# « 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

**Dr. Habib HADJ-MABROUK[1], Dr. Hinda MEJRI[2]**

**[1]Ability to supervise research**
**French Institute of Science and Technology for Transport, Land and networks**
***habib.hadj-mabrouk@ifsttar.fr***

**[2]Assistant Professor**
**Higher Institute of Transport and Logistics**
**University of Sousse, Tunisia**
***hindamejri@yahoo.fr***

**Abstract**

Various researches in artificial intelligence are conducted to understand the transfer of expertise problem. Today we perceive two major independent research activities: the acquisition of knowledge which aims to define methods inspired specially from software engineering and cognitive psychology to better understand the transfer of expertise, and the automatic learning proposing the implementation of inductive, deductive, abductive techniques or by analogy to equip the system of learning abilities. The development of a knowledge-based support system "ACASYA" for the analysis of the safety guided transport systems insisted us to use jointly and complementary both approaches.

The purpose of this tool is to first, to evaluate the completeness and consistency of accidents scenarios and secondly, to contribute to the generation of new scenarios that could help experts to conclude on the safe character of a new system. "ACASYA" consists of three learning modules: CLASCA, EVALSCA and GENESCA dedicated respectively to the classification, evaluation and generation accident scenarios.

***Key-words:*** *Transport system, Safety, Accident scenario, Acquisition, Assessment, Artificial intelligence, Expert system, Machine learning.*

## 1. Regulatory context of research

the safety railway formerly within the competence of the only Member States and occulted a long time by the European Union, gradually will become a nearly exclusive field of the Community policy, this in particular by the means of the project of interworking. The European interest appears thus by the creation of Community institutions to the image of the European railway agency (ERA), with which France will have to collaborate; but also by the installation of safety checking and evaluation tool like the statistic statement of rail transport or the safety common goals and methods. These measurements will be essential on France as it was the case for the introduction of the railway infrastructure's manager and like the case for the national authorities of safety (NAS). Parallel to this European dash, one also notes an awakening in France since the decree 2000-286 of the 30/03/00 relative to the railway security, which replaces the decree of the 22/03/42 which constituted hitherto, the only legal reference on the matter.

France also sets up new mechanisms, contained in laws and regulations in order to improve the security level. We note the introduction of organisms or independent technical services (ITS) in charge of certification, technical organization of investigation or even the decree related to the physical and professional ability conditions of staff. Concerning the aptitude of staff, it is necessary to stress that the next challenge to take up for Europe passes by the necessary harmonization of the work conditions which is at the same time a requirement for the safety and interworking.

This study thus, shows that the safety from a theoretical and legal perspective undergoes and will undergo many changes. We notice in particular the presence of a multiplicity of actors who support and share the responsibility for the railway safety in France and Europe.

That they are public or are deprived, they have all of the obligations to respect and partly subjected to the independent organisms control.

## 2. Introduction

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 analysis of risks (PAR), the functional safety analysis (FSA), the analysis of failure modes, their effects and of their criticality (AFMEC) or analysis of the impact of the software errors [2] and [3]. 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.

The ACASYA tool [4], which is the subject of this paper, provides assistance in particular during the phase in which the completeness of functional safety analysis (FSA) is evaluated. Generally, the aim of FSA is to ensure that all safety measures have been considered in order to cover the hazards identified in the preliminary hazard analyses and therefore, to ensure that all safety measures are taken into account to cover potential accidents. These analyses provide safety criteria for system design and implementation of hardware and software safety. They also, impose a safety criteria related to sizing, exploitation and maintenance of the system. They can bring out adverse security scenarios that require taking the specification.

## 3. Approach used to develop the "ACASYA" system

The modes of reasoning which are used in the context of safety analysis (inductive, deductive, analogical, etc.) and the very nature of safety knowledge (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. The aim of artificial intelligence is to study and simulate human intellectual activities. It attempts to create machines which are capable of performing intellectual tasks and has the ambition to giving computers some of the human mind functions: learning, recognition, reasoning or linguistic expression. Our research has involved three specific aspects of artificial intelligence: knowledge acquisition, machine learning and knowledge based systems (KBS).

A development of the knowledge base in a KBS requires the use of techniques and methods of knowledge acquisition in order to collect structure and formalize knowledge. It has not been possible with knowledge acquisition to extract effectively some types of expert knowledge to analysis and evaluate safety. 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 the tool "ACASYA" 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. 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.

If cognitive psychology and software engineering generated support methods and tools for the knowledge acquisition, the exploitation of these methods remains still limited, in a complex industrial context. We estimate that, located downstream, machine learning can advantageously contribute to complete and strengthen the conventional means of knowledge acquisition.

The application of knowledge acquisition means, described in addition in [5], led primarily on the development of a generic model of accident scenarios representation and on the establishment of a historical knowledge base of the scenarios that includes about sixty scenarios for the risk of collision.

The acquisition of knowledge is however faced the difficulty to extract the expertise evoked in each step of the safety evaluation process. This difficulty emanates from the complexity of the expertise which encourages the experts naturally, to decline their know-how through significant examples or accident scenarios lived on automated transport systems already certified or approved.

Consequently, the update of expertise must be done from examples. Machine learning [[6] and [7]] makes it possible to facilitate the transfer of knowledge, in particular from experimental examples. It contributes to the development of KBS knowledge bases while reducing the intervention of the knowledge engineer.

Indeed, the experts generally consider that it is simpler to describe experimental examples or cases rather than to clarify processes of decision making. The introduction of the automatic learning systems operating on examples allows generating new knowledge that can help the expert to solve a particular problem. The expertise of a field is not only held by the experts but also, implicitly, distributed and stored in a mass of historical data that the human mind finds it difficult to synthesize. To extract from this mass of information a relevant knowledge for an explanatory or decisional aim, constitutes one of the automatic learning objectives.

The learning from examples is however insufficient to acquire all the know-how of experts and requires application of the knowledge acquisition to identify the problem to solve, extract and formalize accessible knowledge by the usual means of acquisition. In this direction, each of the two approaches can fill the weaknesses of the other. To improve the transfer process expertise, it is thus interesting to reconcile these two approaches.
Our approach is to exploit by learning, the base of scenarios examples, in order to produce knowledge that can help the experts in their mission of a system safety evaluation.

## 4. The "ACASYA" system of aid to safety analysis

The ACASYA system [[1] and [4]] is based on the combined utilization of knowledge acquisition techniques and machine learning. This tool has two main characteristics. The first is the consideration of the incremental aspect which is essential to achieve a gradual improvement of knowledge learned by the system. The second characteristic is the man/machine co-operation which allows experts to correct and supplement the initial knowledge produced by the system. Unlike the majority of decision making aid systems which are intended for a non-expert user, this tool is designed to co-operate with experts in order to assist them in their decision making. The ACASYA organization is such that it reproduces as much as possible the strategy which is adopted by experts.
Summarized briefly, safety analysis involves an initial recognition phase during which the scenario in question is assimilated to a family of scenarios which is known to the expert. This phase requires a definition of scenarios classes. In a second phase, the expert evaluates the scenario in an attempt to evolve unsafe situations which have not been considered by the manufacturer. These situations provide a stimulus to the expert in formulating new accident scenarios.

### 4.1. Functional organization of the "ACASYA" system

As is shown in figure 1, this organization consists of four main modules. The first formalization module deals with the acquisition and representation of a scenario and is part of the knowledge acquisition phase. The three other modules, CLASCA, EVALSCA and GENESCA, under the previously general principle, cover the problems of classification, evaluation and generation.

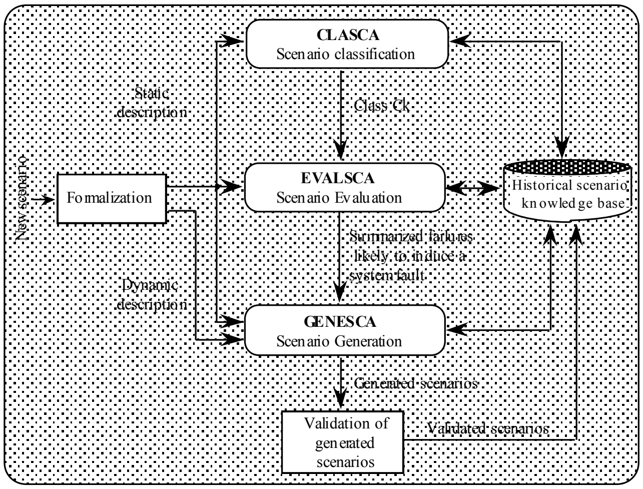

Fig. 1: Functional organization of the ACASYA system [1]

### 4.2. Functional architecture of the "CLASCA" system mock-up

CLASCA [8] is a learning system which uses examples in order to find classification procedures. It is inductive, incremental and dedicated to the classification of accident scenarios. In CLASCA, the learning process is nonmonotonic, so that it is able to deal with incomplete accident scenario data, and on other hand, interactive (supervised) so that the knowledge which is produced by the system can be checked and in order to assist the expert in formulating his expertise. CLASCA incrementally develops disjunctives descriptions of historical scenarios classes with a dual purpose of characterizing a set of unsafe situations and recognizing and identifying a new scenario which is submitted to the experts for evaluation.
CLASCA contains five main modules (figure 2):

1. A scenario input module ;
2. A predesign module which is used to assign values to the parameters and learning constraints which are

required by the system. These parameters mainly affect the relevance and quality of the learned knowledge and the convergence speed of the system;

3. An induction module for learning descriptions of scenario classes ;
4. A classification module, that aims to deduct the membership of a new scenario from the descriptions classes induced previously and by referring to adequacy rate;
5. A dialogue module for the reasoning of the system and the decision of experts. In justification the system keeps track from the deduction phase in order to construct its explanation. Following this rationale phase of classification decisions, the expert decides either to accept the proposed classification (in which case CLASCA will learn the scenario) or to reject this classification. In the second case it is the expert who decides what subsequent action should be taken. He may, for example, modify the learning parameters, create a new class, edit the description of the scenario or put the scenario on one side for later inspection.

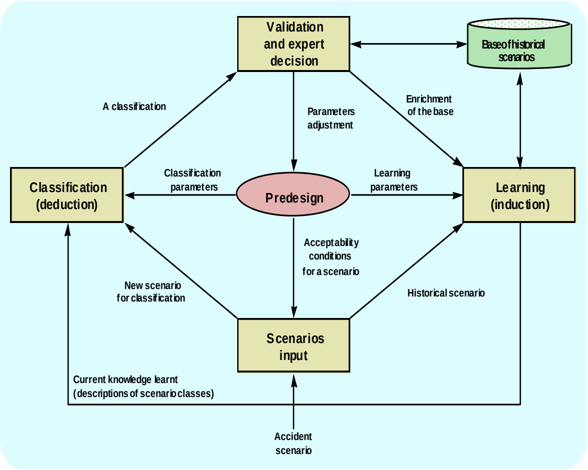

Fig. 2: Architecture of the CLASCA system mock-up

### 4.3. Functional architecture of the “EVALSCA” system mock-up

The objective of the module EVALSCA [[1] and [4]] is to confront the list of the summarized failures (sf) proposed in the scenario to evaluate with the list of archived historical summarized failures, in order to stimulate the formulation of unsafe situations not considered by the manufacturer. A sf is a generic failure, resulting from the combination of a set of elementary failures having the same effect on the system behavior. This evaluation approach allows to attract the attention of the expert on eventual failures not taken into account during the design phase and can cause danger to the safety of the transportation system. In this sense, it can promote the generation of new accident scenarios.

The second level of processing considers the class deduced by CALASCA in order to evaluate the scenario consistency. The evaluation approach is centered on the summarized failures which are involved in the new scenario to evaluate. The evaluation of this scenario type involves the two modules below [4] (figure 3):

- A mechanism for learning CHARADE’s rules [9] which makes it possible to deduce sf recognition functions and so to generate a basic evaluation rules ;
- An inference engine which exploits the above base of rules in order to deduce which sfs are to be considered in the new scenario to assess.

These two steps are detailed below-after:

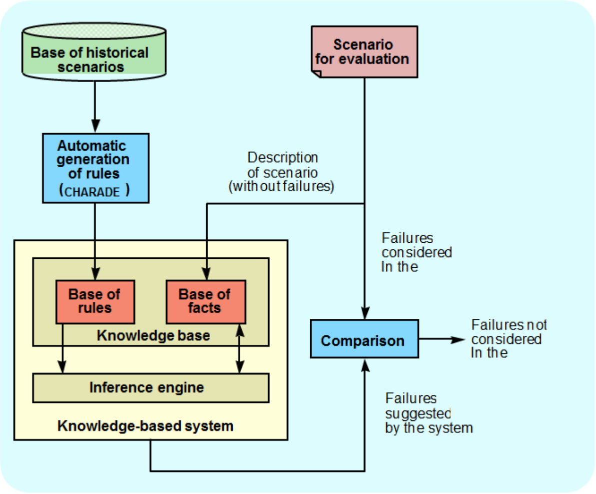

Fig. 3: Architecture of the EVALSCA system mock-up [3]

#### 4.3.1. Learning from failures summarized recognition functions

This phase of learning attempts, using the base of examples which was formed previously, to generate a system of rules reflecting the functions of recognition summarized failures. 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. There is a logic dependency relationship, which can be expressed in the following form:

```
If     Principe of cantonment (PC)
                 and
        Potential risks or accidents (R)
                 and
        Functions related to the risk (FRR)
                 and
        Geographical _ zones (GZ)
                 and
       Actors involved (AI)
                 and
        Incidents _ functions (IF)
Then  Summarized failures (SF)
```

A base of evaluation rules can be generated for each class of scenarios. Any generated rule must contain the PR descriptor in its conclusion. 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 analysis of the existing has led us to choose the CHARADE’s mechanism [9]. 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 an undeniable interest to CHARADE. A sample of some rules generated by CHARADE is given below. These relate to the initialization sequence class.

```
If        Actors involved = operator _ itinerant,
          Incident _functions = instructions
           Elements-involved = operator _in _cc.

Then      Summarized failures = SF11
          (Invisible  element on the zone of completely  automatic driving)
          Actors involved = AD _  with _redundancy,
          Functions related to the risk =train localization,
          Geographical _zones = terminus

If        Principle of cantonment = fixed _cantonment                 [0]
          Functions related to the risk = initialization
          Incident _functions = instructions

Then      Summarized failures = SF10
           (erroneous _re-establishment of safety frequency/high voltage),
          Functions related to the risk = SF10
          (erroneous  _re-establishment  of  safety  frequency/high  voltage
          permission),
           Functions related to the risk
           Functions related to the risk = alarm _management,
           Functions related to the risk = train _localization.
                                                                       [0]
```

### 4.3.2. . Deduction of the summarized failures which are to be considered in the scenario to evaluate

During the previous step, the CHARADE module created a system of rules from the current basis of learning examples and which is relative to the class Ck offered by the CALASCA system. The sf deduction stage requires beforehand, a transfer phase of rules which have been generated and transferred to an expert system in order to construct a scenario evaluation knowledge base. This evaluation contains (figure3):

- The base of rules, which is split into two parts: a current base of rules which contains the rules which CHARADE has generated in relation to a class which CLASCA has suggested at the instant t and a store base of rules, which composed 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 to evaluate and that’s enriched, over interference, from facts or deducted descriptors.

This scenario evaluation knowledge base which has been described above (base of facts and base of rules) exploited by forward chaining by an inference engine, generates the summarized failures which must be involved in the description of the scenario to evaluate.

The plausible sfs deduced by the expert system are analyzed and compared to the sfs which have actually been considered by the scenario to evaluate. This confrontation can generate one or more sfs not taken into account in the design of protective equipment and likely to affect the safety of the transport system. The above suggestion may assist in generating unsafe situations which have not been foreseen by the manufacturer during the specification and design phases of system.

### 4.4. Functional architecture of the “GENESCA” system mock-up

In complement as of two previous levels of treatment which involve the static description of the scenario (descriptive parameters), the third level [10] involves in particular the dynamic description of the scenario (the model of Petri) like to the three mechanisms of reasoning: the induction, the deduction and the abduction. The aid in the generation of a new scenario is based on the injection of a sf, declared possible by the previous level, in a particular sequencing of Petri network marking evolution.

This approach of generation includes two distinct processes: the static generation and the dynamic generation (figure 4). The static approach seeks to derive new static descriptions of scenarios from evaluating a new scenario. It exploits by automatic learning the whole of the historical scenarios in order to give an opinion on the static description of a new scenario.

If the purpose of the static approach is to reveal static elements which describe the general context in which the new scenario proceeds, the dynamic approach is concerned to create a dynamics in this context in order to suggest sequences of events that could lead to a potential accident. The method consists initially, to characterize by learning the knowledge implied in dynamic descriptions of historical scenarios of the same class as the scenario to evaluate and to represent them by a “generic” model. The next step is to animate by simulation this generic model in order to discover eventual scenarios that could eventually lead to one or more adverse safety situations.

More precisely, the dynamic approach involves two principal phases (figure 3):

- A modeling phase which must make it possible to work out a generic model of a class of scenarios. The Modeling attempts to transform a set of Petri networks into rules written in logic of proposals;
- A simulation phase which exploits the previous model to generate possible dynamic descriptions of scenarios.

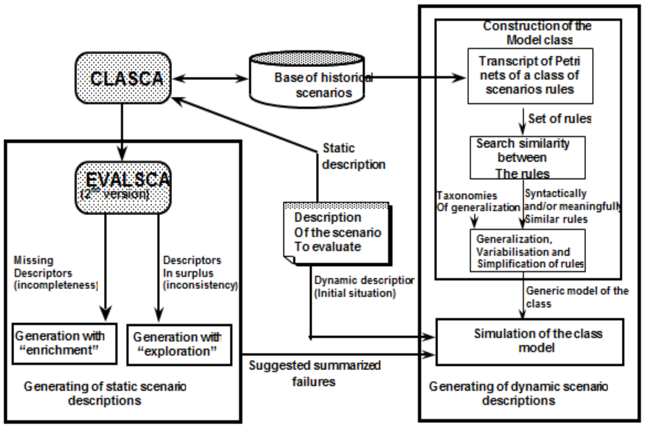
CLASCA
Base of historical scenarios
Construction of the Model class
Transcript of Petri nets of a class of scenarios rules
Set of rules
Search similarity between The rules
Static description
EVALSCA (2nd version)
Taxonomies Of generalization
Syntactically and/or meaningfully Similar rules
Generalization, Variabilisation and Simplification of rules
Description Of the scenario To evaluate
Missing Descriptors (incompleteness)
Descriptors In surplus (inconsistency)
Dynamic description (Initial situation)
Generic model of the class
Generation with “enrichment”
Generation with “exploration”
Simulation of the class model
Suggested summarized failures
Generating of static scenario descriptions
Generating of dynamic scenario descriptions

Fig. 4: Approach help to generating embryos accident scenarios

During the development of model GENESCA, we met with methodological difficulties. The produced model does not make it yet possible to generate new relevant and exploitable scenarios systematically, but only the embryos of scenarios which will stimulate the imagination of the experts in the formulation of accident scenarios. Taking into account the absence of work relative to this field, originality and complexity of problem, this difficulty was predictable and solutions are under investigation.

## 5. Conclusion

The ACASYA system created to assist safety analysis for automated terrestrial transit systems satisfies classification, evaluation and generation objectives of accident scenario. It demonstrates that machine learning and knowledge acquisition techniques are able to complement each other in the transfer of knowledge. Unlike diagnostic aid systems, ACASYA is presented as a tool to aid in the prevention of design defects. When designing a new system, the manufacturer undertakes to comply with the safety objectives. He must demonstrate that the system is designed so that all accidents are covered. At the opposite, the experts of certification aim to show that the system is not safe and, in this case, to identify the causes of insecurity. Built in this second approach, ACASYA is a tool that evaluates the completeness of the analysis proposed by the manufacturer. ACASYA is at the stage of a model whose first validation demonstrates the interest of the aid to safety analysis method and which requires some improvements and extensions.

## References

[1] Hadj-Mabrouk H. "Apport des techniques d'intelligence artificielle à l'analyse de la sécurité des systèmes de transport guidés", Revue Recherche Transports Sécurité, no 40, INRETS, France, 1993.

[2] Hadj-Mabrouk H. "Méthodes et outils d’aide aux analyses de sécurité dans le domaine des transports terrestres guidés", Revue Routes et Transports, Montréal-Québec, vol. 26, no 2, pp 22-32, Été 1996.

[3] Hadj-Mabrouk H. "Capitalisation et évaluation des analyses de sécurité des automatismes des systèmes de transport guidés", Revue Transport Environnement Circulation, Paris, TEC no 134, pp 22-29, Janvier-février 1996.

[4] Hadj-Mabrouk H. "ACASYA: a learning system for functional safety analysis", Revue Recherche Transports Sécurité, no 10, France, Septembre 1994, p 9-21.

[5] Angele J., Sure Y. "Evaluation of ontology –based tools workshop", 13th International Conference on Knowledge Engineering and Knowledge management EKAW *2002*, Siguenza (Spain), September 30th (pp: 63-73)

[6] Cornuéjols A., Micelet L., Kodratoff Y. " Apprentissage artificiel: Concepts et algorithmes", Eyrolles éd, Août 2002.

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

[8] Hadj-Mabrouk H. "CLASCA, un système d'apprentissage automatique dédié à la classification des scénarios d'accidents", 9ème colloque international de fiabilité & maintenabilité. La Baule, France, 30 Mai-3 Juin 1994, p 1183 - 1188.

[9] Ganascia J.-G. "AGAPE et CHARADE : deux mécanismes d'apprentissage symbolique appliqués à la construction de bases de connaissances", Thèse d'Etat, Université Paris-sud, mai 1987.

[10] Mejri L. "Une démarche basée sur l'apprentissage automatique pour l'aide à l'évaluation et à la génération de scénarios d'accidents", Application à l'analyse de sécurité des systèmes de transport automatisés. Thèse de doctorat, Université de Valenciennes, 6 décembre 1995, 210 p.