ANALYZING THE PERFORMANCE OBJECTIVES REGARDING THE SAFETY OF AN ELECTRONIC SYSTEM FOR CENTRALISED COMMAND OF RAILWAY STATIONS

Corneliu Mihail ALEXANDRESCU, University "Politehnica" of Bucharest, Transports Faculty, Bucharest, Romania
Iulian BĂDESCU, University "Politehnica" of Bucharest, Transports Faculty, Bucharest, Romania
Ilias NICOLAE, University of Petrosani
Aurelian NICOLA, SC General Trans AS, Petrosani, Romania

This paper presents several results of a applicative research program, which objective was the technical and scientific foundation of a Romanian solution for obtaining an electronic system based on information technology, dedicated to centralized control of a railway station. The results contain the definition of the safety objectives for the system, global and in detail, at subsystem and module level. The realization of the determined safety objectives according to the presented methods confers the guaranty of safe system behavior, according to the applicable CENELEC standards and to the CFR safety politics.

Introduction

The paper presents results of an applicative research programme which objective was to substantiate, technically and scientifically, a Romanian solution for the realisation of an electronic system, based on information technology, dedicated to centralised control of a railway station.

The Romanian Railway has drastic regulation regarding the railway safety that must be strictly kept by any electronic interlocking system. There are three main European standards (elaborated by CENELEC – *European Committee for Electrotechnical Standardization*) dedicated to the railway systems safety: EN50126, EN50128, EN50129. Any railway safety system, and most of all the electronic interlocking systems, must be developed, tested, verified, validated, installed, maintained, operated and delivered (for the entire life cycle) according to the mentioned standards.

The European standards for railway systems, like any standards, define what it must be done, but not how it has to be done. And exactly "how it has to be done" represents the subject of this research programme. In the present paper we will offer several solutions regarding the definition of safety objectives for such a system. The proposed solutions assure the conformity with the CENELEC standards for railway systems and also with CFR politic in safety area.

The solutions synthetically presented in this paper assure the scientific foundation for the 3rd, 4th and 5th stages of the system life cycle, defined in the EN50126 European standard. Basically, it is about risk quantification for safety and about identification the acceptable risk level to assure a safety level that is compatible with railway system requests.

According with EN50126 provisions, the risk concept it is a combination of two elements:

• The probability to occur an event or a combination of events that could lead to a dangerous situation, or the appearance frequency for such events.

• The consequences of a dangerous situation.

Planning the safety objectives for the system implies the following steps:

• To identify and to evaluate the system associated risks.

• To define and to apply an acceptance criterion for the risk, in order to define the global safety objectives for the system.

• To actuate the detailed safety objectives and to allocate these objectives at subsystem and module level.

Risk evaluation

According to EN50216 provision, the risk evaluation must be done considering the occurrence probability for dangerous events and also the severity of their consequences, in order to establish the risk level generated by these events. The following table presents a "frequency – consequence" matrix. The qualitative categories regarding the dangerous situations frequency and severity are set according to those defined in EN50216 standard.

Table 1. "Frequency-Consequence" matrix

Dangerous situations occurrence frequency	**Dangerous situation severity**			
	Insignificant	Minor	Critical	Catastrophic
Frequent	RISK LEVEL			
Probable				
On occasion				
Rarely				
Unlikely				
Incredibly				

The risk qualitative categories and the possible actions for each category are defined in Table 2, according to EN 50126.

Table 2. Risk qualitative categories

Risk categories	**The actions that are applicable for each risk category**
Unacceptable	It must be eliminated;
Undesirable	It must be accepted if the risk reduction it is impossible and only in agreement with the railway exploitation enterprise or with the railway authority, as the case may be;
Acceptable	Acceptable with an adequate control and in agreement with the railway exploitation enterprise;
Insignificant	Acceptable with/without the acceptance of the railway exploitation enterprise;

Analysing each ***severity-frequency*** combination of the dangerous situations associated to the system according to the CFR politic regarding safety, we obtain a decisional table for risk evaluation, presented in Table 3.

Table 3. Risk evaluation

Dangerous situations occurrence frequency	**Dangerous situation severity**			
	Insignificant	Minor	Critical	Catastrophic
Frequent	Undesirable	Unacceptable	Unacceptable	Unacceptable
Probable	Acceptable	Undesirable	Unacceptable	Unacceptable
On occasion	Acceptable	Undesirable	Undesirable	Unacceptable
Rarely	Insignificant	Acceptable	Undesirable	Undesirable
Unlikely	Insignificant	Insignificant	Acceptable	Acceptable
Incredibly	Insignificant	Insignificant	Insignificant	Insignificant

Using this table, it is possible, by applying a risk acceptance criterion, to determine the acceptable frequency for the occurrence of a dangerous situation, according to its severity degree.

In order to a more rigorous risk evaluation and also to quantify in probability values the acceptable occurrence frequency of dangerous situation, it was drawn the diagram in Figure 1. The final diagram presented in Figure1 it is the result of an interpolation based on the principle of a constant approach for the risk and severity notions.

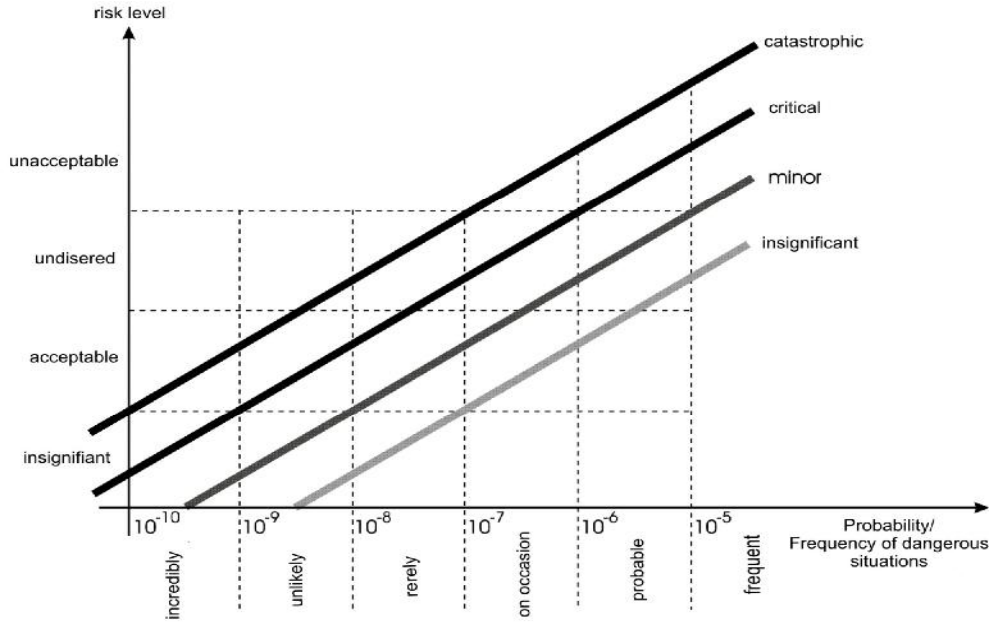

Fig. 1. Risk level – Dangerous situation frequency/probability curve

It is easy to verify that the above curve is in accordance with the decision table presented in Table 3. The final report will be offered details regarding the dangerous situations frequency categories quantification. The final report will also present several aspects regarding the system associated risk identification and evaluation, according to the CFR safety politics.

Risk acceptance and the determination of system safety global objectives

In order to establish the maximal admissible hourly probabilities (frequencies) for dangerous failures of the system, we started from the concept that any dangerous situation it is generated by a multitude of independent events that must occur simultaneously (see the below diagram). The risk analysis highlighted that the dangerous situations associated to the system had a mutual element: the existence of a faulty functionality of the system, generated by a failure that, in this circumstances, must be regarded as a dangerous failure. The dangerous situations were established in the risk analysis, based on the CFR safety politics.

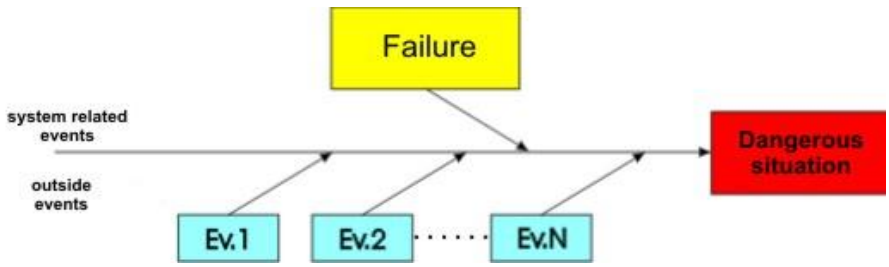

Fig. 2. Analyse of the dangerous situations generated by system failures

As the system failure and the concurrent external events that generate dangerous situations are probabilistically independent, it result that the dangerous situation probability (P_{sp}) is

$$P_{sp} = P_{dp} \cdot P_{ev}, \quad (1)$$

where: P_{dp} – dangerous failure probability;

P_{ev} – external concurrent event global probability.

As the concurrent external events are independent, it results:

$$P_{ev} = p_{ev1} \cdot p_{ev2} \cdot \ldots \cdot p_{evn}. \quad (2)$$

In order to determine the maximal admissible frequency (hourly probabilities) for the system dangerous failures, we proceed according to the following algorithm:

Step 1 Identify the dangerous situations associated to the system. This step was realised inside the risk analysis, where there were identified 29 relevant types of dangerous situations.

Step 2 Determine the maximal severity level for the dangerous situations identified in Step 1. This step was realised inside the risk analysis.

Step 3 Establish the risk acceptance criterion.

Step 4 Establish the acceptable frequencies for the dangerous situations, according to the maximal severity level.

Step 5 Establish the external events that concur to dangerous situations generation and establish their frequencies.

Step 6 Establish for each dangerous situation the maximal frequency of the system dangerous failures, that can concur to the appearance of the dangerous situation.

Step 7 Establish the maximal acceptable frequency for each dangerous failure of the system.

According to EN 50126 provision, the risk acceptance must be based on a general accepted principle. In this project, the risk acceptance analysis is based on ALARP (*As Low as Reasonable Practicable*) principle. So, it was defined a correlation between the ALARP principle associated diagram (defined in EN 50126) and the decision table regarding the risk evaluation defined in Table 3. This correlation is highlighted in the following picture.

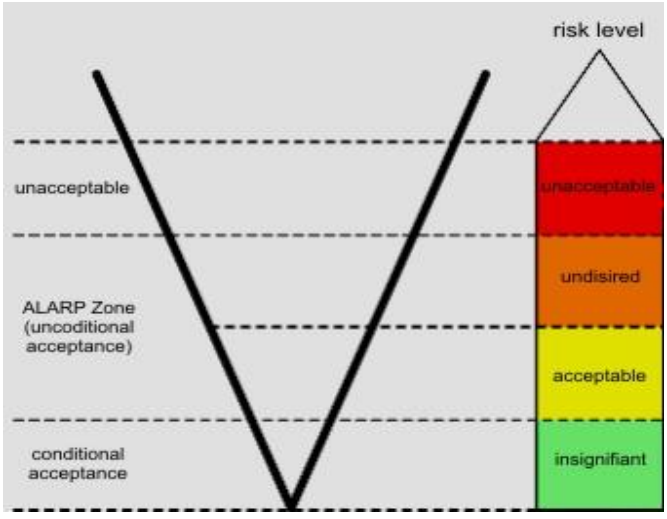

Fig. 3. ALARP Principle: Correlation with risk evaluation procedure

In order to define the maximal acceptable frequencies for the dangerous situations, the correlation represented in the above picture conducts to the identification of the correlation between the risk acceptance criteria (ALARP principle) and the quantitative definition of the risk level, according to the dangerous situation frequency/probability (Figure 1). This correlation is pictured in Figure 4. The curve represents the tool that will be used to determine the maximal acceptable frequencies for the dangerous situations identified in the risk analysis phase.

According to the following curve, the unconditioned acceptance of a risk involves its framing in the "insignificant" category. If the risk reduction measures cost until this level is extremely high, the ALARP principle permits the acceptance of some risk framed in the "acceptable" category. In such situations, according to EN50216 provisions, the acceptance is conditioned by the approval of the railway authority and of the beneficiary. The results of applying the ALARP principle, according to the previously defined method, are highlighted in the following table.

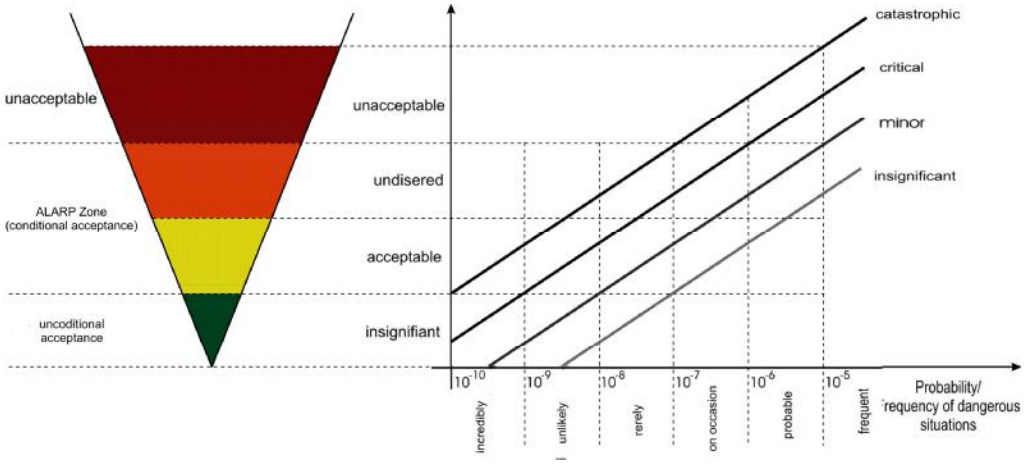

Fig. 4. Definition of the risk acceptance method by using the ALARP principle

Table 4. Numerical determination of the maximal acceptable probabilities of dangerous situation appearance, according with their severity

Dangerous situations occurrence frequency	Maximal acceptable probability [h^{-1}]	
	Unconditioned acceptance	Acceptance with the approval of AFER and CFR
0	**1**	**2**
Catastrophic	10^{-10}	$5*10^{-9}$
Critical	10^{-9}	$5*10^{-8}$
Minor	10^{-8}	$5*10^{-7}$
Insignificant	10^{-7}	$5*10^{-6}$

In the risk analysis there were identified 44 types of dangerous failures for the system that, in certain conditions, can conduct to the dangerous situation appearance. There were also analysed the external events that can encourage the dangerous situation appearance and there were actuated their frequencies.

According to the EN50216 provisions, a safety function can be defined as the function that prevent the appearance of a dangerous failure. So we can say that for each analysed dangerous failure it can be associated a safety function that assure the prevention of the dangerous failure appearance. For each safety function (dangerous failure) there can be associated safety objectives, as follows:

• Quantitative objective, referring to hazardous failures; the maximal acceptable frequency (hourly rate) for the dangerous;

• Qualitative objective, referring to the methodical failures; the safety integrity level allocated to the safety function.

Establishing the detailed safety objectives and their allocation

As mentioned before, the definition of the safety objectives is based on defining the requests for the protection against hazardous failures, respectively against the physical structure failures. Based on the results, there are inferred the safety integrity objectives, or the requests for protection against methodical failures.

The definition of the safety objectives must respect the above described procedure. This means that it is necessary to identify the physical modules of the system to which there can be allocated safety objectives. For each system safety function it must be identified the modules that contribute to its realisation.

The definition of the detailed requests regarding safety will be realised based on an iterative algorithm, shortly presented as follows.

Step 1 Define the functional architecture;

Step 2 Define the architecture of the physical structure;

Step 3 Allocate the function at physical structure subsystem level;

Step 4 Allocate the safety functions at functional architecture modules level;
There are analysed the safety functions in correlation with the functional architecture, in order to establish, for each safety function, the modules involved in that function;

Step 5 Allocate the safety functions at physical architecture subsystems level;

Step 6 De-compose the global safety objectives in detailed objectives, at the physical structure subsystems level;

Step 7 Establish the detailed safety requests an the physical structure subsystems level.

The results of applying this algorithm means a set of safety detailed objectives at each physical structure subsystem level. The values may cover more safety integrity levels. According to the constructive homogeneity principle, a subsystem safety objective it is the most restrictive objective form the set obtained in the following step. In the same time, it is defined the critical safety function at each physical architecture level.

Conclusions

This paper presented several results of a applicative research programme, which objective was the technical and scientific foundation of a Romanian solution for obtaining an electronic system based on information technology, dedicated to centralised control of a railway station. The results contain the definition of the safety objectives for the system, global and in detail, at subsystem and module level. The realisation of the determined safety objectives according to the presented methods confers the guaranty of a safe system behaviour, according to the applicable CENELEC standards and to the CFR safety politics.

Even if the results may not be a novelty in the field, the solutions for the existent systems are producers protected, and so we can sustain that our results are original.

This paper doesn't treat other important aspects regarding other electronic interlocking systems, such as:

- Establishing the performance objectives regarding reliability, availability and maintainability;
- Defining the technical solutions for realising the performance objectives regarding reliability, availability, maintainability and safety;
- Theoretical demonstration of the accomplishment of the performance objectives regarding reliability, availability, maintainability and safety;
- The management of the performance objectives regarding reliability, availability, maintainability and safety on all the system life cycle.
- These aspects are parts of the programme intended to substantiate a viable technical solution for the central control of the railway station.

References

1. EN 50126/2003 – Railway applications – The specifications and demonstration of Reliability, Availability,. Maintenability and Safety (RAMS);
2. EN 50128/2003 – Railway applications – Software for Railway protection control systems;
3. EN 50129/2003 – Railway applications – Safety related electronic systems;
4. AMTRANS – Applicative research programme Risk Management of an Electronic System for Centralised Command of Railway Stations X2C23/2006-2008.