Fundamentals of Implementation of Safety Movement of Trains under Integration of Control Systems with Hardware for Railway Infrastructure Facilities Monitoring

Dmitry Efanov [1,2], German Osadchy [2], Igor Aganov [2]
[1] Peter the Great St. Petersburg Polytechnic University,
29 Polytechnicheskaya str., St. Petersburg, Russian Federation, TrES-4b@yandex.ru, https://www.spbstu.ru/
[2] Scientific and Technical Center “Integrated Monitoring Systems” LLC,
4-K Fuchika str., St. Petersburg, Russian Federation, osgerman@mail.ru, https://ntc-ksm.ru/

Abstract—The authors show that safety systems of railway automation and remote control can’t ensure safety when reaching the limit states of railway infrastructure objects with which they do not directly interact. This is the cause of the train traffic safety incident. Conditions for the safety train control system architecture are formulated. The necessity of integration of hardware for diagnostics and monitoring with train control systems in railway transport for the implementation of the barrier function is noted. It is proposed to output the alarm signal through the hardware interfaces to the train control systems for the speed limits data communication to the train movements controller and the locomotive driver when passing the object under test (up to a complete stop).

Keywords—railway automation and remote control systems, systems of diagnostics and monitoring, railway infrastructure objects, survivability index of the object being diagnosed, integration of control system with monitoring system, train traffic safety, barrier functions of monitoring system.

I. Introduction

Technical diagnostics and monitoring (TDM) systems are widely used in the field of automation of processes control and production, which fully applies to the infrastructure of the railway complex. In each of the facilities (artificial structures, tracks, power supply, automation and remote control, etc.), to maintain high failure robustness and safety of railway infrastructure objects, both manual and automated methods of technical diagnostics and monitoring are used. However, all these methods are designed to automatically obtain diagnostic information for its subsequent analysis by expert technologists. Therefore, TDM systems currently implement only one key function – automatic data acquisition & storage to automate maintenance procedures.

The development of monitoring technologies, the improvement of the hardware components for diagnostics equipment, and methods of recognition and classification of states, forecasting, and complex data analytics contribute to the increase in the number of functions implemented by TDM systems. A large amount of diagnostic information only leads to an increase in the workload on the expert technologist and does not contribute to a quantum leap in improving traffic safety. Today, the scientific community pays attention to this problem. It is high time to increase the importance of TDM systems (not only the railway automatics hardware are discussed here, but attention is paid to the monitoring systems of all the infrastructure facilities), linking them directly with the systems of railway automation and remote control (RARC), as the final links in the entire structure of devices ensuring the safety of train traffic, and their implementation of the barrier function. Please note that with the current state of the operating TDM systems and current regulatory framework, this is not so simple, but it does not look unrealizable either. Let us pay attention to the peculiarities of the implementation of RARC facilities, as well as the possibility of their integration with hardware for diagnostics and monitoring.

II. Railway Automation and Remote Control Systems and their Safety

All specialists in the RARC have known since their student days that RARC systems ensure the safety movement of trains with the required traffic capacity [1, 2]. The architecture of RARC systems is built in such a way as to exclude all possible internal dangerous failures [3].

The theoretical foundations for the synthesis of safety RARC systems, for example, in Russia, were laid in the works of professors Sapozhnikovs [4, 5], where RARC systems are represented as single-cycle and multi-cycle machines (combinational circuits and finite-state machines, FSM). A dangerous failure is defined as a type II error in the operation of circuits – the appearance at the output (or outputs) of the circuit of a false signal of logical 1 (“control signal”), based on which the protection of the circuit from dangerous failures is determined and proposals are formulated for choosing the best structure of safety circuits. It is shown that there are different implementations for the same scheme, but they are different in terms of protection. The introduced concept of a dangerous failure allows proving the theorem on the absence of dangerous failures in a FSM.

Theorem 1. *There are no dangerous failures in the FSM if and only if for all false transitions $S_i \rightarrow S_f$ and for all false events k the condition is satisfied:*

$$E_{S_i \rightarrow S_f} E_{f(k)} \cap E_{dan_k} = \varnothing, \quad (1)$$

where $E_{S_i \rightarrow S_f}$ is a set of words corresponding to false transitions of the FSM from the state S_i to the state S_f; $E_{f(k)}$ is a set of words that transfer the FSM from the state S_f to the states representing false events from the set E_k; E_{dan_k} is a set of words that transfer the FSM into dangerous states.

The conditions introduced based on regular expressions made it possible to formulate algorithms for the synthesis of FSMs that exclude their transitions to dangerous states in case of any failures, the probability of which should be considered. To exclude dangerous failures in the FSM, it is sufficient to prohibit all dangerous false transitions.

Half a century later, the principles of implementation of RARC systems have not changed, and the concept of RARC safety is interpreted in the same and earlier formulated paradigm. RARC systems are implemented according to technologies that imply the use of highly reliable components, elements with asymmetric failure characteristics, self-checking circuits, principles of self-control and self-diagnosis, coding methods, redundancy, and diversification, etc. [6]. RARC systems are certified for compliance with the safety integrity level SIL 4 [7].

The *safety of the transportation process* in railway transport is understood as the ability of the transport system not to compromise the safety of the transported cargo, hardware, environmental objects, to the safety of the health and life of passengers, technical personnel, and the population in the zone of influence of the transportation process.

Here are a few counterexamples showing that although the RARC systems are implemented safely (internal failures do not lead to the initiation of dangerous situations in the movement of trains, external failures do not affect the ability of RARC to perform safety algorithms), but they do not exclude dangerous situations in the transportation process. For example, the widening of the track due to external destabilizing factors, the lowering of the rail as a result of the partial collapse of the ballast section, dangerous buckles of rails, etc. – these are those dangerous conditions of the track bed structure that will not be fixed by means of RARC: if there is an empty track for a movement, the track circuit will continue to work, and a permissive indication will light up at the signal protecting the section of the track. Another example is the collapse of the overhead structures and its falling into the zone of structure clearance conflict also will not lead to the automatic enabling the restrictive indication at the traffic light protecting the site (moreover, such an indication cannot be given in the RARC system manually when such a defect is detected, except by violating principles of their operation). The RARC system is built in such a way that it is safe "in itself" but is not protected from failures of external and interacting with the rolling stock objects that do not directly trigger the automation devices (implementation of the "barrier function"). This feature of the interaction of railway infrastructure facilities is a consequence of a number of accidents and disasters, among which we can mention the recent collapse of the railway bridge across the Kola River (1436 km of the Oktyabrskaya railway, 1 June 2020) [8]. Here, the RARC system did not give an alarm signal to the locomotive, and only the attentiveness of the locomotive driver allowed to avoid a disaster.

The above examples show that the RARC systems realize functions of safety train passage with restrictions. These restrictions are associated with the principles of the implementation of automation equipment: they are simply not designed to record the technical condition of railway infrastructure facilities. RARC systems provide and control the spatial separation of trains, the automation equipment themselves, and partly the condition of the railway track.

Let us go back to expression (1). If we consider it in relation to the railway transport system, then the set E_{dan_k} in it does not include any of words corresponding to false transitions in dangerous states of railway infrastructure facilities, and formula (1) itself does not provide the conditions for the transition to the set of safety states of protected states of the transport systems.

Theorem 2. *Dangerous failures in the operation of railway infrastructure facilities will not appear when any of their transition to a set E_{dan_j} of dangerous states will lead to a transition to a protected state of the train control system:*

$$E_{S_i \rightarrow S_f} E_{f(k)} \cap E_{dan_j} = E_{saf_j}. \quad (2)$$

In (2) E_{saf_j} is a set of words that transfer the FSM into safety states.

Here, the protected state can be interpreted as a decrease in the speed of passing to a certain value, up to a complete stop (analog of a signal with different speed gradations). For example, due to the failure the bridge structures experience an abnormal load automatically recorded by technical diagnostics hardware, at which the speed of movement should be limited, but not the movement itself. Then this information can be "reported" to the train movements controller and the locomotive driver automatically. If the bridge collapsed, then an immediate signal should be received to stop traffic (analog of a restrictive indication of a traffic light signal). These are two examples of protected states of the transport system. It should be emphasized that this protected state should be present precisely in the RARC system since it is responsible for generating a control signal for movement.

III. Concept for the Implementation of a Safety Train Control System

In Fig. 1, conventionally in the form of FSM subgraphs, a safety train control system is presented. For the RARC system, a fragment of the implementation of one of the control functions of floor-standing technological objects was selected. For TDM systems, two states are shown: 1 – parameters are OK, 2 – dangerous state of the object being diagnosed.

In the general case, q TDM systems can be installed at the facility, each of which shall generate an "alarm" $y_j = 1,\ j \in \{i_1, i_2, ..., i_{q-1}, i_q\}$. These are TDM systems for track bed structure objects, overhead line suspension, bridges, the RARC equipment, etc., "high-level prototypes" of which are already used in railways [9 – 16]. Each of such TDM systems measures a number of parameters $\tilde{X}^{i_j} = \tilde{x}_1^{i_j}\tilde{x}_2^{i_j}\cdot\ldots\cdot\tilde{x}_{n_{i_j}-1}^{i_j}\tilde{x}_{n_{i_j}}^{i_j},\ j \in \{i_1, i_2, ..., i_{q-1}, i_q\}$, generates information messages to its users, and also calculates a certain indicator (let us call it as survivability index of the object under diagnosis $I_L \in [0;1]$) and determines the alarm signal value $y_j = 1$, $j \in \{i_1, i_2, ..., i_{q-1}, i_q\}$.

The condition for the transition from any functional state S_f of the train control system to the protected state S_Θ of the train control system can be written as:

$$S_f \to S_\Theta:\ y_{i_1} \vee y_{i_2} \vee \ldots \vee y_{i_{q-1}} \vee y_{i_q} = 1. \quad (3)$$

The functional state S_f here means any of the foreseen states of the RARC system (healthy, operative, or inoperative protective state [6]), are considered in its implementation. Strictly speaking, the signals y_j, $j \in \{i_1, i_2, ..., i_{q-1}, i_q\}$, from various TDM systems should be "included" into the signal groups of the RARC system during its improvement. The conditions for the transition of the RARC system from one state to another state are determined based on the values of the input actions of the system $\tilde{X}^\alpha = \tilde{x}_1^\alpha\tilde{x}_2^\alpha\cdot\ldots\cdot\tilde{x}_{n_\alpha-1}^\alpha\tilde{x}_{n_\alpha}^\alpha$ and the generated vector of alarm signals $\tilde{Y}^\alpha = y_{i_1}y_{i_2}\cdot\ldots\cdot y_{i_{q-1}}y_{i_q}$. In other words, the transitions are carried out when the inputs $\tilde{X}^\alpha\tilde{Y}^\alpha = \left(\tilde{x}_1^\alpha\tilde{x}_2^\alpha\cdot\ldots\cdot\tilde{x}_{n_\alpha-1}^\alpha\tilde{x}_{n_\alpha}^\alpha\right)\left(y_{i_1}y_{i_2}\cdot\ldots\cdot y_{i_{q-1}}y_{i_q}\right)$ are affected, causing the output values of the system $\tilde{Z} = \tilde{z}_1\tilde{z}_2\cdot\ldots\cdot\tilde{z}_{p-1}\tilde{z}_p,$, where p is the set of outputs of the RARC systems. Also, one alarm signal $y = y_{i_1} \vee y_{i_2} \vee \ldots \vee y_{i_{q-1}} \vee y_{i_q}$, generated by a software tool (or a subsystem) with high operational reliability can be used to identify the dangerous state of the object under diagnosis and monitoring with a given reliability $D \in [0;1]$: $D > D_{\lim}$, $D_{\lim}$ – some specified limit of confidence value close to 1. In practice, this value should be normalized and standardized.

From the above considerations, it follows that the RARC facilities are the final links, which must not only ensure their safe functioning in the direct "contact" with the infrastructure facilities but also implement a barrier function when fixing the failures of the objects of the entire railway infrastructure. In addition, the precise following this paradigm in RARC facilities implementation will improve the safety of train traffic and reduce the risks of failure of railway infrastructure facilities.

Since the RARC systems in this paradigm are not implemented at present, their "build-up" can be used in the following sense:

1. Using the risk-based approach, the set of the most probable hazardous states of railway infrastructure facilities is determined.
2. Systems of automatic technical diagnostics and monitoring of parameters are being improved.
3. For each of the dangerous states, control measuring points, diagnostic periods and conditions for the occurrence of events are determined using mathematical modeling methods and technical diagnostics.
4. A subsystem for dangerous events recording is being implemented.
5. A subsystem for integrating with RARC objects is being implemented. Thus, item 5 implies the presence of feedback for considering the monitoring results in the process of regulating train traffic (Fig. 2). The co-authors of this article have repeatedly spoken about the need for such a link in their speeches, reports, and articles.

Currently, there are no technical solutions that would allow linking the monitoring system with the train control system. First of all, this is not determined by regulatory documents, and the monitoring system does not impose requirements for compliance with any of the safety integrity levels. Thus, such integration is possible, but with a highly reliable and safe implementation of the monitoring system. This is definitely a technically difficult task that cannot be done instantly.

The use of technical monitoring hardware allows, in fact, to manage risks caused by failures of the object being diagnosed and from untimely maintenance and repairs (M&R). Here it is necessary to note the function of the possibility of managing the M&R processes, for example, justified and timely professional heating of railway overhead line suspension elements when detecting the conditions of ice formation using monitoring. In fact, the possibility of energy management and energy efficiency improvement of infrastructure facilities is being realized [17].

In the first case, it becomes possible to influence the value of the failure rate λ_F, which, given the constant values of losses Π_F from the failure effect to the technological process helps to reduce the risk due to failure:

$$R_F = \Pi_F \lambda_F. \quad (4)$$

In the second case, it becomes possible to influence the value of the intensity of M&R λ_M, which, with constant values of losses Π_M from a decrease the speed of the technological process, helps to reduce the risk from maintenance:

$$R_M = \Pi_M \lambda_M. \quad (5)$$

A decrease in λ_F value is possible due to early diagnosis of developing malfunctions and detection of catastrophic (limit, pre-failure and other synonyms used in various fields of technology) condition. A decrease in Π_M value is possible due to the formation of the predicted service times of the device and an increase in the service life of the object under diagnosis. Thus, the operation of TDM systems is aimed at minimizing the risk of losses from the operation of the railway infrastructure:

$$\begin{cases} R_F\left(\vec{\lambda}_F\right) \to \min\limits_{\vec{\lambda}_F \in \lambda_F}; \\ R_M\left(\vec{\lambda}_M\right) \to \min\limits_{\vec{\lambda}_M \in \lambda_M}. \end{cases} \quad (6)$$

Reducing risks (6) also helps to reduce dangerous failures in the operation of infrastructure facilities of the railway complex.

Fig. 2 shows the elements of hardware and software controls in rectangular blocks, and processes, messages, actions in blocks with rounded edges. The implementation of TDM systems shall make it possible to move from the automation of measurement procedures to the formation of road maps for the maintenance of facilities under diagnosis, risk management from failures and untimely M&R, as well as to the generation of an alarm signal for the implementation of the barrier function.

Data storage and data processing systems, as well as the organization of ETL (from English “Extract, Transform, Load”) processes for such a system, require careful engineering study at the design and development stage. Monitoring systems shall have universal structures that ensure their modular and easily integrated implementation, which contributes to an increase in the technical immunity of the objects being diagnosed. The integration of TDM systems with train control systems significantly increases the resistance of the latter to manifestations of external destabilizing factors and makes it possible to exclude potential cases of reduced train traffic safety.

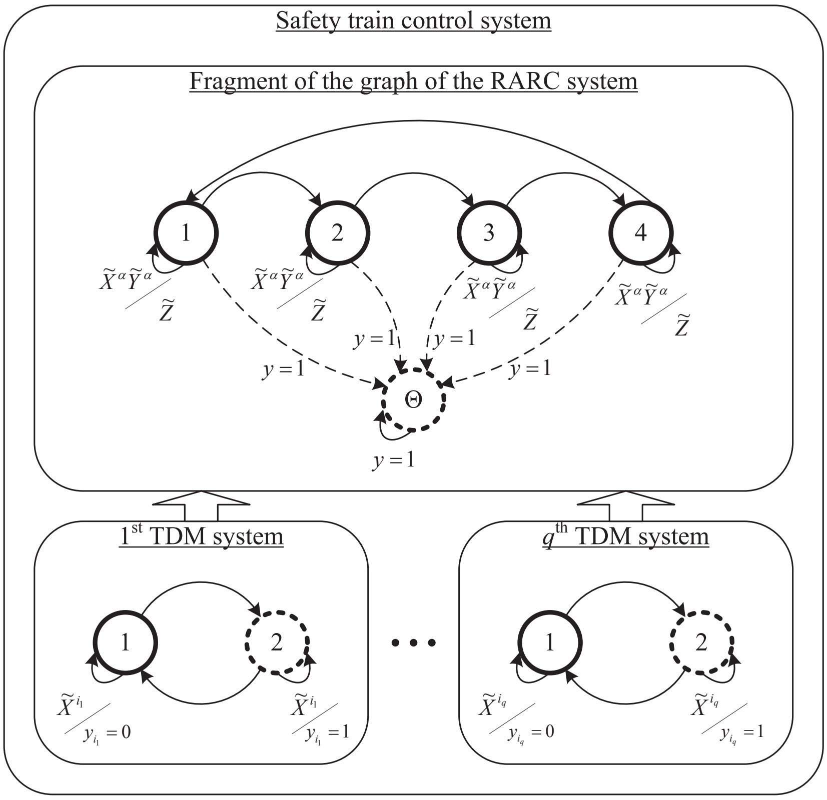
Safety train control system
Fragment of the graph of the RARC system
1
2
3
4
$\tilde{X}^{\alpha}\tilde{Y}^{\alpha} / \tilde{Z}$
$y=1$
Θ
1st TDM system
qth TDM system
$\tilde{X}^{i_1} / y_{i_1}=0$
$\tilde{X}^{i_1} / y_{i_1}=1$
$\tilde{X}^{i_q} / y_{i_q}=0$
$\tilde{X}^{i_q} / y_{i_q}=1$

Figure 1. Principles of TDM systems and train control systems integration

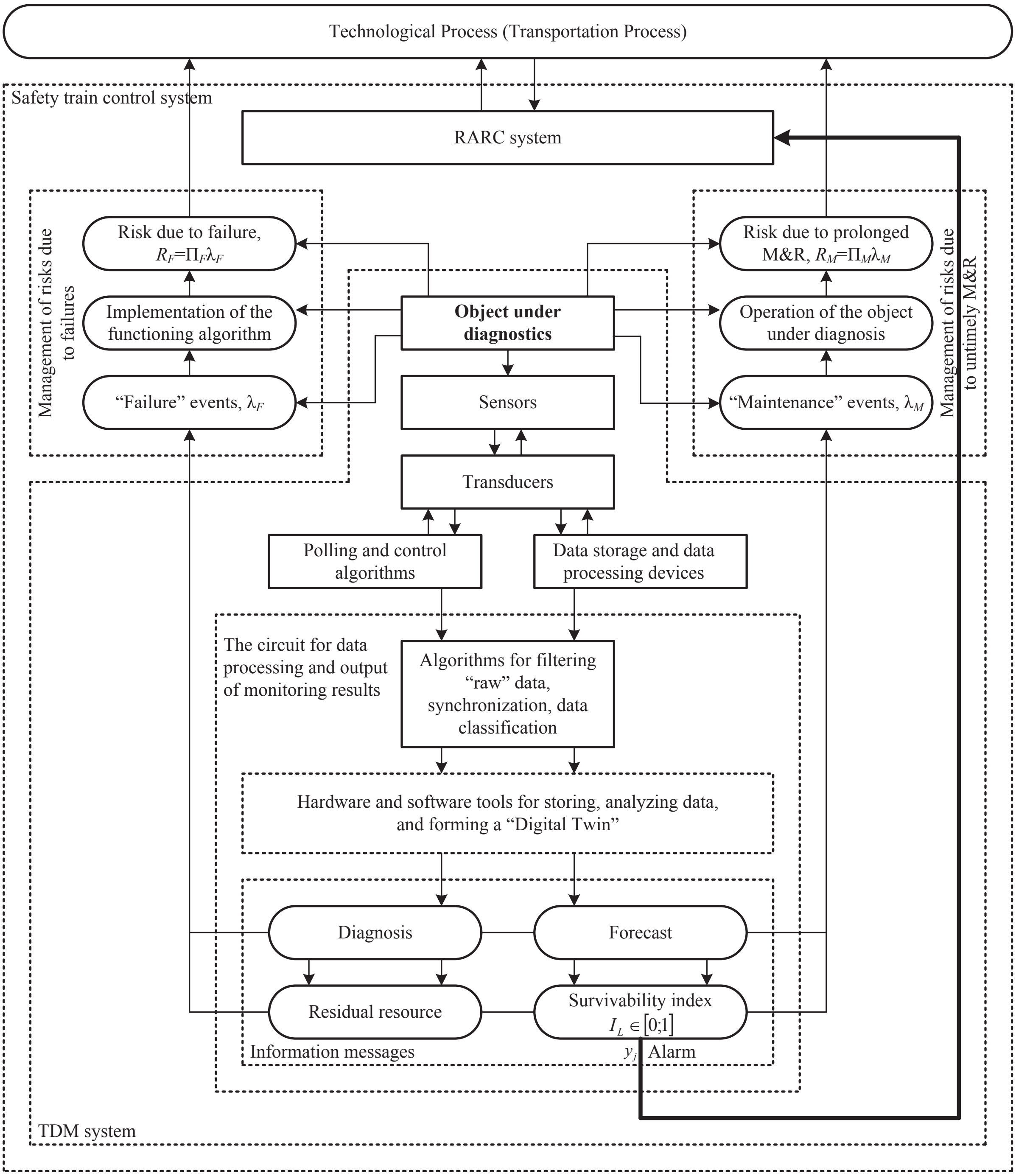
Technological Process (Transportation Process)
Safety train control system
RARC system
Management of risks due to failures
Risk due to failure, $R_F = \Pi_F \lambda_F$
Implementation of the functioning algorithm
"Failure" events, λ_F
Object under diagnostics
Sensors
Transducers
Management of risks due to untimely M&R
Risk due to prolonged M&R, $R_M = \Pi_M \lambda_M$
Operation of the object under diagnosis
"Maintenance" events, λ_M
Polling and control algorithms
Data storage and data processing devices
The circuit for data processing and output of monitoring results
Algorithms for filtering "raw" data, synchronization, data classification
Hardware and software tools for storing, analyzing data, and forming a "Digital Twin"
Diagnosis
Forecast
Residual resource
Survivability index $I_L \in [0;1]$
Information messages
y_j Alarm
TDM system

Figure 2. Structure of a safety train control system

The authors of the article propose at the first stage the integration with the RARC systems in some indirect form – to transfer the alarm signal from the monitoring facilities to the dispatch control system of the RARC devices. Further, this information is perceived by the station duty officer and the train movements controller, which will allow, although not automatically, but much more quickly than in the event of a dangerous event with the direct participation of mobile units [18]. In addition, it is advisable to connect also with warning systems for workers on the way and drivers through train talker. Following such a paradigm, the authors of the paper laid down the possibility of implementing the barrier function in the developed engineering structure monitoring system (ESMS) of railway bridge crossings.

IV. CONCLUSIONS

The authors of the article draw attention to the fact that the train control systems implemented in the modern paradigm are safe with regard to the spatial separation of trains, but not safe taking into account the state of the railway infrastructure, with which they do not directly interact. The conditions are formulated under which it is possible to significantly increase the safety of train traffic, taking into account the technical condition of railway infrastructure facilities. Implementation of a safety train control system is possible by integrating the TDM systems with the RARC systems. In this case, alarms should in a semi-automated (and subsequently in the fully automatic) mode implement barrier functions to limit the speed of trains in the event of a dangerous situation at the object being diagnosed (up to a complete stop of the train).

It should be noted that in the future (and in the very near future), the monitoring systems will be integrated with protective signals, facilities of alerting track workers, as well as with coding subsystems transmitting signals along the rails to the locomotive. This is possible only if the regulatory framework and the TDM systems themselves are improved to such a level that will make it possible to diagnose with high reliability and predict changes in the state and parameters of the objects being diagnosed.

REFERENCES

[1] T. Takashige "Signalling Systems for Safe Railway Transport", *Japan Railway & Transport Review* 21, 1999, pp. 44-50.

[2] C. Hall *"Modern Signalling: 5th edition"*, UK, Shepperton: Ian Allan Ltd, 2016, 144 p.

[3] G. Theeg, and S. Vlasenko *"Railway Signalling & Interlocking: 3ed Edition"*, Germany, Leverkusen PMC Media House GmbH, 2020, 552 p.

[4] V.V. Sapozhnikov, and Vl.V. Sapozhnikov "On Synthesis of Finite Automata Excluding Dangerous Failures", *Automation and Remote Control*, 1972, Vol. 33, Issue 8, pp. 1331-1335.

[5] Vl.V. Sapozhnikov *"Synthesis of Train Traffic Control Systems at Railway Stations with the Exception of Dangerous Failures"* (in Russ.), Moscow: Nauka, 2021.

[6] D.V. Gavzov, V.V. Sapozhnikov, and Vl.V. Sapozhnikov "Methods for Providing Safety in Discrete Systems", *Automation and Remote Control*, 1994, vol. 55, issue 8, pp. 1085-1122.

[7] D.J. Smith, and K.G.L. Simpson *"Functional Safety: A Straightforward Guide to IEC 61508 and Related Standards"*, Butterworth-Heinemann; 1st edition (June 26, 2001), 208 p.

[8] *Russia's Rail Link to Port of Murmansk Severed by Bridge Collapse*, https://www.reuters.com/article/us-russia-bridge/russias-rail-link-to-port-of-murmansk-severed-by-bridge-collapse-idUSKBN2390X7

[9] Y. Park, S.Y. Kwon, and J.M. Kim "Reliability Analysis of Arcing Measurement System Between Pantograph and Contact Wire", *The Transactions of the Korean Institute of Electrical Engineers*, 2012, Vol. 61, No. 8, pp. 1216-1220.

[10] T. Asada *"Novel Condition Monitoring Techniques Applied to Improve the Dependability of Railway Point Machines"*, University of Birmingham, UK, Ph. D. thesis, May 2013, 149 p.

[11] T. Böhm *"Remaining Useful Life Prediction for Railway Switch Engines Using Artificial Neural Networks and Support Vector Machines"*, International Journal of Prognostics and Health Management 8 (Special Issue on Railways & Mass Transportation), December 2017, pp. 1-15.

[12] H. Wang, A. Núñez, Z. Liu, J. Chen, and R. Dollevoet "Intelligent Condition Monitoring of Railway Catenary Systems: A Bayesian Network Approach", *The 25th International Symposium on Dynamics of Vehicles on Roads and Tracks*, 14-18 August 2017, Rockhampton, Australia, pp. 1-6.

[13] Z. Liu, and Vl.L. Markine "Correlation Analysis and Verification of Railway Crossing Condition Monitoring", *Advanced Sensors for Real-Time Monitoring Applications*, eds. O. Korostynska and A. Mason, MDPI, Basel, Switzerland, 2021, pp. 223-243, doi: 10.3390/s19194175.

[14] T. Neumann, D.N. Guzmán, and J.C. Groos "Transparent Failure Diagnostics for Railway Switches Using Bayesian Networks", *Signal+Draht*, 2019 (111), issue 12, pp. 23-31.

[15] M. Wernet, M. Brunokowski, P. Witt, and T. Meiwald "Digital Tools for Relay Interlocking Diagnostics and Condition Assessment", *Signal+Draht*, 2019 (111), issue 11, pp. 39-45.

[16] H. Wang, A. Núñez, Z. Liu, J. Chen, and R. Dollevoet "Intelligent Condition Monitoring of Railway Catenary Systems: A Bayesian Network Approach", *The 25th International Symposium on Dynamics of Vehicles on Roads and Tracks*, 14-18 August 2017, Rockhampton, Australia, pp. 1-6.

[17] D.W. Efanow, and G.W. Osadtschiy "Energy Efficiency Categories for Safety Installations", *Signal+Draht*, 2020 (112), issue 4, pp. 36-42.

[18] J.M. Kokurin, and D.V. Efanov "Technological Foundations of Traffic Controller Data Support Automation", *Proceedings of 17th IEEE East-West Design & Test Symposium (EWDTS'2019)*, Batumi, Georgia, September 13-16, 2019, pp. 176-180, doi: 10.1109/EWDTS.2019.8884410