XIX SCIENTIFIC-EXPERT CONFERENCE ON RAILWAYS RAILCON '20

DETERMINING THE RISK ACCEPTANCE CRITERIA FOR OPERATIONAL CHANGES IN THE RAILWAY SYSTEM USING THE "SAFETY II" PRINCIPLE

Slobodan ROSIĆ[1]
Melanija MITROVIĆ[2]
Dušan STAMENKOVIĆ[3]

Abstract *– One of the key elements of any risk assessment procedure is the definition of the Risk Acceptance Criteria (RAC), often based on the so-called "historical records", ie. statistical data and reports from the previous period of the system operation. Given the essential but also the legal-formal significance of this criterion, its value must be very reliably determined. The railway system is very complex, so despite the large number of statistical data that are usually collected on the railway, we often do not have indicators that directly relate to the part of the system that we certify. Therefore, it is necessary to choose from the available data those that best assess its level of security. Another problem is that the criterion of risk acceptability must be determined on the basis of events that have a relatively low frequency but can have very severe consequences (collisions, slips, etc.). In such cases, even relatively small deviations in the period from which we will take data or types of indicators can drastically affect the value of this criterion. In addition, in practice, more detailed data for a longer period of time (over 10-15 years) are often not available. In order to solve these problems, in this paper the principle of the so-called Safety II concept was applied, which, unlike the traditional approach (so-called Safety I), is not based only on the analysis of unsuccessful events (accidents, incidents), which are relatively few, but also on analysis of successful events, of which there are far more. In this way, the database of the considered data is far expanded and can better reflect the actual level of security achieved in the previous level. The problem with this approach is that traditionally detailed records are kept mainly of unsuccessful events that caused the consequences, while for a large number of activities implemented without problems usually do not have special statistical records, so it is necessary to collect this data in another way. In this paper, this method is applied to define the risk acceptance criteria for on board obstacle detection and track intrusion system that could provide support or replace the driver in the process of railway traffic automation.*

Keywords – Railway safety, Certification, Risk Acceptance Criteria, Safety level

1. INTRODUCTION

Risk assessment is one of the most important elements of certification and authorization of technical, operational and organizational parts of the railway system in the European regulatory framework.

Application of procedure of risk assessment and the method of its implementation is described in a number of EU directives and regulations that regulate this system. Before the enactment of this regulation, ie. before the creation of the common railway market in the EU, risk assessment was mostly a part of engineering and cost-benefit analysis and studies. However, its inclusion into a legal regulative has led to additional demands for implementation of that procedure, because it explicitly questions the compliance with legal conditions and legal responsibility. This is especially relevant in the field of automatic train operation, because without human factor in the process of train control, main legal responsibility in case of accidents during the driving (that are possible even in the most ideal conditions), shifts onto the area of certification and authorization of automatic train control systems.

One of the key elements of every risk assessment procedure, especially with regards to compliance with

[1] Serbian Railways Infrastructure, Nemanjina 6, Belgrade, Serbia, srosic@sbb.rs
[2] Faculty of Mechanical Engineering University of Niš, A. Medvedeva 14, Niš, Serbia, melanija.mitrovic@masfak.ni.ac.rs
[5] Faculty of Mechanical Engineering University of Niš, A. Medvedeva 14, Niš, Serbia, dusan.stamenkovic@masfak.ni.ac.rs

legal conditions, is the definition of RAC - Risk Acceptance Criteria. European regulative in the railway sector does not define the accurate way of determining these criteria, so in practice, general principles from the field of risk assessment are used. Before long, it turned out that this leaves the room for different interpretations of what exactly is a legally acceptable risk, and what is its exact level[1],[2]. Several works from that period outlined the need to describe risk acceptance more accurately. However, this is still not the case, except partially for risk acceptance criteria for technical systems. In practice, there are two methods for defining this criterium:

- based on historical evidence derived from an analysis of statistical data about previous safety performance;
- based on safety system goals that are defined beforehand (project based).

In practice, these criteria are far more commonly defined using the first method[3]. EU Safety Directive 2016/798 in its preamble (5), clause 1 prescribes maintaining the current level of safety as one of its main conditions. Having that in mind, even when risk assessment criteria are project based, it is necessary to compare the expected safety level with the previous one, which represents the minimal necessary risk acceptance criteria. Many works and studies support this conclusion. The first comprehensive study related to european regulative for safety management and interoperability of railway system states the following: „Acceptability of risk should be based on ensuring that at least the same level of safety performance is maintained and every reasonably practicable improvement has been made before the change is implemented" [4] .

This principle of defining the risk acceptance criteria is practically corresponding to GAME (Globalement au moins équivalent) principle: "Any change to an existing system, and the design and manufacture of a new system, must be carried out in such a way that the resulting global level of safety is at least equivalent to as existing systems that are in use." GAME risk acceptance criteria defining principle is legally binding in French railway sector, but is also commonly used in other areas. Based on this, it is possible to conclude that defining the current safety level as a minimal risk acceptance criteria is one of the most important steps in the process of certification and authorization of new railway systems.

2. DETERMINING AND QUANTIFYING THE EXISTING SAFETY LEVEL

Regardless of the significance of this term, especially with regards to regulation compliance and legal responsibility, there are no common rules and norms for determining and quantifying the achieved (or preferred) safety level. National reference values for common safety goals are the exception. Common safety goals represent safety levels that must at least be reached by different parts of the rail system and by the system as a whole, expressed in risk acceptance criteria. Achievement of these goals is assessed through National reference values (NRV).

NRV are reference measures that quantify the existing (reached) level of safety in EU member countries[5]. They are determined as pondered average value of indicators in total and relative number for a period of 6 years using the formula:

$$NRV_Y = \frac{\sum_{i=x}^{N} W_i \times OBS_i}{\sum_{i=x}^{N} W_i} \quad (1)$$

where W_i is ponder that represents the inverse absolute value of difference between yearly OBS_i indicator values, and their average value for a period of 6 years (N). Indicators for which NRV is calculated are number of accidents, number of incidents, number of injured persons, and amount of damage from accidents and incidents. Apart from Common Safety Goals, existing safety level is often used for defining the corporate safety goals within the safety management system or maintainance system of the infrastructure managers, railway undertakers or entitys in charge of maintenance.

By analyzing these documents, it is possible to conclude that the existing safety level within these systems is almost always quantified using average values of statistical data about dangerous events (accidents and incidents) in a certain period. Average value is most commonly calculated as a simple arithmetic mean value, that is expressed in relative number of these events relative to the train or gross tonne kilometres. Time periods for which the values are calculated are usually between 5 and 10 years. This way of determining and quantifying existing safety level can be adequate for the safety goals that the EU railway agency (ERA) considers global, or for high level risk acceptance criteria (Figure 1) [3].

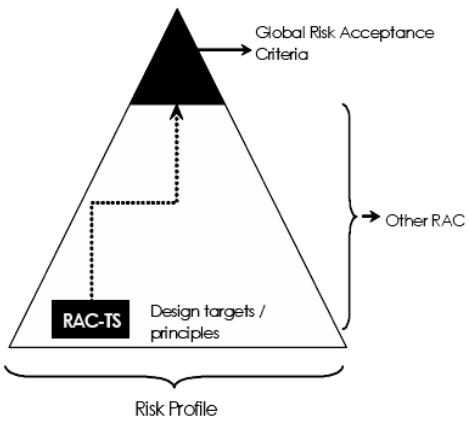

Fig.1. Hierarchy of Risk acceptance Criteria

However, when subjects of authorization and certification are parts of subsystems, or specific areas, other or technical level criteria are relevant (on functional level, hazard level, procedural level or equipment level). In these cases, the method of determining existing safety level in a way that is usual for safety goals (using the average value of unusual events or their consequences during a period of 5-10 years) may be inadequate. One of the reasons for this is that the railway system is very complex, so even with the large amount of statistical data that is usually collected, we do not have the indicators that are directly linked to the part of the system that is certified ie. whose correlation with the safety level specific for the observed part is not great. Second problem is that the safety level must be determined using the events that have relatively low frequency, but can have very serious consequences (collisions, derailment etc.) or can appear regularly in series.

In such cases, even the relatively small deviations in the observed period or the type of indicators can significantly impact the value of this criteria. Possible solution to this problem is the application of the principles of Safety II concept. This concept was developed, and has found its application in more complex systems, such as health systems and flight control. While the traditional approach, Safety I concept, is based on analysis of unsuccessful events (accidents, incidents), and their consequences, Safety II concept is based on analysis of all the events, both successful and unsuccessful. The First concept defines safety as the condition where the number of adverse outcomes (e.g., accidents, incidents and near misses) is as low as possible.

Safety-I is achieved by trying to make sure that things do not go wrong. The Second concept defines safety as a condition where the number of acceptable outcomes is as high as possible. Safety-II is achieved by trying to make sure that things go right, rather than by preventing them from going wrong[6]. When it comes to analyzing data, the main difference between these two concepts is that the first one is only focused on a few exceptional events, while the second one takes into consideration all of the events, and therefore has a wider base (figure 2.) Apart from that, these two concepts are also different in their approach to risk evaluation. While Safety I concept is focused on dangers and incidents, Safety II regards the risk as the state in which management and control of process is difficult[7].

3. QUANTIFYING EXISTING SAFETY LEVEL AS RISK ACCEPTANCE CRITERIUM FOR AUTOMATIC OBSTACLE DETECTION SYSTEM

In accordance with the classical approach, ie. Safety I concept, existing safety level for automatic obstacle detection system would be defined based on statistical data about accidents and incidents in which the train ran into immovable objects (not counting running into people and vehicles on railway crossings). The relevant data for IŽS a.d. railway network in the 2019 - 2020 time period is shown in table 1. It is expressed as the number of these events per milion driving kilometers. As can be seen, values for the year of 2017 deviate significantly when compared to the values for other years, and the difference between minimal and maximal value is around 8,7 times. Depending on the time period that we select for determining the existing safety level, and the way that we calculate average value, we could calculate that acceptable risk level is between 0,41 and 0,71 events per milion driving kilometers.

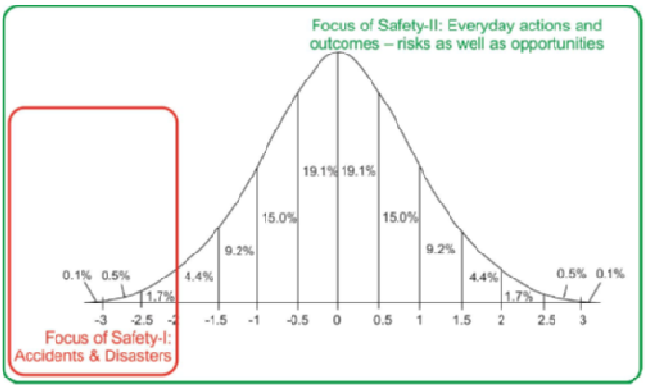

Fig 2. Area of data analysis in Safety I and II concepts

Tab 1. Number of train collisions with obstacles on the IŽS network

year	number of collisions on mil. tkm
2019	0,52
2018	0,33
2017	1,82
2016	0,62
2015	0,70
2014	0,27
2013	0,21
2012	0,78
2011	0,40
2012	0,44

Not only is this range too great for the needs of equipment certification and authorization, but all of these events are not unsuccessful events when seen from the obstacle detection system aspect. In most of the cases, the event in question could not be avoided in any way because of the current conditions (low visibility, short interval between the event and the approach of the train, and similar), but the reaction in a timely manner led to the maximal possible decrease of the consequences of the event. If we apply the Safety II concept, and analyze all events that include an immovable obstacle on the tracks, whether the train ran into it, or it was avoided, and base our risk

analysis on the conditions that led to the event, we can get the results shown in table 2. In this case, different time intervals and ways of calculating the average value of the percentages of successful train driver reaction are not significant, since we get a very small range, from 94,5 to 94,95 percent.

Tab 2. total number of occurrences of obstacles on the IŽS network and the number of unsuccessful reactions of train drivers

year	total number of obstacles	nuber of unsuccessful driver reaction	success rate
2019	14	1	92,9
2018	6	0	100
2017	32	3	90,6
2016	18	1	94,4
2015	25	1	96,0
2014	29	2	93,1
2013	18	1	94,4
2012	28	0	100
2011	13	1	92,3
2010	33	2	93,9

Average value of this indicator for the entire 10 year period would be 94,76% of success rate, and could be used as a good evaluation of existing safety level for detection of immovable objects on tracks, and could be adopted as a minimal criteria for certification of automatic obstacle detection systems.

4. CONCLUSION

Determining the achieved level of safety as a minimum criterion of risk acceptance in the process of certification and authorization of new systems on the railway requires great precision and reliability. the traditional way of determining and quantifying it through indicators of accidents and incidents is often not good enough. Applying the Safety II concept, which analyzes all system-relevant events, both successful and unsuccessful, can give a much better result.

REFERENCES

[1] Jens Braband, *Risk assessment in railroad signaling: Experience gained and lessons learned*, Annual Reliability and Maintainability Symposium Proceedings, Seattle, 2002

[2] Sonja-Lara Kurz, Birgit Milius, *Was ist negligible/broadly acceptable risk,* 10. Bieleschweig-Workshop zum Systems Engineering, Braunschweig, 2007

[3] *Final Report – Risk Acceptance Criteria for Technical Systems and Operational Procedures for European Railway Agency*, Det Norske Veritas Ltd, 2010

[4] E.M.El Koursi, S.Fletcher, L.Tordai, J.Rodriguez, *SAMNET Synthesis Report Safety Management and Interoperability*, Brussels, 2006

[5] *2009/460/EC: Commission Decision of 5 June 2009 on the adoption of a common safety method for assessment of achievement of safety targets*, Official Journal of the European Union L 150/11

[6] Erik Hollnagel, Robert L Wears, Jeffrey Braithwaite, *From Safety-I to Safety-II: A White Paper*, Published simultaneously by the University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia, 2015

[7] Hollnagel, E., Leonhardt, J., Licu, T. & Shorrock, S., *Eurocontrol White Paper on Safety-I and Safety-II*, Eurocontrol, Bruxelles, 2013