Contribution du raisonnement à partir de cas à l'évaluation des effets des erreurs logiciels

Habib Hadj-Mabrouk, Ahmed Maalel, Feyrouz Hamdaoui

SETIT 2009
5th International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications
March 22-26, 2009 – TUNISIA

Contribution du Raisonnement à Partir de cas à l'Evaluation des Logiciels de Sécurité

Habib HADJ MABROUK*, Ahmed MAALEL** and Feyrouz HAMDAOUI***

* *INRETS*
Institut National de Recherche sur les Transports et leur Sécurité
2 avenue du Général Malleret-Joinville, 94114 Arcueil Cedex - France
mabrouk@inrets.fr

** *ISTL Sousse - Tunisie*
maalel_ahmed@hotmail.com

*** *ISSAT Sousse - Tunisie*
feyrouzhamdaoui@gmail.com

Résumé: 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. Dans ce contexte, notre 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.
Mots clés: Analyse des Effets et Erreurs du Logiciel (A.E.E.L.), Raisonnement à partir de cas, SAUTREL, Sécurité, système de transport ferroviaire.

INTRODUCTION

Le processus de construction de la sécurité d'un système de transport guidé fait intervenir trois grandes activités d'analyses de sécurité : l'analyse au niveau système, l'analyse au niveau logiciel et l'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 baptisé " SAUTREL " basé sur le raisonnement à partir de cas. Cet outil a pour but d'aider les experts en matière de sécurité et de certification à juger l'exhaustivité et la cohérence des AEEL critiques d'un nouveau système de transport ferroviaire guidé.

Très schématiquement, le principe du raisonnement à partir de cas consiste à traiter un nouveau problème en se remémorant des expériences passées voisines. Le but de cette étude est d'exploiter des 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. À ce jour, les principaux résultats obtenus sont les suivants [DAR 95, 96], [NDI 96], [HAJ 96, 98, 00, 05] :

- Un formalisme de représentation des fiches AEEL ;
- Une base de 224 cas d'AEEL issue des travaux de recueil et de modélisation des connaissances de deux systèmes de transport guidés déjà certifiés (TVM 430 du TGV Nord et le Métro MAGGALY de Lyon) ;

Une maquette de faisabilité " SAUTREL " d'aide à la capitalisation et à l'évaluation des AEEL basée sur le raisonnement à partir de cas. Cette maquette a été réalisée à l'aide de l'outil logiciel " ReCall " de la société ISOFT.

1. Contexte général de la recherche

L'évaluation de la conception et de la réalisation d'un nouveau système ou de la modification d'un système existant 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) des concepteurs et constructeurs. Cet organisme chargé d'une mission de certification, procédure par laquelle une tierce partie donne une assurance écrite, qu'un produit, un processus ou un service est conforme aux exigences spécifiées.

Concrètement les experts de certification doivent évaluer et vérifier les capacités du système au regard des objectifs de sécurité qu'il doit atteindre et maintenir durant toute la durée de son exploitation. L'OSTI vérifie notamment que la conception et la réalisation sont effectuées conformément aux règlements en vigueur et aux règles de l'art qui sont généralement spécifiées dans un Dossier Préliminaire de Sécurité (DPS). Ce dernier doit exposer 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 [HAJ 03].

Généralement, le processus de construction de la sécurité d'un système (figure1) comporte plusieurs analyses complémentaires hiérarchisées [HAJ 96, 98, 05] : L'analyse préliminaire de risques, l'analyse fonctionnelle de la sécurité, et l'analyse de la sécurité du produit réalisé. 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 plusieurs types d'analyses : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC), Méthode des Combinaisons de Pannes Résumées (MCPR) et Méthode de l'Arbre des Causes (MAC).

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 cet article vise le développement d'un outil logiciel basé sur le raisonnement à partir de cas pour l'aide à l'analyse de la sécurité au niveau logiciel et plus précisément la méthode d'analyse des effets des erreurs du logiciel (AEEL).

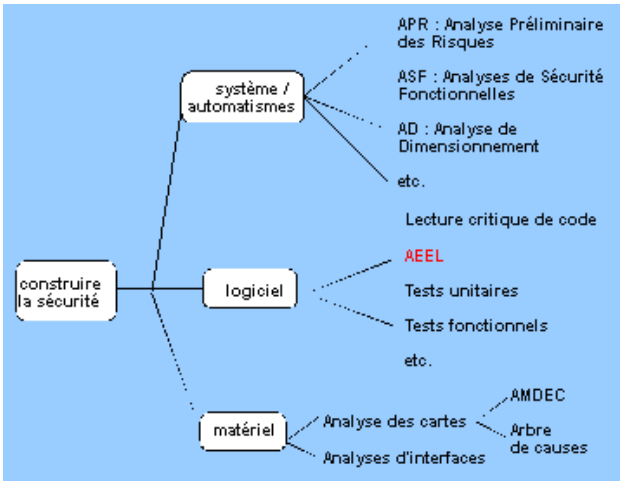

***Figure 1**. Processus de construction de la sécurité d'un système de transport [HAJ 98]*

2. Approche mise en œuvre pour développer l'outil " SAUTREL"

L'approche suivie pour concevoir et mettre en œuvre l'outil d'aide aux AEEL est centrée sur l'emploi des techniques d'intelligence artificielle (IA) et notamment sur l'utilisation des méthodes d'acquisition, de représentation et d'apprentissage automatique. L'élaboration de la base de connaissances d'un outil d'aide aux AEEL nécessite d'avoir recours aux techniques et méthodes d'acquisition de connaissance (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'apprentissage automatique apparaît-elle comme une solution très prometteuse. L'approche retenue pour développer l'outil d'aide à l'AEEL 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 archivées (AEEL historiques) 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 et notamment sur le raisonnement à partir de cas.

L'apprentissage automatique [KOD 86] et [GAN 87] permet de faciliter le transfert de connaissances, notamment à partir d'exemples expérimentaux. Il contribue à l'élaboration des bases de connaissances tout en réduisant l'intervention du cogniticien. 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.

3. Analogie et raisonnement à partir de cas

L'apprentissage automatique repose sur quatre mécanismes de raisonnement ou modes d'inférence : induction, déduction, abduction et analogie. On peut représenter de façon plus formelle ces modes de raisonnement :

- Déduction : à partir de A et de A=>B, on "déduit" B

- Abduction : à partir de B et de A=>B, on "abduit" A
- Induction : à partir de A (z) =>B et de A (t) =>B, on "induit" A (x) =>B

- L'**analogie** procède, quant à elle, du fait au fait : elle consiste à faire l'hypothèse suivante : une propriété vraie d'un objet peut également l'être pour un autre présentant des similitudes avec le premier. La plausibilité de la conclusion dépend de la ressemblance entre ces deux objets. L'analogie est utilisée en pratique pour comprendre ou interpréter de nouvelles situations à partir de situations antérieures déjà mémorisées. L'analogie combine à la fois la notion de similarité (ou ressemblance) et la notion de causalité (figure 2). Plus formellement, une analogie comporte une situation source de la forme (A, B) et une situation cible de la forme (A', B'). Il existe des relations de similarité (et de dissimilarité) entre A et A', respectivement B et B', ainsi que des relations de dépendance, généralement de nature causale, entre A et B, respectivement A et B'.

Faire une analogie, c'est partir d'un schéma incomplet semblable à celui de la figure 2 et le compléter en combinant similarité et causalité. En résumé, l'apprentissage par analogie consiste à reconnaître des similarités entre le concept cible à apprendre et un concept source connu et ensuite à déterminer qu'elles caractéristiques pertinentes peuvent être transférées de la "source" vers la "cible".

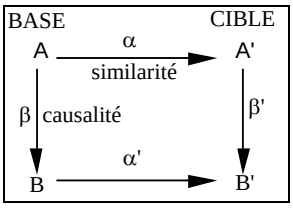

***Figure 2**. Principe du raisonnement par analogie*

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 (figure 3).

Les travaux de [SLA 91], [HAR 91], [KOL 93], [MOT 93] et [PIN 93] retracent de façon assez complète l'évolution des recherches dans le domaine du RàPC.

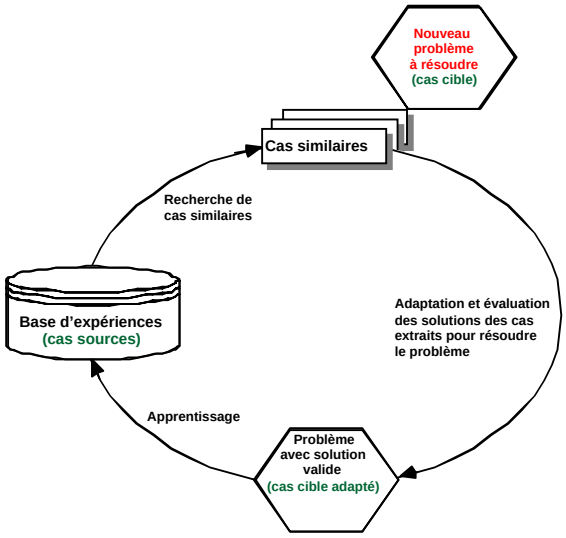

***Figure 3.** Principe général du raisonnement à partir de cas [HAJ 98]*

4. La méthode d'analyse des effets des erreurs de logiciel (AEEL)

Il est actuellement laborieux de démontrer de manière certaine qu'un logiciel est exempt de toute erreur. En France et dans le domaine de la sécurité ferroviaire, la technique du monoprocesseur codé est utilisée pour garantir la sécurité d'exécution des logiciels. Toutefois, cette technique ne garantit pas la 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'AEEL peut, quant à elle, prendre en compte, entre autres, l'analyse de ces erreurs [THI 86], [AFN 90]. Il s'agit d'une démarche d'analyse inductive visant à déterminer la nature et la gravité des effets des défaillances du logiciel. L'AEEL permet aussi 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'apprécier 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 orienter 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 résulter au niveau du système. L'AEEL propose finalement des mesures visant à détecter les erreurs et à consolider la robustesse du logiciel.

L'enchaînement d'un ensemble d'activités mises en œuvre dans un ordre bien déterminé pour réaliser un logiciel est appelé cycle de développement d'un logiciel (figure 4). Les A.E.E.L. sont effectuées au cours de la branche descendante du cycle en " V " du développement du logiciel. Leur place dans le cycle de développement n'est fixée que par la norme française /NF F 71 012/ [AFN 90] qui recommande de les entamer en phase de conception préliminaire lorsque les éléments logiciels de sécurité sont reconnus, et d'en tenir compte lors des phases de conception détaillée et de codage. D'après les travaux de Thireau [THI 86], elles se déroulent en parallèle des phases de conception détaillée et de codage.

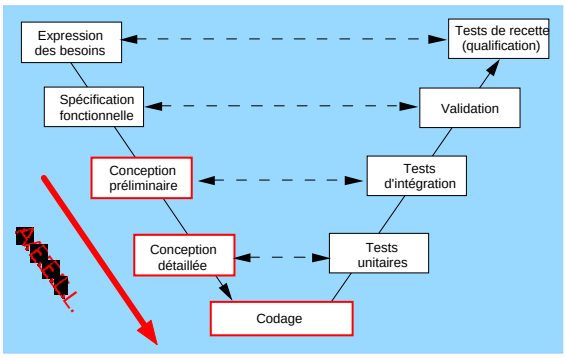

***Figure 4**. Place de l'AEEL dans le cycle de développement d'un logiciel*

5. Maquette de faisabilité d'un outil " SAUTREL " d'aide aux AEEL

5.1. Acquisition et modélisation des connaissances d'AEEL

Cette étape 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. 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 depuis plusieurs années. Sur la base de ce formalisme, nous avons constitué une bibliothèque de 224 cas types.

5.2. Développement de la maquette " SAUTREL "

La maquette " SAUTREL " a été réalisée sur PC à l'aide du logiciel « ReCall » de la société ISOFT et comporte quatre principaux modules [DAR 95] (figure5) :

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.

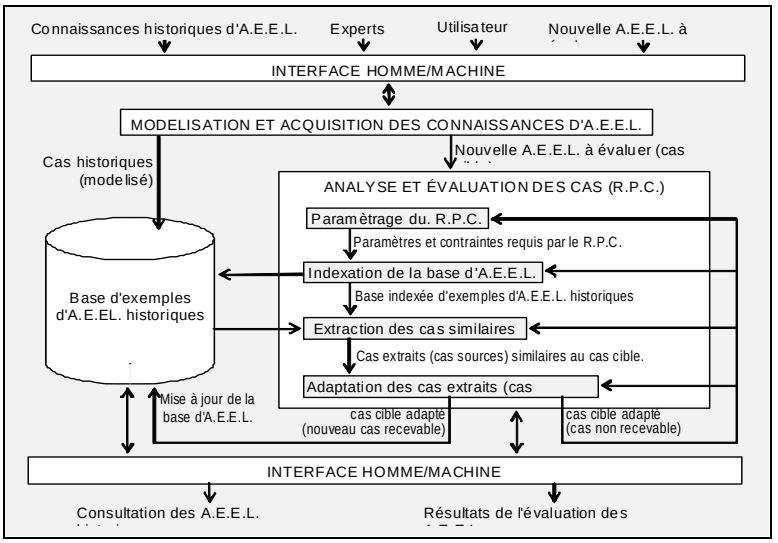

***Figure 5.** Architecture fonctionnelle de la maquette du système " SAUTREL "*

5.3. Exemple d' application

L'utilisation de la maquette " SAUTREL " requiert le passage par les huit étapes détaillées ci-après [DAR 96], [HAJ 98], [HAJ 07].

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 ;
5. Étape d'indexation de la base de cas d'A.E.E.L. ;
6. Étape d'extraction des cas d'A.E.E.L. similaires ;
7. Étape d'adaptation des cas extraits (cas sources) ;
8. Mise à jour de la base de cas d'A.E.E.L.

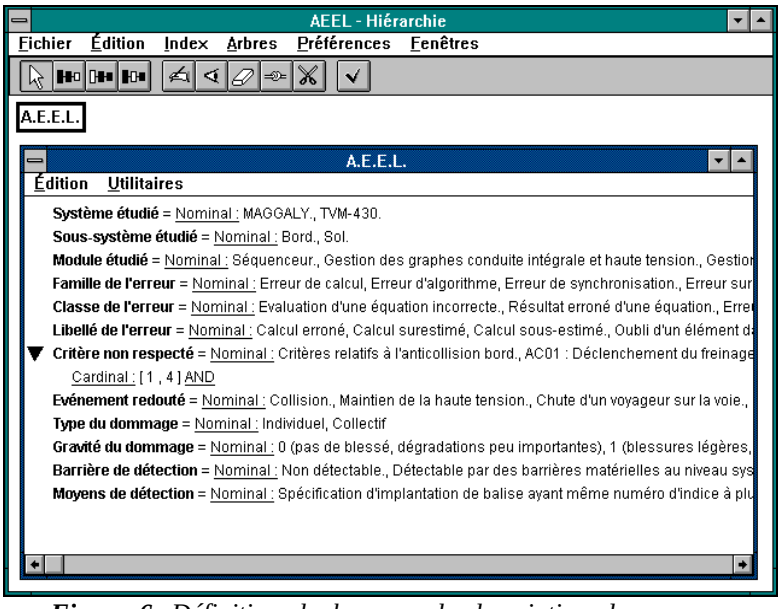

***Figure 6.** Définition du langage de description des exemples d'A.E.E.L.*

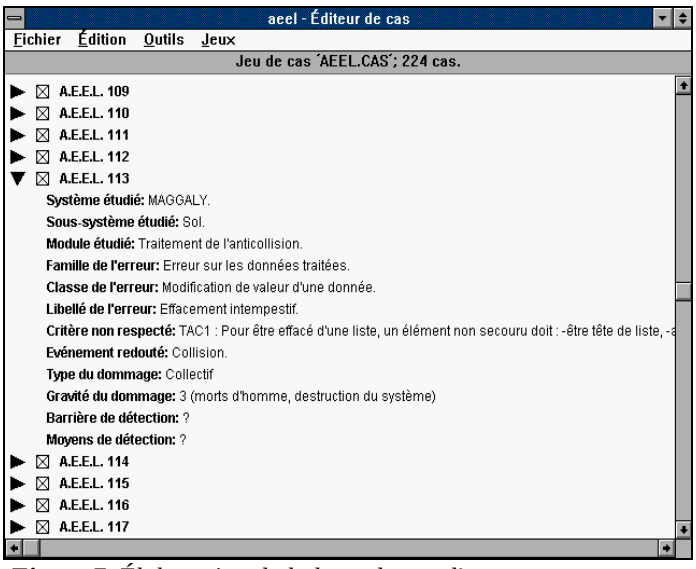

Figure 7. *Élaboration de la base de cas d'A.E.E.L.*

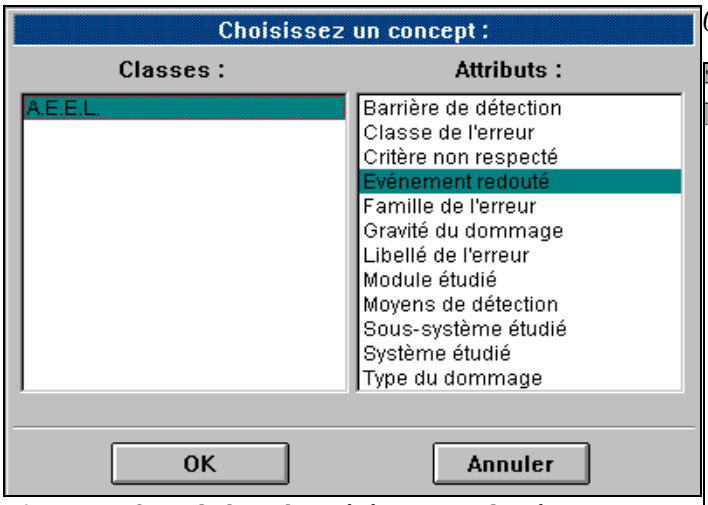

Figure 8. *Choix de l'attribut "événement redouté" comme concept*

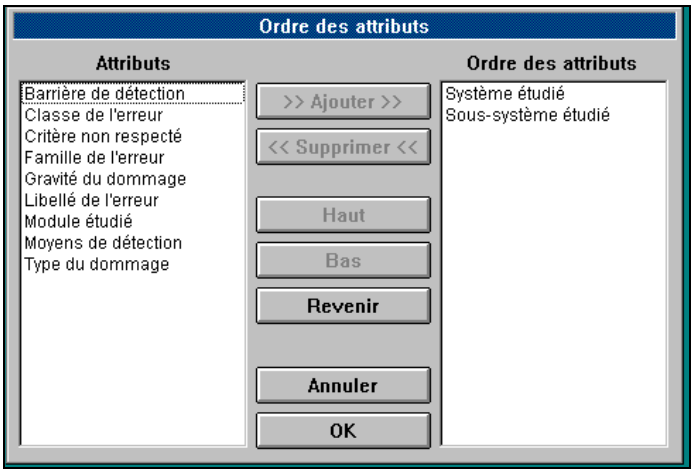

Figure 9. *Choix de l'ordre des descripteurs dans l'arbre d'indexation*

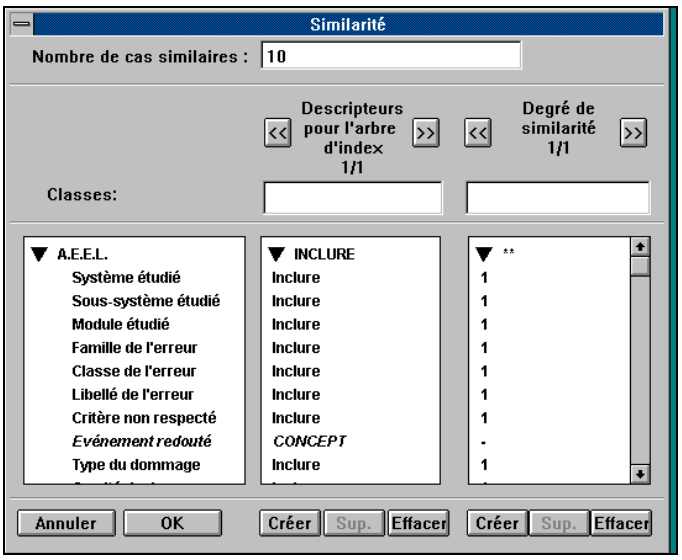

Figure 10*. Paramétrage de la stratégie d'appariement (mesure de similarité)*

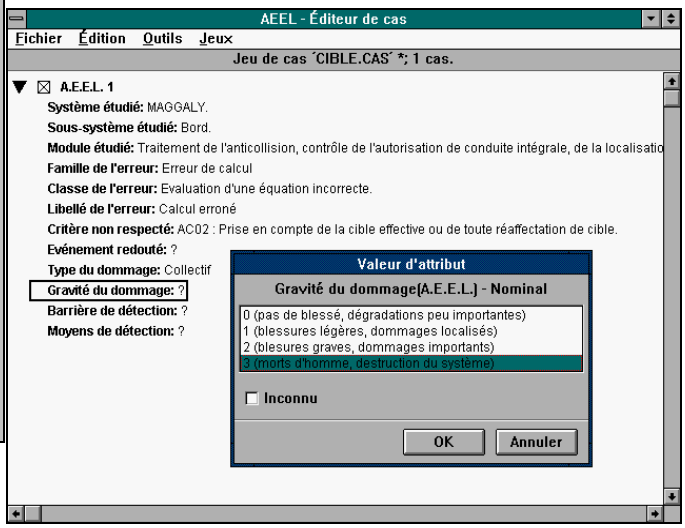

Figure 11*. Exemple de cas cible en cours de saisie.*

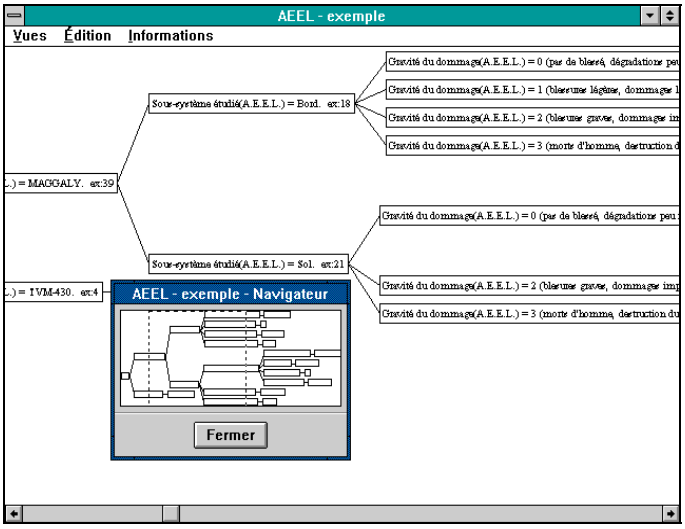

Figure 12. *Exemple d'arbre d'indexation.*

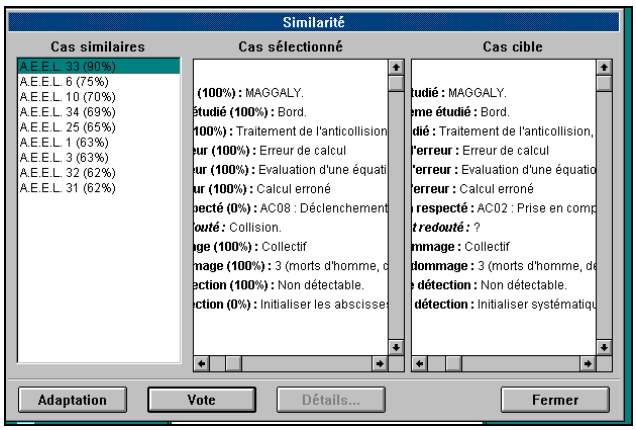

Figure 13. *Visualisation des cas similaires extraits de la base de cas*

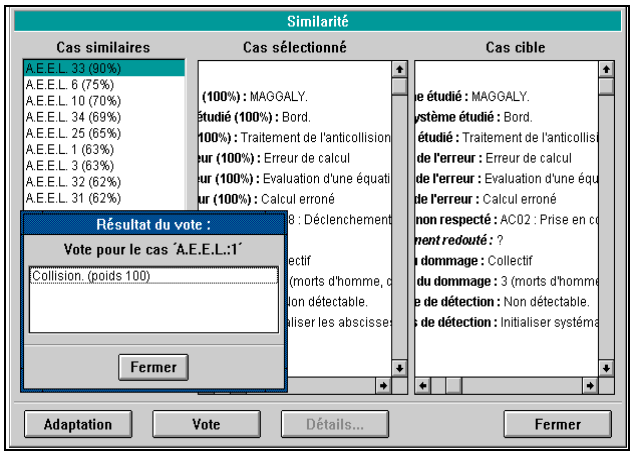

Figure 14. *Exemple d'utilisation de la méthode de vote pour la recherche de cas similaires.*

6. Conclusion

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 [HAJ 96]. 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 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 transports guidés. En particulier, l'exhaustivité et la pertinence des descripteurs retenus pour caractériser une AEEL nécessitent pour certains une étude plus approfondie.

REFERENCES

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

[DAR 95 a] 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*, Rapport de fin d'études d'ingénieur, sous la direction de Hadj-Mabrouk, INRETS, juin 1995

[DAR 95 b] DARRICAU M., HADH-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.

[DAR 96] DARRICAU M., HADH-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, 21-23 août 1996.

[GAN 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, 27 Mai 1987

[HAJ 07] HADH-MABROUK H., Ouvrage collectif : *« Chapitre 4 : Contribution du raisonnement à partir de cas à l'analyse des effets des erreurs du logiciel. Application à la sécurité des transports ferroviaires »*. Éditions Hermes - Lavoisier, pp 123-148, 2007.

[HAJ 05] HADH-MABROUK H., *Apport du raisonnement à partir de cas à l'analyse de la sécurité des logiciels dans les transports ferroviaires*, SETIT 2005, 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, March 27-31, 2005 – TUNISIA

[HAJ 03] HADH-MABROUK H., TRIKI I., *Évolution de la réglementation nationale en matière de sécurité ferroviaire*. Revue Annales des ponts et chaussées, Éditions ELSEVIER, nouvelle série n° 106, avril-juin 2003, pp 45-59.

[HAJ 00] HADH-MABROUK H., DARRICAU M., MEJRI L., *Contribution of case-- based reasonning tio the software error effect analysis*. International conference on artificial and computational intelligence for decision, controle and automation in ingeneering and industrial application. ACIDCA'2000, Tunisie 22-24 march 2000, pp 83-89

[HAJ 98] HADH-MABROUK H., *Acquisition et évaluation des connaissances de sécurité des systèmes industriels. Application au domaine de la certification*

des systèmes de transport guidés. Thèse d'Habilitation à Diriger des Recherches. Université de Technologie de Compiègne, février 1998.

[HAJ 96] HADH-MABROUK H., DARRICAU M., *SAUTREL : outil d'aide aux analyses des effets des erreurs de logiciels de sécurité dans les transports guidés*. LM 10, 10e Colloque national de fiabilité et maintenabilité, France, Saint-Malo, tome 2, pp 790-797, 1996.

[HAJ 92] HADH-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 en automatique industrielle et humaine . Université de Valenciennes, décembre 1992.

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

[IRS 92] IRSE Institution of Railway Signal Engineers, *Safety system validation with regard to cross acceptance of signalling systems by the railways*, IRSE, International Technical Committee, report n°1, 14 janvier 1992.

[KOD 86] KODRATOFF. Y., *Leçons d'apprentissage symbolique automatique*. Cepadues - Édition, 1986

[KOL 93] KOLODNER J., *Case-Based Reasoning*. Morgan-Kaufmann Publishers, Inc., 668 pages, 1993.

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

[NDI 96] 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 n° ESTAS/A-96-36, diffusion restreinte, 17 p, Arcueil, juin 1996.

[PIN 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, 1er octobre 1993.

[QUI 86] QUINLAN R., *Induction of Decision trees*, Machine Learning vol. 1, 1986, p 81-106.

[SLA 91] SLADE S., *Case-Based Reasoning : a Research Paradigm*, Artificial Intelligence Magazine vol.12, spring, 1991, pages 42 à 55.

[THI 86] : THIREAU PH., *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, 1986.