ORIGINAL ARTICLE
DOI: https://doi.org/10.30932/1992-3252-2022-20-3-6

World of Transport and Transportation, 2022,
Vol. 20, Iss. 3 (100), pp. 168–175

Conceptual Foundations of the Synthesis of Safe Train Traffic Control Systems

Dmitry V. EFANOV

Valery V. KHOROSHEV

German V. OSADCHY

Dmitry V. Efanov [1–3]***, Valery V. Khoroshev*** [1]***, German V. Osadchy*** [4, 5]

[1] *Russian University of Transport, Moscow, Russia.*
[2] *LLC Research and Design Institute for Transport and Construction Safety, St. Petersburg, Russia.*
[3] *Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia.*
[4] *LLC STC Complex monitoring systems, St. Petersburg, Russia.*
[5] *Emperor Alexander I St. Petersburg State Transport University, St. Petersburg, Russia.*
✉ [1] *TrES-4b@yandex.ru.*

ABSTRACT

The article analyses the problem of synthesis of the systems of safe control of critical technological processes on the example of railway automation and remote control systems.

It is shown that modern control systems for complex distributed systems, such as a railway transport system, are not implemented with absolute safety. The safety of such systems is limited by considering only their own failures, external failures of control systems and their components, as well as failures of infrastructure objects that directly interact with control devices. Other infrastructure facilities are not considered in any way during automatic control and data transfer to on-board automation.

The objective of the article is to present theoretical concept of the synthesis of safe train traffic control systems, considering the capacity of equipping infrastructure facilities with highly reliable and safe means of technical diagnostics and monitoring.

A shown simplified structure of the central train traffic control centre considers the results of diagnosing and monitoring all the components of the transportation process.

The conditions for the synthesis of completely safe train traffic control systems are formulated along with the accompanying tasks.

A comprehensive accounting of the parameters of railway infrastructure facilities and rolling stock will allow reaching a qualitatively higher level of train traffic safety.

Keywords: train traffic control system, railway automation and remote control, train traffic safety, finite-state automaton (finite-state machine), dangerous failure of a railway infrastructure facility, functional safety of the monitoring system.

Acknowledgments: this work is a continuation of the research of honoured scientists of the Russian Federation, doctors of engineering sciences, Professors Valery Vladimirovich and Vladimir Vladimirovich Sapozhnikov, who have made a significant contribution to development of the theory of synthesis of self-checking, fault-tolerant, reliable and safe control systems for critical technological processes, including train traffic. We express our gratitude to our teachers and colleagues for the basic ideas and created opportunities for the development of intelligent technologies for the synthesis of safe control systems.

For citation: Efanov, D. V., Khoroshev, V. V., Osadchy, G. V. Conceptual Foundations of the Synthesis of Safe Train Traffic Control Systems. World of Transport and Transportation, 2022, Vol. 20, Iss. 3 (100), pp. 168–175. DOI: https://doi.org/10.30932/1992-3252-2022-20-3-6.

The text of the article originally written in Russian is published in the first part of the issue.
Текст статьи на русском языке публикуется в первой части данного выпуска.

INTRODUCTION

A huge number of works of scientists, engineers and researchers are devoted to the issues of synthesis of safe control systems for critical technological processes, including train traffic control in railway transport [1–5]. At the same time, oddly enough, this task remains relevant.

With development of engineering and technology, there emerge the ways to improve safety performance and to consider the functioning and impact of adjacent objects and systems. However, to date, they have owned very limited character being aimed at improving «point» solutions. As an example, one can quote improving reliability and safety of the electrical interlocking system through the use of more reliable components and equipment. This is evidenced by numerous publications in this field, among which we might note the works [6–9].

Improving safety of the train traffic control system can be achieved by implementing more advanced methods of self-diagnosis of the infrastructure complex through the use of external technical means for diagnosing and monitoring. It follows from fundamental works [2; 10] that, for example, in the synthesis of safe systems of railway automation and remote control (RARC), the technical condition of railway infrastructure facilities has still not been fully taken into account. The latter go through the procedure of test and functional diagnostics during operation, but the results there-of are not considered when implementing control algorithms. They are used only to organise procedures for periodic and unscheduled maintenance [11–13]. Moreover, even the automation devices themselves do not fully automatically transmit data on their technical condition to be considered in control processes [14; 15]. This is due, first, to the historically prevalent principles of building control systems in railway transport, to the established institute of standardisation, certification, and to safety evidence, as well as to the lack of techniques to account for data from technical diagnostic and monitoring systems (DMS) for automatic process control.

The task of synthesising a safe control system is solved by eliminating the influence of those events that lead to incorrect implementation of control algorithms and dangerous failures. Such failures not only affect the technological process in the form of its shutdowns, but create conditions for the occurrence of catastrophic disturbances, resulting in damage, accidents, and crashes. Therefore, in the synthesis of safe control systems, a whole range of measures is used to protect and parry dangerous failures: the use of controllable device structures, the use of self-monitoring, self-checking and fault-tolerant logic circuits, the use of elements with an asymmetric failure characteristic, the use of redundant coding, the introduction of structural, informational and temporal redundancy, implementation of safe interface devices, etc. [1–5; 10; 16–20].

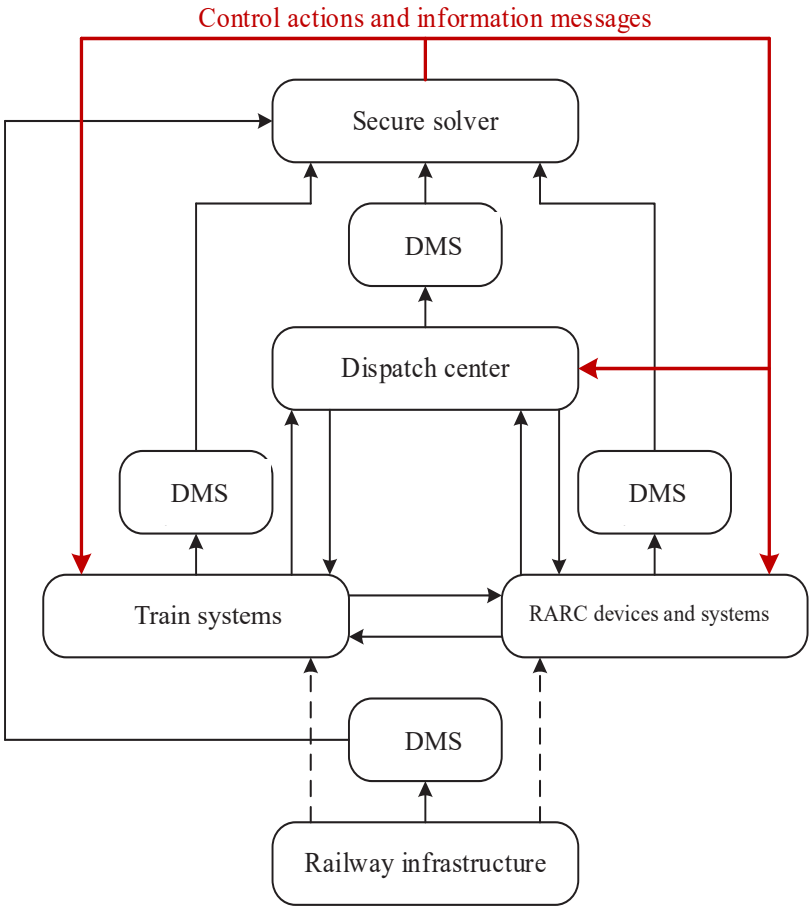
The *objective* of this work is to present theoretical foundations for the synthesis of safe signalling and train traffic control systems on railways. In contrast to previous studies, it is proposed to consider not only safety of functioning of the very means of railway automation and remote control, but also of infrastructure and rolling stock that do not directly interact with them. Such accounting is possible through the use of diagnostic and monitoring systems, which, however, must be implemented according to well-defined principles, be highly reliable, and provide information with a high predetermined reliability [21–23].

RESULTS

1. Train Traffic Control System Safety

In the modern paradigm of organisation of train traffic, it can be argued that the technical means of ensuring movement of trains are partially separated from each other and for the most part are not directly related [5]. Thus, the RARC system is almost completely separated from catenary facilities, partly separated from the objects of the superstructure of the track and artificial structures, partly separated from the state of the rolling stock. For example, the event of a track geometry defect and track width violation (track buckle), while the integrity of the rail is maintained, will not affect the RARC system in any way: a permissive indication will be lit at the traffic light blocking the entrance to the track section with a track defect. Moreover, it is impossible to give a prohibiting indication in the RARC system even artificially in this case without violating the rules for operating automation equipment.

Thus, the reasoning about safety of devices and systems of the RARC becomes not entirely consistent in terms of safety of the transportation process in the absence of consideration for safety



Pic. 1. Conceptual organisational structure of train traffic control [performed by the authors].

of the entire infrastructure facilities and the rolling stock. Many years of experience in the operation and development of RARC systems, as well as an analysis of the scientific and technical literature in this area have shown that, in fact, when considering the safety of RARC devices, one can speak of a certain property of a *limited safety*. Considered fully is internal safety and external safety is considered partially.

Definition 1. *Internal safety means a property of impossibility of the influence of malfunctions and errors in calculations on the execution of algorithms in terms of excluding the transition to dangerous states.*

Definition 2. *External partial safety means a property of possibility of parrying only those external destabilising factors that can be fixed by the automation object.*

The implementation of the RARC devices and systems in such a paradigm has made it possible to build safe control systems but has not allowed achieving absolute safety of train traffic, since the states of infrastructure and rolling stock are only partially taken into account in the controlling systems.

The technical object of the railway infrastructure and rolling stock is characterised by the following sets:

$$<X, Z, A, P, S>, \quad (1)$$

where X is set of inputs;

Z – set of outputs;

A – set of implemented algorithms;

P – set of operating parameters;

S – set of states.

To build a completely safe automation system, it is required to solve the problem of obtaining information about the state of an object involved in the transportation process (or providing it) with a given validity $D \in [0,1]$. In practice, this value should be normalised and standardised. A safe control system should be implemented through the use of technical means of built-in testing and functional diagnostics. Testing and functional diagnostic procedures should be carried out automatically and at pre-selected and scientifically substantiated control points and with pre-established and substantiated periods, implementing a specific monitoring strategy [21–23].

When solving the problem of diagnosing and monitoring, some subset of each of the above sets $X^* \subseteq X$, $Z^* \subseteq Z$, $A^* \subseteq A$, $P^* \subseteq P$, $S^* \subseteq S$ can be controlled. This allows getting a certain subset of correct and incorrect states of each of the checked objects. For each of these objects, a set of correct states S_g and a set of incorrect states S_f are allocated: S_f: $S = S_g \cup S_f$. Within the set S_f, it is possible to single out those S_R states that are associated with a specific given risk for train traffic control: $S_R \subset S_f$.

Statement. *All S_R states for each technical object must be recorded and transmitted to a single safe decision device to develop the proper reactions for switching to protective states for train traffic control and information messages for traffic participants and operation of objects under diagnostics.*

Thus, separate diagnostic and monitoring systems of infrastructure objects, rolling stock and RARC should generate signals about reaching their S_R states with a given validity D. They either directly (which is technically more difficult) or through a secure platform for analytics and decision making should transmit signals for the transportation process control system to go to the set protective states. Pic. 1 shows the structure of the interaction of railway transport objects.

2. Basic rules for the synthesis of a safe train traffic control system

The safety of the transportation process significantly depends on the safety of functioning of the RARC devices and systems [1–3]. In fact, RARC devices and systems play a role of regulatory technical means for transmitting reliable data to a driver. The traditional way of transmission is the use of traffic lights. Each colour signal indicates a specific action for a driver. The number of such signals is very limited, which also limits the gradations for actions.

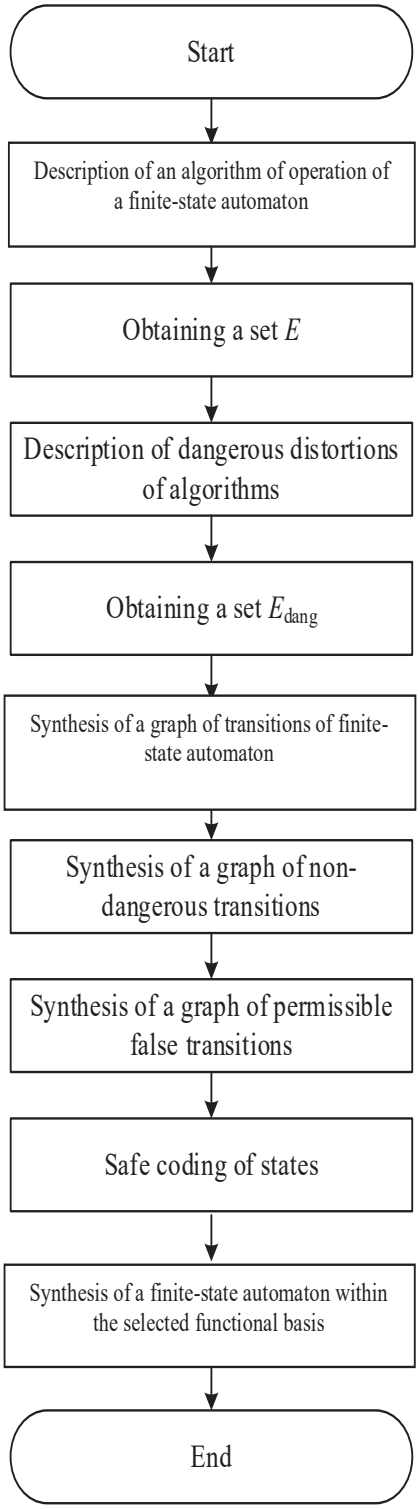
In the process of functioning, any RARC device or the entire system can switch between a finite set of predetermined states. In this case, the model of an abstract finite-state automaton (finite-state machine) Z can be used as a mathematical model of RARC objects:

$$Z = <X, S, \Omega, s_0, \varphi, \psi>, \quad (2)$$

where X is a set of input states corresponding to Boolean vectors generated at the inputs of the object $x_1, x_2, \ldots, x_q$;

S – a set of finite-state machine states corresponding to Boolean vectors of internal variables $y_1, y_2, \ldots, y_r$;

Ω – a set of output states of the finite-state automaton corresponding to Boolean vectors formed at the outputs of the object of internal variables $z_1, z_2, \ldots, z_p$;



Pic. 2. A simplified algorithm for synthesising a safe finite-state automaton [performed by the authors].

s_0 – initial state ($s_0 \in S$);

φ: $X \times S \rightarrow S$ – transition function that maps the set $X \times S$ to the set S;

ψ: $X \times S \rightarrow \Omega$ – transition function that maps the set $X \times S$ to the set Ω.

When synthesising secure finite-state automaton, one can use the algebra of regular events [24]. In this case, the finite-state machine is considered as a converter of input words into output ones. An event E for a finite-state automaton is any set of input words. To describe the algorithm of the finite-state automaton, it is required to find an event that includes all allowed words: such words that are represented in the automaton. This is done using three operations: disjunction, product, and iteration of sets of events. If this is done using the three indicated operations, then the event E is regular. It is known [25] that any finite-state automaton is a regular event and vice versa, any regular event can be represented in a finite-state automaton.

Events in a finite-state automaton can implement correct transitions and incorrect ones, including dangerous ones that violate safety of the technological process implemented by the described object. The set of dangerous events will be denoted by E_{dang}.

Failures in the device, which is described by the finite-state automaton under consideration, lead to false transitions of the finite-state automaton: instead of the state S_i, the finite-state automaton goes into the state S_z ($S_i \rightarrow S_z$). In fact, the original finite-state automaton is transformed, and regular events in it are already described by the expression [24]:

$$E^*_k = E_i E_{z(k)}, \quad (3)$$

where E_i – all events (a set of words) that transfer the original finite-state automaton from the initial state to the state S_i;

$E_{z(k)}$ – all events that transfer the finite-state automaton from state S_i to states representing events E_k, where k is the number of a dangerous event.

Definition 3. *A finite-state automaton is safe if it excludes all false transitions associated with implementation of dangerous events, the probability of which must be taken into account.*

In [10; 24], the following is defined.

Definition 4. *A false transition of a finite-state automaton is called dangerous if, when it occurs, for at least one k, the following condition is satisfied:*

$$E^*_k \cap E_{dang} \neq \varnothing. \quad (4)$$

Definition 5. *A false transition of an automaton is called protective if, when it occurs, for all k, the following condition is satisfied:*

$$E^*_k \cap E_{dang} = \varnothing. \quad (5)$$

The introduced concept of a dangerous failure formed the basis of [24], where the theorem on the absence of dangerous failures in a finite-state automaton was proved.

Theorem 1. *There are no dangerous failures in the operation of a finite-state automaton if and only if for all false transitions $S_i \rightarrow S_z$ and for all false events k the following condition is satisfied:*

$$E_{S_i \rightarrow S_z} E_{z(k)} \cap E_{dang} = \varnothing, \quad (6)$$

where $E_{S_i \rightarrow S_z}$ are events corresponding to false transitions of the finite-state automaton from the state S_i to the state S_z.

The conditions introduced based on regular expressions allowed the authors to formulate algorithms for the synthesis of automata that exclude their transitions to dangerous states in case of any failures, the probability of which must be considered. To exclude dangerous failures in a automaton, it is sufficient to prohibit all dangerous false transitions.

A simplified algorithm for synthesising a safe finite-state automaton is shown in Pic. 2. In it, the final stage supposes safe coding of the states of the finite-state automaton considering the graph of non-dangerous false transitions.

It should be emphasised that in this case, the finite-state automaton describing the operation of a certain device or a certain RARC system will be safe from the following positions:

1) From the standpoint of internal safety: failures and malfunctions will not lead to the transition to any of the risk states for train traffic S_R.

2) From the standpoint of external safety: external destabilising factors will not lead to the transition to any of the states of risk for train traffic S_R.

However, in this case, the finite-state automaton will in no way consider S_R states of those infrastructure and rolling stock objects that do not directly interact with this finite-state automaton. It's just not defined in the E_{dang} event sets. Thus, the finite-state automaton will be safe, but it will only be limitedly safe and will not be able to signal the transition to the protective state during one of the transitions to S_R states of those infrastructure and rolling stock objects that do not directly interact with this finite automation occurs.

Definition 6. *A fully safe finite-state automaton of a train traffic control device or system will be a finite-state machine that is capable of transitioning to a set of protective states upon the occurrence of all given transitions to states with a specified level of risk of violation of train traffic safety for all infrastructure and rolling stock objects.*

One more variable $\theta \in \{0,1\}$ should be added to the set of input actions of the finite-state automaton. The variable θ takes the value 1 if the safe solver detects the transition of one of the monitored objects, the state of which is associated with ensuring safety of the transportation process, to one of S_R states. In other cases, it is equal to 0.

In the described logic of the safe solver operation, the concept of a strict ban on movement is implemented: a virtual obstruction signal (red traffic light). In this case, the transition is made to the single safe state already available for the finite-state automaton: $s_{\text{safety}} \in S$. The exit from this state is carried out with participation of a human.

However, during practical implementation, not a single signal θ, but a code vector $<\theta_1\ \theta_2\ \ldots\ \theta_t>$ corresponding to one of the protected states with a given gradation, can be introduced into the finite-state automaton. For example, if it is required to transmit information about a decrease in speed of passage through the signalling system, then it is possible to adopt an analogue of three colours: «green», «yellow» and «red» ones. This will require two variables to encode. If it is required to transmit a gradation of speeds with a step of 10 km/h in the range from 0 to 300 km/h, then it will be necessary to transmit 30 protective states and, accordingly, five binary variables must be used.

In the general case, an initial introduction of $t = \lceil \log_2 N \rceil$ (N is the number of protective states) variables for coding will be required. In addition, the conditions for exiting them without human intervention should also be specified. This task requires special study in the future.

Hence follows such a conclusion.

Theorem 2. *The finite-state automaton will be safe if:*

$$\forall S_{R_j} : E_{dang} \supset E^j_{dang}, j \in \{1,2,\ldots,n\}, \quad (7)$$

where n – number of diagnostic and monitoring subsystems.

Following (7) and implementing diagnostic and monitoring systems in accordance with the requirements for safe systems, normalising the level of validity of recorded diagnostic events, we can proceed to implementation of transportation process control systems of a new, actually higher, level of safety.

CONCLUSION

Despite the tremendous progress in development of engineering and technology over the past century, control systems in many areas of industry and transport are not implemented in such a way that it can be said that they are completely safe. The limited safety property of control systems is due to various factors. On the one hand, it is due to the human factor, which does not exclude the possibility of introducing errors into the design documentation and errors during the installation of devices and testing during commissioning. On the other hand, it is due to the lack of an integrated approach when considering the process of synthesis of the control system for individual devices or subsystems without full consideration of all interacting objects. This is fully reflected in the example of RARC systems. They are limitedly safe, since they do not transmit to the driver data on permissible speeds for movement considering the state of infrastructure facilities. In this article, the emphasis is on solving this problem and it is proposed to synthesise train traffic control systems with close integration with the means of automatic monitoring of railway infrastructure facilities.

Solving the problem of synthesising a completely safe train traffic control system directly is currently impossible. This is due to the existing set of regulatory documentation, which excludes the use of diagnostic data from external systems directly for controlling. It is required to solve the main subtask: to create a methodology for the synthesis of technical diagnostics and monitoring systems that can be certified at any of the levels of functional safety [26]. Since the task is relatively new, it is advisable to move along the path of evolution of existing, not certified regarding functional safety, external diagnostic and monitoring systems, to systems of a new level of safety (DMS 0 (modern implementation, not certified regarding functional safety) → DMS 1 → ... → DMS 4, according to the number of safety integrity levels SIL 1 ... SIL 4). This will also require solving the following tasks:

• Identification of criteria of a dangerous failure of diagnostic and monitoring systems.

• Identification of functional requirements for the architecture, components and for the monitoring systems themselves.

• Application of the risk-focused approach to identify and rank diagnostic events according to the degree of impact on train traffic safety.

• Normalisation of validity of recorded events.

• Identification of ways to safely link solvers with control systems (these issues, for example, for RARC devices were considered earlier in [21–23]).

Following the principles of integrated accounting of parameters of railway infrastructure facilities and rolling stock, it is possible to achieve a significant increase (and even a jump!) in the quality of train traffic safety.

REFERENCES

1. Gavzov, D. V., Sapozhnikov, V. V., Sapozhnikov, Vl. V. Methods for ensuring safety of discrete systems [*Metody obespecheniya bezopasnosti diskretnykh sistem*]. *Avtomatika i telemekhanika*, 1994, Iss. 8, pp. 3−50. [Electronic resource]: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=at&paperid=3949&option_lang=rus. Last accessed 26.02.2022.

2. Sapozhnikov, V. V., Sapozhnikov, Vl. V., Khristov, Kh. A., Gavzov, D. V. Methods for constructing safe microelectronic systems for railway automatics: Monograph [*Metody postroeniya bezopasnykh mikroelektronnykh sistem zheleznodorozhnoi avtomatiki: Monografiya*]. Ed. by Vl. V. Sapozhnikov. Moscow, Transport publ., 1995, 272 p. ISBN 5-277-01690-2.

3. Lisenkov, V. M. Statistical theory of train traffic safety [*Statisticheskaya teoriya bezopasnosti dvizheniya poezdov*]. Moscow, VINITI RAS publ., 1999, 331 p. ISBN 5-900242-29-3.

4. Bestemyanov, P. F. Methods for ensuring the safety of hardware of microprocessor-based train control systems. *Elektrotekhnika*, 2020, Iss. 9, pp. 2−8. [Electronic resource]: https://elibrary.ru/item.asp?id=44000551 [access restricted for subscribers].

5. Railway Signalling and Interlocking: International Compendium. 3ed ed. Eds.: Dr. G. Theeg, Dr. S. Vlasenko. Germany, PMC Media House GmbH, 2020, 560 p. ISBN 978-3-96245-169-1.

6. Joung, Eui-jin; Lee, Changmu; Lee, Hanmin; Kim, Gil-dong. Software Safety Criteria and Application Procedure for the Safety Critical Railway System. 2009 Transmission & Distribution Conference & Exposition: Asia and Pacific, 26−30 October 2009, Seoul, Korea (South), pp. 1−4. DOI: 10.1109/TD-ASIA.2009.5356897 [access restricted for subscribers].

7. Markov, D. S., Nasedkin, O. A., Manakov, A. D., Vasilenko, M. N., Kotenko, A. G., Belozerov, V. L. Method for Assessing Probabilistic Reliability Estimation and Safety of Railway Automation Systems Redundant Structures. Proceedings of 18th IEEE East-West Design & Test Symposium (EWDTS'2020), Varna, Bulgaria, September 4–7, 2020, pp. 356−361. DOI: 10.1109/EWDTS50664.2020.9224925 [access restricted for subscribers].

8. Huang, Lujiang. The Past, Present and Future of Railway Interlocking System. IEEE 5th International Conference on Intelligent Transportation Engineering (ICITE), 11–13 September 2020, pp. 170–174. DOI: 10.1109/ICITE50838.2020.9231438 [access restricted for subscribers].

9. Qian, Jinlong; Guo, Wei; Zhang, Hongtao; Li, Xiaona. Research on Automatic Test Method of Computer-Based Interlocking System. International Conference on Communications, Information System and Computer Engineering (CISCE), 3–5 July 2020, Kuala Lumpur, Malaysia, pp. 298–302. DOI: 10.1109/CISCE50729.2020.00066 [access restricted for subscribers].

10. Sapozhnikov, Vl. V. Synthesis of train traffic control systems at railway stations with the exception of dangerous failures [*Sintez sistem upravleniya dvizheniem poezdov na zheleznodorozhnykh stantsiyakh s isklyucheniem opasnykh otkazov*]. Moscow, Nauka publ., 2021, 229 p. ISBN 978-5-02-040877-7.

11. Efanov, D. V. Functional control and monitoring of railway automation and telemechanics devices [*Funktsionalniy control i monitoring ustroistv zheleznodorozhnoi avtomatiki i telemekhaniki*]. St. Petersburg, PGUPS publ., 2016, 171 p. ISBN 978-5-7641-0933-6.

12. Fritz, C. Intelligent Point Machines. Signal+Draht, 2018 (110), Iss. 12, pp. 12–16. [Electronic resource]: https://eurailpress-archiv.de/SingleView.aspx?show=469469&lng=en [access restricted for subscribers].

13. Heidmann, L. Smart Point Machines: Paving the Way for Predictive Maintenance. Signal+Draht, 2018, Iss. 9, pp. 70–75. [Electronic resource]: https://eurailpress-archiv.de/SingleView.aspx?show=325895&lng=en [access restricted for subscribers].

14. Efanov, D., Lykov, A., Osadchy, G. Testing of relay-contact circuits of railway signalling and interlocking. Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS'2017), Novi Sad, Serbia, September 29–October 2, 2017, pp. 242–248. DOI: 10.1109/EWDTS.2017.8110095 [access restricted for subscribers].

15. Wernet, M., Brunokowski, M., Witt, P., Meiwald, T. Digital Tools for Relay Interlocking Diagnostics and Condition Assessment. Signal+Draht, 2019 (111), Iss. 11, pp. 39–45. [Electronic resource]: https://eurailpressarchiv.de/SingleView.aspx?show=1136153&lng=en [access restricted for subscribers].

16. Bestemyanov, P. F. Methods for ensuring safety and reliability of microprocessor devices of railway automation and telemechanics [*Metody obespecheniya bezopasnosti i nadezhnosti mikroprotsessornykh ustroistv zheleznodorozhnoi avtomatiki i telemekhaniki*]. *Proceedings of the international symposium «Reliability and quality»*, 2007, Vol. 2, pp. 273–274. [Electronic resource]: https://elibrary.ru/item.asp?id=15619177. Last accessed 26.02.2022.

17. Bochkov, K. A., Sivko, B. V. Selection and determination of the safety function in verification of microprocessor systems of railway automation and telemechanics [*Vybor i opredelenie funktsii bezopasnosti pri verifikatsii mikroprotsessornykh sistem zheleznodorozhnoi avtomatiki i telemekhaniki*]. *Nadezhnost*, 2014, Iss. 2 (49), pp. 101–108.

18. Markov, D. S., Nasedkin, O. A. Tool for assessing the probabilistic indicators of reliability and safety of railway automation systems [*Instrumentalnoe sredstvo otsenki veroyatnostnykh pokazatelei nadezhnosti i bezopasnosti sistem zheleznodorozhnoi avtomatiki*]. *Izvestiya Peterburgskogo universiteta putei soobshcheniya*, 2020, Vol. 17, Iss. 1, pp. 23–34. DOI: 10.20295/1815-588X-2020-1-23-34.

19. Kovkin, A. N. Relay-semiconductor circuit switching in safe interface units based on electromagnetic relays. *Transport Urala*, 2020, Iss. 2, pp. 31–35. DOI: 10.20291/1815-9400-2020-2-31-35.

20. Bochkov, K. A., Komnatny, D. V. Ensuring functional and information safety of microelectronic traffic control systems, taking into account new types of threats. *Vestnik Belorusskogo gosudarstvennogo universiteta transporta: Nauka i transport*, 2020, Iss. 2 (41), pp. 4–8. [Electronic resource]: https://elibrary.ru/item.asp?id=44780175. Last accessed 26.02.2022.

21. Efanov, D. V., Osadchy, G. V., Aganov, I. A. Linking control systems with technical means of diagnosis and monitoring the infrastructure facilities. *Avtomatika, svyaz, informatika*, 2021, Iss. 6, pp. 25–29. DOI: 10.34649/AT.2021.6.6.004 [access restricted for subscribers].

22. Efanov, D. V., Osadchii, G. V., Aganov, I. A. Barrier function of the monitoring systems in connection with train movement management systems. *Transport Rossiiskoi Federatsii*, 2021, Iss. 3, pp. 51–56. [Electronic resource]: https://www.elibrary.ru/item.asp?id=46683409 [access restricted for subscribers].

23. Efanov, D., Osadchy, G., Aganov, I. Fundamentals of Implementation of Safety Movement of Trains under Integration of Control Systems with Hardware for Railway Infrastructure Facilities Monitoring. Proceedings of 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2021), Cracow, Poland, September 22–25, 2021, Vol. 1, pp. 391–396. DOI: 10.1109/IDAACS53288.2021.9660985 [access restricted for subscribers].

24. Sapozhnikov, V. V., Sapozhnikov, Vl. V. On the synthesis of finite automata with the exclusion of dangerous failures [*O sinteze konechnykh avtomatov s isklyucheniem opasnykh otkazov*]. *Avtomatika i telemekhanika*, 1972, Iss. 8, pp. 93–99. [Electronic resource]: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=at&paperid=8917&option_lang=rus. Last accessed 26.02.2022.

25. Shannon, C. E., McCarthy, J. Automata Studies. In: *Annals of Mathematics Studies,* Vol. 34. Princeton, New Jersey, Prinston University Press, 1956, 285 p. ISBN 9780691079165.

26. Smith, D. J., Simpson, K. G. L. Functional safety: A Straightforward Guide to IEC 61508 and Related Standards. 2nd ed., Simpson, Elsevier, Butterworth-Heinemann, Oxford, UK and Burlington, MA, 2004, 263 p. ISBN 978-0750652704.

Information about the authors:

Efanov, Dmitry V., *D.Sc. (Eng), Associate Professor, IEEE member, Professor at the Department of Railway Automation, Remote Control and Communications of Russian University of Transport, Deputy General Director for Research and Scientific Work of LLC Research and Design Institute for Transport and Construction Safety, Professor at Higher School of Transport of the Institute of Mechanical Engineering, Materials and Transport of Peter the Great St. Petersburg Polytechnic University, Moscow / St. Petersburg, Russia, TrES-4b@yandex.ru.*

Khoroshev, Valery V., *Ph.D. (Eng), Senior Lecturer at the Department of Railway Automation, Remote Control and Communications of Russian University of Transport (MIIT), Moscow, Russia, hvv91@icloud.com.*

Osadchy, German V., *Ph.D. (Eng), Deputy General Director – Chief Engineer of LLC STC Complex Monitoring Systems, Senior Lecturer at the Department of Railway Automation and Remote Control of Emperor Alexander I St. Petersburg State Transport University, St. Petersburg, Russia, osgerman@mail.ru.*

Article received 09.02.2022, approved 27.05.2022, accepted 20.06.2022.