ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 3 (63)

UDC 656.25

M. KYCKO[1*]

[1*]Dep. «Quality and Certificicatio Division», Railway Institute, Chłopickiego Józefa St., 50, Warsaw, Poland, 04-275, tel. +48 (84) 473 10 71, e-mail mkycko@ikolej.pl, ORCID 0000-0002-8447-2472

COMMAND – CONTROL AND SIGNALING SYSTEM DOCUMENTATION AND ITS SAFETY

Purpose. The publication presents the importance and influence of railway traffic control system documentation on its safety. Furthermore, it presents certain selected issues of formal and semi-formal description. **Methodology**. Development of correct and complete descriptions of the informal, semi-formal and formal becomes important in terms of safety requirements. Background documentation and forms of command-control and signaling system description are the base documents of proof of safety. It seems necessary to implement the analysis of the design, manufacture process and operation of safety-related equipment into the work of the Polish railways. Firstly, this applies to traffic control devices. **Findings**. This publication also shows the importance of risk analysis, which is essential when deciding on the implementation of signaling systems to operate, which require both in the regulations and making rational decisions about the implementation of the systems. **Originality.** Presented a problem changes the approach to certain records and makes us aware of their validity. **Practical value**. The presented problems can help understand certain legal requirements.

Keywords: control systems; formal description; risk; safety; informal description.

Introduction

Safety is the basis of any rail transport and signaling system. Risk analysis is a key element of safety management systems in rail transport. The method used, good practices, practical and diligent approach to risk analysis largely determine the efficiency of activities and effectiveness of measures designated to improve railway safety. The importance of safety may be analyzed in terms of a wide range of factors.

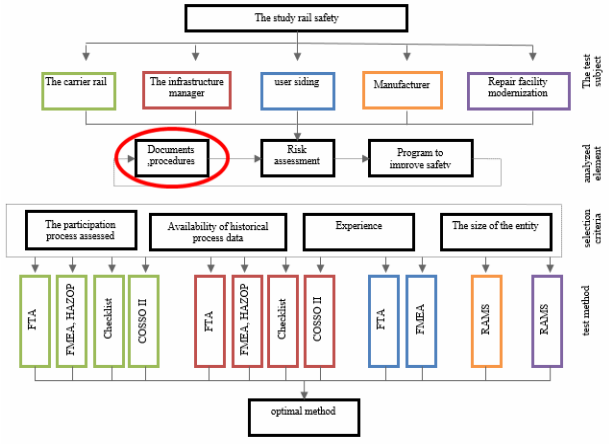

Fig. 1. Safety components and test methods for rail transport

The diagram (Fig. 1) shows that documentation is an important element of the safety components. Within the RTC systems, safety is the key factor which qualifies a particular system for release to service. Following Poland's accession to the EU structures within the area of safety, the following standards have become applicable: PN-EN 50126, EN 50128 and EN 50129]. PN-EN 50126 standard determines the reliability, availability, maintainability and safety (RAMS), as a process based on the system life-cycle. This process defines particular stages of the system and procedures for approval before moving on to the next stage (requirement specification, design, implementation, etc.). Standard EN 50128 specifies the procedures and technical requirements for designing software for secure electronic system of railway control and security [8]. It should be noted that this standard is not fully obligatory. Standard EN 50129 defines the requirements for the design, testing, commissioning and approval of electronic systems, subsystems and related signaling devices with security in railway applications.

Purpose

The introduction of electronic systems in the field of railway traffic control into the railway transport required defining the rules which would replace or supplemented the fail-safe principle. To this end, the safety integrity levels (SIL) were de-

doi 10.15802/stp2016/74711

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)
Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 3 (63)

fined. The fact that they are in use means that the ail-safe principle is applied at the system function or module levels, and at the hardware lever, an analysis is carried out concerning the security measures preventing random and systemic damage, where the occurrence of random damage is associated with defects of memory, processors, etc. and the occurrence of systemic damage is associated with human errors throughout the entire system life cycle, which means that these also include, among other things, its design and maintenance.

Neither the fail-safe principle nor a high level of SIL, usually SIL4, which are interpreted as a guarantee of full security, do not ensure complete elimination of accidents and events in rail transport. According to the Community law, security means the absence of unacceptable risk (i.e. no hazard). In order to achieve security, according to the prevailing approach, in accordance with the Community law, it is necessary to manage security through security monitoring following respective risk management. Risk management involves scheduled application of management policies, procedures and practices in the field of risk analysis, risk valuation and hazard recording by infrastructure managers and railway carriers. Security monitoring is the systematic application of management strategies, priorities and plans by the same managers and carriers in order to maintain security.

Methodology

The process of designing, manufacturing, deployment and operation of computerized control-command and signalling systems due to the complexity and compliance with the safety requirements while maintaining the conditions of integrity of the structure of hardware and software SIL 4 requires application of specific rules and procedures. In the area of knowledge relating to this process, there are a number of different standards developed by individual centres, academic and industrial societies which develop their own standards and do not meet the mutual compatibility requirements. Regardless of any individually developed methods, the process of control-command and signalling system development may proceed methodically based on the recommended scheme called the V cycle, taking into account the assumptions of the RAMS analysis.

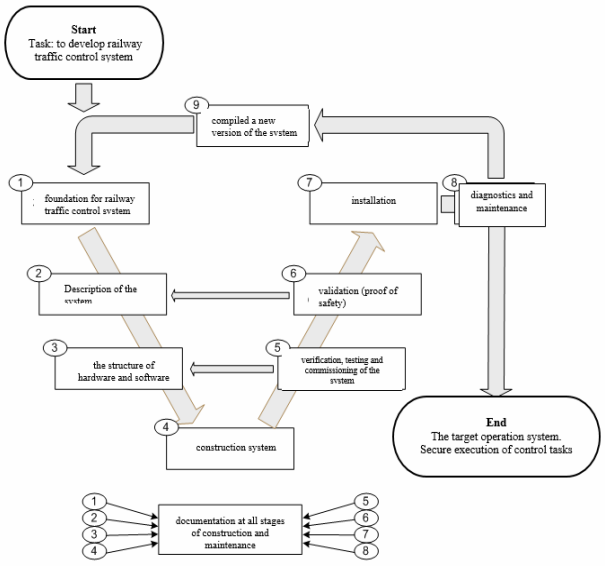

Fig. 2. Cycle V signaling system construction

The diagram (Fig. 2) shows the scheme of the control-command and signalling system implementation process which lists each step of the process and shows that it is important to create records of every stage of the system development. Creation of the said records at every stage is intended to mitigate the number of errors committed in the course of the system development, thus increasing the level of security of such systems. The system design and development begin with the control-command and signalling system assumptions development which include informal description documents. In the Polish design and investment reality, these may include documents prepared at the stage of orders, e.g. Specification of Material Terms and Conditions of Order, Ordered Item Description and other informal documents, including an informal analysis of the specifications or documents specifying additional control-command and signalling system requirements completed a detailed formulation of principles of the control-command and signalling system. Documents such as the Specification of Material Terms and Conditions of Order, Ordered Item Description form the basis of performed tasks, which is why it is important that they contain clear and accurate information.

Once the informal documents are gathered, semi-formal description documents are designed. Based on the semi-formal description formal description is prepared which contains specification of data bases and the dependency relationship. On

doi 10.15802/stp2016/74711

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)
Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 3 (63)

the basis of the formal specifications algorithms and software are developed. The process of creating the semi-formal and formal descriptions may also be automated by use of information systems. A sample description of the sequential formation of the specifications related to the drivers, confirming the adopted principle of applying the subsequent stages of design, was presented e.g. in [3], in accordance with IEC 61131 standard. In the process of creating a control system involves engineers and experts of different specialties including specialists who prepare the informal descriptions in natural language, specialists in control technique and technology as well as IT specialists and programmers. The knowledge and experience of the people involved in the system development is essential, otherwise confusion or errors may arise, which ultimately has material adverse impact on the safety level.

The informal control-command and signalling system description documents include, but are not limited to:

− the above-said Specification of Material Terms and Conditions of Order, Ordered Item Description ;

− instructions, e.g. [4] and other specific documents, depending on the specific requirements and objectives for which the control-command and signalling system is developed;

− station work description (station work technology)

− control-command and signalling equipment scheme.

The formal and semi-formal documents include, but are not limited to conduct ways specification within the station area with the demonstration of the way objects and safety facilities;

− dependency table and/or other related documents;

− scheme and table of inter-relations of a station track scheme (so-called track system model)

− conducts runs cards;

− contradictory runs table.

The formal description documents are collections of data and relations expressed, depending on the accepted standards, by more or less advanced syntactic and editorial forms. The sequence of development of the control-command and signalling system descriptions is shown in Fig. 3.

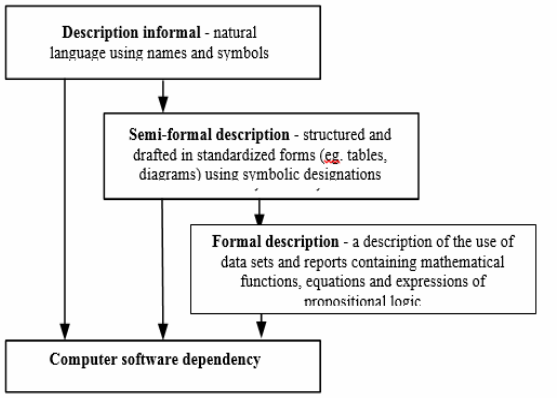

Fig. 3. Descriptions of the control-command and signalling system

Development of informal, semi-formal and formal (i-s-f) descriptions, and consequently the system designing should be in particular consistent with the assumptions and guidelines of many documents and regulations. The beginning of the design process is determined by the informal description documentation underlying the semi-formal description, which in turn becomes the basis for a formal description, which, as the only form of description, enables algorithmization and development of dependency computer software. This means that any errors committed or not detected at the first stage of the process, i.e. in the course of development of informal records, are usually reproduced in subsequent process stages. All forms of «i-s-f» description are mandatory documents also used i.a. for the purposes of validation, i.e. conformity (consistency) verification, assumptions and testing review. However, despite the clearly formulated guidelines for the design principles, in practice, there is no indication of all the substantive description elements. This enables the designers to achieve the various control-command and signalling system concepts. Certain conditions that should be fulfilled by any «i-s-f» descriptions were indicated. These conditions include clarity of information, completeness of documentation and the principle of generation of the subsequent document on the basis of algorithmization he previously developed documents.

The system documentation greatly influences the level of safety of a particular railway traffic control system. The most important documents of the control-command and signalling system include certification documents that are required un-

doi 10.15802/stp2016/74711

der Directive 2008/57/EC of 17 June 2008, and the technical specifications for interoperability (TSI). In accordance with the above Directive, in order to be put into service, each subsystem or interoperability constituent shall receive an EC verification certificate, which is issued by the notified body. The notified body selected by the project contractor will be able to issue the certificate of EC verification after it has checked and confirmed that the subsystem or interoperability constituent meet all relevant Technical Specifications for Interoperability. The TSI requirements are checked at various stages of investment, i.e. at the design, construction and final testing stages.

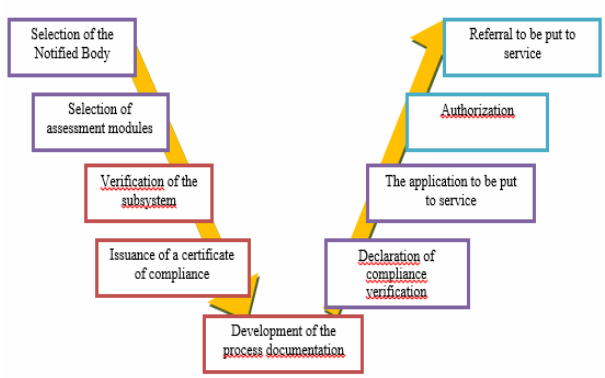

Fig. 4. Stages of the process of obtaining approval to be put to service [5]

In order to be put to service, the documentation of a given control-command and signaling system must be complete and in accordance with the requirements and standards cited in the TSI (Decision 2012/88/EU, as amended), namely also with the safety standards, i.e. PN-EN 50126, BS EN 50128 and BS EN 50129 standards.

The control-company subsystem must be built and installed in accordance with the Community law, and at the same time it must be compatible with the existing railway system to which it is activated. The notified bodies are responsible for the examination of the subsystem conformity with the essential requirements of the Community. On the other hand, the bodies authorized by the Member State of the European Union where the subsystem is to be placed in service, perform the tasks related to verification of compliance of the subsystem with the national regulations.

The certification process is based largely on an assessment of the correctness and consistency of documentation which is not always so obvious. The certification process is designed to increase safety, or to exclude unacceptable risks in the manufactured command-control and signaling system.

Findings

The approach to the safety of rail transport in Poland and in Europe undergoes significant modification. These changes were initiated in 2004 under the provisions of the Directive on rail safety. This Directive makes it clear that all operators of railway systems, infrastructure managers and railway carriers should bear full liability for the security of the system, each one to their respective extent. This issue is a novelty in the rail industry and causes a lot of confusion of interpretation disputes, in particular due to the fact that it falls within the overlaping areas of technical and management sciences. The units assessing the adequacy of the risk management process in railway transport were forced to undertake activitied under the Commission Regulation (EC) No 352/2009 [10] on the adoption of a common safety method on risk evaluation and assessment, and the Commission Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and repealing Regulation (EC) No 352/2009. The introduction of the provisions of these regulations created the need for a systematic approach to risk management processes, including risk evaluation and assessment, which apply to all changes of the railway system considered significant. Risk analysis and risk are inherently connected to the security of the system, therefore they are one of the important elements in deciding on the application of the system.

The provisions of Polish and European standards require that the risk analysis be carried out not only with respect to the safety analysis, but also require that the risk analysis be a mandatory part of the decision-making process concerning the implementation of the system into service. The command-control and signaling system documentation should be prepared at every stage of the manufacturing, implementation or operation process. With the development of appropriate documentation, especially at the stage of the concept and design, the system can be considered safe.

doi 10.15802/stp2016/74711

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)
Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 3 (63)

Currently, a lot of risk analysis methods are applied such as E.g. the event tree analysis, fault tree analysis, or analysis of the types and effects of unfitness. The IEC 60300-3-9 standard recommends a risk analysis in the following order:

− scope delineation (area);
− identification of hazards and their consequences;
− risk assessment (impact and frequency);
− review
− documentation;
− updated analysis.

Originality

The infrastructure managers and railway carriers, by making changes in their activities, and accepting changes in subcontractors, regardless of whether these changes are of a technical nature, whether operational or organizational, are obliged to perform risk valuation, which is assessing the acceptability of risk introduced by the amendment. Such an assessment it is also required from the contracting entities and producers and contractors if they engage a notified body to carry out the EC verification procedure of the subsystem. This requirement means a commitment of contracting entities, manufacturers and contractors to carry out the assessment of the acceptability of risk introduced by the construction, modernization, renewal of the subsystem. Based on the criteria of risk acceptability, the acceptability of a specific risk is assessed; these criteria are used to determine whether the level of risk is low enough not to make it necessary to take immediate action to reduce it. The risk assessment resulting from a significant change, is carried out by verification of application of codes of practice or by comparison with similar systems or by open risk estimation. The choice of method is left to the infrastructure manager, the carrier, the contracting entity, manufacturer or contractor who conducts evaluation of the acceptability of risks arising from the significant changes and cannot be imposed by an independent Assessment Unit. In the event of any significant change it is required to carry out an independent assessment of the adequacy of the risk management process and its results, conducted by the Assessment Unit. With each change into the system or of any risk analysis must be created by appropriate documentation, which would later be assessed by the competent assessment bodies.

At each stage of creating a command-control and signaling system errors may occur, which then affect the proper operation of the system or its safety. The diagram (Fig. 5) shows an example of the cause of errors which, at a certain stage of development of the system, may cause a decrease the level of security.

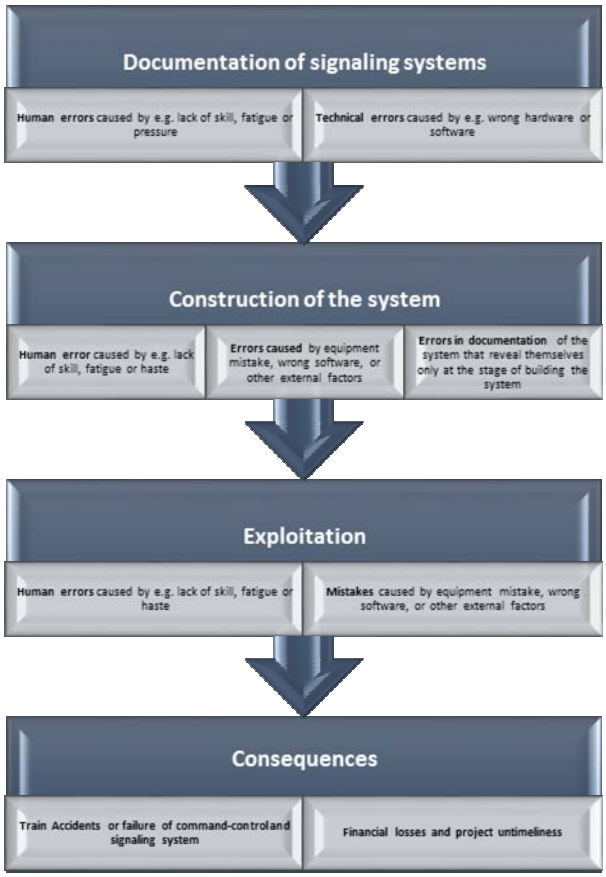

Fig. 5. Scheme of errors and their causes during the construction of the command-control and signaling system

The main factor in reducing the level of security is the human factor. Often at the first stage of the creation of the system documentation errors arise due to lack of knowledge and training among the staff, which at the later stages can lead to serious financial losses, and more. The organization of the competence of personnel of all stakeholders is certainly a difficult challenge.

doi 10.15802/stp2016/74711

Conclusion

The influence of the command-control and signaling system documentation on the safety of such systems, as presented in this publication, demonstrates the importance of correct documentation created in the process of release to service. Preparation of informal and semi-formal description documents is obligatory, but nevertheless they must comply with the relevant requirements and should be analyzed in terms of risk assessment. The formal description documents enable algorithmization by developing a series of tools relevant to the design documentation for the command-control and signaling system of under safe conditions, that is, i.a. the development of the safety confirmation. The question of formalizing the description of signaling systems, although a number of secure computer systems have been developed, is still valid. The search for new forms of standardization of documentation – descriptions of signaling systems, and including the formalization of the description, is used to minimize the risk to preserving the condition of the integrity of the system-level design process. When creating informal or formal documents it is crucial that they are prepared by competent personnel which have a large impact on the correctness of these documents, which of course also results in an increase in the level of security of the system.

LIST OF REFERENCE LINKS

1. Białoń, A. Problemy certyfikacji urządzeń srk na przykładzie ERTMS / A. Białoń, P. Gradowski, A. Toruń // Problemy kolejnictwa. – Warszawa, 2011. – P. 81–85.
2. Białoń A. Bezpieczeństwo i ryzyko na przykładzie urządzeń sterowania ruchem kolejowym Problemy kolejnictwa / A. Białoń, M. Pawlik. – Warszawa, 2014. – Z. 163. – P. 27–28.
3. Dyrektywa 2008/57/WE Parlamentu Europejskiego i Rady z dnia 17 czerwca 2008 r. w sprawie interoperacyjności systemu kolei we Wspólnocie. – P. 8–14.
4. Dyrektywa Parlamentu Europejskiego i Rady 2008/110/WE z dnia 16 grudnia 2008 r. zmieniająca dyrektywę 2004/49/WE w sprawie bezpieczeństwa kolei wspólnotowych.
5. Fischer, S. Systematic Specification of a Logic Controller for a Delayed Coking Drum / S. Fischer, H. Teixeira, S. Engell // Proc. of the 11th Intern. Symposium on Process Systems Engineering. – Singapore, 2012. – Vol. 31. – P. 355–359. doi:10.1016/B978-0-444-59507-2.50063-9.
6. Gradowski, P. Aktualne problem certyfikacji urządzeń sterowania ruchem kolejowym / P. Gradowski, A. Białoń. – Logistyka. – 2014. – № 3.– P. 2183–2184.
7. Instrukcja o prowadzeniu ruchu pociągów Ir-1 (R-1), tekst ujednolicony przyjęty uchwałą Nr 176/2008 oraz zarządzeniami Nr 3/2011 i Nr 13/2014 Zarządu PKP Polskie Linie Kolejowe S.A.
8. Kycko, M. Koncepcja metody oceny i wyboru rozwiązania ERTMS/ETCS dla linii kolejowej o zadanych parametrach ruchowo – przewozowych, praca magisterska / M. Kycko. – Politechnika Warszawska, Wydział Transportu, Warszawa, 2015. – P. 39–58.
9. Maciejewski, W. Basis of the Formalization and the Algorithmization of the Control Functions in ATC Systems / M. Maciejewski, W. Zabłocki // Communications in Computer and Information Science. Transport Systems Telematics. – 2010. – Vol. 104. – P. 253–262. doi: 10.1007/978-3-642-16472-9_28.
10. PN EN 50129:2007. Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signaling. – P. 20–27.
11. PN EN 50128:2011. Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems. – P. 15–16.
12. PN EN 50126:2002. Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety. – P. 7–10.
13. Rozporządzenie Komisji (WE) nr 352/2009 w sprawie przyjęcia wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka. – P. 10–17.
14. Rozporządzenie wykonawcze Komisji (UE) nr 402/2013 w sprawie wspólnej metody oceny bezpieczeństwa w zakresie oceny i wyceny ryzyka i uchylające rozporządzenie nr 352/2009. – P. 13–15.
15. Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym – DG PKP KA nr KA2b-5400-01/98 z dnia 06.02.1998 r.
16. Wytyczne techniczne budowy urządzeń sterowania ruchem kolejowym Ie-4 (WTB-E10), Załącznik do zarządzenia Nr 1/2014 Zarządu PKP Polskie Linie Kolejowe S.A. z dnia 14 stycznia 2014. – P. 100–107.
17. Zabłocki, W. Podstawy opisu formalnego zależności stacyjnych / W. Zabłocki // TRANSPORT: Prace naukowe / Politechnika Warszawska. – Warzsawa, 2007. – Z. 62. – P. 2–6.

doi 10.15802/stp2016/74711

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 3 (63)

М. КІЦКО[1*]

[1*]Каф. «Відділ якості та сертифікації», Залізничний інститут, вул. Хлопіцького Юзефа, 50, Варшава, Польща, 04-275, тел. +48 (84) 473 10 71, ел. пошта mkycko@ikolej.pl, ORCID 0000-0002-8447-2472

УПРАВЛІННЯ, КОНТРОЛЬ, ДОКУМЕНТАЦІЯ СИСТЕМИ СИГНАЛІЗАЦІЇ ТА ЇЇ БЕЗПЕКА

Мета. В науковій статті необхідно розглянути важливість використання документації системи управління рухом поїздів та її вплив на безпеку руху. Крім того, треба висвітлити певні виборчі питання формального і напівофіційного опису цієї документації. **Методика**. Розробка правильних та повних неофіційних, напівофіційних і офіційних описів стає важливою з точки зору вимог безпеки. Пояснювальна документація, форми управління-контролю та опису системи сигналізації є основними документами доказу її безпеки. Необхідним є здійснення аналізу проектування, процесу виробництва та експлуатації обладнання, пов'язаного з безпекою руху в роботі польських залізниць. Перш за все, це відноситься до пристроїв управління дорожнім рухом. **Результати**. Дана публікація показує важливість аналізу ризику, який має суттєве значення для прийняття рішення щодо впровадження систем сигналізації у роботу. Ці результати потрібні також для нормативних актів. **Наукова новизна**. Вирішення представлених проблем змінює підхід до певних даних і доводить до відома про їх дійсність. **Практична значимість**. Розглянуті в статті питання допомагають зрозуміти певні юридичні вимоги.

Ключові слова: системи управління; формальний опис; ризик; безпека; неформальний опис

М. КИЦКО[1*]

[1*]Каф. «Отдел качества и сертификации», Железнодорожный институт, ул. Хлопицкого Юзефа, 50, Варшава, Польша, 04-275, тел. +48 (84) 473 10 71, эл. почта mkycko@ikolej.pl., ORCID 0000-0002-8447-2472

УПРАВЛЕНИЕ, КОНТРОЛЬ, ДОКУМЕНТАЦИЯ СИСТЕМЫ СИГНАЛИЗАЦИИ И ЕЕ БЕЗОПАСНОСТЬ

Цель. В научной статье необходимо рассмотреть важность использования документации системы управления движением поездов и ее влияние на безопасность движения. Кроме того, надо осветить определенные избирательные вопросы формального и полуофициального описания этой документации. **Методика.** Разработка правильных и полных неофициальных, полуофициальных и официальных описаний становится важной с точки зрения требований безопасности. Пояснительная документация, формы управления контроля и описания системы сигнализации являются основными документами доказательства ее безопасности. Необходимо проведение анализа проектирования, процесса производства и эксплуатации оборудования, связанного с безопасностью движения в работе польских железных дорог. Прежде всего, это относится к устройствам управления дорожным движением. **Результаты**. Данная публикация показывает важность анализа риска, который имеет существенное значение для принятия решения по внедрению систем сигнализации в работу. Эти результаты нужны также для нормативных актов. **Научная новизна.** Решение представленных проблем меняет подход к определенным данным и доводит до сведения об их действенности. **Практическая значимость.** Рассмотренные в статье вопросы помогают понять определенные юридические требования.

Ключевые слова: системы управления; формальное описание; риск; безопасность; неформальное описание

Prof. V. G. Sychenko, D. Sc. (Tech.) (Ukraine) recommended this article to be published

Accessed: Feb., 29. 2016
Received: May, 31. 2016

doi 10.15802/stp2016/74711