SAFETY OF RAILWAY CONTROL SYSTEMS: A NEW PRELIMINARY RISK ANALYSIS APPROACH

F. GUENAB, J.-L. BOULANGER & W. SCHÖN
Heudiasyc Laboratory UMR CNRS 6599, Technology University of Compiegne, B.P. 20529, F-60205, Compiègne, France.

ABSTRACT

Preliminary risk analysis (PRA) is a methodology used in critical systems safety studies. It is primarily used at the preliminary stage of the system's design so as to determine the scenarios of potential accidents, to evaluate their probabilities of occurrence (frequency) as well as the severity of the resulting consequences and to propose solutions (preventive and/or mitigative safeguards) in order to reduce the risk level in terms of severity/occurrence (to reduce the frequency of the contributors or reduce the severity of the accident). The PRA was largely used in several industrial fields (aeronautics, weapons systems, chemistry, railways etc.) in order to study the safety of the systems. From one field to another, from one expert to another, many extremely different approaches and methods are used to carry out this analysis. Moreover, the formats representing the results of the PRA are often varied as well as the terminology and the concepts related to the PRA.

The main goal of this paper, completed within the framework of the ANR-PREDIT-SECUGUIDE project (project financed by the National Agency for Research – France. It aims to study the impact of introducing the New Information and Communication Technologies (NICT) into railway systems safety) is to propose a PRA method and to determine standard contents of PRA to be used in the context of the railway control systems by taking into account the impact of NICT.

Keywords: automatic train control, feared events, new information and communication technologies (NICT), preliminary risk analysis (PRA), potential accident, railway safety, risk.

1 INTRODUCTION

Ensuring railway systems safety requires knowledge of all lifecycle phases of these systems. Upstream and downstream phases (concept, definition of the system and its application's conditions, acceptance of the system, operating and maintenance, monitoring of the performances, modifications) are essentially the responsibility for the owners and the official authorities. The central phases of the lifecycle (risks analysis, system requirements, safety requirements allocation, design and realization, manufacture, installation, and validation) are essentially the responsibility of the railway systems suppliers. Within the framework of export businesses, manufacturers take also more and more responsibility in the phases upstream and downstream. The phases corresponding to responsibility transfers between actors are obviously crucial.

Current railway standards EN 50126 [1], EN 50128 [2] and EN 50129 [3] are regularly revised to take into account the permanent technological projections in the electronic materials fields and in the data-processing techniques. Those have an important impact on the railway systems design. However, the standards have not yet formalized the process of the distribution of safety regulations of the railway system on its supporting subsystems, hardware and software. In other words, if the risks are well identified and followed through with demonstrations and safety justifications, it remains to improve the risks analysis and safety requirements allocation steps.

The objective of this work is to propose a method and standard contents for a preliminary risk analysis (PRA) in the context of railway signalling and command and control systems.

This method will integrate the impact of the New Information and Communication Technologies (NICT) on safety in terms of risks induced on the whole system. The evolution of the systems design passes by the integration of the NICT. The NICT are considered as components off the shelf (COTS). The COTS allow one to control the cost of system realization, but on the other hand there is a loss of safety control [4]. Thus, the proposed method will have to take into account the inherent risks in this type of component. Another constraint relates to taking into account human errors.

This paper is organized as follows. Section 2 is dedicated to the columns definition of the PRA and a PRA method is proposed in Section 3. Section 4 is devoted to the description of the phases of the PRA method presented previously. Finally, concluding remarks and perspectives are given in the last section.

2 COLUMNS DEFINITION OF PRELIMINARY RISK ANALYSIS

Since the results of the PRA are presented in a worksheet, along with the various definitions of the terms and concepts related to the PRA, we dedicate this section to detailing these concepts. Based on CENELEC standards EN 50126 [1], EN 50128 [2], EN 50129 [3] and EN 61508-4 [5], we propose definitions of the columns of PRA applied to the railway control systems. A standardization of the principal concepts and associated terminology is indeed proved to be necessary, after study of several railways PRA from various sources (manufacturers, owners etc.), where important inconsistencies could be noted (e.g. the same term is used for different concepts).

- **Operating mode** (exploitation mode, or working mode, or phase or context): knowing that the analysis of hazards and risks is carried out for all the reasonably foreseeable situations, which justifies this column. It is useless to consider a safety measurement "the platform doors must be strictly closed" for a metro that is on line, even in a station where platform doors do not exist… In some cases, it is not mandatory to specify the operating mode.
- **Dangerous entity** (or dangerous element, or hazardous entity/element): a subset of the studied system which is at the origin of the feared event, it is the initial cause of the studied scenario. The function of the dangerous entity can be specified if necessary.
- **Feared event** (or event causing a dangerous situation, or undesirable event, or error): is a dangerous event, it is the event affecting the dangerous entity or its function leading the system in a dangerous situation.
- **Dangerous situation** (or danger): undesirable state of system following the feared event, may lead to a potential accident.
- **Damage** (or consequence): is the result of an accident given in terms of death, physical wounds, injuries, attack on people's health or environment damage.
- **Severity level:** a classification on several levels, it allows one to evaluate and estimate the consequences of potential accidents. According to EN 50126 [1], Table 1 describes typical hazard severity levels and the consequences associated with each severity level for railway systems. In order to avoid improper interpretations of the qualitative terms, some industrialists and/or owners use numbers to describe severity levels (from 1 to 4 in order of increasing severity, where 4=catastrophic).
- **Frequency of occurrence:** the probability of the sequences of events. Qualitative evaluation EN 50126 [1] of the probability or frequency of occurrence of a hazardous event. A description of each category is proposed in Table 2.

Table 1: Hazard severity level.

Severity level	Consequence to persons or environment	Consequence to service
Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment.	
Critical	Single fatality and/or severe injury and/or significant damage to the environment.	Loss of a major system
Marginal	Minor injury and/or significant threat to the environment	Severe system(s) damage
Insignificant	Possible minor injury	Minor system damage

Table 2: Frequency of occurrence of hazardous events.

Category	Description
Frequent	Likely to occur frequently. The hazard will be continually experienced
Probable	Will occur several times. The hazard can be expected to occur often
Occasional	Likely to occur several times. The hazard can be expected to occur several times
Remote	Likely to occur sometime in the system life cycle. The hazard can reasonably expected to occur
Improbable	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur.
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur.

- **Measurements** (safety measures, safety constraints or safety requirements): suitable actions to reduce or eliminate risk. They can be preventive measures or protection measures. This column could describe the subsystem (equipment, system etc.) charged to ensure the safety measures (responsible entity of risk reduction) and its reference.

- **Event causing a potential accident:** it is a dangerous event that transforms a dangerous situation into a potential accident. It does not exist in the case of scenarios of order 1. Columns could appear in the PRA, for the sequences of dangerous events, which allow a dangerous situation to become an accident; this depends on the order of the studied scenario.
- **Potential accident:** a potential accident could be an accident or quasi accident. The effective occurrence of damages (e.g. collision) determines the accidental identity of the potential accident else it is an incident (e.g. crossing over a restrictive signal without an effective collision).

3 PROPOSED METHOD
In Villemeur [6], the objective of the PRA method is:

- To determine thdangers (hazards) and their causes (dangerous entities, dangerous situations, potential accidents).
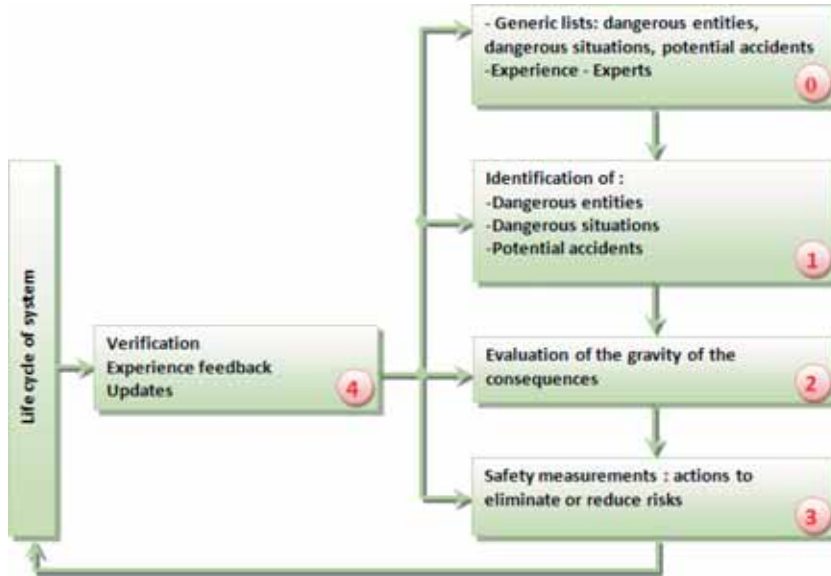
Figure 1: Steps of preliminary risk analysis.

 - To evaluate the severity of the consequences of situations and accidents previously determined.
 - To deduce the measurement and the suitable actions to eliminate or reduce dangerous situations and the potential accidents.

Figure 1 summarizes these steps. The identification of dangerous entities, dangerous situations and the potential accidents rests at the beginning on the experiment and the judgment of the specialists, helped by guide lists which are updated by the experience feedback throughout the lifecycle of the system.

The PRA is generally considered as an inductive approach (proceed from causes to identify consequences); however, certain actors consider it as a deductive approach. A deductive or inductive analysis does not relate to the general method described by Fig. 1 but only to the first step (1): identification of dangerous entities, dangerous situations and potential accidents. During this step, some experts determine the set of potential accidents (consequences) by induction on the basis of the dangerous entities (causes); other experts proceed by deduction to identify the dangerous entities or the dangerous events (causes) from the potential accidents (consequences). When we dispose of a complete list of all potential accidents (dangerous entities/feared events) the deductive approach (inductive approach) alone is valid and lead to acceptable results covering all possible scenarios. On the other hand for systems having a significant number of scenarios and if we do not dispose of complete lists of potential accidents (dangerous entities/feared events), using only deductive approach (inductive approach) is not efficient. In these cases, it is possible that the used approach does not take into account the potential accidents (dangerous entities/feared events) not included in the generic list. To avoid this problem and to have complete results, a deductive–inductive approach should be used.

Figure 2 represents the first step (1) of the PRA illustrated by Fig. 1.
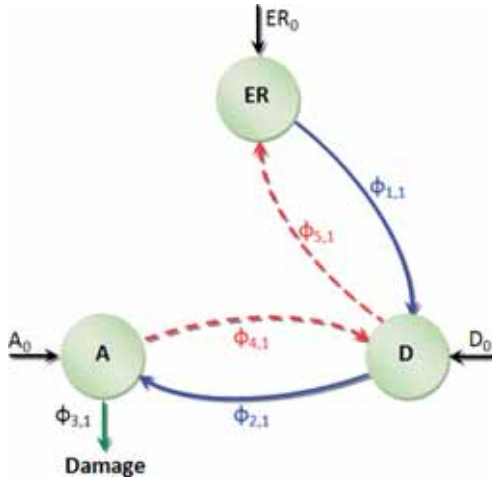
Figure 2: First step of the PRA method.

- ER_0, D_0 and A_0 are the preliminary lists (initial) of dangerous entities/feared events, dangers and potential accidents, respectively. They are defined starting from the generic lists analyzed by experts; the latter can remove incoherent scenarios or add other missing scenarios. We consider that we obtained these lists resulting from the initialization step (step (0) of Fig. 1).
- ER_0, D_0 and A_0 represent the lists of dangerous entities/feared events, dangers and potential accidents, respectively. At the beginning of the analysis they are initialized at ER_0, D_0 and A_0 and they contain the final lists at the end of the analysis.
- The step contains several cyclic phases: two inductive phases (solid line), two deductive phases (broken line) and a phase to generate the list of the consequences (damages) generated by the potential accidents. The phases are noted $\varphi_{i,j}$:
  Where the index "i" indicates the number of phase and the index "j" indicates the current cycle. i.e. $\varphi_{4,1}$ is the 4th phase of the 1st cycle.
- The cycles start with index 1 ($j > 0$), in other words, the first cycle of this step corresponds to "$j = 1$".
- At the beginning of a cycle "j", the sets of the dangerous entities/feared events, dangers and potential accidents are indexed by "$j-1$", ER_{j-1}, D_{j-1} and A_{j-1}. For example at the beginning of cycle 1, the sets ER, D and A are equal to ER_0, D_0 and A_0, respectively.

4 PROCEDURE FOR THE PROPOSED PRA METHOD

In this paragraph we will present the various phases of PRA method presented in the previous paragraph.

At the beginning of cycle 1, the lists of feared events, dangers and potential accidents are initialized at ER_0, D_0 and A_0.

Phase 1 (inductive phase) allows determining the dangers starting from the feared events (Fig. 3).

During this phase, the list ER_0 can generate a list of dangers that corresponds to:

- A part of the preliminary list noted $D_0' \subseteq D_0$. We note by D_0'' the remaining part of the preliminary list D_0 *and*.
- A new list of dangers noted $D_0'^n$ which is added to the preliminary list.

At the end of this phase, the new list of dangers is $\mathbf{D_0} \cup \mathbf{D_0'}^\mathbf{n}$ or $\mathbf{D_0'} \cup \mathbf{D_0''} \cup \mathbf{D_0'}^\mathbf{n}$. The only sub-list of dangers that does not have correspondence in the list of the feared events is $\mathbf{D_0''}$.

Phase 2 allows determining the potential accidents from dangers (inductive phase). During this phase, list of dangers generated from the previous phase ($\mathbf{D_0} \cup \mathbf{D'_0}^\mathbf{n}$) allows generating a list of potential accidents that corresponds to:

- A part of the preliminary list noted $\mathbf{A_0'} \subseteq \mathbf{A_0}$. We note by $\mathbf{A_0''}$ the remaining part of the preliminary $\mathbf{A_0}$ *and*
- A new list of accidents noted $\mathbf{A_0'}^\mathbf{n}$, it is added to the preliminary list.

At the end of this phase, the new list of accidents is $\mathbf{A_0} \cup \mathbf{A_0'}^\mathbf{n}$ or $\mathbf{A_0'} \cup \mathbf{A_0''} \cup \mathbf{A_0'}^\mathbf{n}$.

Phase 3 is used to identify the damages (consequences) from the list of the accidents obtained at the end of the previous phase ($\mathbf{A'_0} \cup \mathbf{A_0''} \cup \mathbf{A_0'}^\mathbf{n}$). It is noted $\mathbf{Dom_1}$.

Phase 4: Knowing that the only sub-list of the potential accidents that does not have correspondence in the dangers list is $\mathbf{A_0''}$, this phase allows determining the possible dangers from the sub-list $\mathbf{A_0''}$ (deductive phase). We note by $\mathbf{D_0''}^\mathbf{n}$ the new obtained list of dangers.
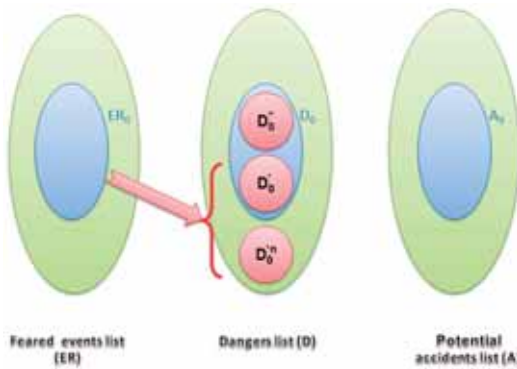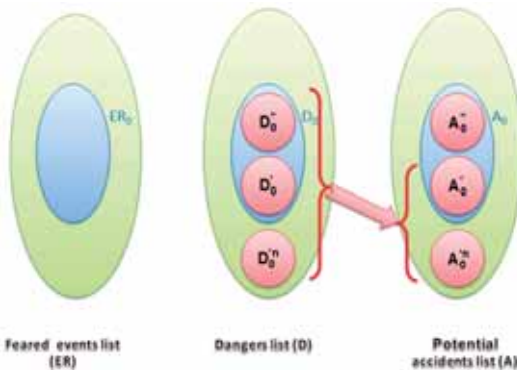

Figure 3: Phase 1.

Figure 4: Phase 2.

At the end of this phase, the new list of dangers is $D_0 \cup D_0'^n \cup D_0''^n$ or $D_0' \cup D_0'' \cup D_0'^n \cup D_0''^n$.

Phase 5: this phase allows determining the feared events list from dangers. The sub-list of dangers that does not have correspondence in the feared events list is $D_0'' \cup D_0''^n$. We note by $ER_0'^n$ the feared events list, which is obtained from this phase, and it corresponds to the dangers list $D_0'' \cup D_0''^n$.
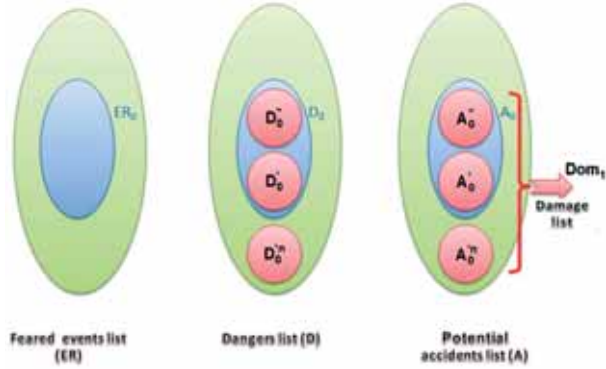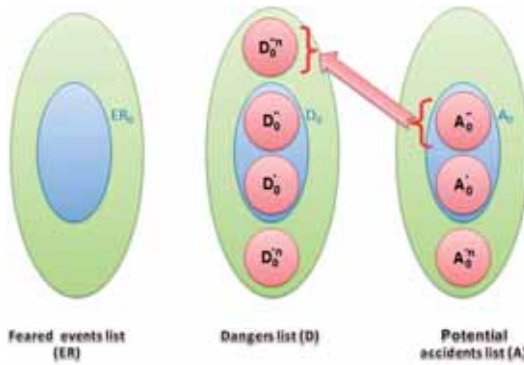

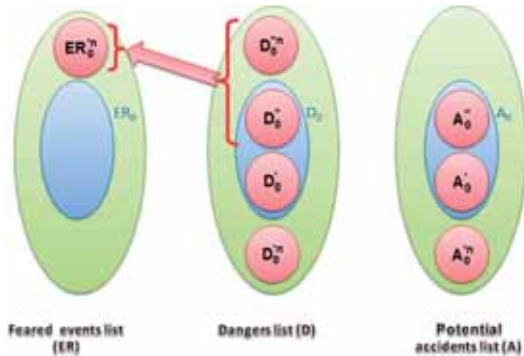Figure 5: Phase 3.

Figure 6: Phase 4.

Figure 7: Phase 5.

At the end of cycle 1, lists **ER**, **D** and **A** are given as follows:

$$\mathbf{ER_1 = ER_0 \cup ER_0'^n}$$
$$\mathbf{D_1 = D_0 \cup D_0'^n \cup D_0''^n = D_0' \cup D_0'' \cup D_0'^n \cup D_0''^n}$$
$$\mathbf{A_1 = A_0 \cup A_0'^n = A_0' \cup A_0'' \cup A_0'^n}$$

From these new lists, we start a new cycle with the same described phases.

The necessary and sufficient condition to stop analysis if during a given cycle defined by index $j = f$:

- Phase $\varphi_{1,f}$ does not generate any more new dangers, *and*
- Phase $\varphi_{2,f}$ does not generate anymore new potential accident.

   In another manner:

- $\mathbf{D_{f\text{-}1}'^n} = \varnothing$ and $\mathbf{A_{f\text{-}1}'^n} = \varnothing$. (e.g. during cycle **1**, we stop analysis if the two lists $\mathbf{D_0'^n} = \varnothing$ and $\mathbf{A_0'^n} = \varnothing$).

   Note that the analysis could also be performed from the potential accidents to the feared events (opposite direction of the cycle). This by reversing the order of the phases in the following way: the cycle starts with phases 4 and 3, phase 5, then the phase 1 and finishes by phase 2.

5 CONCLUSIONS

This paper has presented a PRA method in the context of the railway systems. After presenting the definitions of the used terms in a PRA, we proposed a PRA method using the two approaches: deductive and inductive.

   Our research perspectives are articulated around two points:

- To propose standard contents of the PRA and to develop a method of analysis regarding the command–control and signalling aspects (NICT aspects) of railway systems.
- To formalize links between the functionalities and/or techniques of the NICT and the standard PRA, in order to identify the new risks induced by the NICT and the safety measures to be taken to reduce these risks levels.

REFERENCES

[1] **EN 50126.** Railway Applications –The specification and demonstration of dependability – reliability, availability, maintainability and safety (RAMS). CENELEC. September 1999.
[2] **EN 50128.** Railway Applications – Software for railway control and protection systems. CENELEC.
[3] **EN50129.** Railway Applications – Safety related systems for signalling. CENELEC.
[4] Boulanger, J.L. & Schön, W., Reference systems and standards for safety assessment of railway applications. *ESREL 2007*, Stavanger: Norway, pp. 2609–2613, 2007.

[5] **EN 61508-4.** Functional Safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations. CENELEC.
[6] Villemeur, A., *Sûreté de fonctionnement des systèmes industriels : fiabilitéacteurs humains informatisation*, EYROLLES, Paris, 1988.