International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 8, August 2016)

Methods and Tools to Assist the Acquisition, Modelling, Capitalization and Assessment of the Safety of Transport

Dr. Habib Hadj-Mabrouk

IFSTTAR

French Institute of Science And Technology, for Transport, Development and Networks, 14-20 Boulevard Newton, F-77447 Marne La Vallée, France

Abstract— **This The purpose of the work described in this paper 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,
- 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.

The approach used to achieve this is mainly based on the use of artificial intelligence techniques, in particular knowledge acquisition and modelling techniques, knowledge-based systems, automatic symbolic learning techniques and knowledge validation techniques. This paper presents a general description of four mock-ups of tools which are intended to aid in the analysis and investigation of safety.

Keywords—**Railway transport, Safety, Assessment, Accident prevention, Case-based reasoning, Learning the rules, Expert systems, Knowledge acquisition.**

I. INTRODUCTION

Three main players, each with distinct roles, are involved in developing and operating an automated guide way transit system. This each is as follows [1]:

– 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. These agents, who are responsible for checking the system essentially as regards safety, are allowed access to all technical documents and all test sites. IFSTTAR has as its main objectives the examination and evaluation of the development, validation and approval methods of the system. This activity involves the main stages of checking:

– That the principle standards involved have been correctly applied,
– That the safety objectives are acceptable,
– The quality of the supplied documentation is satisfactory in terms of clarity, consistency and completeness,
– The suitability of the methods and techniques which have been used to demonstrate safety,
- The methods of work, organization and the means implemented in order to design, construct, validate and check the hardware and software equipment which performs safety functions.

The IFSTTAR experts carry out additional analyses of safety independently of manufacturer. 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. These processes are as follows [1] (figure 1):

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

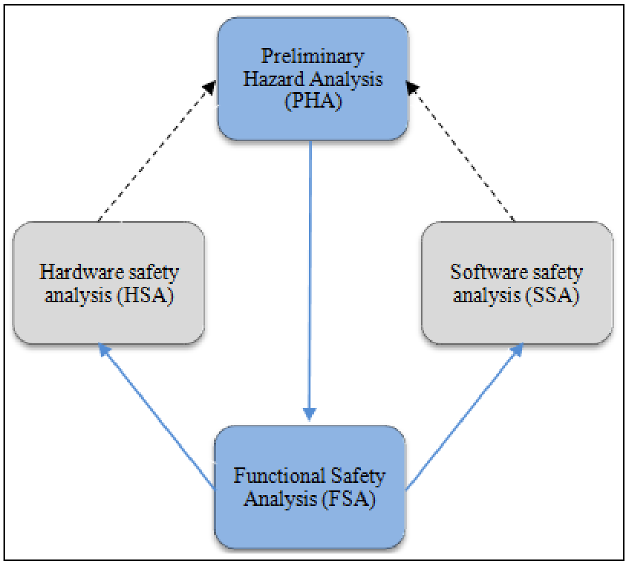

Preliminary Hazard Analysis (PHA)
Hardware safety analysis (HSA)
Software safety analysis (SSA)
Functional Safety Analysis (FSA)

Figure 1: hierarchical process safety analysis

The modes of reasoning which are used in the context of safety analysis (inductive, deductive, analogical, etc.) and the very nature of knowledge about safety (incomplete, evolving, empirical, qualitative, etc.) mean that a conventional computing solution is unsuitable and the utilization of artificial intelligence techniques would seem to be more appropriate. Our research has involved three specific aspects of artificial intelligence: knowledge acquisition, machine learning and knowledge based systems. Development of the knowledge base in a KBS requires the use of knowledge acquisition techniques in order to collect, structure and formalizes knowledge. It has not been possible with knowledge acquisition to extract effectively some types of expert knowledge. Therefore, the use of knowledge acquisition in combination with machine learning appears to be a very promising solution. The approach which was adopted in order to design and implement assistance several tools 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 is called a historical scenario knowledge base (HSKB). 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 combined with expert systems.

This article presents the results of these research activities which are involved in the methodology of safety analysis of guided rail transport systems.

II. Methodological Approach For The Acquisition Of Safety Knowledge

Knowledge acquisition was recognized as a bottle neck from the first appearance of expert systems, or more generally knowledge based systems (KBS). It is still considered to be a crucial task in their creation. Extraction or elicitation refers to the collection of knowledge from experts in the field whereas the concepts of transfer or transmission of expertise refer to the collection and subsequent formalization of the knowledge of a human expert. The term knowledge acquisition refers to all the activities which are required in order to create the knowledge base in an expert system. Knowledge acquisition (KA) is one of the central concerns of research into KBSs and one of the keys not only to the successful development of a system of this type but also to its integration and utilization within an operational environment.

Two main participants are involved in KA: the expert, who possesses know-how of a type which is difficult to express, and the cognitive scientist who has to extract and formalize the knowledge which is related to this know-how, which as far as the expert is concerned is usually implicit rather than explicit. This time-consuming and difficult process is nevertheless fundamental to the creation of an effective knowledge base. While KA was at the outset centered around the expert/cognitive scientist pairing it very soon raised crucial problems such as the identification of the needs of users or the selection of a means of representing knowledge. The excessive divergence between the language which the experts used in order to describe their problem and the level of abstraction used in representational formalizations of knowledge provided the motivation for a large amount of research aimed at facilitating the transfer of expertise.

The new KA approaches aim to specify more effective methodologies and to design software's which assist or partially replace the cognitive scientist [2]. Some work suggests viewing the design of a KBS as a process of constructing a conceptual model, on the basis of all the available sources of knowledge (human or documentary) which relate to solving the problem. In this context KA is perceived as a modeling activity. Other research stresses the benefits of methods which guide the cognitive scientist in the transfer/modeling process. Tools and techniques are used to provide assistance with verbalization, interviews with experts and document analysis. Currently available KA techniques mainly originate in cognitive psychology (human reasoning models, knowledge collection techniques), ergonomics (analysis of the activities of experts and the future user), linguistics (to exploit documents more effectively or to guide the interpretation of verbal data) and software engineering (description of the life cycle of a KBS) [2].

In summary, KA may be defined as being those activities which are necessary in order to collect, structure and formalize knowledge in the context of the design of a KBS. A survey of state of the art research in the domain of knowledge acquisition made it possible to select a method for developing a KBS for aid in the analysis of safety for automated terrestrial transport systems. This method showed itself to be useful for extracting and formalizing historical safety analysis knowledge (essentially accident scenarios) and revealed its limits in the context of the expert safety analysis, which is particularly based on intuition and imagination. In general, current knowledge acquisition techniques have been designed for clearly structured problems. They do not tackle the specific problems associated with multiple areas of expertise and the coexistence of several types of knowledge and it is not possible to introduce the subjective and intuitive knowledge which is related to a rapidly evolving and unbounded field such as safety. Although cognitive psychology and software engineering have produced knowledge acquisition methods and tools, their utilization is still very restricted in a complex industrial context.

Transcribing verbal (natural) language into a formal language which can be interpreted by a machine often distorts the knowledge of the expert. This introduces a bias in passing from the cognitive model of the expert to the implemented model. This disparity is in part due to the fact that the representational languages which are used in AI are not sufficiently rich to explain the cognitive function of experts and in part to the subjective interpretation of the cognitive scientist. These constraints act together to limit progress in the area of knowledge acquisition [2].

One possible way of reducing these constraints is combined utilization of knowledge acquisition and machine learning techniques. Experts generally consider that it is simpler to describe examples or experimental situations than it is to explain decision making processes. Introducing machine learning systems which operate on the basis of examples can generate new knowledge which can assist experts in solving a specific problem. The know-how of experts depends on subjective, empirical, and occasionally implicit knowledge which may give rise to several interpretations.

There is generally speaking no scientific explanation which justifies this compiled expertise. This difficulty emanates from the complexity of expertise which naturally encourages experts to give an account of their know-how which involves significant examples or scenarios which they have experienced on automated transport systems which have already been certified or approved. Consequently, expertise should be updated by means of examples. Machine learning can facilitate the transfer of knowledge, particularly when its basis consists of experimental examples.

It contributes to the development of the knowledge bases while at the same time reducing the involvement of cognitive scientists.

In our approach, learning made use of the HSKB to generate new knowledge likely to assist experts evaluates the degree of safety of a new transport system. 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 [3], [4] [5], [6] and [7].

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 behavior. The design of knowledge acquisition aid tools which include learning mechanisms is essential for the production and industrial development of KBSs. This discipline is regarded as being a promising solution for knowledge acquisition aid and attempts to answer certain questions [5]: 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 [3]: learning consists of making the transition from a succession of experienced situations to knowledge which can be re-utilized in similar situations. Expertise in a domain is not only possessed by experts but is also implicitly contained in a mass of historical data which it is very difficult for the human mind to summarize. One of the objectives of machine learning is to extract relevant knowledge from this mass of information for explanatory or decision making purposes. However, learning from examples is insufficient as a means of acquiring the totality of expert knowledge and knowledge acquisition is necessary in order to identify the problem which is to be solved and to extract and formalize the knowledge which is accessible by customary means of acquisition. In this way each of the two approaches is able to make up for the shortcomings of the other.

In order to improve the process of expertise transfer, it is therefore beneficial to combine both processes in an iterative knowledge acquisition process. Our approach has been to exploit the historical scenario knowledge base by means of learning with a view to producing knowledge which could provide assistance to experts in their task of evaluating the level of safety of a new system of transport [1].

The approach which was adopted involved the following two main activities (Figure 2):

- Extracting, formalizing and storing hazardous situations to produce a library of standard cases which covers the entire problem. This is called a historical scenario knowledge base (HSKB). 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.

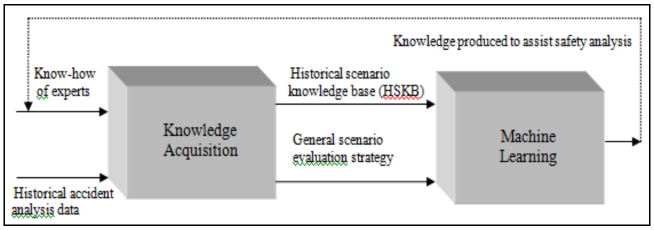

Knowledge produced to assist safety analysis
Know-how of experts
Historical accident analysis data
Knowledge Acquisition
Historical scenario knowledge base (HSKB)
General scenario evaluation strategy
Machine Learning

Figure 2: The general processes of safety knowledge acquisition

III. Methods And Tools To Assist The Acquisition, Capitalization And Assessment Of The Safety

This knowledge-building approach has been applied to the field of rail transport safety. She uncorked on the design and implementation of four complementary research projects (Figure 3):

1. Project CLASCA for capitalization assistance and classification of accident scenarios and in particular for the preliminary hazard analysis (PHA),
2. Project EVALSCA for help in assessing and preventing risks of accidents and especially for functional safety analysis (FSA),
3. Project SAUTREL for help in analyzing critical software safety and in particular analyzes of the effects, software errors (SEEA),
4. Project SASEM for help in analyzing hardware safety and especially the analysis of failure modes, effects and criticality of their (FMECA).

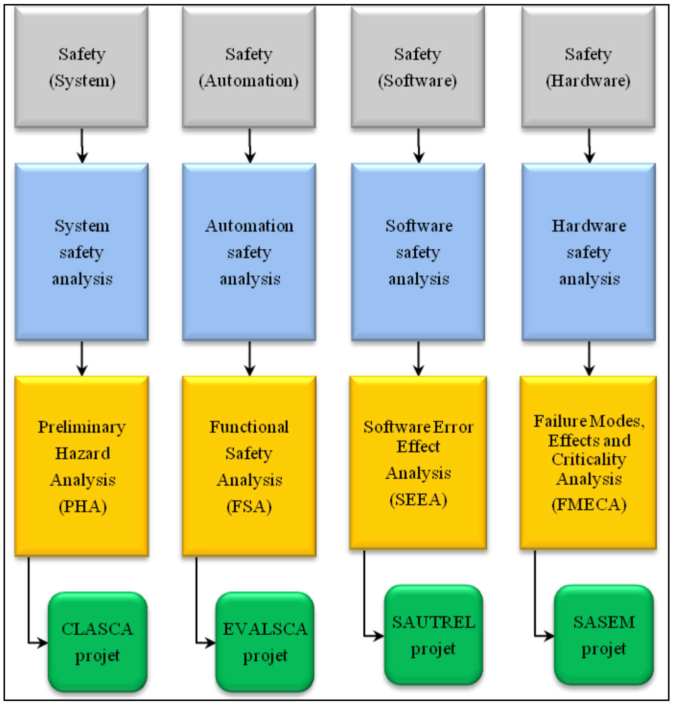


Figure 3: The safety analysis methods and associated research projects

IV. The General Principle Of The "CLASCA" System

The purpose this is to provide the expert with historical scenarios which are partially or completely similar to the new scenario.

This mode of reasoning is analogous to that which experts use when they attempt to find similarities between the situations which have been described by the manufacturer's scenarios and certain experienced or envisaged situations involving equipment which has already been certified and approved.

Classification of a new scenario involves the two following stages (figure 4):

– A characterization (or generalization) stage for constructing a description for each class of scenarios. This stage operates by detecting similarities within a set of historical scenarios in the HSKB which have been pre-classified by the expert in the domain,

– A deduction (or classification) stage to find the class to which a new scenario belongs by evaluating a similarity criterion. The descriptors of the new scenario (static description) are compared with the descriptions of the classes which were generated previously.

This initial level of processing not only provides assistance to the expert by suggesting scenarios which are similar to the scenario which is to be dealt with but also reduces the space required for evaluating and generating new scenarios by focusing on a single class of scenarios Ck.

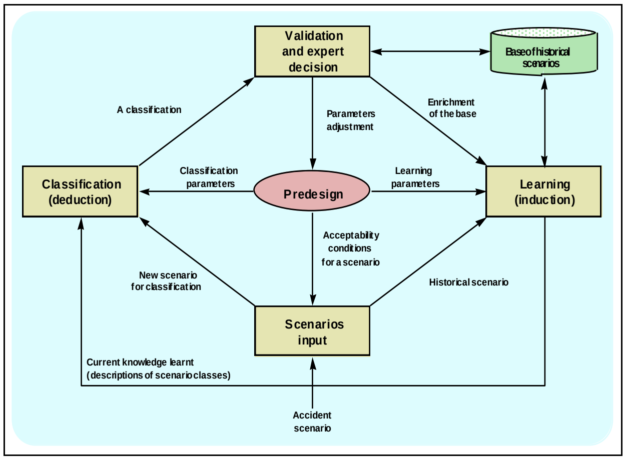

Validation and expert decision
Base of historical scenarios
A classification
Parameters adjustment
Enrichment of the base
Classification (deduction)
Classification parameters
Predesign
Learning parameters
Learning (induction)
Acceptability conditions for a scenario
New scenario for classification
Historical scenario
Scenarios input
Current knowledge learnt (descriptions of scenario classes)
Accident scenario

Figure 4: functional architecture of the CLASCA system

A. *Induction of descriptions of classes of scenarios*

This stage involves generalizing the classes which have been pre-defined by the experts in order to generate a comprehension description for each class which both characterizes the division which has been conducted by the expert and makes it possible to identify to which class the new example belongs. Each description which is learnt is characterized by a combination of three elements: (<Attribute> <Value> <Frequency>).

The frequency of appearance is computed for each descriptor (attribute/value) in order to limit the loss of information. As an example, figure 6 shows the characteristic description of the initialization sequence class which was generated by CLASCA. The description of a class is further enriched by taking into account the associated summarized failures (SF) which are involved. These SFs will subsequently be exploited in order to develop the base of learning examples.

B. *Classification of a new example of a scenario*

In this stage a new example of a scenario is assigned to an existing class Ck. For this it is necessary to define a classification criterion which measures the degree of resemblance between the new example and each of the pre-existing classes.

This similarity criterion is based on statistical calculations and takes account of the semantics of the domain of application. In the situation where CLASCA has assigned the new example of a scenario to a class, this class needs to be updated. The updating process generates four situations as below:

– The phenomenon of particularization of descriptors: descriptors which are considered characteristic at the instant t may lose their significance at the instant (t+1),

– The phenomenon of generalization of descriptors: descriptors which are considered not to be meaningful may become characteristic,

– Phenomena of simultaneous particularization and generalization,

– The learning of new descriptors which enrich the description of the class.

This phenomenon of descriptor changeability demonstrates the no monotonic character of learning in CLASCA.

V. THE GENERAL PRINCIPLE OF THE “EVALSCA” SYSTEM

EVALSCA which is a mock-up for an expert system providing aid for the appraisal of accident scenarios. The purpose of this mock-up, which was developed around the CHARADE rule learning tool [3], is to bring to the attention of experts any failures which were not considered during safety analysis. The evaluation approach is centered around the summarized failures (SFs) which are involved in the manufacturer's scenario. The evaluation of a scenario of this type involves the two modules below (Figure 5):

- A mechanism for learning rules CHARADE [3] which makes it possible to deduce SF recognition functions and thus generate a base of evaluation rules,

- An inference engine which exploits the above base of rules in order to deduce which SFs are to be considered in the manufacturer's scenario.

CHARADE is a learning system whose purpose is to construct knowledge based systems on the basis of examples. It makes it possible to generate a system of rules with specific properties. Rule generation within charade is based on looking for and discovering empirical regularities which are present in the entire learning sample. Regularity is a correlation which is observed between descriptors in the base of learning examples.

If all the examples in the learning base which possess the descriptor d1 also possess the descriptor d2 it can be inferred that d1 → d2 in the entire learning set. In order to illustrate this rule generation principle let us assume that there is a learning set which consists of three examples E1, E2, and E3.

E1 = d1 & d2 & d3 & d4
E2 = d1 & d2 & d4 & d5
E3 = d1 & d2 & d3 & d4 & d6

CHARADE can in this case detect an empirical regularity between the combination of descriptors (d1 & d2) and the descriptor d4. All those examples which are described by d1 & d2 are also described by d4.

The rule d1 & d2 → d4 is obtained.

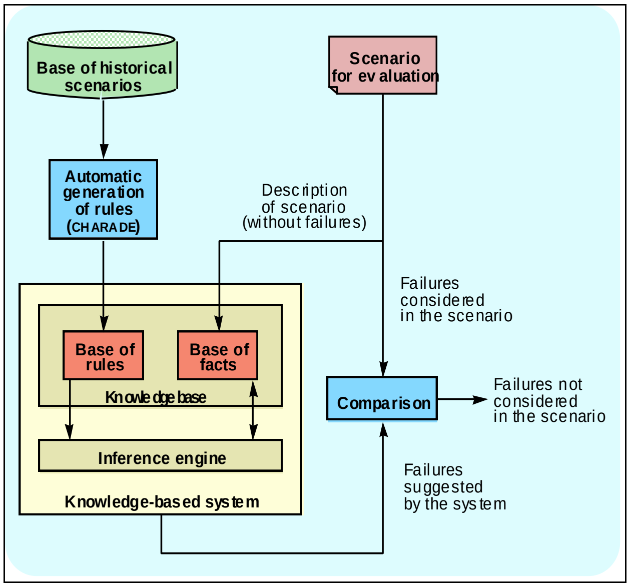

Base of historical scenarios
Scenario for evaluation
Automatic generation of rules (CHARADE)
Description of scenario (without failures)
Failures considered in the scenario
Base of rules
Base of facts
Knowledge base
Inference engine
Knowledge-based system
Comparison
Failures not considered in the scenario
Failures suggested by the system

Figure 5: functional architecture of the EVALSCA system

The purpose of the EVASCA module is to compare the list of SFs which are suggested in a manufacturer scenario to the list of stored historical SF in order to stimulate the formulation of hazardous situations which have not been anticipated by the manufacturer. This evaluation task draws the attention of the expert to any failures which have not been considered by the manufacturer and which might jeopardize the safety of the transport system. It may thus promote the generation of new accident scenarios.

This phase of learning attempts, using the base of examples which was formed previously, to generate a system of rules. The purpose of this stage is to generate a recognition function for each SF associated with a given class. The SF recognition function is a production rule which establishes a link between a set of facts (parameters which describe a scenario or descriptors) and the SF fact. What is involved here is logical dependence, which can be expressed in the following form:

If the facts TBS, H, HRF, GZ, EI, if are shown to be true
Then the consequence is the fact (or descriptor) **SF**

A base of evaluation rules can be generated for each class of scenarios. The conclusion of each rule which is generated should contain the SF descriptor or fact. It has proved to be inevitable to use a learning method which allows production rules to be generated from a set of historical examples (or scenarios). The specification of the properties required by the learning system and a review of the literature has led us to choose the CHARADE mechanism. Charade's ability to generate automatically a system of rules, rather than isolated rules, and its ability to produce rules in order to develop SF recognition functions make it of undeniable interest. A sample of some rules generated by CHARADE is given below. These relate to the “initialization sequence” class.

If Elements_involved = mobile_operator,
Incident_functions = instructions,
Elements-involved = operator_in_pcc.
Then Sumarized Failures = **SF11** (invisible element on the zone of completely automatic driving),
Elements_involved = AD_with_redundancy,
Hazard_related_functions =train localization,
Geographical_zones = terminus.
.

During the previous stage the CHARADE module created a system of rules on the basis of the learning examples.

The SF deduction stage requires a preliminary phase during which the rules which have been generated are transferred to an expert system in order to construct a scenario evaluation knowledge base. This evaluation knowledge base contains the following [1] (figure 5):

- The base of rules, which is split into two parts: a current base of rules which contains the rules which CHARADE has generated the instant t and a store base of rules, which consists of the list of historical bases of rules. Once a scenario has been evaluated, a current base of rules becomes a store base of rules;
- The base of facts, which contains the parameters which describe the manufacturer's scenarios which are to be evaluated.

The scenario evaluation knowledge base which has been described above (base of facts and base of rules) is exploited by forward chaining by an inference engine and generates the summarized failures which must enter into the description of the manufacturer's scenario which is to be evaluated. In the example we are considering the expert system deduced the failure SF19. The result of the deduction is given below:

```
@@   03/08/2016
     -Moving_block,
     -Collision,
     -Management_of_automatic_driving,
     -Train_monitoring,
     -Initialization,
     -Terminus,
     -Operator_at_cc,
     -Ad_without_redundancy,
     -Instructions
DEDUCTION: Summarized failure = SF19 (Silent train)
```

The plausible SFs which the expert system has deduced are analyzed and compared to the SFs which have actually been considered by the manufacturer. One or more SFs which jeopardize the safety of the transit system and which have not been considered by the manufacturer during the design of protection equipment may emerge from this comparison. The above suggestion may assist in generating unsafe situations which have not been foreseen by the manufacturer.

VI. THE GENERAL PRINCIPLE OF THE "SAUTREL" SYSTEM

This paragraph 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 Software safety analysis is generally based on the method of Software Error Effect Analysis (SEEA).

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[8]:

- 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.

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. The production of this mock-up, in the process of validation, involves the use of Case-Based Reasoning (CBR). The basic principle of CBR is to deal with a new problem by remembering similar experiences which have occurred in the past.

A. *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. Learning is intimately connected to generalization: learning consists of making the transition from a succession of experienced situations to knowledge which can be re-utilized in similar situations. The machine learning mechanism is based on four modes of reasoning or inference: induction, deduction, abduction and analogy.

The case based reasoning (CBR) [9] research only looks for similarities or proximity relations between past situations and the current situation. The C.B.R. 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 (figure 6) 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 [10].

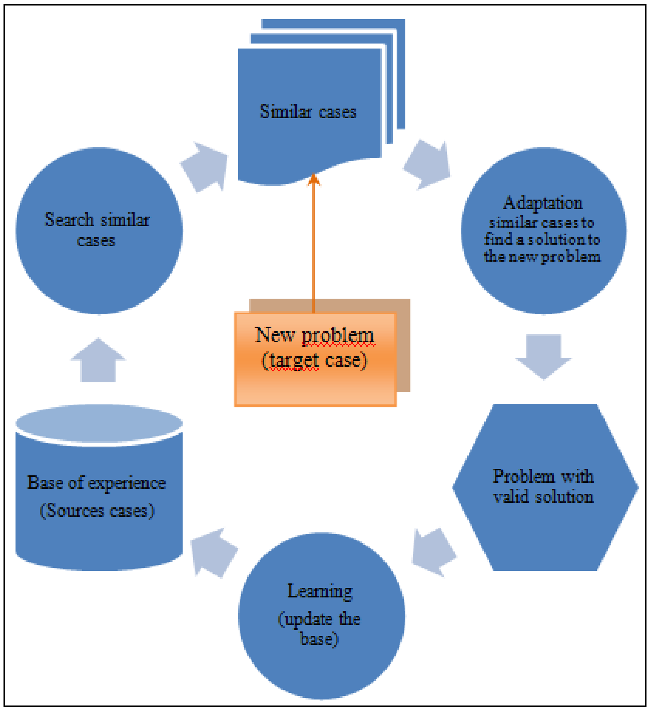

Similar cases
Search similar cases
Adaptation similar cases to find a solution to the new problem
New problem (target case)
Base of experience (Sources cases)
Problem with valid solution
Learning (update the base)

Figure 6: Cycle case based reasoning

B. *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 analyzing the effects of software errors (SEEA - Software Error Effect Analysis). 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 [8] and [10] (figure 7):

1. 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.
2. 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.
3. Development of the SAUTREL tool [8] and [10]. 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.

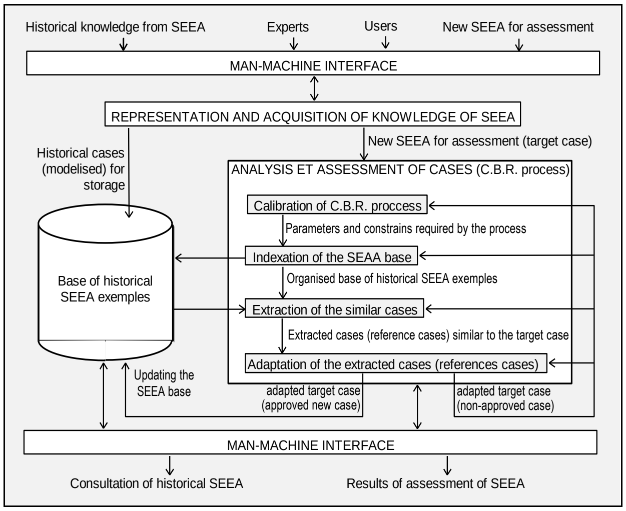
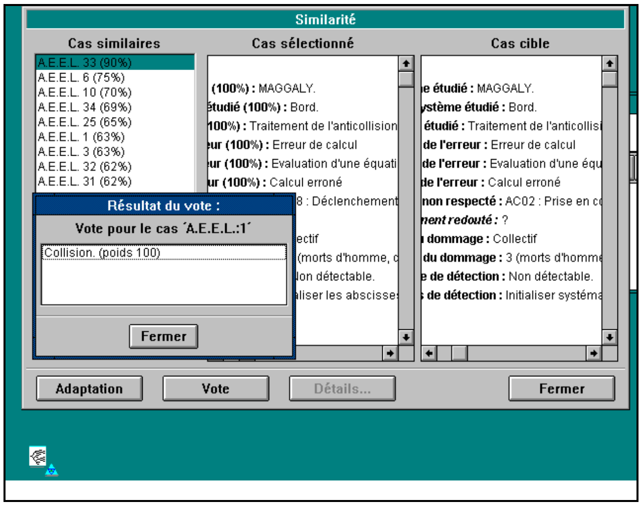

Historical knowledge from SEEA
Experts
Users
New SEEA for assessment
MAN-MACHINE INTERFACE
REPRESENTATION AND ACQUISITION OF KNOWLEDGE OF SEEA
New SEEA for assessment (target case)
Historical cases (modelised) for storage
ANALYSIS ET ASSESSMENT OF CASES (C.B.R. process)
Calibration of C.B.R. proccess
Parameters and constrains required by the process
Indexation of the SEAA base
Organised base of historical SEEA exemples
Base of historical SEEA exemples
Extraction of the similar cases
Extracted cases (reference cases) similar to the target case
Adaptation of the extracted cases (references cases)
Updating the SEEA base
adapted target case (approved new case)
adapted target case (non-approved case)
MAN-MACHINE INTERFACE
Consultation of historical SEEA
Results of assessment of SEEA

Figure 7: Functional architecture of the SAUTREL mock-up

C. *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 [8] and [10]:

1. Definition of SEEA instances description language,
2. Construction of the SEEA base,
3. Calibrating the CBR process,
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 (reference cases),
8. Updating the SEEA base.



A.E.E.L. 33 (90%)
A.E.E.L. 6 (75%)
A.E.E.L. 10 (70%)
A.E.E.L. 34 (69%)
A.E.E.L. 25 (65%)
A.E.E.L. 1 (63%)
A.E.E.L. 3 (63%)
A.E.E.L. 32 (62%)
A.E.E.L. 31 (62%)

(100%) : MAGGALY.
étudié (100%) : Bord.
100%) : Traitement de l'anticollision
eur (100%) : Erreur de calcul
eur (100%) : Evaluation d'une équati
ur (100%) : Calcul erroné
8 : Déclenchement
ectif
(morts d'homme, c
Non détectable.
aliser les abscisse

e étudié : MAGGALY.
ystème étudié : Bord.
étudié : Traitement de l'anticollisi
de l'erreur : Erreur de calcul
de l'erreur : Evaluation d'une équ
de l'erreur : Calcul erroné
non respecté : AC02 : Prise en co
nent redouté : ?
dommage : Collectif
du dommage : 3 (morts d'homme
e de détection : Non détectable.
s de détection : Initialiser systéma

Vote pour le cas ´A.E.E.L.:1´
Collision. (poids 100)

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

VII. THE GENERAL PRINCIPLE OF THE "SASEM" SYSTEM

This goal of the research is to study the feasibility of a knowledge-based system to help the capitalization and the evaluation of the Analyses of the Modes of Failure, of their Effects and Criticality hardware. The knowledge base has been developed from the data involved in Failure Modes, Effects and Criticality Analysis (FMECA) of three systems of rail transport put in service in France: the system Val of Lille, the TVM system 430 of the TGV Nord and the system MAGGALY of Lyon.

"SASEM" is an expert system for the analysis of the modes of failure, of their effects and their criticality.

The analysis of the Failure Modes and their Effects (FMECA) is an inductive method to perform an analysis of the failure modes of the components, their causes, and their effects on the system. Generally, there are four steps to achieve a FMECA:

- Definition of the system, its functions and components,
- Establishment of the failure modes of the components and their possible causes,
- Study and evaluation of the modes of failure on the functions of the system,
- Conclusions and recommendations.

A natural extension of the FMECA is the analysis of the modes of failure, of their effects and criticality. For each failure mode, it allows to assess the couple "probability-gravity". The more likely it is and the more the effects are considered penalising, more the criticality of the failure mode is important and the more it becomes necessary to take corrective and/or preventative measures.

The objective of the study is to exploit the historic FMECA envisaged on equipment certified material such as that of the system the TVM430 of the TGV-Nord with a view to analyze and examine the completeness, consistency and relevance of the FMECA of a new system of rail transport. This section presents the main results of a research on the development of an expert system to help the capitalization and the evaluation of the FMECA in terms of completeness and consistency.

The study of the feasibility of an expert system of assistance to FMECA has led to the following results [11]:

- Development of a new model of representation of the FMECA,
- Constitution of a knowledge base of the FMECA,
- Design of a model of expert system to help the capitalization and the evaluation of the FMECA.

Generally, in the field of railway safety, there are three levels of study for the development of a record of a physical security: a level architecture, a level card and a level interface. In order to show the feasibility of the approach, we limited the study to the first two levels: "architecture" and "card". For each of these levels, we have formed a draft knowledge base:

- The knowledge base of "level architecture" was developed from records TVM 430 of the TGV Nord,
- The basis of knowledge of "level card" has been built from the records of the security of the system Val of Lille and the system MAGGALY of Lyon.

The functional architecture of the "SASEM" system, presented in figure 9, is composed of three main modules: a man/machine interface (expert or user), a knowledge base and an inference engine.

The man/machine interface allows you to ensure the dialog with users and the expert in the field of security. This interface provides two major functions:

1. The expert interface facilitates the introduction and the updating of knowledge:

- Expert knowledge: the expert is essential to provide the strategic knowledge to assess the new folders to FMECA, but also to validate the knowledge produced by the expert system,
- The historical knowledge that comes from the files of FMECA railway systems already certified,
- The new folder of the FMECA to examine and assess.

2. The user interface that allows the consultation of the various knowledge produced by the system and in particular the consultation of historical FMECA and the results of the evaluation of the new folders of FMECA.

The knowledge base, which includes 50 examples of FMECAs, is split into two sub-bases: the first base corresponds to the level "architecture" and the second database contains the rules of the level "card".

The originality of "SASEM" system lies a share in the formalism developed which allows for better structure and organize the knowledge of the FMECA and on the other hand, in the decomposition of the knowledge base in two sub-bases: basis of rules" level architecture" and basis of rules" card level":

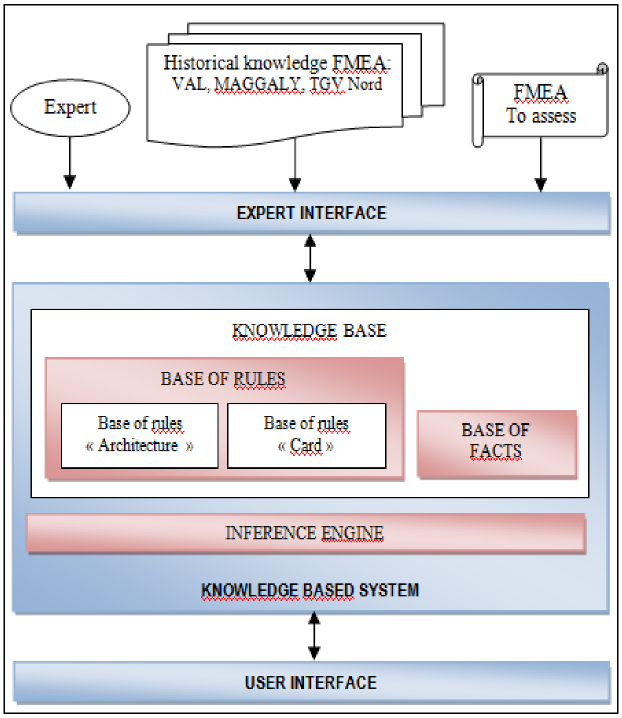


Figure 9: functional architecture of the SASEM system

Example of a rule of "level architecture"

SI system = "xxxxxxxxxxx"
And functionality = "positioning of the output states"
And failure mode = "Incorrect positioning"
THEN failure effect = "state of one or more output ranks the wrong signal"
And protection = "status detection complemented by threshold detector circuit ..."
And protection = "sequence can be only once for the whole subsystem"
And protection = "permanent control of state compliance"
And protection = "control date"
And protection = "alim's safety cut to force the outputs to 0"
And protection = "relay contact non-overlapping"

Example of a rule of "level card"

SI system = "xxxxxxxxxxx"
And functionality = "filtering Resistance input"
And failure mode = "cut of the Resistance"
THEN effect of failure = "disappearance of the output signal of the circuit"
And criticality = "criticality 3"

VIII. CONCLUSION

This paper has presented our contribution to the improvement of the methods which are normally used to analyse and assess the safety of automatic devices in guided transport systems. This contribution is based on the use of artificial intelligence techniques and has involved the development of several approaches and tools which assist in the modelling, storage and assessment of knowledge about safety. The software tools have 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. Currently, these tools are 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] Hadj Mabrouk, H. and Mejri, H. 2015. 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

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

[3] 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, France

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

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

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

[7] Michalski R-S and Wojtusiak, J. 2012. 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

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

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

[10] Hadj-Mabrouk, H. 2007. 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

[11] Caudron C. and Daufes S. 1996. Base de connaissances d'AMDEC. Application à la sécurité des équipements matériels des systèmes de transport guidés. Rapport de projet industriel de l'Ecole Polytechnique Féminine. INRETS-ESTAS, arcueil, 113 p