Safety of railway control systems: A new Preliminary Risk Analysis approach

Fateh Guenab, Jean-Louis Boulanger, Walter Schön

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,
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 preliminary risk analysis was largely used in several industrial fields (aeronautics, weapons systems, chemistry, railway...) 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 project ANR-PREDIT-SECUGUIDE[1], is to propose a PRA method and to determine standard contents of PRA to be used in the context of the railway systems.**

Keywords - **Railway safety, Preliminary risk analysis (PRA), risk, potential accident, feared events, Automatic Train Control.**

I. INTRODUCTION

Ensuring railway systems safety requires knowledge of all life cycle 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 responsibilities in the phases upstream and downstream. The phases corresponding to responsibilities transfers between actors are obviously crucial.

[1] ANR-PREDIT-SECUGUIDE is a project financed by the National Agency for Research - France (http://www.agence-nationale-recherche.fr) which began in January 2006 per 3 years duration. The project aims to study the impact of introducing the NICT into the railway systems on safety.

Current railway standards [1], [2] and [3] were 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 did not formalize yet well the process of distribution of the safety regulations of the railway system on its subsystems, hardware and software which supports them. In other words, if the risks are well identified and followed through demonstrations and safety justifications, it remains to improve the Risks Analysis and Safety Requirements Allocation steps. Authors of [7] have examined the methods for risk analysis and assessment of safety activities and proposed optimized one method for risk estimation.

The objective of this work is to propose a method and standard contents for a PRA in the context of railway signalling and command and control systems. This method will integrate the impact of the 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 controlling the cost of system realization, but on the other hand there is a loss of safety control [6]. Thus the proposed method will have to take into account the inherent risks in this type of component. Another constraint relates to the taking into account of the human errors.

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

II. COLUMNS DEFINITIONS OF PRELIMINARY RISK ANALYSIS

Knowing that the results of the Preliminary Risk Analysis are presented in a worksheet and the various definitions of the terms and concepts related to the PRA, we dedicate this section to detail these concepts. Basing on CENELEC standards [1], [2], [3] and [4] 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 of various sources (manufacturers, owners...), where

important inconsistencies could be noted (for example 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 which is on line, even in station where the platform doors don't 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): it is result of an accident given in terms of death, physical wound, injuries, attack to people health or environment damage.
- **Severity level:** a classification on several levels, it allows to evaluate and estimate the consequences of potential accidents. According to [1], Table I describes typical hazard severity levels and the consequences associated with each severity level for railway systems. In order to avoid bad interpretations of the qualitative terms, some manufacturers and/or owners use numbers to describe severity levels (from 1 to 4 in order of increasing severity, 4 = catastrophic).
- **Frequency of Occurrence**: probability of the sequences of events. As in [1], qualitative evaluation of probability or frequency of occurrence of a hazardous event and a description of each category is proposed in Table II.

TABLE I
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 damage
Insignificant	Possible minor injury	Minor system damage

TABLE II
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 which allows reducing the probabilities of occurrences of the dangerous events or protection measures by using safety devices allowing reducing the severity of damage. This column could describe the subsystem (equipment, system…) charged to ensure the safety measures
- **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 passing from a dangerous situation to an accident, this depends on the studied scenario order.
- **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 effective collision).

III. PROPOSED METHOD

The objective of Preliminary Risk Analysis method is [5]:

- To determine the dangers (hazards) and their causes (dangerous entities, dangerous situations and potential accidents).
- 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.

Fig. 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.

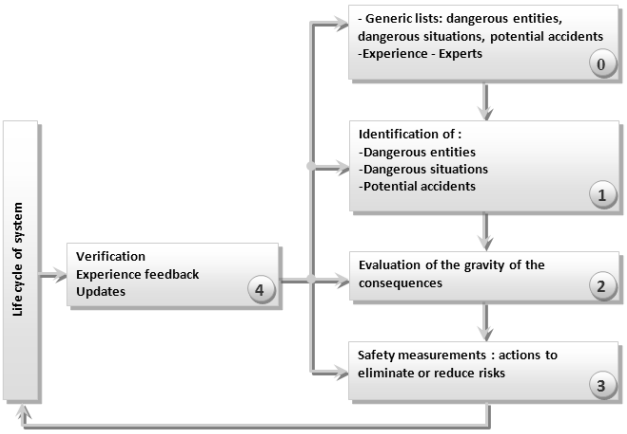


Fig. 1. Steps of Preliminary Risk Analysis

The PRA is generally considered as an inductive approach (proceed from causes to identify consequences), however some 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 (respectively dangerous entities / feared events) the deductive approach (respectively 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 don't dispose of complete lists of potential accidents (respectively dangerous entities / feared events), using only deductive approach (respectively inductive approach) is not efficient. In these cases, it is possible that the used approach does not take into account the potential accidents (respectively dangerous entities / feared events) not included in the generic list. To avoid this problem, a deductive-inductive approach should be used.

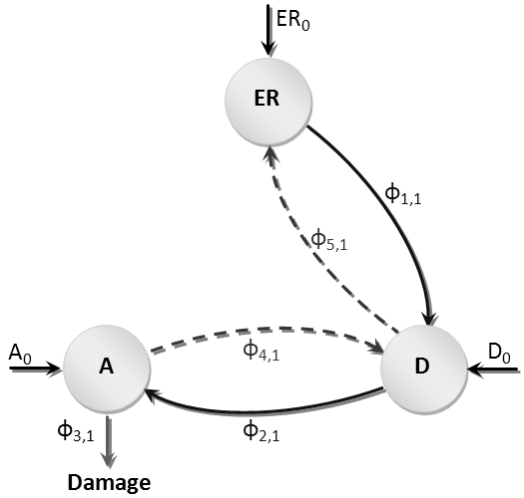


Fig.2. first step of PRA method.

Fig. 2 represents the first step (1) of the PRA illustrated by Fig. 1.

- $\mathbf{ER_0}$, $\mathbf{D_0}$ and $\mathbf{A_0}$ are the preliminary lists of dangerous entities /feared events, dangers and potential accidents respectively. They are defined from the generic lists analyzed by experts; the latter can remove incoherent scenarios or add other missing scenarios. These lists are obtained from the initialization step (step (0) of Fig. 1).
- **ER**, **D** and **A** represent the lists of dangerous entities/feared events, dangers and potential accidents respectively. At the beginning of the analysis they are initialized at $\mathbf{ER_0}$, $\mathbf{D_0}$ and $\mathbf{A_0}$ 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 $\phi_{i,j}$:

  Where the index « *i* » indicates the number of phase and the index « *j* » indicates the current cycle. i.e. $\phi_{4,1}$ is the 4^{th} phase of the 1^{st} 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* », $\mathbf{ER_{j-1}}$, $\mathbf{D_{j-1}}$ and $\mathbf{A_{j-1}}$. For example at the beginning of cycle 1, the sets **ER**, **D** and **A** are equal to $\mathbf{ER_0}$, $\mathbf{D_0}$ and $\mathbf{A_0}$ respectively.

IV. PROCEDURE FOR 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 $\mathbf{ER_0}$, $\mathbf{D_0}$ and $\mathbf{A_0}$

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

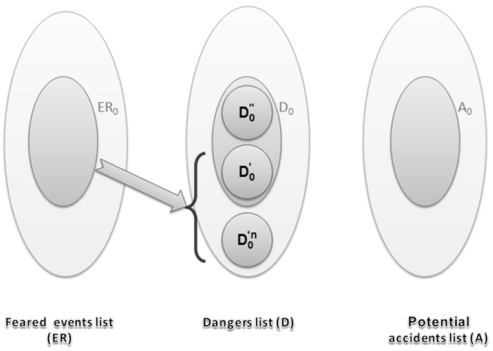


Fig. 3. Phase 1

During this phase, the list $\mathbf{ER_0}$ can generate a list of dangers that corresponds to:

- A part of the preliminary list noted $\mathbf{D_0^{'}} \subseteq \mathbf{D_0}$. We note by $\mathbf{D_0^{''}}$ the remaining part of the preliminary list $\mathbf{D_0}$.

- **And** a new list of dangers noted $\mathbf{D_0^{'n}}$ which is added to the preliminary list.

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

Phase 2 (Fig. 4) allows determining the potential accidents from dangers. During this phase, list of dangers generated from the previous phase ($\mathbf{D_0 \cup D_0^{'n}}$) allows generating a list of potential accidents that corresponds to:

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

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

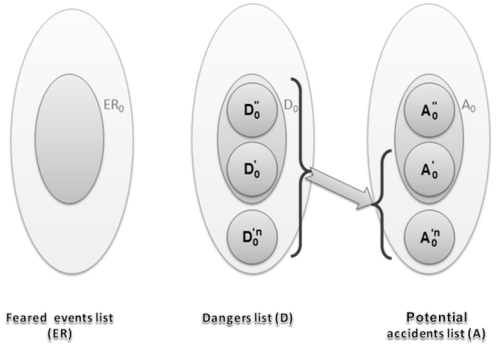


Fig. 4. Phase 2

Phase 3 (Fig. 5) is used to identify the damages from the list of the accidents obtained at the end of the previous phase ($\mathbf{A_0^{'} \cup A_0^{''} \cup A_0^{'n}}$). It is noted $\mathbf{Dom_1}$.

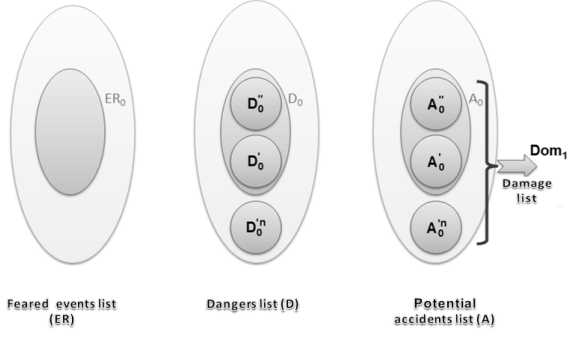


Fig. 5. Phase 3

Phase 4 (Fig.6): Knowing that the only sub-list of the potential accidents which 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 $\mathbf{D_0^{''n}}$ the new obtained list of dangers.

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

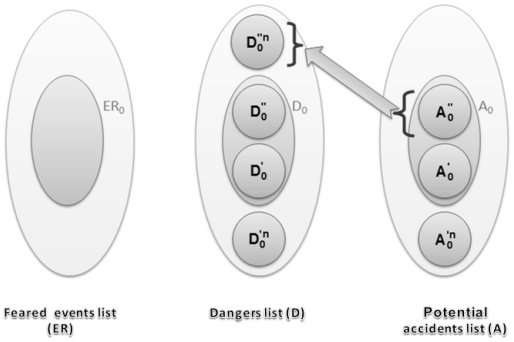


Fig. 6. Phase 4

Phase 5 (Fig. 7): This phase allows determining the feared events list from dangers (deductive phase). The sub-list of dangers which does not have correspondence in the feared events list is $\mathbf{D_0^{''} \cup D_0^{''n}}$. We note by $\mathbf{ER_0^{'n}}$ the feared events list which is obtained from this phase and it corresponds to the dangers list $\mathbf{D_0^{''} \cup D_0^{''n}}$.

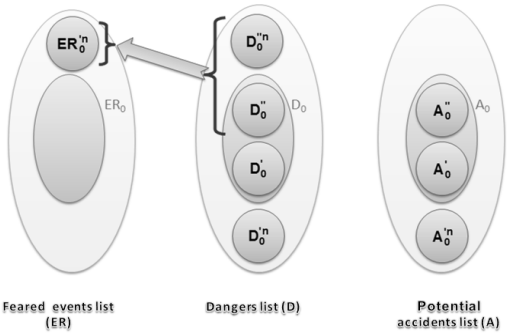


Fig. 7. Phase 5

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

$$\mathbf{ER_1 = ER_0 \cup ER_0^{'n}}$$

$$\mathbf{D_1 = D_0 \cup D_0^{'n} \cup D_0^{''n} = D_0^{'} \cup D_0^{''} \cup D_0^{'n} \cup D_0^{''n}}$$

$$\mathbf{A_1 = A_0 \cup A_0^{'n} = A_0^{'} \cup A_0^{''} \cup A_0^{'n}}$$

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

In another manner: $\mathbf{D_{f-1}^{'n} = \emptyset}$ and $\mathbf{A_{f-1}^{'n} = \emptyset}$.

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 finished by phase 2.

V. EXAMPLE

1) *Scenario description:*

Let us consider system with:

Six feared events er_i, six dangerous situations d_i and six potential accidents a_i where $i = 1..6$.

Each dangerous event er_i could cause a dangerous situation d_i leading to a potential accident a_i and each accident lead to damage dom_i. Moreover,

- The dangerous event n°5 (er_5) lead to two dangerous situations d_4 and d_5.
- The dangerous situation n°4 (d_4) produce two potential accidents a_4 and a_6.

Note that this description is not known a priori, the guide lists **ER₀**, **D₀** and **A₀** are the only known information.

Let us suppose that the guide lists (preliminary lists) are given by the following sets:

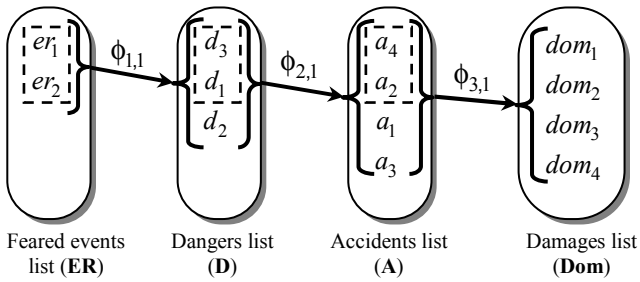
$\mathbf{ER_0} = \{er_1, er_2\}$, $\mathbf{D_0} = \{d_1, d_3\}$ and $\mathbf{A_0} = \{a_2, a_4\}$

2) *Phases of the analysis*

Cycle n°1

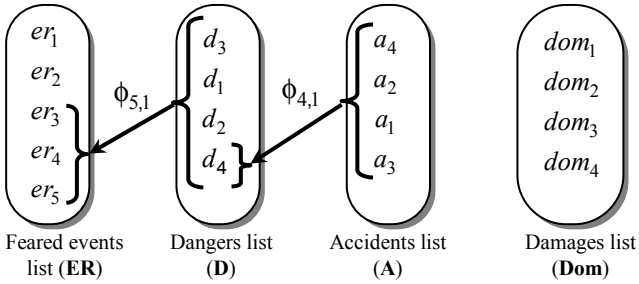
The preliminary lists **ER₀**, **D₀** and **A₀** are represented by dashed square. The damages set **Dom** is initially empty.

- Phases $\phi_{1,1}$, $\phi_{2,1}$ and $\phi_{3,1}$



From preliminary set **ER₀**, the first phase $\phi_{1,1}$ generates a new danger d_2 which is added to the dangers set **D.** it becomes $\mathbf{D}=\mathbf{D_0} \cup \{d_2\} = \{d_1, d_2, d_3\}$. The second phase $\phi_{2,1}$ generates, from $\mathbf{D}=\{d_1, d_2, d_3\}$, two new accidents a_1 and a_3 then the new accident list is given by $\mathbf{A}=\mathbf{A_0} \cup \{a_1, a_3\} = \{a_1, a_2, a_3, a_4\}$. Finally, the damages list produced by the third phase $\phi_{3,1}$ is $\mathbf{Dom}=\{dom_1, dom_2, dom_3, dom_4\}$.

- Phases $\phi_{4,1}$ and $\phi_{5,1}$



The phase $\phi_{4,1}$ generates a new dangerous situation d_4 and the phase $\phi_{5,1}$ produces three new feared events er_1, er_2, er_3. The conditions to stop analysis are not sufficient, thus new cycle must be performed.

Cycle n°2

The same phases are repeated during the second cycle. At the end of this cycle, the obtained lists are given by:

$\mathbf{ER} = \{er_1, er_2, er_3, er_4, er_5, er_6\}$, $\mathbf{D} = \{d_1, d_2, d_3, d_4, d_5, d_6\}$, $\mathbf{A} = \{a_1, a_2, a_3, a_4, a_5, a_6\}$,

$\mathbf{Dom}=\{dom_1, dom_2, dom_3, dom_4, dom_5, dom_6\}$.

Cycle n°3

During this cycle, phases $\phi_{1,3}$ and $\phi_{2,3}$ do not generate anymore new dangers and accidents respectively. It is sufficient condition to stop the analysis.

Note that the analysis has covered all accidents scenarios contrary if only deductive approach (or inductive approach) was used.

VI. CONCLUSION

This paper has presented a Preliminary Risks Analysis 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. Then an example is proposed to illustrate the approach. Our research perspectives are articulated around two points:

- To propose standard contents of the Preliminary Risks Analysis and to develop a method of analysis regarding the command-control and signalling 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.

[2] **EN 50128.** "Railway Applications – Software for railway control and protection systems". CENELEC

[3] **EN50129.** "Railway Applications – Safety related systems for signalling". CENELEC

[4] **EN 61508-4.** "Functional Safety of electrical / electronic / programmable electronic safety related systems – Part 4: Definitions and abbreviations". CENELEC

[5] A. Villemeur, "Sûreté de fonctionnement des systèmes industriels : fiabilité- acteurs humains informatisation", *EYROLLES* 1988.

[6] J.L. Boulanger, W. Schön, "Reference systems and standards for safety assessment of railway applications", in *ESREL 2007*, Stavanger, Norway, pages 2609-2613.

[7] H.J. Jo; J.G. Hwang,"Investigation of risk analysis methods for safety assurance in the train control system", *Electrical Machines & Systems, 2007. ICEMS*, pages 1858-1862