International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 13, Issue 1 (January 2017), PP.37-43

Case-Based Reasoning for the Evaluation of Safety Critical Software. Application to The Safety of Railway Transport.

Dr. Habib Hadj Mabrouk
French Institute Of Science And Technology For Transport, Spatial Planning, Development And Networks
14/20 Boulevard Newton, Champs Sur Marne, 77447 Marne La Vallée, France

ABSTRACT: The purpose of the work described in this paper is to improve the assessment of the safety analyses for railway transport systems in France. The modes of reasoning which are used in the context of safety analysis and the very nature of knowledge about safety mean that a conventional computing solution is unsuitable and the utilization of artificial intelligence techniques would seem to be more appropriate. The approach which was adopted in order to design and implement an assistance tool for safety analysis involved the following two main activities:
– Extracting, formalizing and storing hazardous situations to produce a library of standard cases which covers the entire problem. This process entailed the use of knowledge acquisition techniques;
– Exploiting the stored historical knowledge in order to develop safety analysis know-how which can assist experts to judge the thoroughness of the manufacturer's suggested safety analysis. This second activity involves the use of machine learning techniques in particular the use of Case-Based Reasoning.
This paper presents a mock-up of a tool for storing and assessing Software Error Effect Analysis (SEEA) for the safety of automatic devices of terrestrial guided transport system. The purpose of our work is to exploit historical SEEA, which have already been carried out on approved safety-critical software, in order to assess SEEA of new software.
Keywords: Software Error Effect Analysis (SEEA), Case-based reasoning, Machine learning, Railway safety, Assessment.

I. INTRODUCTION

In recent years knowledge based systems (KBS) have achieved a notable presence within the industry and are no longer considered to be rare products of research laboratories. However, it is unusual for these systems to reach the level of performance of human experts and they frequently fail to answer the real needs of end users. This is due to the difficulty of extracting the required knowledge from one or more experts in the domain and representing this knowledge without distortion in order to produce a cognitive model of the expert. A number of research projects have described the problem of collecting and formalizing the knowledge which is handled by experts while solving a problem. Experts may find it very difficult to describe in clear terms the stages of reasoning which they go through in order to make decisions. Such a description requires experts to undertake a long process of thought which will enable them to explain the unconscious aspect of their activities. The success of a KBS project depends on this difficult and sometimes painful task. In view of the complexity of the knowledge of experts and the difficulty which they have in explaining their mental processes there is a danger that the extracted knowledge will be either incorrect, incomplete or even inconsistent. A variety of research in Artificial Intelligence (AI) is in progress in an attempt to understand this problem of the transfer of expertise.

Research is currently taking place in two major independent areas:

- Knowledge acquisition, which aims to define methods for achieving a better grasp of the transfer of expertise. These methods chiefly involve software engineering and cognitive psychology [1], [2] and [3],
- Machine learning, which involves the use of inductive, deductive, abductive or analogical techniques in order to provide the KBS with learning capacities [4], [5], [6] and [7].

In order to develop a KBS which aids in safety analysis we combined these two approaches and used them in a complementary way [8]. One of the research activities which are currently in progress at the French institute lFSTTAR relates to the certification of automated public transport systems and the Safety of train control systems.

Our study took place within this context and aimed to design and create a software tool to assist certification experts in analysing and assessing the safety of critical security software and in particular to examine the adequacy of the protective measures proposed by the system manufacturer.

The purpose of this tool is to evaluate the completeness and consistency of the accident scenarios which have been put forward by the manufacturers and to play a role in generating new scenarios which could be of assistance to experts who have to reach a conclusion regarding the safety a new system. This paper presents a mock-up of a tool for storing and assessing Software Error Effect Analysis (SEEA) for the safety of automatic devices of terrestrial guided transport system. The purpose of our work is to exploit historical SEEA, which have already been carried out on approved safety-critical software, in order to assess SEEA of new software [9] and [10]. The production of this mock-up, in the process of validation, involves the use of Case-Based Reasoning (CBR) [11] and [12]. The basic principle of CBR is to deal with a new problem by remembering similar experiences which have occurred in the past.

II. THE PROCESS OF VALIDATION, APPROVAL AND CERTIFICATION

As part of its missions of expertise and technical assistance, IFSTTAR evaluates the files of safety of guided transportation systems. These files include several hierarchical analysis of safety such as the Preliminary hazard analysis (PHA),the functional safety analysis (FSA), the analysis of failure modes, their effects and of their criticality (AFMEC) or Software safety analysis and in particular the method Software Error Effect Analysis (SEEA). These analyses are carried out by the manufacturers. It is advisable to examine these analyses with the greatest care, so much the quality of those conditions, in fine, the safety of the users of the transport systems. Independently of the manufacturer, the experts of IFSTTAR carry out complementary analyses of safety. They are brought to imagine new scenarios of potential accidents to perfect the exhaustiveness of the safety studies. In this process, one of the difficulties then consists in finding the abnormal scenarios being able to lead to a particular potential accident. It is the fundamental point which justified this work.

Three main players, each with distinct roles, are involved in developing and operating an automated guide way transit system. This each is as follows [13]:

- The manufacturer validates the system. Validation consists of providing proof (demonstrations, calculations, test results etc.) that the system meets specifications, including those which relate to safety,
- The chief contractor (or the customer) approves the system. The customer grants approval on the basis of the results of the validation performed by the manufacturer, the safety dossier and any other tests and checks which he considers it to be worthwhile carrying out. During this phase the customer may call for an audit and/or the opinion of outside experts,
- The State or the local authority supervises that all those who are involved meet technical safety requirements.

It issues commissioning authorizations which may be withdrawn if there is a failure to comply with safety requirements which apply to design, manufacture or operation.

The commissioning authorization for the transport system is granted by the relevant State departments on the basis of the certification dossier. Certification is the official recognition that a function, a piece of equipment or a system complies with a set of national or international regulations. State departments generally make use of external audits or expert bodies such as IFSTTAR in order to draw up certification notices. IFSTTAR has as its main objectives the examination and evaluation of the development, validation and approval methods of the system. This process consists of devising new scenarios for potential accidents to ensure that safety studies are exhaustive. One of the difficulties involved in this process is finding abnormal scenarios which are capable of generating a specific hazard. This is the fundamental issue which inspired this study. There is a hierarchy of several ranked safety processes which are accepted by IFSTTAR and conducted by the manufacturer in order to identify hazardous situations, potential accidents, hazardous units or equipment and the severity of the consequences which would result [14]. These processes are as follows (figure1):

- Preliminary hazard analysis (PHA),
- Functional safety analysis (FSA),
- Hardware safety analysis (HSA),
- Software safety analysis (SSA).

The tool, which is the subject of this paper, provides assistance in particular during the phase in Software safety analysis (SSA). The Software safety analysis is generally based on the method of Software Error Effect Analysis (SEEA).

This paper presents a mock-up of a tool for storing and assessing Software Error Effect Analysis (SEEA) for the safety of automatic devices of terrestrial guided transport system. SEEA is an inductive process which attempts to determine the consequences and severity of software failures. This analysis is carried out by

envisaging software errors. It allows examining the consequences of these errors on other modules and the failures that ensue from them on the transport system. It also allows to [9]:

- Indicate in detail the modules needing examination and their safety-critical level;
- Estimate the validation effort on the software, guide the code inspection and better focus the tests;
- Suggest measures for detecting errors and increase the software quality.

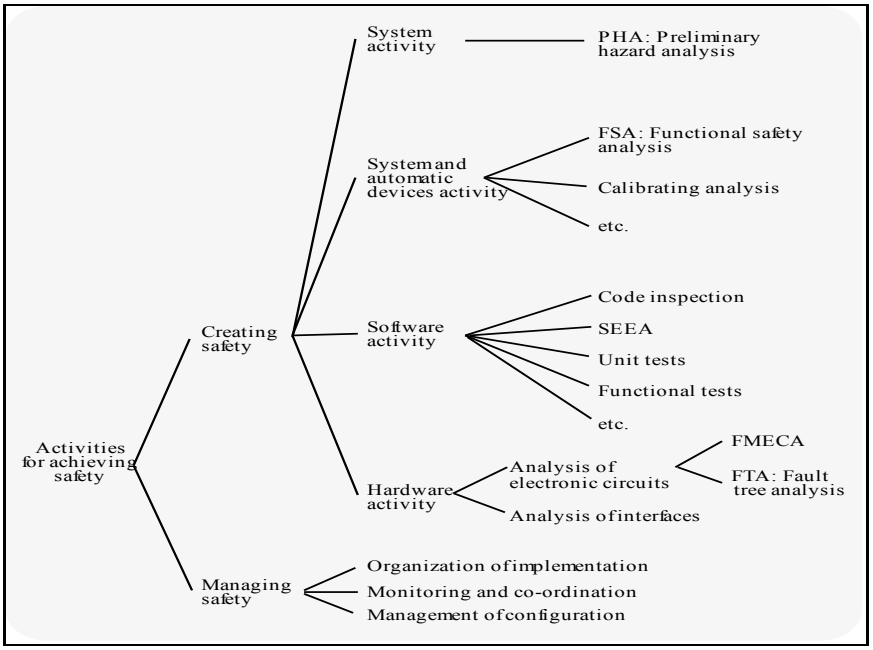

Fig.1: The methods of safety analysis of railway risks

III. MACHINE LEARNING: THE CASE BASED REASONING

Learning is a very general term which describes the process by which human beings or machines increase their knowledge. Learning therefore involves reasoning: discovering analogies and similarities, generalizing or particularizing an experience, making use of previous failures and errors in subsequent reasoning. The new knowledge is used to solve new problems, to carry out a new task or improve performance of an existing task, to explain a situation or predict behaviour [6]. This discipline is regarded as being a promising solution for knowledge acquisition aid and attempts to answer certain questions [4]: how can a mass of knowledge be expressed clearly, managed, added to and modified? Machine learning is defined by a dual objective: a scientific objective (understanding and mechanically producing phenomena of temporal change and the adaptation of reasoning) and a practical objective (the automatic acquisition of knowledge bases from examples). Learning may be defined as the improvement of performance through experience.

Learning is intimately connected to generalization [6]: learning consists of making the transition from a succession of experienced situations to knowledge which can be re-utilized in similar situations. Three types of problems are raised for each of the main learning techniques [4]. The first of these is grouping (which is termed classification in data analysis): given a certain mass of knowledge, how is it possible to discover links between the different items in order to group them into meaningful and simpler sub-groups?

The second problem (discrimination) is that of learning classification procedures: with a given set of examples of concepts, how is it possible to find a method which provides effective recognition of each concept? The third problem is that of generalization: how is it possible, on the basis of concrete examples of a situation, to find a formula which is sufficiently general to describe the situation in question and how is it possible to explain the descriptive ability of this formula?

The machine learning mechanism is based on four modes of reasoning or inference: induction, deduction, abduction and analogy.

The case based reasoning (CBR) research only looks for similarities or proximity relations between past situations and the current situation. The CBR [11] considers reasoning as a process of remembering a small set of practical situations: the cases, it bases its decisions on the comparison of the new situation (target cases) with the old (reference cases). The general principle of CBR is to treat a new problem (target case) by remembering similar past experiences (base case). This type of reasoning rests on the assumption that if a past experience and new circumstances are sufficiently similar, then everything can be explained or applied to past

experience (base case) and remains valid when applied to the new situation which represents the new problem to solve [9] (figure 2).

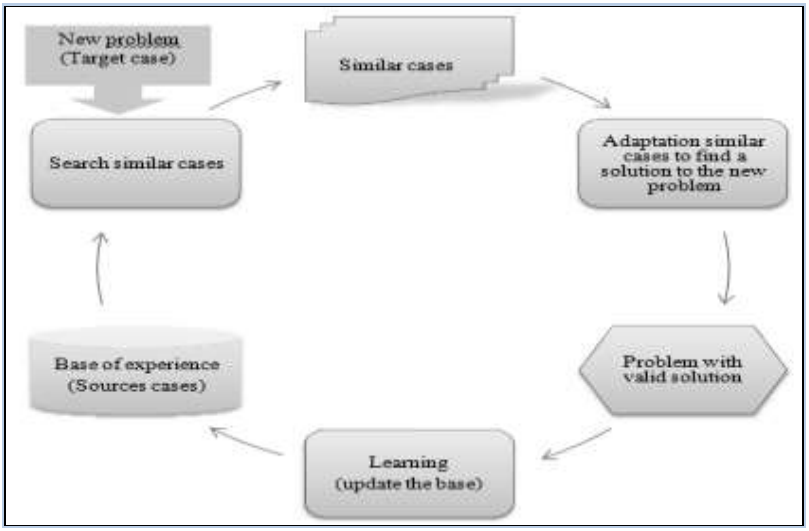

Fig.2: Cycle case based reasoning

IV. "SAUTREL": AN AID SYSTEM FOR THE SOFTWARE ERROR EFFECT ANALYSIS

The SAUTREL project takes place in the framework of software safety analyses, and deals with the method for analysing the effects of software errors (figure 3). SAUTREL assists in drawing up SEEA files for new software and helps also to assess their completeness and coherence. The design and implementation of SAUTREL involved the three following stages (figure 4):

- Knowledge representation and acquisition as regards SEEA. This analysis and abstraction stage resulted in the production of formalism for SEEA which takes account of the practices and experiences of IFSTTAR in this area. This model is based on eight characteristic parameters: the investigated system, the investigated subsystem, the investigated module, the envisaged error (family, class, type), the safety criterion infringed by the error, the feared hazard, the type and severity of possible damage and finally the means of detecting the error and protecting against it.
- Production of a base of SEEA cases. Using the above model we built up a library of 250 cases (examples). These historical examples of SEEAs were drawn from two guided transport systems: MAGGALY and the TVM 430 for the Nord TGV.
- Development of the SAUTREL tool [15]. The mock-up has four main modules: a man/machine interface for inputting, updating and consulting knowledge relating to SEEA, a representation and acquisition module for SEEA sheets, a knowledge base containing 250 examples of SEEA (experience base), and a case-based reasoning process (implemented by the ReCall software). The main components of this CBR process are a mechanism which indexes (or characterizes) target cases and a mechanism which finds similar cases (reference cases) and collects them together.

V. EXAMPLE OF THE MOCK-UP USE

The mock-up has been implemented using the ReCall software, marketed by ISoft firm, which generates CBR process. The following paragraphs show, through an example the use of this mock-up, which requires to go through the eight following stages [16]:

1. Definition of SEEA instances description language (figure 5),
2. Construction of the SEEA base (figure 6),
3. Calibrating the CBR process (figure 7),
4. Input of the SEEA for assessment,
5. Indexation of the SEEA base,
6. Extraction of the similar cases,
7. Adaptation of the extracted cases (figure 8),
8. Updating the SEEA base.

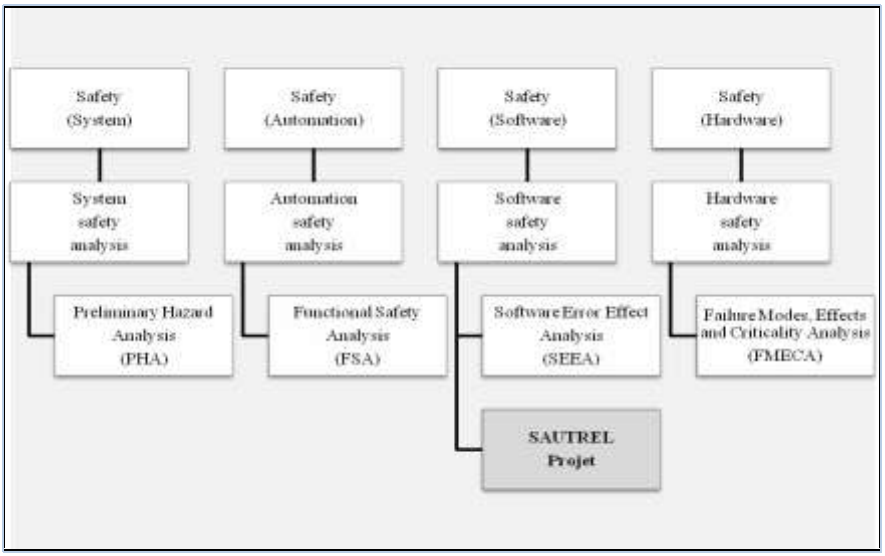

Fig.3: Place of SAUTREL project in the safety analysis for railway transport

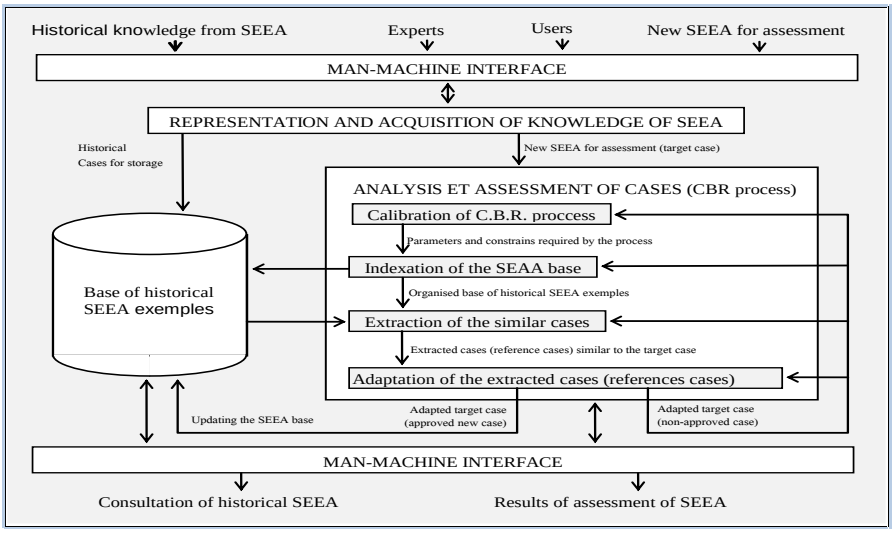

Fig.4: Functional architecture of the SAUTREL mock-up

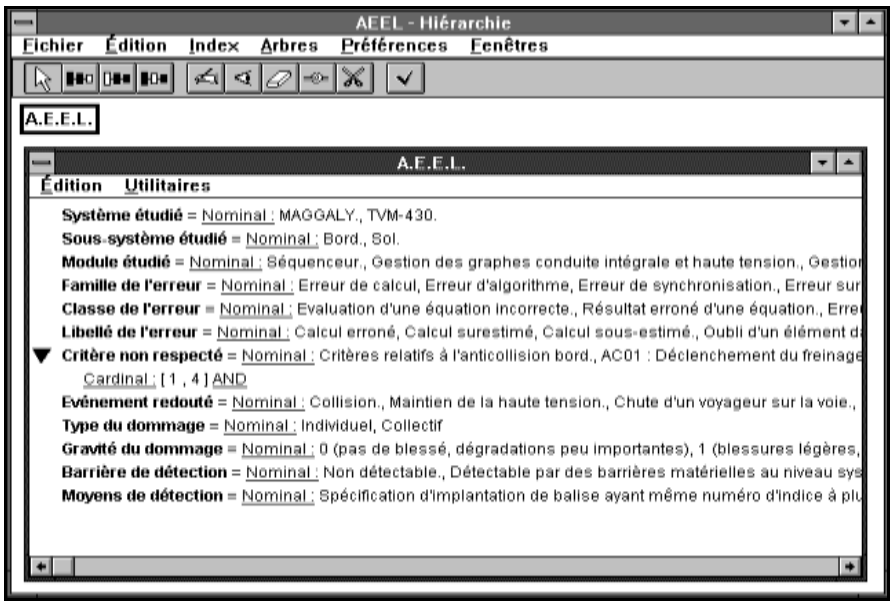

Fig.5: Definition of SEEA instances description language.

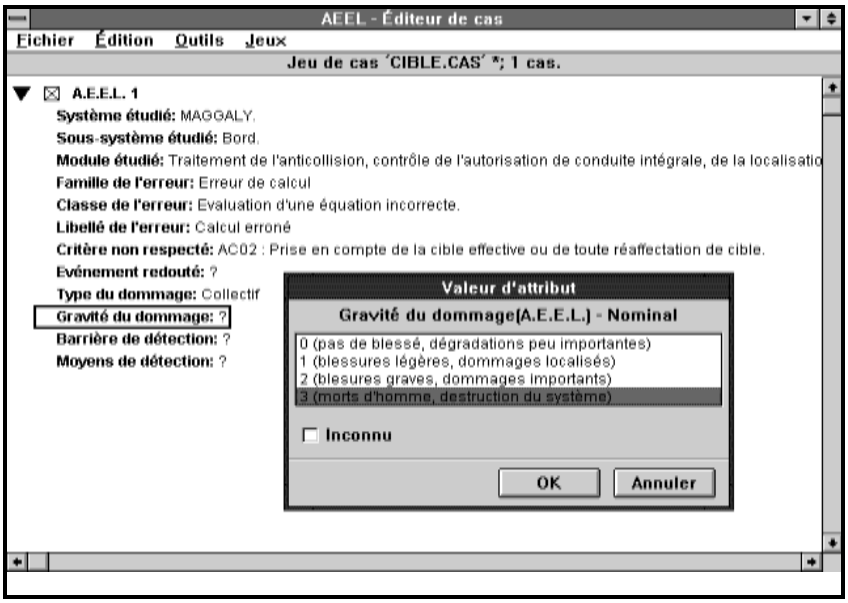

Fig.6: Example of the input of a target case

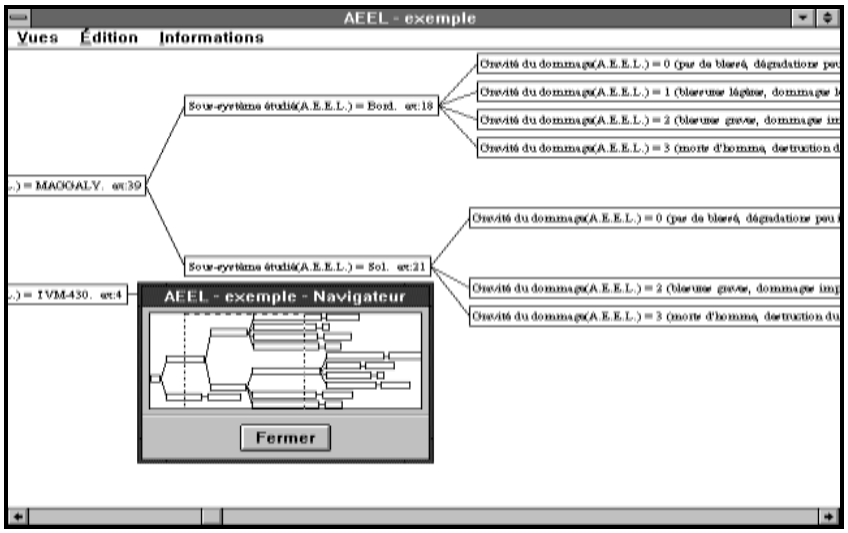

Fig.7: Example of the instances base hierarchy

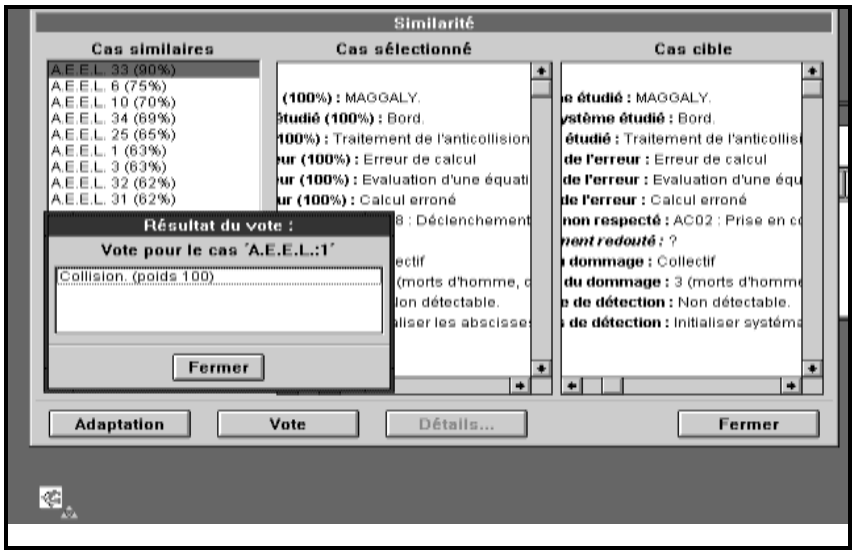

Fig.8: Example of the reference cases consultation and the vote technique use.

VI. CONCLUSIONS

This paper has presented our contribution to the improvement of the methods which are normally used to analyze and assess the safety of automatic devices in guided transport systems. This contribution is based on the use of artificial intelligence techniques (in particular the case-based reasoning) and has involved the development of several approaches and tools which assist in the modeling, storage and assessment of knowledge about safety. SAUTREL project has two main purposes, firstly to record and store experience concerning safety analyses, and secondly to assist those involved in the development and assessment of the systems in the demanding task of evaluating safety studies and in particular the method of Software Error Effect Analysis (SEEA). Currently, the SAUTREL project is at the mock-up stage. Initial validation has demonstrated the interest of the suggested approaches, but improvements and extensions are required before they could be used in an industrial environment or adapted to other areas where the problem of investigating safety arises.

REFERENCES

[1]. R. Dieng, "Méthodes et outils d'acquisition des connaissances", ERGO IA90, Biarritz, France, 19 à 21 septembre 1990.

[2]. B.R. Gaines, "Knowledge acquisition: past, present, and future. International", Journal of Human–Computer Studies, http://dx.doi.org/10, 1016/j.ijhcs, 2012.

[3]. G. Aussenac and F. Gandon, "From the knowledge acquisition bottleneck to the knowledge acquisition overflow: A brief French history of knowledge acquisition", International Journal of Human-Computer Studies, vol. 71, n°2, pp. 157-165, 2013

[4]. Y. Kodratoff, "Leçons d'apprentissage symbolique automatique", Cepadues éd., Toulouse, France, 1986

[5]. J.-G Ganascia "L'intelligence artificielle", Cavalier Bleu Eds, Mai 2007.

[6]. J.-G. Ganascia, "Logical Induction, Machine Learning and Human Creativity", in SWITCHING CODES, University of Chicago Press, ISBN 978022603830, 2011

[7]. R-S.Michalski, and J. Wojtusiak, "Reasoning with Missing, Not-applicable and Irrelevant Meta-values in Concept Learning and Pattern Discovery", Journal of Intelligent Information Systems, 39, 1, 141-166, Springer, 2012.

[8]. H. Hadj Mabrouk, and H. Mejri, "ACASYA: a knowledge-based system for aid in the storage, classification, assessment and generation of accident scenarios. Application to the safety of rail transport systems", ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 4, No.16, 2015.

[9]. H. Hadj-Mabrouk, "Contribution du raisonnement à partir de cas à l'analyse des effets des erreurs du logiciel. Application à la sécurité des transports ferroviaires ", Ouvrage collectif, chapitre 4, Éditions Hermes - Lavoisier, pp 123-148, 2007.

[10]. H. Hadj-Mabrouk, A. Maalel and F. Hamdaoui, "Contribution du raisonnement à partir de cas à l'évaluation des logiciels de sécurité", SETIT2009: 5th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications March 22-26, Tunisia, 2009

[11]. J. Kolodner, "Case-Based Reasoning", Morgan-Kaufmann Pub. Inc., 668p, 1993

[12]. P. Harmon, "Case-based reasoning II, Intelligent Software Strategies", vol. 7, p1-9, 1991

[13]. H. Hadj Mabrouk, "Methods and tools to assist the acquisition, modeling, capitalization and assessment of the safety of transport", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 6, Issue 8, 2016

[14]. H. Hadj Mabrouk, "CLASCA: learning system for classification and capitalization of accident Scenarios of Railway", Journal of Engineering Research and Application, ISSN 2248-9622, Vol. X, Issue X, 2016.

[15]. M. Darricau and H. Hadj-Mabrouk, "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 ses applications, Paris-La-Défense, Nov. 15-17, pp 677-689, 1995

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