Magdalena Kycko
mgr inż.
Instytut Kolejnictwa,
Wydział Transportu,
Politechnika Warszawska
mkycko@ikolej.pl

DOI: 10.35117/A_ENG_17_06_06

Threats and risks in certification processes

Abstract: In recent years, the railway industry in Poland undergoes dynamic changes, characterized by an increase in investment intensity on the railway market. Hence, the concept of risk is becoming more and more important and increasingly significant in investment processes as well as in subsystem certification processes. The publication presents selected threats and risks that can and often occur in subsystem verification processes. In addition, the publication presents methods for identifying these hazards and preventive actions.

Keywords: risk, certification, EC verification.

Introduction

Currently, in the dynamically changing political and economic conditions, making investment decisions and carrying out investments are inseparable from risk. In railway investments, the certification process of subsystems or interoperability constituents plays an important role. Analysing the issue of risk in investments and certification processes, it is indispensable to define the concept of risk and threats. Thus, the threat is a set of conditions that can lead to the occurrence of a series of events that adversely affect people, objects and their surroundings. In contrast, the risk means the frequency of accidents and incidents leading to damage caused by the threat and the degree of severity of this damage [6]. The important thing is that the risk is a potential possibility of realising the threat.

The aim of the risk analysis of the certification and the investment process is to assess the possibility of incurring a loss or not achieving the intended effect. The concept of risk can be extended as a possibility of occurrence of many mutually exclusive substantive results and effects of the decision made, with the possibility to determine for each result its financial value and the probability of any material effect. In the case of a railway investment, including the certification process and subsystems approval, the security of the system, engineering structure or the management and operation system becomes the overriding factor.
The complex issue of risk assessment and its importance when certifying subsystems or interoperability constituents decided to consider these issues.

Legal documents related to risk in certification processes

European law imposes an obligation to introduce interoperability on Polish railways. Therefore, there is a necessity to carry out the certification process, which is aimed at confirming compliance with the subsystem interoperability requirements or inertroperence components. The national part of the systems is also subject to certification and checking in accordance with the requirements of national law. Subsystems will be allowed to be used only when the Contractor receives EC certificates, therefore the certification process plays a big role in the investment process itself, and thus it is a process exposed to threats or risks coming from outside the certification body as well as risks resulting from internal procedures of the certification body.

The approach to safety in rail transport in Poland and in Europe is significantly modified. These changes were initiated in 2004 by the provisions of the Railway Safety Directive [2]. The directive indicates that all railway system operators, infrastructure managers and rail operators should bear full responsibility for the system's safety, everyone in its scope. This issue is new to the railway sector and causes a lot of misunderstanding of the interpretive nature, in particular, because it concerns the interface between technical sciences and management sciences.

During the implementation of certification processes as well as railway investments, contractors are obliged to comply with the requirements of many legal documents, i.e. standards, regulations or technical specifications for interoperability (TSI). However, there are also requirements related to risk analysis that must be met by the certification body. All requirements are directly or indirectly aimed at increasing the level of system security in the implementation of a given investment. The documents listed below are compulsory for use by certification bodies and documents whose requirements must be met by the applicant, i.e. the contractor of the investment.

Documents regarding certification processes in notified bodies:	**Documents regarding the assessment of subsystems and interoperability constituents**

✓ Accreditation documents (PCA):
  ✓ DACW01 - Accreditation of product certification bodies
  ✓ DACS01 - Accreditation of certification bodies for management systems
  ✓ DAK07 - Accreditation of inspection bodies
  ✓ DAK08 - Accreditation of assessment bodies for activities covered by the Commission Implementing Regulation (EU) No 402/2013
✓ ISO 9001: 2015 - Quality management systems
✓ PN-EN ISO / IEC 17020: 2012 Conformity assessment - Requirements for the operation of different types of inspection bodies
✓ PN-EN ISO / IEC 17021-1: 2015-09 Conformity assessment - Requirements for units conducting audits and certification of management systems - Part 1: Requirements
✓ PN-EN ISO / IEC 17065: 2013-03 Conformity assessment - Requirements for bodies certifying products, processes and services
	✓ Technical specifications for interoperability for subsystems
	✓ Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on a common safety assessment method for valuation and risk assessment and repealing Regulation (EC) No 352/2009
	✓ Directive 2004/49 / EC of the European Parliament and of the Council of 29 April 2004 on Community rail safety as amended
	✓ PN-EN 50126: 2002, Railway applications - Specification of reliability, availability, maintenance compliance and security,
	✓ PN-EN 50128: 2002, Railway applications - Communication, signalling and control systems - Programs for railway control and security systems
	✓ PN-EN 50129: 2003, Railway applications - Communication, signalling and control systems - Electronic signalling systems related to safety
	✓ PN-EN 50159: 2011, Railway applications - Communication, traffic control and data processing systems - Secure communication in transmission systems
	✓ Procedure: Technical and operational risk assessment, SMS-PR-02, PKP Polskie Linie Kolejowe S.A., 2014
	✓ Procedure: SMS-PW-17 Allowing components subsystems and for use on railway lines managed by PKP PLK SA, 27/10/2015.

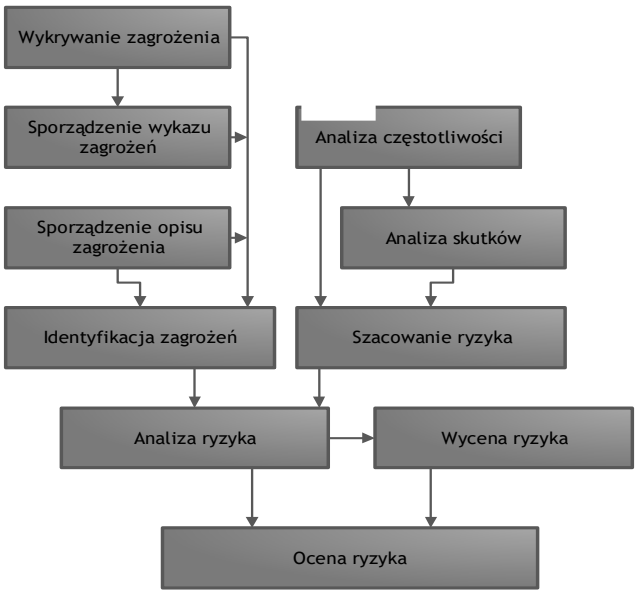
The safety of each system is based primarily on appropriate documentation for this system. The subsystem that is directly responsible for safety is the control subsystem, and hence it is the most complex subsystem and requires more work and expert knowledge during conformity assessment. In connection with Poland's entry into the EU structures in the area of security, the following norms have become applicable: PN-EN 50126 [2], PN-EN 50128 [4] and PN-EN 50129 [3]. The standard [2] defines reliability, readiness, availability and safety (RAMS - Reliability, Availability, Maintainability and Safety) as a process based on the system life cycle. In this process, the individual steps of the system and procedures related to the approval were defined before moving on to the next stage, i.e. specification of requirements, design, implementation, etc. The standard [4] defines the procedures and technical requirements for the design of software for a safe electronic control and protection system on the railway. It should be stated that this standard is not fully obligatory. The standard [3] defines the requirements for the design, testing, acceptance and approval of electronic systems, subsystems and signalling devices related to safety in railway applications. The concept of safe computer systems used in the railway industry assumes a very low intensity of faults, which with the total independence of processing channels (2 or 3) guarantees a negligible probability of a double or multiple failure decisive for a catastrophic and critical failure.

The next document, the requirements of which must be met by contractors of railway investments or equipment manufacturers is Regulation 402/2013 [6]. In Europe, methods and tools are introduced aimed at building a uniform approach to railway safety among the Member States. One such tool is the Common Safety Method for Valuation and Risk Assessment (CSM-RA), which is described in the Commission Implementing Regulation (EU) [6], in force from 21 May 2015.

The basis for developing a common safety assessment method for valuation and risk assessment was the need to harmonize at European Union level the methods used by railway entities involved in the development and operation of the railway system to identify and manage risk and methods for demonstrating compliance of the railway system with safety requirements.

In accordance with the common security method adopted, the entity introducing a change to the railway system is required to assess whether a given change affects safety and, subsequently, whether it has a significant change. The assessment is based on the criteria set out in the Regulation [6].

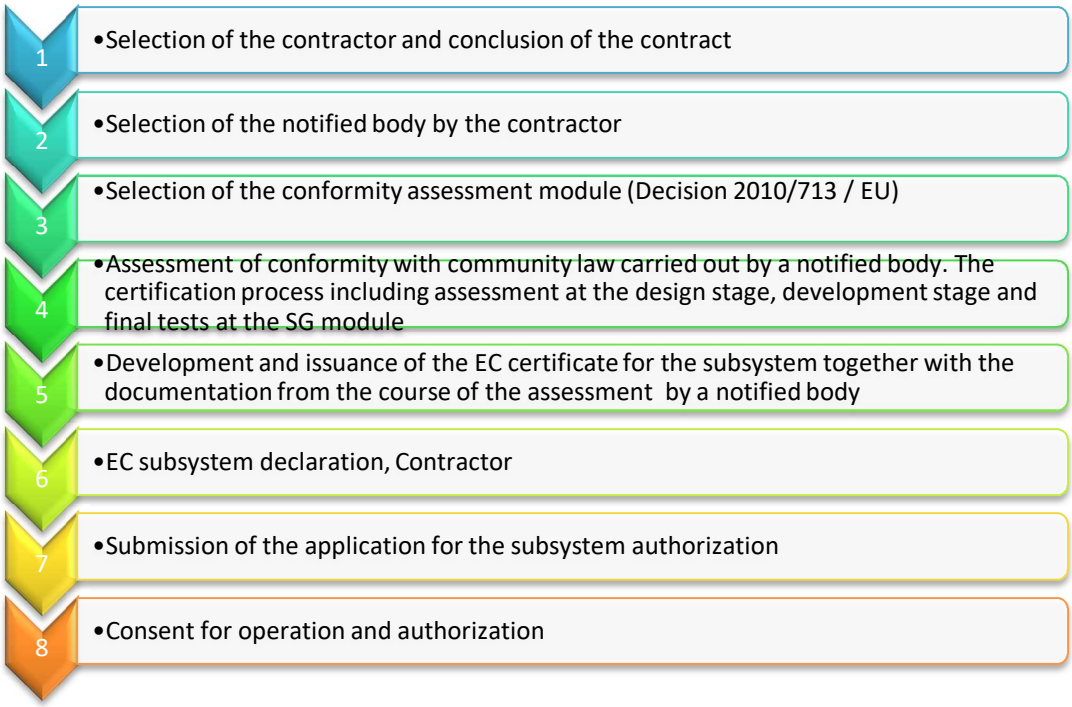
Risk analysis is an important element in the design, production or operation of technical devices. Records appearing in certain device standards and srk systems, especially those related to security, even impose on the design teams and equipment manufacturers an obligation to carry out a risk analysis.



1. Relations between selected concepts contained in the Regulation [6].

Threats and risks occurring in certification processes

Risk assessment becomes an important element of the certification process as well as the entire investment process. As a rule, more risky investments may bring a potentially greater return, which is an obvious incentive for a potential investor. Enterprises, depending on the attitude to risk, as well as the calculation of potential benefits related to investment activities, decide whether or not to accept a given investment project. Therefore, the risk analysis should form a significant part of the investment efficiency statement, including the certification process itself. The risk in certification processes may occur and often occurs at various stages of the process. The figure below shows the individual steps of the subsystem certification process.



2. The course of the EC certification process of the subsystem (source: own study)

Threats and risks in certification processes directly affect the certification process itself and indirectly also safety of certified railway lines. Certification bodies have a lot of responsibility when examining a given subsystem and issuing a certificate that confirms its compliance with the requirements of national or European law. There can be many risks and threats in certification processes, but it is important that threats or risks are detected and analysed at an early stage of the certification process.

Threats and risks that may occur in certification processes include:

- ✓ lack of knowledge among applicants;
- ✓ wrong assessment module;
- ✓ ignorance of the requirements of the relevant TSIs;
- ✓ external pressure;
- ✓ late notification of the certification process to a notified body;
- ✓ no declaration of conformity for interoperability constituents;
- ✓ exceeding the contractual dates;
- ✓ poorly defined certification area, initial and final kilometres of investments, present mainly in projects involving the GSM-R system;
- ✓ choosing an incompetent certification body;
- ✓ separately conducted investment and certification tasks covering the development of the ETCS system, and separate ones covering the GSM-R system;
- ✓ lack of knowledge of the tender documentation entries (SIWZ, PFU);
- ✓ change of regulations and legal requirements during the investment process.

Threats and risks that have been mentioned are one of the few that can be encountered in certification processes. Therefore, an important role of the certification body is to define these risks at the beginning of the certification process and to introduce preventive measures to possible threats.

In connection with accreditation requirements, which also introduce the obligation to monitor risk in certification processes, notified bodies shall establish internal procedures to be followed by personnel conducting certification processes.

In order to reduce the probability of occurrence of risks and threats in certification processes, the following actions can be implemented:

- ✓ change of certification procedures by tightening requirements;
- ✓ staff training;
- ✓ cyclical risk analysis;
- ✓ identification of threats in the first stage of the assessment process;
- ✓ risk and threat monitoring;
- ✓ raising awareness among technical experts;
- ✓ training of investment contractors.

3. Risk management cycle (based on [6])

Risk assessment methods

Various risk analysis methods exist and are currently in use. The choice of the method is conditioned by reference to the system for which the risk analysis will be carried out, as well as the significance and importance of the investment. The implementation stage is also crucial in the method selection. In practice, there is a set of risk analysis methods. Methods that are often used in risk analysis in certification processes are as follows:

- ✓ analysis of the event tree;
- ✓ FMEA analysis (Failure Mode and Effects Analysis), the analysis of the types and effects of possible defects;
- ✓ HAZOP (Hazard and Operability Study), the analysis of threats and operational abilities;
- ✓ threat research and operational readiness;
- ✓ analysis of human reliability;
- ✓ the Delhi method;
- ✓ Monte-Carlo simulation and other simulation methods;
- ✓ review of data in retrospection;
- ✓ RAMS analysis;
- ✓ multi-criteria assessment.

An interesting solution is the multicriteria method that takes into account and synthesizes the assessment of a number of other detailed methods. For each investment,

including for each certification process, an appropriate risk analysis method should be selected that would best describe the risk involved. The choice of risk analysis method depends on many different factors characterizing the investor, as well as the specifics of the certification process itself, which depends on the scope of certification, evaluation module or subsystem.

Conclusions

Certification has long been considered an important element in investment processes, but in recent years this topic is increasingly often discussed, which is, among others, caused by the development of rail transport in Poland. In terms of safety on the railway lines, the most important role is played by the control subsystem in the superior part as well as in the basic part. Also for this reason, the evaluation of the subsystem control is more complicated and requires more work and time than the assessment of other structural subsystems. In order to be able to make an assessment in the certification processes, a group of qualified and experienced specialists is needed, which are often lacking in companies implementing investments. The lack of competence among contractors of investments causes, among other things, problems during the subsystem certification process, and hence the extension of the duration of the investment and financial losses. Therefore, the importance and significance of the certification process in investment processes should be emphasized because it greatly affects the success of investment and security.

The analysis of the risk assessment possibilities in rail transport indicates that the reliability of all components of the rail transport system is extremely important in this respect.

Source materials

[1] Dyrektywa 2004/49/WE Parlamentu Europejskiego i Rady z 29 kwietnia 2004 r. w sprawie bezpieczeństwa kolei wspólnotowych z późniejszymi zmianami
[2] PN-EN 50126:2002 Zastosowania kolejowe -- Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa
[3] PN-EN 50129:2007 Zastosowania kolejowe -- Systemy łączności, przetwarzania danych i sterowania ruchem -- Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem
[4] PN-EN 50128:2011 Zastosowania kolejowe -- Systemy łączności, przetwarzania danych i sterowania ruchem -- Oprogramowanie kolejowych systemów sterowania i zabezpieczenia
[5] Procedura: Ocena ryzyka technicznego i operacyjnego, SMS-PR-02, PKP Polskie Linie Kolejowe S.A., 2014
[6] Rozporządzenie Wykonawcze Komisji (UE) NR 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009
[7] Szopa T., Niezawodność i bezpieczeństwo, Oficyna Wydawnicza PW, Warszawa 2009