

Analyse de la sécurité et facteurs humains dans les transports ferroviaires

Habib Hadj-Mabrouk

▶ **To cite this version:**

Habib Hadj-Mabrouk. Analyse de la sécurité et facteurs humains dans les transports ferroviaires. 42e Congrès annuel de l'Association Québécoise du Transports et des Routes (AQTR'2007), Apr 2007, Québec, Canada. pp.1-14. hal-03244690

HAL Id: hal-03244690
https://hal.science/hal-03244690

Submitted on 1 Jun 2021

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

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

Analyse de la sécurité et Facteurs Humains dans les transports ferroviaires

Dr. HADJ-MABROUK Habib

INRETS
2 avenue du Général Malleret-Joinville
94114 Arcueil – France
Téléphone : + 33 1 47 40 73 52
Courriel : mabrouk@inrets.fr

RÉSUMÉ

La recherche a pour ambition d'améliorer les tâches d'élaboration et d'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 :

- 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 et de traçabilité ;

- 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.

L'objectif de l'étude est triple :

1. Faciliter les missions d'expertise et d'assistance technique confiées à l'INRETS par l'État ;

2. Aider les acteurs impliqués dans le développement des systèmes de transport et notamment les organismes de certification dans leur tâche cruciale d'évaluation des études de sécurité ;

3. 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.

Cet article détaille l'intérêt et l'apport des techniques d'intelligence artificielle au domaine de la sécurité des systèmes de transports ferroviaires. Il montre également qu'il faut prendre en compte la composante humaine dans les analyses afin d'améliorer sensiblement le niveau de sécurité. Notre contribution, qui s'inscrit dans le cadre du projet " FACTHUS ", vise l'intégration des facteurs humains dans les analyses de la sécurité et plus particulièrement dans le processus du retour d'expérience.

1. Principales missions d'assistance technique et d'expertise confiées à l'INRETS-ESTAS

L'évaluation de la conception et de la réalisation d'un nouveau système ainsi que la vérification de ses capacités au regard de l'objectif de sécurité, et du maintien dans le temps de ces capacités, sont assurés par un organisme ou service technique indépendant (OSTI). Cet organisme vérifie notamment que la conception et la réalisation d'un système sont effectuées conformément aux règlements en vigueur et aux règles de l'art qui sont généralement spécifiées dans un dossier préliminaire de sécurité. Ce dernier expose les objectifs et exigences de sécurité poursuivis, les méthodes et techniques mises en œuvre pour atteindre ces objectifs ainsi que la démonstration et la preuve que ces objectifs ont été atteints. Dans ce contexte, 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. Elle 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'État et/ou les organismes ou service technique indépendant (comme CERTIFER) à fonder une appréciation sur le respect des exigences de sécurité portent notamment sur [Hadj-Mabrouk 95] :

- L'adéquation, la complétude, la cohérence et la traçabilité des méthodes et techniques utilisées par le maître d'œuvre pour construire la sécurité (au niveau système, logiciels et matériels) ;
- La bonne application des principales normes et textes législatifs et réglementaires suivies lors de la réalisation du projet ;
- 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 ;
- L'acceptabilité des objectifs de sécurité recherchés par le maître d'ouvrage ;
- Etc.

Nos travaux de recherche s'inscrivent dans le cadre de la phase d'évaluation de la complétude et de la cohérence des méthodes de *construction de la sécurité*.

2. Processus de construction de la sécurité d'un système de transport ferroviaire

Généralement, le processus de construction de la sécurité d'un système (figure 1) comporte plusieurs analyses complémentaires hiérarchisées : L'analyse préliminaire de risques, l'analyse fonctionnelle de la sécurité, et l'analyse de la sécurité du produit réalisé [Hadj-Mabrouk 98].

- 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.

- 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 [Hadj-Mabrouk 95, 98] :

  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] 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 œuvre d'un processus de construction de la sécurité itératif faisant intervenir à la fois des méthodes inductives et déductives.

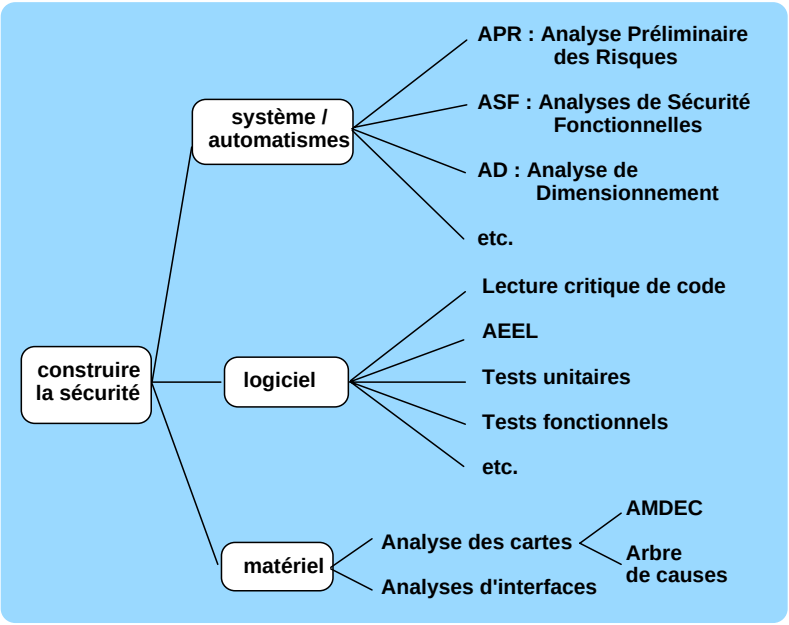


Figure 1 : processus de construction de la sécurité d'un système de transport guidé [Hadj-Mabrouk 95]

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 par la recherche des risques et scénarios contraires à la sécurité non pris en compte lors de l'élaboration du dossier de sécurité. En effet, 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.

3. Motivations et objectif de la recherche

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 96] :

- 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 ;
- 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 ;
- 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, nous avons défini un axe de recherche baptisé " AVIS " (Acquisition et Validation des connaissances de Sécurité).

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 96, 98] :

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.

L'objectif de cet axe de recherche est triple [Hadj-Mabrouk 98] :

1. 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 ;
2. 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 ;
3. 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.

4. Principales composantes de l'axe de recherche « AVIS »

L'axe de recherche " AVIS " est composé de six projets complémentaires illustrés à la figure 2 [Hadj-Mabrouk 96, 98] :

1. SAPRISTI : système expert d'aide 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, basé sur des techniques d'apprentissage automatique ;
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 (AMDEC) des équipements matériels ;
5. SPECIALS : méthode de spécification et d'aide à l'évaluation des logiciels critiques de sécurité basée sur l'utilisation des graphes conceptuels de SOWA ;
6. FACTHUS : Méthode d'intégration des facteurs humains dans les analyses de sécurité.

Conformément au processus de construction de la sécurité, ces projets visent l'amélioration des méthodes conventionnelles d'élaboration et d'évaluation de la sécurité au niveau système, matériel et logiciel. L'on remarque dans la figure 2 l'introduction dans ce processus d'un autre niveau d'analyse essentiel pour améliorer la sécurité du système : le niveau humain. Cette composante liée aux facteurs humains n'est pas encore prise en compte de façon formelle et systématique par les entreprises ferroviaires et le gestionnaire d'infrastructure.

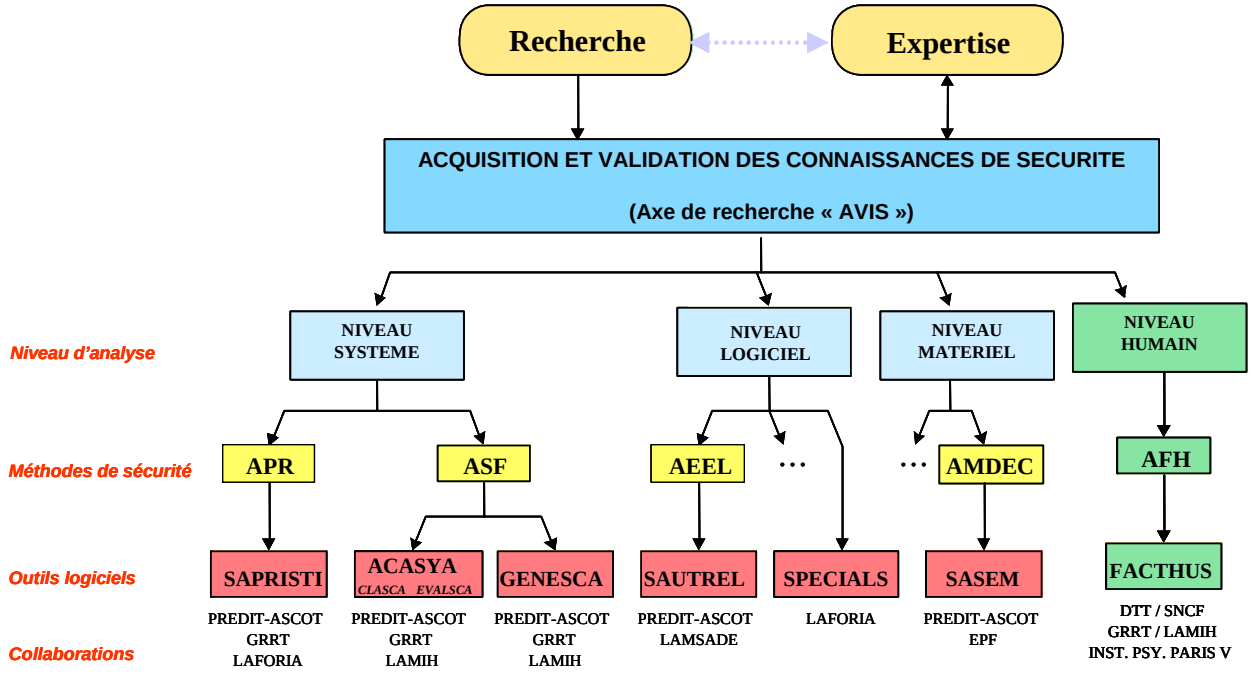


Figure 2 : composantes de l'axe de recherche AVIS [Hadj-Mabrouk 96, 98]

5. Méthodes et techniques mises en œuvre pour développer l'axe de recherche « 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. 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 92, 98]. 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 comme une solution très prometteuse.

En effet, 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 [Kodratoff, 1986], [Ganascia 1987] 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'approche retenue pour développer l'ensemble des outils d'aide à l'analyse de la sécurité implique deux grandes activités [Hadj-Mabrouk 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.

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 3.

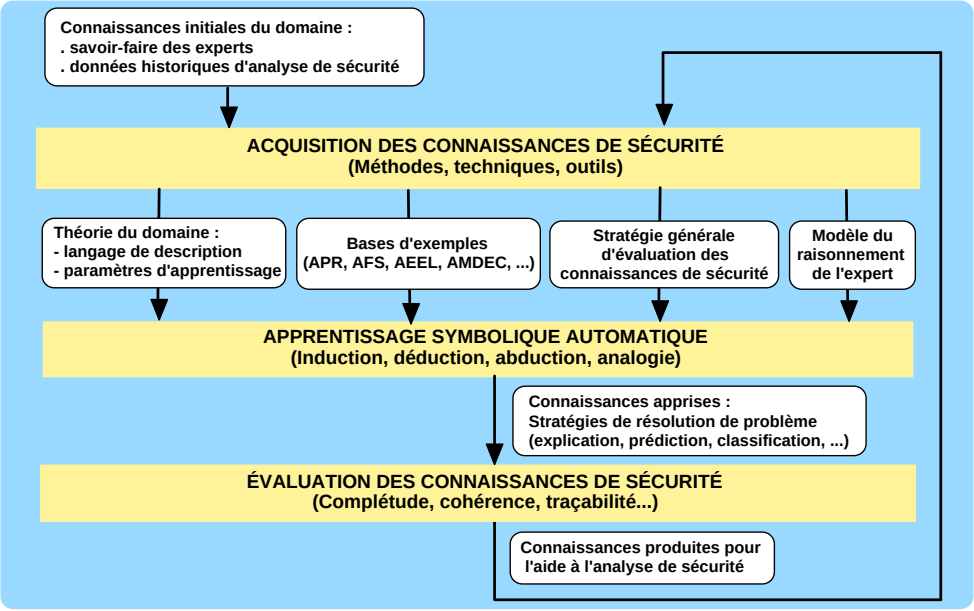


Figure 3 : Processus d'acquisition et d'évaluation des connaissances de sécurité [Hadj-Mabrouk 92, 98]

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.

À 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. 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.

La suite de cet article est consacré à l'analyse de la sécurité au niveau **humain**. Ce niveau d'analyse est relatif au projet " FACTHUS " qui vise l'intégration des facteurs humains non seulement au niveau des analyses de sécurité (APR, ASF, …) mais aussi au niveau des activités de développement du système (spécification, conception, …).

6. Projet " FACTHUS " : Prise en compte des facteurs humains dans la sécurité des transports

Avec l'amélioration de la fiabilité technique, la tendance actuelle est d'attribuer les dysfonctionnements des systèmes, générateurs d'accidents, à une erreur de l'opérateur humain. L'opérateur est considéré comme point faible du système et limiteur de performance et de sécurité. Ainsi, l'erreur humaine constitue un facteur causal majeur de l'émergence des accidents dans plusieurs secteurs de sécurité dont celui des transports ferroviaires. Cependant, les concepteurs de systèmes techniques ont souvent tendance à penser l'opérateur humain comme le maillon faible de ces systèmes. Cette vision conduit, sinon à l'exclusion de l'opérateur humain, au moins à une restriction de ses marges de manœuvre, par des contraintes procédurales ou par une automatisation poussée. Nos travaux de recherche s'écartent clairement de cette perspective : l'opérateur y est considéré sur ces deux aspects, facteur d'infiabilité mais également de fiabilité [Hadj-Mabrouk 04]. La survenue de nouveaux accidents malgré la maîtrise du risque technologique est à la base de l'intérêt renouvelé à l'étude des facteurs humains dans l'analyse de la sécurité.

6.1. Objectif du Projet " FACTHUS "

L'étude 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 mais aussi au niveau des activités de développement du système. 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 principaux acteurs suivants [Hadj-Mabrouk 00, 04] et [Hadj-Mabrouk et Triki 03] : Le Réseau Ferré de France (RFF), lors de l'élaboration du dossier de définition (ou d'initialisation) du système et du règlement de sécurité de l'exploitation ; La SNCF, lors de l'établissement du dossier préliminaire de sécurité, du dossier de sécurité et du dossier d'homologation ; Le constructeur (maître d'œuvre), lors du développement et de la validation de son système ; L'organisme ou service technique compétent et indépendant (ex : CERTIFER), lors de l'élaboration du rapport de certification (ou d'évaluation) ; Le Ministre chargé des transports, lors de l'approbation du dossier de définition du projet, du dossier préliminaire de sécurité, de l'autorisation de mise en service du système et de son suivi en exploitation.

6.2. Démarche poursuivie

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 ; 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 ; de proposer une approche de classification d'erreurs humaines potentielles provoquées par le personnel d'exploitation (Opérateur au PCC et Agent de conduite ADC) ; de réaliser une étude bibliographique sur la prise en compte des facteurs humains et de l'ergonomie dans plusieurs secteurs : armement (DGA), nucléaire (EDF), spatial (CNES), transports (SNCF, RATP), etc.

Cette étude a été complétée par l'analyse de treize méthodes dédiées principalement à la classification et à la quantification de l'erreur humaine : l'approche de Reason, l'approche de Norman, l'approche de Nicolet, le modèle de Rasmussen, les méthodes EPFH, HEART, SHERPA, SLIM, TESEO, THERP, MAFERGO. Malgré l'intérêt indéniable des méthodes étudiées, leur mise en œuvre dans le domaine de la sécurité des systèmes de transport guidés n'est pas suffisante. Aucune méthode, à elle seule, ne permet d'assurer l'exhaustivité de l'analyse. En effet, il est nécessaire de recouper les résultats obtenus par une méthode avec ceux qui sont obtenus par d'autres complémentaires. On mesure alors tout l'avantage de disposer d'une méthode de prise en compte des facteurs humains, dans le développement et l'analyse de sécurité d'un système, commune à tous les constructeurs et exploitants des transports ferroviaires [Hadj-Mabrouk 01, 04].

6.3. Approche retenue

L'approche que nous proposons est inspirée des travaux de Reason qui évoque trois niveaux de classification des erreurs humaines (comportemental, contextuel et conceptuel) correspondant à trois questions que l'on peut se poser sur les erreurs humaines (quoi ? où ? comment ?). Elle est également inspirée des travaux de Rasmussen (80, 82, 86, 87, 90) relatifs au fonctionnement cognitif de l'homme et de Van Eslande (97, 00, 01) relatifs aux scénarios types d'accidents. Centrée sur le déroulement d'un accident potentiel et appuyée par quelques exemples issus du domaine de la sécurité ferroviaire, cette méthode s'articule autour de trois niveaux complémentaires d'analyse de l'erreur humaine et reprend les trois niveaux suggérés par Reason : le niveau contextuel (en amont de l'accident), le niveau conceptuel cognitif (pendant l'accident), et le niveau comportemental (en aval de l'accident).

En pratique, l'analyse de l'accident passe d'abord par l'étude globale de l'environnement et de la situation du travail des opérateurs (en amont de l'accident) et répond ainsi aux questions où ? quand ? et qui ? (type d'opérateur impliqué). La seconde étape d'analyse consiste à étudier la démarche cognitive mise en œuvre face à une situation donnée et répond ainsi à la question comment ? (pendant l'accident). Cette démarche débouche souvent sur une action en termes d'accomplissement d'une tâche. La dernière phase (en aval de l'accident) étudie les conséquences d'une action erronée en termes de dommage sur l'homme, sur l'environnement et sur le système et répond ainsi à la question quoi ?

6.4. Résultats obtenus

La méthode retenue (figure 4) pour analyser l'erreur humaine notamment dans le processus du Retour d'expérience est centrée sur le déroulement d'un Accident/Incident. Elle fait intervenir trois niveaux d'analyse complémentaire (Hadj-Mabrouk 2004 et 2005) :

- En amont de l'accident (niveau contextuel) afin d'étudier les différents facteurs favorisant la production de l'erreur humaine à l'origine de l'accident ;
- Pendant l'accident (niveau cognitif conceptuel) qui vise à identifier les erreurs humaines relatives au processus cognitif humain mis en jeu face à une situation d'insécurité donnée ;
- En aval de l'accident (niveau comportemental) qui s'attache à évaluer les conséquences d'une action erronée en termes de dommage sur l'homme, sur l'environnement et sur le système.

Ainsi, à travers les deux premières étapes de l'approche proposée, on peut identifier les différentes erreurs humaines potentielles ainsi que leurs éventuelles interactions.

C'est pour cette raison que l'approche proposée sera focalisée uniquement sur les deux premières phases d'analyse afin de déterminer les différents facteurs impliqués dans la production des erreurs humaines potentielles à l'origine de l'accident. L'objectif est de prendre en compte l'ensemble de ces facteurs dans la phase de collecte de données après accident ou incident ferroviaire.

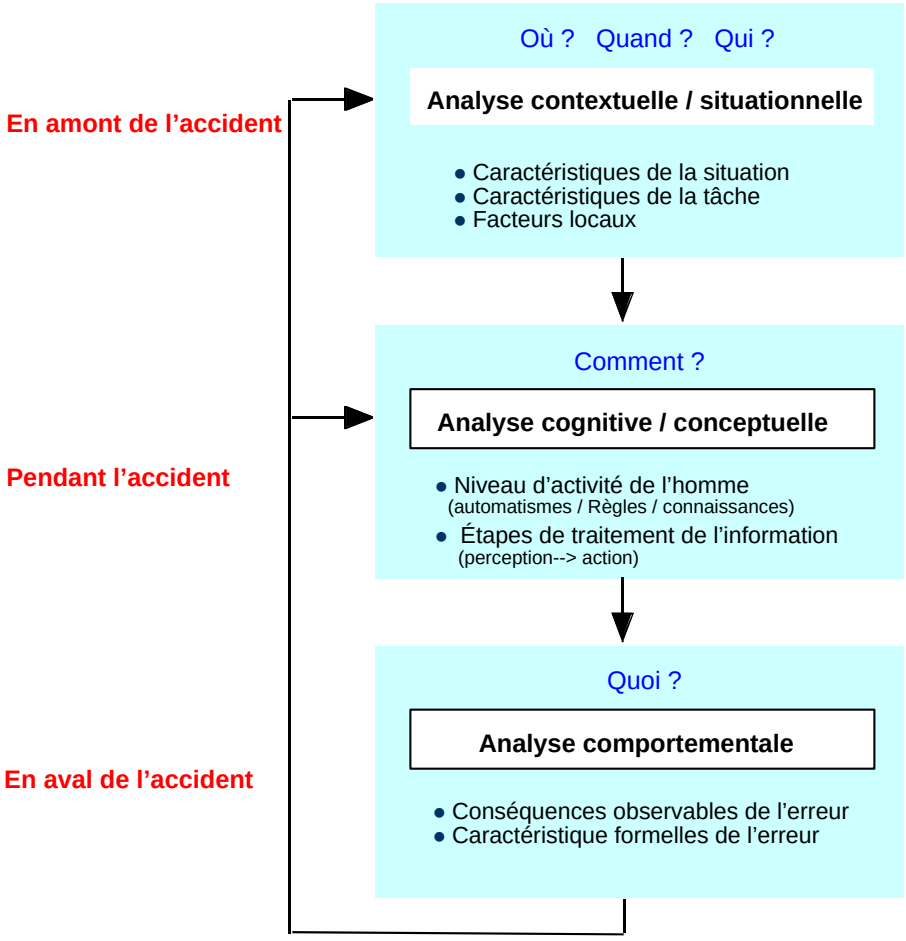


Figure 4 : Approche d'intégration des facteurs humains dans l'analyse des scénarios d'accidents (Hadj-Mabrouk 04)

6.4.1. En amont de l'accident (Analyse contextuelle)

L'analyse contextuelle de l'erreur humaine, en amont de l'accident, consiste à étudier les différentes conditions de travail (caractéristiques de la situation, caractéristiques de la tâche, …) favorisant sa production. Considérant l'opérateur humain dans son environnement de travail et face au système, ce premier niveau d'analyse permet de déterminer les facteurs locaux déclenchant l'erreur ainsi que les interactions entre les circonstances internes et externes. Le but de cette phase consiste à identifier les différentes interactions que subit l'homme avec son environnement du travail, avec les autres opérateurs et avec le système. Ce niveau d'analyse nécessite donc l'étude des trois principales composantes d'un système socio-technique (Homme, Système, Environnement) ainsi que leurs interactions.

Dans un premier temps, il s'agit d'identifier les différents types d'opérateurs impliqués ainsi que les facteurs altérants la performance humaine. Les opérateurs humains impliqués dans le secteur des transports sont variables en fonction du domaine. Dans le domaine ferroviaire, par exemple, les acteurs sont principalement le personnel de maintenance et le personnel d'exploitation. Les erreurs humaines d'exploitation concernent notamment l'opérateur au PCC et l'agent de conduite.

Les erreurs potentielles de l'opérateur au PCC sont souvent relatives au non-respect des procédures, d'accostage, d'initialisation, d'évacuation ou de conduite. Les erreurs potentielles de l'opérateur de conduite se répartissent généralement en deux grandes classes : le non-respect de la signalisation (franchissement de signal d'arrêt, non-respect des feux) et l'erreur de commande ou de manœuvre (freinage intempestif ou brusque, non-respect de la consigne de vitesse, ouverture prématurée ou intempestive des portes, etc) (Hadj Mabrouk et al. 2001).

Dans le cadre de cette première analyse contextuelle et situationnelle de l'erreur humaine, il est également nécessaire d'identifier les principaux facteurs altérants la performance humaine. Ces facteurs peuvent, en effet, influencer de façon directe ou indirecte, le processus cognitif élaboré par l'opérateur lors de son activité. L'objectif est de recenser les facteurs physiques, physiologiques, psychologiques, sociaux, chronobiologiques, comportementaux ou professionnels qui favorisent l'erreur humaine.

Au niveau système, il convient d'identifier, pour chaque type d'équipements, la liste d'erreurs humaines potentielles. Le résultat de cette étude permet au concepteur de prendre en compte, dès la première phase de développement du système (spécification), l'ensemble des erreurs humaines potentielles relatives à chaque type d'équipement et susceptibles de mettre en défaut la sécurité du système. L'objectif consiste donc à intégrer, dès les phases de spécification et de conception du système, les mesures adéquates pour rattraper, tolérer, réduire ou supprimer certaines erreurs humaines. Dans le domaine du transport ferroviaire, on distingue généralement trois types d'équipements : les équipements de sécurité (ou critiques), de surveillance et de disponibilité (ou fonctionnels). Les équipements de sécurité ont pour objectif de remplacer les opérateurs d'exploitation du système ou de faciliter les tâches qui leur sont confiées. Les systèmes de contrôle des équipements de freinage d'urgence, les systèmes d'anti-collision et les systèmes d'élaboration de consignes de vitesse en sont des exemples issus du domaine des transports guidés. Les équipements de surveillance permettent de centraliser les informations et de mieux organiser les actions d'interventions correctives ou préventives sur le système. Ils contribuent à l'amélioration du niveau de sécurité du système mais ils n'empêchent pas la survenue des accidents potentiels. Le système de supervision du service des quais et de traitement des alertes radio sont deux exemples d'équipements de surveillance. Les équipements fonctionnels assurent généralement la disponibilité du système. Le système d'asservissement de trains et le système de localisation des trains en sont deux exemples.

Toujours dans le cadre de la première phase d'analyse contextuelle (en amont de l'accident) et afin de tendre vers l'exhaustivité, il est indispensable d'analyser et de recenser les erreurs humaines potentielles en fonction des modes de conduite du système. Dans le domaine des transports ferroviaires guidés, on distingue généralement deux grands modes d'exploitation : les modes nominaux et les modes dégradés. Les modes d'exploitation *nominaux*, comportent plusieurs modes de conduite : la Conduite Automatique Intégrale sans agent de conduite, la Conduite en Pilotage Automatique avec agent de conduite (erreur de commande des portes et de départ du train), la Conduite Manuelle Contrôlée (erreurs de traction, erreurs de freinage) et la Conduite Manuelle Libre avec agent de conduite (erreur de conduite). Les modes d'exploitation *dégradés* concernent la Conduite Manuelle en Marche à Vue (non respect de l'espacement), la Conduite Manuelle avec Signalisation Auxiliaire (non respect d'une signalisation latérale) et la Conduite Manuelle de Secours (erreur de commande des portes et de départ du train). Les modes d'exploitation dégradés peuvent assurer des fonctionnements comme l'accostage, le scindage ou les services provisoires.

Outre les erreurs humaines relatives aux opérateurs humains et aux système, il convient également de recenser les différents facteurs environnementaux susceptibles d'influencer le bon déroulement de l'activité humaine et notamment l'exécution de la tâche prescrite (de supervision, de surveillance, de conduite, de diagnostic, ...). On peut distinguer deux types de dangers provoqués par l'environnement interne du travail (facteurs ambiants) et l'environnement externe (facteurs météorologiques).

L'identification de ces facteurs environnementaux permet de concevoir et de mettre en oeuvre des dispositions ergonomiques préventives adéquates. La prise en compte de ces facteurs dès la conception garantit une réduction des erreurs humaines lors de l'exploitation du système. L'analyse contextuelle de l'erreur humaine potentielle doit également mettre l'accent sur les différents facteurs d'interactions entre les opérateurs humains, entre l'homme et le système ou entre l'homme et son environnement interne et externe. L'anlyse des interactions entre l'opérateur et le système permet à l'ergonome concepteur de prendre en considération les problèmes liés aux caractéristiques du travail (charge, poste, horaires, ...), à celles de la tâche prescrite (nombre, durée, temps, force, connaissances, ...) et à celles de l'interface Homme-Machine.

6.4.2. Pendant l'accident (Analyse cognitive)

La deuxième phase d'analyse et d'évaluation de l'erreur humaine concerne le processus cognitif mis en jeu lors de déroulement de l'accident (comment ?). L'analyse cognitive de l'erreur humaine, dans ce contexte, vise à étudier les mécanismes cognitifs impliqués dans la production de l'erreur à l'origine de l'accident. Elle tente de savoir comment le processus cognitif de l'opérateur humain, compte tenu de l'analyse contextuelle en amont, a aboutit à une action erronée génératrice d'accident. A ce niveau, les erreurs humaines peuvent être classées de deux manières différentes et complémentaire, soit en se référant aux trois niveaux hiérarchiques de l'activité de l'homme (basé sur les automatismes, sur les règles ou sur les connaissances) soit relativement aux différentes étapes de traitement de l'informationn, de raisonnement humain ou de prise de décision. En s'inspirant des différents modèles conceptuels de traitement de l'information (notamment de Rasmussen et de Rouse), la figure 5 présente, au travers un modèle simplifié mais qui se prète mieux à une application industrielle, quelques exemples d'erreur humaine (dans les transports ferroviaires) relatives aux différentes phases de traitement de l'information ou de résolution de problème.

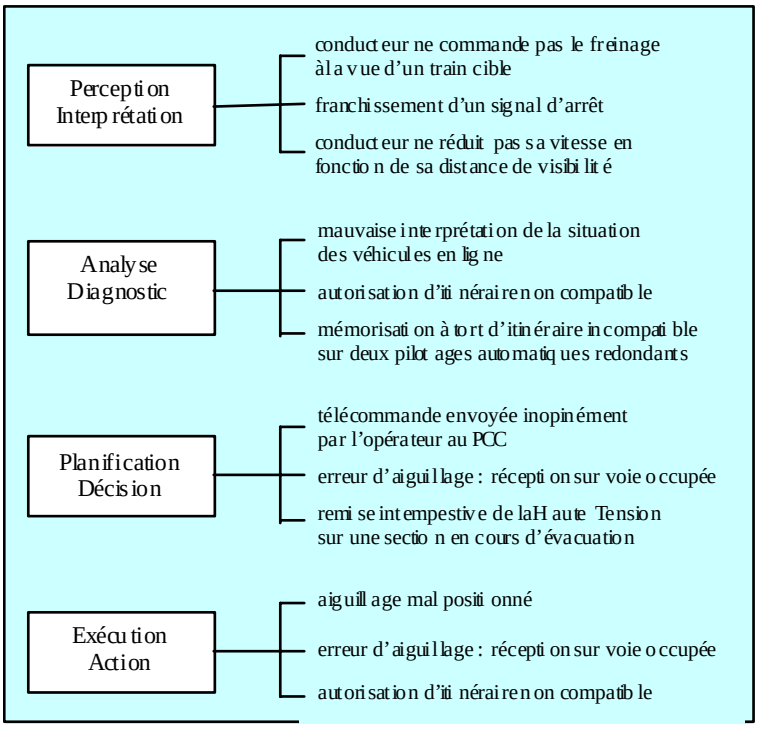


Figure 5 : Exemples d'erreurs humaines relatives aux étapes de traitement de l'information [Hadj-Mabrouk 04]

7. Conclusion

Cet article 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 leur tâche pénible d'évaluation des études de sécurité. À 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 êtres exploitables en milieu industriel.

Ce travail montre qu'il faut également prendre en compte la composante humaine dans les analyses afin d'améliorer sensiblement le niveau de sécurité d'un système de transport. En effet, l'ensemble des méthodes, techniques et outils développés (projets SAPRISTI, ACASYA, SAUTREL,…) 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. Il s'agit d'ajouter une autre composante fondamentale qui est souvent négligée dans le processus de construction de la sécurité à savoir la composante humaine (projet FACTHUS).

Enfin, à mon sens, la principale innovation des travaux réalisés 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 de transports ferroviaires.

8. Bibliographie

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

2. HADJ-MABROUK A., HADJ-MABROUK H. (2004) : *Approche d'intégration de l'erreur humaine dans le retour d'expérience. Application au domaine de la sécurité des transports ferroviaires.* Ouvrage de synthèse INRETS n° 43, février 2004, 107 p

3. HADJ-MABROUK H, (1992). Thèse de doctorat en Automatique Industrielle et Humaine. Université de Valenciennes. 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 ".*

4. HADJ-MABROUK H, (1998). Thèse d'Habilitation à Diriger des Recherches. Université de Technologie de Compiègne. Titre : *Acquisition et évaluation des connaissances de sécurité des systèmes industriels. Application au domaine de la certification des systèmes de transport guidés ".*

5. HADJ-MABROUK H, DESFRAY P. (2000). *" Législation et réglementation de la sécurité dans les transports publics guidés* ". Revue Générale des Chemins de Fer, Éditions DELVILLE, n° 7, juillet/août 2000, pp 11-23.

6. 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.

7. 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, vol. 26, n° 2, 1996.

8. HADJ-MABROUK H. (2004) : " *Rôles et obligations des acteurs impliqués dans la sécurité des transports ferroviaires ".* Colloque LM14, " Risques et Opportunités ", Bourges 12-14 octobre 2004, pp 757-764.

9. HADJ-MABROUK H. ; TRIKI I. (2003) : *La réglementation européenne en matière de sécurité ferroviaire.* Revue Générale des Chemins de Fer, Éditions DELVILLE, avril 2003, pp 5-20.

10. HADJ-MABROUK H., HADJ-MABROUK A., DOGUI M. (2001) : *" Sécurité ferroviaire et facteurs humains. Apport de la chronobiologie de la vigilance "*. Ouvrage de synthèse INRETS n° 38, juillet 2001, 138 p

11. KODRATOF Y. (1986). *« Leçons d'apprentissage symbolique automatique »*, Cepadues éditions, Toulouse, France, 1986.

12. LIEVENS C. (1976). *"Sécurité des systèmes"*. Cépaduès Éditions, Toulouse, 1976.

13. RASMUSSEN J. (1980) ; *What can be learned from human error reports* ? in : Duncan K., Grunuberg M and Dallis D. (Eds) , Changes in Working Life, (Wiley, Chichester), 97-113

14. RASMUSSEN J. (1982) ; *Human errors : a taxonomy for describing human malfunction in industrial installations* ; Journal of Occupational Accidents, 4, 1982, 311-335

15. RASMUSSEN J. (1986) ; *Information Processing and Human-machine Interaction,* : an approch to cognitive engineering, New York, North –Holland series in system science and engineering, 12, Ed. Sage A.P.

16. RASMUSSEN J. (1987), *The definition of Human Error and a Taxonomy for technical system design*, New Technology and Human Error (Rasmussen J. , Duncan K. et Leplat J.), Wiley John & sons, 1987, 23-30

17. RASMUSSEN J. (1990), *The role of error in organizing behaviour*, Ergonomics, 1990, vol 33, n° 10/11, 1185-1199

18. REASON J. (1990), *L'erreur humaine* ; Presses Universitaires de France ; 1990

19. REASON J. (1977) ; *Skill and error in everyday life* ; in HOWE M. J. A. (éd), LEY J.W., Adult learning, New York, 1977, 21-24

20. REASON J. (1979) ; *Actions not as planned : The price of automatization* ; in Underwood G. et Steven R. (Eds), Aspects of consciouness , vol 1, Psychological Issues, London, Academic Press, London, 1979, 67-89

21. ROUSE W.B. et ROUSE S.H. (1983) , *Analysis and classification of human error*, IEEE Transactions on systems, man and cybernetics, vol SMC-13, 3, 1983, 539-549

22. ROUSSEL B. (1991); *Substances éveillantes et transports* ; Le maintien de la vigilance dans les transports; Sous la direction de M. Vallet; Edition Paradigme ; 1991 ; p : 41-49

23. VAN ESLANDE P. (2000) ; *L'erreur humaine dans les scénarios d'accident : cause ou conséquence ?*; RTS n° 66 ; Mars 2000

24. VAN ESLANDE P. (2001). *De l'analyse clinique des dysfonctionnements aux scénarios d'erreur*. Séminaire Sécurité Routière ; 24 avril 2001, Aix en Provence

25. VAN ESLANDE P. et al. (1997); *Scénarios-types de production de l'erreur humaine dans l'accident de la route, Problématique et analyse quantitative*; Rapport INRETS n° 218 ; Juin 1997

26. VAN ESLANDE P. et ALBERTON L. (1997). *L'accident de la route : chercher l'erreur*. In GANACIA JG., colloque Sécurité et Cognition, Ed HERMES, 16-17 sept 1997, pp 205-222

27. VILLEMEUR A. (1988). *"Sûreté de fonctionnement des systèmes industriels"*. Éditions Eyrolles, Paris, 1988.