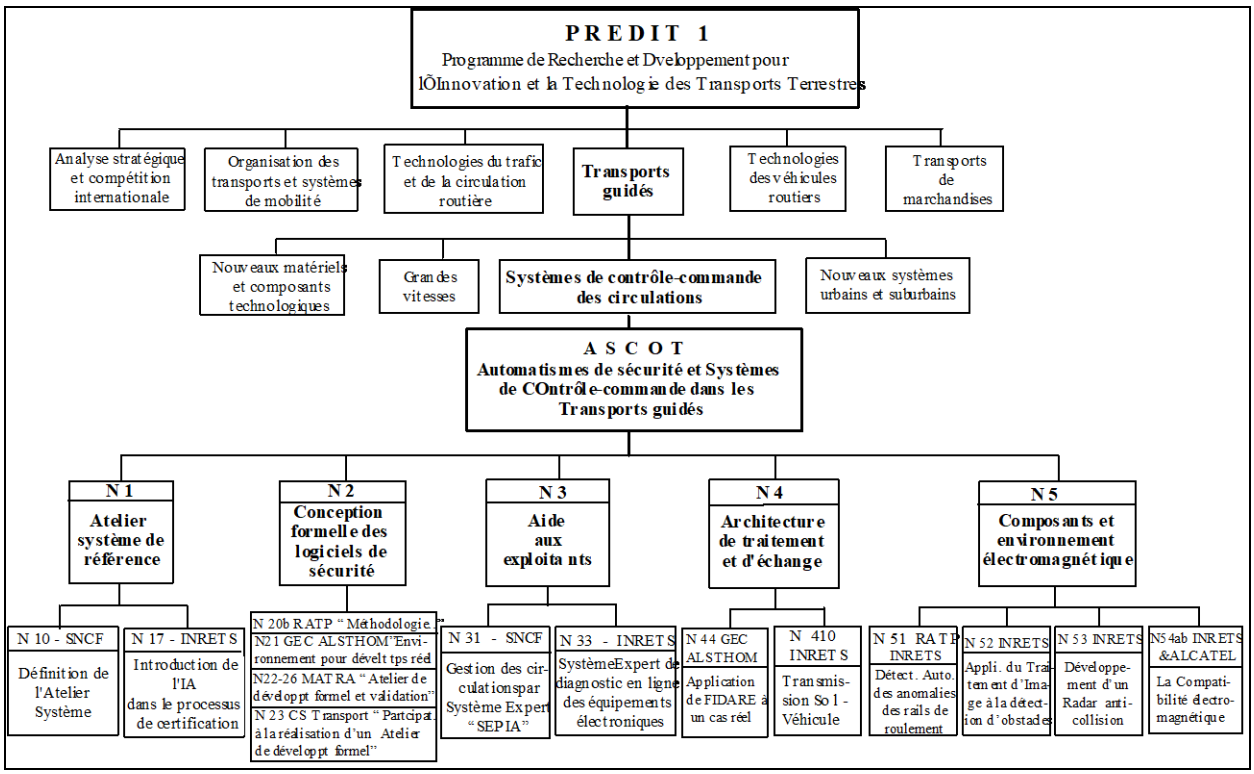

Figure 3 : Organisation et projets du programme PREDIT - ASCOT [Hadj-Mabrouk et Jézéquel 97].

Mes travaux de recherche, qui sont soutenus par le programme PREDIT-ASCOT-NoyauN1-FicheINRETS17, intéressent également la nouvelle agence de certification ferroviaire CERTIFER présentée ci-après.

5.2. Agence de certification ferroviaire CERTIFER

En décembre 1995, l'INRETS, la RATP, la SNCF et la Fédération des industries ferroviaires (FIF) ont constitué une association pour l'étude d'un organisme français de certification ferroviaire (AEOCF). La forme juridique retenue est une association régie par la loi du 1er Juillet 1901. Le terme certification désigne l'intervention (ou l'action) d'une tierce partie qui atteste la conformité à un "référentiel". Dans les autres cas, on parle plutôt d'homologation. Jusqu'à présent en France, l'homologation ferroviaire est effectuée essentiellement par les exploitants comme la SNCF ou la RATP. Compte tenu des besoins d'échanges exprimés au sein de l'Union Européenne (harmonisation des moyens), la certification par une tierce partie est devenue indispensable notamment dans le domaine de la sécurité ferroviaire. En effet, les principes de l'homologation ne pouvaient être laissés en l'état, à cause des préceptes juridiques, des trafics terrestres et des marchés ferroviaires Européen. L'évolution des esprits s'est accélérée en 1994 sous l'effet du projet de directive 96/48 relatif à l'interopérabilité du Réseau Européen des trains à grande vitesse. L'objectif de ce projet de directive est double :

1. permettre, sur le futur réseau européen de lignes à grande vitesse, la libre circulation des trains conçus à cet effet, sans entraves techniques ou réglementaires ;
2. la création d'un marché unique de composants, sous-ensembles et sous-systèmes dans l'Union Européenne.

Cette directive exige que tout produit ou service de son domaine appelé à être mis sur le marché doit être certifié (évaluer la conformité à un référentiel ou à des exigences essentielles) par un organisme indépendant notifié par un état membre auprès de la Communauté Européenne. La FIF, la RATP, la SNCF et l'INRETS se sont donc associés pour créer en février 97 l'agence de certification ferroviaire CERTIFER. Dans le domaine des transports guidés et notamment ferroviaires, les principaux objectifs de cette association sont les suivants (figure 4) :

- Evaluer la conformité aux textes législatifs et réglementaires, spécifications techniques, normes ou tout autre référentiel :
  . Des produits, sous-systèmes ou systèmes et de leur mode d'utilisation ;
  . Des services et de leur mode de réalisation,
  Et de les certifier ;
- Contrôler et/ou surveiller, pendant la validité d'un certificat, le maintien de la conformité au référentiel utilisé lors de la certification ;
- Contribuer à des travaux de réglementation et de normalisation ;

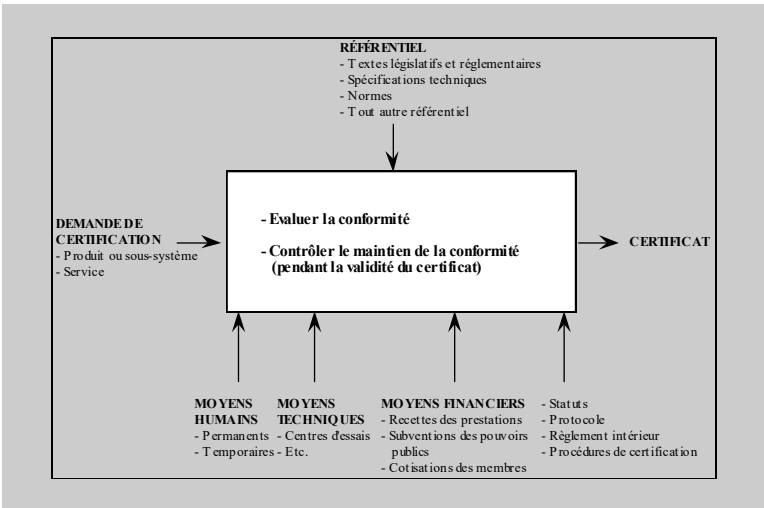

Figure 4 : Objectif de l'agence de certification ferroviaire CERTIFER

L'agence de certification ferroviaire est en mesure d'exercer des activités de certification dans deux domaines : le domaine réglementaire et le domaine volontaire. Dans le domaine réglementaire, CERTIFER doit répondre aux exigences de la direction n° 96/48 du 23 Juillet 96 du Conseil de l'Union Européenne relative à l'interopérabilité du réseau européen de trains à grande vitesse qui spécifie à l'article 20 qu'il doit être fait appel à des organismes, notifiés par un état membre, pour effectuer toute attestation de conformité. Dans le domaine volontaire, un certificat délivré par CERTIFER sera un véritable gage de qualité des produits ou services.

Ce certificat apportera en effet, une plus value indéniable au système, sous-système ou composant certifié. Les figures 5 et 6 schématisent le principe de fonctionnement et la composition de l'agence CERTIFER. Pour assurer ses missions, CERTIFER a mis en place une structure permanente et une structure temporaire. La structure permanente comprend essentiellement le Directeur Général, le secrétariat technique, les comités sectoriels, le coordinateur-Evaluateur et le conseil de surveillance et d'appel. L'association fait appel également à des structures temporaires (entités compétentes extérieures) qui peuvent être des laboratoires, des experts, des auditeurs, etc.. Cette structure permet d'effectuer notamment des travaux d'évaluation et d'essais.

Le secrétariat technique instruit les demandes de certification, désigne le coordinateur-évaluateur, gère la liste des entités compétentes, présente avec le coordinateur-évaluateur le rapport final au comité sectoriel concerné, etc... Les comités sectoriels ont pour objet de statuer sur la délivrance des certificats, intervenir dans certains litiges avec le client et garantir le répertoire des entités compétentes. Les certificats de conformité sont signés conjointement par les Présidents des Comités sectoriels et le Directeur Général. Le coordinateur-évaluateur, qui demeure l'interlocuteur technique du demandeur, arrête conjointement avec le secrétariat technique les conditions nécessaires au programme de certification (notamment en choisissant les entités compétentes), coordonne la réalisation du programme de certification, élabore le rapport final et participe à sa présentation au comité sectoriel concerné.

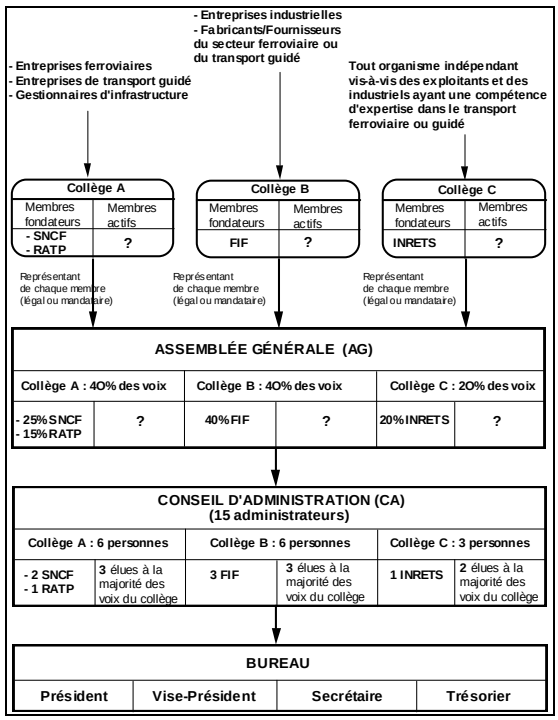

Figure 5 : Composition de l'agence de certification ferroviaire CERTIFER

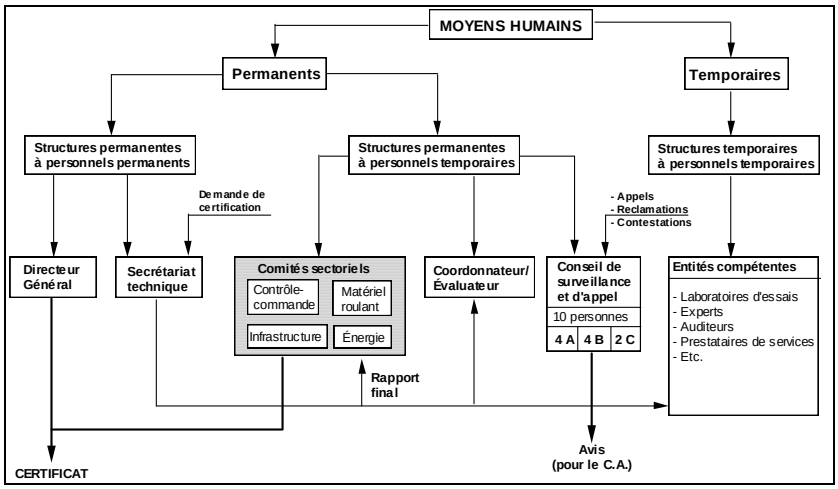

Figure 6 : Fonctionnement de l'agence de certification ferroviaire CERTIFER

6. INTRODUCTION AU THÈME DE RECHERCHE « AVIS »

6.1. Organismes demandeurs ou financeurs

L'axe de recherche « AVIS » qui vise le développement des méthodes, techniques et outils logiciels destinés à renforcer et systématiser les démarches usuelles d'analyse et d'évaluation de la sécurité, est soutenu par plusieurs organismes : Programme interministériel de recherche sur les transports (PREDIT-ASCOT), Direction des Transports Terrestres du Ministère des transports (DTT), Groupement régional de recherche sur les transports du Nord-Pas-de-Calais (GRRT), Société Nationale des Chemins de Fer Français (SNCF), Régie Autonome des Transports Parisiens (RATP), Agence de certification ferroviaire (CERTIFER), Centre technique des industries mécaniques (CETIM), Centre Produit Neuf de GIEN - Département méthodes de conception des ascenseurs (OTIS) et MATRA Transport.

6.2. Moyens humains

Les moyens humains mis en œuvre pour développer l'axe de recherche « AVIS » sont essentiellement des doctorants et stagiaires :

Chargé de recherche : Habib HADJ-MABROUK

Doctorants :
- Lassaâd MEJRI__ bourse Région/INRETS __ Thèse soutenue le 6/12/95 au LAMIH de l'UVHC
- Gilles CHOPARD-GUILLAUMOT __ bourse MESR __ Thèse démarrée en octobre 1994
- Bertrand TELLE __ bourse Région/INRETS __Thèse démarrée en novembre 1995
- Myriam DARRICAU __ bourse MESR __ Thèse démarrée en décembre 1995

Stagiaires (DEA, DESS, Ingénieur) :
- CAUDRON C.
- DARRICAU M.
- DAUFES S.
- DERENTY V.
- GABER K.
- KAUTZMANN J.
- MEJRI L.
- NDIAYE A.
- RAÏS F.

6.3. Motivations des travaux de recherche

L'autorisation de mise en service d'un système de transport guidé est accordée par les services compétents de l'État au vu d'un dossier d'homologation conçu par le maître d'ouvrage (comme la SNCF) et d'un rapport d'évaluation (ou de certification) élaboré par l'INRETS. Cette autorisation peut être retirée en cas de non respect des exigences de sécurité que doit satisfaire le système. Dans le cadre de ses missions d'expertise et d'assistance technique, l'INRETS procède donc pour le compte de la Direction des transports terrestres (DTT) du ministère des Transports à l'évaluation de dossiers de sécurité de systèmes de transport guidés tels que le Val de Lille, le système de contrôle de vitesse TVM430 du TGV-Nord ou le métro Maggaly de Lyon. Ces dossiers comportent plusieurs analyses de sécurité hiérarchisées telles que les analyses préliminaires de risques, les analyses fonctionnelles de sécurité ou les analyses de sécurité des logiciels. Ces analyses sont réalisées par les constructeurs, MATRA Transport ou GEC-Alsthom par exemple. Il convient d'examiner ces analyses avec le plus grand soin, tant la qualité de celles-ci conditionne *in fine* la sécurité des usagers des systèmes de transport.

Or, si l'analyse de la sécurité représente l'une des tâches fondamentales du processus de mise en sécurité d'un système de transport, elle n'en demeure pas moins aujourd'hui la pierre d'achoppement. En effet, l'analyse attentive de ce processus permet d'en révéler certaines lacunes [Hadj-Mabrouk 96b] :

- les méthodes usuelles d'analyse de sécurité ne font pas toujours l'objet d'un consensus et les usages sont parfois éloignés des rares recommandations théoriques. De ce fait, les formats de représentation des résultats des analyses sont souvent extrêmement variés d'un constructeur à l'autre ;
- la terminologie, les démarches et les concepts liés aux analyses de sécurité sont très fluctuants, voire contradictoires d'un système de transport à l'autre ;

- l'élaboration et l'évaluation d'un dossier de sécurité sont des exercices particulièrement délicats et fastidieux qui ne sont pas toujours soutenus par une stratégie formalisée. En effet, l'exhaustivité et la cohérence des analyses demeurent essentiellement fondées sur le savoir-faire, l'intelligence et l'intuition des experts du domaine ;
- enfin, l'erreur humaine reste très présente dans les transports guidés et elle n'est pas prise en compte de façon formelle dans les analyses de sécurité. Aussi le processus de mise en sécurité d'un système doit-il désormais prendre en compte non seulement les erreurs au niveau système, logiciel et matériel (comme c'est le cas actuellement) mais aussi au niveau humain.

Afin de mieux appréhender ces lacunes, et de tenter, le cas échéant, de les combler, j'ai défini un axe de recherche baptisé « AVIS » (Acquisition et Validation des connaissances de Sécurité). Le paragraphe suivant présente les principales composantes de cet axe de recherche.

6.5. PRINCIPALES COMPOSANTES DE L'AXE DE RECHERCHE « AVIS »

L'axe de recherche « AVIS » a pour ambition d'améliorer l'élaboration et l'évaluation des différentes analyses de sécurité, en traquant l'erreur non seulement au niveau système, matériel et logiciel, mais aussi au niveau humain, selon deux axes d'investigation [Hadj-Mabrouk 96a]:

1. un axe méthodologique, en s'interrogeant sur les perfectionnements possibles des démarches usuelles d'analyse de sécurité et en proposant des méthodes et stratégies d'évaluation de ces analyses en termes de cohérence, de complétude, de traçabilité...
2. un axe opérationnel, en développant des outils logiciels d'aide à la conception et à l'examen des analyses de sécurité qui intègrent notamment des systèmes d'acquisition, de modélisation, de capitalisation et d'évaluation de ces analyses.

« AVIS » vise le développement des méthodes, techniques et outils logiciels permettant d'une part la capitalisation des connaissances en matière d'analyse de sécurité et d'autre part d'aider les organismes de certification dans leurs missions d'expertise. L'objectif de cet axe de recherche est triple [Hadj-Mabrouk 96b] :

- faciliter les missions d'expertise et d'assistance technique confiées à l'INRETS-ESTAS par l'État en stimulant la création de scénarios d'accidents et en rationalisant et systématisant la démarche usuelle d'examen de la sécurité ;
- aider les acteurs impliqués dans le développement des systèmes de transport guidés et notamment les organismes de certification dans leur tâche cruciale d'évaluation des études de sécurité ;
- capitaliser et pérenniser l'expertise en matière de sécurité et de certification qui se caractérise par sa rareté, sa vulnérabilité et sa répartition entre les mains de plusieurs experts.

L'axe de recherche « AVIS » est composé de sept projets complémentaires illustrés à la figure 7 et détaillés dans le chapitre suivant [Hadj-Mabrouk 96c]:

1. SAPRISTI : système à base de connaissances pour l'aide à l'élaboration et à l'évaluation des analyses préliminaires de risques (APR),
2. ACASYA : système d'aide à la capitalisation, à la classification, à l'évaluation et à la génération des scénarios d'accidents,
3. SAUTREL : système d'aide aux analyses des effets des erreurs de logiciels (AEEL) de sécurité basé sur le raisonnement à partir de cas,
4. SASEM : système à base de connaissances pour l'aide à l'analyse des modes de défaillance, de leurs effets et de leur criticité des équipements matériels,
5. FACTHUS : méthode d'intégration des facteurs humains dans l'analyse de sécurité et le développement des systèmes,
6. SPECIALS : méthode de spécification et d'aide à l'évaluation des logiciels critiques de sécurité basée sur l'utilisation conjointe des techniques du génie cognitif et du génie logiciel,
7. VALIDE : méthode de validation des connaissances de sécurité.

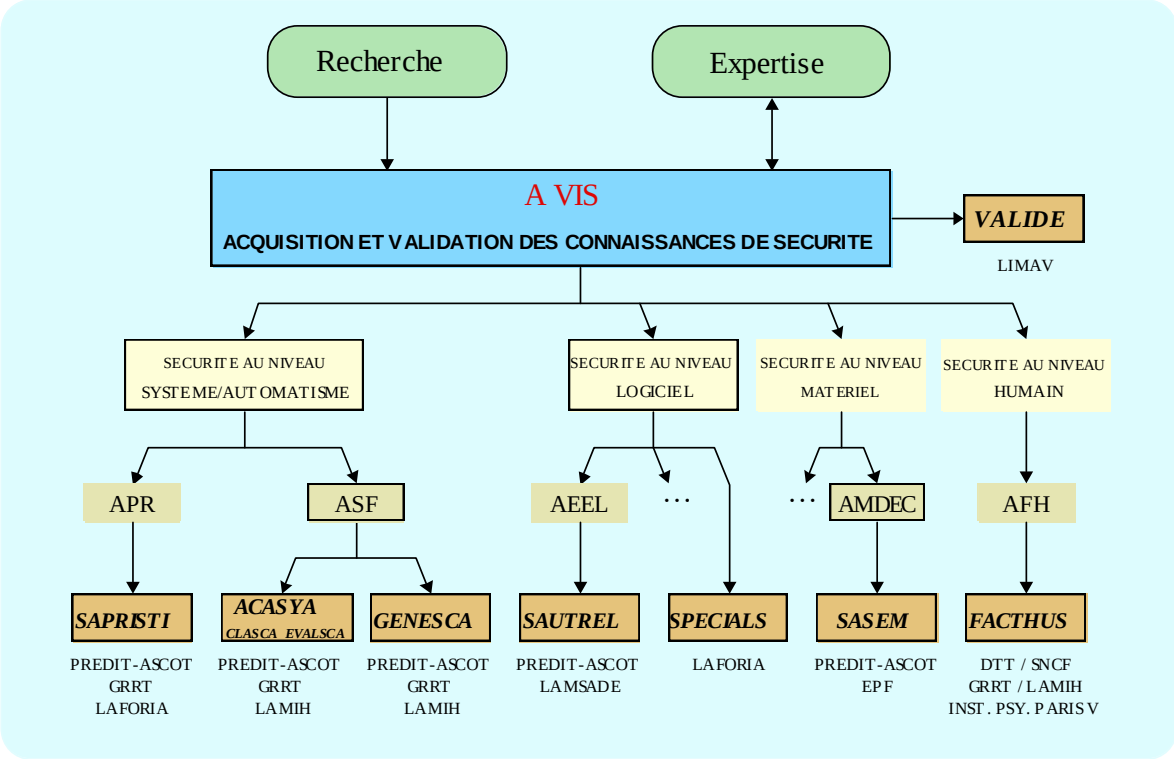

Figure 7 : composantes de l'axe de recherche AVIS [Hadj-Mabrouk 96c]:

Conformément au processus de construction de la sécurité décrit dans le paragraphe 4, ces projets visent l'amélioration des méthodes conventionnelles d'élaboration et d'évaluation de la sécurité au niveau système, matériel et logiciel. Nous remarquons dans la figure 7 l'introduction dans ce processus d'un autre niveau d'analyse qui nous semble essentiel pour améliorer la sécurité du système : le niveau humain. Nous montrons plus loin que cette composante liée aux facteurs humains n'est pas encore prise en compte dans le processus d'analyse de sécurité et qu'elles sont les approches envisagées pour intégrer les facteurs humains dès la phase de spécification du système.

7. MÉTHODES ET TECHNIQUES MISES EN OEUVRE POUR DÉVELOPPER « AVIS »

L'approche suivie pour concevoir et mettre en œuvre l'axe de recherche AVIS est centrée sur l'emploi des techniques d'intelligence artificielle et notamment sur l'utilisation des méthodes d'acquisition, de représentation et de validation de connaissances, d'apprentissage symbolique automatique et des systèmes à base de connaissances [Hadj-Mabrouk 91, 92, 93, 94a, 95a, 95c, 96a, 97]. En effet, malgré l'intérêt indéniable des méthodes usuelles d'analyse et d'évaluation de la sécurité, l'exhaustivité de l'analyse demeure essentiellement fondée sur le savoir-faire, l'intelligence et l'intuition de l'expert humain. Or, une étude attentive des mécanismes de raisonnement de l'expert, de ses stratégies et heuristiques de résolution de problème, montre qu'il fait principalement intervenir des données symboliques, évolutives, qualitatives et qu'il fait simultanément appel à des inférences de type inductif, déductif, par analogie,... C'est ce qui nous a conduit à recourir aux techniques d'Intelligence Artificielle afin de systématiser la démarche des experts et par conséquent de renforcer les méthodes conventionnelles d'analyse de sécurité.

En effet, les modes de raisonnement utilisés en matière d'analyse de sécurité (inductif, déductif, par analogie…) ainsi que la nature même des connaissances de sécurité (incomplètes, évolutives, empiriques, qualitatives…) confirment qu'une solution informatique conventionnelle n'est pas adaptée et que le recours aux techniques de l'intelligence artificielle (IA) semble mieux approprié [Hadj-Mabrouk 93]. L'IA s'efforce de créer des machines capables d'un comportement intelligent et a pour vocation ambitieuse de doter l'ordinateur de quelques unes des facultés de l'esprit humain : apprendre, reconnaître, raisonner ou encore s'exprimer à l'aide d'un langage. Pour nos travaux, nous avons eu recours essentiellement à trois aspects particuliers du domaine de l'IA : l'acquisition de connaissances (AC), l'apprentissage automatique (AA) et les systèmes à base de connaissances (SBC).

L'élaboration de la base de connaissances d'un SBC nécessite le recours aux techniques et méthodes d'AC pour recueillir, structurer puis formaliser les connaissances. L'AC n'a pas permis, à elle seule, d'extraire efficacement certaines connaissances expertes d'analyse de sécurité. Aussi, l'utilisation conjointe de l'AC et de l'AA apparaît-elle comme une solution très prometteuse. L'approche retenue pour développer l'ensemble des outils d'aide à l'analyse de la sécurité implique deux grandes activités [Hadj-Mabrouk 92] et [Hadj-Mabrouk et al 92] :

1. Extraire, formaliser et archiver les situations d'insécurité de façon à constituer une bibliothèque de cas types couvrant l'ensemble du problème. Cette activité a nécessité le recours aux techniques d'acquisition de connaissances ;
2. Exploiter les connaissances historiques archivées afin d'en dégager un savoir-faire en analyse de sécurité susceptible d'aider les experts à juger l'exhaustivité de l'analyse de sécurité proposée par le constructeur. Les approches mises en œuvre pour cerner cette deuxième activité sont fondées sur l'emploi des méthodes d'apprentissage automatique.

Les paragraphes suivants présentent ces deux activités impliquées dans la méthodologie d'analyse de la sécurité.

7.1. Systèmes à base de connaissances (SBC)

Avant d'aborder le problème de l'acquisition de connaissances, il convient de rappeler les principales caractéristiques d'un SBC. Cette présentation est faite sans en détailler les spécificités et le fonctionnement, fort bien décrits par ailleurs dans [Lauriere 84], [Farreny 85], [Farreny et Ghallab 87], [Benchimol 86], [Cordier 87] et [Hart 88]. Depuis la naissance de l'informatique, les ordinateurs sont considérés comme des machines à programmer. Il existe une grande variété de langages de programmation qui possèdent en commun les caractéristiques suivantes : ils ordonnent à la machine des opérations déterminées, ces opérations sont elles-mêmes entrées de façon ordonnée, figée et seuls les informaticiens peuvent y accéder. Cela limite donc leur intérêt car, si la machine sait exécuter les ordres, elle ne peut ni dialoguer avec l'utilisateur ni lui expliquer son raisonnement. Le recours aux SBC a permis de pallier cette lacune. Ceux-ci tentent de reproduire la démarche intellectuelle d'un spécialiste, ce qui en fait à l'heure actuelle, un outil précieux déjà opérationnel dans plusieurs secteurs. Habituellement, un SBC se présente comme l'association d'une Base de Connaissances (BC), d'un moteur d'inférences et d'une interface Homme-Machine.

- La base de connaissances détient la connaissance spécifique d'un domaine d'application (savoir-faire et modes de raisonnement de l'expert). Elle est couramment organisée autour des deux entités suivantes :
  - une base de faits représentant les informations qui décrivent des situations établies par l'utilisateur ou déduites par le moteur d'inférences (ou mécanisme de raisonnement),
  - une base de règles qui constitue le savoir-faire sur le domaine et indique donc les actions à entreprendre lorsqu'on est en présence d'une situation précise.
- Le moteur d'inférence exploite les données contenues dans la base de connaissances en vue d'élaborer la solution des problèmes posés. Il met en œuvre des mécanismes déductifs (fonctionnement en chaînage avant) ou inductif (fonctionnement en chaînage arrière). L'objectif est de résoudre un problème décrit par les données contenues dans la base de faits, en sélectionnant et déclenchant les règles contenues dans la base de règles.
- L'interface Homme-Machine permet d'assurer le dialogue avec les utilisateurs et/ou l'expert du domaine. Cette interface peut être scindée en deux parties :
  - une interface utilisateur à travers laquelle l'utilisateur décrit les données du problème posé et reçoit la solution accompagnée d'une trace, reflet de la résolution du problème.
  - une interface d'acquisition permettant le remplissage, la révision et la mise à jour de la base de connaissances.

L'évocation de ces trois composantes révèle ce qui différencie fondamentalement un SBC d'un logiciel classique : la séparation entre les connaissances du domaine et le mécanisme chargé de leur traitement.

Traditionnellement, on distingue trois principaux groupes d'acteurs autour d'un projet SBC :

- Le groupe des experts humains détient une grande partie de la connaissance spécifique à un domaine et possède le savoir-faire lié à la résolution du problème. Par nature les connaissances sont vagues, ambiguës et évolutives. Leur organisation dans la mémoire de l'expert est complexe, ce qui rend difficile leur extraction.
- Le groupe des cogniticiens est chargé d'identifier, recueillir, expliciter, analyser et formaliser les connaissances et modes de raisonnement de l'expert pour élaborer la base de connaissance du SBC. Le cogniticien joue un rôle primordial dans le transfert d'expertise, malgré le biais ou la distorsion que peut provoquer son intervention.
- Le groupe des utilisateurs exploite finalement les connaissances expertes emmagasinées dans le SBC.

L'évocation du rôle de ces acteurs nous amène à mettre en évidence des problèmes majeurs liés à l'élaboration de la base de connaissances d'un SBC. La conception d'une base de connaissances nécessite l'extraction, l'analyse, la structuration et la formalisation du savoir-faire d'un domaine auquel on accède à travers un ou plusieurs individus, qualifiés d'experts. Dès lors, le transfert de cette expertise soulève les questions délicates suivantes : qui détient réellement l'expertise ?, comment peut-on y accéder ?, comment l'extraire ?, comment la formaliser sans la déformer ?, quelle représentation choisir ?, comment valider et maintenir les connaissances recueillies ? Diverses recherches sont menées pour mieux cerner ces problèmes inhérents à l'acquisition de connaissances et à la conception d'un SBC. Des moyens (méthodes, techniques, outils) pour l'acquisition des connaissances sont aujourd'hui accessibles au cogniticien et à l'expert et offrent un cadre méthodologique pour le développement d'un SBC.

7.2. L'acquisition de connaissances

L'acquisition de connaissances, reconnue comme un *goulot d'étranglement* dès l'avènement des systèmes experts ou plus généralement des systèmes à base de connaissances est encore de nos jours considérée comme une tâche cruciale de leur réalisation. L'*extraction* ou l'*élicitation* désigne le recueil des connaissances auprès de l'expert du domaine alors que les notions de *transfert* ou *transmission* d'expertise désignent le recueil puis la formalisation des connaissances d'un expert humain. Le terme *acquisition de connaissances* désigne quant à lui l'ensemble des démarches nécessaires à l'élaboration d'une base de connaissances d'un système expert. L'acquisition des connaissances (AC) constitue l'un des thèmes centraux des recherches sur les SBC et l'une des clés non seulement du succès du développement d'un tel système, mais aussi de son intégration et de son utilisation en milieu opérationnel. L'AC fait intervenir essentiellement deux acteurs : l'expert, détenteur d'un savoir-faire par nature difficilement exprimable et le cogniticien ou ingénieur de la connaissance qui doit extraire et formaliser les connaissances relatives à ce savoir-faire, généralement implicite chez l'expert. Ce processus long et délicat est pourtant fondamental pour réaliser une base de connaissances efficace. Initialement centrée sur le couple expert/cogniticien, l'AC a très vite soulevé des problèmes cruciaux tels que l'identification des besoins des utilisateurs ou le choix d'un mode de représentation des connaissances. Le décalage trop important entre le langage utilisé par les experts pour décrire leur problème et le niveau d'abstraction des formalismes de représentation des connaissances a motivé de nombreuses recherches visant à faciliter le transfert d'expertise.

Les nouvelles approches de l'AC visent la définition de méthodologies plus efficaces et la conception de logiciels permettant d'aider ou de remplacer partiellement le cogniticien. Certains travaux proposent de voir la conception d'un SBC comme un processus de construction d'un modèle conceptuel, à partir de toutes les sources de connaissances (humaines ou documentaires) disponibles sur la résolution du problème à traiter. Dans ce contexte, l'AC est perçue comme une activité de modélisation. D'autres travaux soulignent l'intérêt de méthodologies visant à guider le cogniticien dans ce processus de transfert/modélisation. Des outils et méthodes permettent notamment de faciliter la verbalisation, les interviews d'experts et les analyses de documents. Les méthodes d'AC disponibles actuellement proviennent pour l'essentiel de la psychologie cognitive (modèles de raisonnement humain, techniques de recueil des connaissances), de l'ergonomie (analyse des l'activités de l'expert et du futur utilisateur), de la linguistique (pour rendre plus efficace l'exploitation des documents ou guider l'interprétation de données verbales) et du génie logiciel (description du cycle de vie d'un SBC). En résumé l'AC peut être défini comme l'ensemble des démarches nécessaires pour recueillir, structurer puis formaliser des connaissances dans le processus de conception d'un SBC. Pour aider l'expert ou le cogniticien dans cette phase de transfert d'expertise, il existe plusieurs méthodes, techniques et outils [Aussenac 1989], [Visser 88, 90], [Dieng 1990] et [Benkirane 1991] :

- Des méthodologies de développement d'un SBC. Dans la littérature, on distingue généralement deux approches pour décrire le cycle de vie d'un SBC : le *prototypage rapide* dont l'objectif est de réaliser dès que possible une maquette de faisabilité et l'*acquisition structurée* des connaissances qui s'attache à modéliser la totalité de la connaissance avant son implémentation ;
- Des méthodes d'acquisition de connaissances (comme KOD, MACAO ET KADS) qui proposent un cadre méthodologique pour l'acquisition des connaissances lors de la conception d'un SBC ;
- Des techniques d'extraction ou de recueil d'expertise, souvent inspirées des travaux en psychologie. Parmi les techniques fréquemment utilisées, notons les interviews, les questionnaires, l'analyse de protocoles et le tri conceptuel ;
- Des outils d'extraction des connaissances qui visent à automatiser certaines étapes du processus d'acquisition en élaborant directement la base de connaissances d'un SBC. Ces outils (exemple AQUINAS, ROGET, MOLE) sont fondés sur l'emploi d'une ou plusieurs techniques d'extraction de connaissances.

7.3. Limites des moyens d'acquisition de connaissances

L'état de l'art sur les travaux menés dans le domaine de l'acquisition de connaissances a permis de choisir une méthode [Benkirane 1991] pour le développement d'un SBC d'aide à l'analyse de la sécurité. Cette méthode, appliquée au domaine de la certification, a montré son intérêt pour extraire et formaliser les connaissances historiques d'analyse de sécurité (essentiellement des scénarios d'accidents) et ses limites au niveau de l'extraction de la démarche experte de d'évaluation de la sécurité, fondée notamment sur l'intuition et l'imagination. Généralement, les méthodes actuelles d'acquisition des connaissances ont été conçues pour des problèmes bien structurés. Elles n'abordent pas les spécificités liées à la multi-expertise et à la cohabitation de connaissances diverses et n'autorisent pas l'accès aux connaissances subjectives et intuitives liées à un domaine fortement évolutif et non borné comme l'est celui de la certification. Si la psychologie cognitive et le génie logiciel ont généré des méthodes et outils d'aide à l'acquisition des connaissances, l'exploitation de ces méthodes demeure encore limitée, dans un contexte industriel complexe. Nous estimons que, situé en aval, l'apprentissage automatique peut avantageusement contribuer à compléter et renforcer les moyens conventionnels d'acquisition de connaissances [Hadj-Mabrouk 94c] et [Hadj-Mabrouk 97]. Le paragraphe suivant montre l'intérêt de l'apprentissage pour l'élaboration d'une base de connaissances.

7.4. Apport de l'apprentissage automatique au domaine de l'analyse de la sécurité

L'acquisition de connaissances s'est heurtée à la difficulté d'extraire l'expertise évoquée à chaque étape de la démarche d'analyse et d'évaluation de la sécurité. Cette difficulté émane de la complexité de l'expertise qui incite naturellement les experts à décliner leur savoir-faire au travers d'exemples significatifs ou scénarios d'accidents vécus sur des systèmes de transport automatisés déjà certifiés ou homologués. Dès lors, la mise à jour de l'expertise doit se faire à partir d'exemples. L'apprentissage automatique permet de faciliter le transfert de connaissances, notamment à partir d'exemples expérimentaux. Il contribue à l'élaboration des bases de connaissances des SBC tout en réduisant l'intervention du cogniticien.

L'apprentissage est un terme très général qui décrit le processus selon lequel l'être humain ou la machine peut accroître sa connaissance. Apprendre c'est donc raisonner : découvrir des analogies et des similarités, généraliser ou particulariser une expérience, tirer parti de ses échecs et erreurs passés pour des raisonnements ultérieurs. Les nouveaux acquis sont utilisés pour résoudre de nouveaux problèmes, accomplir une nouvelle tâche ou accroître les performances dans l'accomplissement d'une tâche existante, expliquer une situation ou prédire un comportement. L'émergence et le développement industriel des systèmes à base de connaissances exigent la conception d'outils d'aide à l'acquisition des connaissances, incluant des mécanismes d'apprentissage.

Cette discipline, considérée comme une solution prometteuse pour l'aide à l'acquisition de connaissances, tente notamment de répondre à certaines questions : comment représenter explicitement une masse de connaissances, comment la gérer, l'accroître, la modifier ? Selon Ganascia [1987], l'apprentissage automatique se définit par un double objectif ; un objectif scientifique, comprendre et mécaniser les phénomènes d'évolution dans le temps et d'adaptativité des raisonnements et un objectif pratique, acquérir automatiquement des bases de connaissances à partir d'exemples. L'apprentissage peut être défini par l'amélioration des performances avec l'expérience. En effet, d'après Ganascia [1990], l'apprentissage est intimement lié à la généralisation : apprendre c'est passer d'une succession de situations vécues à un savoir réutilisable dans des situations similaires.

Pour chacune des principales méthodes d'apprentissage existantes, trois types de problèmes se posent [Kodratoff, 1986]. Le premier est celui du *regroupement* (qu'on appelle *classification* en analyse de données) : étant donnée une masse de connaissances, comment découvrir des traits communs entre elles, de sorte que l'on puisse les regrouper en sous-groupes plus simples et ayant une signification ? Le second problème (de *discrimination*) est celui de l'apprentissage de procédures de classification : étant donné un ensemble d'exemples de concepts, comment trouver une méthode qui permette efficacement de reconnaître chaque concept ? Le troisième problème est celui de la *généralisation* : comment, à partir d'exemples concrets d'une situation, trouver une formule assez générale pour décrire cette situation et comment expliquer la capacité de description de cette formule ?

Un processus d'apprentissage se caractérise par les données d'entrée et de sortie, les contraintes à respecter ainsi que les mécanismes à mettre en œuvre pour effectuer cet apprentissage (figure 8) [Hadj-Mabrouk 92] et [Hadj-Mabrouk 95a].

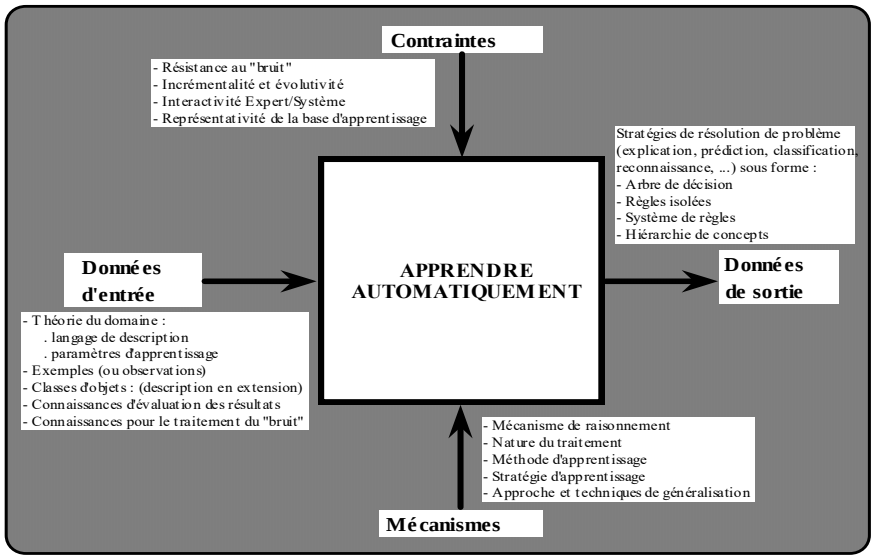

Figure 8 : Caractérisation d'un système d'apprentissage [Hadj-Mabrouk 92] et [Hadj-Mabrouk 95a].

7.5. Complémentarité de l'acquisition de connaissances et de l'apprentissage automatique pour améliorer le processus de transfert d'expertises dans le domaine de la sécurité

L'analyse du domaine de la sécurité a montré que le processus de transfert de connaissances des experts vers la machine est complexe et peu étudié et que le fameux *goulot d'étranglement* du développement d'un SBC ne se limite pas à la seule phase d'extraction de connaissances mais est également lié aux caractéristiques et à la formalisation des connaissances ainsi qu'à la collaboration entre l'expert et le cogniticien. Le savoir-faire des experts de certification repose sur des connaissances subjectives, empiriques et parfois implicites qui peuvent générer plusieurs interprétations. Il n'existe généralement pas d'explication scientifique pour justifier cette expertise compilée. Ces connaissances ne sont pas toujours conscientes chez l'expert, compréhensibles par un novice ou même exprimables par l'intermédiaire d'un langage. La transcription d'un langage verbal (naturel) en langage formel interprétable par une machine provoque souvent une distorsion de la connaissance experte. Ceci introduit un biais entre le modèle cognitif de l'expert et le modèle implémenté. Ce décalage est dû non seulement au fait que les langages de représentation employés en IA ne sont pas d'une richesse suffisante pour expliciter le fonctionnement cognitif de l'expert mais aussi à l'interprétation subjective du cogniticien. Toutes ces contraintes restreignent le champ d'investigation de l'acquisition de connaissances.

L'utilisation conjointe des techniques d'acquisition de connaissances et d'apprentissage automatique est une solution pour affaiblir ces contraintes [Hadj-Mabrouk 92], [Hadj-Mabrouk et Houriez 92], [Hadj-Mabrouk et al. 92] et [Hadj-Mabrouk 94c, 96b]. En effet, les experts considèrent généralement qu'il est plus simple de décrire des exemples ou des cas expérimentaux plutôt que d'expliciter des processus de prise de décision. L'introduction des systèmes d'apprentissage automatique fonctionnant sur des exemples permet d'engendrer de nouvelles connaissances susceptibles d'aider l'expert à résoudre un problème particulier. L'expertise d'un domaine est non seulement détenue par les experts mais aussi répartie et emmagasinée implicitement dans une masse de données historiques que l'esprit humain éprouve des difficultés à synthétiser. Extraire de cette masse d'informations des connaissances pertinentes dans un but explicatif ou décisionnel constitue l'un des objectifs de l'apprentissage automatique [Kodratoff et Diday, 1991].

L'apprentissage à partir d'exemples est toutefois insuffisant pour acquérir la totalité du savoir-faire des experts et nécessite le recours à l'acquisition de connaissances pour identifier le problème à résoudre, extraire et formaliser des connaissances accessibles par les moyens usuels d'acquisition. En ce sens, chacune des deux approches peut combler les faiblesses de l'autre. Pour améliorer le processus de transfert d'expertise, il est donc intéressant de concilier ces deux approches dans le processus itératif d'acquisition de connaissances présenté dans la figure 9 [Hadj-Mabrouk 92, 94c].

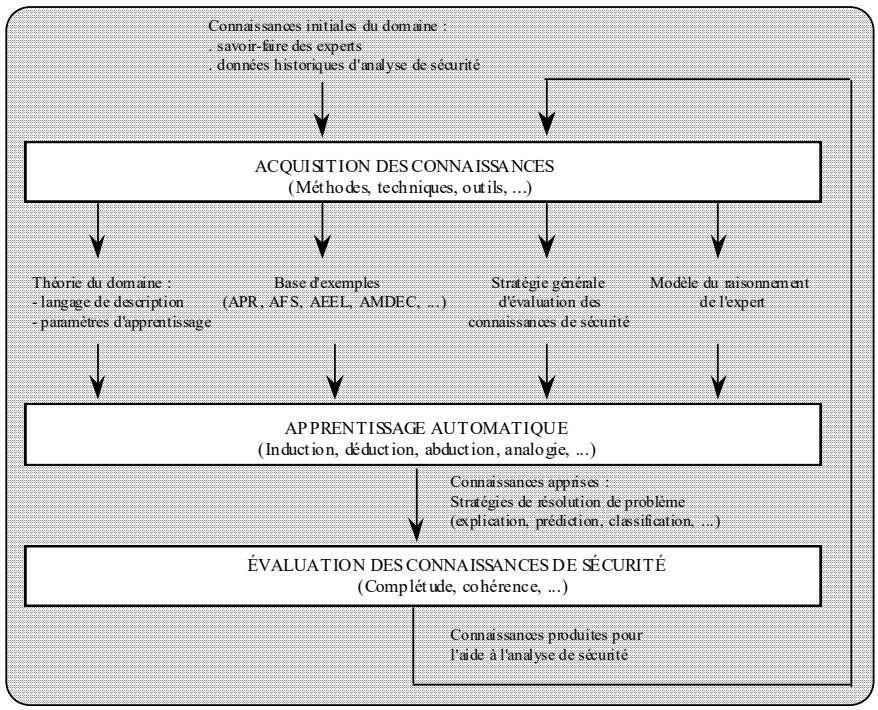

Figure 9 : Processus itératif d'acquisition et d'évaluation des connaissances de sécurité [Hadj-Mabrouk 92, 94c]

Notre approche consiste à exploiter par apprentissage l'ensemble des bases de connaissances historiques relatives aux APR, ASF, AMDEC, AEEL, ..., en vue de produire des connaissances susceptibles d'aider les experts de certification dans leur mission d'évaluation du degré de sécurité d'un nouveau système de transport.

A partir des connaissances initiales du domaine (connaissances expertes et historiques), l'acquisition de connaissances permet notamment de construire un modèle du raisonnement de l'expert et un modèle de représentation des exemples et d'obtenir un ensemble d'exemples et de classes d'objets (figure 9). Ces connaissances acquises sont exploitées par apprentissage pour produire de nouvelles connaissances apprises qui seront ensuite évaluées par l'expert du domaine. La confrontation des connaissances découvertes par l'apprentissage aux connaissances acquises auprès de l'expert permet d'enrichir les connaissances initiales du domaine. Il y a toujours un décalage entre les connaissances acquises et les connaissances réellement détenues par l'expert. En effet, on peut rarement extraire du premier coup l'ensemble des connaissances expertes mais lorsqu'on présente à l'expert les connaissances apprises par le système, il est conscient de leur intérêt, repère des contradictions, des "trous" ou des règles pertinentes. Il peut fournir un avis sur le choix des exemples et des descripteurs, interpréter les résultats produits par apprentissage, améliorer le modèle d'expertise acquis préalablement, corriger et compléter le langage de description des exemples et ajuster les paramètres d'apprentissage. En incitant l'expert à mieux verbaliser son expertise, on contribue donc à l'enrichissement des connaissances du domaine.

8. BIBLIOGRAPHIE

[Aussenac 89] : Aussenac N. « Conception d'une méthodologie et d'un outil d'acquisition de connaissances expertes ». *Thèse de doctorat*, Université de Toulouse, octobre 1989.

[Benchimol et al. 86] : Benchimol G., Levine P, Pomerol J.C. « Systèmes experts dans l'entreprise » Paris, *éditions HERMES*, mai 1986.

[Benkirane 91] : Benkirane M. « Contribution à la méthodologie d'extraction de connaissances dans le domaine du diagnostic technique ». *Thèse de doctorat*, Université de Valenciennes, mars 1991.

[Cordier 87] : Cordier M.O. « Les systèmes experts » La recherche en Intelligence Artificielle, *Edition SEUIL* 1987, p177-210.

[Dieng 90] : Dieng R. « Méthodes et outils d'acquisition des connaissances », *ERGO IA 90*, Biarritz, France, 19 à 21 septembre 1990.

[Farreny 85] : Farreny H. « Les systèmes experts : principes et exemples ». *Editions CEPADUS* , Paris,1985, 363p.

[Farreny et Ghallab 87] : Farreny H.,. Ghallab M. « Eléments d'Intelligence Artificielle ». Paris, *Editions HERMES*, 1987, 363p.

[Ganascia 87] : Ganascia J.-G. »AGAPE et CHARADE : deux mécanismes d'apprentissage symbolique appliqués à la construction de bases de connaissances », *Thèse d'état*, Université Paris-sud, mai 1987.

[Ganascia 90] : Ganascia J.-G « L'âme Machine : les enjeux de l'Intelligence Artificielle », *Le Seuil Editions*., janvier 1990.

[Hadj-Mabrouk 91] : Hadj-Mabrouk H. « Apport des techniques d'apprentissage pour l'aide à la certification des systèmes de transport automatisés ». LAFORIA, Université de Paris VI, 6 Juin 1991.

[Hadj-Mabrouk 92] : Hadj-Mabrouk H. « Apprentissage automatique et acquisition des connaissances : deux approches complémentaires pour les systèmes à base de connaissances. Application au système ACASYA d'aide à la certification des systèmes de transport automatisés ». *Thèse de Doctorat*, Université de Valenciennes, France, 15 décembre 1992.

[Hadj-Mabrouk et Houriez 92] : Hadj-Mabrouk H., Houriez B. « Acquisition de connaissances et apprentissage automatique pour l'élaboration d'une base de connaissances ». *Actes des 1ères Journées Francophones d'Apprentissage et d'Explicitation des Connaissances (JFAEC).* AFIA-AFCET, PRC GRECO IA, Dourdan, 15-17 Avril 1992, p 29-46.

[Hadj-Mabrouk et al 92] : Hadj-Mabrouk H., Houriez B., El Koursi M., Le Trung B. « Méthodologie d'analyse et d'évaluation de la sécurité basée sur les techniques d'intelligence artificielle », *Revue européenne de diagnostic et sûreté de fonctionnement*, Hermes éd., volume 2, n° 1/1992, 1992.

[Hadj-Mabrouk 93] : Hadj-Mabrouk H. « Apport des techniques d'intelligence artificielle à l'analyse de la sécurité des systèmes de transport guidés ». *Revue Recherche Transports Sécurité*, n° 40, Inrets, France,1993.

[Hadj-Mabrouk et al. 93] : Hadj-Mabrouk H., Le Trung B., Bied-Charreton D. « Rôle de l'INRETS-CRESTA dans le processus de développement et d'exploitation d'un système de transport guidé ». *INRETS-CRESTA, CR/A-93-54*, Édition provisoire, Arcueil, Août 1993.

[Hadj-Mabrouk 94a] : Hadj-Mabrouk H. « ACASYA : a learning system for functional safety analysis ». *Revue Recherche Transports Sécurité*, n° 10, France, Septembre 1994, p 9-21.

[Hadj-Mabrouk 94b] : Hadj-Mabrouk H. « Techniques d'apprentissage automatique pour l'aide à la classification et à l'évaluation des scénarios d'accidents. Application au domaine de la sécurité des transports guidés ». *Pôle Intelligence Artificielle*, INRETS-Arcueil, 18 novembre 1994.

[Hadj-Mabrouk 94c] : Hadj-Mabrouk H. « Introduction des techniques d'apprentissage automatique et d'acquisition des connaissances dans l'analyse de la sécurité des transports guidés ». *Troisième conférence maghrébine en génie logiciel et intelligence artificielle*, Rabat, Maroc, 11-14 avril 1994, pp 331-340.

[Hadj-Mabrouk 95a] : Hadj-Mabrouk H. « L'apprentissage automatique : principes et exemple d'application au domaine de la sécurité ». *JE'95, Journées électronique et informatique pour la sûreté*, Commissariat à l'Énergie Atomique. Gif-sur-Yvette, France, 7-9 février 1995, pp 187-197.

[Hadj-Mabrouk 95b] : Hadj-Mabrouk H. « La maîtrise des risques dans le domaine des automatismes des systèmes de transport guidés : Le problème de l'évaluation des analyses préliminaires de risques » *Revue Recherche-Transport-Sécurité*, numéro 49, Arcueil - Paris, France, décembre 1995.

[Hadj-Mabrouk 95c] : Hadj-Mabrouk H. « Introduction des techniques d'intelligence artificielle dans le processus de construction de la sécurité ». Exposé, *Conseil scientifique du GRRT*, Villeneuve d'Ascq, 15 février 1995, 25 p.

[Hadj-Mabrouk 96a] : Hadj-Mabrouk H. « Capitalisation et évaluation des analyses de sécurité des automatismes des systèmes de transport guidés ». *Revue Transport Environnement Circulation*, N° 134, France, janvier-février 1996, pp 22-29.

[Hadj-Mabrouk 96b] : Hadj-Mabrouk H. « Méthodes et outils d'aide aux analyses de sécurité dans le domaine des transports terrestres guidés ». *Revue Routes et Transports*, Montréal-Québec, vol. 26, n° 2, pp 22-32, Été 1996.

[Hadj-Mabrouk 96c] : Hadj-Mabrouk H. « L'axe de recherche AVIS : des méthodes et des outils d'aide à l'élaboration et à l'évaluation des analyses de sécurité ». *Journée cellule ASCOT*, programme PREDIT, Villeneuve d'Ascq, 14 mai 1996, 29 p.

[Hadj-Mabrouk et al. 96] : Hadj-Mabrouk H., Chopard-Guillaumot G., Darricau M. « Tools for providing aid for modelling, storing and assessing safety analyses in the area of terrestrial guided transport ». *29th International Symposium on Automotive Technology and Automation (ISATA)*, Florence, Italie, 3-6 juin 1996.

[Hadj-Mabrouk 97] : Hadj-Mabrouk H. « L'acquisition des connaissances pour l'élaboration d'une base de scénarios d'accidents ». *Lettre de la sûreté de fonctionnement*, Édition EC2 & Développement, Paris, septembre 1997 (A paraître).

[Hadj-Mabrouk et Jézéquel 97] : Hadj-Mabrouk H., Jézéquel R. « Description générale du programme inter-ministériel de recherche sur les transports PREDIT/ASCOT. Description de la fiche INRETS 17 ». Convention INRETS/ASCOT, rapport provisoire n° ESTAS/A-97-53, diffusion restreinte, Arcueil, 26 septembre 1997.

[Hart 88] : Hart A. « Acquisition du savoir pour les systèmes experts ». *Editions Masson* , Paris 1988, 142p.

[Kodratoff 86] : Kodratoff Y. « Leçons d'apprentissage symbolique automatique », *Cepadues éditions*, Toulouse, France, 1986.

[Kodratoff et Diday 91] : Kodratoff Y, Diday E. « Induction symbolique et numérique à partir de données », *Cepadues éditions*, Toulouse, 1991.

[Lauriere 84] : Lauriere J.L. « Les systèmes experts : caractéristique, état de l'art et perspective ». *Colloque international d'intelligence artificielle*. Marseille 24-27 Octobre 1984.

[Lievens 76] : Lievens C. « Sécurité des systèmes ». E.N.S.A.E., Toulouse, 1976, 352 p.

[Villemeur 88] : Villemeur A. « Sûreté de fonctionnement des systèmes industriels - fiabilité, facteurs humains, informatisation ». *Edition Eyrolles*, Paris 1988, 795 p.

[Visser 88] : Visser W. « Méthodes pour l'accès à l'expertise. L'utilisation concurrente de différentes méthodes de recueil de données pour l'étude de l'activité de programmation ». *Psychologie Française 33.3*, Novembre 1988, p 127-132.

[Visser 90] : Visser W. « Acquisition de connaissances : l'approche de la psychologie cognitive illustrée par le recueil d'expertise en conception ». *Journée Acquisition de Connaissances (JAC),* Lannion 27, Avril 1990.

TROISIÈME PARTIE

L'AXE DE RECHERCHE « AVIS »

Des méthodes et des outils pour l'aide à l'acquisition, à la capitalisation, à l'élaboration et à l'évaluation des analyses de sécurité

INTRODUCTION

Ce chapitre détaille mes activités de recherche menées au sein de l'unité de recherche ESTAS de l'INRETS. Ces contributions résultent du travail de l'équipe que j'ai constituée pour le développement de l'axe de recherche « AVIS » qui s'articule autour de plusieurs projets complémentaires détaillés tout au long de ce chapitre. Ces projets sont classés en trois thèmes, conformément au processus de construction de la sécurité d'un système présenté dans le deuxième partie de ce mémoire :

1. Analyse de la sécurité au niveau système/automatismes. Ce niveau d'analyse comporte deux projets de recherche complémentaires : « SAPRISTI » pour l'aide aux analyses préliminaires de risques (APR) et « ACASYA » pour l'aide aux analyses fonctionnelles de la sécurité (AFS) ;

2. Analyse de la sécurité au niveau logiciel. Ce niveau d'analyse s'articule autour de deux grands projets : « SAUTREL » pour l'aide aux analyses des effets des erreurs du logiciel (AEEL) et « SPECIAL » pour l'aide à l'élaboration, la réutilisation et l'évaluation des spécifications des logiciels critiques ;

3. Analyse de la sécurité au niveau matériel. Le projet « SASEM » est développé pour l'aide aux analyses des modes de défaillance, de leurs effets et de leurs criticités (AMDEC).

Pour chacun de ces projets, on indique le contexte général de l'étude, la problématique scientifique, les motivations, les techniques et méthodes mises en oeuvre, l'application réalisée et les résultats obtenus.

I/ Aide à l'analyse de la sécurité au niveau « SYSTÈME/AUTOMATISMES »

INTRODUCTION

Cette section présente les principaux résultats des travaux effectués dans le cadre de deux projets : « SAPRISTI » et « ACASYA » dont l'objectif est d'améliorer respectivement les analyses préliminaires de risques (APR) et les analyses de sécurité fonctionnelles (ASF).

Le projet « SAPRISTI » vise le développement d'une maquette de système à base de connaissance pour l'aide à l'élaboration et à l'évaluation des analyses préliminaires de risques (APR). Le projet « ACASYA » consiste à concevoir et mettre en oeuvre une maquette de système d'apprentissage automatique d'aide à la capitalisation, à la classification, à l'évaluation et à la génération des scénarios d'accidents.

Le projet « SAPRISTI » est en cours de développement en collaboration avec le Laboratoire d'Informatique de Paris 6 : LIP6 (ex. LAFORIA). Une partie de ce projet fait l'objet de la thèse de G. Chopard-Guillaumot démarrée en octobre 1994. L'encadrement de ce thésard est assuré conjointement par le Professeur Jean-Gabriel GANASCIA et moi-même.

Le projet « ACASYA » a été réalisé en grande partie en collaboration avec le LAMIH de l'Université de Valenciennes (équipe IICHM du Professeur Patrick MILLOT). Ce projet, que j'ai initié au LAMIH en collaboration avec l'unité de recherche ESTAS de l'INRETS (Miloudi El-Koursi), a fait d'une part l'objet de ma thèse soutenue en 1992 et d'autre part l'objet de la thèse de L. MEJRI soutenue en 1995 au LAMIH.

Nous présentons en premier lieu le projet « ACASYA » qui est à la base de ma recherche en matière d'acquisition, d'apprentissage et d'évaluation des connaissances de sécurité des automatismes des systèmes de transports guidés.

Projet « ACASYA »

« Maquette d'un système à base de connaissances basé sur l'utilisation conjointe des techniques d'apprentissage automatique et d'acquisition des connaissances, pour l'aide à la modélisation, à la capitalisation, à la classification, à l'évaluation et à la génération des scénarios d'accidents ».

1. CONTEXTE GENERAL DE LA RECHERCHE ET COLLABORATIONS SCIENTIFIQUES

Ce paragraphe présente une description générale du système « ACASYA » qui est à la base de notre recherche sur l'acquisition et l'évaluation des connaissances de sécurité des systèmes de transport guidés. En effet, mes premiers travaux menés en matière d'acquisition, de modélisation, d'apprentissage et d'évaluation des connaissances de sécurité ont débouché sur ma thèse de doctorat soutenue en décembre 1992. Ils consistent en l'étude et la mise en œuvre d'une méthode de classification, d'évaluation et d'aide à la génération des scénarios d'accidents permettant d'assister les experts de certification dans leur tâche cruciale d'examen des analyses fonctionnelles de la sécurité des automatismes des systèmes de transport guidés.

Une première maquette de système expert basée sur l'emploi des méthodes d'apprentissage automatique a été développée. Cette maquette appelée « ACASYA » [Hadj-Mabrouk 92] a permis de concrétiser les deux premières étapes de la démarche proposée, par le développement de deux modules « CLASCA » et « EVALSCA » dédiés respectivement à la classification et à l'évaluation des scénarios contraires à la sécurité.

Développée au LAMIH de l'Université de Valenciennes, la maquette « ACASYA » a été par la suite améliorée à l'INRETS-ESTAS [Hadj-Mabrouk 93]. Ces améliorations ont porté essentiellement sur l'enrichissement de la base de scénarios d'accidents ainsi que sur l'amélioration du module de classification des scénarios.

Bien que cet outil « ACASYA » ait été développé dans le cadre de mon doctorat, il est à la base de tous les travaux qui ont suivi, compte tenu de l'originalité de la méthodologie d'aide à l'analyse de la sécurité qui est fondée sur l'utilisation conjointe des techniques d'acquisition des connaissances et d'apprentissage automatique. En effet, la troisième étape de la méthodologie proposée a fait l'objet de la thèse de L. MEJRI (boursier INRETS/Région) soutenue le 15 décembre 1995 à l'Université de Valenciennes et qui a porté essentiellement sur la conception et la réalisation du module « GENESCA » d'aide à la génération des scénarios d'accidents [Mejri 95]. L'encadrement scientifique de cette thèse a été assuré conjointement par le Professeur Bernard HOURIEZ et moi-même.

Dans le cadre du projet « ACASYA », j'ai également assuré l'encadrement scientifique de deux stagiaires en DEA automatique industrielle et humaine [Mejri 91] et [Gaber 92], d'un Ingénieur en informatique de l'ENSI de Tunis [Mejri 91] et d'un stagiaire en DESS informatique et communication Homme-Machine [Derenty 92]. Les travaux de ces stagiaires ont porté essentiellement sur la réalisation de l'interface Homme-Machine du système « ACASYA », le recueil et la formalisation des scénarios d'accidents ainsi que sur la conception et la mise en oeuvre d'un algorithme d'apprentissage incrémental dédié à la classification des scénarios d'accidents.

L'ensemble de ces travaux qui s'inscrivent dans le cadre du programme de recherche du GRRT ont été réalisés en collaboration avec le LAMIH de l'Université de Valenciennes (équipe IICHM du Professeur Patrick MILLOT). Ces travaux de recherche ont également reçu le soutien du programme interministériel de recherche sur les transports PREDIT-ASCOT.

Cette section présente les résultats significatifs de cette recherche sur la modélisation, la capitalisation, la classification, l'évaluation et l'aide à la génération des scénarios d'accidents.

2. OBJECTIF DE L'ÉTUDE

Diverses recherches en intelligence artificielle (IA) sont menées pour appréhender le problème de transfert d'expertise. On perçoit aujourd'hui deux grandes activités de recherche indépendantes : l'acquisition de connaissances dont le but est de définir des méthodes inspirées notamment du génie logiciel et de la psychologie cognitive pour mieux cerner le transfert d'expertise et l'apprentissage automatique qui propose la mise en œuvre de techniques inductives, déductives, abductives ou par analogie permettant de doter le système à base de connaissances (SBC) de capacités d'apprentissage. La méthodologie d'aide à l'analyse de sécurité développée repose sur l'utilisation conjointe et complémentaire de ces deux approches. ACASYA est l'environnement logiciel développé pour supporter cette méthodologie. Il est composé de trois modules principaux : CLASCA, EVALSCA et GENESCA, respectivement dédiés à la classification, à l'évaluation et à la génération des scénarios d'accidents [Hadj-Mabrouk, 1997]. Par opposition aux systèmes d'aide au diagnostic, ACASYA peut être perçu comme un outil d'aide à la prévention des accidents dès le stade de conception du système.

L'objectif de cet outil est, d'une part d'évaluer la complétude et la cohérence des scénarios d'accidents proposés par les constructeurs et d'autre part de contribuer à la génération de nouveaux scénarios susceptibles d'aider les experts de certification qui doivent conclure sur le caractère sécuritaire d'un nouveau système. Plus précisément, l'outil ACASYA [Hadj-Mabrouk 94] permet d'aider les experts de l'INRETS, voire même le constructeur et le maître d'ouvrage, notamment dans la phase d'évaluation de la complétude des analyses fonctionnelles de sécurité (AFS). Généralement, le but des AFS est de justifier que l'architecture de conception du système est sécuritaire vis-à-vis des risques identifiés par l'Analyse Préliminaire de Risques (APR) et par conséquent de s'assurer que toutes les dispositions de sécurité sont prises en compte pour couvrir les risques. Ces analyses fournissent des critères de sécurité pour la conception du système et la réalisation des équipements matériels et logiciels de sécurité. Elles imposent aussi des critères de sécurité liés au dimensionnement, à l'exploitation et à la maintenance du système. Les AFS peuvent mettre en évidence des scénarios contraires à la sécurité qui nécessitent une reprise de la spécification.

3. APPROCHE RETENUE POUR LE DÉVELOPPEMENT DU PROJET « ACASYA »

L'élaboration de la base de connaissances d'un SBC nécessite le recours aux techniques et méthodes d'acquisition de connaissances pour recueillir, structurer puis formaliser les connaissances. L'acquisition de connaissances n'a pas permis, à elle seule, d'extraire efficacement certaines connaissances expertes de certification. Aussi, l'utilisation conjointe de l'acquisition de connaissances et de l'apprentissage automatique apparaît-elle comme une solution très prometteuse. L'approche retenue pour concevoir et mettre en œuvre un outil d'aide à l'analyse de la sécurité implique les deux grandes activités suivantes [Hadj-Mabrouk et al. 1992], [Hadj-Mabrouk, 1997] :

1. Extraire, formaliser et archiver les situations d'insécurité de façon à constituer une bibliothèque de cas types couvrant l'ensemble du problème. Celle-ci est appelée base de scénarios historiques. Cette activité a nécessité le recours aux techniques et méthodes d'acquisition de connaissances,
2. Exploiter les connaissances historiques archivées afin d'en dégager un savoir-faire en analyse de sécurité susceptible d'aider les experts à juger l'exhaustivité de l'analyse de sécurité proposée par le constructeur. Les approches mises en oeuvre pour cerner cette deuxième activité sont fondées sur l'emploi des méthodes d'apprentissage automatique.

4. APPLICATION DU MODÈLE CONCEPTUEL DES SYSTÈMES D'INGÉNIERIE DE CONNAISSANCES DE BENKIRANE POUR L'ACQUISITION DES CONNAISSANCES DE SÉCURITÉ

Dans le cadre de l'étude de faisabilité d'un SBC d'aide à l'analyse de sécurité, nous avons inscrit notre démarche dans l'esprit du modèle conceptuel proposé par Benkirane [1991]. L'application de ce modèle au domaine de l'évaluation de la sécurité a permis de caractériser précisément le domaine d'expertise, d'en recenser l'ensemble des concepts fondamentaux et a débouché sur l'élaboration d'un modèle *générique* pour la représentation des scénarios d'accidents. Les scénarios collectés à ce jour dans la base de connaissances historiques, concernent le problème de la *collision* et sont élaborés à partir des dossiers de sécurité relatifs aux systèmes VAL, POMA 2000, MAGGALY et TVM430 du TGV-nord ainsi que du savoir-faire des experts et chercheurs de l'INRETS-ESTAS [Ll-Koursi et al. 1992], [Le-Trung et al., 1992]. La figure 1 donne un exemple de classification d'un accident potentiel relatif au risque de collision.

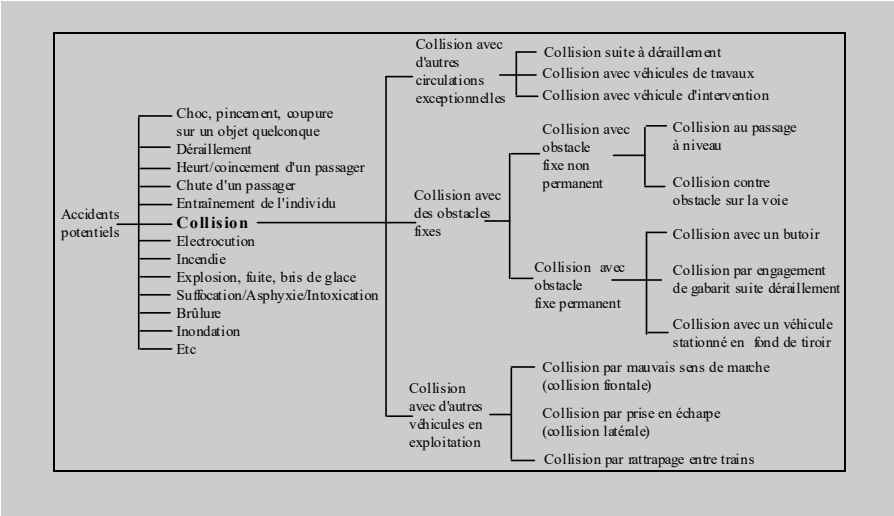

Figure 1 : Exemple de classification d'un accident potentiel : collision [Hadj-Mabrouk 95]

En revanche, malgré le nombre important de sessions d'extraction de connaissances (une trentaine de sessions), ainsi que l'emploi de plusieurs techniques de recueil de connaissances (interviews, questionnaires, analyse de protocoles, tri conceptuel…), le modèle d'acquisition de connaissances n'a pas permis d'identifier de manière détaillée les mécanismes de raisonnement de l'expert, ses stratégies et heuristiques de résolution de problème. Cet obstacle est dû notamment à l'originalité et à la complexité du domaine ainsi qu'au caractère intuitif, évolutif et créatif du mode de raisonnement des experts. Nous présentons ci-dessous les résultats de l'acquisition des connaissances concernant l'analyse et la caractérisation d'un scénario d'accident.

4.1. Caractérisation et modélisation d'un scénario d'accident

Un scénario d'accident décrit un concours de circonstances qui peut conduire à une situation non désirable, voire dangereuse. Il est caractérisé par un contexte et un ensemble d'événements et de paramètres. L'acquisition des connaissances a débouché sur la mise en forme d'un modèle fondé notamment sur l'identification des huit paramètres décrivant un scénario d'accident (figure 2).

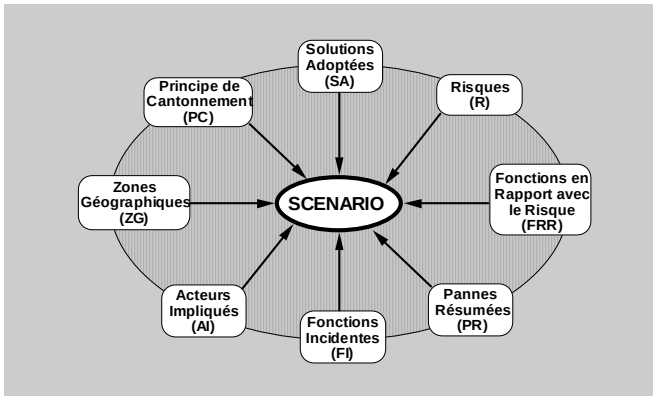

Figure 2 : Paramètres descriptifs d'un scénario d'accident

L'analyse du concept de *scénario* a révélé deux aspects fondamentaux. Le premier, statique, permet de caractériser le contexte, et le second, dynamique, met en évidence les possibilités d'évolution dans ce contexte, tout en soulignant le cheminement qui débouche sur une situation d'insécurité [Hadj-Mabrouk et al. 92]. Le formalisme retenu pour la description statique est celui d'une fiche dans laquelle plusieurs paramètres descriptifs essentiels sont décrits en termes de paires attribut/valeur. Très schématiquement, les systèmes de transport guidés sont considérés comme un assemblage de *briques* de base et un nouveau système possède des *briques* communes avec des systèmes déjà connus. Dans le cadre de la présente étude, les *briques* de base identifiées à ce jour sont regroupées dans la fiche descriptive, alors que les *briques* communes sont recherchées puis exploitées par l'outil ACASYA pour déduire la classe d'appartenance d'un nouveau scénario (module CLASCA) ou évaluer sa complétude (module EVALSCA).

Pour la description dynamique nous avons repris le formalisme déjà utilisé des réseaux de Pétri, tout en le structurant de façon à mettre en évidence trois composantes essentielles (figure 3) [Hadj-Mabrouk 92], [El-Koursi et al. 92] : l'environnement externe du système (partie opérative), l'environnement interne (partie commande) et l'interface qui assure la communication entre les deux environnements. Le réseau de Pétri permet de focaliser l'étude sur un environnement particulier du système pour lequel diverses séquences d'animation peuvent être envisagées. Chacune de ces séquences correspond à un scénario et est décrite sous forme d'un tableau dit « tableau de séquencement du marquage ».

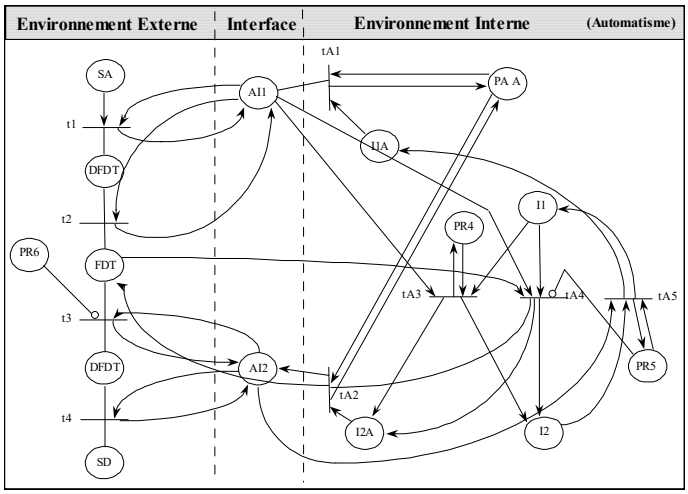

Figure 3 : Exemple de description dynamique d'un scénario d'accident

(Scénario n°2 : Commutation inopinée d'itinéraires par le pilote automatique)

4.2. Limites des moyens d'acquisition de connaissances

L'application des moyens d'acquisition de connaissances a débouché essentiellement sur l'élaboration d'un modèle générique de représentation des scénarios d'accidents et sur la constitution d'une base de scénarios qui regroupe une soixantaine de scénarios relatifs au risque de collision [Hadj-Mabrouk et al., 91, 92, 93, 94, 95]. L'acquisition de connaissances s'est toutefois heurtée à la difficulté d'extraire l'expertise évoquée à chaque étape de la démarche d'analyse et d'évaluation de la sécurité. Cette difficulté émane de la complexité de l'expertise qui incite naturellement les experts à décliner leur savoir-faire au travers d'exemples significatifs ou scénarios d'accidents vécus sur des systèmes de transport automatisés déjà certifiés ou homologués. Dès lors, la mise à jour de l'expertise doit se faire à partir d'exemples. L'apprentissage automatique permet de faciliter le transfert de connaissances, notamment à partir d'exemples expérimentaux. Il contribue à l'élaboration des bases de connaissances des SBC tout en réduisant l'intervention du cogniticien. Dans notre approche, l'apprentissage exploite la base d'exemples de scénarios d'accidents pour engendrer de nouvelles connaissances susceptibles d'aider les experts de certification à évaluer le degré de sécurité d'un nouveau système de transport.

5. LE SYSTÈME « ACASYA » D'AIDE A L'ANALYSE DE LA SÉCURITÉ

Le système ACASYA [Hadj-Mabrouk, 92, 97, 98] repose sur l'utilisation conjointe des techniques d'acquisition de connaissances et d'apprentissage automatique. Les deux principales caractéristiques de cet outil sont la prise en compte de l'incrémentalité nécessaire à une évolution progressive des connaissances apprises par le système et de la coopération homme/machine pour permettre à l'expert de corriger et compléter les connaissances initiales et/ou produites par le système. Contrairement à la majorité des systèmes d'aide à la décision qui s'adressent à un utilisateur non expert, l'outil conçu ici est un système destiné à coopérer avec un expert pour l'assister dans sa décision. ACASYA est organisé de façon à reproduire en grande partie la stratégie utilisée par les experts. Pour la resituer brièvement, la démarche d'évaluation des études de sécurité fait appel à une première phase de reconnaissance qui apparente le scénario étudié à une famille de scénarios connue de l'expert. Cette phase rend nécessaire la définition de classes de scénarios. Dans une seconde phase, l'expert évalue le scénario afin de dégager d'éventuelles situations d'insécurité non considérées par le constructeur. Ces dernières stimulent l'expert pour la formulation de nouveaux scénarios d'accidents.

5. 1. Organisation fonctionnelle du système « ACASYA »

Comme le montre la figure 4, nous retrouvons dans cette organisation quatre modules essentiels. Le premier module de formalisation concerne l'acquisition et la représentation d'un scénario, il est du ressort de la phase d'acquisition de connaissances. Les trois autres modules, CLASCA, EVALSCA ET GENESCA, conformément au principe général énoncé précédemment, concernent les problèmes de classification, d'évaluation et d'aide à la génération des scénarios.

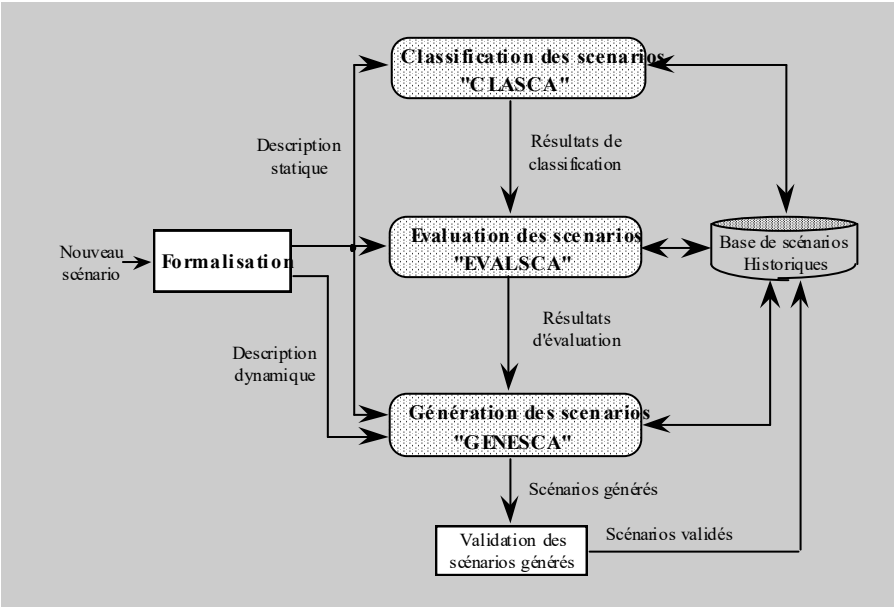

Figure 4 : Organisation fonctionnelle de la maquette du système ACASYA [Hadj-Mabrouk, 94a]

5.2. Architecture fonctionnelle de la maquette du système « CLASCA »

CLASCA [Hadj-Mabrouk, 91, 92, 93, 94] est un système d'apprentissage par recherche des procédures de classification à partir d'exemples. Il est inductif, incrémental et dédié à la classification des scénarios d'accidents. L'apprentissage dans CLASCA est d'une part non monotone, de façon à prendre en compte les données bruitées et incomplètes relatives aux scénarios d'accidents ; il est d'autre part interactif (supervisé) pour contrôler les connaissances produites par le système et aider l'expert à mieux formuler son expertise. CLASCA élabore incrémentalement des descriptions conjonctives de classes de scénarios historiques en vue d'une part de caractériser un ensemble de situations d'insécurité et d'autre part de reconnaître et d'identifier un nouveau scénario soumis pour évaluation aux experts. CLASCA est constitué des cinq principaux modules (figure 5) [Mejri, 91], [Gaber, 92] et [Derenty 92] :

1. Un module de saisie des scénarios ;

2. Un module de préconception utilisé pour fixer les différentes valeurs des paramètres et contraintes d'apprentissage requis par le système. Ces paramètres agissent principalement sur la pertinence et la qualité des connaissances de classification apprises, ainsi que sur la rapidité de convergence du système ;

3. Un module d'induction pour l'apprentissage des descriptions de classes de scénarios ;

4. Un module de classification dont l'objectif est la déduction de la classe d'appartenance d'un nouveau scénario à partir des descriptions de classes induites précédemment et en référence à un taux d'adéquation ;

5. Un module de dialogue pour l'argumentation du système et la décision de l'expert. Dans l'argumentation ou la justification, le système conserve une trace de la phase de déduction pour construire son explication. Suite à cette phase de justification des décisions de classification, l'expert décide, soit d'accepter la classification proposée et dans ce cas le scénario sera appris par CLASCA, soit de rejeter la classification. Dans le deuxième cas il appartient à l'expert de décider de la suite à donner. Il peut par exemple ajuster les paramètres d'apprentissage, créer une nouvelle classe, modifier la description du scénario ou mettre le scénario en attente pour un examen ultérieur.

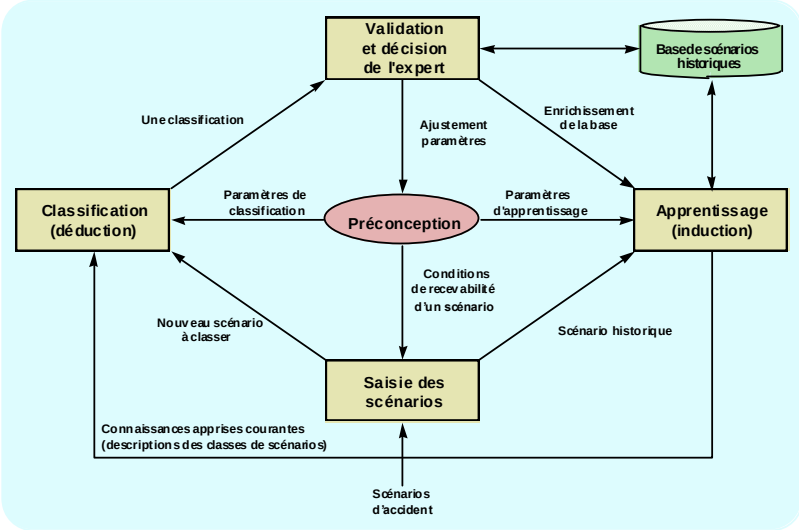

Figure 5 : Architecture fonctionnelle de la maquette du système CLASCA [Hadj-Mabrouk 94b]

5.3. Architecture fonctionnelle de la maquette du système « EVALSCA »

Le deuxième niveau de traitement considère la classe d'appartenance déduite par CLASCA pour évaluer le contenu et la cohérence du scénario constructeur. La démarche d'évaluation est centrée sur les pannes résumées (PR) impliquées dans le scénario constructeur. Une panne résumée (PR) est une panne générique, résultant du groupement d'un ensemble de pannes élémentaires ayant la même conséquence sur le comportement du système L'évaluation d'un tel scénario fait intervenir les deux modules suivants (figure 6) [Hadj-Mabrouk 92] :

- un mécanisme d'apprentissage de règles CHARADE [Ganascia 87] qui permet de déduire les fonctions de reconnaissance des PR et donc d'engendrer une base de règles d'évaluation,
- un moteur d'inférence qui exploite cette base de règles en vue de déduire les PR à considérer dans le scénario constructeur.

Le but du module EVALSCA est de confronter la liste des PR proposées dans un scénario constructeur à la liste des PR historiques archivées, pour stimuler la formulation de situations d'insécurité non prévues par le constructeur. Cette démarche d'évaluation permet d'attirer l'attention de l'expert sur d'éventuelles pannes non prises en compte par le constructeur et susceptibles de mettre en cause la sécurité du système de transport. En ce sens, elle pourra favoriser la génération de nouveaux scénarios d'accidents.

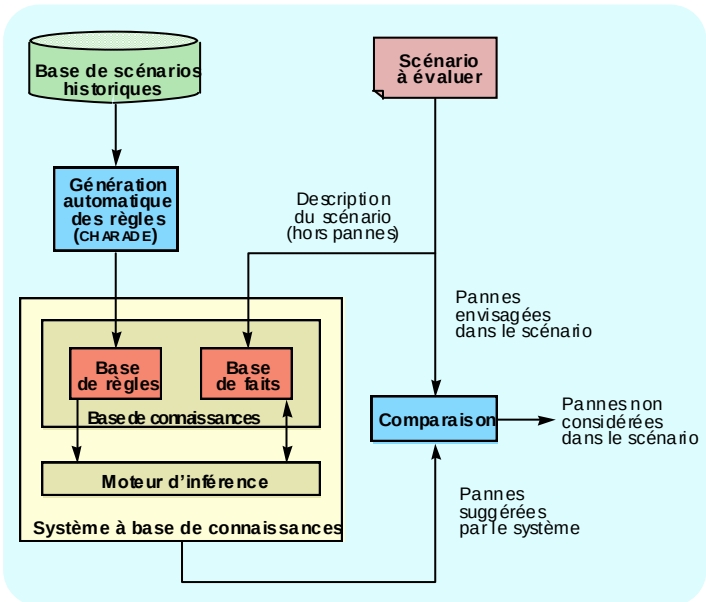

Figure 6 : Architecture fonctionnelle de la maquette du système EVALSCA [Hadj-Mabrouk 92]

5.3.1. Apprentissage des fonctions de reconnaissance des PR

À partir de la base d'exemples constituée précédemment, cette phase d'apprentissage s'attache à engendrer un système de règles traduisant les fonctions de reconnaissance des PR. Cette étape a pour but d'induire une fonction de reconnaissance de chacune des PR impliquées dans une classe. La fonction de reconnaissance d'une PR est une règle de production qui établit une relation entre un ensemble de faits (paramètres descriptifs d'un scénario ou descripteurs) et le fait PR. Il s'agit d'une relation de dépendance logique que l'on peut mettre sous la forme :

SI	Principe de cantonnement (PC)
ET	Risques ou accidents potentiels (R)
ET	Fonctions en rapport avec le risque (FRR)
ET	Zones géographiques (ZG)
ET	Acteurs impliqués (AI)
ET	Fonctions incidentes (FI)
ALORS	Pannes résumées (PR)

Pour chaque classe de scénarios on peut induire une base de règles d'évaluation. Toute règle engendrée doit contenir le descripteur ou fait PR dans sa conclusion. Le recours à une méthode d'apprentissage permettant d'engendrer, à partir d'un ensemble d'exemples (ou scénarios) historiques, des règles de production s'avère indispensable. La spécification des propriétés requises par le système d'apprentissage, ainsi que l'analyse de l'existant, ont orienté le choix vers le mécanisme CHARADE. L'induction automatique d'un système de règles et non pas des règles isolées, ainsi que la possibilité de structurer les règles pour élaborer des fonctions de reconnaissance des PR, confèrent à CHARADE un intérêt indéniable. Un échantillon de quelques règles engendrées par CHARADE, relatives à la classe *séquence d'initialisation*, est donné ci-dessous (figure 7) :

Si	acteurs_impliqués = opérateur_itinérant, fonctions_incidentes = consignes, acteurs_impliqués = operateur_au_pcc	
Alors	pannes_résumées = PR11 (élément invisible sur la zone de conduite automatique intégrale), acteurs_impliqués = pa_avec_redondance, fonctions_en_rapport_avec_le_risque = localisation_des_trains, zones_géographiques = terminus.	[0]
Si	principe_de_cantonnement = canton_fixe, fonctions_en_rapport_avec_le_risque = initialisation, fonctions_incidentes = consignes	
Alors	pannes_résumées = PR10 (rétablissement erroné de FS/HT), fonctions_en_rapport_avec_le_risque = autorisation_ CI _ HT, fonctions_en_rapport_avec_le_risque = gestion_des_alarmes, fonctions_en_rapport_avec_le_risque = localisation_des_trains.	[0]

Figure 7 : Échantillon de quelques règles engendrées par le système d'apprentissage CHARADE [Ganascia 87]

5.3.2. Déduction des pannes résumées à considérer dans le scénario à évaluer

Lors de l'étape précédente le module CHARADE a créé un système de règles à partir de la base d'exemples d'apprentissage courante relative à la classe C_k proposée par le système CLASCA. L'étape de déduction des PR nécessite au préalable une phase de transfert des règles engendrées vers un système expert pour construire une base de connaissances d'évaluation des scénarios. Cette base de connaissances d'évaluation contient :

- la base de règles qui est scindée en deux parties : une base de règles *courante* qui contient les règles induites par CHARADE relatives à une classe proposée par CHARADE à l'instant t et une base de règles *archive*, composée de la liste des bases de règles historiques. Après évaluation, une base de règles courante devient une base de règles archive,
- la base de faits qui contient les paramètres descriptifs du scénario constructeur à évaluer et qui s'enrichit, au fil de l'inférence, des faits ou descripteurs déduits.

Cette base de connaissances d'évaluation des scénarios (base de faits et base de règles), exploitée en chaînage avant par un moteur d'inférence, permet d'engendrer les pannes résumées qui doivent être impliquées dans la description du scénario constructeur à évaluer. Pour notre exemple, le système expert a déduit la panne PR19. La trace de la déduction est présentée ci-après (figure 8).

```
@@ 17/04/1996
        . canton_mobile
        . collision
        . gestion_de_conduite_automatique
        . suivi_des_trains
        . initialisation
        . terminus
        . opérateur_au_pcc
        . pa_sans_redondance
        . consignes

DÉDUCTION :
        Panne_résumée  = PR19 (Élément muet)
```

Figure 8 : Trace de la déduction du système expert

Les PR envisageables déduites par le système expert sont analysées et comparées aux PR envisagées réellement par le constructeur. Cette confrontation peut engendrer une ou plusieurs PR non prises en compte par le constructeur lors de la conception des équipements de protection et susceptibles de mettre en cause la sécurité du système de transport. Cette suggestion est à même d'aider à la génération de situations d'insécurité non prévues par le constructeur.

5.4. Architecture fonctionnelle de la maquette du système « GENESCA »

En complément des deux niveaux de traitement précédents qui font intervenir la description statique du scénario (paramètres descriptifs), le troisième niveau fait appel notamment à la description dynamique du scénario (le modèle de Pétri) ainsi qu'aux trois mécanismes de raisonnement [Mejri et al., 92, 93, 94, 95] : l'induction, la déduction et l'abduction. L'aide à la génération d'un nouveau scénario repose sur l'injection d'une PR, déclarée envisageable par le niveau précédent, dans un séquencement particulier d'évolution du marquage du réseau de Pétri.
Cette approche de génération comporte deux processus distincts [Mejri 95] : la génération statique et la génération dynamique (figure 9).

L'approche statique cherche à dériver de nouvelles descriptions statiques de scénarios à partir de l'évaluation d'un nouveau scénario. Elle exploite par apprentissage automatique l'ensemble des scénarios historiques en vue de donner un avis sur la description statique d'un nouveau scénario. Si l'approche statique a pour but de révéler des éléments statiques qui décrivent le contexte général dans lequel se déroule le nouveau scénario, l'approche dynamique se préoccupe de créer une dynamique dans ce contexte de façon à suggérer des enchaînements d'événements susceptibles de déboucher sur un accident potentiel. La méthode consiste d'abord, à caractériser par apprentissage les connaissances impliquées dans les descriptions dynamiques des scénarios historiques de la même classe que celle du scénario à évaluer et de les représenter par un modèle « générique » caractéristique. Il s'agit ensuite d'animer par simulation ce modèle générique dans le but de découvrir d'éventuels scénarios pouvant mener éventuellement à une ou plusieurs situations contraires à la sécurité Plus précisément, l'approche dynamique fait intervenir deux principales phases [Mejri 95] :

- une phase de modélisation qui doit permettre d'élaborer un modèle générique d'une classe de scénarios. La modélisation s'attache à transformer un ensemble de réseaux de Pétri en règles écrites en logique des propositions ;
- une phase de simulation qui exploite le modèle précédent pour engendrer d'éventuelles descriptions dynamiques de scénarios.

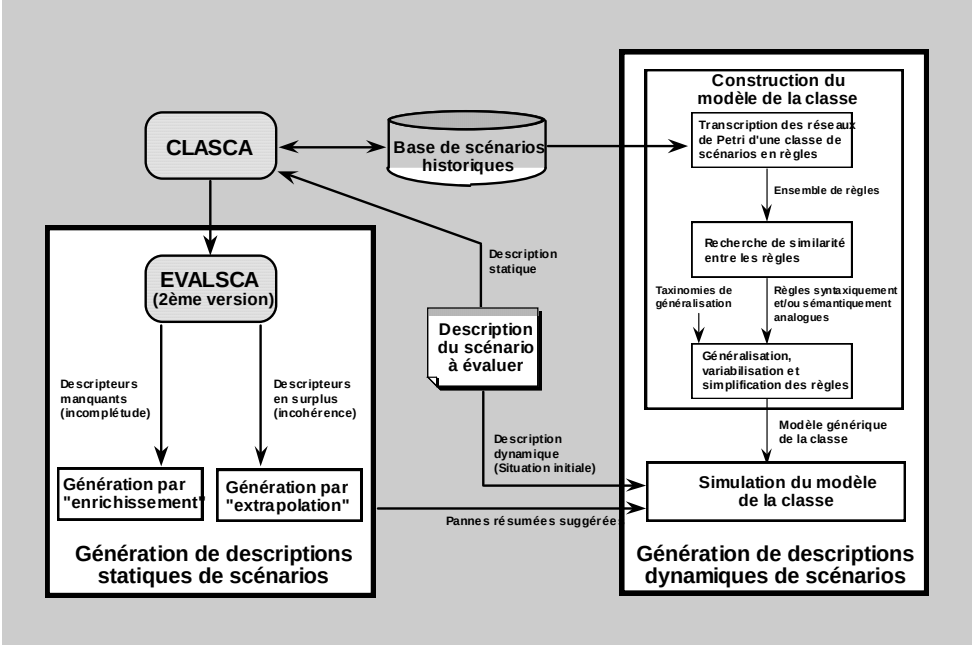

Figure 9 : Démarche d'aide à la génération d'embryons de scénarios d'accidents

Lors du développement de la maquette GENESCA, nous avons rencontré des difficultés d'ordre méthodologique. La maquette réalisée ne permet pas encore d'engendrer systématiquement de nouveaux scénarios pertinents et exploitables, mais seulement des embryons de scénarios qui stimuleront l'imagination des experts dans la formulation de scénarios d'accidents. Compte-tenu de l'absence de travaux relatifs à ce domaine, de l'originalité et de la complexité du problème, cette difficulté était prévisible mais des solutions sont à l'étude.

6. CONCLUSION

Le système ACASYA réalisé pour l'aide à l'analyse de la sécurité des systèmes de transport terrestres automatisés répond aux objectifs de classification, d'évaluation et d'aide à génération des scénarios d'accidents. Il montre la complémentarité des techniques d'apprentissage automatique et d'acquisition de connaissances pour faciliter le processus de transfert des connaissances de sécurité. Il prend en compte l'interactivité expert/système pour contrôler et compléter les connaissances produites. Le formalisme de représentation des scénarios d'accidents composé des deux descriptions statique et dynamique permet d'aider les experts à mieux structurer et conceptualiser leur savoir et de proposer éventuellement aux constructeurs des systèmes de transport un cadre méthodologique pour une définition plus exhaustive des scénarios. Renforcer en aval les méthodes classiques d'analyse de sécurité constitue l'un des apports originaux d'ACASYA. Contrairement aux systèmes d'aide au diagnostic, ACASYA se présente comme un outil d'aide à la prévention des défauts de conception.

Lors de la conception d'un nouveau système, le constructeur s'engage à respecter les objectifs de sécurité définis. Il doit démontrer que le système est réalisé de telle sorte que l'ensemble des accidents potentiels est couvert. À l'opposé, les experts de certification visent à montrer que le système n'est pas sécuritaire et dans ce cas à déceler les causes d'insécurité. Construit dans cette seconde optique, ACASYA est un outil qui évalue la complétude de l'analyse proposée par le constructeur.

ACASYA est au stade d'une maquette dont la première validation montre l'intérêt de la méthode d'aide à l'évaluation de la sécurité proposée et qui requiert certaines améliorations et extensions. Les connaissances d'analyse de sécurité acquises à ce jour sont loin d'être représentatives du domaine et nécessitent, d'une part, d'être complétées par d'autres scénarios relatifs au problème de collision et d'autre part, d'être étendues à plusieurs autres accidents potentiels (déraillement, électrocution…). L'ensemble des travaux d'évaluation et d'amélioration visent l'extension et l'adaptation de la maquette de faisabilité du système ACASYA en vue de son exploitation pour aider à l'analyse fonctionnelle de sécurité.

7. BIBLIOGRAPHIE

Thèse

Lassaâd MEJRI. « Une démarche basée sur l'apprentissage automatique pour l'aide à l'évaluation et à la génération de scénarios d'accidents. Application à l'analyse de sécurité des systèmes de transport automatisés ». Thèse de doctorat, Université de Valenciennes, 6 décembre 1995, 210p.

Mémoires de D.E.A. de DESS et d'Ingénieur

1. DERENTY V. « Réalisation d'une interface Homme-Machine pour l'exploitation de deux mécanismes d'apprentissage symbolique-numérique : CLASCA et EVALSCA ». Rapport de stage de DESS-ICHM. Laboratoire d'Automatique Industrielle et Humaine, Université de Valenciennes, mars 1992.

2. DERENTY V. « Extraction et formalisation des scénarios d'accidents potentiels pour un système d'apprentissage symbolique-numérique ». Stage de DESS-ICHM effectué à INRETS-CRESTA de Lille en collaboration avec le LAIH de l'Université de Valenciennes, juin 1992

3. GABER K. « Contribution à la réalisation et à l'évaluation d'un système d'apprentissage inductif par classification ». Mémoire de DEA en automatique industrielle et humaine, Université de Valenciennes, Juin 1992.

4. MEJRI L. « Réalisation d'une maquette de faisabilité d'un système d'apprentissage de descriptions de classes d'objets ». Rapport de stage de fin d'études d'Ingénieur en informatique de l'ENSI de Tunis. LAIH de l'Université de Valenciennes, janvier 1991.

5. MEJRI L. « Apport des méthodes d'apprentissage automatique au domaine de la certification des systèmes de transport automatisés ». Mémoire de DEA en automatique industrielle et humaine. Université de Valenciennes, Juin 1991.

Revues avec comité de lecture

1. HADJ-MABROUK H., STUPARU A., BIED-CHARRETON D. (1998). « Exemple de typologie d'accidents dans le domaine des transports guidés ». *Revue Générale des Chemins de Fer*, Éditions Dunod, Paris, mars 1998 (A paraître).

2. HADJ-MABROUK H. (1997).« L'acquisition des connaissances pour l'élaboration d'une base de scénarios d'accidents ». *Lettre de la sûreté de fonctionnement*, n° 50, Édition EC2 & Développement, Paris, septembre 1997, pp 3-16.

3. HADJ-MABROUK H. (1997). « CLASCA, EVALSCA et GENESCA : trois mécanismes d'apprentissage dédiés respectivement à la classification, à l'évaluation et à la génération des scénarios d'accidents ». *La lettre de l'intelligence artificielle*, n° 126/127, Édition EC2 & Développement, Paris, septembre/octobre 1997, pp 9-15.

4. HADJ-MABROUK H. (1996). « Méthodes et outils d'aide aux analyses de sécurité dans le domaine des transports terrestres guidés ». *Revue Routes et Transports*, Montréal-Québec, vol. 26, n° 2, pp 22-32, Été 1996.

5. HADJ-MABROUK H. (1996). « Capitalisation et évaluation des analyses de sécurité des automatismes des systèmes de transport guidés ». *Revue Transport Environnement Circulation*, Paris, TEC n° 134, pp 22-29, Janvier-février 1996.

6. HADJ-MABROUK H. (1994). « ACASYA : a learning system for functional safety analysis ». *Revue Recherche Transports Sécurité*, n° 10, pp 9-21, France, Septembre 1994.

7. HADJ-MABROUK H. (1993). « Apport des techniques d'intelligence artificielle à l'analyse de la sécurité des systèmes de transport guidés », *Revue Recherche Transports Sécurité*, n° 40, pp 3-16, France, Septembre 1993.

8. HADJ-MABROUK H., HOURIEZ B., EL KOURSI M., LE TRUNG B. (1992). « Méthodologie d'analyse et d'évaluation de la sécurité basée sur les techniques d'intelligence artificielle ». *Revue européenne de diagnostic et sûreté de fonctionnement*, Éditions Hermès 1992, France, volume 2 - n° 1/1992, pp 5-35, juin 1992.

Congrès internationaux avec actes et comité de lecture

1. HADJ-MABROUK H., MEJRI L. (1998). « ACASYA : a knowledge-based system for aid in the storage, classification, assessment and generation of accident scenarios ». ». *Congress IEEE, Computational engineering in systems applications.* Nabeul-Hammamet, Tunisia, April 1-4, 1998. (A paraître).

2. HADJ-MABROUK H. (1994). « Introduction des techniques d'apprentissage automatique et d'acquisition des connaissances dans l'analyse de sécurité des transports guidés ». *Troisième conférence maghrébine en génie logiciel et intelligence artificielle*. Rabat, Maroc, 11-14 Avril 1994, p 331-340.

3. HADJ-MABROUK H., MEJRI L., EL KOURSI M., HOURIEZ B. (1992). « Méthodologie d'aide à l'évaluation de la sécurité des systèmes de transport automatisés, basée sur l'apprentissage automatique ». *Forum de la SCGM (Sté Canadienne de Génie Mécanique), TRANSPORT 1992+,* Université Concordia (session : Sécurité dans les transports), Montréal, Québec, Canada 1-4 Juin 1992, volume III, p 957-964.

4. HADJ-MABROUK H., MEJRI L., EL KOURSI M., HOURIEZ B (1992). « Système expert à apprentissage pour l'aide à l'analyse de sécurité. Application à la certification des systèmes de transport automatisés ». *12èmes Journées Internationales d'Avignon 92*. Conférence Intelligence Artificielle, Défense et Sécurité civile. Avignon 2-3 Juin 1992, France, volume 2, p 97-112.

5. HADJ-MABROUK H., HOURIEZ B. (1992). « Acquisition de connaissances et apprentissage automatique pour l'élaboration d'une base de connaissances ». *7èmes Journées Francophones d'Apprentissage et d'Explicitation des Connaissances (JFAEC).* AFIA-AFCET, PRC GRECO IA, Dourdan, 15-17 Avril 1992, France, p 29-46.

6. LE TRUNG, M. EL KOURSI B., HOURIEZ B., HADJ-MABROUK H. (1992). « Knowledge base for safety analysis in unmanned metro system ». *COMPRAIL 92*, 18-20 August 1992, WASHINGTON DC, USA.

7. MEJRI L., HADJ MABROUK H., EL KOURSI M., HOURIEZ B. (1993).« Un système expert d'aide à la génération des scénarios d'accidents basé sur l'apprentissage automatique ». ITTG 93, *Symposium International sur l'innovation technologique dans les transports guidés*. Lille, 28-30 septembre 1993, p 627-638.

8. MEJRI L., HADJ MABROUK H., EL KOURSI M., HOURIEZ B. (1993). « Deux approches contextuelles et hors contexte basées sur l'apprentissage pour l'aide à la génération d'exemples. Application à la certification des systèmes de transport automatisés ». *Huitièmes Journées Francophones sur l'Apprentissage (JFA*). Saint-Raphaël, France, 29 Mars-2 Avril 1993.

9. MEJRI L., HADJ MABROUK H., EL KOURSI M., HOURIEZ B. (1992).« Learning based assistance tool for the generation of scenarios for automated transport systems certification ». *11th European Annual Conference on Human decision making and manual control*. Valenciennes, France, 17-19 november 1992, 14p.

Congrès nationaux avec actes et comité de lecture

1. EL KOURSI M., LE TRUNG B., HADJ-MABROUK H., HOURIEZ B. (1992). « Base de connaissances pour l'aide à l'analyse de sécurité des systèmes de transports terrestres automatisés ». *8ème colloque de fiabilité et de maintenabilité*, Grenoble 6-8 Octobre 1992, France.

2. HADJ-MABROUK H. (1995). « L'apprentissage automatique : principes et exemple d'application au domaine de la sécurité ». JE'95*, Journées électronique et informatique pour la sûreté*, Commissariat à l'Énergie Atomique. Gif-sur-Yvette, 7-9 février 1995, pp 187-197.

3. HADJ-MABROUK H. (1994). « CLASCA, un système d'apprentissage automatique dédié à la classification des scénarios d'accidents ». *9ème colloque international de fiabilité & maintenabilité*. La Baule, France, 30 Mai-3 Juin 1994, p 1183 - 1188.

4. HADJ-MABROUK H., MEJRI L., HOURIEZ B. (1992). « Complémentarité des deux mécanismes d'apprentissage : CLASCA et CHARADE pour le développement d'un système à base de connaissances ». *3èmes Journées symbolique-numérique*. SFC-AFCET-AFIA, Paris 14-15 Mai 1992, France, p 157-170.

5. HADJ-MABROUK H., EL KOURSI M., HOURIEZ B., MILLOT P. (1991). « Approche méthodologique d'aide à la certification des systèmes de transport automatisés basée sur l'apprentissage ». *5èmes Journées Acquisition de Connaissances*. Sète 17 Mai 1991, France.

Rapports de conventions/contrats

1. HADJ MABROUK H., MEJRI L., EL KOURSI M., BIED-CHARRETON D., LE TRUNG B., HOURIEZ B. (1994). « Base de scénarios d'accidents ». Convention Région Nord-Pas de Calais/INRETS-CRESTA /LAIH-UVHC. Dossier technique INRETS-CRESTA, Indice E, CR/A-94-16, Arcueil 21 Mars 1994, 213p.

2. HADJ MABROUK H. (1994). « Bilan sur les connaissances acquises pour le développement d'un système d'aide à l'examen de la sécurité des transports guidés ». Résultat des sessions de recueil de connaissances du 15/02/90 au 22/02/94. Rapport de convention Région Nord-Pas de Calais/INRETS-CRESTA/LAIH-UVHC. CR/A-94-28, Arcueil 22 Avril 1994, 34p.

3. HADJ MABROUK H., BIED-CHARRETON D. (1993). « Mise à jour de la BCHS : Base de Connaissances Historiques des Scénarios d'accidents potentiels ». Convention Région Nord-Pas de Calais/INRETS-CRESTA/LAIH-UVHC. Dossier technique INRETS-CRESTA, Indice C, CR/A-93-36, Arcueil Mai 1993.

4. HADJ MABROUK H., HOURIEZ B., MILLOT P. (1992). « CLASCA et EVALSCA deux mécanismes d'apprentissage Symbolique-Numérique pour le développement d'un système à base de connaissances d'aide à la certification des systèmes de transport automatisés ». Rapport de fin de contrat de la convention Région Nord-Pas de Calais/INRETS n°89 0882 et du contrat VALUVAL-LAIH/INRETS-CRESTA du 15/01/91 n°90090065. MAIH, Université de Valenciennes, Juin 1992.

5. HADJ MABROUK H., HOURIEZ B., MILLOT P. (1991). « Étude de faisabilité d'un système à base de connaissances pour l'aide à la certification des systèmes de transport automatisés ». Rapport de fin de contrat de la convention Région Nord-Pas de Calais/INRETS n°89 0882 et du contrat VALUVAL-LAIH/INRETS-CRESTA du 15/01/91 n°90090065. MAIH, Université de Valenciennes, Juin 1991.

6. HADJ MABROUK H., HOURIEZ B., MILLOT P. (1990). « Développement d'un système d'aide à la certification des systèmes de transport automatisés ». Convention Région Nord-Pas de Calais/INRETS n°89 0882. LAIH, Université de Valenciennes. Deux rapports d'activité, Octobre 1990 et Juin 1991.

7. MEJRI L., HADJ-MABROUK H., HOURIEZ B., MILLOT P. (1995). « Un système d'aide à la génération de scénarios contraires à la sécurité ». Rapport de fin de contrat, convention INRETS/LAMIH, Université de Valenciennes, janvier 1995, 31 p.

8. MEJRI L., HADJ MABROUK H., HOURIEZ B., BIED-CHARRETON D., BARANOWSKI F., MILLOT P. (1994). « Validation de la maquette du système d'aide à la génération de scénarios contraires à la sécurité. Etape n°1 : validation de l'approche statique ». Rapport sur convention LAMIH-UVHC/INRETS-ESTAS. Université de valenciennes, novembre 1994, 40p.

2/ Projet « SAPRISTI »

Maquette de système à base de connaissance pour l'aide à l'élaboration et à l'évaluation des analyses préliminaires de risques (APR).

1. CONTEXTE GENERAL DE LA RECHERCHE ET COLLABORATIONS SCIENTIFIQUES

Le processus de construction de la sécurité des automatismes d'un système de transport terrestre guidé fait intervenir trois grandes activités d'analyses de sécurité complémentaires et itératives : analyse de sécurité au niveau système, analyse de sécurité au niveau matériel et analyse de sécurité au niveau logiciel. Les travaux de recherche qui font l'objet du projet « SAPRISTI » s'inscrivent dans le cadre de la première analyse de sécurité au niveau système et portent plus précisément sur la conception et la mise en oeuvre d'une nouvelle méthode d'aide à l'élaboration, à la capitalisation et à l'évaluation des analyses préliminaires de risques (APR). Ces travaux s'exercent principalement dans le cadre du Programme interministériel de recherche sur les transports PREDIT-ASCOT. Ils sont soutenus notamment par le Groupement régional de recherche sur les transports du Nord-Pas-de-Calais (GRRT). Cette étude est effectuée en collaboration avec le laboratoire d'informatique de Paris 6 (LIP6) de l'Université de Pierre et Marie Curie. Dans le cadre de ce projet j'ai assuré, conjointement avec le Professeur J-G. Ganascia, l'encadrement du doctorant G. Chopard-Guillaumot (thèse démarrée en octobre 94 à l'unité de recherche ESTAS de l'INRETS). En 1996, j'ai également assuré la responsabilité scientifique de F. Raîs, stagiaire de l'Institut d'Informatique d'Evry (IIE-CNAM). Son mémoire de stage a porté sur la conception et la réalisation d'une partie de l'interface Homme-Machine du logiciel d'élaboration des APR.

2. L'ANALYSE PRÉLIMINAIRE DE RISQUES

L'analyse préliminaire de risques (APR) permet d'identifier essentiellement les accidents potentiels liés au système et à ses interfaces afin d'évaluer leur probabilité d'occurrence ainsi que la gravité des dommages qu'ils pourraient causer et enfin de proposer des solutions qui permettront de les réduire, les contrôler ou les supprimer [Hadj-Mabrouk, 97]. Les résultats de cette analyse permettent de définir les exigences et critères de sécurité du système à prendre en compte lors des phases de conception et de réalisations des équipements matériels et logiciels et enfin d'établir les grandes lignes des analyses de sécurité situées en aval (analyse fonctionnelle de la sécurité, analyse de la sécurité des logiciels, analyse de la sécurité des matériels. En effet, la constitution d'une liste d'accidents potentiels permet de recenser les points du système qui peuvent être critiques pour la sécurité et qui méritent une attention particulière dans la conception, la réalisation, la validation et la maintenance du système.

Lorsqu'on se limite à évaluer (généralement qualitativement) la gravité des dommages que pourraient causer les accidents potentiels, on parle d'analyse préliminaire des dangers, ou APD [Villemeur, 88]. Une APR nécessite une bonne connaissance de la mission du système et de son environnement. Elle est indispensable pour les systèmes qui font appel à des technologies mal connues. Elle bénéficie d'une part de l'expérience et de l'imagination du constructeur et d'autre part du suivi en exploitation (retour d'expérience). L'APR est un dossier qui reste généralement ouvert pendant toute l'étude et est constamment mis à jour. Du fait que cette analyse est réalisée très tôt dans le déroulement du programme, ses résultats peuvent être incomplets et imprécis. Une APR doit être donc complétée et mise à jour jusqu'à ce que la conception du système soit assez avancée. Ceci permet de vérifier qu'à chaque accident potentiel de la liste correspond, dans la conception, une fonction, une précaution ou disposition pour contrôler, réduire ou éliminer sa probabilité d'occurrence [Hadj-Mabrouk, 95].

L'analyse préliminaire de risques est généralement classée en théorie parmi les démarches inductives [Lievens, 76], [Villemeur 88] et [BNAE 86]. Dans la démarche inductive, le raisonnement va du plus particulier au plus général, ce qui conduit à une étude détaillée des effets d'une défaillance sur le système et son environnement. Autrement dit, les méthodes inductives partent des événements élémentaires, soit pour rechercher directement les conséquences (ex : AMDE, AEEL), soit pour identifier les combinaisons d'événements qui peuvent avoir des conséquences critiques (ex : MCPR). Dans le cadre de l'APR, il s'agit de rechercher principalement, par induction, l'ensemble des accidents potentiels à partir de dangers (ou éléments dangereux). Cependant, dans la pratique et notamment dans le domaine de la sécurité des transports guidés, on utilise essentiellement une démarche déductive telle que la méthode de l'arbre de causes (MAC).

Afin de renforcer la qualité des APR en termes de complétude et de cohérence, nous suggérons une méthode qui combine ces deux approches [Hadj-Mabrouk, 94a]. En effet, l'analyse de sécurité d'un système complexe nécessite de la part des experts du domaine la mise en œuvre d'un processus d'analyse itératif faisant intervenir à la fois des approches inductives et déductives. Il est généralement indispensable de recouper les résultats obtenus par une approche avec ceux obtenus au moyen d'une autre approche complémentaire.

Le format couramment utilisé pour représenter les résultats d'une APR est celui d'un tableau à colonnes. La figure 1, présente un exemple de tableau d'APR. Cet exemple souligne l'existence d'un consensus au niveau du formalisme suggéré en théorie. En effet, les descripteurs proposés pour caractériser une APR dans la recommandation aéronautique RE.Aéro 701 11 [BNAE 86] ainsi que dans l'ouvrage de A. Villemeur [Villemeur 88] sont identiques à ceux employés dans l'ouvrage de C. Lievens [Lievens 76]. Cependant, dans la pratique et en particulier dans le domaine de la sécurité ferroviaire, il en est autrement [Hadj-Mabrouk, 94b]. En effet, les représentations employées par les constructeurs des systèmes de transport guidés sont diverses (figures 2) et éloignées de ce qui est recommandé par la théorie.

Sous - système ou fonction	Phase	Éléments dangereux	Événement causant une situation dangereuse	Situation dangereuse	Événement causant un accident potentiel	Accidents potentiel	Effets ou conséquences	Classification par gravité	Mesures préventives	Application de ces mesures

Figure 1 : Paramètres descriptifs d'une analyse préliminaire de risques [Lievens 76], [BNAE 86], [Villemeur 88]

Équipement : .....
Mode de fonctionnement : .....
Rédacteur : .....

Item	Risque	Effet	Gravité	Mesure préventive	Fonction concernée	Remarques

LIGNE : ..... Phase : ..... Édition : .....
Folio : ..... Date : .....

Événements dangereux			**Mesures prises**			
Accident potentiel	Situation dangereuse	Éléments dangereux	Éléments concernés	Type	Application remarques	Gravité

Repère	**Identification**	**Description**	**Référence**
1	Accident potentiel		
2	Phase position		
3	Événement initiateur possible		
4	Mode fonctionnement		
5	Situation dangereuse		
6	Sous fonctions assurées		
7	Circonstances		
8	Éléments dangereux		
9	Hypothèses liées au système		
10	Commentaire (mesures supplémentaires)		

Figure 2 : Extrait de tableaux d'analyses préliminaire de risques des systèmes de transport [Hadj-Mabrouk, 94b, 97]

3. MOTIVATIONS DE L'ETUDE

Bien que primordiale dans le processus de construction de la sécurité, l'APR est très différemment développée et demeure mal définie. Les documents recommandés sont peu précis et s'écartent parfois des usages. Les formats de représentation des résultats de l'analyse sont souvent extrêmement variés. En outre, la terminologie et les concepts liés aux APR sont très fluctuants, voire contradictoires. Enfin, l'élaboration et l'évaluation d'une APR sont des pratiques laborieuses et fastidieuses qui ne sont pas habituellement soutenues par une stratégie formalisée [Hadj-Mabrouk, 96a, 96b]. Afin d'appréhender ces lacunes, nous avons développé une nouvelle méthode d'analyse préliminaire de risques dont l'ambition est de renforcer et perfectionner les démarches conventionnelles. Le paragraphe suivant propose une méthode originale d'élaboration et d'aide à l'évaluation des APR qui tienne compte des usages, de la théorie et de notre expérience dans ce domaine [Hadj-Mabrouk, 94a], [Hadj-Mabrouk et Bied-Charreton 95].

4. ÉLABORATION D'UNE MÉTHODE ORIGINALE D'ANALYSE PRÉLIMINAIRE DE RISQUES

Ce paragraphe présente les grandes lignes de la méthode en précisant le principe général et le contenu des différentes étapes impliquées. L'élaboration de cette méthode originale nécessite en premier lieu le recours à un vocabulaire normalisé.

4.1. Définition d'un vocabulaire normalisé

Afin de définir une terminologie commune et d'unifier le vocabulaire de base employé en matière d'analyse préliminaire de risques, nous avons eu recours non seulement à l'analyse d'un ensemble de normes relatives à la sécurité [Hadj-Mabrouk, 95], [Chopard-Guillaumot, Hadj-Mabrouk et Ganascia, 95], [Chopard-Guillaumot et Hadj-Mabrouk 96], [Hadj-Mabrouk 97], mais aussi à l'expérience et le savoir-faire acquis à l'INRETS dans ce domaine [Hadj-Mabrouk 94a, 94b, 94c, 95], [Hadj-Mabrouk et Bied-Charreton 95]. La figure 3 présente les principaux résultats de cette étude en précisant les définitions retenues. La figure 4 illustre l'articulation des principaux paramètres descriptifs d'une analyse préliminaire de risques

Paramètres descriptifs d'une APR	Définitions retenues	Références
Dommage	Blessure physique et/ou atteinte à la santé ou dégât causé aux choses.	Mémorandum n° 9, Cen/Cenelec [CENE 94a]
Accident	Événement ou succession d'événements imprévus ayant pour résultat une atteinte à l'intégrité physique des personnes ou des destructions de matériel.	NF F 71-011 [BNCF 90]
Quasi-accident	Dysfonctionnement du système ou une succession de dysfonctionnements du système conduisant à un état non spécifié dans lequel il n'y apas atteinte à l'intégrité physique des personnes ni destruction de matériel, mais pour lequel une condition non maîtrisée par le système auraît pu conduire à une atteinte à l'intégrité physique des personnes et/ou un endommagement notable de matériel.	NF F 00-101 [BNCF 93]
Accident potentiel	Evénement ou serie d'événement non désirés suceptible de donner lieu à un accident mais ne donnant pas nécessairement lieu à un accident. (Accident ou quasi-accident : NF F OO-101, 1993)	pr EN 50126, CENELEC [CENE 94b]
Danger	Condition pouvant donner lieu à un accident ou un accident potentiel	pr EN 50126, CENELEC [CENE 94b]
Événement dangereux	Événement créant un danger.	pr EN 50126, CENELEC [CENE 94b]
Niveau de probabilité d'occurrence d'un accident potentiel	- A : Fréquent - B : Probable - C : Occasionnel - D : Rare - E : Improbable - F : Extrêmement improbable	NF F 00-101 [BNCF 93]
Niveau de gravité d'un dommage	- I : Mineur ou nul - II : Significatif - III : Critique - IV : Catastrophique	NF F 00-101 [BNCF 93]
Risque	La combinaison de la fréquence (ou de la probabilité) d'un accident potentiel et des conséquences de l'accident (gravité des dommages)	pr EN 50129, CENELEC [CENE 93]
Mesure de prévention ou de protection	- Mesure de prévention : réduire ou annuler la probabilité d'un accident potentiel. - Mesure de protection : affaiblir la gravité des dommages provoqués par un accident potentiel. (Moyen pour réduire le niveau de risque)	RE.Aéro 7O1 11 [BNAE 86]
Sécurité	Absence de tout niveau de risque inacceptable.	pr EN 50129, CENELEC [CENE 93]

Figure 3 : définitions des principaux paramètres descriptifs d'une analyse préliminaire de risques

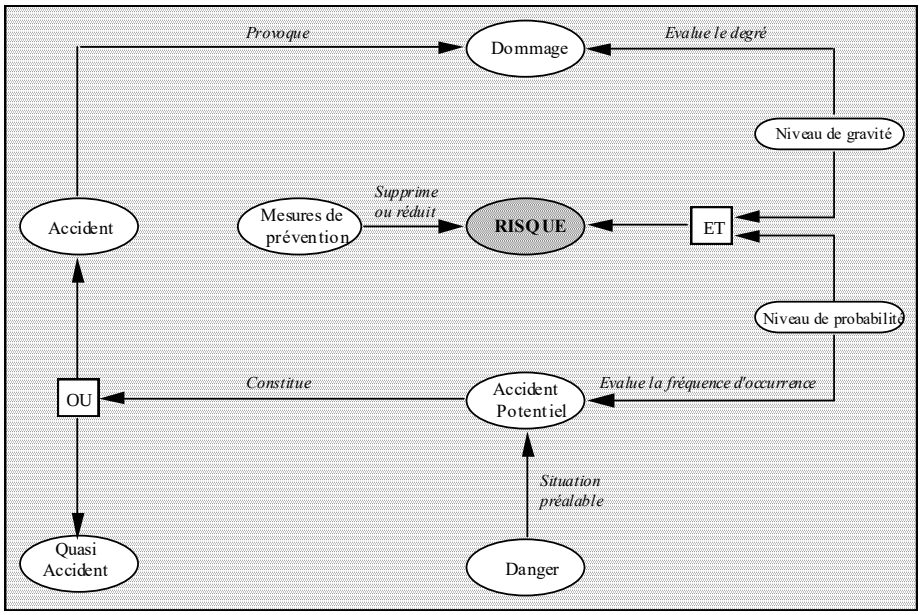

Figure 4 : articulation des principaux paramètres descriptifs d'une APR [Hadj-Mabrouk 97].

4.2. Description générale de la méthode d'analyse préliminaire de risques proposée

Dans le paragraphe précédent nous avons proposé une terminologie de base nécessaire à la clarté des analyses préliminaires de risques (APR). Le présent paragraphe précise le principe et les grandes étapes d'une nouvelle méthode d'élaboration et d'aide à l'évaluation des APR. Si la théorie préconise une approche inductive, les démarches réellement appliquées dans le domaine de la sécurité des transports guidés sont en majorité déductives. La démarche d'APR que nous recommandons combine les deux approches de manière explicite en vue de renforcer la qualité des analyses en termes de complétude et de cohérence. En effet, l'analyse de sécurité d'un système complexe nécessite de la part des experts du domaine la mise en œuvre d'un processus d'analyse itératif faisant intervenir à la fois des approches inductives et déductives. La méthode proposée s'articule autour de trois étapes complémentaires et itératives [Hadj-Mabrouk, 94a, 94c, 95, 96a, 96b, 97], [Chopard-Guillaumot, Hadj-Mabrouk et Ganascia, 96] :

1. une analyse inductive et déductive à partir des accidents potentiels,
2. une analyse déductive et inductive à partir des dangers,
3. une analyse inductive à partir des éléments dangereux.

A partir des accidents potentiels, la première étape permet de déterminer par **induction** la liste des dommages que pourrait causer un accident et par **déduction** la liste des dangers qui peuvent se manifester dans le système. La deuxième étape utilise les dangers précédents pour identifier par **déduction** la liste des éléments dangereux et, par **induction**, celle des accidents potentiels. Etablir à nouveau la liste des accidents potentiels à partir des dangers permet éventuellement d'engendrer de nouveaux accidents potentiels non considérés lors de la première étape. Dans ce cas, la première étape de l'analyse doit être reprise en vue d'enrichir la liste des dangers précédemment déduite. Il s'agit en fait d'une action de vérification qui permet d'accroître davantage la liste initiale des accidents potentiels.

La troisième étape de l'analyse consiste, à **induire** des dangers, à partir des éléments dangereux déduits lors de la deuxième étape. Le catalogue des dangers établi à l'issue de cette troisième analyse est confronté à celui qui est déduit lors de la première étape de l'analyse à partir des accidents potentiels. L'invention de nouveaux dangers impose de recommencer la deuxième étape d'analyse et éventuellement la première. Ce processus de contrôle itératif permet d'assurer la complétude et de tendre ainsi vers l'exhaustivité de l'analyse préliminaire de risques (APR).

La figure 5 schématise les différentes étapes impliquées dans le processus d'analyse de risque que nous préconisons [Hadj-Mabrouk 97].

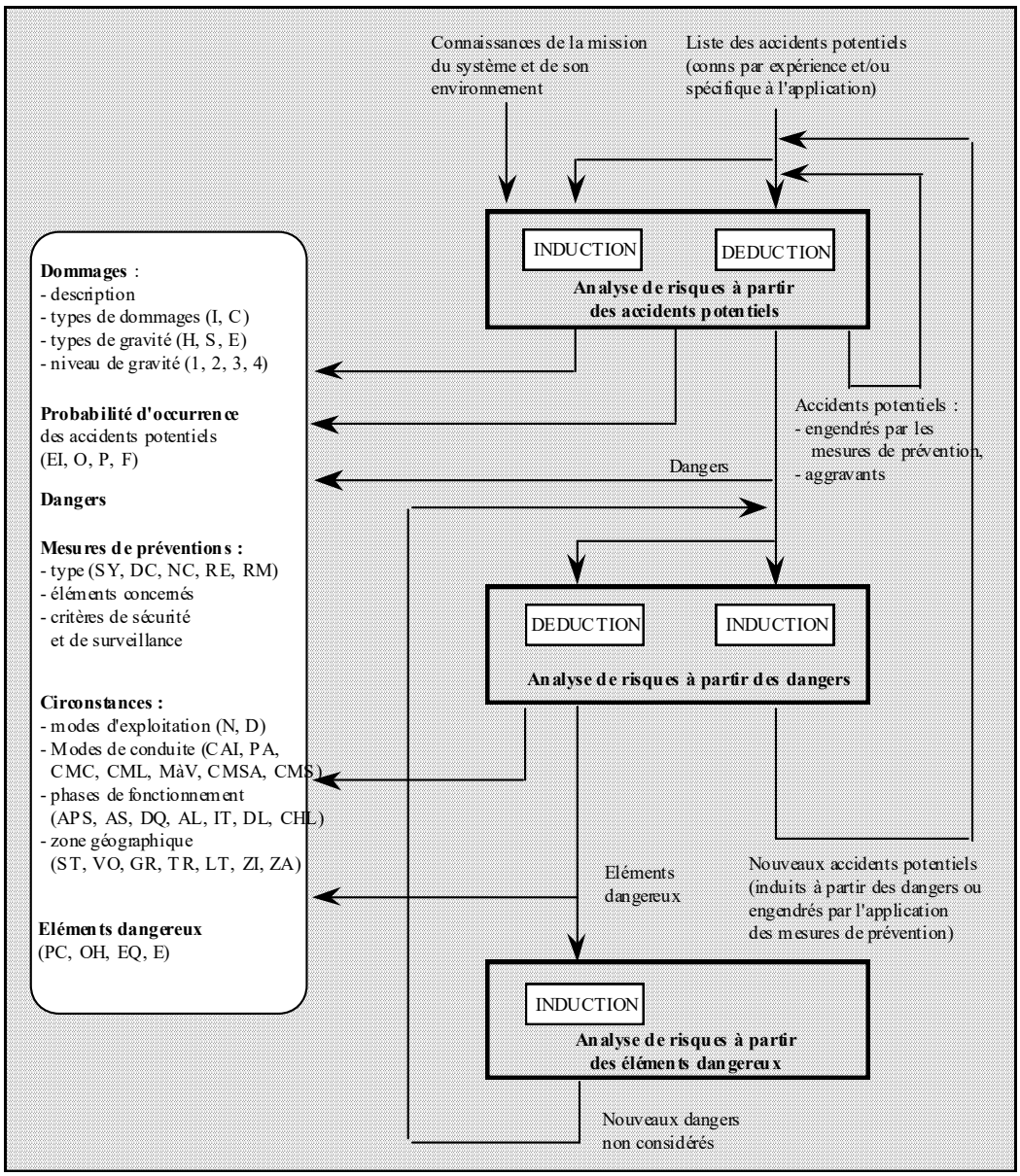

Figure 5 : Méthode d'élaboration d'une analyse préliminaire de risques [Hadj-Mabrouk 97]

5. ARCHITECTURE DE LA MAQUETTE DU SYSTÈME « SAPRISTI »

Les paragraphes précédents ont détaillé les différentes phases de conception du système « SAPRISTI ». L'étude de faisabilité de ce système, appliquée au domaine de la sécurité des automatismes des systèmes de transport guidés, a débouché sur la réalisation d'une maquette (en cours de validation) de capitalisation et d'aide à l'élaboration des APR. L'objectif principal de cet outil est non seulement de capitaliser les connaissances en matière d'APR mais aussi d'assister les experts chargés d'élaborer ou d'évaluer de nouveaux dossiers d'APR.

L'architecture fonctionnelle de la maquette du système « SAPRISTI » est constituée de quatre principaux modules suivants illustrés par la figure 6 [Hadj-Mabrouk 97] :

- Une interface Homme-Machine qui permet d'assurer le dialogue avec les utilisateurs et/ou l'expert du domaine. Cette interface assure deux grandes fonctions. La première concerne la saisie et la mise à jour des connaissances nécessaires pour élaborer ou évaluer une APR. La seconde fonction permet la consultation des différentes connaissances produites par le système (résultats d'évaluation d'une nouvelle APR, la base des APR historiques, ...).

- Un module d'acquisition et de modélisation des connaissances. Chaque APR saisie est formalisée selon une terminologie (paramètres descriptifs) et un format de représentation des connaissances préétablis. Ce module permet également de contrôler certaines conditions nécessaires pour accepter une APR. Ces critères de recevabilité concernent par exemple le respect de contraintes et critères de construction de l'APR qui sont intrinsèquement imposés par le formalisme de représentation défini ou encore le respect de la présence de descripteurs « clés » ou minimaux » pour élaborer une APR pertinente. En résumé, ce module permet non seulement le recueil et la formalisation des connaissances mais il constitue également le premier niveau d'évaluation syntaxique d'une APR.

- Un module d'élaboration de nouvelles APR. Ce module permet de dérouler successivement les trois étapes de la méthode d'APR : analyse « inductive-déductive » à partir des accidents potentiels, analyse « déductive-inductive » à partir des dangers et enfin analyse « inductive » à partir des éléments dangereux ». La coalition de ces trois analyses itératives permet de s'assurer de la complétude de l'analyse de risque. En ce sens, ce module représente le deuxième niveau d'évaluation d'une APR en termes de complétude.

- Un module d'évaluation des APR. Ce module, qui constitue le troisième niveau d'évaluation, fait appel à des connaissances expertes d'évaluation (règles, stratégies et heuristiques) en vue de produire des recommandations en termes de consistance, de pertinence et d'adéquation de l'APR.

- Une base de connaissances qui regroupe les APR historiques archivées, les nouvelles APR en cours d'évaluation et les avis émis par le module d'évaluation qui représentent des suggestions, des recommandations ou des explications.

A ce jour, seule une partie des deux modules d'acquisition et d'élaboration permettant le remplissage de la base de connaissances est opérationnel [Raîs 96]. A titre d'exemple, nous présentons ci-après (figure 7) quelques exemples d'écrans de l'interface réalisée qui permet d'aider l'utilisateur d'une part à élaborer une APR et d'autre part à enrichir et mettre à jour la base de connaissances. Dans le cadre de l'étude de faisabilité du système « SAPRISTI », notre premier souci a été de valider la méthode proposée plutôt que de privilégier une étude approfondie et coûteuse des outils et langages de développement nécessaires au développement d'un système. La maquette a donc été implémentée sur station Sun grâce au langage de programmation Tcl-Tk. Ce langage qui permet d'effectuer des développements d'interfaces, a la particularité d'être exploitable sur d'autres machines : station, PC ou Macintosh

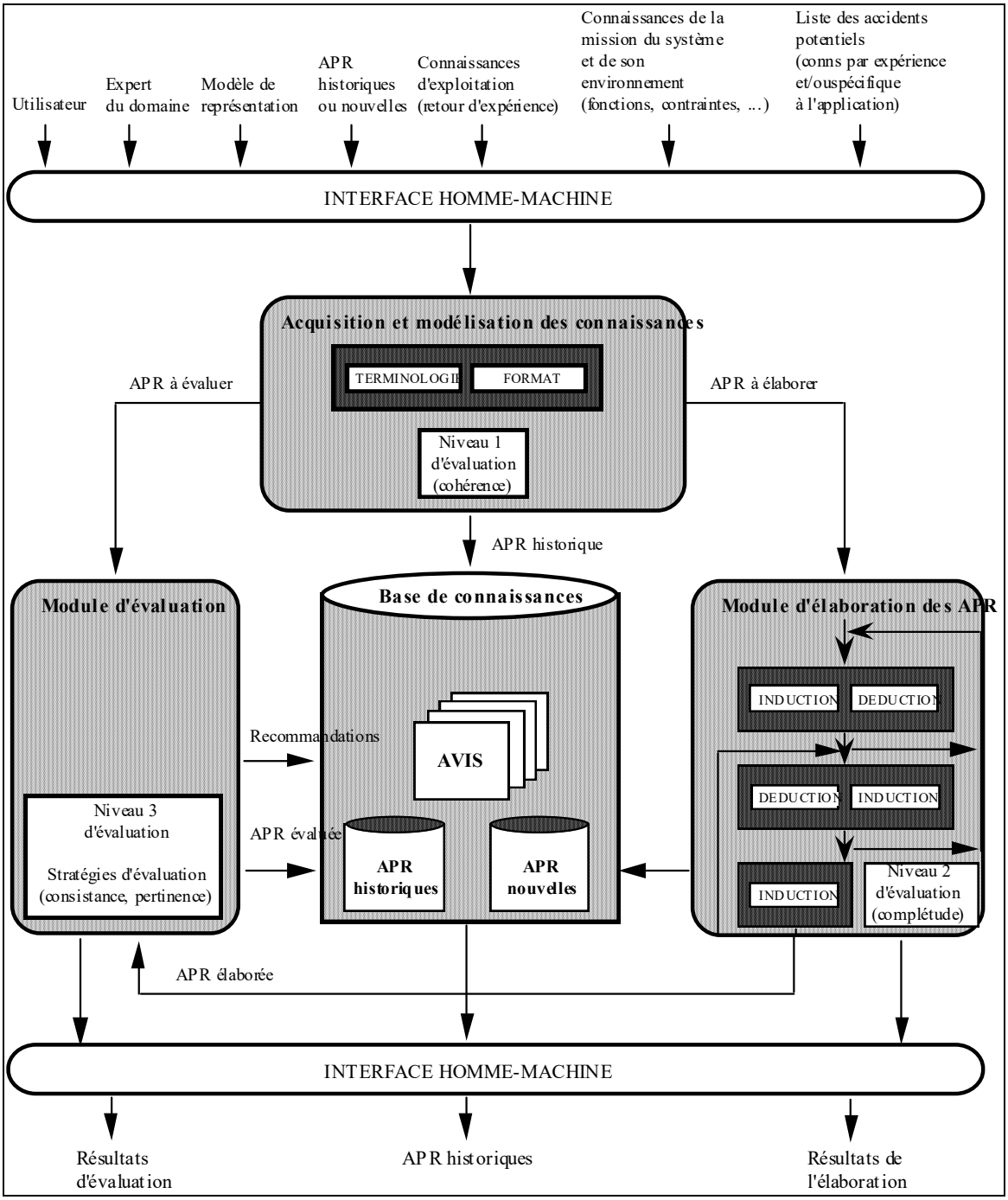

Figure 6 : architecture fonctionnelle de la maquette du système « SAPRISTI » [Hadj-Mabrouk 97]

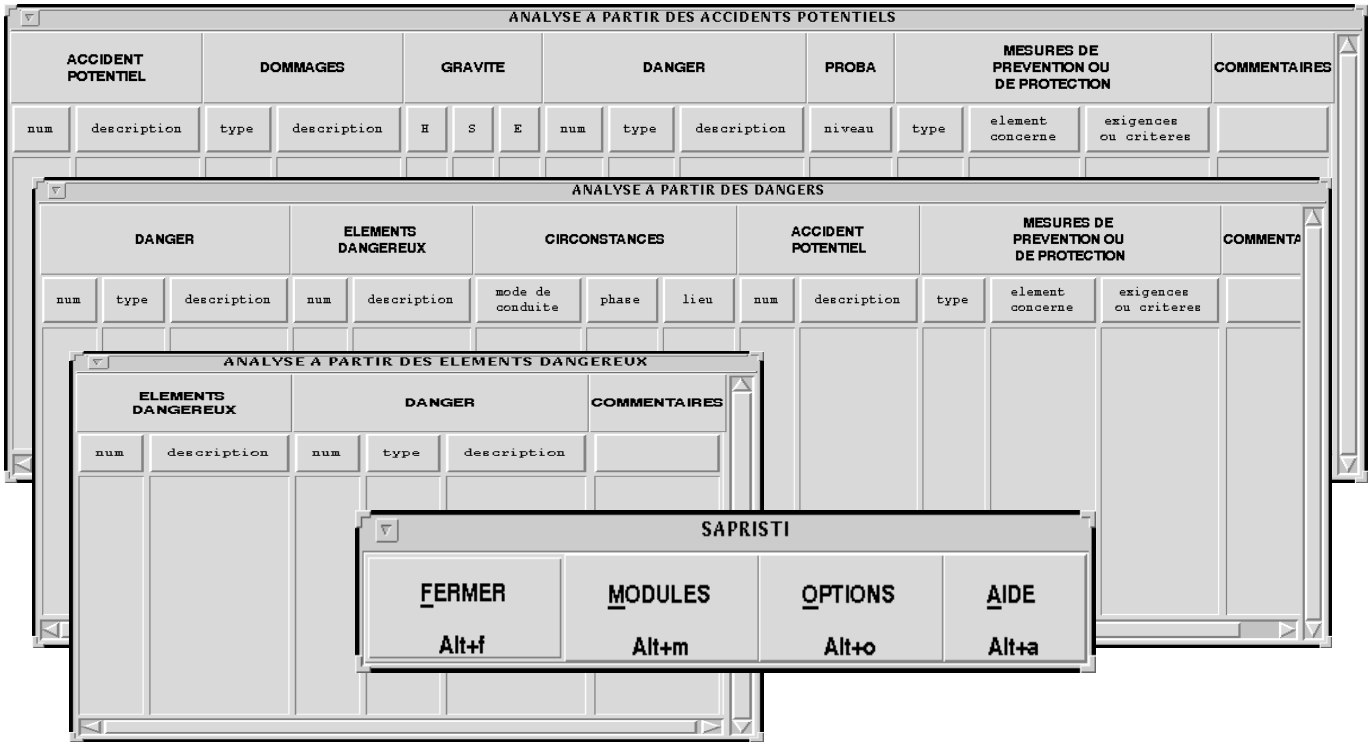

Figure 7 : Exemples d'écrans de l'interface d'aide à l'acquisition et à l'élaboration des APR [Raîs 96]

6. CONCLUSION

Bien que primordiale dans le processus de construction de la sécurité, l'analyse préliminaire de risques est très différemment exercée et demeure mal définie. Plus particulièrement, le vocabulaire, la démarche d'élaboration et le format de représentation ne sont pas consolidés. Le recours à une démarche d'analyse rigoureuse et admise par tous les acteurs qui prennent part à l'élaboration d'un dossier de sécurité s'impose. Cette méthode qui repose sur un format de représentation tabulaire, s'articule autour de trois étapes d'analyse complémentaires et itératives incluant conjointement des processus d'induction et de déduction. La principale originalité de cette nouvelle démarche réside essentiellement au niveau de la cohérence et de la complétude de l'analyse des risques. Cette méthode a pour vocation d'aider l'ensemble des acteurs (maître d'oeuvre, maître d'ouvrage, organismes de certification,...) qui participent à l'élaboration et à la validation d'un dossier de sécurité et contribue à l'amélioration du processus de construction de la sécurité des systèmes.

Pour montrer la faisabilité et la validité de cette nouvelle méthode d'analyse préliminaire de risques, une évaluation a été effectuée qui s'appuie sur un exemple d'application issu du domaine de la sécurité d'automatismes des systèmes de transport guidés. En dépit de quelques limites, cette première évaluation montre le double intérêt de la démarche proposée : d'une part l'association de ces trois analyses itératives permet de tendre vers l'exhaustivité de l'analyse préliminaire de risques et d'autre part le modèle proposé tolère la représentation de différentes analyses préliminaires de risques dans un même format. En ce sens, cette nouvelle méthode facilite les tâches d'élaboration et d'évaluation des nouvelles analyses et par conséquent permet de rationaliser les démarches conventionnelles.

Les domaines d'application de cette méthode sont diverses et concernent notamment les secteurs où la sécurité est une exigence absolue, comme les transports ferroviaires, aériens ou maritimes, ou encore l'industrie nucléaire. Cette méthode est en cours de mise en oeuvre dans d'autres conditions industrielles afin de valider et éventuellement d'améliorer la méthode proposée.

7. BIBLIOGRAPHIE

[BNAE 84] : Bureau de Normalisation de l'Aéronautique et de l'Espace (BNAE). «Principe de construction de la sécurité d'un système missile ou spatial». Recommandation RE.Aéro 701 10, Boulogne-Billancourt, 1984.

[BNAE 86] : Bureau de Normalisation de l'Aéronautique et de l'Espace (BNAE). «Guide des méthodes courantes d'analyse de la sécurité d'un système missile ou spatial». Recommandation RE.Aéro 701 11, Boulogne-Billancourt, 1986.

[BNCF 90] : Bureau de Normalisation des Chemins de Fer (BNCF). «Installations fixes et matériel roulant ferroviaires - Informatique - Sûreté de fonctionnement des logiciels - Généralités». Norme française homologuée NF F 71-011, Paris, 1990.

[BNCF 93] : Bureau de Normalisation des Chemins de Fer (BNCF). «Matériel ferroviaire en général - Fonctions de sécurité - Méthode de détermination et règles de traitement». Norme française homologuée NF F 00-101, Paris, 1993.

[CEI 94] : Commission Électrotechnique Internationale (CEI). «Analyse de risques des systèmes technologiques - Guide d'application». Projet de comité CEI 56 (sec) 410, Genève, 1994.

[CENE 93] : Comité Européen de Normalisation Électrotechnique (Cenelec). «Applications aux Chemins de Fer : Systèmes Électroniques de Sécurité de Commande et de Contrôle des Chemins de Fer». Projet de norme prEN 50129, Bruxelles, 1993.

[CENE 94a] : Comité Européen de Normalisation / Comité Européen de Normalisation Électrotechnique (Cen/Cenelec). Mémorandum n°9. «Principes directeurs pour inclure dans les normes les aspects liés à la sécurité». Première édition. Bruxelles, 1994. (Version européenne modifiée du Guide Iso/CEI n°51).

[CENE 94b] : Comité Européen de Normalisation Électrotechnique (Cenelec). «Spécification et preuve de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) pour les applications ferroviaires». Version 00.06, Projet de norme prEN 50126, Bruxelles, 1994.

[CENE 94c] : Comité Européen de Normalisation Électrotechnique (Cenelec). «Applications aux Chemins de Fer : Logiciels pour Systèmes de Commande et de Protection Ferroviaire». Version 0.6, Projet de norme prEN 50128, Bruxelles, 1994.

[Chopard-Guillaumot, Hadj-Mabrouk et Ganascia, 95] : « Proposition d'un modèle générique d'analyses préliminaires de risques pour les transports guidés ». Rapport ESTAS/A-95-03, convention INRETS/LAFORIA, diffusion restreinte, Arcueil, juin 1995, 45 p.

[Chopard-Guillaumot, Hadj-Mabrouk et Ganascia, 96] : « Contribution à une meilleure définition de l'analyse préliminaire de risques pour les systèmes de transport guidés ». *Journal Européen des Systèmes Automatisés (RAIRO-APII-JESA),* Paris, vol. 30, n° 1, pp 121-143, Avril 1996.

[Chopard-Guillaumot et Hadj-Mabrouk 96] : Chopard-Guillaumot G., Hadj-Mabrouk H. « Définition des principaux concepts relatifs à la notion de sécurité dans les transports guidés ». *Revue Générale des Chemins de Fer*, Paris, n° 2, pp 23-36, Février 1996.

[Hadj-Mabrouk 94a] : Hadj-Mabrouk H. « Examen du dossier Analyse Préliminaire des Risques (APR) du système KVBP/KVIM du projet ANTARES ». Rapport INRETS-ESTAS CR/A-94-64, diffusion restreinte, Arcueil, 2 Décembre 1994, 35p.

[Hadj-Mabrouk 94b] : Hadj-Mabrouk H. « L'analyse préliminaire des risques dans le domaine de la sécurité des transports guidés ». LAFORIA , Université de Paris VI, 21 septembre 1994.

[Hadj-Mabrouk 94c] : Hadj-Mabrouk H. « Formalisme de représentation et d'acquisition des Analyses Préliminaires des Risques ». Rapport de convention dans le cadre du programme PREDIT-ASCOT, diffusion restreinte, Arcueil, CR/A-94-46, 30 Juin 1994, 48 p.

[Hadj-Mabrouk et Bied-Charreton 95] : Hadj-Mabrouk H., Bied-Charreton D. « Avis de l'INRETS sur le document Analyse Préliminaire des Risques (APR) du système KVBP/KVIM du projet ANTARES ». Rapport ESTAS/A-95-15, diffusion restreinte, Arcueil, 16 mars 1995, 38 p.

[Hadj-Mabrouk 95] : Hadj-Mabrouk H. « La maîtrise des risques dans le domaine des automatismes des systèmes de transport guidés : Le problème de l'évaluation des analyses préliminaires de risques ». *Revue Recherche-Transport-Sécurité*, numéro 49, France, décembre 1995, pp 101-112.

[Hadj-Mabrouk 96a] : Hadj-Mabrouk H. « Méthodes et outils d'aide aux analyses de sécurité dans le domaine des transports terrestres guidés ». *Revue Routes et Transports*, Montréal-Québec, vol. 26, n° 2, pp 22-32, Été 1996.

[Hadj-Mabrouk 96b] : Hadj-Mabrouk H. « Capitalisation et évaluation des analyses de sécurité des automatismes des systèmes de transport guidés ». *Revue Transport Environnement Circulation*, Paris, TEC n° 134, pp 22-29, Janvier-février 1996.

[Hadj-Mabrouk et al. 96] : Hadj-Mabrouk H., Chopard-Guillaumot G, Darricau M. « Tools for providing aid for modelling, storing and assessing safety analyses in the area of terrestrial guided transport ». 29th Isata, *29e Symposium international sur les technologies de l'automobile et de l'automatique*, Florence-Italie, pp 357-364, 3-6 juin 1996.

[Hadj-Mabrouk 97] : Hadj-Mabrouk H. « Projet SAPRISTI : proposition d'une méthode et d'une maquette de système d'aide à l'élaboration et à la capitalisation des analyses préliminaires de risques ». Rapport d'avancement des travaux de recherche n° ESTAS/A-97-66, INRETS, Arcueil, 19 novembre, 1997, 17p.

[Lievens 76] : Lievens C. «Sécurité des systèmes». Cépaduès Éditions, Toulouse, 1976.

[RAÎS 96] : RAÎS F. « Analyse et conception de l'interface d'un logiciel d'élaboration des analyses préliminaires de risques ». *Rapport de stage de fin de 2ème année d'école d'ingénieur* - Institut d'informatique d'entreprise (CNAM-IIE). INRETS, Arcueil, septembre 1996, 30 p.

[Villemeur 88] : Villemeur A. «Sûreté de fonctionnement des systèmes industriels». Éditions Eyrolles, Paris, 1988.

II/ Aide à l'analyse de la sécurité au niveau LOGICIEL

INTRODUCTION

Cette section présente successivement deux projet de recherche qui s'inscrivent dans le cadre des analyses de sécurité au niveau logiciel :

- Projet « SAUTREL » : maquette de système d'aide aux analyses des effets des erreurs de logiciels (AEEL) de sécurité basé sur le raisonnement à partir de cas ;

- « SPECIALS » : méthode de spécification et d'aide à l'évaluation des logiciels critiques de sécurité basée sur l'utilisation des graphes conceptuels de Sowa.

1/ Projet « SAUTREL »

Maquette de système d'aide aux analyses des effets des erreurs de logiciels (AEEL) de sécurité basé sur le raisonnement à partir de cas

1. CONTEXTE GÉNÉRAL DE LA RECHERCHE ET COLLABORATIONS SCIENTITIQUES

Le processus de construction de la sécurité d'un système de trasport guidé fait intervenir trois grandes activités d'analyses de sécurité : analyse au niveau système, analyse au niveau logiciel et analyse au niveau matériel. Notre recherche s'inscrit dans le cadre de l'analyse de sécurité des logiciels et porte plus précisément sur la méthode d'Analyse des Effets des Erreurs du Logiciel (AEEL). L'objectif de l'étude est le développement d'un outil logiciel « SAUTREL » basé sur l'utilisation conjointe des techniques d'apprentissage automatique et d'acquisition des connaissances pour aider à capitaliser et à juger l'exhaustivité et la cohérence des AEEL critiques d'un nouveau système. Les principaux résultats obtenus sont :

- un formalisme de représentation des AEEL,
- une base de 250 cas d'AEEL issue des travaux de recueil et de modélisation des connaissances de deux systèmes de transport guidés déjà certifiés,
- une maquette «SAUTREL» d'aide à la capitalisation et à l'évaluation des AEEL basée sur le raisonnement à partir de cas,
- une démarche de génération automatique des critères d'évaluation des AEEL fondée essentiellement sur l'emploi d'un système d'apprentissage de règles.

Cette recherche a été réalisée en collaboration avec le Laboratoire d'Informatique de Paris 6 (ex. LAFORIA), le Laboratoire LAMSADE de l'Université de Paris Dauphine et l'Ecole Polytechnique Féminine (EPF). Dans le cadre de cette étude, j'ai encadré un DEA IARFA (Intelligence Artificielle, Reconnaissance des Formes et Application) [Darricau 95b], un stage de DESS d'Ingénierie de l'aide à la décision [Ndiaye 96] et un Ingénieur de l'Ecole Polytechnique Féminine [Darricau 95a]. L'organisme intéressé par les résultats de cette recherche est MATRA Transport.

2. L'ANALYSE DES EFFETS DES ERREURS DU LOGICIEL (AEEL)

Il est actuellement impossible de démontrer de manière irréfutable qu'un logiciel est exempt de toute erreur. En France et dans le domaine ferroviaire, la technique du monoprocesseur codé est utilisée pour assurer la sécurité d'exécution des logiciels. Cependant, cette technique n'assure pas de protection vis-à-vis des erreurs de conception du logiciel, des erreurs de conformité du code, des erreurs du logiciel de sécurité non codé et enfin des erreurs d'implémentation du processeur codé. L'analyse des effets des erreurs de logiciel (AEEL) peut, quant à elle, prendre en charge, entre autres, l'analyse de ces erreurs. L'analyse des effets des erreurs de logiciel [Thireau 86] [AFNOR 90] [Darricau 95a 95b] [Darricau et Hadj-Mabrouk 95a] est une démarche d'analyse inductive dont le but est la détermination de la nature et de la gravité des conséquences des défaillances du logiciel. L'AEEL permet également de guider les activités de validation et de maintenance du logiciel en indiquant les modules les plus critiques vis-à-vis de la sécurité. En effet, l'AEEL permet d'estimer le niveau d'effort de validation à effectuer sur les divers éléments du logiciel et en particulier, de guider les relectures de code et de mieux cibler les tests. Cette analyse est réalisée en envisageant des hypothèses d'erreurs de logiciels et en examinant les conséquences de ces erreurs sur les autres modules ainsi que les défaillances qui pourraient en découler au niveau du système. L'analyse des effets des erreurs de logiciel propose finalement des mesures visant à détecter les erreurs et à améliorer la robustesse du logiciel.

Les analyses des effets des erreurs de logiciel (AEEL) sont effectuées au cours de la branche descendante du cycle en «V» de développement du logiciel. Leur place dans ce cycle n'est fixée que par la norme française NF F 71-012 [AFNOR 90] qui préconise de les débuter en phase de conception préliminaire lorsque les éléments logiciels de sécurité sont identifiés, et d'en tenir compte lors des phases de conception détaillée et de codage. Les AEEL sont souvent utilisées par les sociétés ferroviaires européennes. En effet, les AEEL sont recommandées par la SNCF, hautement recommandées par la SNCB (Société Nationale des Chemins de Fer Belge), la FS (Ferrovié dello Stato), la société italienne Ansaldo, et le LUL (London Underground Limited) et exigées par British Railways et GEC Alsthom. Enfin, les AEEL sont exigées par l'association des ingénieurs de la signalisation des chemins de fer pour contribuer à prouver la sûreté du logiciel.

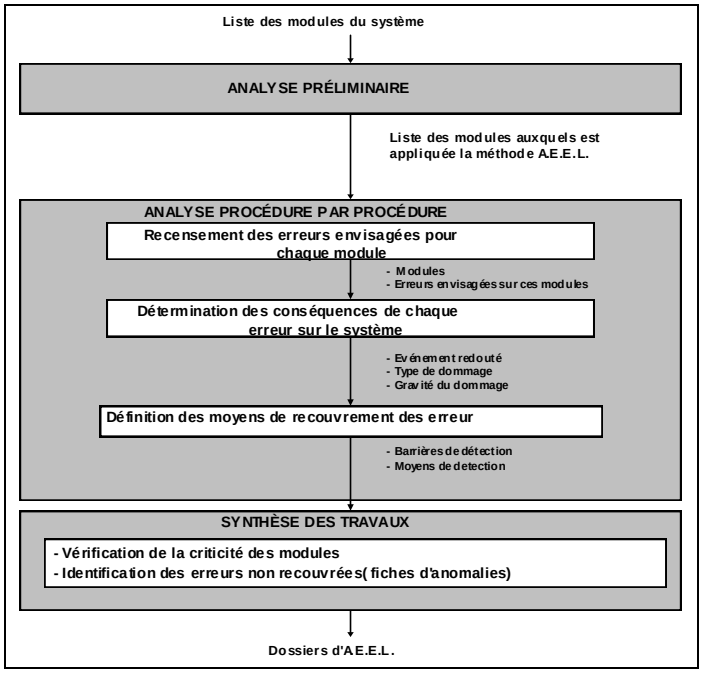

Figure 1 : Démarche d'élaboration d'une AEEL [AFNOR 90].

3. MOTIVATIONS DE L'ETUDE

Toutes les constatations précédemment citées montrent que l'AEEL est considérée comme une pièce importante du dossier de sécurité d'un système. C'est un document fondamental dans le processus de construction et de validation de la sécurité des logiciels critiques. Néanmoins, l'analyse attentive de certains dossiers d'AEEL des systèmes de transport guidé déjà certifiés ou homologués permet d'en révéler certaines lacunes[Hadj-Mabrouk et Darricau 96]. D'une part, les fiches d'AEEL ont des formats de représentation extrêmement variés d'un constructeur à l'autre (figure 2) et d'autre part la démarche d'élaboration et d'évaluation d'un dossier AEEL se révèle être un exercice particulièrement délicat et fastidieux qui n'est soutenu par aucune stratégie formalisée. En effet, l'exhaustivité et la cohérence des analyses demeurent essentiellement fondées sur le savoir-faire, l'intelligence et l'intuition des experts du domaine.

Exemple de fiche AEEL du système A

N° item	Procèdure étudié	Erreur envisagée	Conséquences sur le module	Critère non respecté	Criticité	Moyen de détection	Critère si détection	Criticité si détection

Exemple de fiche AEEL du système B

Mission analysée	Mode de défectuosité	Risques systémes	Gravité	Détection	Criticité

Exemple de fiche AEEL du système C

Composant	Sortie	Erreurs considérées	Effets sur les composants critiques	Effets sur le système

Figure 2 : Exemples de fiches AEEL des systèmes de transport guidés

4. APPROCHE RETENUE POUR DEVELOPPER L'OUTIL « SAUTREL »

Pour apporter un élément de réponse à ces problèmes, nous avons développé un outil logiciel d'aide à la capitalisation et à l'évaluation des dossiers AEEL, baptisé « SAUTREL ». L'approche retenue pour concevoir et mettre en œuvre cet outil repose en grande partie sur l'emploi des techniques d'intelligence artificielle (techniques d'acquisition de connaissances, raisonnement à partir de cas, apprentissage de règles à partir d'exemples,...) [Hadj-Mabrouk 93, 95] et fait intervenir les trois principales étapes suivantes [Hadj-Mabrouk 96a] : modélisation et acquisition des connaissances d'AEEL, constitution d'une base de cas d'AEEL et enfin développement de l'outil « SAUTREL ».

4.1 Modélisation et acquisition des connaissances d'AEEL

Cette étape d'analyse et d'abstraction a débouché sur l'élaboration d'un formalisme d'AEEL qui tient compte des usages et de l'expérience de l'INRETS en la matière. Ce modèle est fondé sur huit paramètres caractéristiques : Système étudié, Sous-système étudié, Module étudié, Erreur envisagée (famille, classe, type), Critère de sécurité non respecté par l'erreur, Evénement redouté, Type et gravité du dommage, Barrière et moyens de détection de l'erreur. Ce formalisme a été établi à partir de l'examen de 800 fiches AEEL relatives à deux systèmes de transport guidés. Il propose un cadre méthodologique d'élaboration des dossiers AEEL et contribue ainsi à assurer la qualité des analyses futures. Un extrait de ce formalisme est présenté dans la figure 3.

PARAMETRES CARACTERISTIQUES D'UNE A.E.E.L.		
SYSTEME ETUDIE		
SYSTEME A		
SYSTEME B		
SOUS-SYSTEME ETUDIE		
Bord		
Sol		
MODULE ETUDIE		
Localisation de l'élément et du train.		
Evacuation et surveillance des portes.		
...		
ERREURS ENVISAGEES		
Familles d'erreur.	**Classes d'erreurs.**	**Erreurs.**
Erreur de calcul.		
	Evaluation d'une équation incorrecte.	
		Calcul erroné.
...	**...**	**...**
Erreur d'algorithme.		
	Erreur de séquencement d'instruction.	
		Oubli d'un cas possible lors d'un test.
...	**...**	**...**
CRITERES DE SECURITE NON RESPECTES PAR L'ERREUR		
Critères relatifs à l'anticollision bord		
Déclenchement du FU en cas d'itinéraire du PA de type inconnu ou de non-concordance de position d'aiguille.		
...		
EVENEMENTS REDOUTES		
collision		
Maintien de la HT		
Chute d'un voyageur sur la voie		
...		
DOMMAGES		
type		
individuel		
collectif		
gravité		
Niveau 0 (pas de blessé, dégradations peu importantes)		
Niveau 1 (blessures légères, dommages localisés)		
Niveau 2 (blessures graves, dommages importants)		
Niveau 3 (morts d'homme, destruction du système)		
DETECTION DE L'ERREUR		
barrière de détection		
Non détectable.		
Détectable par des barrières matérielles au niveau système.		
Détectable par des barrières logicielles implantées dans d'autres modules.		
Détectable par des barrières logicielles implantées dans le module.		
Moyens de détection		
Spécification d'implantation de balise ...		
...		

Figure 3 : Extrait du formalisme élaboré pour la représentation des fiches A.E.E.L.[Darricau, Hadj-Mabrouk 95a]

4.2 Constitution d'une base de cas d'AEEL

Sur la base du modèle de représentation précédent, nous avons constitué une bibliothèque de 220 cas types. Ces exemples historiques d'AEEL sont issus de l'examen de deux systèmes de transport guidés : MAGGALY de Lyon et TVM 430 du TGV Nord.

4.3 Développement de la maquette « SAUTREL »

L'objectif visé par cet outil est d'exploiter les AEEL historiques (base de cas), menées sur des logiciels de sécurité déjà certifiés, en vue d'aider à l'élaboration et à l'évaluation de la complétude, de la cohérence et de la pertinence des AEEL d'un nouveau logiciel critique. L'approche suivie pour réaliser cet outil est fondée notamment sur l'utilisation d'une technique de raisonnement à partir de cas [Darricau et Hadj-Mabrouk 95a], [Hadj-Mabrouk 96c]. Le raisonnement à partir de cas (ou *Case Based Reasoning* : C.B.R.) est un des types de raisonnement en intelligence artificielle, dans le domaine de l'apprentissage automatique.

L'apprentissage est un terme très général qui décrit le processus selon lequel l'être humain ou la machine peut accroître sa connaissance. Apprendre c'est donc raisonner : découvrir des analogies et des similarités, généraliser ou particulariser une expérience, tirer parti de ses échecs et erreurs passés pour des raisonnements ultérieurs. Le principe général du CBR consiste à traiter un nouveau problème (cas cible) en se remémorant des expériences passées voisines (cas de référence). Ce type de raisonnement repose sur l'hypothèse suivante : si une expérience passée et la nouvelle situation sont suffisamment similaires, alors tout ce qui peut être expliqué ou appliqué à l'expérience passée (base de cas) reste valide si on l'applique à la nouvelle situation qui représente le nouveau problème à résoudre (figure 4).

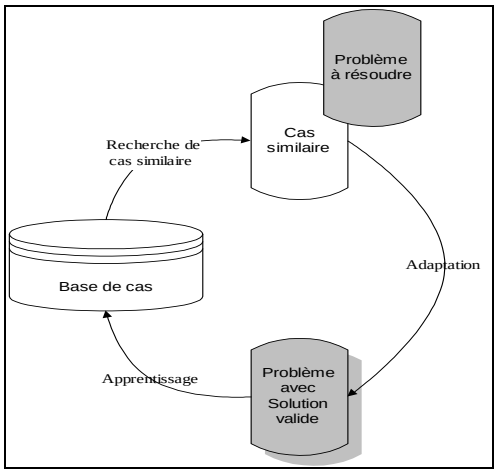

Figure 4 : Cycle du raisonnement à partir de cas

Les travaux de [Slade 91], [Harmon 91], [Rougegrez 93], [Kolodner 89, 91, 92, 93], [Beaubouche r 93], [Mott 93], [Pinson 93], [Smail 93], [Lieber 93] et [Darricau et Hadj-Mabrouk 95b], retracent de façon assez complète l'évolution des recherches dans le domaine du raisonnement à partir de cas.

La maquette « SAUTREL » a été réalisée sur PC à l'aide du logiciel Recall et comporte quatre principaux modules [Darricau et Hadj-Mabrouk 95a], [Hadj-Mabrouk et Darricau 96b] (figure 5) :

- Interface Homme/Machine pour l'introduction, la mise à jour et la consultation des connaissances des AEEL ;
- Module de formalisation et d'acquisition des fiches AEEL ;
- Base de connaissances qui regroupe 250 cas d'AEEL (base d'expériences) ;
- Processus de raisonnement à partir de cas qui comporte principalement :
  - un mécanisme d'indexation (ou de caractérisation) de cas cible ;
  - un mécanisme de recherche et de recueil de cas similaires (cas source) ;
  - un mécanisme d'adaptation des solutions des cas extraites afin de résoudre le problème spécifié par le cas cible.

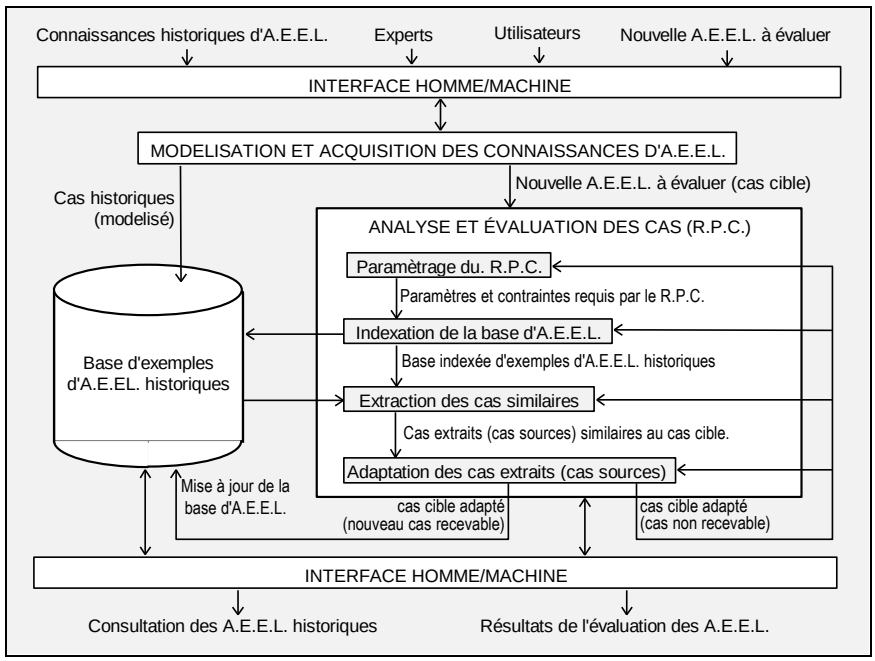

Figure 5 : Architecture fonctionnelle de la maquette du système « SAUTREL » d'aide aux AEEL [Darricau et Hadj-Mabrouk 95a], [Hadj-Mabrouk 96b]

5. EXEMPLE D'APPLICATION DE LA MAQUETTE DU SYSTEME « SAUTREL »

L'utilisation de la maquette « SAUTREL » requiert le passage par les huit étapes détaillées ci-après [Darricau et Hadj-Mabrouk 96b], [Hadj-Mabrouk et Darricau 96].

5.1. Définition du langage de description des exemples d'A.E.E.L.

Cette étape permet de saisir le langage de description d'une AEEL qui repose sur les huit descripteurs énoncés plus haut (figure 3). Un descripteur est un couple (attribut, valeur). Tous les attributs sont symboliques. Trois types de descripteurs ont pu être distingués : descripteurs énumérés, descripteurs multi-valués, descripteurs inconnus.

5.2. Élaboration de la base de cas d'A.E.E.L.

Il s'agit ici de créer des cas en affectant une valeur à chacun des attributs du langage de description. Cette base de cas pourra par la suite être modifiée ou consultée. L'acquisition du cas cible se fait en saisissant la ou les valeurs des différents attributs. Lors de cette étape de construction de la base de cas, le descripteur concept « événement redouté » est laissé inconnu car il représente la solution que nous recherchons dans la base de cas.

5.3. Paramétrage du R.P.C.

Lors de cette étape, l'utilisateur doit fixer différents paramètres permettant de configurer le processus de RPC. Ces choix concernent aussi bien le descripteur qui représentera la solution du problème que les stratégies d'indexation, d'appariement ou d'adaptation. Lors de cette étape, l'utilisateur doit fixer les différents paramètres suivants :

- Le descripteur « concept ». L'utilisateur doit choisir parmi les descripteurs celui qui représentera la solution du problème. Ce descripteur est appelé le "concept". Dans notre exemple, le concept est le descripteur "événement redouté". Le problème, quant à lui, sera caractérisé par tous les autres descripteurs.
- Les stratégies d'indexation. L'outil propose plusieurs stratégies permettant de hiérarchiser la mémoire. L'utilisateur peut paramétrer cette hiérarchisation en triant les descripteurs ou en élaguant la hiérarchie. Dans notre exemple, nous construisons la hiérarchie en prenant en compte tous les descripteurs et en imposant les descripteurs "système étudié" et "sous-système étudié", dans cet ordre, comme premier et deuxième niveau. Ensuite, le choix entre les descripteurs restant pour les niveaux suivants sera effectué par un algorithme de classification : ID3 [Quinlan 86].
- les stratégies d'appariement. L'utilisateur peut intervenir de plusieurs manières dans le calcul de la similarité entre deux attributs. Il peut préciser les descripteurs qui ne devront pas être pris en compte lors du calcul. Il peut donner un vecteur de poids pour indiquer l'importance relative d'un descripteur par rapport aux autres. Dans notre exemple, nous avons choisi de n'extraire que les 10 cas les plus similaires, et de donner un poids équivalent à tous nos descripteurs.
- Les stratégies d'adaptation. A ce jour, l'outil ne propose aucune méthode d'adaptation mais permet à l'utilisateur de programmer ses propres méthodes par des démons. Actuellement, cette adaptation peut se faire soit implicitement par l'expert, en comparant les cas similaires au cas cible, soit par la technique du vote : la valeur de l'attribut à adapter est calculée sur l'ensemble des cas similaires par un vote pondéré par le pourcentage de similarité de chacun des cas.

5.4. Saisie de l'A.E.E.L. à évaluer

L'acquisition du cas cible se fait en saisissant la ou les valeurs des différents attributs. La figure 6 montre un exemple de saisie de cas. Les attributs dont la valeur est "?" n'ont pas encore été renseignés et sont inconnus par défaut. En outre, nous laisserons le descripteur concept « événement redouté » inconnu car il représente la solution que nous recherchons dans la base de cas.

5.5. Étape d'indexation de la base de cas d'A.E.E.L.

Lors de cette étape d'indexation ou de hiérarchisation, l'utilisateur sélectionne la base de cas à indexer, puis il lance la construction de la hiérarchie. Dans notre exemple (figure 7), les deux premiers niveau de la hiérarchie sont construits à partir des descripteurs "système étudié" et "sous-système étudié". Les niveaux suivants sont déterminés par l'algorithme de classification. Ici, le troisième niveau porte sur le descripteur "gravité du dommage".

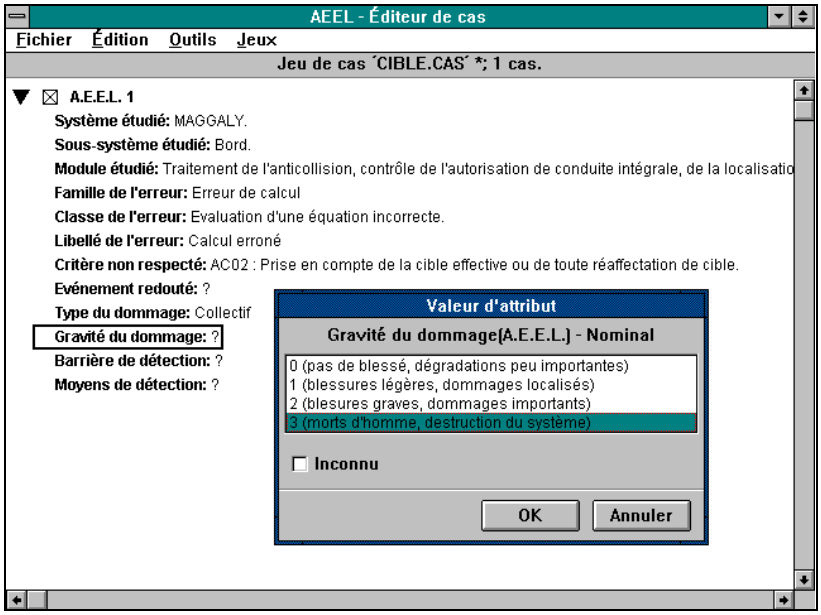

Figure 6. Exemple de cas cible en cours de saisie.

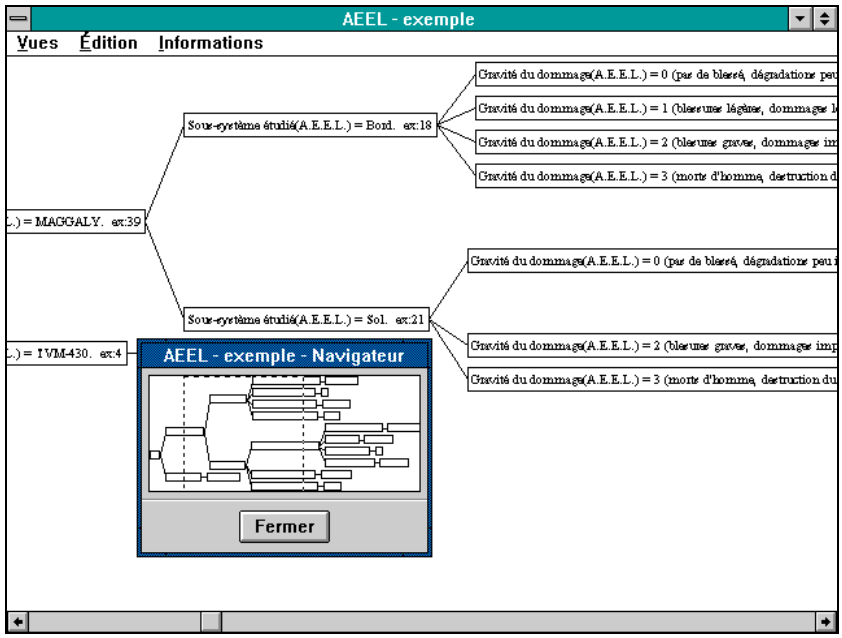

Figure 7 : Exemple d'arbre d'indexation.

5.6. Étape d'extraction des cas d'A.E.E.L. similaires

Cette étape permet de retrouver les AEEL historiques les plus proches de l'AEEL à examiner (cas cible). L'étape d'extraction des cas similaires est réalisée lorsqu'un cas cible a été sélectionné par l'utilisateur. L'écran présenté dans la figure 8 montre, pour notre exemple, le résultat de la recherche des cas similaires. Le cas cible est rappelé dans la colonne de droite, la colonne de gauche propose les 10 premiers cas les plus similaires et la colonne du milieu permet de visualiser un des cas similaires (ici le cas n°33).

5.7. Étape d'adaptation des cas extraits (cas sources)

A ce jour, l'outil ne proposant pas de stratégies d'adaptation, celle-ci est laissée à la charge de l'utilisateur. Avec l'écran présenté en figure 8, l'utilisateur peut consulter la valeur prise par l'attribut concept "événement redouté" dans chaque cas similaire et choisir lui-même la valeur à donner à l'attribut concept pour le cas cible. L'utilisateur peut aussi faire appel à la technique du vote. Dans notre exemple, l'outil propose une seule valeur pour l'attribut "événement redouté" : la collision.

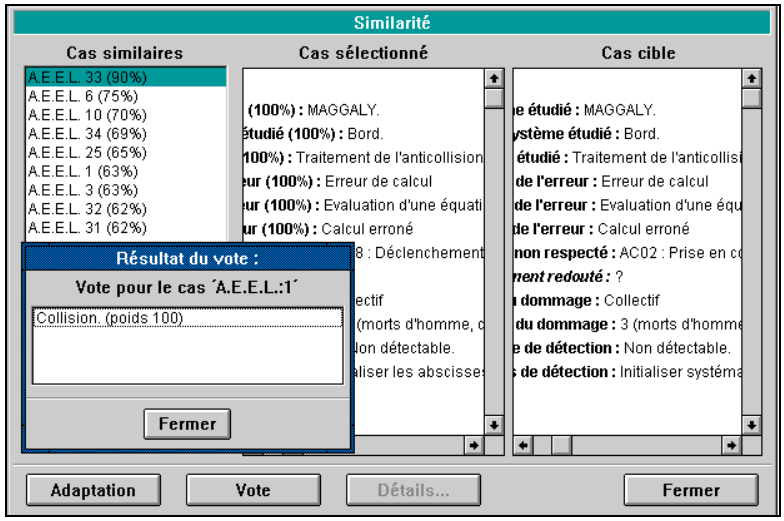

Figure 8 : exemple d'utilisation de la méthode de vote pour la recherche des cas similaires.

5.8. Mise à jour de la base de cas d'A.E.E.L.

Cette étape de mise à jour consiste à réaliser l'apprentissage en ajoutant le cas cible adapté dans la base de cas. Actuellement, cet apprentissage n'est pas incrémental. Le nouveau cas sera ajouté dans la hiérarchie sans que celui-ci soit reconstruit. C'est à l'utilisateur de prendre l'initiative de relancer l'indexation de la base de cas.

6. APPORTS ET LIMITES DE LA MAQUETTE « SAUTREL »

L'originalité de cet outil d'aide aux AEEL réside non seulement au niveau de sa capacité à capitaliser, à pérenniser et à diffuser l'expertise en matière d'AEEL mais il représente aussi les premiers travaux de recherche sur l'application du raisonnement à partir de cas aux AEEL [Hadj-Mabrouk 96a]. En effet, il n'existe pas actuellement, à notre connaissance, d'outil d'aide à l'élaboration et à l'évaluation des AEEL dans le domaine des systèmes de transport guidés. L'outil SAUTREL est à ce jour une maquette dont la première validation montre l'intérêt de la démarche d'aide aux AEEL proposée et qui, de ce fait, requiert certaines améliorations et extensions. Ces améliorations portent notamment sur le choix des critères d'évaluation des nouveaux cas d'AEEL, l'amélioration des stratégies d'adaptation des solutions proposées par le système, l'enrichissement de la base de cas d'AEEL pour couvrir l'ensemble du problème et enfin l'amélioration et la validation du formalisme de représentation des AEEL élaborées. En effet, ce modèle est perfectible et il ne s'agit encore que d'une base de travail pour la définition d'un modèle générique acceptable par tous les acteurs qui participent au développement des systèmes de transport guidés. En particulier, l'exhaustivité et la pertinence des descripteurs (ou paramètres) retenus pour caractériser une AEEL nécessitent pour certains une étude plus approfondie.

Le paragraphe suivant apporte un élément de reponse au premier problème soulevé ci-dessus : la recherche d'une démarche d'aide à la génération automatique des critères d'évaluation des nouveaux cas d'AEEL. Cette étude a été réalisée en collaboration avec le LAMSADE de l'Université de Paris Dauphine et dans le cadre d'un stage de fin d'étude en DESS d'Ingénierie d'aide à la décision [Ndaye 96] dont j'ai assuré l'encadrement scientifique. Dans ce même projet, une autre collaboration a été lancée avec le Professeur Jean-Gabriel GANASCIA du LIP6 qui a mis à notre disposition à l'INRETS-ESTAS son système d'apprentissage automatique des règles CHARADE [Ganascia 87]. En fait, l'objectif de la recherche engagée pour appréhender certaines limites de la maquette du système « SAUTREL » consiste à étudier la faisabilité d'engendrer automatiquement des critères d'aide à l'évaluation d'un dossier AEEL en ayant recours à une méthode d'apprentissage par détection de régularités empiriques.

7. DÉMARCHE D'AIDE À LA GÉNÉRATION AUTOMATIQUE DES CRITÈRES D'ÉVALUATION

L'objectif de la recherche que nous avons engagé pour appréhender certaines limites de la maquette du système « SAUTREL » consiste à étudier la faisabilité d'engendrer automatiquement des critères d'aide à l'évaluation d'un dossier AEEL en ayant recours à une méthode d'apprentissage par détection de régularités empiriques [Ndaye et Hadj-Mabrouk 96a, 96b]. Pour atteindre cet objectif, il est nécessaire de définir des critères d'évaluation des dossiers d'A.E.E.L. L'évaluation des dossiers d'A.E.E.L. est une tâche difficile, fastidieuse qui repose en grande partie sur le savoir-faire et l'expérience des experts du domaine.

Les connaissances détenues par ces experts sont essentiellement empiriques, évolutives et subjectives. De ce fait, l'extraction de la démarche d'évaluation pose problème. Pour apporter un élément de réponse à ce problème, l'étude a été orientée vers la recherche de critères d'évaluation à partir de la base de cas existante qui est notre seule matière première. Le présent paragraphe détaille l'utilisation du système d'apprentissage automatique CHARADE [Ganascia 87] en vue d'identifier, à partir des règles engendrées, des critères d'évaluation. L'utilisation de CHARADE, dans notre contexte, s'est déroulé en trois étapes détaillées ci-après [Ndaye 96] : transformation de la base de cas existante en base d'apprentissage, définition des contraintes d'apprentissage et enfin génération de règles.

7.1. Transformation de la base de cas existante en base d'apprentissage

Finalement, la base d'apprentissage regroupe deux fichiers :

- un fichier de descripteurs qui contient 11 descripteurs. Chaque descripteur est décrit par son nom, son type et son domaine (ensemble des valeurs possibles),
- un fichier d'exemples qui regroupe 224 exemples. Chaque exemple est une conjonction de descripteurs.

Les figures 9 et 10 suivantes présentent un échantillon de chaque fichier de la base d'apprentissage.

```
(defatt Systeme_etudie enumere
(valeurs Systeme_A Systeme_B  ))
(defatt Sous_systeme enumere
(valeurs Bord Sol ))
(defatt Module_etudie enumere
(valeurs Sequenceur Gestion_des_graphes_conduite_integrale_et_haute_tension
Gestion_du_tableau_des_elements_controles  ...))
(defatt Famille_erreur enumere
(valeurs Erreur_de_calcul Erreur_d_algorithme ...))
(defatt Classe_erreur enumere
(valeurs Autres Evaluation_d_une_equation_incorrecte ...))
(defatt Libelle_erreur enumere
(valeurs Calcul_errone Calcul_surestime Calcul_sous_estime ...))
(defatt Evenement_redoute enumere
(valeurs Collision Maintien_de_la_HT Maintien_de_la_haute_tension ...))
(defatt Type_dommage enumere (valeurs Individuel Collectif Aucun ))
(defatt Gravite_dommage enumere
(valeurs Zero_pas_de_blesse_degradations_peu_importantes ... ))
 (defatt Barriere_de_detection enumere
(valeurs Non_detectable Detectable_par_des_barrieres_materielles_au_niveau_systeme ...))
```

Figure 9 : Échantillon du fichier des descripteurs

```
defex Systeme_B_34 {
        (Systeme_etudie == Systeme_B)
        (Sous_systeme == Bord)
        (Module_etudie == Localisation_de_l_element_et_du_train)
        (Famille_erreur == Erreur_de_calcul)
        (Classe_erreur == Evaluation_d_une_equation_incorrecte)
        (Libelle_erreur == Calcul_surestime)
        (Evenement_redoute == Collision)
        (Type_dommage == Collectif)
        (Gravite_dommage == Trois_morts_d_homme_destruction_du_systeme)
}
```

Figure 10 : Échantillon du fichier d'exemples

7.2. Définition des contraintes d'apprentissage

L'utilisation de CHARADE nécessite de fixer différentes contraintes d'apprentissage [Ganascia 87]. Pour notre étude de faisabilité, nous n'avons exploité que les deux contraintes suivantes :

- Le facteur de bruit est égal à 0 afin de détecter toutes les régularités observables dans la base d'exemple,
- La structuration du système de règles de la façon suivante (figure 11):

Prémisses :	- Sous-système étudié,	***conclusions :*** - Événement redouté,	
	- Module étudié,		- Type du dommage,
	- Famille de l'erreur,		- Gravité du dommage,
	- Classe de l'erreur,		- Barrière de détection,
	- Libellé de l'erreur.		- Moyens de détection.

Figure 11 : structuration du système de règles

Ce choix s'explique par le fait que, pour réaliser les A.E.E.L., on envisage des erreurs sur des modules pour déterminer leurs conséquences sur le système et proposer des moyens de détection. Nous avons voulu traduire ce concept en choisissant comme prémisses les attributs qui décrivent l'erreur dans son contexte et comme conclusions les conséquences de l'erreur et les moyens mis en oeuvre pour les recouvrer. La figure 12 présente le fichier de description de la structure des règles adoptée. Dans ce fichier, le paramètre "roles" définit les prémisses (obs) et les conclusions (solution) des règles à générer. Le paramètre "infŽrence" précise l'orientation des règles (ici obs => solution). Et enfin le paramètre "tache" donne le nom de l'opération à exécuter (ici classifie).

```
roles {
        obs (   Sous_systeme
                Module_etudie
                Famille_erreur
                Classe_erreur
                Libelle_erreur)
        solution (      Gravite_dommage
                        Barriere_de_detection
                        Moyens_de_detection ) }
inference {
        classifie (obs) -> solution }
tache {
        classifie }
```

Figure 12 : Fichier de description de la structure des règles à générer

7.3. Génération des règles

A partir des fichiers de descripteurs, d'exemples, et de contraintes, CHARADE à engendrer plusieurs règles dont quelques une nous paraissent intéressantes pour dégager des critères d'évaluation des A.E.E.L. (figure 13).

```
(defrule classifie-R5 "1"
(classifie)
(Module_etudie == Traitement_de_l_anticollision)
(Libelle_erreur == Calcul_surestime)
=> (assert ( Type_dommage == Collectif )))
; Systeme_B_124; Soient 1 exemples.
**************************************************************************************************
(defrule classifie-R7 "4"
(classifie)
(Module_etudie == Localisation_de_l_element_et_du_train)
(Libelle_erreur == Calcul_sous_estime)
=> (assert ( Type_dommage == Collectif )))
;  Systeme_B_36  Systeme B_37  Systeme_B_51  Systeme_B_60;
Soient 4 exemples.
**************************************************************************************************
(defrule classifie-R12 "14"
(classifie)
(Module_etudie == Gestion_du_tableau_des_elements_controles)
=> (assert ( Type_dommage == Collectif )))
;   Systeme_B_89   Systeme_B_90   Systeme_B_91   Systeme_B_92   Systeme_B_93   Systeme_B_97   Systeme_B_100   Systeme_B_102
Systeme_B_104 Systeme_B_105 Systeme_B_106 Systeme_B_108  Systeme_B_109  Systeme_B_110;
Soient 14 exemples.
```

Figure 13 : Exemple de règles générées par le système d'apprentissage CHARADE

Les deux premières règles permettent à partir d'une erreur et d'un module, de conclure sur un type de dommage. En effet, selon la norme française [NF F 71-013], l'un des objectifs de l'A.E.E.L. est d'identifier les composants logiciels et évaluer leur niveau de criticité. Pour répondre à cet objectif, il est intéressant de connaître le type du dommage (individuel, ou collectif) pour une erreur donnée. Cette information peut aider à vérifier la criticité du module étudié. Concernant la règle R12, nous l'avons retenue car elle est couverte par 14 exemples. En effet, pour identifier les composants logiciels à évaluer, il peut être utile de savoir que pour un module, le type de dommage est généralement *collectif* (indépendamment de l'erreur).

8. CONCLUSION

Cette recherche a montré l'intérêt d'utiliser les méthodes d'apprentissage automatique pour aider à l'évaluation des analyses des erreurs de logiciel (AEEL) dans le domaine des automatismes des transports guidés. En effet, la maquette « SAUTREL », qui est encore au stade de validation, montre la faisabilité :

- d'employer le raisonnement à partir de cas (logiciel RECALL) pour capitaliser et aider l'expert dans sa tache cruciale d'évaluation des nouveaux dossiers d'AEEL par la recherche des cas similaires déjà traités et validés ;
- d'utiliser un système d'apprentissage de règles (CHARADE) pour aider à la définition de critères d'évaluation des A.E.E.L.

Les travaux en cours portent non seulement sur l'analyse et l'examen de l'ensemble des règles engendrées en vue d'extraire des critères d'évaluation des AEEL pertinents mais aussi sur l'enrichissement de la base d'exemples d'apprentissage.

9. BIBLIOGRAPHIE

[AFNOR 90] : « Installations fixes et matériel roulant ferroviaires. Informatique - Sûreté de fonctionnement des logiciels ». *Norme française F 71 012 et F 71 013*, décembre 1990.

[Beauboucher 93] : Beauboucher N. « La Similarité : un Problème Crucial en Intelligence Artificielle ». *Séminaire Raisonnement à Partir de Cas*, LAFORIA, rapport 93/42, 1 oct. 1993.

[Darricau 95a] : Darricau M. « Apport du raisonnement à partir de cas à l'analyse des effets des erreurs de logiciels. Application à la sécurité des logiciels critiques dans les transports guidés ». *Rapport de fin d'études d'ingénieur de l'École Polytechnique Féminine*. INRETS, Arcueil, juin 1995, 106 p.

[Darricau 95b] : Darricau M. « Maquette de faisabilité d'un outil basé sur le raisonnement à partir de cas pour l'aide à la capitalisation et à l'analyse des erreurs de logiciels. Application à la sécurité des logiciels dans les transports guidés ». *Mémoire de DEA IARFA (Intelligence Artificielle, Reconnaissance des Formes et Applications),* Université Paris 6 - Jussieu. INRETS, Arcueil, septembre 1995, 22 p.

[Darricau, Hadj-Mabrouk 95a] : Darricau M., Hadj-Mabrouk H. « Étude de faisabilité d'un outil d'aide aux analyses des effets des erreurs des logiciels, basé sur le raisonnement à partir de cas. Application à la sécurité des systèmes de transport guidé ». *Huitièmes journées internationales du génie logiciel et de ses applications*. Paris-La-Défense, 15-17 novembre 1995, pp 677-689.

[Darricau, Hadj-Mabrouk 95b] : Darricau M., Hadj-Mabrouk H. « Le raisonnement à partir de cas : une étude bibliographique ». *Rapport INRETS-ESTAS/A-95-28*, Arcueil, juin 1995, 20 p.

[Darricau, Hadj-Mabrouk 96a] : Darricau M., Hadj-Mabrouk H. « Applying case-based reasoning to the storing and assessment of software error-effect analysis in railway systems ». Comprail 96, *5e Conférence internationale sur la conception, la construction et l'exploitation assistées par ordinateur dans les systèmes de transport ferroviaires*, Berlin, pp 483-492, 21-23 août 1996.

[Darricau, Hadj-Mabrouk 96b] : Darricau M., Hadj-Mabrouk H. « L'analyses des effets des erreurs des logiciels, basé sur le raisonnement à partir de cas. Application à la sécurité des systèmes de transport guidé ». *La lettre de la sûreté de fonctionnement*, numéro 42-43, mai - juillet 1996, pp 677-689.

[Ganascia 87] : Ganascia J.-G. « AGAPE et CHARADE : deux mécanismes d'apprentissage symbolique appliqués à la construction de bases de connaissances ». *Thèse d'état*, Université Paris-sud, mai 1987.

[Hadj-Mabrouk 93] : Hadj-Mabrouk H. « Apport des Techniques d'Intelligence Artificielle à l'Analyse de la Sécurité des Systèmes de Transport Guidés». Revue Recherche - Transport - Sécurité n°40, sept. 1993.

[Hadj-Mabrouk 95] : Hadj-Mabrouk H. « L'apprentissage automatique : principes et exemple d'application au domaine de la sécurité ». JE'95*, Journées électronique et informatique pour la sûreté*, Commissariat à l'Énergie Atomique. Gif-sur-Yvette, 7-9 février 1995, pp 187-197.

[Hadj-Mabrouk 96 a] : Hadj-Mabrouk H., Chopard-Guillaumot G. Darricau M. « Tools for providing aid for modelling, storing and assessing safety analyses in the area of terrestrial guided transport ». 29th Isata, *29e Symposium international sur les technologies de l'automobile et de l'automatique*, Florence-Italie, pp 357-364, 3-6 juin 1996.

[Hadj-Mabrouk 96b] : Hadj-Mabrouk H. « Capitalisation et évaluation des analyses de sécurité des automatismes des systèmes de transport guidés ». *Revue Transport Environnement Circulation*, N° 134, France, janvier-février 1996, pp 12-22.

[Hadj-Mabrouk 96c] : Hadj-Mabrouk H. « Méthodes et outils d'aide aux analyses de sécurité dans le domaine des transports terrestres guidés ». *Revue Routes et Transports*, Montréal-Québec, vol. 26, n° 2, pp 22-32, Été 1996.

[Hadj-Mabrouk, Darricau 96] : Hadj-Mabrouk H., Darricau M. « SAUTREL : outil d'aide aux analyses des effets des erreurs de logiciels de sécurité dans les transports guidés ». λμ 10, *10e Colloque national de fiabilité et maintenabilité*, France, Saint-Malo, tome 2, pp 790-797, 1-3 octobre 1996.

[Harmon 91] : Harmon P. « Case-based reasoning II ». *Intelligent Software Strategies*, Vol. VII (12), p.1-9, 1991.

[Kolodner 89] : Kolodner J., Riesbeck C. « Cased-based reasoning (tutorial program) ». *Eleventh International Joint Conference on Artificial Intelligence*, August 1989.

[Kolodner 91] : Kolodner J. « Improving Human Decision Making through Case-Based Decision Aiding ». *Artificial Intelligence Magazine* vol. 12, summer 1991, pages 52 à 68.

[Kolodner 92] : Kolodner J. « An introduction to case-based reasoning ». *Artificial Intelligence Review*, Vol. 6 (1), p. 3-34, 1992.

[Kolodner 93] : Kolodner J. « Case-Based Reasoning ». *Morgan-Kaufmann Publishers*, Inc., 668 pages, 1993.

[Lieber 94] : Lieber J. « Le Raisonnement à Partir de Cas ». *Exposé au Pôle Intelligence Artificielle de l'INRETS*, 9 décembre 1994.

[Mott 93] : Mott S. « Case-based reasoning: Market, applications, and fit with other technologies ». *Expert Systems With Applications*, Vol. 6, p.97-104, 1993.

[Ndiaye 96] : Ndiaye A. « Aide à l'évaluation des analyses des effets des erreurs du logiciel. Application à la sécurité des systèmes de transports guidés. ». *Mémoire de stage de D.E.S.S. d'Ingénierie de l'aide à la décision*, Université Paris IX Dauphine. INRETS, Arcueil, septembre 1996, 40 p.

[Ndiaye, Hadj-Mabrouk 96a] : Ndiaye A., Hadj-Mabrouk H. « Apports et limites d'un outil d'aide aux analyses des effets des erreurs des logiciels ». Convention INRETS/LAMSADE, *rapport INRETS n° ESTAS/A-96-36*, diffusion restreinte, 17 p, Arcueil, juin 1996.

[Ndiaye, Hadj-Mabrouk 96b] : Ndiaye A., Hadj-Mabrouk H. « Identification de critères d'évaluation des A.E.E.L. à l'aide d'un système d'apprentissage : une étude de faisabilité ». Convention INRETS/LAMSADE, *rapport INRETS n° ESTAS/A-96-52*, rapport confidentiel, 24 p, Arcueil, septembre 1996.

[Pinson 93] : Pinson S., Maurice-Demourioux M., Laasri B., Levallet C. « Le Raisonnement à Partir de Cas: Panorama et Modélisation Dynamique». *Séminaire Raisonnement à Partir de Cas*, LAFORIA, rapport 93/42, 1 oct. 1993.

[Quinlan 86] : Quinlan R. « Induction of Decision trees », *Machine Learning*, 1986, 1, 81-106.

[Rougegrez 93] : Rougegrez S. « Le Raisonnement à Partir de cas ». *Séminaire Raisonnement à Partir de Cas*, LAFORIA report n°93/42, octobre 1993.

[Slade 91] : Slade S. « Case-Based Reasoning : a Research Paradigm ». *Artificial Intelligence Magazine*, 1991, 12, 42-55.

[Smail 93] : Smail M., Crehange M. « Adaptation par Cas des Stratégies de Recherche d'Information». *Séminaire Raisonnement à Partir de Cas*, LAFORIA, rapport 93/42, 1 oct. 1993.

[Thireau 86] : Thireau P. « Méthodologie d'Analyse des Effets des Erreurs du Logiciel (A.E.E.L.) appliquée à l'étude d'un logiciel de haute sécurité ». *5° colloque international de fiabilité et de maintenabilité*, Biarritz, France, 1986.

2/ Projet « SPECIALS »

Méthode de spécification et d'aide à l'évaluation des logiciels de sécurité
basée sur l'utilisation des graphes conceptuels

1. CONTEXTE GENERAL DE L'ETUDE ET COLLABORATION SCIENTIFIQUE

L'objectif de la recherche consiste à étudier l'apport du génie cognitif au génie logiciel dans le cadre de l'évaluation des logiciels de sécurité. Il s'agit plus précisément d'étudier la faisabilité d'une nouvelle méthode d'élaboration et d'évaluation des spécifications des logiciels de sécurité basée sur l'emploi des graphes conceptuels. L'intérêt pressenti de cette nouvelle démarche de développement de logiciels critiques réside essentiellement dans la clarté des spécifications, la maintenabilité du logiciel et la réutilisation des spécifications. Cette étude, qui s'inscrit dans le cadre du projet « SPECIALS » est réalisée en collaboration avec le laboratoire d'informatique de l'Université de Paris VI, fait l'objet, en partie, de la thèse de Myriam DARRICAU et a débuté en décembre 1995. L'encadrement scientifique de cette thèse est assuré conjointement par le Professeur Jean-Gabriel Ganascia et moi -même.

Cette section présente une approche méthodologique permettant de faciliter la tâche d'interprétation des besoins de l'utilisateur et par conséquent de mieux cerner les activités d'élaboration et d'évaluation des spécifications de logiciels. Parmi les méthodes et outils existant dans le domaine du génie logiciel, il n'existe pas, à ce jour et à notre connaissance, d'outils opérationnels permettant d'appréhender la première étape de développement d'un logiciel : la traduction des besoins d'un utilisateur en spécifications exploitables. Cette étape d'interprétation fastidieuse et complexe à réaliser, est cependant primordiale dans le cycle de vie d'un logiciel car elle conditionne les phases avales de réalisation et d'évaluation. Pour apporter un élément de réponse à ce problème, notre approche repose sur la réutilisation des spécifications existantes et validées pour aider à rédiger et à évaluer de nouvelles spécifications. Il s'agit plus précisément de recueillir, modéliser, capitaliser et réutiliser les spécifications de logiciel des systèmes déjà certifiés en vue de construire un modèle « générique » de spécification.

Ce modèle, basé en grande partie sur l'emploi des graphes conceptuels de Sowa [Sowa 84] pour représenter et organiser les connaissances, servira, d'une part, de base de travail lors de l'élaboration de nouvelles spécifications et, d'autre part, de « grille d'évaluation » lors de l'analyse et de l'examen de spécification existantes. L'application de cette nouvelle approche à un problème représentatif du domaine des transports guidés : le système de pilotage automatique, a permis de montrer sa faisabilité et son bien fondé. Les principaux résultats de cette étude sont présentés dans les paragraphes suivants.

2. DEVELOPPEMENT ET EVALUATION DES LOGICIELS

Un logiciel est une création intellectuelle comprenant "des programmes, procédures, règles et tout document associé, liés à la mise en œuvre du système programmé" [IEC 91]. Plus précisément, un logiciel est matérialisé par des spécifications, un code (ou programme) et une documentation [Huet et Paulin-Mohring 93]. Un logiciel ne peut être dangereux que dans la mesure où il équipe un système dont les défaillances peuvent avoir des conséquences catastrophiques [Place et Kang 93], [Barroca et Mac Dermid 92]. De tels logiciels sont de plus en plus fréquents, que ce soit pour guider l'atterrissage des avions ou commander le freinage d'urgence dans les trains et sont fréquemment désignés par les termes «logiciels de sécurité» ou «logiciels critiques». Selon la norme française NF F 71-011 [NF 90a], un logiciel de sécurité est défini comme «un logiciel dont l'exécution participe à des fonctions impliquées dans la sécurité d'un système». On distingue dans la littérature les logiciels fiables et les logiciels sûrs [Laprie 92], [Place et Kang 93] et [Barroca et Mac Dermid 92].

Dans le cadre des logiciel sûrs, les défaillances ne doivent pas provoquer des conséquences catastrophiques. Cependant, un logiciel non fiable peut être sûr si les défaillances qu'il engendre sur le système et l'environnement ne sont pas dangereuses. La technique de sécurité intrinsèque est un exemple type où toutes les défaillances doivent conduire le système à un état restrictif vis-à-vis de la sécurité. Le comportement du système en cas de panne ou de perturbation ne doit pas passer dans une situation moins permissive que la situation dans laquelle il se trouvait avant la défaillance, la situation la moins permissive étant généralement l'arrêt complet [David 88]. A l'opposé, un logiciel peut être fiable et non conçu en sécurité. Ce dernier peut assurer sa mission (disponibilité) mais risque d'engendrer un comportement contraire à la sécurité. Par exemple, dans le domaine des transports guidés, un logiciel dédié à la gestion des itinéraires d'un système peut continuer à assurer correctement son service en dépit de la défaillance d'un de ses composants mais proposer un itinéraire incompatible conduisant à une collision.

Afin d'identifier les caractéristiques générales requises pour une spécification de logiciel, nous avons examiné plusieurs normes et projets de normes dans le domaine ferroviaire et nucléaire : NF F 71-011 [NF 90a], NF F 71-012 [NF 90b], NF F 71-004 [NF 91], pr EN 50128 [CENE 94], CEI 880 [CEI 86] et CEI 65A [CEI 91].

L'étude de ces normes nous a permis de dégager les trois caractéristiques suivantes [Darricau et al. 97a, 97b] :

- Une spécification doit décrire ce qu'il faut faire : le « quoi » et non pas la manière de le faire : le « comment » ;
- Une spécification doit respecter des critères de qualité et de précision tels que l'exhaustivité, la cohérence et la non ambiguïté.
- Une spécification se matérialise par deux documents principaux, appelés respectivement «spécifications du système» qui précisent les exigences globales demandées au système et «spécifications fonctionnelles du logiciel» dont l'objet est de présenter les fonctions logicielles du système.

Evaluer un logiciel critique revient à démontrer que son comportement ne provoque pas de situations contraires à la sécurité. Généralement, pour des logiciels complexes, les méthodes conventionnelles d'évaluation ne permettent pas cette démonstration [David 88] et [Nicola 93). Elles visent néanmoins à augmenter la confiance que l'on peut avoir dans le comportement du logiciel.
Dans la littérature, le terme « évaluation » fait appel aux notions de validation et d'évaluation. Selon les normes, le terme **validation** est défini comme : « le processus d'examen d'un produit en vue de déterminer la conformité aux besoins de l'utilisateur » ISO 8402 [ISO 94] ou « le processus de contrôle visant à vérifier que les fonctions requises sont effectivement obtenues » NF F 71-011 [NF 90a] ou encore « la procédure de démonstration, par essais et analyse, du fait que le système considéré satisfait en tous points à ses spécifications » pr EN 50126 [CENE 93a] et pr EN 50129 [CENE 93b]. De même, le terme **vérification** s'analyse comme : « le processus d'examen du résultat d'une activité en vue de déterminer la conformité aux exigences fixées pour ladite activité » [ISO 94] ou « la procédure déterminante pour chaque phase du cycle de vie que les résultats satisfont à tous égards aux objectifs et exigences imposés pour cette phase, par exemple traçabilité à long terme depuis les spécifications de besoin et pour chaque phase de la documentation d'étude, jusqu'à la conception définitive ; la vérification peut comporter des essais » [CENE 93a] ou encore « le processus consistant à démontrer, par essais et analyse, lors de chaque phase du cycle de vie, si le produit élaboré répond aux spécifications issues de la phase précédente » [CENE 93b].
Face à cette variété de définitions, il nous est difficile de donner une idée claire et précise des termes «validation» et «vérification». Par conséquent, on préfère employer le terme « évaluation » ou « appréciation » que nous définissons comme suit : « évaluer un logiciel consiste à s'assurer que le comportement du logiciel est conforme aux besoins de l'utilisateur » (figure 1). Pour contribuer à mieux définir cette activité d'évaluation, nous proposons dans la figure 2 une décomposition des différents niveaux d'évaluation qui repose sur les principaux états par lesquels passe tout logiciel durant son cycle de vie [Darricau et al. 96, 97b] : interprétation des besoins, développement des spécifications et exécution du code final. L'étape d'interprétation permet de traduire le besoin de l'utilisateur en spécifications utilisables par les concepteurs. L'étape de développement permet de produire un programme informatique, c'est-à-dire un code, conforme à ce qui est exigé par les spécifications. Enfin, l'étape d'exécution permet de mettre en œuvre le code et d'observer le comportement du logiciel.

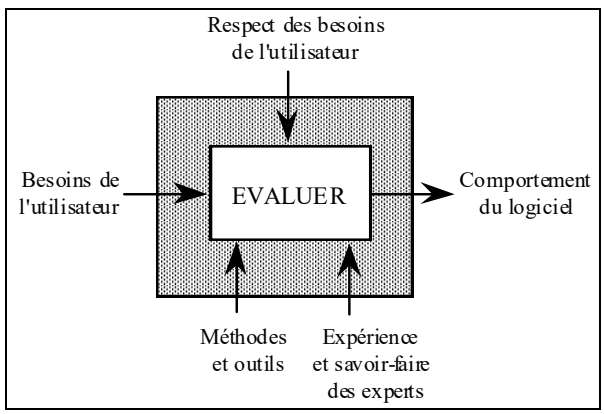

Figure 1 : l'activité d'évaluation d'un logiciel

Une étude bibliographique sur les principaux méthodes, techniques et outils contribuant à la tâche d'évaluation des logiciels a permis de distinguer neuf catégories de méthodes [Darricau et al. 96] :

1. Langages et méthodes de spécifications (ex. : SADT, Grafcet, Réseau de Pétri);
2. Méthodes de développement (ex. : VDM, B);
3. Méthodes d'analyses statiques (ex. : revue détaillée de programme, AEEL, Métriques);
4. Preuves de programmes (ex. : Calcul des constructions);
5. Synthèse de programmes (dériver des programmes automatiquement depuis les spécifications);
6. Environnements de programmation et ateliers logiciels (ex. : COQ, AGE);
7. Gestionnaires de versions;
8. L'aide à la programmation (ex. : Pfort, Pbasic);
9. Les tests dynamiques (ex. : exploration de code, mutation de code).

Les sept premières catégories sont employées principalement lors du passage des spécifications au code final (niveau 2), tandis que les deux dernières catégories permettent d'assister le passage du code final à l'état traduisant le comportement du logiciel (niveau 3). Le niveaux 1 d'évaluation qui s'attache à contrôler que les spécifications du logiciel sont conformes aux besoins de l'utilisateur, constitue une tâche très pénible à réaliser car les besoins de l'utilisateur sont généralement exprimés de manière informelle, incomplète, imprécise ou encore incohérente. Cette tâche n'est soutenue par aucune méthode car elle repose essentiellement sur l'expérience et le savoir-faire des experts du domaine. Les principes et les objectifs de ces méthodes sont décrites en grande partie dans [Musa et al. 87], [Hennebert 87], [Gaudel 89,93], [Nicola 93], [Wirsing 93], [Huet 94], [Vignes 95] et [André et Royer 96]. Les travaux de Darricau, Hadj-Mabrouk et Ganascia [Darricau et al. 96] retracent de façon assez complète l'évolution de la recherche dans le domaine de l'évaluation des logiciels.

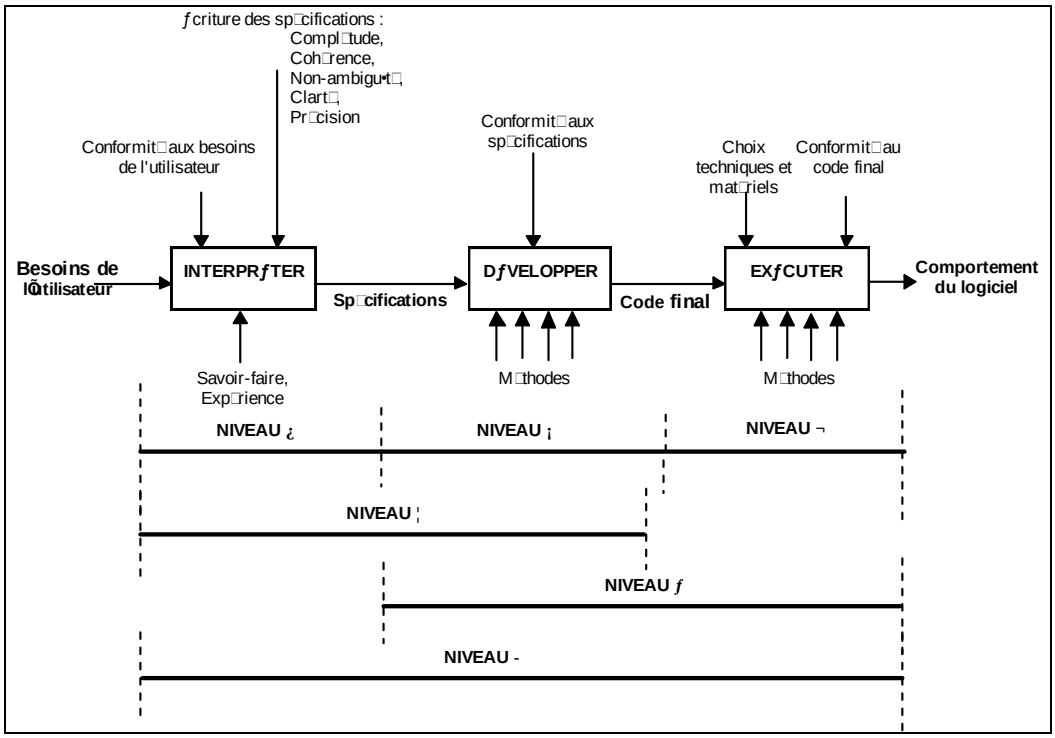

Figure 2 : décomposition de l'activité d'évaluation des logiciels [Darricau et al. 96, 97b]

3. MOTIVATIONS ET OBJECTIF DE L'ETUDE

La tâche d'évaluation des logiciels devient de plus en plus cruciale lorsque ces derniers assurent des fonctions critiques sur le plan de la sécurité. Les catastrophes survenues au cours des dernières décennies dans la plupart des secteurs industriels montrent l'inexistence d'activités à risque nul vis-à-vis de l'homme, de l'environnement et des biens ou équipements. C'est notamment le cas dans le domaine des transports ferroviaires où les systèmes sont de plus en plus complexes et automatisés (Val, Maggaly, Sacem) et chargés d'exécuter des tâches de sécurité comme le pilotage et la localisation des trains, la gestion des itinéraires, l'élaboration des consignes de vitesse, le contrôle du sens de marche ou encore, la gestion et le contrôle du freinage d'urgence. La conception et l'exploitation de ces systèmes exigent en particulier la mise en œuvre d'outils et méthodes d'évaluation de plus en plus performants et opérationnels. En effet, la conception des systèmes et logiciels dont on exige des niveaux de sécurité acceptables ne peut être réalisée sans méthodes de contrôles et de validation. Ces contrôles constituent pour l'INRETS-ESTAS un domaine d'activité primordiale, tant pour la recherche que pour l'expertise.

Il existe aujourd'hui de nombreuses méthodes, outils et langages de développement et d'évaluation des logiciels Malgré l'intérêt indéniable de ces méthodes, le problème d'évaluation des logiciels de sécurité demeure entier. En effet, il est presque impossible d'accorder une confiance totale au comportement des logiciels et par conséquent de démontrer qu'ils sont sûrs. De plus aucune méthode ne permet, à elle seule, de développer et d'évaluer un logiciel dans sa totalité. Il est donc nécessaire de combiner plusieurs méthodes pour réaliser ces deux activités. Pour compléter et renforcer ces méthodes usuelles et par conséquent augmenter la confiance que l'on peut avoir dans un logiciel critique, nous avons convenu de concevoir une nouvelle approche de spécification et de validation de logiciels fondée sur l'emploi des techniques d'intelligence artificielle et plus particulièrement sur l'utilisation des graphes conceptuels de Sowa [Sowa 84] en vue de modéliser les connaissances de spécification.

Notre recherche s'est focalisée sur la première phase de développement d'un logiciel : interprétation des besoins de l'utilisateur en une spécification exploitable. Cette phase qui constitue actuellement le goulot d'étranglement du développement d'un logiciel, consiste à convertir des besoins par nature informels, imprécis et incomplets, en une spécification cohérente, précise et exploitable. Cette activité d'interprétation est rude mais décisive car elle conditionne l'ensemble des activités de développement du logiciel. Or, l'étude des différentes méthodes de développement et d'évaluation des logiciels montre que cette phase n'est soutenue par aucune méthode ni outils et qu'elle repose principalement sur le savoir-faire et l'expérience des experts concepteurs. C'est ce point fondamental qui a motivé le présent travail qui fait l'objet du système « SPECIAL » dont l'architecture fonctionnelle est détaillée ci-après.

4. ARCHITECTURE FONCTIONNELLE DU SYSTEME « SPECIALS »

L'architecture fonctionnelle de la maquette du système « SPECIALS » s'articule autour des cinq principaux modules suivants dont le contenu est détaillé ci-après (figure 3) :

1. Module pour la construction d'un modèle « générique » de spécification ;
2. Module d'aide à l'élaboration de nouvelles spécifications ;
3. Module d'aide à l'évaluation des spécifications existantes ;
4. Module d'apprentissage automatique des spécifications.

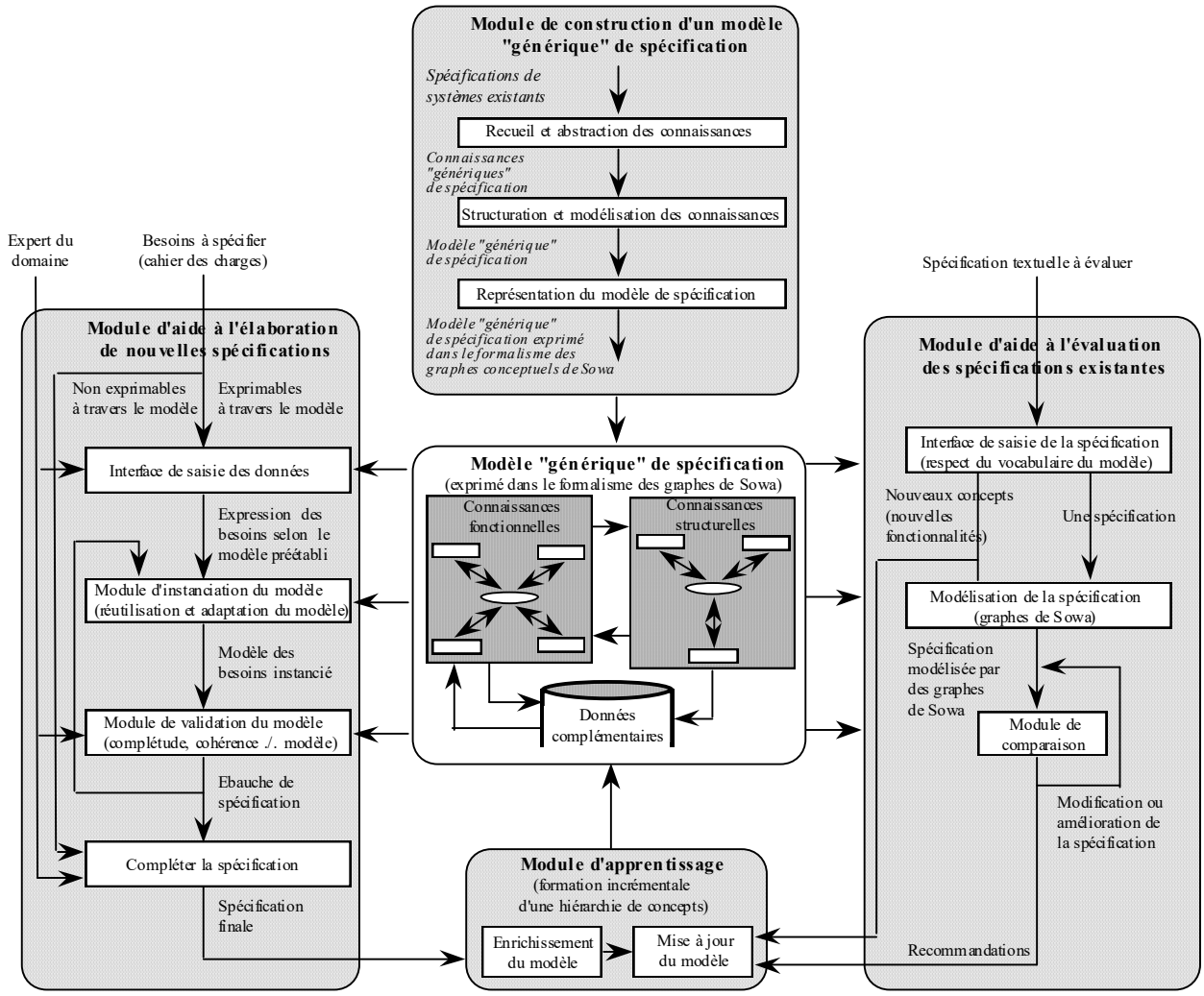

Figure 3 : structure fonctionnelle du système « SPECIALS » proposée

4.1. CONSTRUCTION D'UN MODELE « GENERIQUE » DE SPECIFICATION

La phase de construction du modèle « générique » de spécification suppose le passage par les trois étapes suivantes : recueil et abstraction des connaissances, structuration et modélisation des connaissances et représentation des connaissances.

4.1.1. Recueil et abstraction des connaissances

Afin de montrer la faisabilité de l'approche proposée et limiter l'étendue du problème, nous avons focalisé notre étude sur un sous-problème représentatif du domaine de la sécurité des transports guidés : le système de pilotage automatique. Ainsi, l'étape de recueil de connaissances a porté sur l'examen de deux dossiers de spécifications de pilote automatique différents. L'un des systèmes est sans conducteur, l'autre avec. Deux types de dossiers de spécifications ont été étudiés (Darricau et al. 97b) : les documents de spécifications du système et les documents de spécifications fonctionnelles du pilotage automatique. Afin d'aboutir à un modèle « générique » et de s'affranchir des particularismes propres aux logiciels étudiés, une attention particulière a été portée sur les données semblables. Cette tâche de confrontation et l'abstraction des connaissances montre qu'il existe des analogies entre les différentes spécifications étudiées. En final, la phase de recueil de connaissance a permis de recenser un ensemble de données permettant de construire une première ébauche de modèle de spécifications d'un pilotage automatique.

4.1.2. Structuration et modélisation des connaissances

Les connaissances acquises ont été par la suite organisées en trois types de connaissances [Darricau et al 97c, 98] : connaissances structurelles, connaissances fonctionnelles, et données complémentaires. Quatre types de liens ont été identifiés, afin d'expliciter les relations existantes entre ces connaissances : liens structurels, liens fonctionnels, liens séquentiels et contraintes. La figure 4 illustre l'ensemble de ces connaissances ainsi que leurs relations.

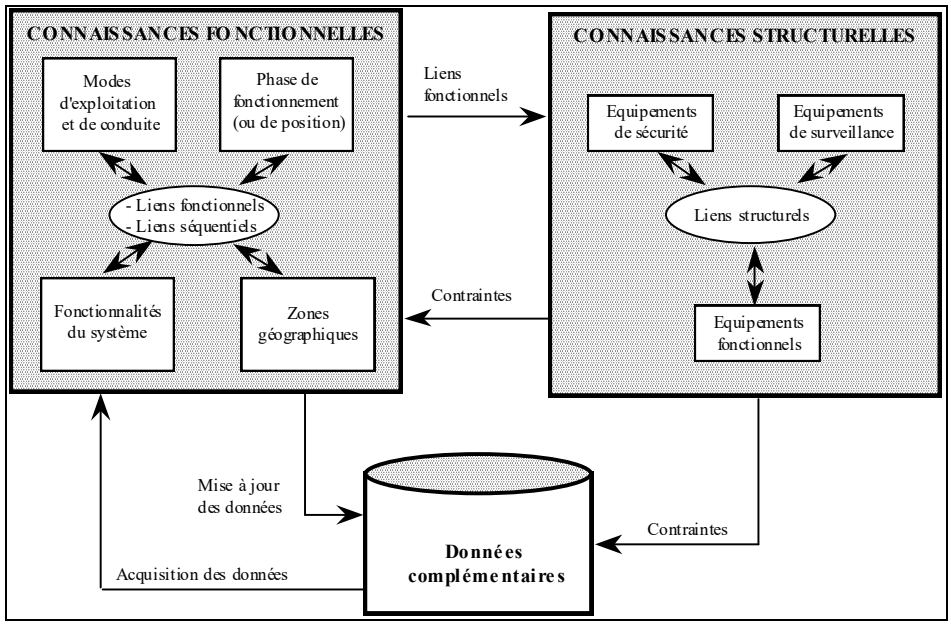

Figure 4 : principaux types de connaissances impliquées dans une spécification
[Darricau et al 97c]

Relations entre les connaissances

Nous avons identifié quatre types de relations qui permettent aux connaissances de coopérer entre elles [Darricau et al. 98] :

1- Liens structurels qui assurent la décomposition hiérarchique des connaissances. Par exemple, un train est composé de voitures.
2- Liens de séquencement qui structurent les connaissances dans le temps et les ordonnent séquentiellement. Par exemple, le train doit être arrêté en station avant d'ouvrir les portes.
3- Liens fonctionnels qui traduisent la coopération entre plusieurs connaissances en vue d'exécuter une tâche donnée. Par exemple, le calcul de la vitesse nulle est nécessaire pour déterminer l'arrêt du train en station.
4- Contraintes qui présentent des conditions imposées à certaines connaissances par d'autres connaissances. Par exemple, les quais doivent être plus long que les trains.

L'ensemble de ces relations permettent aux trois types de connaissances présentés ci-après d'interagir entre elles.

Types de connaissances

Le modèle de spécification proposé repose sur l'emploi de trois types de connaissances : connaissances structurelles, connaissances fonctionnelles et données complémentaires.

Connaissances structurelles. Ce type de connaissances définit les éléments de base d'une structure physique caractérisée par la nature des constituants et par leur agencement les uns par rapport aux autres [Marrakchi 86]. Généralement le modèle de représentation le plus adapté, pour une telle description, est un modèle basé sur une structure hiérarchique. Chaque système est décomposé en sous-systèmes qui, à leur tour, sont décomposés en modules ou composants et de proche en proche, on définit l'ensemble de la structure avec des éléments terminaux. Le résultat d'une telle description est donc un graphe orienté. Dans le domaine des transports ferroviaires, les connaissances structurelles manifestent des infrastructures physiques du système de transport, de son environnement et de son matériel. Afin de mieux structurer ces connaissances, nous avons distingué trois classes d'équipements : les équipements de sécurité (ex : système d'anticollision), les équipements de surveillance (ex : système de traitement des alertes radio) et les équipements fonctionnels (ex : système d'asservissement des trains).

- Connaissances fonctionnelles. En complément des connaissances structurelles, notre modèle prend en compte les connaissances fonctionnelles. Ces connaissances permettent de traduire la façon dont certains constituants du système contribuent à la mise en œuvre des différentes fonctions globales du système. Dans le cadre de notre application, nous avons distingué plusieurs catégories de connaissances fonctionnelles [Hadj-Mabrouk 95a] :

    1. Fonctionnalités du système : (ex : localisation des trains, élaboration des consignes de vitesse, gestion des alarmes, gestion des itinéraires, initialisation).
    2. Modes d'exploitation (ex : nominal, dégradé).
    3. Modes de conduite (ex : conduite automatique intégrale, conduite en pilotage automatique avec agent de conduite, conduite manuelle contrôlée, conduite manuelle libre, conduite en marche à vue à vitesse restreinte, conduite manuelle avec signalisation auxiliaire).
    4. Phases de fonctionnement ou de position (ex : approche station, arrêt station, dégagement de quai, arrêt ligne, inter-station, départ ligne, conduite hors ligne).
    5. Zones géographiques (ex : station, voie, garage, terminus, limite de tronçon, zone d'injection de rame, zone d'aiguillage).

- Données complémentaires. Les deux types de connaissances que nous avons définis permettent d'apporter les éléments de connaissances nécessaires à la modélisation des composantes structurelles et fonctionnelles du système ou équipement. Ces connaissances de base doivent être complétées par d'autres connaissances qualifiées de « données complémentaires ». Ces connaissances sont utilisées essentiellement pour compléter les connaissances fonctionnelles (par exemple, le freinage d'urgence précise la fonctionnalité «s'arrêter») ou les connaissances structurelles (par exemple, la vitesse de consigne prend en compte la pente de la voie). En outre, elles permettent d'exprimer des contraintes (par exemple, la vitesse de consigne qui contraint la vitesse des véhicules). Ces données complémentaires sont régulièrement calculées et rafraîchies lors du fonctionnement du système.

4.1.3. Représentation des connaissances

Compte tenu de la nature des connaissances extraites ainsi que des objectifs fixés, nous avons retenu les graphes conceptuels de J. Sowa [Sowa 84] pour exprimer les connaissances impliquées dans le modèle de spécification. Un graphe conceptuel est formé de plusieurs triplets (concept + relation + concept). Les concepts sont représentés par des rectangles qui interagissent ente eux grâce à des relations orientées et schématisées par des ellipses. La connaissance exprimée par des graphes conceptuels comporte deux niveaux [Guinaldo 96] : un niveau terminologique constitué essentiellement d'un ensemble ordonné de concepts (treillis des concepts) et d'un ensemble ordonné de relations entre concepts (treillis des relations) et un niveau assertionnel qui est composé de graphes construits à partir de la terminologie. Les concepts sont généralement hiérarchisés entre eux au moyen d'un treillis de spécialisation dont l'élément le plus haut est le concept « univers » et l'élément le plus bas est le concept « absurde ». Une hiérarchie exprime des liens de spécialisation entre les concepts. Par exemple le concept A « est-un » ou « est-une-sorte-de » concept B, on dit alors que B est le père ou l'ascendant de A (ou B est plus généralisé que A). De même A est le fils (le descendant) de B ou le plus spécialisé que B. Le principal apport des graphes conceptuels de Sowa réside dans les différents traitements à réaliser : fusionner deux graphes, éclater des graphes en un ensemble de triplets (concepts + relation + concept), simplifier un graphe en supprimant des concepts ou des relations redondantes, etc.

La figure 5 présente un exemple de graphe conceptuel incluant à la fois des connaissances structurelles, des connaissances fonctionnelles et des données complémentaires, ainsi que les relations : liens structurels, liens fonctionnels et contraintes [Darricau et al 97b].

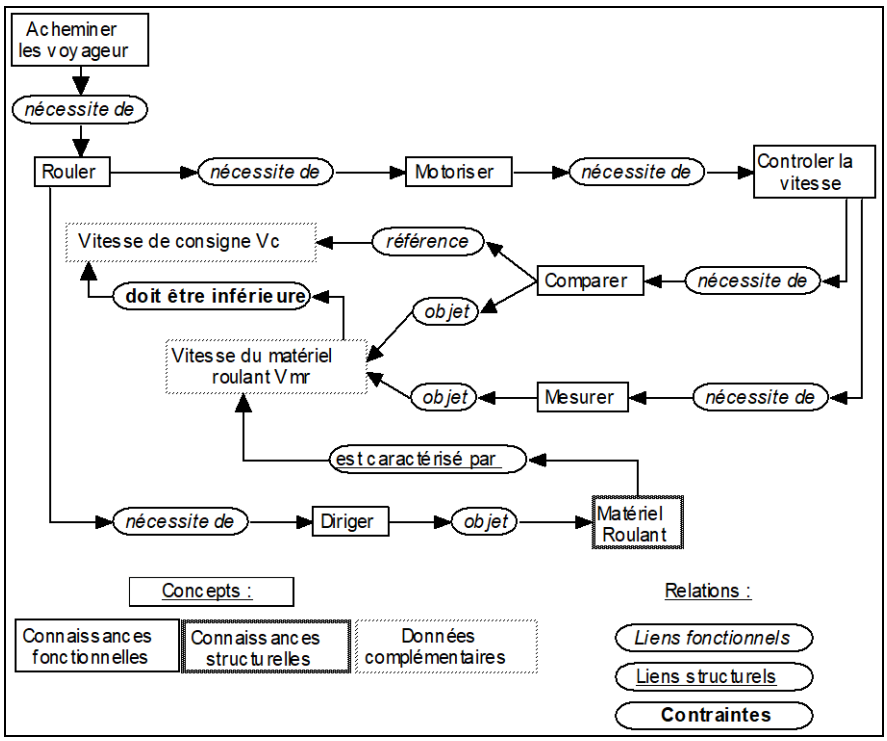

Figure 5 : Extrait de graphe conceptuels représentant des connaissances impliquées dans les spécifications d'un pilote automatique [Darricau et al. 97b].

Après avoir recueilli, structuré, et représenté les connaissances nécessaires à l'élaboration d'un modèle « générique » de spécifications, les paragraphes suivants présentent l'approche envisagée pour aider à l'élaboration et à l'évaluation des spécifications à partir du modèle établi.

4.2. MODULE D'AIDE A L'ELABORATION DE NOUVELLES SPECIFICATIONS

Le modèle « générique » de spécification précédemment construit est exploité comme base de travail pour aider à établir de nouvelles spécifications. Ce modèle qui contient les principaux éléments de connaissances considérées comme indispensables à l'élaboration d'une nouvelle spécification peut être enrichi et adapté à la nouvelle application. Le développement de nouvelles spécifications, à partir du modèle, suppose le passage par les principales étapes suivantes :

- Etape de saisie des données exprimables selon le modèle. Lors de cette étape des requêtes sont proposées à l'utilisateur en vue de l'aider à exprimer ses besoins. Ces requêtes sont effectuées en ayant recours au modèle préétabli (vocabulaire, grammaire et graphes conceptuels).
- Etape d'instanciation du modèle qui permet de réutiliser et/ou d'adapter les connaissances impliquées dans le modèle en vue de construire le nouveau modèle de spécification.
- Etape de validation du modèle précédemment instancié en termes de complétude et de cohérence. Cette validation est réalisée d'une part en s'appuyant sur le modèle « générique » et d'autre part en faisant appel au savoir-faire et l'expérience de l'expert du domaine. Cette étape débouche en final sur une première ébauche de spécification.
- Etape de complétition de l'ébauche de spécification. Lors de cette étape, les besoins non exprimables à travers le modèle « générique », seront exploités par l'expert du domaine pour construire l'intégralité de la spécification. Cette dernière étape d'élaboration engendre éventuellement un enrichissement et par conséquent la mise à jour du modèle « générique ». Cette phase est du ressort du module d'apprentissage automatique de formation incrémentale d'une hiérarchie de concepts présenté plus loin.

4.3. MODULE D'AIDE A L'EVALUATION DES SPECIFICATIONS

Lors de cette phase, le modèle « générique » est considéré comme une « grille de comparaison » pour aider à évaluer des spécifications existantes. Les spécifications textuelles à évaluer sont d'abord modélisées à l'aide des graphes conceptuels de Sowa et ensuite comparées au modèle « générique ». Cette confrontation permet éventuellement de détecter des incomplétudes (en comparant le graphe au modèle), des incohérences (en contrôlant le graphe) ou des imprécisions. L'ensemble des données incomplètes ou incohérentes permet de stimuler l'utilisateur ou l'expert à formuler les recommandations nécessaires pour donner un avis sur la consistance et le fondement des spécifications évaluées. La tâche d'évaluation des spécifications peut également produire, lors de l'étape de saisie, de nouveaux concepts ou nouvelles fonctionnalités du système non considérées par le modèle « générique » et qui nécessitent la mise à jour du modèle par l'intermédiaire du module d'apprentissage présenté ci-après.

4.4. MODULE D'APPRENTISSAGE AUTOMATIQUE DES SPECIFICATIONS

L'objectif principal du module d'apprentissage est d'accroître et de réparer éventuellement le modèle « générique ». Cette opération nécessite une phase d'apprentissage incrémentale en vue d'enrichir ou de mettre à jour une partie du graphe conceptuel voire même sa totalité. Cette caractéristique d'apprentissage incrémental est nécessaire dans notre application car elle permet l'utilisation des connaissances impliquées dans le modèle qui n'est pas au début suffisamment représentatif de l'ensemble du problème considéré. En effet ce type d'apprentissage est fort appréciable lorsque les données couvrant le domaine d'application sont en nombre considérable et qu'elles ne peuvent être recensées de façon exhaustive ou lorsqu'elles sont longues à acquérir [Hadj-Mabrouk 92, 95b]. L'évolution de la connaissance au cours d'un processus d'apprentissage engendre deux types d'incrémentalité : monotone et non monotone [Sebag et Schoenauer 90]. Dans l'incrémentalité monotone (croissance ou décroissance continue des connaissances) l'apprentissage ne fait que produire de nouvelles connaissances qui complètent les connaissances initiales sans remettre en cause les connaissances déjà apprises. Il s'en suit, comme le souligne Ganascia [Ganascia et al. 90], que la capacité à reconnaître ses propres erreurs semble absente. L'incrémentalité monotone n'est pas adaptée au traitement des données bruitées ou évolutives.

L'algorithme ADECLU [Decaestecker 89a, 89b] qui construit incrémentalement des hiérarchies de concepts permet d'illustrer le type d'apprentissage non monotone. Il s'attache à intégrer un nouvel objet (exemple) dans une hiérarchie existante, tout en restructurant cette dernière. L'arbre est construit en utilisant quatre opérateurs : création d'un nœud, suppression d'un nœud, fusionnement de deux nœuds et éclatement en deux d'un nœud. En présence d'un nouvel exemple à classer, le processus d'apprentissage peut défaire ce qu'il a appris dans l'étape antérieure : détruire un nœud déjà créé, éclater un nœud précédemment fusionné. Cette réversibilité du processus permet une évolution non monotone des connaissances.

Contrairement à l'approche monotone, l'apprentissage non monotone est mieux adapté aux données bruitées, en revanche le processus n'offre plus de garanties de convergence et devient théoriquement capable d'osciller ou de boucler [Sebag et Schoenauer 90]. Dans le cadre de notre application, l'approche envisagée pour adapter et faire évoluer le modèle « générique » de spécification repose sur l'emploi d'une technique d'apprentissage non monotone et plus précisément l'apprentissage par classification conceptuelle en vue de former incrémentalement une hiérarchie de concepts. Une étude des algorithmes COBWEB [Fisher 87], UNIMEM [Lebowitz 87], CLASSIT [Gennari et al. 89] et ADECLU [Decaestecker 89a, 89b] est en cours de réalisation afin de choisir l'algorithme le plus adapté à notre application.

5. CONCLUSION

Une étude approfondie des méthodes, techniques et outils de développement et d'évaluation des logiciels a révélé l'absence de méthodes et outils permettant de réaliser la phase d'interprétation des besoins de l'utilisateur en spécifications de logiciel. En effet, cette phase, primordiale dans le développement d'un logiciel, n'est soutenue par aucune méthode et elle repose en grande partie sur l'expérience et le savoir faire des experts du domaine. Pour apporter un élément de réponse à ce problème, nous avons proposé une approche méthodologique qui repose sur l'emploi des techniques d'intelligence artificielle et notamment sur l'utilisation des graphes conceptuels de Sowa, l'apprentissage automatique et l'acquisition des connaissances. Cette approche a débouché sur la conception et la mise en œuvre d'un modèle « générique » de représentation des connaissances de spécification. Ce modèle qui est représenté par des graphes conceptuels de Sowa, s'articule autour de trois types de connaissances : structurelles, fonctionnelles, complémentaires. L'intérêt de ce modèle est double : il peut être utilisé, d'une part, comme base de travail pour élaborer de nouvelles spécifications, et d'autre part, comme une « référence » pour évaluer des spécifications existantes. En ce sens, il favorise la réutilisation de spécifications déjà développées et validées.

Afin de montrer le bien fondé de l'approche proposée, une maquette de faisabilité est en cours de développement. Cette maquette utilise la plate-forme logicielle CoGITo, qui a été aimablement mise à notre disposition par l'équipe «Graphes conceptuels» du laboratoire d'informatique, de robotique et de micro-électronique de Montpellier

(LIRMM). Cette étude de faisabilité a focalisé dans un premier temps sur un problème représentatif du domaine de la sécurité des transports guidés : le système de pilotage automatique.

Ces travaux se poursuivent aujourd'hui et portent notamment sur :

- la validation et l'enrichissement du modèle de spécification élaboré,
- la poursuite de l'utilisation de la plate-forme logicielle CoGITo afin de montrer son apport et ses limites pour représenter et aider à l'évaluation en termes de cohérence des spécifications,
- le développement du module d'apprentissage.

6. BIBLIOGRAPHIE

[André et Royer 96] : André P., Royer J.C. « Un point de vue sur les méthodes formelles à objet ». L'objet, Vol. 2, n°4, février 1996.

[Barroca et Mac Dermid 92] : Barroca L.M., Mac Dermid J.A. « Formal methods : use and relevance for the development of safety-critical systems ». *The Computer Journal*, Vol. 35, n° 6, 1992.

[CEI 86] : Commission Électrotechnique Internationale. Norme 880 - Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires, 1986.

[CEI 91] : Commission Électrotechnique Internationale. Norme 65A 122 - Software for computers in the application of industrial safety-related systems, 1991.

[CENE 93a] : Projet de Norme Européenne pr EN 50126 - Spécification et preuve de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FMDS) pour les applications ferroviaires, CENELEC, 1993.

[CENE 93b] :: Projet de Norme Européenne pr EN 50129 - Applications aux chemin de fer : systèmes électroniques de sécurité de commande et de contrôle des chemins de fer, CENELEC, 1993.

[CENE 94] : Comité Européen de Normalisation Électrotechnique. Projet de norme Pr EN 50128 - Applications aux chemins de fer : logiciels pour systèmes de commande et de protection ferroviaire, 1994.

[Darricau et al. 96] : Darricau M., Hadj-Mabrouk H., Ganascia J-G. « Méthodes contribuant à l'évaluation des logiciels de sécurité. Étude bibliographique ». *Convention INRETS/LAFORIA*, rapport n° ESTAS/A-96-62, diffusion restreinte, 44 p, Arcueil, novembre 1996.

[Darricau et al. 97a] : Darricau M., Hadj-Mabrouk H., Ganascia J-G. « Acquisition and structuration of knowledge of safety critical software specifications ». *8th IFAC Symposium on Transportation Systems*, Chania, Greece, Volume 3, pp 1227-1231, 16-18 june 1997.

[Darricau et al. 97b] : Darricau M., Hadj-Mabrouk H., Ganascia J-G. « Acquisition et représentation des connaissances impliquées dans les spécifications des logiciels de sécurité. Application au système de pilotage automatique ». *Convention INRETS/LAFORIA*, rapport n° ESTAS/A-97-29, diffusion restreinte, 40 p, Arcueil, 10 juin 1997.

[Darricau et al. 97c] : Darricau M., Hadj-Mabrouk H., Ganascia J-G. « Une approche pour la réutilisation des spécifications de logiciels. Application au domaine de la sécurité des systèmes de transport guidés ». *Revue Génie Logiciel*, n° 45, Editions EC2 & Développement, .Paris, septembre 1997, pp 2-8

[Darricau et al. 98] : Darricau M., Hadj-Mabrouk H., Ganascia J-G. « Amodel for reusing specifications of safety-critical software in the field of automated people movers ». *Congrès IEEE, Computational engineering in systems applications.* Nabeul-Hammamet, Tunisia, April 1-4, 1998. (A paraître).

[David 88] : David Y. « L'évolution des méthodes de certification de la sécurité face au développement des applications de la microinformatique dans les transports terrestres ». *Annales des Ponts et Chaussées*, n° 45, 1er trimestre 1988.

[Decaestecker 89] : Decaestecker C. « Formation incrémentale de concepts par un critère d'adéquation ». *4èmes Journées Françaises de l'apprentissage*. Saint-Malo 22-24 Mai 1989, p 63-77.

[Decaestecker 89] : Decaestecker C. « Incremental Concept Formation with attribute selection ». *EWSL : European Working Session on Learning,* 1989, p 49-58.

[Fisher 87] : Fisher D.H. « Knowledge Acquisition via Incremental Conceptual Clustering ». *Machine Learning*, vol 2, 1987, p 139-172.

[Ganascia 90] : Ganascia J.G. « L'âme Machine - les enjeux de l'Intelligence Artificielle ». *Editions du SEUIL*, Janvier 1990, 280p.

[Ganascia et al. 90] : Ganascia J.G., Puget J.F., Helft N. « Comportement des systèmes d'apprentissage : vers une modélisation générale ». *Actes des 3èmes Journées Nationales PRC-GDR Intelligence Artificielle*, 5-7 Mars 1990, Edition HERMES, Chapitre 5, p 237-269.

[Gaudel 89] : Gaudel M.-C. « Le génie logiciel ». Rapport de recherche n° 469 du laboratoire de Recherche en Informatique, mars 1989.

[Gaudel 93] : Gaudel M.-C. « Le génie logiciel ». Dossier scientifique, La recherche en informatique, Le courrier du CNRS n°80, février 1993.

[Gennari et al. 89] : Gennari J.H., Langley P., Fisher D.H. « Models of Incremental Concept Formation ».*Artificial Intelligence*, vol 40, 1989, p 11-61.

[Guinaldo 96] : Guinaldo O. « Étude d'un gestionnaire d'enembles de graphes conceptuels ». *Tèse de doctorat*, Université de Montpellier II, décembre 1996.

[Hadj-Mabrouk 92] : Hadj-Mabrouk H. « Apprentissage automatique et acquisition de connaissances : deux approches complémentaires pour les systèmes à base de connaissances. Application au système ACASYA d'aide à la

certification des systèmes de transport automatisés ». *Thèse de doctorat*, Université de Valenciennes, décembre 1992.

[Hadj-Mabrouk 95a] : Hadj-Mabrouk H. « La maîtrise des risques dans le domaine des automatismes des systèmes de transport guidés : Le problème de l'évaluation des analyses préliminaires de risques ». *Revue Recherche-Transport-Sécurité*, numéro 49, Éditions Dunod, pp 101-112, France, Décembre 1995.

[Hadj-Mabrouk 95b] : Hadj-Mabrouk H. « L'apprentissage automatique : principes et exemple d'application au domaine de la sécurité ». JE'95*, Journées électronique et informatique pour la sûreté*, Commissariat à l'Énergie Atomique. Gif-sur-Yvette, 7-9 février 1995, pp 187-197.

[Hennebert 87] : Hennebert C. « De nouveaux outils : ateliers de qualification de logiciels ». *Revue RATP Études-Projets*, 4° trimestre 1987.

[Huet 94] : Huet G. « Certification du logiciel : méthodes et outils - État de l'art des méthodes formelles en génie logiciel ». *Rapport de fin de contrat SGDN n°11*, SGDN/STS/VST/5, 22 avril 1994.

[Huet et Paulin-Mohring 93] : Huet G., Paulin-Mohring C. « Preuves et construction de programme ». Dossier scientifique, La recherche en informatique, Le courrier du CNRS n°80, février 1993.

[IEC 91] : IEC 65A 122 - International Electrotechnical Commission Standard - Software for computers in the application of industrial safety-related systems, 1991.

[ISO 94] : ISO 8402 - Norme internationale - Management de la qualité et assurance de la qualité. Vocabulaire, 1994.

[Laprie 92] : Laprie J.C. « Sûreté de fonctionnement : concepts de base et terminologie », Dependable Computing and Fault-tolerance Systems, Vol. 5, 1992.

[Lebowitz 87] : Lebowitz M. « Experiments with Incremental Concept Formation : UNIMEM ». *Machine Learning*, vol 2, 1987, p 103-138.

[Marrakchi 86] : Marrakchi M. « Représentation des connaissances pour l'aide au diagnostic industriel : application au système expert SEDIAG ». *Thèse de doctorat*, Université de Valenciennes, mars 1986.

[MIL 93] : MIL-STD-882C : Military standard - System safety program requirements - Departement Of Defense, 1993.

[Musa et al. 87] : Musa J.D., Iannino A., Okumoto K. « Introduction à la fiabilité du logiciel ». Technique et Science Informatiques, vol. 6, n°4, 1987.

[NF 90a] : Norme française NF F 71-011 - Installations fixes et matériel roulant ferroviaires - Informatique - Sûreté de fonctionnement des logiciels - généralités, 1990.

[NF 90b] : Norme française NF F 71-012 - Installations fixes et matériel roulant ferroviaires - Informatique - Sûreté de fonctionnement des logiciels - Contraintes sur le logiciel, 1990.

[NF 91] : Norme française NF F 71-004 - Installations fixes et matériel roulant ferroviaires - Informatique - Méthodologies de développement des équipements microinformatiques et documentation associée, 1991.

[Nicola 93] : Nicola C. « État de l'art sur la méthodes et les outils de validation des logiciels ». *Rapport MASI* 93.14, avril 1993.

[Place et Kang 93] : Place P.R.H., Kang K.C. « Safety-Critical Software : Status Report and Annotated Bibliography », Software Engineering Institute, technical report CMU/SEI 92-TR-5 ESC-TR-93-182, juin 1993.

[Sebag et Schoenauer 90] : Sebag M., Schoenauer M. « Apprentissage de règles par découverte ». *5èmes Journées Françaises de l'Apprentissage* : JFA 90, Lannion 25-26 Avril 1990, p 213-231.

[Sommerville 88] : Sommerville I. « Le génie logiciel et ses applications ». *InterEditions*, 1988.

[Sowa 83] : Sowa J. « Conceptual structures : information processing in mind and machine », Ch. 3, Addison Publishing Company, 1983.

[Vignes 95] : Vignes S. « Le développement de logiciel : étapes, méthodes, outils et procédures » Dossier Génie logiciel, *Revue d'Électronique et d'Électricité*, n°1, juin 1995.

[Wirsing 93] : Wirsing M. « Développement de logiciel et spécification formelle ». *Technique et Science Informatiques*, vol. 12, n°4, 1993.

III/ Aide à l'analyse de la sécurité au niveau MATÉRIEL

Projet « SASEM »

Maquette de système expert pour l'aide à l'analyse des modes de défaillance, de leurs effets
et de leur criticité des équipements matériels

1. CONTEXTE GENERAL DE L'ETUDE ET COLLABORATION SCIENTIFIQUE

L'objectif de la recherche consiste à étudier la faisabilité d'un système à base de connaissances d'aide à la capitalisation et à l'évaluation des analyses des modes de défaillance, de leurs effets et de leur criticité (AMDEC) des équipements matériels. La base de connaissances a été élaborée à partir des données impliquées dans les AMDEC de trois systèmes de transport guidés : VAL de Lille, TVM 430 du TGV Nord et MAGGALY de Lyon. Ce travail qui s'inscrit dans le cadre du programme interministériel de recherche sur les transport PREDIT-ASCOT, a été effectué en partie par deux stagiaires (Catherine CAUDRON et Sandrine DAUFES) de l'Ecole Polytechnique Féminine de Sceaux dont j'ai assuré l'encadrement scientifique.

2. METHODES ET OUTILS D'ANALYSE DE LA SECURITE DES EQUIPEMENTS MATERIELS

L'analyse de la sécurité des équipements matériels porte notamment sur les cartes électroniques et les interfaces définies comme étant de sécurité. Cette analyse met en œuvre deux approches: une approche de type inductif par AMDEC (analyse des modes de défaillance, de leurs effets et de leur criticité) généralement complétée par une MCPR (méthode des combinaisons de pannes résumées) et une analyse de type déductif par recherche de scénarios d'insécurité mettant en défaut le respect des critères de sécurité issus des analyses de sécurité fonctionnelles (ASF). Cette analyse déductive nécessite généralement le recours à la méthode de l'arbre des causes (MAC). L'Analyse des Modes de Défaillance et de leurs Effets (AMDE) est une méthode inductive permettant d'effectuer une analyse des modes de défaillance des composants, de leurs causes, et de leurs effets sur le système. On distingue quatre étapes principales pour réaliser une AMDE (Villemeur 88) : Définition du système, de ses fonctions et de ses composants ; Etablissement des modes de défaillance des composants et de leurs causes envisageables ; Etude et évaluation des modes de défaillance sur les fonctions du système; Conclusions et recommandations. Une extension naturelle de l'AMDE est l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC). Pour chaque mode de défaillance, elle permet d'évaluer le couple «probabilité-gravité». Plus la probabilité est grande et plus les effets sont jugés pénalisants, plus la criticité du mode de défaillance est importante et plus il devient nécessaire de prendre des mesures correctives et/ou préventives. Une étude bibliographique sur les outils permettant de soutenir les méthodes évoquées est synthétisée dans la figure 1 [Caudron et Daufes 96].

Outils	Société	AMDE	AMDEC	MAC	MCPR	Autres méthodes possibles
FIABEX	DATACEP	OUI	OUI	OUI	NON	Analyse fonctionnelle, Bloc diagramme, disponibilité de production, fiabilité prévisionnelle, Graphe de Markov, HAZOP
FIGARO	EDF	NON	NON	OUI	NON	Bloc diagramme, disponibilité de production, fiabilité prévisionnelle, maintenabilité prévisionnelle, Graphe de Markov, Réseau de Pétri
SPIRAL	CEA	NON	NON	NON	NON	
FURAX	CEA	OUI	NON	OUI	NON	Graphe de Markov
SOFIA	SOFRETEN	OUI	OUI	OUI	NON	Analyse fonctionnelle, allocation SdF, bloc diagramme, disponibilité de production, HAZOP

Figure 1: exemples d'outils d'aide à l'analyse de la sécurité des équipements matériels

3. MOTIVATIONS ET OBJECTIF DE L'ETUDE

Ces méthodes prévisionnelles d'analyse des défaillances présentent un intérêt indéniable pour l'analyse de la sécurité des équipements matériels. Elles permettent d'évaluer et d'analyser les dangers liés à l'utilisation du système et d'identifier les effets, les causes ainsi que les combinaisons des modes de défaillance des composants. Cependant, leur mise en œuvre présente au moins trois inconvénients : la nécessité d'utiliser plusieurs méthodes à la fois, la difficulté d'analyse due à la taille considérable des données manipulées (telles que les arbres de causes) et, enfin, la

difficulté d'être exhaustif pour l'analyse des défaillances significatives dans le cas d'un équipement ou système de transport complexe. En conclusion, ces méthodes, bien qu'indispensables pour analyser la sécurité des systèmes, ne sont pas suffisantes. Aucune méthode, à elle seule, ne permet d'assurer l'exhaustivité de l'analyse de sécurité.
Il est souvent nécessaire de recouper les résultats obtenus par une méthode avec ceux obtenus par une autre, complémentaire. Pour de telles méthodes, l'exhaustivité de l'analyse de sécurité demeure essentiellement fondée sur l'intelligence et l'intuition humaine. Nos travaux se sont donc orientés vers la spécification de démarches d'analyse et d'évaluation de la sécurité basées sur les techniques d'intelligence artificielle. L'objectif final est de compléter et de renforcer les méthodes actuelles.

L'étude a été motivée par diverses constatations révélées par la phase d'identification du problème :

- Le besoin d'améliorer l'expertise et la qualité de décision dans le domaine d'analyse de la sécurité des matériels (ASM) par l'archivage, la formalisation et la diffusion du savoir-faire des experts ;
- La difficulté d'exploiter la masse considérable de connaissances impliquées par l'ASM ;
- Le souci d'aider les experts du domaine à juger l'exhaustivité du dossier d'ASM,
- L'exigence d'un formalisme précis, rigoureux et explicite pour représenter les ASM. En effet, comme le montre la figure 2, les formats de représentation des résultats (d'une AMDEC par exemple) sont extrêmement variés et ne font pas l'objet d'un consensus.

Ces raisons ont orienté le cahier des charges vers l'étude de faisabilité d'un outil d'aide à la capitalisation et à l'évaluation des analyses de sécurité des équipements matériels dans le domaine des transports guidés. Cette étude fait l'objet du projet de recherche « SASEM ». Les premiers travaux réalisés en collaboration avec l'École Polytechnique Féminine ont porté seulement sur la conception d'une maquette de système à base de connaissances d'aide aux AMDEC des équipements matériels relatifs à trois systèmes de transport guidés. L'objectif est d'exploiter les AMDEC historiques envisagées sur des équipements matériels certifiés tels que celui du système TVM430 du TGV-NORD en vue d'analyser et d'examiner l'exhaustivité, la cohérence et la pertinence des AMDEC d'un nouveau système de transport. Les paragraphes suivants présentent les principaux résultats de cette étude de faisabilité.

Code n°..... Nom de l'analyste..... Nom de l'ingénieur de conception.....

Désignation de l'équipement	Fonction	Repère	Modes de défaillances	Causes de défaillances	Effets de défaillances		Détection de la défaillance	Dispositif de remplacement	Probabilité de défaillance	Niveau critici
					Effet local	Effet final				

Format de représentation d'une AMDEC selon la norme X60-510

BLOC : .....
ELEMENT : ....

Fonctions	Modes de défaillances	Causes de défaillances	Effets de défaillances	Gravité	Moyens de détection	Actions correctives

Format de représentation d'une AMDEC proposé lors du séminaire DINOV [Barbet et Lansade 93]

MODES DE DEFAILLANCES, ANALYSE DES EFFETS ET DE LA CRITICITE De : ..... Numéro : ..... Edition : ..... Date
Equipement : Sous-Système : Système : Phase opérationnelle : Phase de
Référence du circuit : Liste de composants : Bloc diagramme Fonctionnel de fiabilité :

N°	Dénomination	Bloc	Fonctions	Modes de défaillances et causes possibles	Fonctionnement résultant et effets sur l'équipement / le sous-système / le système	Symptômes observables	Méthode de prévention ou de compensation	Gravité

Format de représentation d'une AMDEC utilisée dans le cadre du système de transport guidé A

Sous-Système : ..... Mission : ..... Module : .....

Fonctionnalités	Modes possibles de défaillances	Effets sous ensemble	Situations contraires à la sécurité	Contraintes de sécurité	Protections	Implantation des protections	Moyens de détection	Temps de mise en états de sécurité

Format de représentation d'une AMDEC utilisée dans le cadre du système de transport guidé B

Figure 2 : exemples de formats de représentation des résultats d'une AMDEC

4. PRINCIPAUX RESULTATS OBTENUS

L'étude de faisabilité d'un système à base de connaissances d'aide aux AMDEC, appliquée au domaine de la sécurité des systèmes de transports guidés, a débouché sur les principaux résultats suivants détaillés dans [Caudron et Daufes 96] :

- Elaboration d'un nouveau formalisme de représentation des AMDEC qui tient compte des usages dans le domaine des transports guidés et tente de respecter ce qui est préconisé par la norme X60-510 ;
- Constitution d'une base de connaissances des AMDEC à partir de l'analyse des dossiers de sécurité des équipements matériels des systèmes suivants : VAL de Lille, MAGGALY de Lyon et TVM 430 du TGV Nord ;
- Conception d'une maquette de faisabilité (en cours de développement) d'aide à la capitalisation et à l'évaluation des AMDEC.

4.1. Proposition d'un format de représentation des AMDEC

Le format retenu pour caractériser un tableau d'AMDEC est présenté dans la figure 3 et comporte les paramètres descriptifs suivants :

1. Système (ex : VAL, MAGGALY, TVM 430)
2. sous-système (ex : bord, sol)
3. Niveau d'étude (ex : architecture, carte, interface)
4. Module (ex : carte CESS, carte CSS, carte CEU)
5. Mission du module (ex : acquisition d'états d'entrées de sécurité, assurer le traitement des informations)
6. Fonctionnalité (ex : détection de l'état d'entrée, amplification du courant, alimentation de la carte)
7. Mode de défaillance (ex : perte de signature, séquence erronée, déclaration à tord de l'état restrictif ou permissif). La figure 4 présente une liste non exhaustive de modes de défaillance génériques recommandés par la norme X60-510.
8. Cause de défaillance (les causes de défaillance des AMDEC examinées n'ont pas été renseignées)
9. Type de défaillance. En pratique, ce paramètre n'est pas renseigné. La norme X60-500 propose néanmoins, une définition des différents types de défaillances (figure 5).
10. Effet de la défaillance. On distingue dans cette rubrique les effets « locaux » qui ont des conséquences sur l'élément étudié, des effets « externes » ou « finals » qui ont des conséquences sur le système dans son ensemble. (ex : émission à tort des séquences caractéristiques, disparition du signal de sortie du circuit)
11. Détection de la défaillance. Dans les dossiers examinés, les valeurs attribuées à ce paramètre sont analogues aux valeurs assignées au paramètre effet de la défaillance.
12. Dispositif de remplacement ou de protection. Ce paramètre précise le dispositif à utiliser en cas de défaillance ou les mesures de protection à mettre en place pour éviter l'apparition des défaillances ou réduire leur probabilité d'occurrence. (ex : contrôle permanent de conformité d'état, coupure en sécurité de l'alimentation pour forcer les sorties à 0).
13. Probabilité de défaillance (ex : très probable, fréquent, improbable).
14. Niveau de criticité (mineur, critique, catastrophique). Dans la pratique, pour définir les niveaux de criticité, on parle de panne sécuritaire (critère non retenu), de panne non détectée (sans conséquence sur le signal) ou encore de panne sûre (panne détectée).

ANALYSE DES MODES DE DEFAILLANCES, DE LEURS EFFETS ET DE LEUR CRITICITE

Fait par : ..... Date : .....

Système : .....
Sous-Système : .....
Niveau d'étude : .....
Module : .....
Mission du module: .....

Fonctionnalité	Modes de défaillances	Causes de défaillances	Type de défaillances	Effets de défaillances		Détection de la défaillance	Dispositif de remplacement ou de protection	Probabilité de défaillances	Niveau de criticité
				Effet local	Effet externe				

Figure 3 : Formalisme de représentation d'une AMDEC proposé [Caudron et Daufes 96]

1	Défaillance structurelle (rupture)	17	Ecoulement réduit
2	Blocage physique ou coincement	18	Mise en marche erronée
3	Vibrations	19	Ne s'arrête pas
4	Ne reste pas en position	20	Ne démarre pas
5	Ne s'ouvre pas	21	Ne commute pas
6	Ne se ferme pas	22	Fonctionnement prématuré
7	Défaillance en position ouverte	23	Fonctionnement après le délai prévu (retard)
8	Défaillance en position fermée	24	Entrée erronée (augmentation)
9	Fuite interne	25	Entrée erronée (diminution)
10	Fuite externe	26	Sortie erronée (augmentation)
11	Dépasse la limite inférieure tolérée	27	Sortie erronée (diminution)
12	Est en dessous de la limite inférieure tolérée	28	Perte de l'entrée
13	Fonctionnement intempestif	29	Perte de la sortie
14	Fonctionnement intermittent	30	Court-circuit (électrique)
15	Fonctionnement irrégulier	31	Circuit ouvert (électrique)
16	Indication erronée	32	Fuite (électrique)

Figure 4 : Modes de défaillance génériques selon la norme X60-510

TYPE DE DEFAILLANCE	DEFINITION
En fonction de la vitesse d'apparition	
progressive	défaillance due à une évolution dans le temps de certaines caractéristiques d'une entité
soudaine	défaillance brutale due à une évolution quasi instantanée des caractéristiques d'une entité
En fonction de l'instant d'apparition	
en fonctionnement	défaillance se produisant sur l'entité, alors que la fonction requise est utilisée
à l'arrêt	défaillance se produisant sur l'entité, alors que la fonction requise n'est pas utilisée
à la sollicitation	défaillance se produisant au moment où la fonction requise est sollicitée
En fonction du degré d'importance	
partielle	défaillance qui entraîne l'inaptitude d'une entité à accomplir certaines fonctions requises, mais non toutes
complète	défaillance qui entraîne l'inaptitude totale de l'entité à accomplir toutes les fonctions requises
En fonction de la vitesse d'apparition et du degré d'importance	
par dégradation	défaillance qui est à la fois progressive et partielle
catalectique	défaillance qui est à la fois soudaine et complète
En fonction des causes	
par faiblesse inhérente (de conception ou de fabrication)	défaillance attribuable a une faiblesse inhérente à l'entité elle-même lorsque les contraintes ne dépasse les niveaux prévus lors de la conception
par emploi inapproprié	défaillance causée par l'application de contraintes en utilisation qui dépassent les possibilités spécifiées de l'entité, ou attribuable à un manque de précaution dans son utilisation
par fausse manoeuvre	défaillance d'une entité causée par une opération incorrecte de son utilisation
par vieillissement	défaillance causée par une dégradation dans le temps des caractéristiques de l'entité, liée à des phénomènes physico-chimiques, mécaniques,... tels qu'usure, fatigue, corrosion.
primaire	défaillance d'une entité dont la cause directe ou indirecte n'est pas une défaillance ou une panne d'une autre entité
secondaire	défaillance d'une entité dont la cause directe ou indirecte est une défaillance ou une panne d'une autre entité
En fonction de son origine	
interne à l'entité	défaillance dont l'origine est attribuée à l'entité elle-même
externe à l'entité	défaillance dont l'origine est attribuée à des facteurs externes à l'entité
En fonction de leur caractère	
systématique	défaillance liée d'une manière certaine à une cause qui ne peut être éliminé que par une modification de la conception, du procédé de fabrication, du mode d'emploi, de la documentation ou d'autres facteurs appropriés
reproductible	défaillance qui peut être provoqué à volonté en simulant ou en reproduisant sa ou ses causes
non reproductible	défaillance se produisant dans des conditions telles que l'application de sa ou ses causes (volontairement ou involontairement) ne reproduit jamais la défaillance ou que la reproduction est impossible à réaliser
de cause commune	défaillance affectant ou pouvant affecter simultanément ou en cascade à partir d'une même cause tout ou partie des composants d'une entité ou éventuellement plusieurs entités à la fois

Figure. 5 : Définition des différents types de défaillances selon la norme [X60-500, 1988]

4.2. Constitution d'une base de connaissances des AMDEC

Sur la base du formalisme de représentation des AMDEC précédemment établi, nous avons constitué une première ébauche de base de connaissances à partir des documents constructeurs des systèmes de transport guidés. Comme nous l'avons déjà évoqué, il existe plusieurs niveaux d'étude pour la conception d'un dossier de sécurité matérielle : niveau architecture, niveau carte et niveau interface. Afin de montrer la faisabilité de l'approche envisagée, nous avons limité l'étude aux deux premiers niveaux : architecture et carte. Pour chacun de ces niveaux, nous avons constitué une ébauche de base de connaissances.

La base de connaissances de niveau architecture à été élaborée à partir des dossiers TVM 430 du TGV Nord réalisés par CSEE Transport, tandis que celle du niveau carte a été construite à partir des dossiers du VAL de Lille et de MAGGALY de Lyon réalisés par MATRA Transport. L'examen des documents constructeurs a permis de révéler plusieurs lacunes : d'une part que la terminologie et les concepts liés aux AMDEC sont très fluctuants et parfois contradictoires d'un constructeur à un autre et d'autre part, la majorité des paramètres descriptifs d'une AMDEC ne sont pas en pratique renseignés. Par conséquent, le formalisme que nous avons proposé et qui se rapproche de très près de celui préconisé par la norme X60-510 est difficilement exploitable. Ceci est dû non seulement à la grande précision du formalisme proposé mais aussi à l'incomplétude et au manque de pertinence des AMDEC examinées. L'exemple suivant montre le caractère d'incomplétude des AMDEC réalisées :

- Système = A
- sous-système = Circuit ET20EF
- Niveau d'étude = Carte
- Module = Bloc 1
- Mission du module = Oscillateur
- Fonctionnalité = Résistance de filtrage de l'entrée
- Modes de défaillances = Coupure de la résistance
- Effets de défaillances = Disparition du signal de sortie du circuit
- Niveau de criticité = Criticité 3 (Panne sûre : panne détectée)
- ~~Causes de défaillances = **?**~~
- ~~Type de défaillances = **?**~~
- ~~Détection de la défaillance = **?**~~
- ~~Dispositif de remplacement ou de protection = **?**~~
- ~~Probabilité de défaillances = **?**~~

4.3. Développement d'une maquette de faisabilité d'un système expert d'aide aux AMDEC

La finalité de nos travaux vise le développement d'une maquette de faisabilité d'un système à base de connaissances d'aide à la capitalisation et à l'évaluation de la complétude et de la cohérence des AMDEC. Cette maquette est actuellement en cours d'élaboration et sa validation doit faire l'objet d'une étude ultérieure. L'architecture fonctionnelle de cette maquette, présentée en figure 6, est composée de trois principaux modules : une interface homme/machine (expert ou utilisateur), une base de connaissances et un moteur d'inférence.

L'interface homme/machine permet d'assurer le dialogue avec les utilisateurs et/ou l'expert. Cette interface assure deux grandes fonctions :

1. L'interface EXPERT facilite l'introduction et la mise à jour de connaissances dans le système. Les connaissances impliquées sont :

   - les connaissances expertes : l'expert est indispensable pour fournir les connaissances stratégiques pour évaluer les nouveaux dossiers d'AMDEC, mais aussi pour valider les connaissances produites par le système,
   - les connaissances historiques qui proviennent des dossiers AMDEC des systèmes de transport guidés déjà certifiés,
   - les nouveaux dossiers d'AMDEC a évaluer.

2. L'interface UTILISATEUR qui permet la consultation des différentes connaissances produites par le système, et notamment la consultation des AMDEC historiques et les résultats d'évaluation des nouveaux dossiers d'AMDEC.

La base de connaissances qui regroupe à ce jour une cinquantaine d'exemples d'AMDEC issus des systèmes de transport, est scindée en deux sous-bases : la première correspond au niveau architecture et la seconde contient les règles du niveau carte.

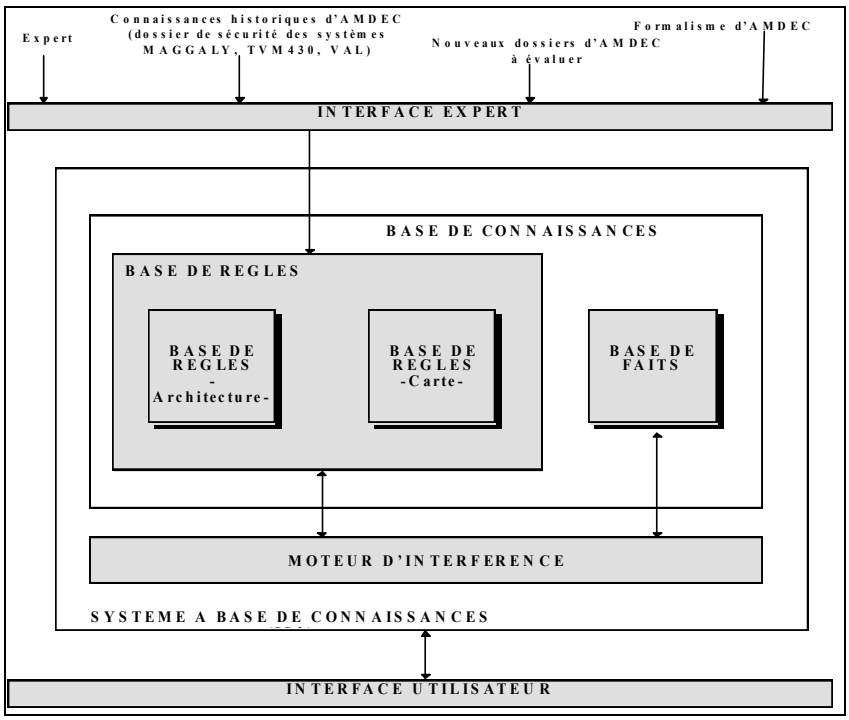

Figure 6 : architecture de la maquette du système expert d'aide aux AMDEC

Exemples de règles de « niveau architecture »

REGLE 1
SI systeme=" xxxxxxxxxxx "
  ET fonctionnalité="temporisation à l'attraction"
  ET mode de défaillance="diminution de la durée de temporisation"
ALORS effet de défaillance="passage libéral plus rapide"
  ET protection="temporisation à l'attraction à mini garanti en securite pour la sortie physique"
REGLE 2
SI systeme=" xxxxxxxxxxx "
  ET fonctionnalité="élaboration de séquences caractéristiques"
  ET mode de défaillance="perte de l'élaboration d'une ou plusieurs entrées de sécurité"
ALORS effet de défaillance="impossibilité dÕŽmettre un code"
  ET effet de défaillance="état déclaré restrictif"
  ET protection="non contraire à la sécurité"
REGLE 3
SI systeme=" xxxxxxxxxxx "
  ET fonctionnalité="positionnement des états de sortie"
  ET mode de défaillance="positionnement erroné"
ALORS effet de défaillance="état d'un ou plusieurs rangs de sortie du signal erroné"
  ET protection="détection d'état complémenté par circuit détecteur de seuil..."
  ET protection="une séquence ne peut exister qu'une fois pour tout le sous système"
  ET protection="contrôle permanent de conformité d'états"
  ET protection="contrôle de la date"
  ET protection="coupure en sécurité de l'alim permettant de forcer les sorties à 0"
  ET protection="relais à contact non chevauchant"

Exemples de règles de « niveau carte »

REGLE 1
SI systeme=" xxxxxxxxxxx "
  ET fonctionnalite="Résistance de filtrage de l'entrée"
  ET mode de défaillance="Coupure de la résistance"
ALORS effet de la défaillance="disparition du signal de sortie du circuit"
  ET criticité="criticité 3"
REGLE 2
SI systeme=" xxxxxxxxxxx "
  ET fonctionnalite="diode de compensation en température du transistor"
  ET mode de défaillance="court-circuit de la diode"
ALORS effet de la défaillance="disparition du signal de sortie du circuit"
  ET criticité="criticité 2"
REGLE 3
SI systeme=" xxxxxxxxxxx "
  ET fonctionnalite="condensateur de découplage de la base du transistor"
  ET mode de défaillance="coupure d'une patte du condensateur"
ALORS effet de la défaillance="disparition du signal de sortie du circuit"
  ET criticité="criticité 3"

5. CONCLUSION ET PERSPECTIVES

Cette section a présenté les principaux résultats d'une recherche sur le développement d'un système à base de connaissances d'aide à la capitalisation et à l'évaluation des AMDEC en termes de complétude et de cohérence. A ce jour, cette étude a permis de proposer un modèle de représentation des connaissances impliquées dans les AMDEC, de constituer une première ébauche de base de connaissances et enfin de concevoir une maquette de faisabilité. L'originalité de cette étude réside d'une part dans le formalisme élaboré qui permet de mieux structurer et organiser les connaissances d'AMDEC et d'autre part, dans la décomposition de la base de connaissances en deux sous-bases : base de règles de niveau architecture et base de règles de niveau carte. Ce travail doit se poursuivre et doit porter essentiellement sur les points suivants :

- L'acquisition et la modélisation des connaissances expertes (critères, stratégies et heuristique) d'analyse et d'examen d'une AMDEC ;
- L'étude plus fine des deux niveaux de connaissances identifiés en vue d'établir le lien (traçabilité) entre la connaissance de niveau architecture et celle de niveau carte ;
- L'enrichissement de la base de connaissances par d'autres exemples d'AMDEC afin qu'elle soit représentative du domaine. En effet, la phase d'acquisition des connaissances a permis uniquement de recenser une cinquantaine de lignes d'AMDEC
- La validation et l'amélioration du formalisme de représentation des AMDEC élaborées ;
- La poursuite du développement de l'outil logiciel d'aide à la capitalisation et à l'évaluation des AMDEC.

6. BIBLIOGRAPHIE

[Caudron et Daufes 96] : Caudron C., Daufes S. « Base de connaissances d'analyse des modes de défaillances, de leurs effets et de leur criticité. Application à la sécurité des équipements matériels des systèmes de transport guidés ». Rapport de projet industriel de l'Ecole Polytechnique Féminine. INRETS-ESTAS, Arcueil, janvier 1996, 113p (rapport confidentiel).

[Churchill et Rabouin 91] : Churchill D., Rabouin J. « Les études de sûreté de fonctionnement à la RATP », RATP Etudes-Projets, premier trimestre 1991.

[Dinov 93] : « Analyse et évaluation de la sécurité de fonctionnement des matériels et logiciels » - Séminaire DINOV, juin 1993.

[Isdf 93] : « Recensement des logiciels des SdF » - Institut de Sûreté De Fonctionnement, juillet 1993.

[Lievens 76] : Lievens C. « Sécurité des systèmes », Cepadue-Edition 1976.

[Mignot et Mur 92] : Mignot J., Mur JL. « Modéliser pour comprendre : étude sûreté d'une système mécanique à l'aide de l'outil FIABEX », Textes des conférences du 8ème colloque de fiabilité et de maintenabilité, CEA, octobre 1992.

[Moureau 95] : Moureau R. « FURAX, Outils d'aide à l'analyse qualitative et quantitative de la fiabilité des systèmes », Recueil des actes de la journée électronique, CEA, février 1995.

[Re-Aéro 701 11] : « Guide des méthodes courantes d'analyse de la sécurité d'un système missile ou spatial », novembre 1986.

[Villemeur 88] : Villemeur A. « Sûreté de fonctionnement des systèmes industriels. Fiabilité, facteurs humains, informatisation », édition Eyrolles 1988.

[X60-500] : Terminologie relative à la fiabilité, maintenabilité, disponibilité, octobre 1988.

[X60-510] : Technique d'analyse de la fiabilité des systèmes - Procédures d'analyses des modes de défaillances et de leurs effets 19??.

QUATRIÈME PARTIE

CONCLUSIONS ET PERSPECTIVES

1. BILAN DES TRAVAUX RÉALISÉS ET NOUVELLES ORIENTATIONS

L'ensemble des méthodes, techniques et outils présentés tout au long de ce mémoire (projets SAPRISTI, ACASYA, SAUTREL, SPECIALS, SASEM) apportent certes une aide lors de la phase d'évaluation de la complétude et de la cohérence des méthodes de *construction de la sécurité* au niveau système, matériel et logiciel. Cependant, plusieurs analyses de terrains montrent l'insuffisance de ces approches et l'intérêt de développer d'autres méthodes complémentaires. D'une part, il me semble indispensable d'ajouter une autre composante fondamentale et souvent négligée dans le processus de construction de la sécurité d'un système industriel à risques à savoir la composante humaine. Il s'agit de développer une démarche globale intégrant les facteurs humains non seulement dans les activités d'analyses de sécurité mais aussi dans le cycle de développement d'un système. Cette nouvelle approche s'inscrit dans le cadre du projet « FACTHUS » que j'ai initié à l'INRETS et qui est en cours de développement en collaboration avec plusieurs partenaires universitaires et industriels. D'autre part, pour parfaire et mieux rationaliser les démarches conventionnelles d'analyse des études de sécurité d'un système, j'ai débuté l'élaboration d'un guide méthodologique d'évaluation de la sécurité qui fait l'objet du projet « VALIDE ».

Ce chapitre dresse un bilan de l'ensemble des travaux réalisés à ce jour dans le cadre de ces deux projets (FACTHUS et VALIDE) ainsi que les perspectives envisagées. Il présente enfin les activités de recherche que j'ai récemment lancées.

2. AIDE À L'ANALYSE DE LA SÉCURITÉ AU NIVEAU HUMAIN : projet « FACTHUS »

Une étude a montré que l'erreur humaine reste très présente dans le domaine ferroviaire et a aussi révélé l'absence de formalisme dans l'expression des besoins au regard des facteurs humains. Ces constatations sont issues d'une étude préliminaire des statistiques d'accidents ferroviaires, d'une analyse de terrain (visites techniques des sites SNCF) et enfin d'une étude sur la prise en compte des facteurs humains dans plusieurs secteurs : armement (DGA), nucléaire (EDF), spatial (CNES), transport (SNCF, RATP),...

Cette section présente les principaux résultats des travaux en cours de réalisation ainsi que les travaux envisagés dans le cadre du projet de recherche « FACTHUS » dont l'objectif est la conception et la mise en œuvre d'une méthode d'intégration des facteurs humains dans l'analyse de la sécurité et le développement des systèmes de transport guidés.

2.1. Contexte général de l'étude et collaborations scientifiques

Dans le cadre de ses missions de recherche, l'INRETS s'intéresse au rôle de l'homme dans la sécurité des systèmes de transport guidés. Les travaux qu'il mène sur ce thème sont actuellement regroupés dans le projet « FACTHUS » que j'ai défini en février 1995 et qui constitue l'une des composantes du programme de recherche de l'INRETS (axe n° A3-13). Cette étude s'inscrit dans le cadre des travaux de recherche prévus dans l'accord cadre DTT-INRETS sous le thème transport guidé et sous-thème automatismes et systèmes de contrôle-commande.

Ce projet est développé en collaboration avec les laboratoires et instituts suivants :
- Laboratoire d'Automatique et de Mécanique industrielle et Humaine (LAMIH) de l'Université de Valenciennes (équipe Informatique Industrielle et Communication Homme-Machine du Professeur Patrick MILLOT),
- Institut Polytechnique de Sévenans (Professeur MAZOUET),
- Institut de Psychologie de l'Université René Descartes Paris V (Professeur J-C. SPERANDIO),
- Laboratoire HEUristique et DIAgnostic des SYstèmes Complexe (HEUDISYC) de l'Université de Technologie de Compiègne (Professeurs P. MORIZET-MAHOUDEAUX et M. SIDAHMED),

Les principaux organismes intéressés par les résultats de cette recherche sont les suivants :
- Direction des Transports Terrestres du Ministère des transports (Mme Jacqueline GAUDOT),
- Groupement régional de recherche sur les transports du Nord-Pas-de-Calais (GRRT),
- Département facteur humain de la SNCF (M. Pierre VIGNES, M. Blatter et Mme P. JOST),
- Régie Autonomes des Transports Parisiens (Mme Dominique SILHOL).

En septembre 1995, ce projet a permis de lancer la thèse de Bertrand TELLE. En octobre 1995, le projet FACTHUS a reçu le soutien de la Direction des Transports terrestres (DTT) du Ministère des Transports. Un contrat de recherche DTT/INRETS a été établi. En novembre 1995, la Région Nord Pas-de-Calais et l'INRETS ont convenus d'assurer le cofinancement d'une allocation de recherche attribuée à Bertrand TELLE. En mars 1996, une convention de recherche avec le LAMIH de l'Université de Valenciennes a été établie (équipe IICHM du Professeur Patrick MILLOT).

L'INRETS a proposé de confier à ce laboratoire la direction scientifique et l'encadrement effectif de M. TELLE, sans cependant renoncer à sa mission d'orientation et de validation des travaux de ce dernier. Cette mission est assurée par mes soins

A partir d'avril 1996, j'ai assuré l'encadrement scientifique de Joël Kotzmann, d'abord dans le cadre de son mémoire de stage de DESS d'Ergonomie de l'Institut de Psychologie de l'Université de Paris V, ensuite dans le cadre de son mémoire de stage de fin d'études d'ingénieur de l'Institut Polytechnique de Sevenans. Ces travaux ont porté essentiellement sur une étude bibliographique approfondie sur la prise en compte de l'ergonomie et des facteurs humains dans plusieurs secteurs industriels [Kotzmann 96a, 96b].

En mai 1997 le Laboratoire Heudisyc de l'Université de Technologie de Compiègne et l'INRETS ont convenus d'associer leurs efforts et de coordonner leurs actions en vue d'effectuer des travaux de recherche sur ce même thème. Cette recherche est soutenue par une convention (en cours de signature) est a pour but dans un premier temps d'étudier les principes d'intégration des facteurs humains dans les activités d'analyse de sécurité et de développement des systèmes de transport terrestre guidés. Plus précisément, cette étude suppose le passage par les trois grandes étapes suivantes :

1. Analyse des méthodes et outils existants, en matière de facteur humain, en vue d'étudier leurs apports au domaine des transports guidés ;
2. Etude de l'applicabilité de ces méthodes et outils au domaine concerné et mise en évidence d'éventuelles lacunes;
3. Etude de faisabilité d'une approche méthodologique adaptée au problème.

Enfin, ce projet s'inscrit pleinement dans le programme incitatif « Sciences de la cognition appliquées aux transports ».

2.2. Introduction aux facteurs humains

C'est dans l'aéronautique que naissent les premières préoccupations de fiabilité humaine vis-à-vis du pilotage des avions. Les premières analyses prévisionnelles de fiabilité de systèmes incluant des erreurs humaines et leur quantification ont été effectuées en 1957. Entre 1950 et 1960, il y a eu l'apparition d'une nouvelle discipline appelée « Ergonomie » en Europe et « Facteurs Humains » aux États Unis. Entre 1970 et 1975, l'Évaluation Prévisionnelle de Fiabilité Humaine (EPFH) est réalisée par RASMUSSEN sur deux centrales nucléaires. A la demande des autorités de sûreté américaines SWAIN et GUTTMANN publient en 1983 un ouvrage sur les EPFH appliquées aux centrales nucléaires. Au Danemark, RASSMUSSEN effectue des études sur la variabilité des performances humaines et sur les causes des erreurs humaines et leurs mécanismes. En France, dans le domaine de l'aéronautique, une prise en compte des facteurs humains dans les études prévisionnelles de fiabilité des systèmes de sécurité des avions (Concorde, Airbus) a été réalisée. En France, dans le nucléaire, EDF a introduit le concept de redondance humaine pour le diagnostic des incidents. Elle a également développé des simulateurs pour la formation et l'étude du comportement des opérateurs en situation [Villemeur & Mosneron-Dupin, 88].

L**'ergonomie** est constituée de plusieurs disciplines, plus exactement de parties de disciplines qui concourent à la connaissance scientifique de l'homme au travail, sous les divers aspects physiologiques, psychologiques, sociologiques et médicaux du Travail Humain. Cette connaissance scientifique vise un objectif pratique qui conditionne et justifie l'existence même de l'Ergonomie : l'adaptation du travail à l'homme [Spérandio 88]. Suivant le contexte, «Ergonomie» désigne « la discipline scientifique qui étudie le fonctionnement de l'homme au travail et l'ensemble des méthodes et techniques qui permettent l'analyse puis la fiabilisation des situations de travail » norme FD Z 68-002 [AFNOR, 93]. Selon De Montmollin [De Montmollin 95], il est assez difficile de cerner les frontières et les contenus de l'Ergonomie. En effet le terme Ergonomie renvoie à des approches diverses et parfois opposées. L'auteur distingue deux types d'ergonomie qui se caractérisent par des modèles, des cadres théoriques et des méthodes différentes:

- L'ergonomie classique représentée par le courant américain *Human Factors*, que l'on peut traduire par "composant humain". Le but de cette discipline est de concevoir des dispositifs techniques adaptés aux "caractéristiques et limites" des êtres humains et ceci sans identifier précisément les types d'opérateurs et le contexte de travail. Ce courant a mis en place de nombreuses normes et recommandations générales pour l'adaptation des systèmes. Quelque soit la situation de travail, les ergonomes du courant *Human Factors* se cantonnent à les appliquer.

- L'ergonomie centrée sur l'activité humaine qui est cantonnée surtout dans les pays francophones. De Montmollin définit cet ergonomie comme le prolongement du courant *Human Factors*, qui a mis en place des bases indispensables au travail de l'opérateur (assise, éclairage, disposition des informations...). L'ergonomie francophone se base sur une analyse fine de l'activité de l'opérateur en situation réelle de travail. Elle aboutit généralement sur une étude du traitement de l'information effectué par l'opérateur : l'ergonomie cognitive.

En ce qui concerne le terme **facteur humain**, il est défini par « le corps des faits scientifiques concernant la diversité et la variabilité humaine, recouvrant les aspects biomédicaux, cognitifs, environnementaux, physiologiques, psychologiques et psychosociaux. Les facteurs humains incluent les principes et les applications dans les domaines de l'ergonomie, de la sélection du personnel, de la performance à l'emploi et de l'évaluation de la performance humaine » [DGA 94]. Selon la norme FD Z 68-002 [AFNOR 93] le terme facteur humain désigne « les connaissances scientifiques applicables à une situation de travail et leur mise en œuvre afin de modifier la situation vers un objectif donné ». En conception, les méthodes associées au courant *Human Factors* font appel à l'expérimentation sur un nombre restreint de variables contrôlées, alors que l'ergonomie s'attache davantage à l'analyse de situations de références réelles. Selon le projet de norme pr EN 50126 [CENE 94], les facteurs humains concernent « les aspects des caractéristiques humaines qui ont un effet sur l'obtention des objectifs d'un système. Ils ont trait aux aspects anatomiques, physiologiques et psychologiques de l'être humain et à son comportement, dans la mesure où ces aspects et ce comportement ont un effet sur le système concerné ». Ce terme est également défini par Amalberti [Amalberti et Mosneron-Dupin 97] par « l'ensemble de connaissances sur l'opérateur humain et de méthodes visant l'adéquation entre l'opérateur humain et son travail ».

La fiabilité humaine est « la probabilité pour qu'un individu, une équipe, une organisation humaine, accomplisse une mission, dans des conditions données, à l'intérieur de limites acceptables, pendant une certaine durée » [Nicolet et al. 89]. La fiabilité humaine est une technologie (de mise en œuvre de connaissances sur l'homme au travail) dont l'objet est l'aménagement du couplage entre les composantes humaines et techniques d'un système, afin que celui-ci réponde plus efficacement à sa tâche ou à sa mission [Leplat et De Terssac 90]. Le Projet de Norme CEI 56 (secrétariat) 410 [CEI 94] donne quelques précisions sur l'appréciation de la fiabilité humaine (HRA). La HRA traite de l'impact des opérateurs humains et des agents de maintenance sur la performance du système et peut être utilisée pour évaluer les influences des erreurs humaines sur la sécurité et la productivité. La HRA est une discipline qui rassemble plusieurs domaines tels que les techniques de fiabilité, la psychologie ou l'ergonomie. Elle identifie les possibilités de récupération d'erreurs (actions qui peuvent remédier à des erreurs précédentes). Selon ce projet de norme, la HRA comporte trois étapes.

La première étape concerne l'analyse de la tâche qui a pour but de caractériser la tâche à analyser pour identifier l'erreur humaine et évaluer l'IHM. La deuxième étape consiste à identifier l'erreur humaine. Cette étape permet de cerner les actions erronées lors de l'exécution d'une tâche ainsi que les causes d'actions erronées, de suggérer des mesures pour réduire la probabilité d'erreurs humaines, d'améliorer les possibilités de récupération, de réduire les conséquences d'actions erronées et enfin de fournir des données d'entrée pour la gestion du risque. La troisième étape, dont l'objectif est la quantification de la fiabilité humaine, permet d'estimer la probabilité d'exécution correcte d'une tâche ainsi que la probabilité des actions erronées.

Le terme « **erreur humaine** » a un sens générique, qui couvre tous les cas où une séquence planifiée d'activités mentales ou physiques ne parvient pas à ses fins désirées, et quand ces échecs ne peuvent être attribués à l'intervention du hasard [Reason 90]. Selon A. Villemeur [Villemeur 88], l'erreur humaine est définie comme une déviation par rapport à une action, à une séquence d'actions ou à une stratégie supposées optimales et servant de référence. Elle résulte de dysfonctionnements au niveau des activités sensorielles, mentales ou physiques de l'opérateur humain. Reason a introduit une typologie des erreurs qui distingue deux types d'actions [Reason 90] : les actions non voulues (l'intention d'agir correctement était présente) qui comportent les ratés liées à l'exécution des actions et les lapsus ou échecs du stockage de l'information et les déficiences du jugement qui concernent notamment les fautes et les échecs de la planification. Selon R. Amalberti et F. Mosneron-Dupin [Amalberti et Mosneron-Dupin 97], l'erreur est l'écart par rapport à une action, une séquence d'actions ou une stratégie servant de référence. Une erreur est susceptible de conduire à une défaillance. Une défaillance est un événement survenant lorsque le comportement du système s'écarte de la fonction attendue.

Les erreurs humaines sont souvent dépendantes. Une erreur peut en entraîner une autre. Il s'agit d'un écart entre le comportement de l'opérateur et ce qu'il aurait dû être. Il existe plusieurs causes de la défaillance humaine : erreur humaine, incapacité humaine d'origine interne (maladie, ...), incapacité humaine d'origine externe (perturbation des conditions de travail, formation insuffisante, ...), etc. Le système "homme mort" sur les trains est un exemple type de précaution pour réduire les probabilités des incapacités humaines. Dans la littérature, on distingue différents types d'erreurs : erreur opératoire, erreur de représentation et erreur de conception. L'erreur opératoire est une action incorrecte ou non réalisée en temps voulu lors de la conception des systèmes, il faut être conscient que l'opérateur humain dispose bien souvent de très peu de temps pour réagir. L'erreur de représentation résulte généralement d'une mauvaise interprétation de l'opérateur humain au travers de sa propre image mentale du système. Enfin l'erreur de conception est définie comme l'inadéquation des systèmes aux besoin de l'opérateur. Il existe plusieurs facteurs favorisant l'occurrence d'erreurs [Swain 83] : facteurs externes (situation de travail, équipement), facteurs internes (formation, condition physique) et facteurs de stress (d'origine physiologique ou psychologique)

En ergonomie, on parle d' « **analyse des tâches** ». Il s'agit d'une technique permettant de décrire les activités des opérateurs humains à un poste de travail. L'analyse des tâches décrit le système dans lequel les tâches sont effectuées, les conditions du travail et les opérations à effectuer. L'analyse des tâches décrit "ce qui est à faire" [De Montmollin 95). L'analyse des tâches prescrites consiste en interrogations (interviews, entretiens) de la hiérarchie et en consultations de documents. L'analyse des tâches réelles repose sur les déclarations spontanées ou sollicitées de l'opérateur. Généralement on distingue la tâche prescrite (ce que l'on attend de l'opérateur) et la tâche effective (ce qu'il fait effectivement). La tâche prescrite est celle qui est définie par celui qui en commande l'exécution, et formalisée sous forme documentaire. A côté de la tâche prescrite qui définit ce qu'on attend du sujet, une autre tâche (réelle) correspond à ce que l'utilisateur fait effectivement [Leplat 85]. Edwards (Edwards 73) propose une classification des tâches de l'opérateur humain : tâches simples (ouvrir une vanne manuelle), tâches complexes (réalisation d'un diagnostic d'accident), tâches de vigilance (détection d'une alarme, d'un signal), tâches de contrôle (surveillance et contrôle d'un processus) et tâches post-incidentelles ou post-accidentelles (activité de l'opérateur après un incident : réponse apprise ou recherche d'une stratégie nouvelle).

2.3. Motivations de la recherche

Les principales motivations du projet FACTHUS sont les suivantes [Hadj-Mabrouk 95, 96a] :

- La participation de l'INRETS-ESTAS à la certification d'un certain nombre de systèmes de transport guidés a révélé l'absence de formalisme dans l'expression des besoins au regard des facteurs humains lors de la définition des nouveaux systèmes de transport. En effet, les dossiers (de spécification, de conception, de réalisation, de validation, d'études de sécurité...) ne prennent pas en compte les critères et exigences liés aux facteurs humains. Il nous semble donc indispensable de considérer ces aspects humains afin d'améliorer sensiblement le degré de sécurité du système.
- [BCEOM 74]. La direction des transports terrestres a confié au BCEOM une étude ayant pour objectif l'analyse des causes et des conséquences des accidents dans les transports collectifs urbains. Les résultats de cette étude montrent que la défaillance humaine (faute, imprudence, maladresse,..) constitue la cause essentielle des accidents ($\geq$ 90%).
- [HSE 90]. Ce rapport contient un tableau distinguant les accidents par causes primaires. Il fait apparaître l'erreur humaine comme cause première de 270 accidents sur 1283 dont 113 collisions et 67 déraillements.
- [THE 93]. Cet article présente un tableau sélectif de statistiques d'accidents entre 1971 et 1991 qui montre que l'erreur humaine a été la cause de 103 déraillements par an en moyenne sur 1971-75, de 72 en 1987, de 64 en 1988, de 28 en 1989 et de 43 en 1990.
- [Joing 93]. Cet article évoque le sujet spécifique du respect de la signalisation et fait état d'un chiffre de 100 franchissements de signaux d'arrêt par an, dont 36 % avec engagement du point à protéger, la probabilité d'occurrence d'un accident grave étant de l'ordre de 3,5 accidents pour 1.000 franchissements avec engagement du point à protéger. Ce document évoque également une évaluation de la probabilité de défaillance d'un conducteur dans une séquence d'arrêt. Cette probabilité est estimée à 2×10^{-5} par séquence. De plus, cette étude fait apparaître que l'amélioration du niveau de sécurité ne peut être atteinte que si le KVB a peu d'influence sur le comportement futur du conducteur.
- [SNCF 94]. Ce rapport précise que les principales causes d'accidents proviennent notamment de défaillances humaines lors des manœuvres de conduite de trains. Le nombre de franchissements de signaux avec engagement du point protégé (25 en 1992 et 36 en 1993) n'est pas satisfaisant.
- [Flages et Churchill 94]. Selon les auteurs, l'expérience à la RATP montre que les erreurs humaines (fausse manœuvre, alarme négligée, mauvaise transmission d'information, ...) sont directement à l'origine d'environ 65% des défaillances d'un système et indirectement en cause dans pratiquement tous les cas restants.
- [Gonin 95]. 16 personnes meurent dans la collision entre un train de marchandises et le Paris-Nice en gare de Melun le 17 octobre 1991. Conclusion de l'enquête : erreur humaine. L'erreur humaine est à l'origine de 66% des accidents, les causes techniques ne représentent que 34% (VIAL - SNCF).
- [Keravel 95]. Selon l'auteur, pour obtenir les performances requises d'un système, le besoin d'intégrer les sciences humaines s'inscrit à toutes les étapes d'un projet de conception selon des objectifs précis : comprendre l'homme en situation et se donner des repères de conception pour intégrer les caractéristiques humaines dès la définition des fonctionnalités du système.
- [Jost 96]. Dans le cas de projets touchant la sécurité (notamment le développement de nouveaux systèmes techniques), les spécialistes de la SNCF s'efforcent de prendre en compte les facteurs humains. Pourtant, l'auteur constate « encore trop souvent des dysfonctionnements, surtout en phase de démarrage des projets, mais aussi en phase d'exploitation ou de maintenance. L'analyse de ces dysfonctionnements montre qu'ils ont souvent pour origine le fait que cette prise en compte des facteurs humains au cours des différentes phases de déroulement du projet reste encore insuffisante, partielle, trop tardive ou pas assez professionnelle : mauvaise ergonomie des postes de travail, organisation du travail inadaptée, notamment dans les situations perturbées ou transitoires,

manque de pertinence dans la sélection ou la formation du personnel, accompagnement social du projet insuffisant... ».

Tous les chiffres et les constatations précédents démontrent abondamment que l'erreur humaine reste très présente dans le domaine de l'exploitation ferroviaire et qu'elle doit être prise en compte non seulement dans les analyses de sécurité mais aussi tout au long du cycle de développement du système de transport [Hadj-Mabrouk 96a].

2.4. Objectif du projet « FACTHUS »

La recherche consiste à élaborer une méthode de développement d'un système de transport guidé intégrant les facteurs humains non seulement au niveau des analyses de sécurité (analyse préliminaire de risques, analyse fonctionnelle de la sécurité, ...) mais aussi au niveau des activités de développement du système de transport (spécification, conception, ...). L'intérêt premier de cette étude est d'élargir le champ de compétence de l'INRETS-ESTAS et de la DTT par la prise en compte des facteurs humains dans les tâches de certification et par conséquent d'optimiser le processus de mise en sécurité des systèmes de transport guidés. Cette recherche doit donc déboucher sur l'élaboration d'une approche méthodologique décrivant les principaux critères et contraintes liés aux facteurs humains à considérer lors des activités d'analyses de sécurité et de développement du système. L'ensemble de ces critères et contraintes doivent être pris en compte par les quatre principaux acteurs suivants [Hadj-Mabrouk 96b] :

- Le maître d'ouvrage lors de la définition et de l'homologation du système.
- Le maître d'œuvre lors du développement et de la validation de son système.
- L'INRETS-ESTAS lors de l'élaboration du rapport de certification (ou d'évaluation).
- La Direction des Transports Terrestres lors de l'autorisation de mise en service du système.

2.5. Principaux travaux réalisés et nouvelles orientations

Les premiers travaux de cette recherche ont permis d'identifier et de spécifier le problème, d'effectuer une étude préliminaire des statistiques d'accidents ferroviaires [David et al. 94], [Hadj-Mabrouk 95], d'effectuer une analyse de terrain lors d'une série de visites techniques sur différents sites de la SNCF en vue d'étudier la prise en compte des facteurs humains chez les exploitants [Telle et Vanderhaegen 96] et enfin de réaliser une étude bibliographique sur la prise en compte des facteurs humains et de l'ergonomie dans plusieurs secteurs [Kotzmann et Hadj-Mabrouk 96a, 96b] : armement (DGA), nucléaire (EDF), spatial (CNES), transports (SNCF, RATP), communications (poste), imprimerie de presse, etc.

2.5.1. Bilan des pratiques sur la prise en compte des facteurs humain en France

Nous présenterons ci-après les principaux résultats d'une étude bibliographique sur les pratiques de la prise en compte des Facteurs Humains en France [Hadj-Mabrouk 96b].

Intérêt de quelques démarches pour une application dans les transports guidés.

Certaines démarches proposées peuvent être d'un apport bénéfique au domaine de la sécurité des transports guidés :

- Démarche proposée par le centre d'étude de sécurité de la SNCF [Chollet et al. 92]. La combinaison entre une étude de sûreté de fonctionnement et une étude ergonomique peut être adaptable pour le développement des systèmes de transport guidé. En effet, ces deux approches sont complémentaires pour optimiser le processus de développement et d'analyse de sécurité d'un système.
- Démarche proposée par le DGA [DGA 1994]. L'aspect le plus important dans cette démarche est l'élaboration de documents facteur humain après chaque phase du projet. Ces documents permettent une meilleure transmission des résultats à tous les acteurs du projet.
- Démarche proposée par une entreprise française de la presse quotidienne [Garrigou, 92]. L'intérêt de cette démarche réside essentiellement dans la mise en place d'un groupe de suivi et des groupes de travail dans lesquels les futurs utilisateurs vont être impliqués pour la conception du futur système.
- Démarche proposée par l'EDF [Dien et Lagrange, 95]. Cette démarche nous semble intéressante car elle repose sur une bonne étude ergonomique fondée sur l'emploi de plusieurs analyses complémentaires (analyse de l'activité, retour d'expérience, utilisation de maquettes et de prototypes...).
- Démarche proposée par le CNES [Suchet, 92]. L'utilisation conjointe de l'analyse opérationnelle (rôle des opérateurs) et de l'analyse fonctionnelle (fonctions et contraintes du système) pour élaborer le modèle mental de l'opérateur cosmonaute, nous semble être d'un apport bénéfique pour élaborer des spécifications prenant en compte les facteurs humains.
- Démarche proposée par le département facteurs humains de la SNCF [Vignes, 95]. Cette démarche est intéressante puisqu'elle couvre une grande partie des étapes de développement d'un projet. Cependant, cette

démarche sociotechnique n'est pas soutenue par un exemple d'application permettant d'apprécier sa faisabilité dans le domaine ferroviaire.

- Démarche proposée par l'INRS [Fadier et Neboit, 96]. Cette démarche est intéressante car elle permet de mener conjointement deux types d'analyse : analyse de la fiabilité et analyse ergonomique. En outre, elle a été appliquée dans plusieurs domaines : métallurgie, conduite de processus chimique, procédé discontinu.

Points de convergence des méthodes étudiées

- Les pratiques employées par les entreprises pour améliorer la fiabilité humaine peuvent être scindées en deux catégories. La première de type "curatif" se base en grande partie sur le retour d'expérience en vue de rechercher les causes de dysfonctionnement et pour y remédier. La seconde de type "préventif" porte essentiellement sur la sélection, la formation et l'entretien des connaissances du personnel ; l'intégration des futurs utilisateurs dès les phases de spécification et de conception du système et enfin sur l'évolution vers l'automatisation des installations afin de minimiser les erreurs des opérateurs.
- Beaucoup d'entreprises utilisent la simulation comme un moyen de validation de certains concepts. Il s'agit généralement d'effectuer une expérimentation sous forme de maquette ou de prototype auprès de futurs utilisateurs. Cependant, cette manière de procéder soulève de nombreux problèmes. La simulation n'est pas totalement représentative de la situation réelle et elle ne correspond qu'à une partie du système global. En outre, les requêtes et les opinions des utilisateurs sont trop subjectives pour être correctement interprétées.
- Il semble qu'un consensus existe à propos des objectifs et de la place d'une démarche facteur humain au sein d'un projet, il en va autrement de la terminologie, des techniques et démarches employées.

Principaux motifs de divergences des méthodes étudiées

Les méthodes proposées par les auteurs ne font pas toujours l'objet d'un consensus même au sein d'un même secteur d'activité.

- Il n'existe pas suffisamment de recommandations normatives dans le domaine du facteur humain qui est en pleine évolution. Les usages sont très variés, ce qui est préjudiciable à la qualité des méthodes de développement des projets où la sécurité est primordiale.
- Les objectifs des entreprises dans le domaine des facteurs humains ne sont pas toujours les mêmes. Certaines développent des démarches pour réduire les erreurs des opérateurs humains dans l'exécution d'une tâche, d'autres pour améliorer les conditions de travail des opérateurs et d'autres encore pour quantifier la probabilité d'erreurs humaines ou d'étudier les incidences du système sur l'activité des opérateurs.
- La terminologie et les démarches sont très fluctuantes, voire contradictoires d'un secteur à l'autre. Le vocabulaire utilisé souffre d'imprécisions ou de confusions. Par exemple, les concepts de facteur humain, d'ergonomie, de fiabilité humaine..., souffrent de l'absence de définitions rigoureuses et admises par tous. Cette diversité menace la bonne compréhension des documents et démarches analysés.
- Enfin, ces méthodes ont été conçues pour des problèmes bien spécifiques.

Limite des méthodes étudiées

- Certaines démarches proposées sont en grande partie théoriques et ne sont pas soutenues par des applications industrielles. Ceci nous empêche d'apprécier leur bien fondé. Les secteurs les plus en pointe dans ce domaine sont le nucléaire (EDF), l'armement (DGA) et l'aéronautique (CNES).
- Rares sont les entreprises qui prennent en compte les besoins des futurs utilisateurs en amont d'un projet (spécification des besoins).
- L'acceptation d'une démarche facteur humain par les chefs de projet pose parfois des problèmes et des craintes : alourdissement du projet, allongement des délais de réalisation du projet et enfin, augmentation du coût des projets.
- Ces méthodes ne préconisent pas d'approche permettant d'analyser l'état psychologique des opérateurs humains, leur charge de travail, la variabilité de leur compétence ou encore leur état de stress, par exemple, dans des situations d'urgence où la sécurité est menacée.
- Aucune entreprise ne propose dans le cahier des charges d'un projet un volet spécifique aux facteurs humains.
- Aucune méthode, à elle seule, ne permet de couvrir l'ensemble des étapes de développement et d'analyse de sécurité d'un système de transport guidé.

Figure 1 : Synthèse des démarches de prise en compte des facteurs humains en France [Kautzmann 96b], [Kautzmann et Hadj-Mabrouk 96a] et [Hadj-Mabrouk 96b]

Entreprise	Secteur	Référence	Titre de la publication	Place dans le cycle de vie	Type d'analyse	Objectif de la méthode
SNCF Service d'ergonomie et facteur humain	Transport	(Lancien, 94)	Facteur humain et transport ferroviaire, application aux programmes de recherche : Cas du projet ASTREE	- Spécification - Validation - Exploitation	Ergonomie	- Etude des incidences du système sur l'activité des OH - Définition et expérimentation de l'IHM
SNCF Service d'ergonomie et facteur humain	Transport	(Jost, 96)	La démarche sociotechnique, démarche de fiabilisation des systèmes	- Spécification	Ergonomie	Proposition des principes de base pour développer la prise en compte des FH dans un projet
SNCF Service d'ergonomie et facteur humain	Transport	(Blatter, 96)	Prise en compte des FH dans un projet (cours DESS)	- Spécification - Exploitation	Ergonomie	Démarche théorique d'intégration des FH dans un projet de développement
SNCF Service d'ergonomie et facteur humain	Transport	(Vignes, 95)	Les activités liées à la mission sociotechnique dans le cadre d'un projet	- Spécification - Conception - Réalisation - Exploitation	Ergonomie	Démarche générale d'intégration des FH dans un projet
SNCF Service de Psychologie	Transport	(Macaire, 94)	La mise en oeuvre et le maintien de la fiabilité humaine du personnel de sécurité à la SNCF		Psychologie	Evaluation psychologique des aptitudes des futurs embauchés
SNCF Centre d'étude de sécurité	Transport	(Chollet, 92)	Analyse de le sécurité des procédures	- Spécification - Exploitation	- Ergonomie - S d F	Elaboration de recommandations pour améliorer la sécurité d'un système
RATP	Transport	(Flages & Churchill,94) (Silhol, 96)	La fiabilité humaine dans les métiers de sécurité à la RATP	Exploitation	Fiabilité humaine	Quantification de la probabilité d'erreurs humaines dans le domaine de la sécurité
D G A Délégation Générale pour l'armement	Militaire	(DGA, 94)	Guide pour la prise en compte des FH et de l'ergonomie dans les programmes d'armement	- Spécification - Conception - Réalisation - Exploitation	Ergonomie	Intégration des FH dans la conduite des programmes d'armement
CNES Centre National d'Etudes Spatiales	Spatial	(Suchet, 92)	Les FH dans la préparation d'un vol spatial habité	- Spécification - Conception - Validation - Exploitation	- Ergonomie - Psychologie	- Intégration des FH dans un processus de développement - Modélisation des activités d'un cosmonaute
EDF Service Réacteurs Nucléaires et Echangeurs	Nucléaire	(Dien & Lagrange, 95)	Une démarche d'ergonomie de conception pour définir la coopération Homme/machine	- Spécification - Conception - Réalisation - Exploitation	Ergonomie	Développement de systèmes homme/machine utilisables lors de la conception des salles de contrôle/commande des centrales nucléaires
INRS Institut National de Recherche et de sécurité	Sécurité	(Neboit, 90)	De l'analyse du système à l'analyse de l'interaction opérateur/tâche	- Spécification - Conception	- Ergonomie - Fiabilité - Sécurité	- Conception de situations de contrôle de processus - Recherche des dysfonctionnements d'un opérateur pour améliorer le système
INRS Institut National de Recherche et de sécurité	Sécurité	(Fadier & Neboit, 96)	Proposition d'une méthode d'analyse de fiabilité opérationnelle intégrant l'analyse ergonomique	- Spécification - Conception	- Ergonomie - Fiabilité - Sécurité	Améliorer la fiabilité et la sécurité des systèmes socio-techniques
AFNOR Association Française de Normalisation	Normalisation	NF EN 614-1 X35-004-1 Avril 1995	Actions ergonomiques à prendre en compte durant le processus de conception	- Spécification - Conception - Validation - Exploitation	Ergonomie	Démarche ergonomique qui s'intègre dans un processus de développement de machine. L'objectif est de pallier aux problèmes de sécurité
Imprimerie de Presse	Presse	(Garrigou, 92)	Les apports des confrontations d'orientations socio-cognitives au sein de processus de conception participatifs : le rôle de l'ergonomie	- Spécification - Conception	Ergonomie	Participation au processus de conception d'une imprimerie pour améliorer les conditions de travail.
La Poste (Lyon, St-Priest)	Communication	(Arnaud, 95)	Etude ergonomique d'un prototype de système d'aide à la manutention des sacs messagerie	- Spécification - Conception	Ergonomie	Amélioration des conditions de travail au poste de chargement d'un système d'aide à la manutention des sacs messagerie.

Après avoir dressé un bilan des pratiques en matière de facteur humain en France, nous présentons ci-après les premiers travaux réalisés dans le cadre du projet « FACTHUS » ainsi que les orientations et les grandes lignes à suivre.

2.5.2. Prise en compte des facteurs humains dans le cycle de développement d'un système

L'enchaînement d'un ensemble d'activités mises en œuvre dans un ordre bien déterminé pour réaliser un système est appelé cycle de développement ou cycle de vie d'un système. Le cycle de vie du système est classiquement synthétisé par un diagramme en «V» comprenant une branche descendante pour la spécification et la conception du système et une branche ascendante pour l'intégration et la validation du système. Cette méthodologie de développement suppose le passage par les cinq phases chronologiques suivantes (figure 2) : spécification du système, conception du système, réalisation des équipements, intégration du système et validation fonctionnelle du système. L'approche retenue pour développer le projet FACTHUS vise la prise en compte des facteurs humains dans les différentes activités de développement du système de transport et notamment lors des phases de spécification et de conception [Hadj-Mabrouk 95].

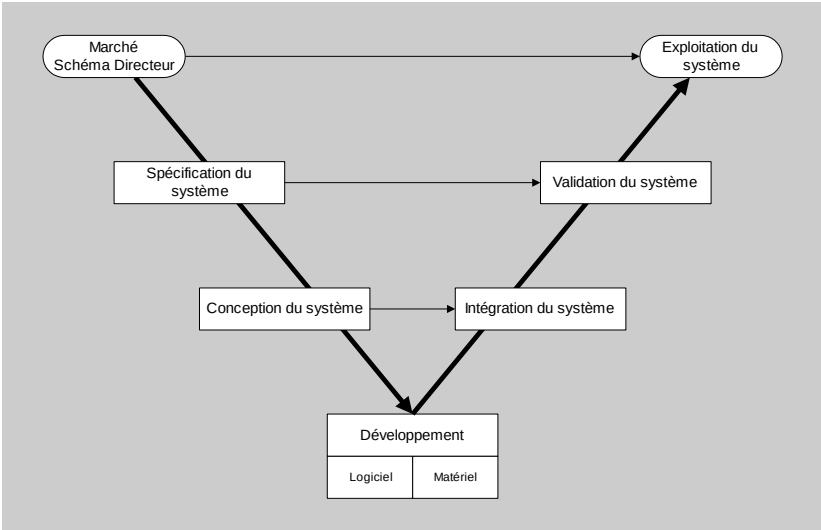

Figure 2 : prise en compte des facteurs humain dans le cycle de développement d'un système

2.5.3. Prise en compte des facteurs humains dans le processus de construction de la sécurité d'un système

Le processus de mise en sécurité d'un système de transport guidé comporte deux grandes activités : construire la sécurité et administrer la sécurité. Pour construire la sécurité, il existe plusieurs analyses hiérarchisées admises par l'INRETS, et réalisées par le constructeur : analyse préliminaire de risques, analyse de la sécurité fonctionnelle et analyse de la sécurité du produit réalisé qui concerne l'analyse de la sécurité des logiciels et l'analyse de la sécurité des matériels. L'approche retenue pour développer le projet FACTHUS consiste à intégrer les facteurs humains non seulement dans les activités de développement du système de transport (spécification, conception, réalisation, ...) mais aussi dans le processus de construction de la sécurité en distinguant quatre composantes [Hadj-Mabrouk 96a] : système, matériel, logiciel et humaine (figure 3). Cette prise en compte des facteurs humains dans le processus de construction de la sécurité permet de s'assurer de l'exhaustivité des analyses de sécurité.

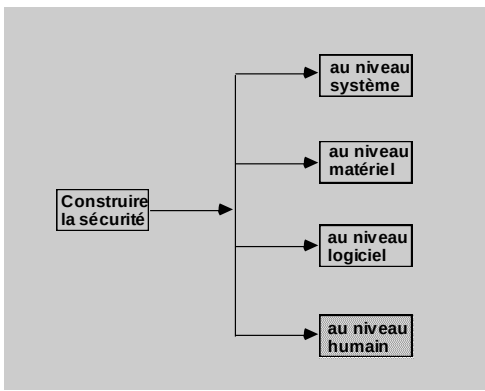

Figure 3 : prise en compte des facteurs humains dans le processus de construction de la sécurité

2.5.4. Principaux éléments à considérer lors du développement du projet « FACTHUS »

Les principaux éléments à considérer lors du développement de cette étude sont [Hadj-Mabrouk 96b] :

- L'identification des différentes tâches confiées aux opérateurs (agents de conduite, opérateurs au PCC, opérateurs de maintenance, ...) : tâches de surveillance et de contrôle (informations visuelles et sonores), tâches d'action (informations de commandes).
- La classification des tâches de l'OH : tâches simples (ouvrir une vanne manuelle), tâches complexes (réalisation d'un diagnostic d'accident), tâches de vigilance (détection d'une alarme, d'un signal), tâches de contrôle (surveillance et contrôle d'un processus) et tâches post-incidentelles ou post-accidentelles (activité de l'OH après un incident : expérience acquise ou comportement basé sur les connaissances par la recherche d'une stratégie nouvelle).
- L'identification et la classification des principales erreurs des opérateurs humains.
- L'identification des limites potentielles des opérateurs en vue de suggérer des spécifications pour la conception d'outils d'aide adaptés au fonctionnement réel de l'opérateur.
- L'analyse approfondie des scénarios d'accidents pour rechercher les principaux éléments initiateurs de dysfonctionnement propres aux opérateurs.
- La démarche à mettre en oeuvre pour concevoir et réaliser l'interface Homme-Machine respectant non seulement les contraintes d'exploitation mais aussi les facteurs humains.
- L'analyse de l'activité de l'opérateur lors de sa tâche de conduite. Cette analyse doit permettre de mettre l'accent sur les supports d'informations réellement utilisés parmi ceux prévus et disponibles, sur les besoins réels de l'opérateur en informations et sur les stratégies adoptées par l'opérateur lorsqu'une information nécessaire à la conduite est absente.

2.5.5. Exemple de classification d'erreurs humaines dans les transport guidés

Les figures 4 et 5 proposent deux exemples de classification d'erreurs humaines potentielles provoquées par le personnel d'exploitation (Opérateur au PCC et Agent de conduite ADC) [Hadj-Mabrouk 95, 98].

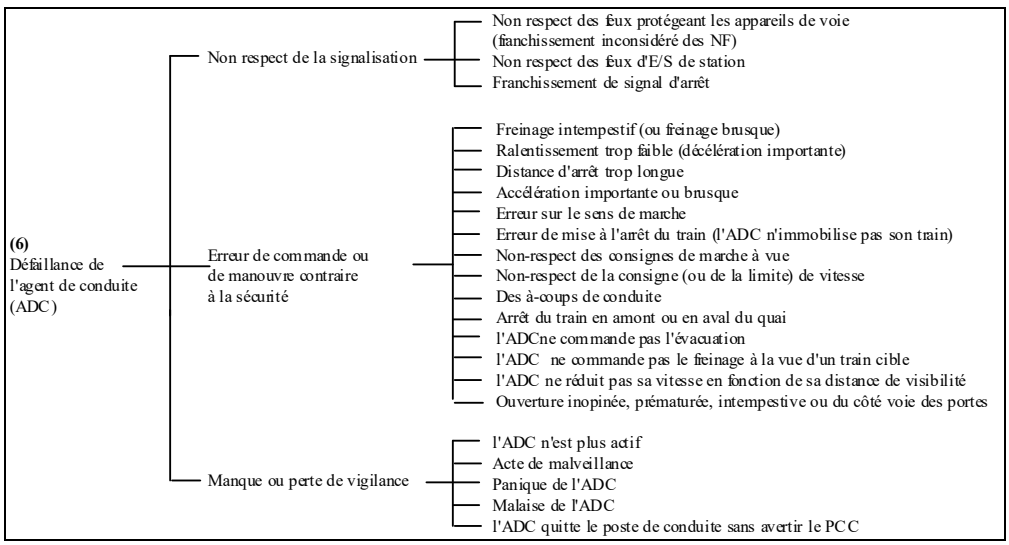

Figure 4 : Exemples d'erreurs potentielles provoquées par l'opérateur « agent de conduite »

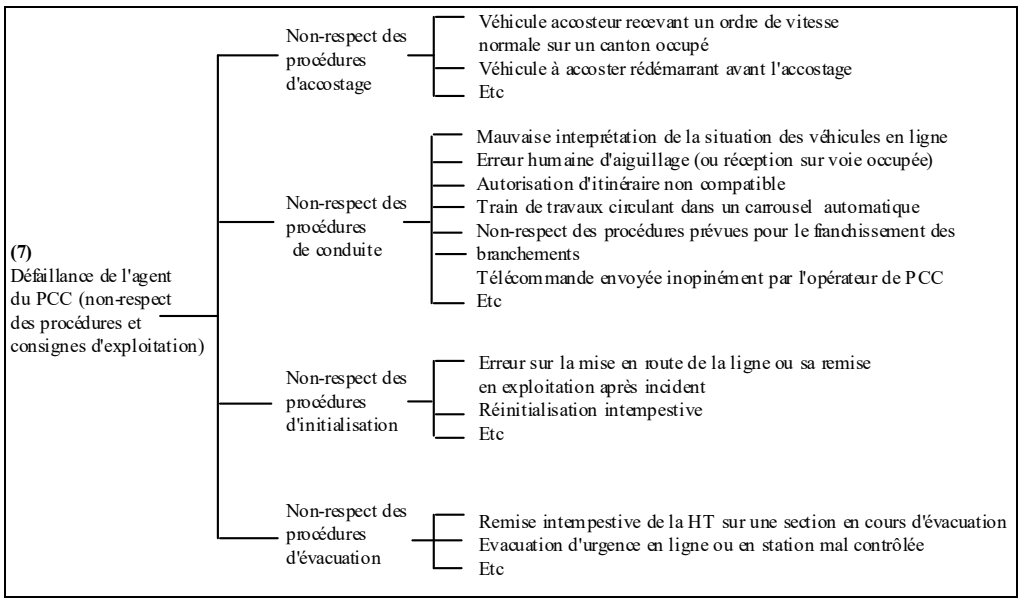

Figure 5 : Exemples d'erreurs potentielles provoquées par l'opérateur « agent du PCC »

2.5.6. Mise en place d'une équipe de spécialistes des facteurs humains

Une équipe de spécialistes des facteurs humains devra être mise en place dès le début du projet (lors de l'élaboration du marché et du schéma directeur). Cette équipe pourra s'étoffer au fur et à mesure que le projet prend de l'importance. Elle permet principalement de vérifier si les missions du futur système sont en adéquation avec les caractéristiques et les besoins des utilisateurs. Cette équipe doit réunir deux types de personnes [Kautzmann 96b] : des ergonomes représentant le maître d'ouvrage qui ont pour mission d'effectuer l'analyse du travail auprès des utilisateurs futurs du système et des ergonomes représentant le maître d'oeuvre qui devront posséder une bonne connaissance techniques afin de pouvoir assister correctement les concepteurs. Cette équipe aura également en charge l'organisation du groupe de suivi et des groupes de travail opérateurs-concepteurs [Garrigou, 92].

Le groupe de suivi est une entité qui a pour mission le pilotage politique de l'intervention ergonomique. La mission de ce groupe est la mise en place de l'intervention ergonomique ainsi que l'évaluation de la pertinence des différents pronostics sur les solutions des concepteurs et des demandes de modifications élaborées au sein des groupes de travail. Les principaux participants du groupe de suivi sont les chefs de projet, les représentants des opérateurs et l'équipe facteurs humains. Les groupes de travail ont une fonction technique et ergonomique durant les phases de spécification et de conception du projet. Ils permettent avant tout de confronter dans un cadre formel, les concepteurs aux utilisateurs. C'est en leur sein que sont réalisées les approches de l'activité future et l'élaboration de pronostics qui peuvent donner lieu à des demandes de modification du système. Les principaux participants à ces groupes de travail sont les opérateurs du système, les ergonomes et les concepteurs concernés(figure 6).

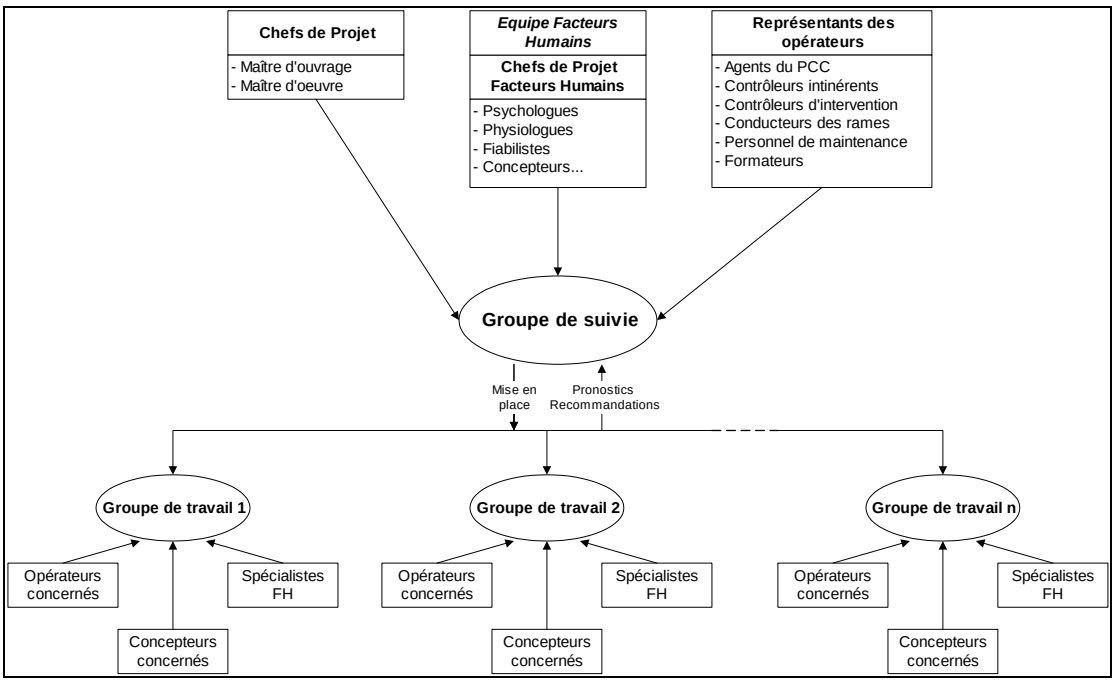

Figure 6 : Exemple de structure de conduite d'un projet "Facteur Humain"

2.5.7. Exemple d'intégration des facteur humain dans le développement d'un projet de système de transport guidé

La figure 7 rappelle les activités de développement et d'analyse de sécurité d'un système de transport guidé. En face de chaque activité, nous précisons de manière non exhaustive les différentes approches et méthodes de prise en compte des facteurs humains à effectuer. Cette première ébauche d'analyse est focalisée notamment sur la première activité de développement d'un projet : la spécification du système.

Activités de développement	Méthodes de sécurité	Prise en compte des facteurs humain
MARCHE Définir la faisabilité et les objectifs		- Définir la faisabilité humaine - Définir les objectifs du système Homme - Machine - Analyse du retours d'expériences - Analyse du travail de l'existant et de sites de référence
Spécification du système : - Mettre en place l'organisation du projet - Définir les besoins fonctionnels - Définir les interfaces externes au système - Définir la stratégie de validation - Identifier les risques liés au système	Analyse préliminaire de risques (APR)	- Mettre en place la structure de l'équipe Facteur Humains. - Définir les besoins fonctionnels des opérateurs humains (OH) - Définir les contraintes d'environnement sur les OH - Définir la stratégie de validation ergonomique du système - Identifier et classer les risques humains - Identifier les interfaces Homme - Machine - Recenser les données ergonomiques - Analyser la fiabilité humaine (Ex : SHERPA) - Modéliser les comportements des OH en situation nominal et dégradés - Constituer d'une bibliothèque de situations caractéristiques
Conception du système	Analyse fonctionnelle de la sécurité	- Prédire l'activité future des OH sur le système - Evaluer les solutions de conception (simulateurs, prototypes, maquettes...)
Réalisation des équipements	- MAC, AMDEC, MCPR - AEEL, ...	- Participer à la définition technique des fonctions réalisées par les matériels et les logiciels de chaque équipement
Intégration du système		Tests ergonomiques d'intégration du système
Validation du système		- Validation ergonomique des équipements - Tests ergonomiques des équipements sur le site
Exploitation du système		- Formation des opérateurs - Retour d'expérience Facteurs Humains

Figure 7 : Exemple d'intégration des facteurs humains dans le développement d'un système de transport guidé

3. PROJET « VALIDE» : METHODE DE VALIDATION DES CONNAISSANCES DE SÉCURITÉ

3.1. Contexte général de l'étude et collaboration scientifique

Le projet « VALIDE » a pour ambition de développer un guide méthodologique d'évaluation de la sécurité permettant de faciliter les missions d'expertise et d'assistance technique confiées à l'INRETS-ESTAS par l'État en rationalisant la démarche usuelle d'examen de la sécurité et en aidant les experts dans leur tâche cruciale d'évaluation des études de sécurité. En avril 1996, et dans le cadre d'une convention de recherche, le LIMAV (Laboratoire d'Informatique et de Mathématiques Appliquées) de l'Université de Valenciennes (équipe du Professeur Arnaud FREVILLE) et l'INRETS-ESTAS ont convenus d'associer leurs efforts et de coordonner leurs actions en vue d'effectuer des travaux de recherche sur le thème suivant : « Etude de faisabilité d'une démarche mathématique pour la validation de connaissances sur la sécurité des systèmes de transport terrestre guidés». A ce jour, cette étude a débouché sur la mise en œuvre d'une première ébauche de méthode globale d'évaluation de la sécurité présentée dans la suite de ce paragraphe. Les résultats de cette recherche peuvent être d'un apport bénéfique à l'agence de certification ferroviaire (CERTIFER).

3.2. Description générale de la démarche d'évaluation proposée

L'approche retenue pour examiner la cohérence, la complétude, la traçabilité et l'adéquation des méthodes et techniques de développement, de validation et d'homologation d'un système, s'articule autour de quatre grandes étapes illustrées par les figures 1 et 2 [Hadj-Mabrouk et al. 93], [Hadj-Mabrouk 94], [Hadj-Mabrouk et Bied-Charreton 94a, 94b, 94c] et [Hadj-Mabrouk et Tabka 96] : identification du problème, macro-analyse de la sécurité, micro-analyse de la sécurité et élaboration du rapport d'évaluation. Pour mieux cerner l'activité d'évaluation, la méthodologie envisagée sera appliquée en distinguant les trois niveaux d'analyse suivants : évaluation au niveau système, évaluation au niveau matériel et évaluation au niveau logiciel. Les étapes de cette méthodologie s'enchaînent de manière cyclique et reposent sur une idée simple et indispensable à la réalisation d'une évaluation exhaustive : il est important de procéder progressivement en élaborant des remarques et/ou questions à chaque étape. Cette approche est descendante car l'analyse s'effectue du général au spécifique. Elle part d'une analyse qui exploite des connaissances d'un niveau d'abstraction élevé (connaissances de "surface") et aboutit à une analyse fine faisant intervenir des connaissances d'analyse de bas niveau (connaissances "profondes"). Par analogie avec ces deux terminologies, l'étape de Macro analyse exploite et produit des connaissances de "surface" alors que l'étape de Micro analyse exploite et produit des connaissances "profondes".

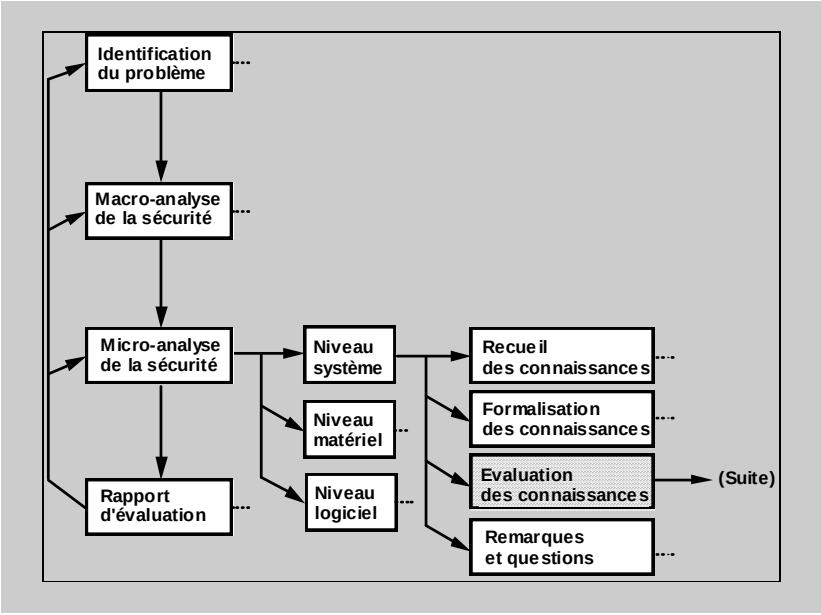

Figure 1: Projet «VALIDE» - démarche d'évaluation des connaissances de sécurité [Hadj-Mabrouk et Tabka 96]

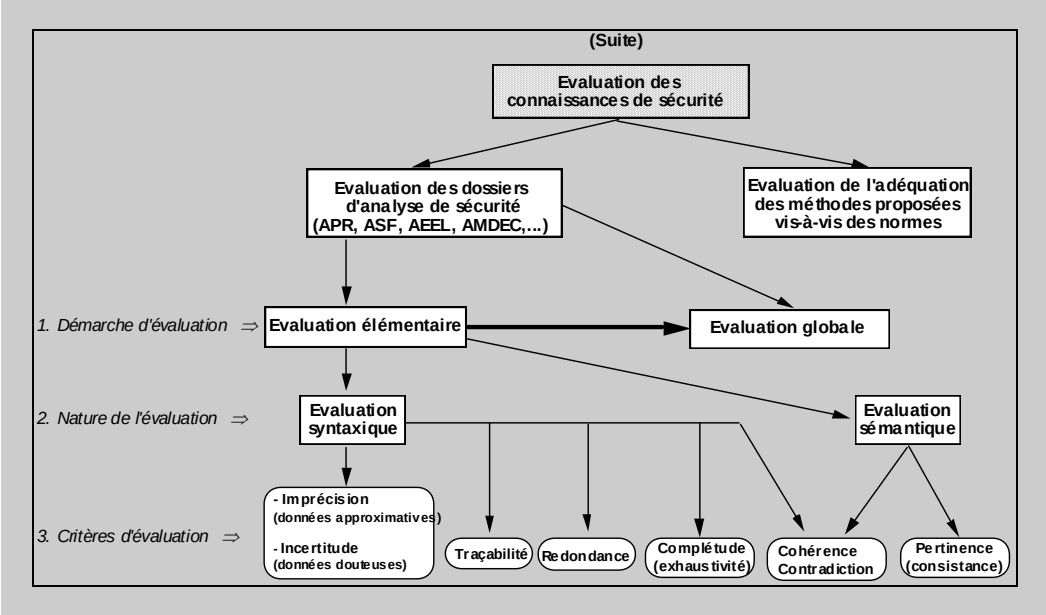

Figure 2 : Projet «VALIDE» - démarche d'évaluation des connaissances de sécurité [Hadj-Mabrouk et Tabka 96]

3.2.1. Identification du problème étudié et de son environnement

Cette première étape d'identification du problème a pour but d'identifier notamment le type de problème à traiter, la structure de conduite du projet, les aspects du problème risquant de soulever des difficultés sur le plan de la sécurité et qui nécessite de la part des experts évaluateurs une attention particulière, la nature des travaux confiés aux évaluateurs, les principaux documents du projet nécessaires aux évaluateurs pour remplir la mission, les procédures et méthodes de travail convenues entre les différents acteurs du projet, les principales normes de référence appliquées dans le projet, etc. En final, l'étape d'identification permet aux experts évaluateurs de se faire une première idée du problème à traiter, de les sensibiliser et les familiariser au domaine de l'étude. Elle constitue en fait le point de départ de la deuxième étape de la démarche : Macro analyse.

3.2.2. Macro analyse de la sécurité

La deuxième étape de Macro analyse porte notamment sur l'examen des documents généraux du projet (Plan de sécurité du projet, plan de développement, spécification des besoins utilisateur, ...) ainsi que sur les documents techniques de définition (dossier de spécification interne, dossier de spécification externe, ...). L'objectif principal de cette étape est d'apporter une appréciation générale sur l'adéquation et la cohérence des méthodes de développement du système ainsi que sur le processus de mise en sécurité proposé par le maître d'oeuvre.

3.2.3. Micro analyse de la sécurité

L'étape de Micro analyse s'attache à analyser et à évaluer les documents techniques de réalisation, les documents d'étude de sécurité et les documents techniques de validation. Plus précisément, si l'étape de Macro analyse consiste à évaluer la consistance et l'adéquation des méthodes de développement et d'analyse de sécurité envisagées, en revanche l'étape de Micro analyse vise à évaluer le respect de ces méthodes tout au long du cycle de développement du système. Elle permet essentiellement de contrôler la traçabilité du processus hiérarchique de construction de la sécurité.

3.2.4. Elaboration du rapport d'évaluation

Les étapes de Macro analyse et de Micro analyse débouchent en final sur d'éventuelles remarques et questions. Chaque remarque est appréciée subjectivement en fonction de son degré d'importance : mineure, majeure ou critique. L'ensemble des remarques formulées par les experts du domaine, des réponses apportées par le maître d'ouvrage ainsi que les éventuelles constatations recueillies à partir des visites des différentes installations d'essais sont synthétisées et analysées. Un avis sur le respect des exigences de sécurité que doit satisfaire le système est finalement formulé qui fait l'objet de la quatrième et dernière étape de la démarche d'évaluation envisagée.

Le rapport d'évaluation comporte les quatre principaux paragraphes suivants :

- Un rappel sur la mission confiée aux experts évaluateurs. Le but est de s'assurer que les experts ont bien assuré la totalité des tâches de travail qui lui ont été confiées ;
- Une synthèse des différentes étapes conduites par les experts pour réaliser leur mission ;
- Un bilan sur les diverses remarques et questions formulées par les experts évaluateurs et les réponses établies par le maître d'ouvrage.
- Conclusion des experts sur la cohérence, la complétude, la traçabilité et l'adéquation des méthodes et techniques de développement, de validation et d'homologation du système. Ceci permet d'aider les autorités compétentes à fonder une appréciation sur le niveau de sécurité du système en vue de délivrer l'autorisation de sa mise en service commercial.

3.3. Conclusion et perspectives

Ce paragraphe a présenté les premiers travaux réalisés pour le développement d'un guide méthodologique d'analyse et d'évaluation de la sécurité des systèmes de transport guidés. Ces travaux de synthèse sont issus en grande partie de notre expérience acquise lors de l'évaluation des études de sécurités relatives à deux systèmes de transport : TVM 430 du TGV Nord et ANTARES RER Ligne C. L'objectif de l'étude est de dégager à partir du savoir-faire des experts et chercheurs de l'INRETS-ESTAS une approche méthodologique générale permettant de mieux maîtriser, systématiser et rationaliser la démarche d'examen des études de sécurité des systèmes de transport guidés. L'approche envisagée repose sur l'utilisation des techniques et méthodes "cogniticiennes" d'acquisition de connaissances permettant de recueillir, structurer et formaliser l'expertise en matière d'analyse et d'évaluation de la sécurité. Ce guide permettra d'offrir un cadre de travail méthodologique et de pérenniser l'expertise du domaine. En outre, ce guide est indispensable dans le cas de l'accréditation de l'INRETS au statut d'organisme notifié car il constitue un élément de base du futur Plan Qualité INRETS-ESTAS. La suite des travaux, porte principalement sur la conception et la mise en oeuvre de méthodes et algorithmes mathématiques afin de préciser et de formaliser les critères d'évaluation de connaissances relatives à la sécurité et en particulier, les notions de cohérence (consistance?), complétude etc. [Hadj-Mabrouk et Tabka 96].

4. PROPOSITION D'UN PROGRAMME DE RECHERCHE SUR LE RETOUR D'EXPÉRIENCE DANS LA SECURITE DES TRANSPORTS FERROVIAIRES

En octobre 1997, j'ai initié en collaboration avec Mme Anca STUPARU et M. Robert JÉZÉQUEL un programme de recherche à partenaires multiples en vue de développer une base de scénarios d'accidents (ou de quasi-accidents) à partir du retour d'expérience [Hadj-Mabrouk et al 97]. Cette idée est issue des conclusions de la réunion du groupe « Métro du futur » du 12 septembre à la Direction des Transports Terrestres (DTT) du Ministère des transports et notamment des interventions de M. NALIN (DTT/SI1) et M. FERBECK (MATRA Transport). Les principaux organismes impliqués avec l'INRETS-ESTAS dans la réalisation de ce programme de recherche sont :

- RATP : Régie Autonome des Transports Parisiens (M. Jacques VALENCOGNES),
- SLTC : Société Lyonnaise de Transports en Commun (M. Alain QUÉRÉ),
- SNCF : Société Nationale des Chemins de Fer Français (Mme Michèle BÉRRIEAU),
- Département Mathématiques et informatique de la Faculté des sciences de Bizerte (Dr. Lassaâd MEJRI).

4.1. Contenu et déroulement du programme

Le programme de recherche envisagé va porter sur la réalisation des tâches suivantes [Hadj-Mabrouk et al. 97]:

1. Identification du domaine : cette étape de la méthodologie d'acquisition de connaissances permet de vérifier que le contexte du problème est favorable pour recueillir les connaissances et notamment les scénarios d'accidents (ou quasi-accidents). Elle permet notamment de vérifier l'existence et la disponibilité d'un ou plusieurs experts, la présence d'une expertise en adéquation avec les objectifs de l'étude et la possibilité d'assister à des traitements de cas réels sur le site (analyse de terrain). L'étape d'identification du domaine permet aussi d'identifier la nature et l'origine des informations utilisées par l'expert ainsi que la spécification de la forme de solution à élaborer. Plusieurs techniques de recueil de connaissances telles que l'interview ou les questionnaires seront employées pour identifier le domaine d'expertise. La phase d'identification du problème débouche finalement sur les sources de connaissances (ingénieurs concepteurs, exploitants, historiques tels que archives, manuels, comptes-rendus de réunions, bases de données, ...), les types et caractéristiques des connaissances manipulées (statiques, dynamiques, empiriques, évolutives, incomplètes, ...), les propriétés essentielles de la base de données de scénarios à développer pour l'archivage et la capitalisation des scénarios d'accidents ou des quasi-accidents, etc...

2. Structuration et modélisation des connaissances. Lors de cette étape, il s'agit de définir notamment un formalisme précis, rigoureux et explicite pour la représentation des scénarios d'accidents et des quasi-accidents. L'objectif est d'élaborer un cadre pour une définition exhaustive des scénarios.

3. Recueil et classification des scénarios : accidents provoqués par le système (les utilisateurs du système de transport sont passifs et subissent des dommages imputables à des défaillances des équipements du système) ; accidents provoqués par l'environnement (circonstances anormales de l'environnement ou conditions météorologiques) ; accidents provoqués à la fois par le système et l'utilisateur et enfin accidents provoqués par l'homme. Ces accidents potentiels n'ont généralement que peu de rapport avec le système qui représente seulement le cadre du déroulement de l'accident. L'utilisateur est l'initiateur des dommages engendrés à cause de ses actions qui peuvent être des fautes, des imprudences ou des maladresses. Dans ce contexte, les accidents potentiels (ou quasi-accidents) peuvent être liés soit à des défaillances du personnel de maintenance soit à des interventions de passagers (imprudence, maladresse, ...) ou à des défaillances du personnel d'exploitation (contrôleur itinérant, personnel d'intervention, agent de conduite, agent du PCC (non respect des procédures d'exploitation).

4. Développement d'une base de données relative aux scénarios d'accidents. Cette base sera organisée autour des deux entités suivantes (deux sous-bases). La première regroupe les scénarios imaginés lors des phases de spécification (analyse préliminaire de risques), de conception (analyse fonctionnelle de la sécurité), de réalisation (AMDEC, AEEL, MCPR, Arbre des causes). A cet effet, la base de scénarios développée à l'INRETS peut constituer la base de travail envisagée [Hadj-Mabrouk 92, 94, 97]. La deuxième sous-base est constituée de l'ensemble des scénarios issus du retour d'expérience (exploitation et maintenance du système).

5. Évaluation et validation de la base de scénarios développée. La qualité d'une base de scénarios se mesure généralement en évaluant la validité et l'utilité des connaissances acquises. Une connaissance est valide si elle est adéquate et cohérente par rapport à ce que l'on sait déjà du domaine de l'analyse de sécurité. Elle est utile si elle contribue à réaliser les objectifs définis, c'est à dire à améliorer le degré de sécurité des nouveaux systèmes de transports guidés.

6. Exploitation des connaissances. Cette phase permet d'exploiter les scénarios historiques archivés afin d'en dégager un savoir-faire susceptible d'aider l'ensemble des acteurs impliqués. Cela leur permettra de juger de la complétude de l'analyse de sécurité et par conséquent renforcera les méthodes classiques employées lors de la spécification et la conception d'un nouveau système de transport. Les approches envisagées pour cerner cette activité de recherche sont basées essentiellement sur l'emploi des techniques d'intelligence artificielle et notamment par l'utilisation des techniques d'apprentissage automatique.

4.2. Intérêt scientifique de la recherche envisagée

L'essentiel de la tâche d'analyse et d'examen de la sécurité consiste à imaginer de nouveaux scénarios d'accidents susceptibles soit de démontrer le caractère exhaustif de l'analyse de sécurité effectuée par le constructeur soit de la contredire. En ce sens, améliorer la qualité de décision des experts par la mise en oeuvre d'une base de scénarios historiques représente une aide substantielle pour les experts. Le développement de cette base nécessite la définition d'un formalisme précis, rigoureux et explicite pour la représentation des scénarios d'accidents. L'intérêt d'élaborer un modèle de représentation des scénarios d'accidents est majeur. Cela permet d'une part, d'aider les experts de certification à mieux structurer leurs connaissances et d'autre part de proposer éventuellement aux constructeurs des systèmes de transport, un cadre pour une définition exhaustive des scénarios d'accidents. Cette base de scénarios permet d'aider à rechercher des similarités et des analogies entre plusieurs configurations ou situations d'insécurité. En présence d'une situation contraire à la sécurité décrite sous forme de scénario par le constructeur, l'expert de certification raisonne par analogie. Il tente de rapprocher cette nouvelle situation d'insécurité de certaines situations vécues sur des équipements ou systèmes analogues déjà certifiés ou homologués. Pour effectuer cette analyse, l'expert de certification recherche des parallèles entre le cas qui lui est soumis et l'ensemble des cas typiques simulés ou vécus auxquels il a déjà été confronté.
En outre, le développement d'une base de scénarios permet de pérenniser l'expertise du domaine de la sécurité . En effet, l'expertise existante en matière de certification et d'analyse de sécurité des systèmes est rare, vulnérable et répartie entre plusieurs experts. Comme elle n'est ni consignée dans des manuels, ni enseignée, les experts de l'INRETS souhaitent l'approfondir en vue de conserver et de diffuser ce capital intellectuel auprès des jeunes experts. Cette base doit être évolutive et enrichie au fur et à mesure de la certification des nouveaux système car on ne peut raisonnablement pas attendre des experts qu'ils délivrent d'emblée leurs connaissances.

L'intérêt économique du sujet pour les systèmes de transports terrestres est clair. Il s'inscrit totalement dans les thèmes développés à l'INRETS-ESTAS depuis plusieurs années dans le cadre du PREDIT-ASCOT et du GRRT. En effet, ce sujet est une approche à la fois plus globale et complémentaire des travaux que j'ai menés sur la modélisation et la capitalisation des scénarios d'accidents. En effet, ce thème est l'une de mes préoccupations depuis 1989. D'abord dans le cadre de ma thèse de Doctorat en 1992 au LAMIH de l'université de valenciennes (en collaboration avec l'INRETS). Cette thèse a débouché sur la conception et la mise en oeuvre de la maquette du système « ACASYA » d'aide à la classification et à l'évaluation des scénarios d'accidents. Ensuite à l'unité de recherche ESTAS de l'INRETS en tant que chargé de recherche depuis janvier 1993 où j'ai participé à l'encadrement de la thèse de Lassaâd MEJRI (soutenue au LAMIH de l'UVHC en 1995) qui a porté sur le développement d'une approche d'aide à la génération des scénarios d'accidents. Les travaux d'acquisition des connaissances, conduits depuis huit ans dans le cadre d'une convention réunissant la Région Nord-Pas de Calais, le LAMIH-UVHC et l'INRETS-ESTAS, ont débouché principalement sur la constitution d'une base de 70 scénarios d'accidents [Hadj-Mabrouk 92, 97].

Cette base de scénarios est loin d'être représentative du domaine et nécessite, d'une part, d'être complétée par d'autres scénarios relatifs au problème de la collision et d'autre part, d'être étendues à plusieurs autres accidents potentiels (déraillement, électrocution…). De plus, malgré l'intérêt indéniable de cette base pour capitaliser, archiver et diffuser le savoir-faire en matière d'analyse de sécurité, il nous semble indispensable de la compléter par d'autres types de scénarios issus de la phase d'exploitation du système (retour d'expérience). Cette deuxième approche est complémentaire de celle réalisée jusqu'à présent dans le cadre de mes recherches car elle permet de tendre vers l'exhaustivité des analyses de sécurité d'un nouveau système. En effet, cette base issue du retour d'expérience permet non seulement de pérenniser les connaissances d'exploitation du système, mais aussi d'améliorer la sécurité de nouveaux systèmes de transport guidés par la prise en compte des nouvelles situations contraires à la sécurité éventuellement non prévues lors du développement d'un nouveau système. La sécurité ne peut malheureusement s'améliorer qu'après connaissance des accidents en phase d'exploitation. En outre, cette connaissance permet éventuellement d'améliorer l'aspect facteur humain : mettre en oeuvre la formation des opérateurs humains (OH), éviter certaines erreurs humaines d'exploitation, concevoir des systèmes tolérants aux erreurs éventuelles de l'OH, mieux préciser la contribution de l'OH dans un système, mieux organiser et structurer le retour d'expérience, comprendre l'OH en situation nominale et dégradée [Hadj-Mabrouk et al. 98].

5. JUSQU'OU L'AUTOMATISATION DE LA FONCTION DE CONDUITE POURRA -T- ELLE ETRE MENEE POUR LE RESEAU FERROVIAIRE ?

5.1. Contexte général de la recherche et collaboration scientifique

En septembre 1997, une collaboration avec l'Institut des Transports et de Planification de l'Ecole Polytechnique Fédérale de Lausanne (Professeur R-E. RIVIER, M. D. EMERY et M. J-D. BURI) a été amorcée en vue d'apporter un élément de réponse à la question suivante : jusqu'où l'automatisation de la fonction de conduite pourra-t-elle être menée pour le réseau ferroviaire européen classique ? Une étude a débuté afin d'identifier les différents modes de conduites impliqués dans les transports ferroviaires ainsi que les rôles successifs de l'opérateur humain et des automatismes en modes d'exploitation nominal et dégradé [Hadj-Mabrouk et Stuparu 97] et [Hadj-Mabrouk et al. 98]. Nous présentons ci-après les quelques réflexions préliminaires engagées dans le cadre de cette nouvelle recherche.

5.2. L'homme a-t-il encore sa place dans l'exploitation des transports guidés

À l'INRETS, le département ESTAS est chargé, pour le compte de la Direction des Transports Terrestres, d'une mission d'analyse de la sécurité des nouveaux systèmes de contrôle/commande mis en service en France, notamment dans les métros automatiques tels que le VAL, ou MAGGALY où l'homme continue à intervenir. Il intervient d'abord au niveau de la conception et de la réalisation des systèmes. En premier lieu, c'est à la recherche des erreurs pouvant survenir à ce stade qu'ESTAS travaille. Son rôle se situe également au niveau de l'exploitation : même dans les systèmes totalement automatiques, des opérateurs au poste de contrôle/commande (PCC) et des agents de conduite (ADC) demeurent. Ces derniers peuvent également jouer un rôle dans des situations dégradées, après une défaillance des automatismes par exemple [David et al., 94], [Hadj-Mabrouk, 96a]. Enfin, dans de nombreux systèmes non complètement automatisés, un conducteur cohabite en cabine de conduite avec des aides à la conduite de nature diverse. ESTAS est amené à prendre en compte la présence de ces opérateurs humains (OH) dans les analyses de sécurité.

Cependant, la tendance actuelle des exploitants est de ne plus accorder une confiance totale aux OH. En effet, ils sont considérés comme des composants faillibles, et l'on ne souhaite plus leur confier de tâches essentielles sans une protection par des équipements électroniques beaucoup plus fiables que l'être humain [David et al., 94], [Hadj-Mabrouk, 96b]. Cette démarche a été menée très loin, dans le cas des transports urbains à conduite automatique intégrale dans laquelle l'intervention de l'homme dans des processus mettant en jeu la sécurité a été minimisée. A un niveau moindre, la SNCF double actuellement la signalisation visuelle latérale sur une grande partie de son réseau par un système de protection par balises, le KVB [Auclair 91], [Hadj-Mabrouk 96c], qui a pour fonction d'arrêter le train automatiquement si un conducteur ne respecte pas une séquence d'arrêt. Cependant, on est encore loin d'un stade où les OH ne joueraient plus aucun rôle dans la sécurité des systèmes de transport terrestre, et où les risques ne découleraient plus que des erreurs se manifestant au niveau de la conception et de la réalisation des systèmes. En effet, la complexité et l'originalité de nouveaux systèmes de transport confèrent un rôle déterminant à l'OH dans la sécurité relative à la circulation des trains. Sa place doit être renforcée : il doit être assisté d'outils visant à l'aider dans ses tâches de conduite. La difficulté éprouvée par l'OH, lors de l'accomplissement d'une tâche, est d'autant plus importante que le système et l'interface Homme-Machine ne sont pas adaptés aux tâches dont il a la charge [Kolski 89, 93, 95], [Moussa 92] et [Tendjaoui 92].

Malgré l'avènement des automatismes, l'opérateur humain (OH) reste l'élément clef du système de transport et demeure indispensable. Parfois son action est la seule défense pour éviter qu'une panne initiale ne devienne un accident. L'OH est un élément paradoxal : en situation de stress ou de fatigue, il peut être un élément de la perte de la fiabilité d'un système. Cependant, dans certaines situations critiques, il peut être un élément de fiabilité, en rétablissant un processus, parfois par des actions non prévues par le règlement mais liées à une connaissance d'expert ; il rattrape alors des erreurs commises par le concepteur. Il faut donc optimiser la place de l'OH dans le système de transport en pleine connaissance de ses capacités mais aussi de ses limites. La sélection et la formation des hommes ne suffisent plus à obtenir la performance escomptée. Pour obtenir une performance mieux maîtrisée des systèmes de transport, il est nécessaire de concevoir des systèmes tolérants aux erreurs éventuelles de l'OH, de préciser la contribution de l'OH dans un système, de mieux organiser et structurer les retours d'expérience, d'analyser la charge de travail des OH [Millot 87]. Il convient également de développer des outils d'aide à la décision, de développer des systèmes dont les fonctionnalités procurent à l'OH flexibilité et adaptabilité, de comprendre l'OH en situation nominale et dégradée, de dégager des moyens pour améliorer la situation de travail afin de prévenir les conséquences négatives et favoriser les conséquences positives. En somme, il faut intégrer les facteurs humains dès la spécification des besoins et dès la conception du système et enfin de concevoir des systèmes qui s'adaptent à l'OH et non le contraire.

5.3. Principaux rôles de l'opérateur de conduite dans l'exploitation du système de transport

Dans le domaine de la sécurité des automatismes des systèmes de transport guidés, on distingue deux grands modes d'exploitation : modes nominaux et modes dégradés (figure 1). Les modes d'exploitation nominaux, comportent plusieurs modes de conduite [Hadj-Mabrouk et Stuparu 97] et [Hadj-Mabrouk et al. 98] : la conduite automatique intégrale sans l'opérateur de conduite, la conduite en pilotage automatique avec opérateur de conduite, la conduite manuelle contrôlée et la conduite manuelle libre avec opérateur de conduite. Les modes d'exploitation dégradés comportent principalement la conduite manuelle en marche à Vue, la conduite manuelle avec signalisation auxiliaire et la conduite manuelle de secours. Les modes d'exploitation dégradés peuvent assurer des fonctionnements comme l'accostage, le scindage ou les services provisoires.

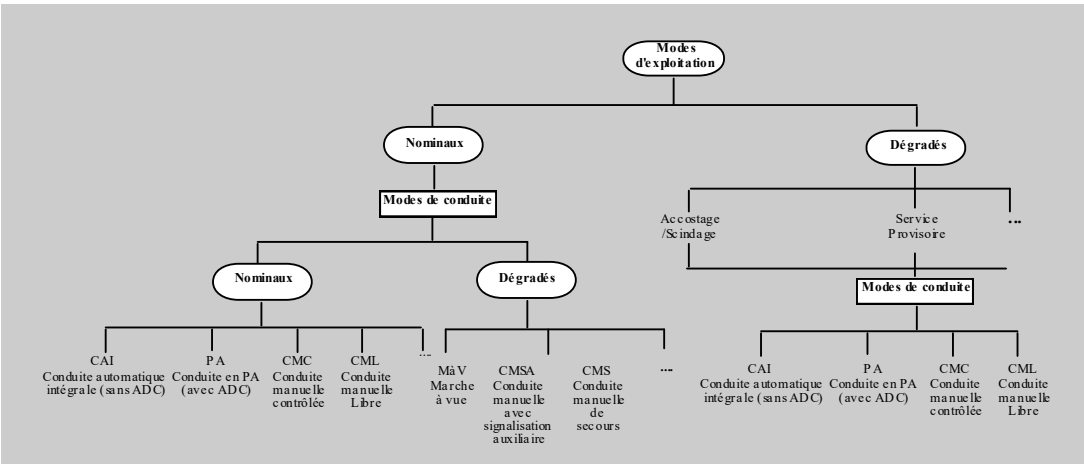

Figure 1 : exemple de classification des modes d'exploitation et de conduite [Hadj-Mabrouk et al. 98]

Conduite automatique intégrale. On parle de « conduite automatique intégrale » lorsqu'en mode d'exploitation nominal, on prévoit une conduite en pilotage automatique sans opérateur de conduite ni accompagnateur à bord.

Conduite en pilotage automatique avec opérateur de conduite. En pilotage automatique, les commandes d'accélération, de freinage et d'arrêt en station sont exécutées par le pilote automatique fonctionnel sous la surveillance des automatismes de sécurité nommés. Dans ce contexte, l'intervention de l'opérateur de conduite est limitée à quelques tâches : donner l'ordre de départ, commander la fermeture des portes, provoquer éventuellement l'arrêt d'urgence du train en cas d'incidents contraires à la sécurité, etc.

Conduite manuelle contrôlée. L'opérateur de conduite conduit le train en donnant les ordres de traction, de freinage, de commande des portes et de départ. Les automatismes de sécurité assurent la surveillance de la vitesse ainsi que le non-franchissement des signaux fermés.

Conduite manuelle libre. Les ordres de mouvement ou d'arrêt du train résultent à tout moment de l'action de l'opérateur de conduite. La conduite manuelle n'est considérée que sur ordre ou dans le cadre de consignes générales. Elle nécessite le respect des règles relatives au type de marche qui lui est associé.

Conduite en marche à vue. C'est une conduite en mode dégradé (ex : fonctionnement anormal de la signalisation) réalisée par l'opérateur de conduite. Dans le cadre de ce type de marche, l'opérateur de conduite est responsable de la marche de son train, il doit respecter les départs sur ordres ainsi que la signalisation. En effet, lorsque l'opérateur de conduite manoeuvre le commutateur de conduite pour le placer en position conduite manuelle, il devient responsable de la sécurité d'espacement de la rame. La vitesse de circulation est limitée à une valeur compatible avec la visibilité.

Conduite manuelle avec signalisation auxiliaire. Les ordres de déplacement du train résultent à tout moment de l'action de l'opérateur de conduite en respectant une signalisation latérale simplifiée. Elle nécessite le respect des règles relatives au type de marche qui lui est associé.

Le tableau de la figure 2 présente une classification des modes de conduite, en distinguant le rôle de l'opérateur de conduite, le rôle des automatismes de sécurité et enfin quelques exemples de systèmes de transport guidés [Hadj-Mabrouk et al. 98].

Mode de conduite nominal	Mode de conduite dégradé	Rôle de l'opérateur de conduite	Rôle des automatismes	Exemples de systèmes
Pilotage Automatique Intégral		Pas d'opérateur à bord des mobiles	- Conduire le train - Contrôler la vitesse - Commander le FU - Commander les portes	VAL, MAGGALY, METEOR, POMA 2000 de Laon.
Pilotage Automatique avec opérateur de conduite		L'opérateur de conduite commande les portes ainsi que le départ du train.	- Contrôler la vitesse - Commander le FU - Commander les portes	Métro de Paris, Métro de Lyon lignes A et B, Métro du Caire ligne 2
Conduite Manuelle Contrôlée		L'opérateur de conduite fournit les ordres de traction et de freinage, il commande les portes ainsi que le départ du train	Contrôler la vitesse ainsi que le non-franchissement des signaux fermés.	KVB, KVBP, KMT de la ligne C de Lyon, Métro du Caire ligne2
			Contrôler la vitesse, le non-franchissement des signaux fermés et l'affichage en cabine de la vitesse maximale autorisée	SACEM, TVM 300, TVM 430.
Conduite Manuelle Libre		Conduire le train, commander les portes ainsi que le départ du train	Pas d'automatisme de sécurité	Métro de Paris, Tramway ,Trains SNCF.
	Conduite en Marche à vue à vitesse restreinte	Il fournit les ordres de traction et de freinage, il commande les portes, le départ du train ainsi que le respect de l'espacement	Contrôler la vitesse limitée	Métro de Lyon lignes A et B, Métro du Caire ligne 2.
	Conduite Manuelle avec ~~Signalisation~~ Auxiliaire	Conduire le train, commander les portes ainsi que le départ du train en ~~respectant une sign~~alisation latérale simplifiée	L'automatisme de sécurité est totalement inactif	Métro de Lyon lignes A et B.
	Conduite Manuelle de Secours	Conduire le train, commander les portes, le départ et l'arrêt du train	L'automatisme de sécurité est totalement inactif	Métro de Lyon lignes A et B.

Figure 2 : principaux rôles de l'opérateur de conduite relatifs aux modes d'exploitation [Hadj-Mabrouk et al. 98]

BIBIOGRAPHIE

[AFNOR 93] : Norme FD Z 68-002, Automatisation industrielle - Ergonomie et facteurs humains - en technique de fabrication avancée (TFA), Octobre 1993.

[AFNOR 95] : Norme NF EN 614-1, réf.: X 35-004-1, Sécurité des machines - Principes ergonomiques de conception - Partie 1 : terminologie et principes généraux, Avril 1995,.

[Amalberti et Mosneron-Dupin 97] : Amalberti R., Mosneron-Dupin F. « Facteurs humains et fiabilité. Quelles démarches pratiques ? ». *Octarès Éditions*, 1997, 136p.

[Arnaud 95] : Arnaud. "Etude ergonomique d'un prototype de système d'aide à la manutention des sacs messagerie ». *Rapport de stage RA 4338*, La Poste, 25 juillet 1995.

[Auclair 91] : Auclair. « Sécurité de la conduite. Le contrôle de vitesse ». *Colloque Sécurité dans les transports*. PARIS 10 déc. 1991.

[BCEOM 74] : « La sécurité dans les Transports collectifs ». Étude BCEOM, 1974.

[Blatter 96] : Blatter. « Cours sur l'intervention ergonomique dans un projet » - DESS d'Ergonomie de Paris V.

[CEI 94] : Commission Électrotechnique Internationale (CEI). «Analyse de risques des systèmes technologiques - Guide d'application ». Projet de comité CEI 56 (sec) 410, Genève, 1994.

[CENE 94b] : Comité Européen de Normalisation Électrotechnique (Cenelec). « Spécification et preuve de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) pour les applications ferroviaires ». Version 00.06, Projet de norme prEN 50126, Bruxelles, 1994.

[Chollet et al. 92] : Chollet, Gaufreteau, Joing. « Analyse de la sécurité des procédures". *8ème Colloque de fiabilité et de maintenabilité*, 6-8 octobre.

[Daniellou 87] : Daniellou. « Les modalités d'une ergonomie de conception : introduction dans la conduite des projets industriels". *Cahier de note documentaire* n° 129, 4e trimestre 1987.

[Daniellou 88] : Daniellou. « Ergonomie et démarche de conception dans les industries de processus continus, quelques étapes clés » - *Le travail humain*, Tome 51 n°2, 1998.

[Daniellou 92] : Daniellou. « Le statut de la pratique et des connaissances dans l'intégration ergonomique de conception » - *Thèse d'habilitation à diriger des recherches*, Université de Toulouse Le Mirail, juin 1992.

[Daniellou et Garrigou 92] : Daniellou, Garrigou. « L'utilisation des représentations des situations passées et des situations futures dans la participation des opérateurs à la conception » - In Dubois, Rabardel, Weil-Fassina, Représentation par l'action.

[David et al. 94] : David Y., Le Trung B., Hadj-Mabrouk H. « L'erreur humaine dans les systèmes de transport guidés ». *Journée spécialisée INRETS - L'erreur humaine : question de points de vue ?* Centre Reille, Paris 17 novembre 1994, 10p.

[De Montmollin 95] : De Montmollin. « Vocabulaire de l'ergonomie » - *Éditions Octarès*, 1995.

[DGA 94] : « Guide pour la prise en compte du facteur humain et de l'ergonomie dans les programmes d'armement ». DGA Mission assurance de la qualité, Ministère de la Défense, 1995.

[Dien et Lagrange 95] : Dien, Lagrange. « Une démarche d'ergonomie de conception pour définir la coopération homme/machine : des propositions pour une conception centrée opérateurs ». EDF-DER-ESF HT54/95/007A, avril 1995.

[Fadier 94] : Fadier. « L'état de l'art dans le domaine de la fiabilité humaine ». *Éditions Octarès*, 1994.

[Fadier et Neboit 96] : Fadier, Neboit. « Proposition d'une méthode d'analyse de la fiabilité opérationnelle intégrant l'analyse ergonomique ». *Actes du 11ème colloque national de Fiabilité et Maintenabilité,* Tome 1, 1-3 octobre 1996, St Malo.

[Flages et Churchill 94] : Flages M. Churchill G. « La quantification des métiers de sécurité à la RATP par le retour d'expérience ». *9e Colloque national de fiabilité et maintenabilité*, France, La Baule, 30 mai -3 juin 1994.

[Garrigou 92] : Garrigou. « Les apports des confrontations d'orientations socio-cognitives au sein de processus de conception participatifs : le rôle de l'ergonomie ». *Thèse de doctorat d'ergonomie* - Conservatoire National des Arts et Métiers, 14 octobre 1992.

[Gonin 95] : Gonin P. « 50 millions de consommateurs », n° 282, 1995.

[Hadj-Mabrouk et al. 93] : Hadj-Mabrouk H., Le Trung B., Bied-Charreton D. « Rôle de l'INRETS-CRESTA dans le processus de développement et d'exploitation d'un système de transport guidé ». INRETS-CRESTA, CR/A-93-54, Édition provisoire, Arcueil, Août 1993.

[Hadj-Mabrouk 94] : Hadj-Mabrouk H. « Examen du dossier Analyse Préliminaire des Risques (APR) du système KVBP/KVIM ». *Convention INRETS/DTT,* Rapport INRETS-ESTAS n° CR/A-94-64, Arcueil, 2 Décembre 1994, 35p. *(confidentiel).*

[Hadj-Mabrouk et Bied-Charreton 94a] : Hadj-Mabrouk H., Bied-Charreton D. « Évaluation des méthodes de développement, de validation et d'homologation du système ANTARES de signalisation, de contrôle de vitesse et d'aide à la conduite du RER-Ligne C-Paris. Étape 1 : Identification du problème ». *Convention INRETS/DTT,* Rapport INRETS n° CR/A-94-01, 3ème Édition, Arcueil, Avril 1994, 91p. *(confidentiel).*

[Hadj-Mabrouk et Bied-Charreton 94b] : Hadj-Mabrouk H., Bied-Charreton D. « Évaluation des méthodes de développement, de validation et d'homologation du système ANTARES de signalisation, de contrôle de vitesse et d'aide à la conduite du RER-Ligne C-Paris. Étape 2.1. : Macro analyse au niveau système ». *Convention INRETS/DTT*, Rapport INRETS n° CR/A-94-10, Arcueil, Mai 1994, 79p. *(confidentiel).*

[Hadj-Mabrouk et Bied-Charreton 94c] : Hadj-Mabrouk H., Bied-Charreton D. « Examen des documents généraux (PDP, PSP) et de définitions (SBU, DSE) du système KVBP/KVIM du projet ANTARES. Bilan des remarques et questions ». *Convention INRETS/DTT*, Rapport INRETS n° CR/A-94-15, 2ème Édition, Arcueil, 11 Mars 1994, 25p. *(confidentiel).*

[Hadj-Mabrouk 95] : Hadj-Mabrouk H. « Le besoin d'introduire les facteurs humains dans le développement et l'analyse de sécurité des systèmes de transport guidés ». *Convention INRETS/DTT,* Rapport ESTAS/A-95-30, Arcueil, juillet 1995, 55 p.

[Hadj-Mabrouk et Tabka 96] : Hadj-Mabrouk H., Tabka J. « Projet VALIDE : méthode d'évaluation de la sécurité des transports guidés. Étape n° 1 : identification du problème ». *Convention INRETS/LIMAV*, rapport n° ESTAS/A-96-61, diffusion restreinte, INRETS, Arcueil, mai 1996.

[Hadj-Mabrouk 96a] : Hadj-Mabrouk H. « La nécessité de prendre en compte l'erreur humaine dans l'analyse de sécurité et le développement des systèmes de transport guidés ». *OCTARES Éditions*, collection colloques, l'erreur humaine : question de points de vue ? France, pp 85-98, 1996.

[Hadj-Mabrouk 96b] : Hadj-Mabrouk H.« Projet FACTHUS : prise en compte des facteurs humains dans le développement des projets industriels ». *Convention INRETS/DTT*, rapport n° ESTAS/A-96-65, diffusion restreinte, 73 p, Arcueil, décembre 1996.

[Hadj-Mabrouk 96c] : Hadj-Mabrouk H. « Exemples de systèmes de contrôle de vitesse dans les transports terrestres : principes de fonctionnement ». Etude bibliographique, rapport INRETS n° ESTAS/A-96-01, 16 p, Arcueil, janvier 1996.

[Hadj-Mabrouk et Stuparu 97] : Hadj-Mabrouk H., Stuparu A. « Exemple de typologie d'accidents dans le domaine de la sécurité des systèmes de transport guidés ». *Rapport INRETS n° ESTAS/A-97-47*, 18p, Arcueil, août 1997.

[Hadj-Mabrouk 97] : Hadj-Mabrouk H. « L'acquisition des connaissances pour l'élaboration d'une base de scénarios d'accidents ». *Lettre de la sûreté de fonctionnement*, n° 50, Édition EC2 & Développement, Paris, septembre 1997, pp 3-16.

[Hadj-Mabrouk et al. 98] : Hadj-Mabrouk H., Stuparu A., Bied-Charreton D. « Exemple de typologie d'accidents dans le domaine des transports guidés ». *Revue Générale des Chemins de Fer*, ÉDditions Dunod, Paris, mars 1998 (A paraître).

[Hadj-Mabrouk et Stuparu, 98] : Hadj-Mabrouk H., Stuparu A. « What is the human driver's place in the automatic guided transportation ? ». Comprail 98*, Sixth Intrnational Conference on Computer Aided Design, Manufacture and Operation in the Railway and other advanced Mass Transit Systems*, Lisbon, Portugal, 2-4 September 1998 (proposition).

[HSE 90] : « Railway Safety ». Report on the safety record of the railways in Great Britain during HSE. London, 1990.

[Joing et Cozzi 93] : Joing M., Cozzi B. « Gestion des risques à la SNCF *». Revue Générale des Chemins de Fer*, mai 1993.

[Joing et Keravel 93] : Joing M., Keravel. « Retour d'expérience et analyse du facteur humain » - *Revue générale des chemins de fer*, n°6, juin 1993.

[Jost 96] : Jost P. « La démarche sociotechnique, démarche de fiabilisation des systèmes ». lm10, *10e Colloque national de fiabilité et maintenabilité*, France, Saint-Malo, 1-3 octobre 1996.

[Kautzmann 96a] : Kautzmann J. « Exemples d'intégration des facteurs humains dans le développement des projets industriels ». *Mémoire de stage de D.E.S.S. d'Ergonomie* de l'institut de psychologie de l'université de ParisV. INRETS, Arcueil, juillet 1996, 59 p.

[Kautzmann 96b] : Kautzmann J. « Apports et limites des méthodes de prise en compte des facteurs humains au domaine des systèmes de transport guidés ». *Mémoire de stage de fin d'études d'ingénieur* de l'institut polytechnique de Sevenans. INRETS, Arcueil, octobre 1996.

[Kautzmann et Hadj-Mabrouk 96a] : Kautzmann J., Hadj-Mabrouk H. « Étude bibliographique sur la prise en compte des facteurs humains ». *Convention INRETS/COSINUS*, rapport n° ESTAS/A-96-35, diffusion restreinte, 23 p, Arcueil, juin 1996.

[Kautzmann et Hadj-Mabrouk 96b] : Kautzmann J., Hadj-Mabrouk H.« Exemples de prise en compte des facteurs humains à la SNCF et à EDF ». *Convention INRETS/COSINUS*, rapport n° ESTAS/A-96-50, diffusion restreinte, 17 p, Arcueil, août 1996.

[Keravel 95] : Keravel F. « Intégration des facteurs humains à la conception des systèmes électroniques ». *Journées CEA/ETI/DEIN*, 7-9 février 1995, Saclay, France.

[Kolski 89] : Kolski C. « Contribution à l'ergonomie de conception des interfaces graphiques Homme-Machine dans les procédés industriels : application au système expert SYNOP ». *Thèse de Doctorat*, Université de Valenciennes, Janvier 1989.

[Kolski 93] : Kolski C. « Ingénierie des interfaces homme-machine, conception et évaluation ». *Éditions Hermès*, Paris, août 1993, 372p.

[Kolski 95] : Kolski C. « Méthodes et modèles de conception et d'évaluation des interfaces homme/machine ». *Thèse d'habilitation à diriger des recherches*, , Université de Valenciennes et du Hainaut Cambrésis, janvier 1995.

[Lancien et al. 94] : Lancien, Raimond, Bernard, Loncle. « Facteurs Humains et transport ferroviaire, application aux programmes de recherches : cas du projet ASTREE ». *Actes du congrès mondial de la recherche ferroviaire* (WCRR'94), Volume 2, Paris, 14 - 16 novembre 1994.

[Leplat 85] : Leplat. « Erreur humaine, Fiabilité humaine dans le travail ».*Armand Colin*, 1985.

[Leplat et De Terssac 90] : Leplat, De Terssac. « Les facteurs humains de la fiabilité dans les systèmes complexes ». *Editions Octarès*, 1990.

[Macaire 94] : Macaire. « La mise en oeuvre et le maintien de la fiabilité humaine du personnel de sécurité à la SNCF ». *Actes du congrès mondial de la recherche ferroviaire (WCRR'94),* Paris, 14 - 16 novembre 1994.

[Mazeau et Christol 94] : Mazeau, Christol. « Retour d'expérience, l'approche statistique et l'approche clinique». *Performances techniques & humaines*, n°69, mars - avril 1994.

[Millot 87] : Millot P. « Coopération Homme-Machine dans les tâches de supervision des procédés automatisés ». *Thèse de Docteur ès Sciences*, Université de Valenciennes, Septembre 1987.

[Moussa 92] : Moussa F. « Contribution à la conception ergonomique des interfaces de supervision dans les procédés industriels : application au système ERGO-CONCEPTEUR ». *Thèse de Doctorat*, Université de Valenciennes, Juillet 1992.

[Neboit et al 90] : Neboit, Guillermain, Fadier. « De l'analyse du système à l'analyse de l'interaction opérateur/tâche : proposition méthodologique ». - in Les facteurs humains de la fiabilité, Octarès.

[Nicolet et al 89] : Nicolet, Carino, Wanner. « Catastrophe ? Non merci ! ». La prévention des risques technologiques et humains - Collection Le Nouvel Ordre Economique, *édition Masson*, 1989.

[Reason 90] : Reason. « L'erreur humaine » - *Presses Universitaires de France*, 1990.

[SNCF 94] : « Rapport sur la sécurité des circulations en 1993 ». Juin 1994.

[Sperandio 88] : Sperandio. « L'ergonomie du travail mental ». *Editions Masson*, 1988.

[Sperandio 93] : Sperandio. « L'ergonomie dans la conception des projets informatiques ». *Editions Octarès*, 1993.

[Suchet 92] : Suchet. « Le facteur humain dans la préparation d'un vol spatial habité ». *8e colloque de fiabilité et de maintenabilité*, 6-8 octobre, 1992.

[Telle et Vanderhaegen 96] : Telle B., Vanderhaegen F. « Analyse de terrain. Rapport descriptif sur l'analyse fonctionnelle d'un système ferroviaire ». *Rapport de convention LAMIH/INRETS*, Université de Valenciennes, 31 juillet 1996.

[Tendjaoui 92] : Tendjaoui M. « Contribution à la conception d'interface intelligente pour le contrôle de procédés industriels : application au module décisionnel d'imagerie ». *Thèse de Doctorat*, Université de Valenciennes, novembre 1992.

[THE 93] : « The 1991-92 Railway Safety report ». Modera Railways. May 1993.

[Vignes 95] : Vigne. « Les activités liées à la mission sociotechnique, démarche de fiabilisation des systèmes ». Service d'ergonomie et facteur humain de la SNCF, 1995.

[Villemeur 88] : Villemeur « Sûreté de Fonctionnement des Systèmes industriels » - Collection de la Direction des Études et de Recherches d'EDF, Paris, *Editions Eyrolles*, 1988.

CONCLUSION GENERALE

Ce mémoire a présenté notre contribution à l'amélioration des méthodes usuelles d'analyse et d'évaluation de la sécurité employées dans le cadre de la certification des automatismes des systèmes de transport terrestre guidés. Cette contribution, basée sur l'utilisation des techniques d'intelligence artificielle, s'est concrétisée par l'élaboration de plusieurs approches et outils d'aide à la modélisation, à la capitalisation et à l'évaluation des connaissances de sécurité. Les outils logiciels développés ont deux principales vocations : d'une part archiver et pérenniser l'expérience en matière d'analyse de sécurité et d'autre part aider les acteurs impliqués dans le développement et la certification des systèmes de transport, dans leurs tâche difficile d'évaluation des études de sécurité.

A ce jour, ces outils sont au stade de maquettes dont la première validation montre l'intérêt des approches proposées. Ils requièrent certaines améliorations et extensions afin de pouvoir être non seulement exploitables en milieu industriel, mais aussi adaptables à d'autres domaines où le problème d'examen de la sécurité se pose.

L'ensemble des travaux effectués dans le cadre de l'analyse de la sécurité et de la certification des systèmes de transport montre qu'il faut également prendre en compte la composante humaine dans les analyses afin d'optimiser le processus de mise en sécurité d'un système de transport.

A mon sens, la principale innovation qui doit être mise en avant concerne l'introduction des facteurs humains et des techniques d'intelligence artificielle dans l'aide à la certification des systèmes et logiciels de sécurité. C'est là le point central qui demeure tout à fait original car il a permis de renouveler l'approche classique des questions d'évaluation des études de sécurité et de certification des systèmes et des logiciels critiques.