Towards a computer-aided assessment of railway system preliminary hazard analysis

G. Chopard-Guillaumot\textsuperscript{a,b}, H. Hadj-Mabrouk\textsuperscript{a}, J.-G. Ganascia\textsuperscript{b}

\textsuperscript{a} Institut National de Recherche sur les Transports et leurs Sécurités, 94114 Arcueil, France
\textsuperscript{b} Laforia, Université Pierre et Marie Curie, F-75005 Paris, France

Abstract

Preliminary hazard analyses (PHAs) lack a precise and sound definition of their vocabulary, method and presentation format. The purpose of the work described in this paper is to improve the production and assessment of PHAs by providing experts with a software assistance. This paper presents the first stages of the study. These are: the definition of a basic vocabulary for PHAs, the definition of a new method for PHAs, the design of a tabular presentation of the results and, finally, the design of the software assistant architecture.

1 Introduction

By way of introduction, we shall give a brief review of the place and objective of preliminary hazard analyses (PHAs) in the framework of railway system safety analyses. We shall then describe the purpose of the work presented in this article.

1.1 A brief presentation of preliminary hazard analysis

Quoted in several standards, such as MIL-STD-882C [1], prEN 50126 [2] and IEC 56 (sec) 410 [3], preliminary hazard analysis belongs to the safety analyses that are ordinarily carried out before the construction of a guided transport system. PHA is generally considered to be the first part of the safety file for a railway system (Churchill [4]). It occurs very early in the development of the system, immediately after this has been specified. However, a PHA can be modified or enlarged during the design or construction of the system.

As for the main aims of the preliminary hazard analysis of a guided transport system, they are four in number:
1. to identify potential accidents which might affect the system,
2. to show the possible causes for potential accidents,
3. to evaluate the probability of these potential accidents occurring and the severity of the damage which they could cause,
4. to determine measures which could reduce the probability of potential accidents occurring and/or the severity of the damage which they could cause.

It is a fundamental document for achieving the safety of a guided transport system, as the quality of subsequent analyses, and hence that of the entire system, depends on that of the PHA (see Hadj-Mabrouk [5]).

1.2 Aim of the study

In the framework of its expertise activities, INRETS carries out appraisals of transport system safety files, such as those of the VAL in Lille, of the TVM430 speed control system or of the unmanned metro MAGGALY in Lyons. These safety files contain several hierarchical analyses, conducted by manufacturers, among which preliminary hazard analyses.

The examination of many cases has revealed a considerable difference in the way PHAs are dealt with from one manufacturer to another. This makes it even more difficult for INRETS to assess preliminary hazard analyses, and question the quality of the analysis as a whole.

With the support of the French national research programme for transport called PREDIT, INRETS decided to work at improving the PHA process. Two complementary directions of research have been chosen:
• our work addresses the harmonization of PHAs themselves, as regards the approach as well as the presentation of results;
• we also try to define an efficient assessment process of PHAs.

In both cases, on of the major goals of the study is to design and implement software tools that will assist experts in their respective tasks of performing and assessing preliminary hazard analyses. While our project has reached the implementation stage of a software assistant for PHAs, we take stock in this paper of the work done so far.

2 Four steps towards a software assistant for PHAs

As was pointed out above, PHA is, at the moment, ill-defined: if its aims are clearly identified, neither a precisely defined working method, nor a unique terminology and presentation format could emerge. The difficulty when building a tool for PHAs lies thus mainly in the necessity of better specifying the PHA itself. Therefore, before implementing the software, we had:
• firstly, to give a basic vocabulary for PHAs;
• secondly, to define a method for carrying out PHAs;
• lastly, to design a new presentation of the results of a PHA.

2.1 Definition of a basic vocabulary for PHAs

The terminology used in PHAs is not often defined and varies considerably
from one document to another. For instance, the same concept of "potential accident" may be called, according to the case: "potential accident" (in very few PHAs...), "effect", "consequence", "accident with consequences for the system", "hazard" or even "risk".

Figure 1: Semantic network of a basic vocabulary for PHAs (Chopard-Guillaumot [6]).
In order to find a widely recognized vocabulary we have reviewed some existing safety standards. After the analysis of sixteen documents, we could finally propose a coherent set of definitions [6]. We have created a semantic network as well to show the structure of the proposed definitions (Figure 1).

2.2 Definition of a method for PHAs

According to Lievens [7] and to Villemeur [8] the recommended method for preliminary hazard analysis is inductive. It consists in determining the potential accidents that may be provoked by some hazardous factors drawn from an ad hoc list. Some other attributes are also considered, such as the damage caused by the potential accidents and their severity. Appropriate prevention or protection measures are then described for each potential accident.

In actual practice, however, manufacturers often perform an approach that is an essentially deductive one: instead of hazardous factors, potential accidents are the starting point of a PHA. For each potential accident, all preceding hazards are identified. Yet, a description of prevention or protection measures remains the final part of this conventional, although poorly defined, method.

With the aim of improving the quality of PHAs in view, we have suggested to combine both the theoretical inductive method and the usual deductive approach [9]. This hybrid method can be broken down into three complementary analyses (Figure 2):

1. an inductive and deductive analysis on the basis of potential accidents,
2. an inductive and deductive analysis on the basis of hazards,
3. an inductive analysis on the basis of the factors which lead to hazards.

Thus, starting from an existing catalogue of potential accidents, a first analysis is carried out (stage 1). It allows to establish by induction a list of the damage that could cause an accident. A list of the hazards that may occur in the transport system is also determined by deduction.

In stage 2, it is made use of the previous list of hazards to identify all the hazardous factors (deductively) and all potential accidents (inductively). Drawing up the inventory of the potential accidents another time, but on the basis of the list of hazards, is an efficient validation procedure. It may add to the initial list of potential accidents, in which case the first stage must be carried out again for the previously missing potential accidents.

A third analysis (stage 3) consists in using the list of hazardous factors, an outcome of stage 2, for making a new inventory of hazards by induction. Again, this cross-validation process may result in revising the second stage and, possibly, the first one.

As for the other attributes of a preliminary hazard analysis, they are determined as they would in a conventional PHA.
Ultimately, then, the two main features of our recommended approach are the following:

- the introduction of "loops" in the construction of a PHA: these loops allow a cross-validation of the key attributes "hazards" and "potential accidents"; they help to reach a satisfactory level of completeness;
- the segmentation of the method in three independent stages: it is a good way to avoid redundant data and, consequently, to improve the coherence of PHAs.

2.3 Design of a presentation format for PHAs

After dealing with the methodological aspects of preliminary hazard analysis, we designed a new tabular presentation of the results of the analysis. This format facilitates the implementation of the method above. Because the approach is divided into three stages the presentation has also been broken into three separate tables (Figures 3 to 5).

Although PHAs are almost always shown in a tabular form, splitting the presentation of preliminary hazard analyses in this way is indeed uncommon! But it has the following advantages [9]:

1. The attributes related to hazards (e.g. hazardous factors) are clearly separated from those linked to potential accidents (e.g. level of probability).
2. As was stated above, no redundant data are required while filling the proposed tables. For instance, a given potential accident may appear many times in a regular PHA. As it usually comes with the evaluation of its level of severity, and because this level is therefore repeated as many times as the potential accident, there exists a real danger of incoherence. This is not possible, however, with the presentation tables that we have designed.
3. Lastly, since there are no redundant data (replaced by cross-references), the
<table>
<thead>
<tr>
<th>Potential accident no</th>
<th>Damage type</th>
<th>Level of severity</th>
<th>Hazards level of probability</th>
<th>Prevention or protection measures type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>I C</td>
<td></td>
<td>H0H1H2H3S0S1S2S3E0E1E2E3</td>
<td>A B C D SYDCNCRERM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1: individual
C: collective
0: no damage
1: not important
2: important
3: catastrophic
A: highly prob.
B: probable
C: improbable
D: highly impr.
SY: control and safety systems
DC: observance of standards
NC: calibrating, tests
RE: exploitation rules

Figure 3: Table of results for the analysis based on potential accidents (stage 1)

<table>
<thead>
<tr>
<th>Hazard no</th>
<th>Hazardous factors type</th>
<th>Circumstances mode</th>
<th>Potential accidents phase</th>
<th>Protection accidents place</th>
<th>Prevention or protection measures type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SYDCNCRERM</td>
<td></td>
</tr>
</tbody>
</table>

H: human
S: system
E: environment
SY: control and safety systems
DC: standards observance
NC: calibrating tests
RE: exploitation rules

Figure 4: Table of results for the analysis based on hazards (stage 2)
three tables we propose take less space than the presentation format we have seen.

<table>
<thead>
<tr>
<th>Hazardous factors</th>
<th>Hazards</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>no description</td>
<td>no description</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5: Table of results for the analysis based on hazardous factors (stage 3).

We have successfully filled our tables with data taken from the preliminary hazard analyses of two recent railway systems. Rewriting PHAs in the new format constitutes a first, albeit incomplete, empirical validation of the proposed tables.

2.4 Design of the architecture of a software assistant for PHAs

On the basis on the previous definitions (a vocabulary, an approach and a presentation format for preliminary hazard analyses), we are now designing and implementing, a software tool for aid in the production and assessment of PHAs. INRETS is well experienced in designing such tools (see, for example, Darricau [10] or Hadj-Mabrouk [11 & 12]). One of their main features is that they resort to artificial intelligence techniques.

As shown on figure 6, the functional architecture of our tool can be broken into five parts. These are:
1. a knowledge base;
2. a "production unit";
3. an "acquisition unit";
4. a "first level validation unit";
5. a "second level validation unit".

2.4.1 Knowledge base It is the heart of the software in that it contains all the necessary knowledge: the data collected from PHAs, the recommendations made during the assessment, but also the taxonomies of possible values for each attribute of PHA and some parameters representing experts’ preferences. All this knowledge is used in the production unit and in the second level validation unit.

2.4.2 Production unit This unit is being implemented. It provides experts with an aid for carrying out preliminary hazard analyses. It reproduces the tables presented in §2.3 and helps to fill them according to the method described in §2.2. To some extent it behaves like a computerized application guide for PHAs.

Moreover, it is able to show experts the data that appear in former PHAs: for instance it can recall all the potential accidents that have been associated to a specific hazard, or, if needed, only those potential accidents that are usually related to the hazard in question.
2.4.3 **Acquisition unit** Essentially, this unit can be looked as a subset of the production unit. It allows to rewrite a PHA that was not carried out according to our method, nor presented in the format that we have designed. It makes use of the vocabulary defined in §2.1, but does not take into account the method of §2.2.

2.4.4 **First level validation unit** A PHA carried out according to our method respects certain quality criteria by construction. However, the PHAs rewritten
with the help of the acquisition unit may infringe these criteria. It makes it necessary to check these later PHAs for "construction criteria" such as intrinsic coherence. For example, we must establish that a given potential accident has always the same level of criticity. If need be, remarks on the PHA under consideration are issued and transmitted to the second level unit.

2.4.5 Second level validation unit  As far as we know, no assessment method has ever been specified for PHAs. Until now, the thoroughness of the appraisal of PHAs has remained the product of the know-how, experience and intuition of assessors. The design of this second level validation unit may be, in this regard, the first attempt to define formally the assessment process.

Even though this unit is not yet totally specified, its main features are already set. In fact, the definition of this unit is inspired by works on the validation and verification of knowledge bases. In these works, as shown by Ayel [13], a knowledge base is compared with a "conceptual model", that is the requirements or constraints that the base is supposed to respect. We too need to ascertain criteria such as coherence or completeness, but our approach is different and original: instead of comparing a knowledge base with somewhat static and absolute requirements, the tool notes the differences between a new PHA and former ones, thus carrying out an experience-based assessment.

3 Conclusion

We have presented in this paper our work concerning the design and implementation of a software tool for aid in the production and assessment of preliminary hazard analyses. We have detailed the three stages prior to the definition of the tool: the definition of a vocabulary, the conception of a method and the design of a three-table presentation format for PHAs. Then, the functional architecture of the tool and its most striking features have been discussed.

On the basis of the experience related here, we think that it should be stressed out that no efficient computer aid may be provided for the assessment of a safety analysis if the analysis itself is not precisely defined. The main reason for this is that production process and assessment process are close ones, as it appears in the architecture of our tool.

As for computational techniques, they turned out inappropriate for our purpose, leading us to the definition of a new validation approach.

Ultimately, then, by attempting to provide assessors of PHAs with a tool we have revealed shortcomings in the performance of preliminary hazard analyses as well as in their assessment. Our researches constitute a partial answer to these weaknesses. Naturally, this answer requires further work but it is, as far as we know, the first one to be given.
502 Computers in Railways

References