Capitalisation et exploitation des connaissances de sécurité

Habib Hadj Mabrouk

CAPITALISATION ET EXPLOITATION DES CONNAISSANCES DE SÉCURITÉ

CAPITALIZATION AND EXPLOITATION OF THE KNOWLEDGE OF SAFETY

Hadj-Mabrouk H.
INRETS, 23 rue Alfred Nobel
77420 Champs sur Marne
mabrouk@inrets.fr

Résumé

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 :

- 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 ;
- 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.

Afin de mieux appréhender ces lacunes, et de tenter, le cas échéant, de les combler, nous avons défini un projet de recherche baptisé AVIS (Acquisition et Validation des connaissances de Sécurité). Ce projet a pour ambition d'améliorer l'élaboration et l'évaluation des différentes analyses de sécurité, en traquant l'erreur au niveau système, matériel et logiciel, 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, 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.

Cet article propose une description générale de trois maquettes d'outils d'aide à l'analyse et à l'examen de la sécurité :

- « SAPRISTI » pour l'aide à l'élaboration et à l'évaluation des analyses préliminaires de risques (APR) ;
- « SAUTREL » pour l'aide aux analyses des effets des erreurs de logiciels (AEEL) ;
- « FACTHUS » pour l'aide à l'intégration des facteurs humains dans le retour d'expérience (Rex).

Summary

While the analysis of safety is one of the fundamental tasks involved in making a transport system safe it nevertheless still remains a stumbling block and close scrutiny of the process reveals certain shortcomings:

- There is not always agreement regarding the usual methods of safety analysis, and practices sometimes ignore the few theoretical recommendations which exist. As a result, the formats used to present the results of analyses differ greatly from one manufacturer to another;
- Finally, the production and appraisal of a safety file are particularly difficult and tedious tasks which are not always backed up by a formalized strategy. The thoroughness and coherence of analyses remain essentially the product of the know-how, intelligence and intuition of experts.

In order to gain a better understanding of these shortcomings and attempt, where possible, to remedy them, we have set up a research project named AVIS (Acquisition and Validation of Safety Knowledge). The aim of this project is to improve the production and assessment of the different types of safety analyses by searching for errors at system level and in the hardware and software by following two directions of investigation:

- A methodological direction, which attempts to improve the methods which are normally used for safety analyses and suggests methods and strategies for the appraisal of these analyses as regards coherence, completeness and traceability, etc.
- An operational direction, which aims to develop software tools to aid in the design and examination of safety analyses. In particular these include systems for the acquisition, modelling, storage and appraisal of these analyses.

This paper presents a general description of three mock-ups of tools which are intended to aid in the analysis and investigation of safety. These are:

- "SAPRISTI", for aid in the production and assessment of preliminary hazard analyses ;
- "SAUTREL", for aid in the examination of software error effect analyses ;
- "FACTHUS", for aid the integration of human factors in the experience feedback.

1. Motivations et objectifs de la recherche

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) conformément à la nouvelle réglementation Nationale et Européenne. 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 :

- 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.

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 non seulement au niveau système, logiciels et matériels, mais aussi au niveau humain. Généralement, le processus de construction de la sécurité d'un système comporte plusieurs analyses complémentaires hiérarchisées : L'analyse préliminaire de risques (APR), l'analyse fonctionnelle de la sécurité (AFS), et l'analyse de la sécurité du produit réalisé qui concerne l'analyse de la sécurité des équipements logiciels (ASL) et l'analyse de la sécurité des équipements matériels (ASM). 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.

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:

- 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 et systématique 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. Le présent papier propose une description rapide de trois méthodes et outils permettant d'améliorer sensiblement la tâche d'évaluation des études de sécurité et par conséquent d'aider les experts du domaine dans le processus d'homologation et de certification d'un nouveau système de transport ferroviaire guidés :

1. Au niveau **système** : Projet SAPRISTI - Modèle en spiral d'analyse préliminaires de risques (APR) ;
2. Au niveau **logiciel** : Projet SAUTREL - Outil d'aide aux analyses des effets des erreurs de logiciels (AEEL) de sécurité basé sur le raisonnement à partir de cas ;
3. Au niveau **Humain** : Projet FACTHUS - Méthode d'intégration des facteurs humains dans le retour d'expérience.

2. Approche retenue

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.
L'approche retenue pour développer l'ensemble des méthodes et outils d'aide à l'analyse de la sécurité implique deux grandes activités :

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.

Notre approche consiste donc 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.

Les paragraphes suivant présentent successivement trois nouvelles approches méthodologiques d'analyse et d'évaluation de la sécurité : Au niveau **système** (projet SAPRISTI), au niveau **logiciel** (projet SAUTREL) et au niveau **Humain** (projet FACTHUS).

3. Niveau système : Modèle en « spirale » d'analyse préliminaire des risques

Selon l'article 48 du chapitre III du titre V du décret n°2006-1279, le dossier préliminaire de sécurité (DPS) précise les objectifs de sécurité poursuivis et les méthodes qui seront appliquées pour les atteindre, les méthodes de démonstration et les principes dont le respect permettra le maintien du niveau de sécurité pendant toute la période d'exploitation du système. L'arrêté d'application de 08/01/2002 du décret n°2000-286 précise que le DPS comporte notamment un document relatif à l'organisation du projet et s'appuie sur les résultats d'une Analyse Préliminaire des Risques (APR). Cet arrêté précise aussi que le dossier de sécurité (DS) a pour objet de décrire le système tel que réalisé, d'apporter la preuve du respect des mesures de sécurité exposées dans le DPS. Il contient les conclusions des études de sécurité réalisées et les attestations de couverture des risques identifiées dans l'APR. 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 H. 1995] et [Hadj-Mabrouk H. 1998]. 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).

3.1. Méthode d'APR proposée

Notre méthode d'APR s'articule autour de trois étapes complémentaires et itératives (La figure 1). 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).

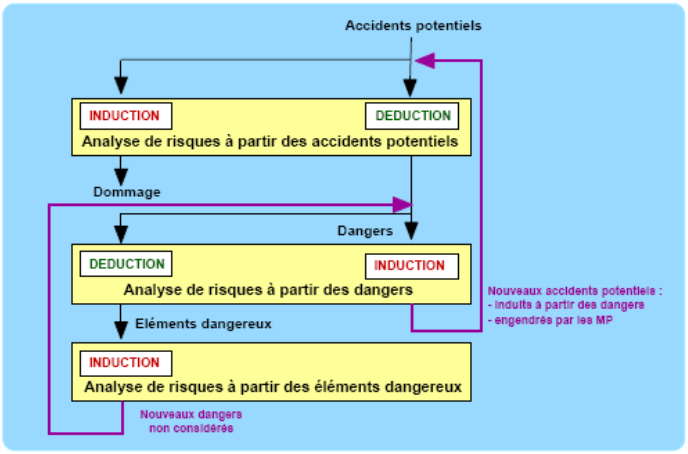

Figure 1. Principe général de la méthode d'APR proposée [Hadj-Mabrouk 2006]

3.2. Description détaillée de la méthodologie proposée

La méthodologie proposée, illustrée par la figure 2, se base sur un modèle en spirale formé par trois couches qui interagissent en vue de garantir la complétude et l'exhaustivité de l'APR. Le noyau du modèle proposé est le processus d'APR retenu (figure 1) qui s'articule autour de trois analyses complémentaires et itératives. Sur ce noyau, se superposent les cinq principes du processus du retour d'expérience (REX) : connaître le risque, le comprendre, l'archiver, l'apprendre et enfin proposer des recommandations; en formant ainsi la deuxième couche du modèle. Ces cinq principes du REX sont associés aux cinq phases de collecte des données relatives à un événement d'insécurité - analyse et traitement - stockage et mémorisation - exploitation - recommandations. La troisième et dernière couche du modèle est composée des différentes étapes du cycle de développement d'un système : spécification, conception, réalisation, intégration, validation, certification, homologation, mise en service, exploitation et maintenance.

La méthodologie constitue, en fait, un modèle compact et itératif garantissant ainsi l'interaction entre ces différentes couches d'une manière systématique. En effet, conformément à la réglementation en vigueur, des enquêtes techniques de sécurité doivent être effectuées après les accidents/incidents survenus sur le système tout en prenant en compte les informations relatives aux erreurs humaines, technologiques et environnementales (figure 2). La première phase de collecte de données du REX correspond à rechercher et recueillir tous les éléments tant descriptifs qu'explicatifs ayant conduit à un événement d'insécurité. Ainsi, cette phase se base sur les résultats issus des différents rapports d'enquêtes. Après avoir analyser et stocker les données déjà collectées, la phase d'exploitation du processus de REX consiste à utiliser et interpréter ces données. L'objectif principal est d'extraire l'événement réellement prédictif, de prendre en considération les cas isolés et de prédire ou d'imaginer des futurs scénarios d'accidents ou évènements indésirables. A partir des résultats de cette phase, on peut explicitement extraire les listes des accidents potentiels et les utiliser directement comme entrées de l'APR (figure 2). En effet, la phase ultime de la démarche de REX correspond à recommander des mesures de prévention (afin de minimiser l'occurrence des accidents potentiels) et des mesures de protections (en vue d'affaiblir la gravité des dommages engendrés). Ces recommandations ont pour but l'action sur les facteurs humains, les aspects techniques et l'environnement. Systématiquement, ces mesures sont prises en compte, dès la spécification, dans le cycle de développement de tout nouveau système afin de limiter la reproduction de tel évènement d'insécurité. A notre sens, l'originalité du modèle en spirale proposé réside dans le fait de considérer le REX comme étant le maillon fondamental qui enchaîne exploitation vers la phase de spécification. Ainsi, la méthodologie proposée garantie la traçabilité de la gestion de risque en le suivant dès son apparition jusqu'à la mise en œuvre concrète des mesures de protection et/ou de prévention.

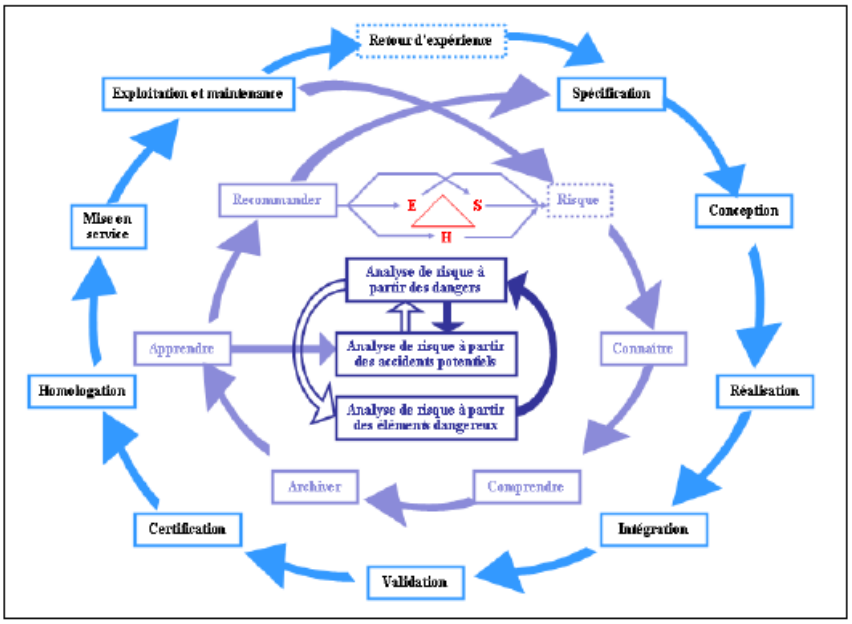

Figure 2. Modèle en Spirale d'intégration du REX dans l'APR [Hamdaoui, Hadj-Mabrouk 2008]

4. Niveau Logiciel : Outil d'aide aux analyses des effets des erreurs de logiciels (AEEL) basé sur le raisonnement à partir de cas

L'une des méthodes les plus appliqués lors de l'analyse de sécurité au niveau logiciel d'un système de transport ferroviaire guidé, est celle d'Analyse des Effets et Erreurs du Logiciel (A.E.E.L.). Néanmoins, la vérification de l'exhaustivité et de la cohérence des AEEL représente, pour les experts de certification, une tâche fastidieuse. L'étude vise le développement d'un outil logiciel baptisé « SAUTREL », basé sur le raisonnement à partir de cas, dont le but est d'exploiter les A.E.E.L. historiques, menées sur des logiciels déjà certifiés, en vue d'évaluer l'exhaustivité, la cohérence et la pertinence de l'A.E.E.L. d'un nouveau logiciel. Le raisonnement à partir de cas (RàPC) est une forme de raisonnement par analogie. L'analogie proprement dite recherche les relations de cause à effet dans les situations passées pour les transposer à la situation courante ainsi que les ressemblances entre les situations passées et la situation courante. Le RàPC recherche seulement les ressemblances ou les relations de proximité entre les situations passées et la situation courante. Le RàPC envisage le raisonnement comme un processus de remémoration d'un petit ensemble de situations concrètes : les cas. Il fonde ses décisions sur la comparaison de la nouvelle situation (cas cible) avec les anciennes (cas sources). 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. D'un point de vue très global, le RàPC met en œuvre une base d'expériences ou de cas, un mécanisme de recherche et d'extraction des cas similaires et un mécanisme d'adaptation et d'évaluation des solutions des cas extraits pour résoudre le problème spécifié.
Cette étude 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 formalisme a été établi à partir de l'analyse et de l'examen de 800 fiches AEEL relatives à deux systèmes de transport ferroviaires déjà certifiés et fonctionnent actuellement en France. Sur la base de ce formalisme, nous avons constitué une bibliothèque de 224 cas types. La maquette " SAUTREL " a été réalisée sur PC à l'aide du logiciel « ReCall » et comporte quatre principaux modules (figure 3) :
1. Interface Homme/Machine pour l'introduction, la mise à jour et la consultation des connaissances relatives aux AEEL ;
2. Module de formalisation et d'acquisition des fiches AEEL ;
3. Base de connaissances qui regroupe 224 cas d'AEEL (base d'expériences) ;
4. Processus de raisonnement à partir de cas.

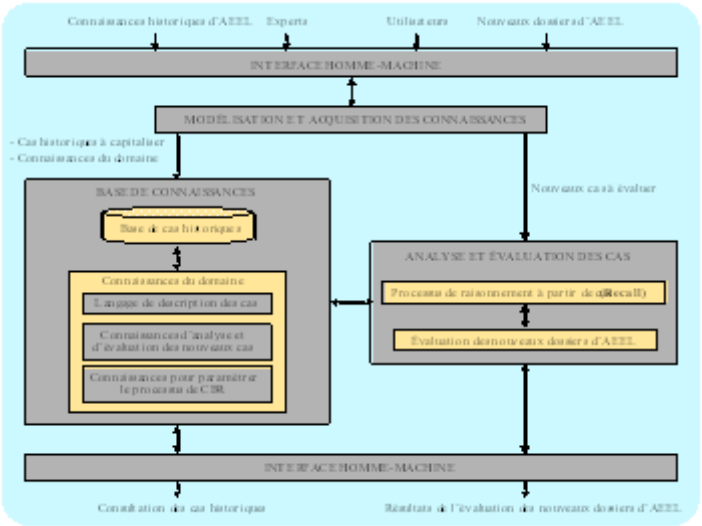

Figure 3. Architecture fonctionnelle de la maquette du système " SAUTREL" [Hadj-Mabrouk 2007]

L'utilisation de la maquette " SAUTREL " requiert le passage par les huit étapes suivantes :
1. Définition du langage de description des exemples d'A.E.E.L. ;
2. Élaboration de la base de cas d'A.E.E.L. ;
3. Paramétrage du RàPC ;
4. Saisie de la fiche A.E.E.L. à évaluer (figure 4) ;
5. Étape d'indexation de la base de cas d'A.E.E.L. (figure 5) ;
6. Étape d'extraction des cas d'A.E.E.L. similaires (figure 6) ;
7. Étape d'adaptation des cas extraits (cas sources) ;
8. Mise à jour de la base de cas d'A.E.E.L.

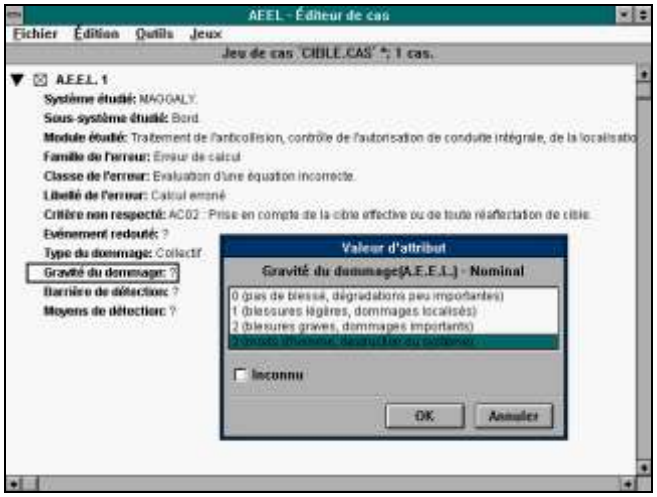

Figure 4. Exemple de cas AEEL cible en cours de saisie.

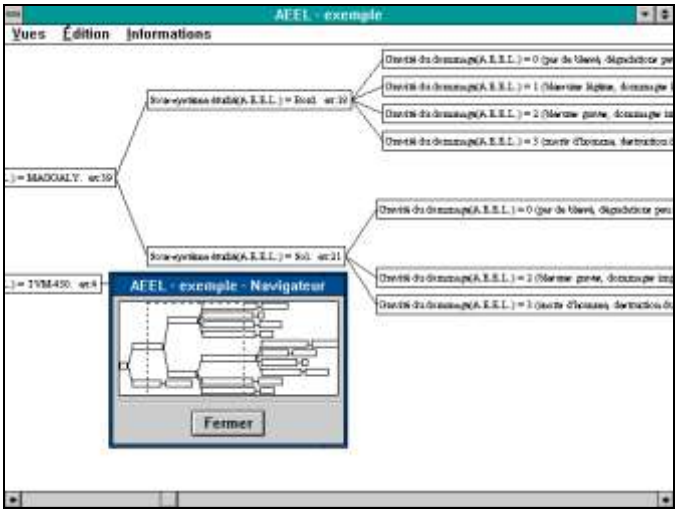

Figure 5. Exemple d'arbre d'indexation.

Figure 6. Exemple d'utilisation de la méthode de vote pour la recherche de cas AEEL similaires.

L'originalité de la maquette de faisabilité développée pour l'aide à l'Analyse des Effets des Erreurs du Logiciel (AEEL) réside non seulement au niveau de sa capacité à capitaliser et à diffuser les connaissances en matière d'AEEL, mais elle représente aussi les premiers travaux de recherche sur l'application du RÀPC aux AEEL [Hadj-Mabrouk 2007]. 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 proposées 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, le traitement des valeurs manquantes, l'amélioration des stratégies d'adaptation des solutions proposées par le système, l'enrichissement de la

4. Niveau Humain : Méthode d'intégration de l'erreur humaine dans le retour d'expérience

La méthode 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 relatifs au fonctionnement cognitif de l'homme et de Van Eslande relatifs aux scénarios types d'accidents. Centrée sur le déroulement d'un accident potentiel, cette méthode (figure 7) 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). 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.

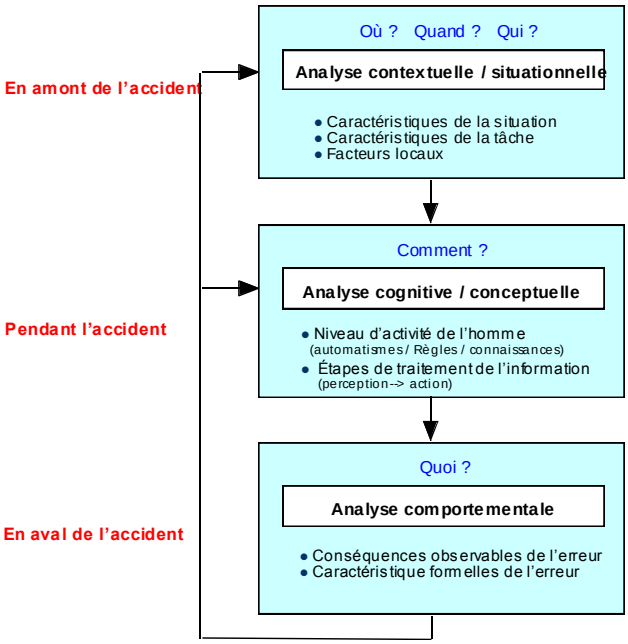

Figure 7. Approche d'intégration des facteurs humains dans l'analyse des scénarios (Hadj-Mabrouk 2004)

3.1 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). 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.

Outre les erreurs humaines relatives aux opérateurs humains et au 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 œuvre 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.

3.2 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, consiste 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 abouti 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 8 présente, au travers un modèle simplifié mais qui se prête 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. La figure 9 récapitule le modèle de Rasmussen et de Reason et illustre quelques exemples d'erreur humaine (issus des transports ferroviaires) liées au mode de fonctionnement humain basé sur les automatismes, sur les règles ou sur les connaissances.

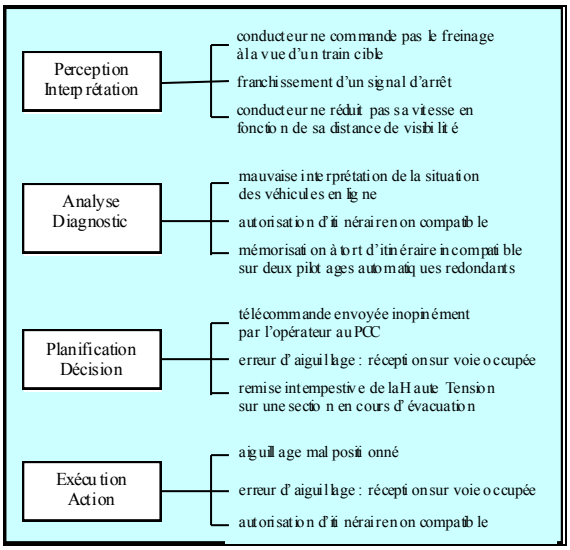

Figure 8. Exemples d'erreurs humaines relatives aux étapes de traitement de l'information

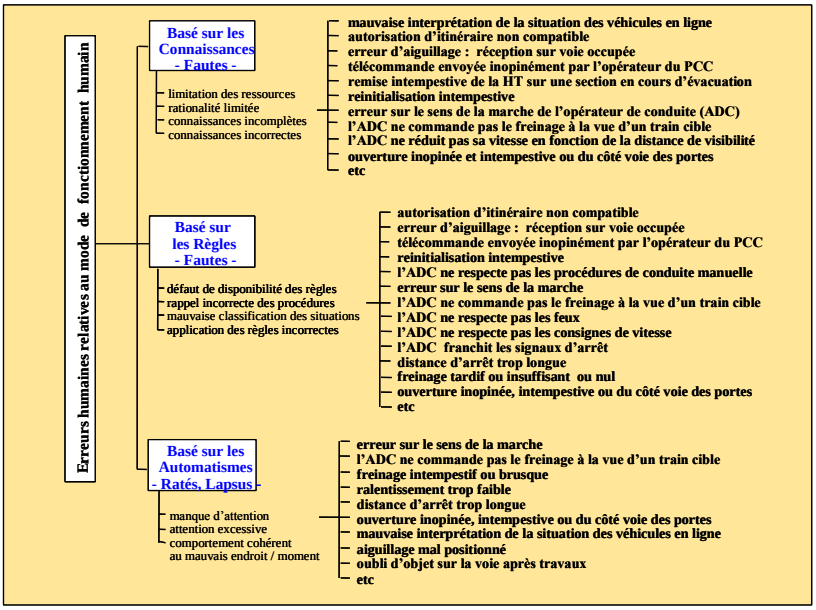

Figure 9. Exemples d'erreurs humaines relatives aux niveaux d'activités de l'opérateur

Conclusion

Ce papier 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, 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, 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 notre 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.

Références

Décret n°2003-425 du 9 mai 2003 relatif à la sécurité des transports publics guidés.

Décret n°2006-1279 du 19 octobre 2006 relatif à la sécurité des circulations ferroviaires et à l'interopérabilité du système ferroviaire.

Hadj-Mabrouk H. (2007). Chapitre 4 d'un ouvrage collectif – « Contribution du raisonnement à partir de cas à l'analyse des effets des erreurs du logiciel. Application à la sécurité des transports ferroviaires ». Editions Hermès-Lavoisier, pp 123-148, 2007

Hadj-Mabrouk A. et 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, Lavoisier février 2004, 104 p.

Hadj-Mabrouk H. (2006), « Méthode d'analyse préliminaire des risques dans les transports ferroviaires ». 15ème congrès de maîtrise des risques et de Sûreté de fonctionnement, Lille, 10-12 Octobre 2006.

Hamdaoui F. and Hadj-Mabrouk H. (2008), "Complementarity of Preliminary Hazard Analysis and Field Data Feedback to improve security - Application to rail transport", 20 - 22 décembre 2008, Sousse - Tunisie

Joing M. (1991), « le retour d'expérience à la SNCF », colloque la sécurité des transports collectifs, décembre 1991, Paris, 178- 180.

LOI 2002-3 du 03 janvier 2002 relative à la sécurité …, aux enquêtes techniques après événement de mer, accident ou incident de transport terrestre ou aérien …

Maalel A. and Hadj-Mabrouk H. (2010), "Contribution of case based reasoning (CBR) in the exploitation of return of experience "Application to accident scenarii in rail transport" 3d. International Conference on Information Systems and Economic Intelligence, p 99-109, 2010.

Villemeur A. (1998), Sureté de fonctionnement des systèmes industriels, Collection de la direction des Etudes et de Recherches d'EDF, Paris, Editions Eyrolles, 1998.