Technical Sciences
Academy of Romania
www.jesi.astr.ro

Journal of Engineering Sciences and Innovation
Volume 9, Issue 3 / 2024, pp. 321-334

E. Civil Engineering and Transport Engineering

*Received **16 Apryl 2024*** *Accepted **3 September 2024***
*Received in revised form **9 August 2024***

Critical safety systems development. Railway applications

RADU ZLATIAN[1,2*], OVIDIU DREȘCĂ[1], DANIELA RACHIERU[1], ȘTEFAN BOȘTINĂ[1]

[1]*Softronic Co., Calea Severinului 40, 200609 Craiova, Romania*
[2] *Technical Sciences Academy of Romania, 26 Dacia Blvd, 030167, Bucharest, Romania*

Abstract. The article presents the issues of hazards from the point of view of the European Union's policy on consumer protection and the railway industry. In this regard, Union policy establishes that legislative regulations for any product group must only relate to the essential requirements that can significantly influence the safety of people, the environment, and property, while the technical characteristics are established by harmonized standards. The European Union has issued legislative regulations for all fields of activity. These regulations establish the essential requirements and how they should be reflected in the product or service being developed. In the railway field, the legislation consists of the Directive on the interoperability of the railway system, the Directive on railway safety, and the implementing regulations.
Essential requirements comprise functional, technical, contextual, and safety requirements. Achieving a product that meets essential requirements and is safe for people, the environment, infrastructure, and property is possible through a special process – *design for safety* – whose principles are outlined in this article.

Keywords: hazard; safety; hazard in railway; safety systems; design for safety.

1. Introduction

Since the beginning of association in the European Economic Community (Treaty of Rome, 1957), the European states have sought the elimination of barriers and the free movement of goods within a single market open to all economic agents. Later, to this objective were added others necessary to ensure a fair competitive environment and consumer protection.
During the last 60 years of European integration, policies and legislation have evolved, reaching the *New Approach* policy developed in 1985. This policy [21, 23]

*Correspondence address: radu.zlatian@softronic.ro

is based on a clear separation between the EU legislation and standardization, and the legislation is limited to the essential requirements. The essential requirements establish the safety requirements of general interest that must be met for the movement of goods to be carried out protecting consumers and the environment that surrounds them, while the technical details are established by harmonized European standards [24]. The standards offer a guarantee of quality concerning the essential requirements of the EU legislation.

The implementation of the new legislative framework [21, 23] also required the development of tools to assess compliance with essential requirements, accreditation for market surveillance, and control of products from outside the EU. The principle of resorting to standards in terms of technical regulations determined the development of a European policy of standardization which was the basis of the activity of European organizations in the field.

European organizations designated for issuing harmonization standards are CEN – European Committee for Standardization, CENELEC – European Committee for Electrotechnical Standardization, and ETSI – European Telecommunications Standardization Institute. A harmonized standard is recognized if it is published in the Official Journal of the European Union (OJEU).

2. Safety and essential requirements

According to the new approach policy, the essential requirements that must be met by a product are mandatory to be introduced and used on the European market. The essential requirements define the results to be achieved and the hazards to be dealt with to avoid any negative impact on people, the environment, and property, but do not specify the technical solutions by which they are met; therefore, the manufacturers are free to choose how to meet these requirements while respecting the clauses of the relevant applicable standards.

The essential requirements, always, regardless of the economic field, include reliability, availability, maintainability, and safety related to the health of people and, the protection of the environment and goods. A product that meets these requirements gives the consumer and the market confidence that it is safe for use. Compliance with these requirements is a complex process of research and analysis through which the designer identifies all situations that do not meet the conditions of safe use and finds solutions that, once implemented, eliminate the dangerous situations or, if this is not possible, reduce their negative effects to an acceptable or tolerable level.

A product is considered to comply with essential requirements if the designer and manufacturer ensure that, during manufacture, storage, installation, commissioning, long-term use, maintenance, and decommissioning, it will not adversely affect, in any way, the lives of people, the environment and the integrity of tangible or intangible assets. For this, during the lifetime of a product intended for use in a certain field, the hazards and risks associated with them must comply with the requirements imposed by the relevant legal regulations and applicable standards.

In general, when evaluating the safety of a product, the assessor considers the most relevant factors [5, 6, 13, 14, 22]:

- the quality of implementation of the functional, technical, contextual, and safety requirements
- categories of consumers who use the product, especially vulnerable people such as children, the old, or disabled people
- cyber security adopted for protection in case an external intervention could have an impact on security
- applicable European, international, and national standards
- EU safety assessment recommendations or guidelines
- compliance with regulations, rules, and decisions issued by European regulatory bodies
- state of the art and technology, opinions of recognized scientific bodies
- codes of good safety practice.

New railway systems, but also systems used in other fields, are developed and put into production intending to increase performance, efficiency, safety of use, and maintenance. For this, it is necessary to know the processes of use from the perspective of dangerous situations that could injure people or cause damage to the environment and property. To achieve this objective, a wide range of methods have been developed, some standardized at the international level, others presented in various specialized publications. It is certain that we currently have a set of standards [31, 33, 34, 35] that regulate some methods widely used by most developers and manufacturers. Product certification [23, 21] as the only unanimously accepted method for placing products on the EU market obliges the adoption of harmonized standards thus ensuring consumer protection and the free movement of goods.

As systems increasingly incorporate new architectures, components, and technologies, becoming less dependent on humans and more on automation, the importance of having a cost-effective way to assess accident risk is increasing. Every project that replaces old, conventional systems must provide a full safety assessment for the protection of people, the environment, and property.

The identification of hazards and their assessment is carried out with a certain cost whose value is dependent on the complexity of the future product, and the mission it is to perform in the required operational context. In addition to the cost of the hazard assessment itself, there is also the cost of redesigning the systems if they do not meet the specified safety requirements. Since the design of a system is expensive, every effort should be made to avoid re-design in later stages of development due to missing or non-conforming safety requirements at the beginning of the design phase.

Therefore, the hazard assessment methodology should be applied before starting the design. In this sense, requirements engineering [1, 2, 7] should be the main support for action, its role is to contribute to the development of a coherent set of functional, contextual, technical, and safety requirements that meet the needs and

expectations of stakeholders.
Unfortunately, there are still many projects for which hazards are not assessed [6] in the pre-design phase, companies do not have consolidated processes and procedures, or if they do, they do not work satisfactorily. These projects reach the market with systems that can cause events accompanied by consequences resulting in death or damage, the repair of which can cost lives and incredibly large amounts of money. Of course, in creating and keeping a safe market for consumers also are certification bodies that should check how the developer has analyzed and removed the hazards whose consequences exceed a limit unanimously acceptable by the society at a given time.
In principle, the development of a new system is determined by the performance of the functions under operational conditions that ensure the safety of use [3, 5]. Of course, there are no perfect systems that are unaffected by hazards that generate events with negative impacts on people, environment, or property. Considering this possibility, designers must analyze and decide which solutions to adopt to obtain a product with maximum safety, and to do this they need effective and easily applicable methods and procedures.

3. Hazards and modern society

Under certain conditions, everything that surrounds us, natural or man-made, can have an unwanted impact on our lives, the environment we live in, and the goods we create to make our lives easier. Often these natural phenomena, activities, or human actions have particularly serious consequences. In everyday life, we face floods, earthquakes, fires, droughts, extreme temperatures, and accidents involving airplanes, ships, automobiles, trains, machine tools, forklifts, pressure vessels, instruments, tools, chemicals, medicines, etc. All of this has produced and produced damage, sometimes irreparable that happens at moments that are difficult to predict.
There is no system of any kind that cannot be affected by these unwanted events and its functions always perform exactly as they were designed. This is because nature is not driven by deterministic phenomena and in carrying out any action absolutely cannot consider all the situations that the system is likely to face.
In a world where random phenomena play a much more important role than deterministic ones, with a certain probability, higher or lower, all people, activities, goods, or processes can be affected by events whose consequences are loss of life, injuries, and destruction of the environment or property. The idea that a certain process, action, or activity can be "hazard-free" is neither theoretically nor practically supported. The awareness of the fact that we are part of a universe in which events occur according to laws in which probability plays a decisive role must draw our attention to the hazards that we can inevitably be part of. In this context, no event is exactly like another, and no hazard has the same consequences as another. The fact that the events and their consequences are different supports the theory of the infinity of space, matter, and states. By their very nature hazards are not a

certainty, and uncertainty can only come from ignorance, and ignorance can be the result of wrong formulation of the problem, subjective approach, linguistic imprecision, incorrect logic, and causation, non-specific or inconclusive evidence, data, information, interpreting probability and statistical variation or mathematical modeling with wrong assumptions or data.

To prevent situations that may have unwanted consequences, it is necessary to identify the hazards, and their frequency of occurrence in all possible conditions, quantify the consequences, and develop the measures that can be taken so that the unwanted effects have the smallest possible impact. This approach is based on human experience resulting from hundreds or even thousands of years – *the costs of prevention are always lower than the costs of repair*. As a result of the fact that, regardless of our desire, there are situations that can have undesirable consequences, analysis and decision methods have been developed to help in finding the safest solutions and the best decisions regarding their application. Of course, these solutions do not give recipes that eliminate the risks[1] that the hazards can generate but only mitigate their effects, at least, to a bearable threshold.

Ignoring or partially applying the measures developed to mitigate the risks generated by various hazards is a common situation that leads to undesirable consequences that are difficult to anticipate and evaluate. If goods or the environment can be recovered at some cost, serious bodily injury or life cannot be recovered and have long-term effects impossible to assess. In this sense, for example, specialized bodies identify the hazards that can be generated by driving cars on a road, take the necessary measures to reduce the risks of skidding, frontal collision, exiting the scenery, etc. by mounting warning or restriction signals, but they are not respected by drivers, which makes the danger of accidents to be maximum instead of being reduced to an acceptable minimum.

In modern society, a multitude of factors are at work that increase the frequency of hazards and the severity of the consequences. Among them, the most active ones seem to be [2, 14, 17]:

- the aggressive and competitive environment in which companies operate
- the high operating speed of the machines and processes
- the very fast pace of technological changes
- relationships between people and machines
- continuous growth of production and service activities
- the constant demand to increase the speed of cars, trains, machines
- the rapid development of technologies
- the high degree of integration of systems with information and communication technologies
- the use of an insufficiently trained labor force
- pollution
- climate instability and climate change

[1] risk is the characteristic of a hazard expressed by the probability of occurrence and the severity of the consequences.

- sabotage and terrorism.

The unwanted consequences of these events have been and remain the focus of scientists who are looking for ways to identify them and know their causes. Of course, knowing the causes and effects one can imagine various methods of mitigation or, in some cases, even elimination.

The need to study the unwanted impact of human actions through the installations, and equipment of the machines that he created gave birth to a new science, the *science of safety*. Its object of study is the hazard that can be generated using machines, equipment, tools, etc., which in certain conditions, sometimes encountered very rarely, can seriously damage the integrity of people, environment, or property.

The approaches, which have already become commonplace, aim at designing and manufacturing machines, equipment, etc. the use of which is safe in the sense that the unwanted impact on the integrity of people, the environment, and goods is minimal. For this, in the action of establishing the functional, contextual, technical, and safety requirements, the relationship with these entities must be explicitly considered and they must be designed in such a way that they benefit from reliability and capacity to be maintained preventively and correctively that allow the avoidance of certain events which may have unintended consequences.

4. Hazards in the railway system

Each developer of a railway product must undertake to protect people against accidental death, injury, or occupational disease, and to protect the environment, infrastructure, and any other assets against accidental destruction or damage during the execution of transport missions [10, 16]. Furthermore, each design [3, 5, 9, 15] must ensure that the product performs the functions for which it was created, will not fail more times than required, and will not degrade over the specified lifetime. Any deviation must be identified so that by design it can be eliminated, or its effects minimized.

How this desire can be ensured is reduced to the identification of hazards and the management of the risks associated with each hazard in all phases of the development life cycle [9, 15, 31]. Identifying hazards [4, 11, 16] and methods to eliminate or reduce the effect of their consequences contributes to improving the safety and security performance of the product. For this, hazard identification and analysis are systematically carried out at each stage of the life cycle from concept to disposal [9, 15, 31, 35, 36].

At the level of detail, commensurate with the objectives of the analysis, with the life cycle stage of the development process, with the available information and resources, the questions on which a hazard analysis is based are:

- to identify hazards – Are there situations/threats that can generate unwanted events? Which are those? What can go wrong?
- for assessing the consequences – What can the consequences be? How large are they? and, How serious are they?

- for probability forecasting – What is likely to happen? When is it likely to happen? How often could it happen in a given time (month, year)?

The answer to these questions must be sought only at the level of analysis necessary to develop a valid decision. A cursory analysis does not provide enough information to make a good decision, while an overly thorough analysis provides too much information, some of which is irrelevant to the decision process, wasting resources unnecessarily. It is obvious that as the studies become more detailed, the cost per scenario analyzed increases. Therefore, in an analysis process, only those scenarios that can have a significant impact should be considered.

To manage the safety of a system [9, 15, 35], one first identifies the hazards, and then assesses the risks associated with each hazard, determining for each whether it is tolerable or not. An incorrect perception of a hazard or the associated risk could lead either to the ineffective use of resources to eliminate or reduce unwanted effects, or to the acceptance of risks whose tolerance exceeds the degree of affordability of the organization or community. To benefit from the advantages of a design that considers possible hazards, it is necessary to identify and analyze them in the early stages of the project. Understanding the hazards and risks identified and assessed from these analyses forms the basis for determining the safety management activities that the organization will undertake.

Hazard identification and associated risk assessment is performed at all phases of a system's life cycle - conceptual, preliminary, detailed design, manufacturing, operation, or decommissioning. However, the earlier a hazard is identified, the lower the costs of elimination or control will be.

Mainly, a hazard analysis should deliver:

- the documented analysis of the hazards that may have an impact on the system
- assessing the risks associated with each hazard in terms of probability of occurrence and cost of the consequences
- documented risk tolerance criteria of the organization or community
- proposals for elimination or control measures for each risk
- documentation of the effect after the application of control measures
- assessment of residual risks remaining after the application of control measures
- evaluation of the effect of risk control (impact on operation and maintenance costs, reduction of downtime, etc.).

In this endeavor, the only viable solution is to approach product development by applying the principles of systems engineering. At the same time, participation in the development process of specialists in safety and system security, fire protection, occupational health, and the environment alongside automatists, mechanics, chemists, electricians, electronics, and software engineers will ensure obtaining products that satisfy the most demanding safety requirements and security.

In most situations, the damage caused by a hazard is much less if preventive measures are taken that eliminate or mitigate the effects of the consequences. Experience has shown that the amounts spent on prevention are always much lower

than the amounts spent on repairing the effects of hazardous event actions.
In all fields of activity, the applicable preventive measures are regulated. In this sense, EU has developed the legislation that regulates the essential requirements. This consists of Directives [25, 26] and implementing Regulations, and to meet these requirements at the required quality level, the regulations indicate the applicable harmonized standards. E.g. regulations were developed in the fields of fire protection, transport (road, rail, naval, and air), pressure vessels, lifting installations, explosive atmospheres, working with dangerous substances, etc. To know if a product meets the safety requirements, it is necessary to identify the hazards, establish those that can generate losses greater than the assumed losses, and develop the measures that can be applied to reduce the damage to an a priori accepted level.

5. Impact of hazards on the railway

In the railway sector, hazards can generate events [27] with serious consequences (deaths or serious injuries resulting in permanent incapacity to work, major damage to the environment, destruction of some goods), moderate (injuries resulting in temporary incapacity to work, reparable damage to the environment and damage to some goods) or minor (slight injuries, minor damage to the environment, easily repairable damage to some goods). In general, serious events have a relatively low frequency, but most often result in fatalities and destruction or major damage to vehicles and/or infrastructure.
In the EU, in the last ten years, the number of serious railway accidents has slightly decreased (Fig. 1) but remains at a worrying rate. In 2022, there were 1, 615 significant railway accidents in the EU, with a total of 808 persons killed and 593 seriously injured, 15.9 % more railway accidents in the EU compared with 2021. The deaths were due to collisions (6 people), derailments (6 people), level crossing accidents (237 people), accidents by rolling stock in motion (555 people), fires in rolling stock (1 person), other types of accidents (3 people). Hazards that can lead to collisions, derailments, fires or other types of accidents affect both passenger and freight trains. In all cases, potentially hazardous events occur because during design, manufacture, operation, or maintenance some hazards were not considered.
If the damage to the environment, infrastructure, and other assets is added, the impact of the hazards becomes worrisome. In EU 27, in 2022 the total costs of railway accidents are around 3,2 billion EUR (cost of fatalities 2.111 mil EUR, costs of serious injuries 233 mil EUR, material damage, costs of non-use of rolling stock, cost of delays and costs to environment 594 mil EUR and other costs 214 mil EUR).

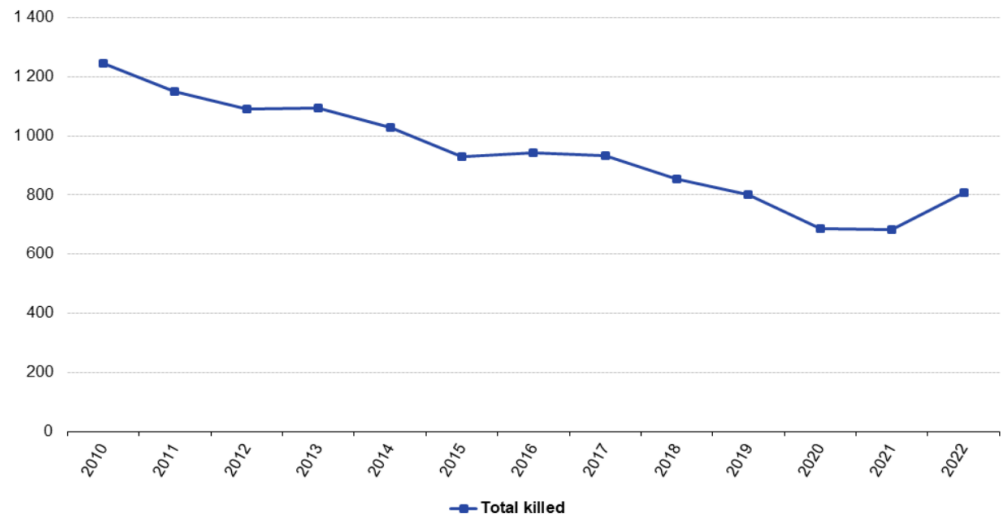

Fig. 1. Deaths in railway accidents, EU 2010 – 2022 (source: Eurostat).

5. Design for safety

Design for safety is a development process [5, 13, 15, 19] by which designers ensure the implementation of functional, technical, contextual, and essential requirements in a validated prototype. Among other requirements in the group of essential requirements are the requirements of reliability, availability, maintainability, safety, and security.

In the design process, the potential hazards and associated risks are analyzed at each phase of the life cycle, seeking and implementing solutions that eliminate or reduce the consequences of hazardous events. The prevention of potentially hazardous situations can be done if appropriate measures are taken in the design, prototype manufacturing, validation, certification, and experimentation phases under nominal working conditions before placing on the market. At the same time, the operation and maintenance manuals and the disposal project are drawn up.

In the incipient phases of the project, the possible hazards that could arise are identified and analyzed [4, 11]. For each hazard, solutions are sought that, implemented by designers, can lead to elimination. If hazards cannot be eliminated - the most common situation - solutions are sought which, through application, diminish consciousnesses to a tolerable level. These solutions generate safety

requirements that are introduced in the Safety Requirements Specification [7, 9, 15] along with implicit safety requirements as a result of legal regulations or clauses of agreed standards [31, 36, 37, 38].
The hazard identification [10, 11, 17] is repeated after each phase of the life cycle, taking the necessary measures to eliminate or reduce the consequences. In this process, it must also be considered that the people who design, manufacture, operate, or maintain, consciously or unconsciously, can introduce new hazards. Conventional methods such as HAZID, HAZOP, ETA, FMECA, etc. are used to identify hazards.
Hazard assessment is a multi-step process which consists of [1, 7, 13]:

- hazard identification
- identification of dangerous events that each hazard generates
- estimation of the frequency of dangerous events of each hazard
- estimation and analysis of the severity of the consequences of the action of hazardous events
- defining the tolerance threshold of damage caused by hazardous events
- develop a plan of measures to eliminate the hazards (if possible), and reduce the consequences to a tolerable level
- re-evaluation and updating the Safety Requirement Specifications after each stage of the life cycle, if necessary.
-

Hazard analysis uses all available information to identify and forecast the frequency of transformation into a hazardous event and estimate the consequences and severity of their actions. A hazard can generate several hazardous events. For example, in certain situations, the fire hazard can result in death, serious, moderate, major, or minor injuries, and damage to affected assets and the environment.
Often the hazardous events have the same frequency of occurrence, but the consequences are different. The analysis of each hazardous event to estimate the frequency and severity of the consequences is a *risk analysis*. Hazard analysis and risk analysis generate safety requirements that the design will need to consider in the development of product manufacturing documentation.
The purpose of the analysis is to develop solutions to eliminate hazards, where possible, and to minimize the effects of events generated where those hazards cannot be eliminated. This activity covers hazards that apply to systems/ subsystems/ products/ equipment/ infrastructure (including hardware and software) during design, testing, manufacturing, commissioning, use, and disposal.
Once the requirements specification has been checked and validated [8, 9, 20] the prototype design phase can be moved on (Fig.2). To see if new hazards were introduced during the design or if the already identified ones were treated incorrectly, the hazard analysis is repeated. If new hazards have appeared, the design is restarted to remove them. If there are no solutions to eliminate the newly introduced hazards, the risk analysis is resumed, and solutions are sought to mitigate the consequences up to the tolerable limit.
In general, the prototype project documents [15, 30] include the execution

drawings, work instructions, control instructions, installation, operation and maintenance manuals, and test specifications to prove the fulfillment of the requirements as established. Finally, traceability of requirements across development phases is verified and validated [8, 9, 20]. If the project meets the established functional, technical, contextual, and safety requirements, it can proceed to prototype manufacturing.

Validation of the entire development activity includes evaluation of the quality of project management, design documents, safety analysis, and the prototype's fulfillment of functional, technical, contextual, and safety requirements. All this is also the support of the safety assessment by an independent assessor. Positive reports from the validator and the independent safety evaluator entitle the prototype to be tested in commercial operation. If the analysis of the test results shows that the product is safe for use and performs its functions in the given operational context it can be considered accepted for commercial use. Acceptance for commercial use brings the transfer to the operator and maintainer of mandatory rules to ensure safe use. These rules aim to treat the residual risks that result from the designer's application of the most appropriate solutions to eliminate the consequences of dangerous events.

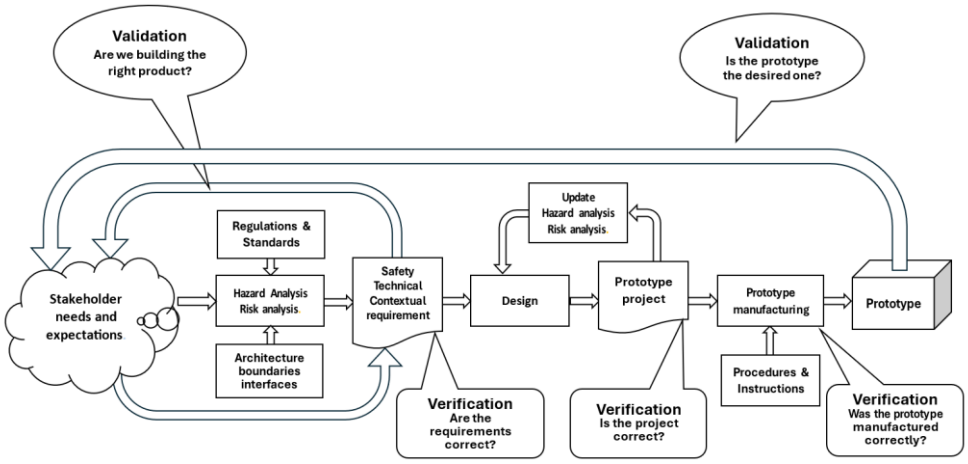

Fig. 2. Design for safety.

5. Conclusion

Railway equipment that is safe to operate does not endanger the health of the people, and does not harm the environment, infrastructure, or other assets is the

result of *design for safety*. This process is based on identifying and analyzing the hazards and risks associated with each hazard in the initial phase of the project, finding and applying solutions to eliminate or reduce possible effects. Confidence in the results of the process is given by the verification and validation of the design documents and the prototype. Maximum safety and security performance is obtained using, in the same project, the principles of *design for reliability, availability, maintainability, and safety* or *design for RAMS.*

Once the prototype meets all the functional, technical, contextual, and safety requirements it is subjected to experimentation in real operating conditions. Any hazard not identified until this phase, but identified during experimentation leads to the resumption of the project from wet phases, it is identified that the new hazard can be eliminated, or its consequences reduced to an accepted level of losses. Finally, after experimentation has shown that the hazards have either been eliminated or the consequences of their effects have been reduced to an acceptable level, the product can be considered safe for use.

References

[1] Akao Yoji, *Quality Function Deployment: Integrating Customer Requirements Into Product Design*, Taylor & Francis 2004.

[2] American Institute of Chemical Engineers, Inc., Guidelines for defining process safety competency requirements, Willey, 2015.

[3] Bozzano, M., Villafiorita A., *Design and safety assessment of critical systems*, Auerbach Pub, 2010.

[4] Ericson, Clifton A., *Hazard analysis techniques for system safety*, John Wiley & Sons, Inc. 2005.

[5] Gruhn P., Cheddie H., *Safety instrumented systems: design, analysis, and justification*, ISA - The Instrumentation, Systems, and Automation Society USA, 2006.

[6] Hassami A.G., *A Systems View of Railway Safety and Security*, INTECH 2015, http://dx.doi.org/10.5772/62080

[7] INCOSE, *Guide to wright requirements*, 2023.

[8] INCOSE, *Guide to Verification and Validation*, 2022.

[9] INCOSE, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, John Wiley and Sons Inc, 2015.

[10] Perpiñà Xavier, *Reliability and Safety in Railway*, IntechOpen 2012.

[11] Macdonald, D. M, *Practical hazops, trips and alarms*, IDC Technologies 2004.

[12] Melnick Edward L., Everitt Brian S., *Encyclopedia of quantitative risk analysis and assessment*, Willey, 2008.

[13] Saleh J. H., Marais K. B., Favaro F. M., *System Safety Principles: A Multidisciplinary Engineering Perspective*, https://works.bepress.com/francesca-favaro/6/

[14] NASA System Safety Handbook Volume 1, *System Safety Framework and Concepts for Implementation*, 2011.

[15] Project Management Institute, *A guide to the project management body of knowledge* (*PMBOK® guide*), The Seventh edition, 2021.

[16] Sasidharan M., Burrow M. P.N., Ghataora G. S., *A review of risk management applications for railways*, Railway Engineering-2017, DOI: 10.25084/raileng.2017.0065

[17] Smith David J., Simpson Kenneth G. L., *Safety Critical Systems Handbook*, Elsevier

(Butterworth- Heinemann), 2020.

[18] Walls Lesley, Revie Matthew, Bedford Tim, *Risk, reliability and safety: innovating theory and practice*, CRC Press Taylor & Francis Group 2017

[19] Zlatian R., Girnita I., Rachieru D., Dresca O., *The process of development of railway vehicle subsystems*, 2023, 10th International Conference on Modern Power Systems (MPS), DOI: 10.1109/MPS58874.2023.10187584

[20] Zlatian R., Dresca O., *Verification and validation of safety-critical systems*, 2023 International Conference on Electromechanical and Energy Systems (SIELMEN), DOI: 10.1109/SIELMEN59038.2023.10290853

[21] European Commission notice The "Blue Guide" on the implementation of EU product rules 2022 (2022/C 247/01), Document 52022XC0629(04) Official Journal of the European Union, C 247/1

[22] Regulation (UE) 988/2023 of the European Parliament and of the Council regarding the general safety of the products, Document 32023R0988 Official Journal of the European Union, L135/1

[23] Regulation (EC) no. 765/2008 of the European Parliament and of the Council of 9 July 2008 establishing the requirements for accreditation and market surveillance with regard to the marketing of products and Decision 768/2008/EC of the European Parliament and of the Council of 9 July 2008 regarding a framework common for the marketing of products European Union – Agency for Railways Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety, Document 32008R0765 Official Journal of the European Union, L218/30

[24] Regulation (EU) 2012/1025 of the European Parliament and of the Council of 25 October 2012 on European standardization, Document 32012R1025 Official Journal of the European Union, L316/12

[25] Directive (EU) 797/2016 of the European Parliament and of the Council on interoperability of the rail system within the European Union, Document 32016L0797, Official Journal of the European Union, L138/44

[26] Directive (EU) 798/2016 of the European Parliament and of the Council on Railway Safety, Document 32016L0798 Official Journal of the European Union, L138/102

[27] European Union, Agency for Railways, Safety Overview, Publications Office of the European Union 2023

[28] European Union, Agency for Railways. Guideline for the application of harmonized design target (CSM-DT) for technical systems as defined in (EU) Regulation 2015/1136 within the risk assessment process of Regulation 402/2013, ver. 1.1, ERA-REC-116-2015-GUI 2017

[29] European Union, Agency for Railways, Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment, Document 32013R0402 Official Journal of the European Union, L121/8

[30] European Union, Agency for Railways, Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment, Document 32015R1136 Official Journal of the European Union, L185/6

[31] CENELEC EN 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety - Part 1: Generic RAMS

[32] CENELEC EN 50126-2 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety - Part 2: Systems Approach to Safety

[33] CENELEC EN 50129 Railway Applications. Communication, signalling, and processing systems. Safety-related electronic systems for signalling

[34] CENELEC EN 50128 Railway applications - Communication, signaling, and processing systems. Software for railway control and protection systems

[35] ISO 31010 Risk management - Risk assessment technique

[36] ISO 21500 Guidance on project management

[37] IEEE Std 24748-1™-2011 Systems and Software Engineering - Life Cycle Management - Part 1: Guide for Life Cycle Management

[38] MIL-STD-882E, USA DoD, System safety.