International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 6, Issue 2 (February 2017), PP. 51-58

Preliminary Hazard Analysis (PHA): New hybrid approach to railway risk analysis

Dr. Habib Hadj-Mabrouk
French Institute Of Science And Technology For Transport, Spatial Planning, Development And Networks
Marne La Vallée, France

Abstract: The Preliminary hazard analysis (PHA) is used to essentially identify potential accidents related to the system and its interfaces to assess their probability of occurrence and the severity of the damage they may cause and finally propose solutions that will reduce, control or eliminate. Although essential in the process of analysis and safety evaluation of high-risk industrial system, the method PHA is very differently developed and remained unclear. This method is generally classified in theory by an inductive approach. However, in practice, a deductive approach is essentially used as the Fault tree analysis. To enhance the quality of the safety analysis in terms of completeness and consistency, we suggest a new hybrid method that combines these two modes of reasoning: induction and deduction. Indeed, the safety analysis of a complex system requires from experts in the field implementation of an iterative analysis process involving both inductive and deductive approaches. The ambition of this new method is to deconsolidate and renovate conventional approaches. In addition, this method is based on the use of a standardized vocabulary and a rigorous analytical approach likely to be accepted by all actors who participate in the development of safety documentation. Indeed, in accordance with national and European regulations and in particular the Railway Safety Directive, this paper proposes a generic approach for development assistance, assessment and prevention of risks which takes account of uses, theory and our experience in this domain.

Keywords: PHA; Railway transport; Safety; Accidents; Risk; Dangers; Hazard ; Hybrid reasoning

I. INTRODUCTION

The assessment of the design and implementation of a new Rail transport system or the modification of an existing system and the verification of its capabilities with regard to the safety objective, and maintenance over time of its capabilities, are generally performed by an independent technical body such as the CERTIFER organization in France. These agencies are responsible for an assurance engagement, a procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements. Experts from these certification bodies must assess and check the capabilities of the system in terms of safety objectives it must achieve and maintain during its operations. This certification body checks that the design and implementation of the system are in compliance with regulations and rules of art that are usually specified in a Preliminary File Safety. This folder must state the objectives and security requirements, methods and techniques used to achieve these objectives and the demonstration and evidence that these objectives have been achieved. Particular attention should be paid to the examination of all the methods of safety analysis proposed by the manufacturer of the transport system and evaluated by the certification body. Very schematically, here main players, each with distinct roles, are involved in developing and operating a rail transport system [1] (figure 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 National safety 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 CERTIFER or 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 [2]:

- 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 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 in order to identify hazardous situations, potential accidents, hazardous units or equipment and the severity of the consequences which would result. Generally, the construction process of the security of a system contains several analyses: Preliminary hazard analysis (PHA); Functional safety analysis and Security Analysis of the resulting product. The study presented in this article focuses only on the method of Preliminary hazard analysis (PHA). The PHD method essentially consists of identifying potential accidents related to the system and its interfaces to evaluate and propose solutions to eliminate reduce or control them. If the theory advocates an approach to risk analysis "inductive" actually applied in practice procedures are mostly "deductive". The PHD approach we recommend combines the two approaches explicitly to strengthen the quality of analysis in terms of completeness and consistency. This new approach fits well within the framework of the new French and European National regulations and particular orientations, and meets the European Directive of 2014 on the implementation of the common safety methods for all Member States.

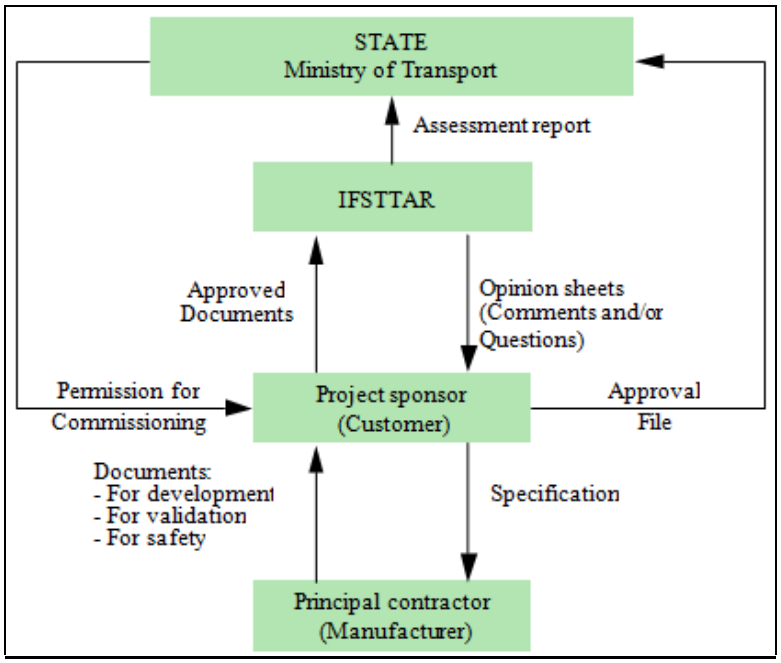

Figure 1. Key players involved in the development of a railway system [1]

II. PROCESS FOR THE SAFETY DEVELOPMENT OF RAIL

Generally, the construction process of the security of a system (Figure 2) contains several hierarchical analyses [3]: Preliminary hazard analysis (PHA), Functional safety analysis (FSA) and Security Analysis of the resulting product which includes two analyzes: Hardware safety analysis (HSA) and Software safety analysis (SSA). Preliminary hazard analysis (PHA) is essentially to identify potential accidents related to the system and

its interfaces to evaluate and propose solutions to eliminate reduce or control them. This preliminary analysis is important to ensure a satisfactory level of safety. Indeed, the results obtained by this analysis are exploited by all the safety studies of the system and in particular by Functional safety analysis (FSA). Indeed, the FSA method aims to justify the system design architecture is safe against potential accidents identified by PHA and therefore to ensure that all safety measures are taken into account cover hazards or potential accidents. The Software safety analysis (SSA) is generally based on the method Software Error Effect Analysis (SEEA) as well as the critical reading code. The method Hardware safety analysis (HSA) shall include information on electronic cards and interfaces defined as security. This analysis is implementing several types of analysis [4], [5]:

- Failure Modes, Effects and Criticality Analysis (FMECA),
- Method of Combining Summarized Failures (MCSF),
- Fault tree analysis (FTA).

In this safety process, one of the difficulties is to ensure the completeness and consistency of the various analyses by the research risks and scenarios contrary to safety not taken into account when developing the safety record. The study presented in this article focuses only on the method of Preliminary hazard analysis (PHA) and aims to develop a new methodological approach for preliminary hazard analysis to help experts in the field and in particular the certification bodies in their crucial task of analysis and assessment of completeness and consistency of the risk analysis of a rail transport system.

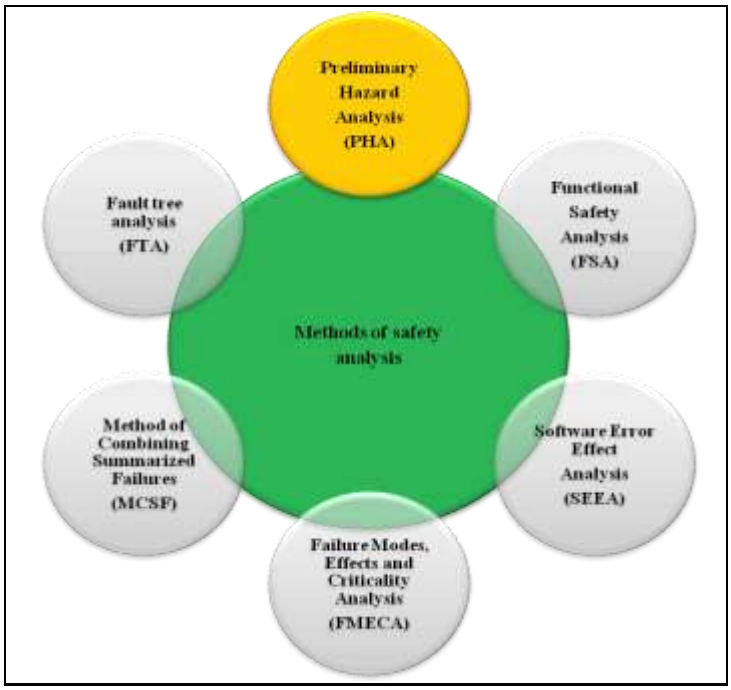

Figure 2. Main safety analysis methods [2]

III. OBJECTIVE PRELIMINARY HAZARD ANALYSIS (PHA)

The Preliminary hazard analysis (PHA) [6] and [7] is used to essentially identify potential accidents related to the system and its interfaces to assess their probability of occurrence and the severity of the damage they may cause and finally propose solutions that will reduce, control or eliminate. The results of this analysis are the definition of the requirements and system security criteria to be considered during the design phases and achievements of hardware and software (Figure 3) and finally to establish the broad lines of safety and security analysis located downstream (functional safety analysis, safety analysis software, security analysis equipment). Indeed, the creation of a list of potential accidents helps to identify points in the system that may be critical for the safety and deserve special attention in the design, implementation, validation and maintenance. When is limited to assessing (usually qualitatively) the severity of damage that could cause potential accidents, it is called Hazard Analysis [6], [7].

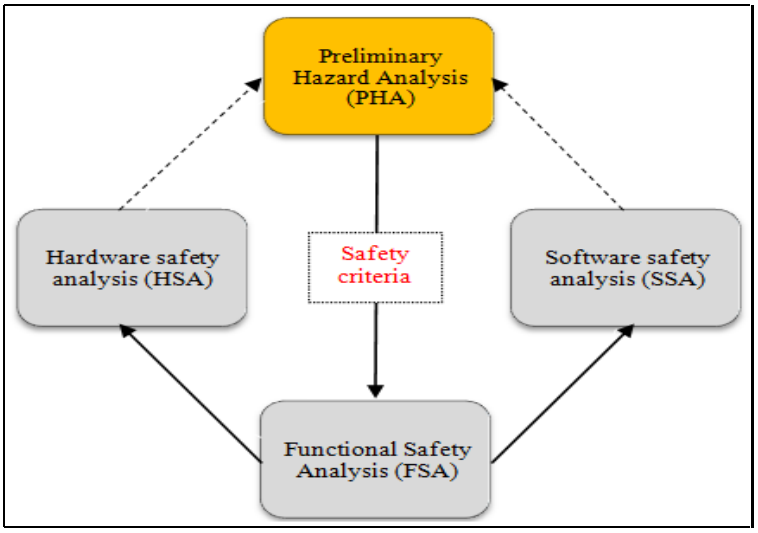

Figure 3. Position the PHA in the safety construction process [2] and [3]

A PHA requires a good understanding of the mission of the system and its environment. It is essential for systems that use unfamiliar technologies. It takes advantage not only of the experience and imagination of the manufacturer but also of the monitoring operation for the implementation of an Experience feedback [3]. The PHA is an issue that usually remains open throughout the study and is constantly updated. Because this analysis is performed early in the course of the program, its results may be incomplete and inaccurate. A PHA should therefore be supplemented and updated until the system design is advanced enough (Figure 4). This ensures that every potential accident in the list is in the design, function, or a precautionary arrangement to control, reduce or eliminate its probability of occurrence.

Preliminary hazard analysis (PHA) is generally classified in theory from inductive approaches [6], [7], [8], [9] [10] [11] and [12]. In the inductive approach, the reasoning goes from the most particular to the more general, which leads to a detailed study of the effects of a failure of the system and its environment. In other words, the inductive methods leave elementary events, or to search the consequences directly (e.g. FMECA, SEEA), or to identify combinations of events that may have critical consequences (e.g. MCSF). In the context of PHA, it is mainly to search, by induction, the set of potential accidents from hazards (or hazardous elements). However, in practice, a deductive approach is essentially used as the Fault tree analysis (FTA). To enhance the quality of PHA in terms of completeness and consistency, we suggest a method that combines these two approaches [2]. Indeed, the safety analysis of a complex system requires from experts in the field implementation of an iterative analysis process involving both inductive and deductive approaches. It is usually necessary to cross check the results obtained by an approach with those obtained by means of another complementary approach [3].

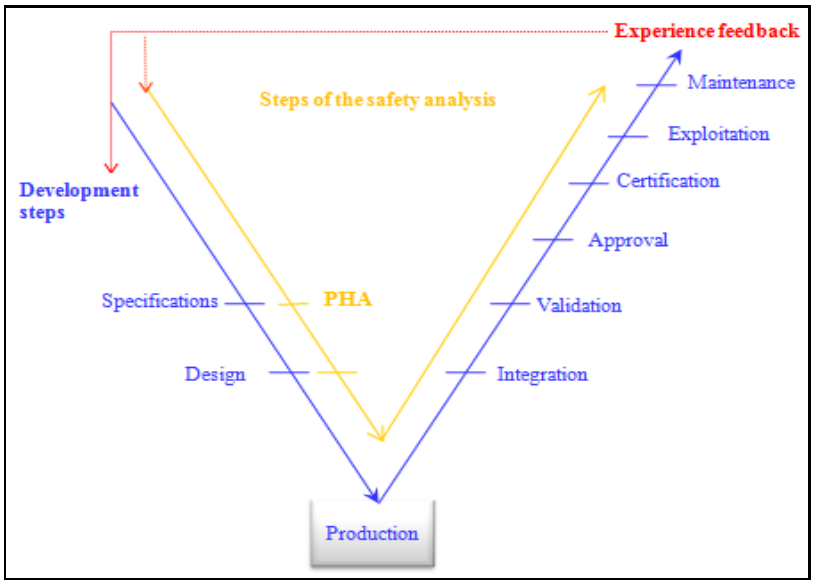

Figure 4. Position of the PHA in the project development cycle [3]

IV. DEFINITION OF A STANDARDIZED VOCABULARY

In order to define a common terminology and unify the basic vocabulary used in preliminary risk analysis, we used not only to the analysis of a set of safety standards (Table 1: [13], [14], [15], [16] and [17]), but also to the experience and know-how to IFSTTAR institute and in particular during the expert missions and certification [19], [20] and [21]. Thus, several definitions have been established, particularly regarding the concepts of potential accidents, danger, damage, risk and prevention or protection measures. Figure 5 presents the main results of this study as a conceptual model showing semantically articulation of all the descriptive parameters of a Preliminary hazard analysis (PHA) [22].

Table 1. Definitions of the main parameters descriptive of PHA

Descriptive parameters of an PHA	Definitions adopted	References
Damage	Physical injury and / or damage to health or damage caused to things.	Mémorandum n° 9, Cen/Cenelec [CENE 94]
Accident	Occurrence or succession of unforeseen events resulting in an attack on the physical integrity of persons or the destruction of equipment.	NF F 71-011, [BNCF 90]
Near-accident (Incident)	Dysfunction of the system or a succession of malfunctions of the system leading to an unspecified state in which the physical integrity of the persons is not affected or destruction of equipment but for which a condition not controlled by the system could have led damage to the physical integrity of persons and / or material damage.	NF F 00-101, [BNCF 93]
Potential Accident	An event or series of unwanted events that may give rise to an accident but does not necessarily give rise to an accident. (Accident or near-accident: NF F OO-101, 1993)	European Standard NF EN50126, [CENELEC 00]
Hazard	Condition that could result in an accident or potential accident	European Standard NF EN50126, [CENELEC 00]
Hazardous Occurrence	Event creating a hazard.	European Standard NF EN50126, [CENELEC 00]
Level of probability of occurrence of a potential accident	A: Frequent ; B: Probable ; C: Occasional ; D: Rare ; E: Improbable ; F: Extremely unlikely	NF F 00-101, [BNCF 93]
Level of severity of damage	I: Minor or nil ; II: Significant ; III: critique ; IV: Catastrophic	NF F 00-101, [BNCF 93]
Risk	The combination of the frequency (or likelihood) of a potential accident and the consequences of the accident (severity of damage)	European Standard NF EN50129, [CENELEC 03]
Prevention or protection measures	- Prevention measure: to reduce or cancel the probability of a potential accident. - Protection measure: to reduce the severity of damage caused by a potential accident. (Middle to reduce the level of risk)	RE.Aéro 7O1 11, [BNAE 86]
Safety	Absence of any unacceptable level of risk.	European Standard NF EN50129, [CENELEC 03]

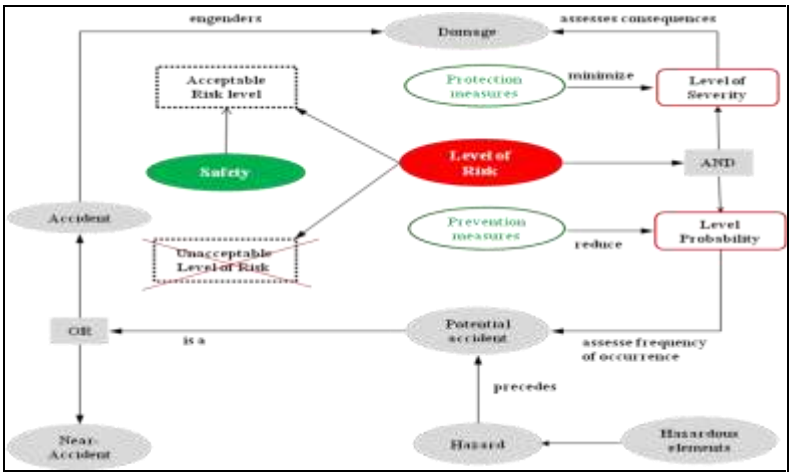

Figure 5. Articulation descriptive parameters involved in the PHA [22]

V. METHOD OF ANALYSIS OF PROPOSED RISKS

If the theory advocates an approach to risk analysis "inductive" actually applied in practice procedures are mostly "deductive". The PHD approach we recommend combines the two approaches explicitly to strengthen the quality of analysis in terms of completeness and consistency. Indeed, the safety analysis of a complex system requires from experts in the field implementation of an iterative analysis process involving both inductive and deductive approaches. This method of PHD is structured around three stages of complementary and iterative analysis together including induction and deduction process (Figure 6):

1. From potential accidents, the first step to determine by "induction" the list of damages that could cause a crash and "deduction" list of hazards that may occur in the system.
2. The second step uses the above hazards identified by "dipping" the list of dangerous elements, and "induction", the potential accidents. Re-establishing the list of potential accidents from dangers potentially enable to generate new potential accidents not considered in the first stage. In this case, the first step of the analysis must be taken to enrich the list of dangers previously deducted. This is in fact a verification action that allows furthering increasing the initial list of potential accidents.
3. The third step in the analysis is to "induce" the dangers from hazardous items deducted during the second stage. The catalog of hazards established at the end of this third analysis is faced with one that is deducted at the first step of the analysis from potential accidents. The invention of new dangers requires starting the second stage of analysis and possibly the first.

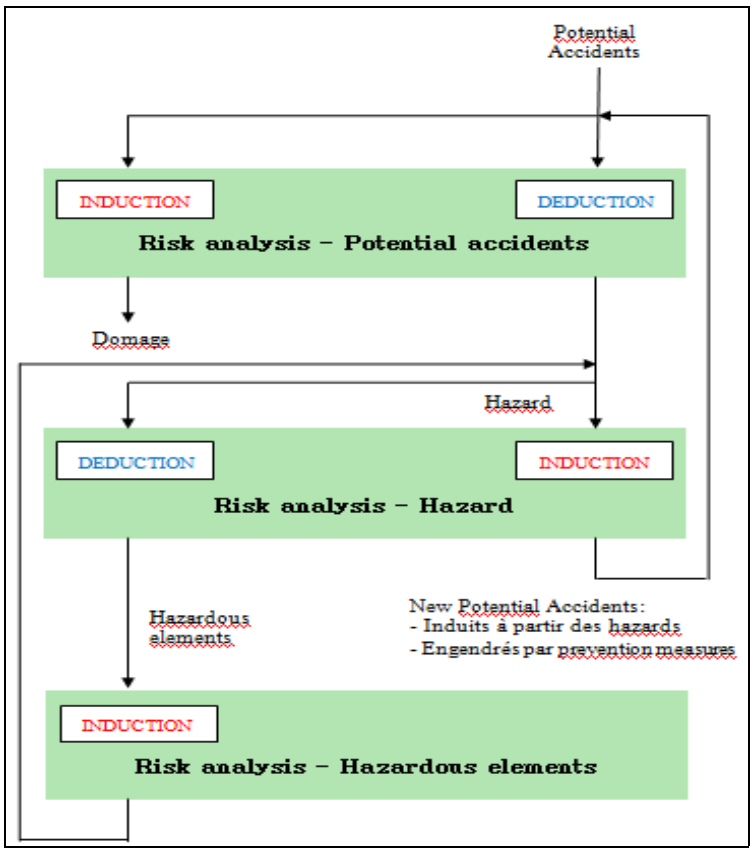

Figure 6. General description of the analytical method proposed Risks [22]

VI. A TOOL TO ASSIST IN THE DEVELOPMENT AND EVALUATION OF RISK ANALYSIS

The previous paragraphs have detailed the different phases of design of a system to assist with risk analysis and assessment. The feasibility study of this system, applied to the field of safety of rail transport, led to the realization of a software tool. The main objective of this tool is not only to capitalize knowledge on risk analysis but also to assist experts in the development and evaluation of new PHA. The functional architecture of the aid system for railway risk analysis consists of five main modules illustrated in Figure 7:

- A human-machine interface that ensures dialogue with users and / or the security domain expert. This interface provides two main functions. The first is to capture and update the knowledge needed to develop or evaluate a PHA. The second function allows the consultation of the different knowledge produced by the system and in particular the evaluation results of a new PHA, the basis of historical PHAs,

- A knowledge acquisition and modeling module. Each PHA entered is formalized according to a terminology (figure 5 and table 1) and a representation format of pre-established knowledge. This module also allows you to control certain conditions necessary to accept a PHA. These eligibility criteria concern, for example, compliance with certain constraints and criteria for the construction of the PHA which are intrinsically imposed by the defined representation formalism or the respect of the presence of "key" or "minimal" descriptors to develop a relevant PHA. In summary, this module not only collects and formalizes knowledge; it is also the first level of "syntactic" evaluation of a PHA.
- A module for developing new PHAs. This module allows the three steps of the method proposed in paragraph V to be carried out successively: (1) "inductive-deductive" analysis based on potential accidents, (2) "deductive-inductive" analysis based on hazards and (3) "inductive" analysis from hazardous elements. The coexistence of these three iterative analyzes ensures the completeness of the risk analysis. In this sense, this module represents the second level of evaluation of a PHA in terms of completeness.
- A PHA evaluation module. This module, which is the third level of evaluation, uses expert evaluation knowledge (rules, strategies and heuristics) to produce recommendations in terms of the consistency, relevance and adequacy of PHA knowledge.
- A knowledge base that brings together the archived PHAs, the new PHAs being evaluated, and the opinions of the evaluation module that represent suggestions, recommendations or explanations.

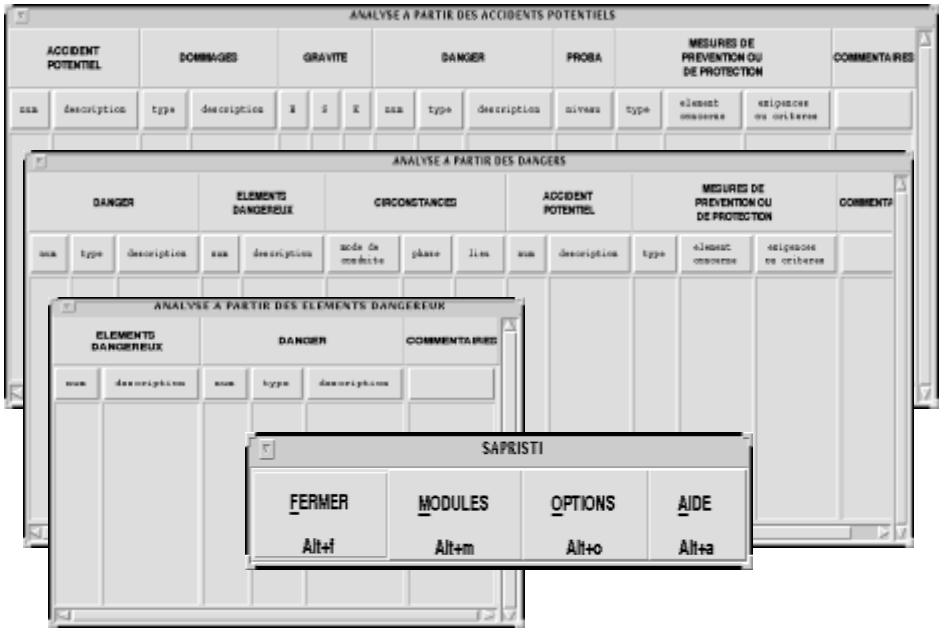

Figure 7. Examples of interface screens for acquisition and development of PHAs [23].

To date, only a part of the two acquisitions and elaboration modules allowing the knowledge base to be filled is operational [23]. By way of example, we present below (figure 7) some examples of screens of the interface realized which makes it possible to help the user on the one hand to develop a PHA and on the other hand to enrich and Up-to-date knowledge base. As part of the feasibility study, our first concern was to validate the method proposed rather than to favor a thorough and costly study of the development tools and languages necessary for the development of an operational system.

VII. CONCLUSION

This risk analysis method, which provides iterative control to ensure the completeness and to tend to the completeness of risk analysis, not only to capitalize on knowledge in risk analysis on accidents, but also to assist experts to develop or evaluate new folder Preliminary hazard analysis (PHA). The main originality of this approach lies essentially in terms of consistency and completeness of the risk analysis. This approach goes beyond the framework of guided rail (first application of the method) and could be well applied to other areas where security is an absolute requirement. However, despite the interest of this method, completeness and quality of risk analysis are still based on the know-how, intelligence and intuition of experts in the field [5]. This method is the first step towards a definition of the preliminary risk analysis recommended for players who take part in the realization of a safety record. This new approach fits well within the framework of the new French and European National regulations and particular orientations, and meets the European Directive of 2014 [24] on the implementation of the common safety methods for all Member States. The proposed approach for risk

analysis and assessment is also falls within the framework of the work proposed by the standard ISO 31000 on risk management [25].

However, the proposed method requires its implementation in other industrial conditions, to validate and, if necessary, improve what remains a proposal.

REFERENCES

[1] H. Hadj Mabrouk, La maîtrise des risques dans le domaine des automatismes des systèmes de transport guidés: Le problème de l'évaluation des analyses préliminaires des risques, Revue Recherche-Transport-Sécurité (RTS), Numéro 49, 1995, pp. 101-112.

[2] H. Hadj Mabrouk, Méthode d'analyse préliminaire des risques, Congrès LM15, Maîtrise des Risques et sûreté de fonctionnement, Risques et Performances, ImdR-IsdF, Lille 10-12 octobre, 2006.

[3] H. Hadj Mabrouk and F. Hamdaoui, Analyse préliminaire des risques et Retour d'expérience, Conférence Internationale Francophone d'Automatique (CIFA), Bucarest Roumanie 3-5 septembre, 2008.

[4] 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, Vol. 6, Issue 8, 2016, pp.1-11

[5] 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. 6, Issue 8, 2016, pp.91-98

[6] C. Lievens, Sécurité des systèmes, Eds. Cépaduès, Séries Sup'Aéro, Toulouse 1976, ISSN 0337-6192, 341 p.

[7] A. Villemeur, Sûreté de fonctionnement des systèmes industriels, Eds. Eyrolles, Paris, 1988.

[8] INERIS, Méthodes d'analyse des risques générés par une installation industrielle, Ref. INERIS-DRA, 2006-P46055-CL47569, 2006.

[9] Y. Mortureux, Analyse préliminaire de risques-Méthode, Eds. Techniques de l'ingénieur, L'entreprise industrielle, Sécurité et gestion des risques, 2002.

[10] A. Desroches, J-F. Leroy and F. Vallé, La gestion des risques-principes et pratiques, Eds. Lavoisier, 2003, pp. 29–44.

[11] A. Desroches, J-F. Leroy, Quaranta and F. Vallée, Dictionnaire d'analyse et de gestion des risques, Eds. Hermes, 2005.

[12] A. Desroches, D. Baudrin and M. Dadoun, L'Analyse Préliminaire des risques-principes et pratiques, Eds. Hermes, 2009.

[13] [CENE 94]: "Principes directeurs pour inclure dans les normes les aspects liés à la sécurité", Comité Européen de Normalisation / Comité Européen de Normalisation Électrotechnique (Cen/Cenelec), Mémorandum n°9, Première édition, Bruxelles, 1994. (Version européenne modifiée du Guide Iso/CEI n°51).

[14] [BNCF 90]: "Installations fixes et matériel roulant ferroviaires, Informatique, Sûreté de fonctionnement des logiciels, Généralités", Bureau de Normalisation des Chemins de Fer (BNCF), Norme française homologuée NF F 71-011, Paris, 1990.

[15] [BNCF 93]: "Matériel ferroviaire en général, Fonctions de sécurité, Méthode de détermination et règles de traitement", Bureau de Normalisation des Chemins de Fer (BNCF), Norme française homologuée NF F 00-101, Paris, 1993.

[16] [CENELEC 00]: European Standard NF EN50126, Railway applications – The specification & demonstration of reliability, availability, maintainability and safety (RAMS), CENELEC, 2000

[17] [CENELEC 03]: European Standard NF EN50129, "Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling", CENELEC, 2003

[18] [BNAE 86]: "Guide des méthodes courantes d'analyse de la sécurité d'un système missile ou spatial", Bureau de Normalisation de l'Aéronautique et de l'Espace (BNAE), Recommandation RE.Aéro 701 11, Boulogne-Billancourt, 1986.

[19] H. Hadj Mabrouk, Review of the Preliminary Risk Analysis file of the KVBP/KVIM system of the ANTARES project, Report INRETS-ESTAS-CR/A-94-64, Arcueil, France, 2 december 1994, 35p.

[20] H. Hadj Mabrouk and D. Bied-Charreton, Opinion of INRETS on the document Preliminary Risk Analysis of the KVBP/KVIM system of the ANTARES project, Report INRETS-ESTAS-CR/A-95-15, Arcueil, France, 16 March 1995, 38p.

[21] H. Hadj Mabrouk, Formal representation and acquisition of preliminary risk analyzes, Convention report under the PREDIT-ASCOT program, Report INRETS-ESTAS-CR/A-94-46, Arcueil, France, 30 june 1994, 48p.

[22] H. Hadj-Mabrouk and B. Harguem, Méthode originale d'Analyse Préliminaire des Risques, Ouvrage collectif, Gestion des risques naturels, technologiques et sanitaires, ISBN: 9782364931596, Référence: 1159, Éditions Cépaduès, 2014.

[23] F. Raîs, Analyse et conception de l'interface d'un logiciel d'élaboration des analyses préliminaires de risques, Rapport de stage de fin de 2ème année d'école d'ingénieur, Institut d'informatique d'entreprise (CNAM-IIE), INRETS, Arcueil, septembre 1996, 30 p.

[24] Directive 2004/49/EC, Directive of the European Parliament and of the Council on safety on the Community's railways, Brussels, Official Journal of the European Union, Commission of the European Communities, 2004.

[25] NF ISO 31000, Management du risque - Principes et lignes directrices, Norme internationale AFNOR, Afnor Editions, 2010.