Complementarity of Preliminary Hazard Analysis and field data feedback to improve security. Application to rail transport

Feyrouz Hamdaoui, Habib Hadj-Mabrouk

▶ **To cite this version:**

Feyrouz Hamdaoui, Habib Hadj-Mabrouk. Complementarity of Preliminary Hazard Analysis and field data feedback to improve security. Application to rail transport. 9th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, STA _2008, Dec 2008, Sousse, Tunisia. pp.1-8. hal-03250338

HAL Id: hal-03250338
https://hal.science/hal-03250338

Submitted on 4 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Complementarity of Preliminary Hazard Analysis and Field Data Feedback to improve security - Application to rail transport -

Feyrouz Hamdaoui[1], Habib Hadj-Mabrouk[2]

[1] Institut Supérieur des Sciences Appliqués et de Technologie de sousse – Tunisie
30 avenue 20 mars, cité Jawhara 4000 Sousse
feyrouzhamdaoui@gmail.com

[2] INRETS – France
2 av du Général Malleret-Joinville 94114 Arcueil Cedex, France mabrouk@inrets.fr

Abstract. *The development of risk project requires at first the census particularly of potential accidents list. This study is generally made during the risks Preliminary Hazard Analysis method. The collection of these potential accidents requires mainly, not only experts' expertise of the field, but also Field Data Feedback. Up to Now, this crucial problem remains the archway key of the improvement of the system security level. Indeed, there is no explicit procedure to exploit systematically the results stemming from Field Data Feedback to elaborate out Preliminary Hazard Analysis. This article suggests a methodology allowing to exploit in a systematic way the Field Data Feedback in order to work out the Preliminary Hazard Analysis on one hand and take into account the potential accidents from the specification stage of the project on the other hand.*

keywords. *Field Data Feedback, Preliminary Hazard Analysis, System Development Cycle, Security, Risks control, regulation.*

1. General context of the research

Despite the requirement of the statutory and normative texts related to rail system security, the interaction between the process of the Preliminary Hazard Analysis (PHA), the Field Data Feedback (FDF) and the cycle of system development still remains ill structured and even inexistent. Indeed, PHA allows to identify basically potential accidents linked to the system and its interfaces in order to evaluate their instance probability and also the seriousness of injuries they can create, and at last to

suggest solutions allowing to master the risks. Effectively, the Preliminary Hazard Analysis is considered as the major piece in the construction process of security and represents also a key task in the activities of security analysis.

Yet, the relevance of PHA depends on the completeness of the potential accidents list which com be identified mainly from FDF. In spite of its undeniable importance, PHA comes up against the absence of an explicit methodology which integrates in a systematic way the FDF results.

The FDF is generally defined as a dynamic process of collection, stocking, analysis and exploitation of data connected with situations contrary to security (accident/incident). The target is to get profit out of the lessons of actual experience to avoid its reproduction with the implementation of appropriate corrective preventive measures in order to avoid the reproduction of such risky scenarios.

This article successively presents the legislative and statutory framework connected with the process of the FDF and PHA, the PHA method, the FDF process and the remaining methodology to improve risks analysis from the FDF process.

1.1. The PHA regulation framework

The decree number 2000-286 of 30/03/2000 related to security of the National Rail Network (NRN) [1] defines the content and the methods of elaborating the security preliminary file (SPF). According to the 08/01/2002 enforcement decree [1], the SPF includes particularly a document connected with the project organization and relies on PHA results. This decree also precises that security file (SF)'s purpose is to describe the system as it is carried out and to bring the proof of respecting security measures exposed in the SPF. It includes the conclusions of security studies carried out and the certificates of the risks insurance identified in the PHA. Because the PHA is carried out very early in the cycle of system development (since the specification stage), its results can be incomplete or inaccurate. Thus, the PHA file remains open and constantly updated during the FDF development.

1.2. FDF regulation framework

A set of national regulation and legislative recent texts and European directives indicate the principles, the objectives and methods of FDF process. These regulations concern specially the technical inquiries after rail accidents and incidents. According to 23/01/2002 directive, an inquiry is a procedure allowing to present accidents and incidents and aims at collecting and analyzing information; it draws conclusions including determining causes and if the need arises, formulates recommendations as regards security.

2. Suggested methodology

The methodology we have developed intervenes two methods in a related and complementary way: the FDF and the PHA. The two following paragraphs present successively a general description of the FDF method and the PHA method.

2.1. Field Data Feedback (FDF)

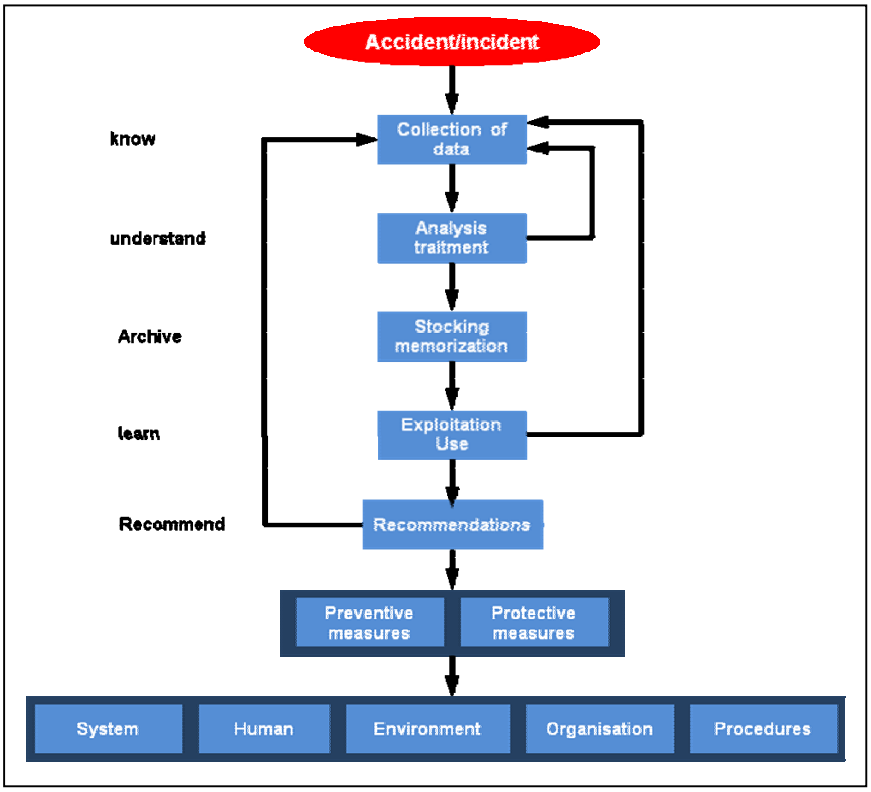

Fig. 1. Different steps' articulations of FDF process

The global approach of the FDF course illustrated by figure 1, adopts five stages: collection of data related to any insecurity event, their analysis and treatment, their stocking and memorization, their exploitation and use, and suggestion of recommendations. These stages correspond respectively to the five complementary and iterative principles: know, understand, archive, learn and recommend. After presenting the

approach of the remaining FDF, the following paragraph deals with the adopted PHA method.

2.2. Preliminary Hazard Analysis (PHA)

The PHA method illustrated by figure 2, mainly based on a preliminary list of potential accidents turns on three complementary and iterative steps jointly including induction and deduction processes. The following paragraphs successively present a general and detailed description of the suggested methodology.

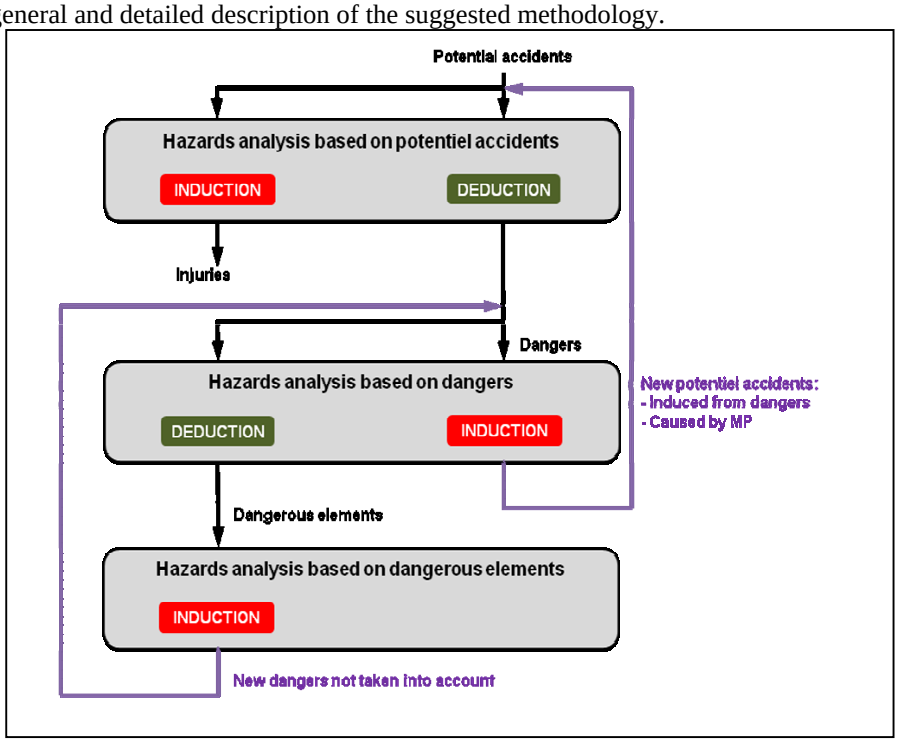

Fig. 2. General principle of PHA process

2.3. General description of the methodology

The article 5 of the decree n°2003-425 of May 9 2003 relative to the security of guided public transports [4] requires that "every new system of guided public transport, or every modification of an existing system is conceived and carried out in such a way that security global level towards users, exploitation personals be at least equivalent to the existing level of security or to the standard of existing systems securing comparable services" (principal GAME). The notion of equivalence introduced by the decree does nothing but introduces the objective of non regression of

security level in comparison with the standard of an existing system that is renowned to be sure.

It is at this level exactly that the FDF gives all its benefit. Indeed, being based on the results of technical inquiries, the process FDF purpose is to get profit out of actual experience to improve security level requiring taking into account some recommendations. Thus, it would be necessary and even essential to implement the recommended measures since the stage of specification of a new system (figure 3). So, our methodology guarantees the explicit implementation of the notion of equivalence of the principle GAME and consequently the improvement of security level. Up to now, the identification of the necessary potential accidents list to elaborate PHA is greatly based on experience and expertise of the domain.

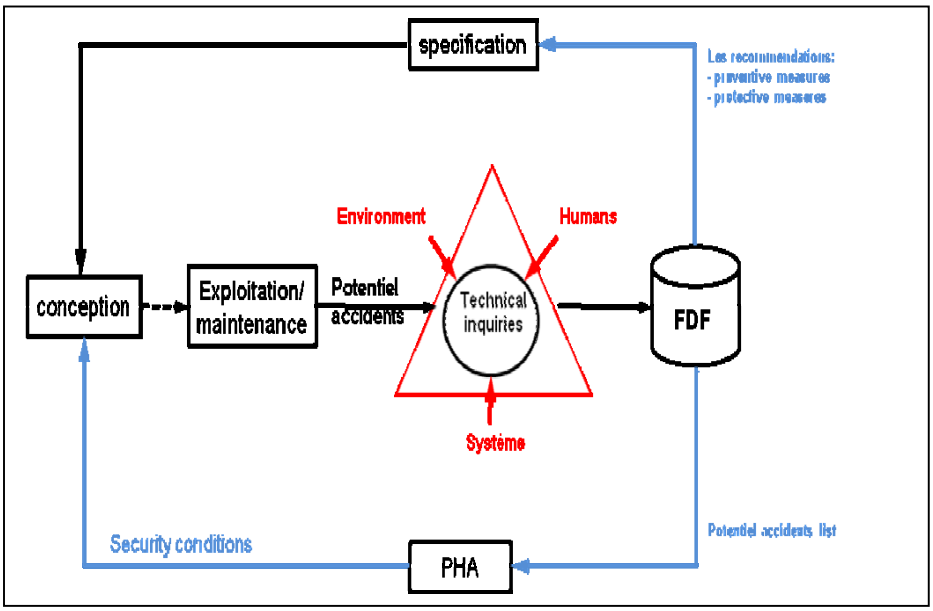

Fig. 3. General description of the suggested methodology

In fact, this task remains crucial for any system designer. Yet, the quality, the pertinence and completeness of the PHA file depends on potential accidents exhaustiveness. Moreover, as its name indicates it, the PHA generally remains open along the cycle of development project and constantly requires updating. To give an answer to this problem, we suggest exploiting systematically accidents scenarios provided by the FDF and particularly the potential accidents lists (figure 3). Thus, this approach contributes to improving the PHA quality. The PHA results allow to define the requirements and the criteria of system security to be taken into account during the stage of conception and carrying out of material and software equipments (figure 3).

2.4. Detailed description of the methodology

The suggested methodology, illustrated by figure 4, is based on a three situations' pattern interacting to guarantee PHA exhaustiveness and completeness.

2. 4.1. *Pattern stratums*

The nucleus of the suggested pattern is the kept PHA process, which turns on three complementary and iterative analysis: from potential accidents analysis, we deduce a hazards list; this hazards analysis allows to induce a potential accidents new list and at the same time to deduce the hazardous elements; thus, the hazardous elements analysis contributes to induction of hazards new list. On this nucleus, are superposed the five principles of the FDF: know the risk, understand file, learn it and at last suggest recommendations, making, in this way the second stratum of the pattern. These five principles of the FDF are combined with the five stages of: data collection related with insecurity event, analysis and processing, stocking and memorization, exploitation and use, and recommendations. The third and last stratum of the pattern is composed of the various steps of the system development cycle: specification, conception, carrying out, integration, authentication, certification, approval, putting into service, exploitation and maintenance.

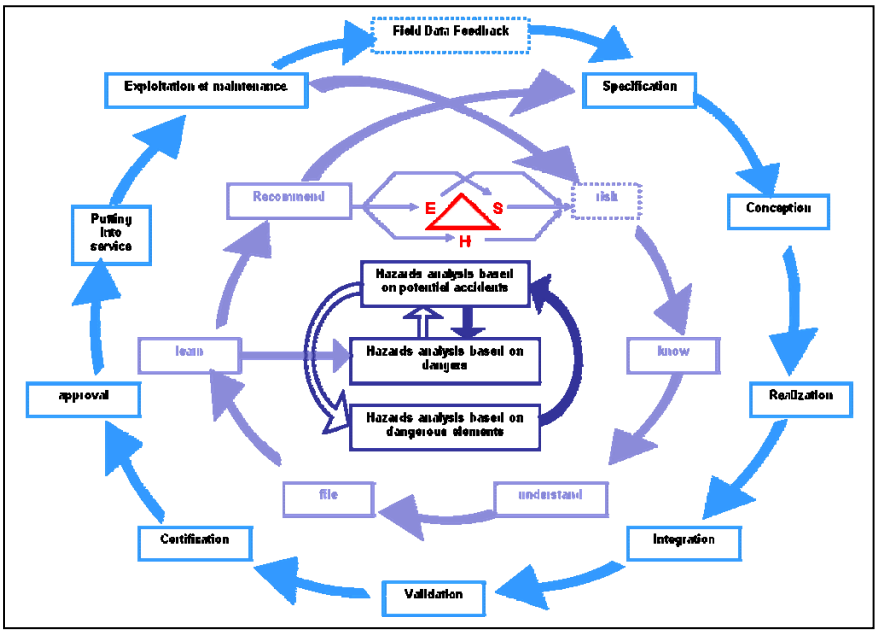

Fig. 4. Spiral pattern of FDF integration in PHA

2. 4.2. *Pattern articulations*

In fact, the methodology makes up a complementary and iterative compact pattern guaranteeing in this manner the interaction between these different stratums in a systematic way. Indeed, inconformity with the current regulation, security technical inquiries must be done after serious accidents / incidents occurring on the system taking into account the information relative to environmental, technological and human errors (figure 4). The first stage of FDF data gathering consists in finding out and collecting all the descriptive and explicative elements which have led to an insecurity event. Thus, this stage is based on the results stemming from the different inquiries reports (figure 4). After having analyzed and stocked the data already collected, the exploitation stage of the FDF process consists in using and interpreting these data. The main goal is to extract the really predicative event, to take into account the isolated cases and to predict or imagine future scenarios of accidents or undesirable events. From these stage results, we can explicitly extract the potential accidents lists and use them directly as entries to the PHA (figure 4).

Indeed, the ultimate stage of the FDF procedure consists in recommending prevention measures (in order to minimize the instance of potential accidents) and protection measures (to weaken the seriousness of created injuries). The aim of these recommendations is the action on the human factors, technical aspects and environment.

Systematically, these measures are taken into account from the specification in the development cycle of any new system in order to limit the reproduction of such an insecurity event (figure 4). The originality of our pattern consists in considering the FDF as being the fundamental link which connects exploitation towards the specification stage (figure 4). Thus, the suggested methodology guarantees the outline of the risks management following it since its appearance till the concrete implementation of protection and prevention measures.

3. Conclusion

The initial target of our methodology intends to improve the PHA completeness in order to have an exhaustive available list of potential accidents to take into account during the project development.

To apprehend this problem, we have suggested a pattern in three stratums including successively the steps of the PHA, the FDF process stages and the steps of a system development as well. The whole of these stratums interact between one another in an explicit manner.

We have demonstrated how to exploit systematically the results stemming from FDF, not only to bend to exhaustiveness of the potential accidents list (necessary to have at one’s disposal a solid PHA method), but also to draw lessons to be taken into account from the stage of project specification.

In this way, we have contributed to decrease the level of the system risk and consequently improve the system security. Despite the undeniable importance of this pattern, research tasks are in progress way in order to authenticate and demonstrate

the well-founded of the suggested approach through a real case stemming from the rail transport field.

References

[1] Décret n°2000-286 du 30 mars 2000 relatif à la sécurité du réseau ferroviaire national (RFN) et son arrêté d'application du 08 janvier 2002.
[2] HADJ-MABROUK A. et HADJ-MABROUK H. « Approche d'intégration de l'erreur humaine dans le retour d'expérience. Application au domaine de la sécurité des transports ferroviaires ». Synthèse INRETS n°43, février 2004, 104 p.
[3] HADJ-MABROUK H. « méthode d'analyse préliminaire des risques dans les transports ferroviaires ». 15ème congrès de maîtrise des risques et de Sûreté de fonctionnement, Lille, 10-12 Octobre 2006.
[4] Décret n°2003-425 du 9 mai 2003 relatif *à la* sécurité des transports publics guidés.
[5] HADJ-MABROUK H. « Réglementation en matière de retour d'expérience dans les transports ferroviaires ». Workshop International: Logistique & Transport 2006 (LT'2007) a technically IEEE/SMC co-sponsored workshop, 30 avril - 2 mai 2006, Hammamet - Tunisie.
[6] HADJ-MABROUK H. « Rôles et obligations des acteurs impliqués dans la sécurité des transports ferroviaires ». Congrès LM 14, Maîtrise des risques et sûreté de fonctionnement, Bourges, 12-14 octobre 2004.
[7] JOING M. et KERAVEL F. « Retour d'expérience et analyse des facteurs humains'. Revue générale des Chemins de Fer, Juin 1993, pp5 – 8.
[8] AMALBERTI R. et BARRIQUAULT C. « Fondements et limites du REX ». Annales des Ponts et Chaussées n°91, 1999.
[9] LOI 2002-3 du 03 janvier 2002 relative à la sécurité …, aux enquêtes techniques après événement de mer, accident ou incident de transport terrestre ou aérien …