Original article
DOI: 10.21683/1729-2646-2019-19-2-33-41

Indicator-based approach to safety management of railway infrastructure facilities

Leonid A. Baranov, *Russian University of Transport (MIIT), Russian Federation, Moscow*
Vladimir V. Kulba, *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences (ICS RAS), Russian Federation, Moscow*
Alexey B. Shelkov, *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences (ICS RAS), Russian Federation, Moscow*
Dmitry S. Somov, *Sberbank, Russian Federation, Moscow*

Leonid A. Baranov

Vladimir V. Kulba

Alexey B. Shelkov

Dmitry S. Somov

Abstract. *The Aim of this paper is to develop the methods of analysis and simulation of the processes of occurrence and development of emergencies at complex railway infrastructure facilities. It cites analysis data on the threats, causes and consequences of sudden emergencies at complex railway infrastructure facilities. For the purpose of ensuring reliable operation of technical objects, as well as timely identification of faults, it is proposed to use the indicator-based approach that allows diagnosing and formally analyzing the processes of occurrence and propagation of malfunctions across the elements of complex technical systems. For the purpose of simulating the processes of propagation of the disturbances (hazards of emergencies) that occur as the result of malfunctions, it is proposed to use the theoretic graph approach that involves model and visual representation of the structure of a technical system under consideration in the form of a directed graph that shows the correlations between its elements. Each node and edge of a graph is assigned certain parameters or functionals that reflect the processes of correlated operation of the elements of the simulated system. The propagation of disturbances within a system is simulated with pulse processes initiated in one or several nodes. The paper refers to the developed formalized models of disturbance propagation in a technical system based on the construction of structural components and correlation matrices. The authors introduce the concept of critical element of a technical system that helps identify the event of its failure. Two basic criteria of technical system failure, i.e. the exclusive (a system is considered to have failed if the disturbance has reached any of the critical elements) and absolute criterion (failure occurs if the disturbance has reached the specified subset of critical elements) are defined. The paper provides an analytical example that illustrates the capabilities of the proposed model of disturbance propagation within the structure of a technical system. For the purpose more efficient diagnostics of the hazard of emergencies in railway infrastructure facilities the paper proposes a model of application of structurally integrated indicators that consists in the integration of indicators within the structure of a technical system that would immediately deliver the required and sufficient information in case of emergency. The main task would be to identify a set of indicators with the primary purpose of reducing the information-related stress and concentration of dispatchers' or operators' attention on the processes within a technical system that are most relevant in terms of accident-free and safe operation. Basic criteria are identified for the generation of the set of indicators within a complex technical system: maximum of reliability of the disturbance consequences estimate, maximum of accuracy of emergency causes identification, minimum of emergency identification time, minimum of nonrecurrent and current costs. A modified graph model of disturbance propagation in a complex technical system is provided that is the prerequisite for solving the multicriterion problems of optimal location of indicators within the structure of a technical system in terms of completeness, accuracy and timeliness of detection of failures of various types. Automation of the processes of generation of indicator sets using models of disturbance propagation in technical systems will allow using the proposed methods as part of further development of the URRAN methodology in terms of improvement of the decision support in railway infrastructure facilities management.*

Keywords: *control, railway transportation, infrastructure facility, technical system, emergency, sensors, indicators, simulation.*

For citation: *Baranov LA, Kulba VV, Shelkov AB, Somov DS. Indicator-based approach to safety management of railway infrastructure facilities. Dependability 2019;2: 33-41. DOI: 10.21683/1729-2646-2019-19-2-33-41*

Introduction

Being a crucial part of the Russian transportation industry railways play an essential role in the process of the country's socio-economic development, since this type of transport has practically no alternative in terms of the volume and structure of freight and passenger traffic. The leading role of railway transportation is also determined by the country's specific characteristics, including significant transport distances, remoteness of primary main mining facilities and sources of raw materials from the points of processing and consumption, as well as seaports, insufficient infrastructure development of other types of transport in Siberia and the Far East, which are of strategic importance for the national development. The condition, safety and quality of rail transportation define not only the prospects for further social and economic development, but also the nation's ability to effectively perform such essential functions as protecting its sovereignty and security, providing citizens with transportation and creating conditions for more even economic development of individual regions, etc.

The URRAN integrated system for management of resources, risks and dependability of railway infrastructure facilities at lifecycle stages is being developed and widely implemented by specialized organizations and divisions of the Russian Railways since 2010 [1]. Essentially, the system implements a comprehensive process of dependability, resources and functional safety management in railway transportation and is essentially an extended RAMS (reliability, availability, maintainability and safety) and LCC (life cycle cost) methodology.

The primary strategic railway safety objectives are [2]:

1. Improving the efficiency of the main activity, utilization of infrastructure, technical reliability and fixed assets availability,
2. Ensuring the quality of products, services and processes,
3. Ensuring transportation safety.

The system of railway facilities and processes is a massive geographically distributed multi-purpose infrastructure that includes JSC Russian Railways facilities (track and structures, signalling, communication, electrification and power facilities; locomotive, car and passenger facilities) that are different in purpose and solve different process-specific tasks. At the same time, the complexity of the technical systems included in the above facilities continuously increases, which inevitably leads to an increase in the number and variety of risks associated with the production, adjustment, maintenance, operation and upgrading of these systems [3].

Ensuring safety and dependability becomes especially important with the use of "driverless" vehicles. According to the International Association of Public Transport, there are 5 Grades of Automation of trains (from GOA0 to GOA4). When GOA4 level is implemented, there is no operational personnel onboard rolling stock. Under these conditions, centralized automatic train control systems for subways should contain subsystems that ensure the completeness, accuracy and timeliness of detection of failures of various types and preventive decision making [4].

Today, the technological development goes hand in hand with the increase in the number of elements involved in technical systems (dimensional complexity), the increase in the diversity of interaction structures of these elements (structural complexity) and the increase in the diversity of the forms and methods of this interaction (functional complexity). This significantly complicates the task of ensuring the reliable operation of complex technical systems (CTS) that are part of the railway infrastructure facilities, since, depending on their structural and functional features, the manifestation of the risks and the nature of failures and faults propagation in the considered systems may differ [5]. In this case, the realization of risks may take the form of the possibility of malfunctioning or failure of a separate node and the entire system. The aim of this paper is to develop the methods of analysis and simulation of the processes of occurrence and development of emergencies at complex railway infrastructure facilities from indicator-based approach point of view.

1. Simulation of disturbance propagation in the technical system

The extensive experience of operating CTS of various types and purposes shows that the occurrence of failures and faults of various nature, as well as incidents and emergencies they lead to (hereinafter referred to as sudden emergencies, or SE) is usually preceded by the stage of accumulation of defects in the equipment or deviations in a particular process [6]. The duration of this stage can vary significantly (from minutes to days). At the same time, at first the defects or deviations themselves do not pose an immediate threat of SE occurrence. In practice the processes of accumulation of such deviations are usually associated either with the unobservability of the CTS elements and subsystems due to the lack of effective monitoring and diagnostic tools, or, even more often, with the fact that personnel are accustomed to such deviations, since they do not always lead to accidents. At the next stage a sudden so-called initiating event occurs, which leads to an avalanche-like development of unfavorable processes and the occurrence of SE, the consequences of which are significantly aggravated by the lack of organizational and technical countermeasures, as well as lack of time and resources for their effective implementation. It is obvious that the SE, occurring at the third stage as a result of the rapid development of events, for the most part would be impossible without the accumulation of deviations and errors in the first stage.

Thus, one of the main tasks of ensuring the smooth operation of CTS is the timely identification of malfunctions, other disorders in the technical system, pre-emergency (emergency) situations and the transfer of information on their occurrence to the visualization, dispatching and situational management systems at various levels (to decision makers (DM), dispatchers, operators, etc.). The sources of information on possible abnormal deviations (malfunctions) in CTS or their subsystems (nodes) operation are sensors, elements of the system that can register various parameters of the system state, environment, parameters of the CTS operation, etc.

The resulting risk of malfunction, failure, accident, SE or other disruption of the normal CTS operation, registered by the sensor, is called a threat. In this case, the occurrence of a certain threat presumably leads to the processes of disturbance propagation along the structural elements of CTS accordance with their interaction scheme. Since, in accordance with the definition above, threats can be of different nature (type, nature of occurrence and manifestation, etc.), the CTS elements can interact with each other in various ways during the disturbance propagation process. As a result, schemes of interaction between elements will be different for each type of threat. Hence, the disturbances will also propagate through the elements of the CTS along different paths.

Technical systems of high structural, dimensional and functional complexity usually include a large number of sensors, which makes it significantly more difficult to monitor their readings, diagnose abnormal situations, and most importantly, make timely accurate control decisions in the event of reading deviation from the norm and especially the threat of SE occurrence. Thus, problem of choosing the structure of the dispatching or situational management information system arises. It should allow reducing the operator's stress in order to increase the emergency response rate without a significant loss of awareness about safety critical processes [5, 7-8].

For the purpose of simulating the processes of propagation of the disturbances that occur as the result of malfunctions, the theoretic graph approach will be used. The representation of the structure of a technical system in the form of a graph is widely used for visualization and modeling of the correlations between system elements. At the same time, the structure of the system can be rigidly fixed or undergo certain regular changes (which is typical of dynamic systems) depending on the process or phenomenon being simulated.

In this approach the structure of a system and the interactions between its elements are represented in the form of a directed graph. Each node and edge of a graph is assigned certain parameters and functionals that reflect the processes of operation of the simulated system elements. The initial pulse (disturbance) applied to one or several nodes is propagated through the whole graph changing the parameters of the nodes. In the general case, the magnitude of the pulse itself can change as well in accordance with the functionals assigned to the edges of the graph. The simulation uses discrete time with a fixed step Δt. This approach to simulation of dynamic systems has now found application in a number of areas [9].

Let us assume that $A=\{a_1, a_2, ..., a_n\}$ is a set of elements in a model, where n is their number. At any point in time any element can take on a value of 0 or 1. One stands for an active state (the disturbance has reached the element), zero stands for inactive state. The state of element a_i at the point of time t will be designated as $a_i(t)$, and the row-vector of states of model elements ($a_1(t)$, $a_2(t)$, ..., $a_n(t)$) will be designated as $\overline{A}(t)$. The set of sensors constitute a subset of model elements $A \supseteq D=\{d_1, d_2, ..., d_{n_D}\}$, where n_D is the number of sensors.

Adjacency matrix M shall mean $n \times n$ binary matrix, indexed along both axes by the set of model elements. Positions $(i, j), i, j \in \overline{1, n}$ of the adjacency matrix contain 1 if and only if the relation R_1 between model elements a_i and a_j is such that when element a_i is active at the moment t_1, the element a_j will also be active at the moment $t_2 = t_1 + \Delta t$. In other words, relation R_1 specifies the paths of disturbance propagation through the system. By relation R_1 we shall mean an adjacency relation or reachability of depth of 1 relation. The adjacency relation between model elements a_i and a_j will be designated as $a_i \underline{R_1 a}_j$ and the absence of such relation will be designated as $a_i R_1 a_j$. If there is no adjacency relation R_1 between elements a_i and a_j, there is a 0 in the position (i, j) of the adjacency matrix M. Let us suppose that the adjacency relation has reflexive property, i.e. $\forall a \in A \quad aR_1a$. Within the model, this means that once activated, the element remains activated during the entire simulation time. For each specified type of threat, its own adjacency relationship can be defined, R_1^1, R_1^2, R_1^3 and so on. Accordingly, each type of threat has its own adjacency matrix. The adjacency matrix M corresponds to the digraph of the cause-effect relationships of the model elements $G(A, R_1)$, the nodes of which are the set of model elements, and the edge (a_i, a_j) corresponds to one in the matrix position (i, j). This graph will be called the relationship digraph.

The activation of the model elements is described by the Boolean equation $\overline{A}(t_{i+1}) = \overline{A}(t_i) \times M$. In other words, all elements of the model connected by edges with already active elements are activated at further steps. In this case, once activated elements remain activated during the entire simulation, since the diagonal elements of the adjacency matrix are equal to 1.

Among the set of model elements the subset of sensors $D=\{d_1, d_2, ..., d_{n_D}\}$ is selected. The sensors register the specified parameters of the CTS and indicate the occurrence of a threat. The disturbance caused by this threat spreads from the sensors to other elements of the system along the edges of the correlation graph $G(A, R_1)$. The set of model elements, the correlation matrix and the subset of sensors are determined together with the system designer according to the results of the system operation scheme analysis at the development stage. The subset of critical elements $K=\{k_1, k_2, ..., k_{n_K}\}$ that determine the criterion for system failure is also selected among the elements of the model. Different sets of critical elements can be considered for each type of threat (edge coloring).

Simulation starts at the moment of activation of the first sensor t_0 and continues either until the moment of stabilization (termination of change in the state of the model elements), or until the system fails in accordance with the selected system failure criterion.

The time of system failure will be designated as t_S. The criterion for system failure is determined by critical elements. Depending on the features of the system or node under consideration, as well as other features of the problem being solved, different criteria for evaluating the system failure can be selected. There are two basic criteria among them.

Exceptional criterion for system failure. The system is considered failed if the disturbance has reached any of the critical elements: $t_S = \min(t : \exists k \in K : k(t) = 1)$.

Absolute criterion for system failure. The system is considered failed if the disturbance has reached a given subset $K^* \subseteq K$ of (in the degenerate case of all) critical elements: $t_s = \min(t : \forall k \in K^* : k(t) = 1)$.

Other criteria can also be considered, for example, those related to the number, mutual arrangement and other parameters of the critical element set to which the disturbance has reached.

To illustrate the possibilities of the proposed model of disturbance propagation in the structure of a CTS, let us consider a simplified example. Let us suppose that the structure of the system include 12 elements, n=12, A={a_1, a_2, ..., a_{12}}. Elements a_1 and a_2 are sensors, $d_1 = a_1$, $d_2 = a_2$, D={d_1, d_2}= {a_1, a_2}, n_D=2. Elements a_{11} and a_{12} are critical elements, $k_1 = a_{11}$, $k_2 = a_{12}$, K={k_1, k_2}= {a_{11}, a_{12}}, n_K=2. The adjacency matrix M is defined as:

$$M = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline 1&0&1&0&0&0&0&0&0&0&0&0\\
\hline 0&1&0&1&1&0&0&0&0&0&0&0\\
\hline 0&0&1&1&0&0&0&1&0&0&0&0\\
\hline 0&0&0&1&0&1&0&0&0&0&0&0\\
\hline 0&0&0&0&1&0&1&0&0&0&0&0\\
\hline 0&0&1&0&0&1&1&0&0&0&0&0\\
\hline 0&0&0&0&0&0&1&0&0&1&0&0\\
\hline 0&0&0&0&0&0&0&1&1&0&0&0\\
\hline 0&0&0&0&0&0&0&0&1&0&1&0\\
\hline 0&0&0&0&0&0&0&0&1&1&0&1\\
\hline 0&0&0&0&0&0&0&0&0&0&1&0\\
\hline 0&0&0&0&0&0&0&0&0&0&0&1\\
\hline
\end{array}.$$

The relation R_1, defined by the matrix M forms the relation digraph $G(A, R_1)$ shown in Figure 1, where the sensors are designated by a circle 🟡, and the critical elements are indicated by a square 🟥. Let us suppose that there is only one type of threat, hence, only one set of critical elements, one adjacency relationship and one relationship graph are defined.

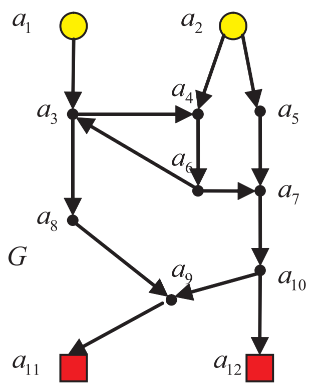


Figure 1. Relation graph G

Let us suppose that at time $t = t_0$ the sensor d_1=a_1 registers a threat $a_1(t_0)$=1, $a_{i,j\neq1}(t_0)$=0, $\overline{A}(t_0) = \underbrace{(1,0,0,...,0)}_{12}$.

Then, the states of the model elements at the time point $t = t_1 = t_0 + \Delta t$ are calculated as follows:

$$\overline{A}(t_1) = \overline{A}(t_0) \times M = \underbrace{(1,0,1,0,0,...,0)}_{12}.$$

Figure 2 shows the process of disturbance propagation along the edges of the relation graph G from active elements (marked by an additional circle) to inactive ones, as well as the states of the corresponding model elements at different points in time. The disturbance spreads along the edges of the graph from the active elements to the inactive ones, covering one edge at a step. The state of the elements at a specific time point is determined by a Boolean formula $\overline{A}(t_i) = \overline{A}(t_0) \times M^i$.

The elements status lines for different points in time are as follows:

$$\overline{A}(t_0) = (1,0,0,0,0,0,0,0,0,0,0,0);$$

$$\overline{A}(t_1) = (1,0,1,0,0,0,0,0,0,0,0,0);$$

$$\overline{A}(t_2) = (1,0,1,1,0,0,0,1,0,0,0,0);$$

$$\overline{A}(t_3) = (1,0,1,1,0,1,0,1,1,0,0,0);$$

$$\overline{A}(t_4) = (1,0,1,1,0,1,1,1,1,0,1,0);$$

$$\overline{A}(t_5) = (1,0,1,1,0,1,1,1,1,1,1,0);$$

$$\overline{A}(t_6) = (1,0,1,1,0,1,1,1,1,1,1,1).$$

As the above example shows, at the time point t=t_4 the first critical element is activated. If the system uses an exceptional criterion for system failure, then at the time point t_4 the system would fail. With absolute criteria, the system fails at the time point t=t_6.

2. Models of using the indicator-based approach

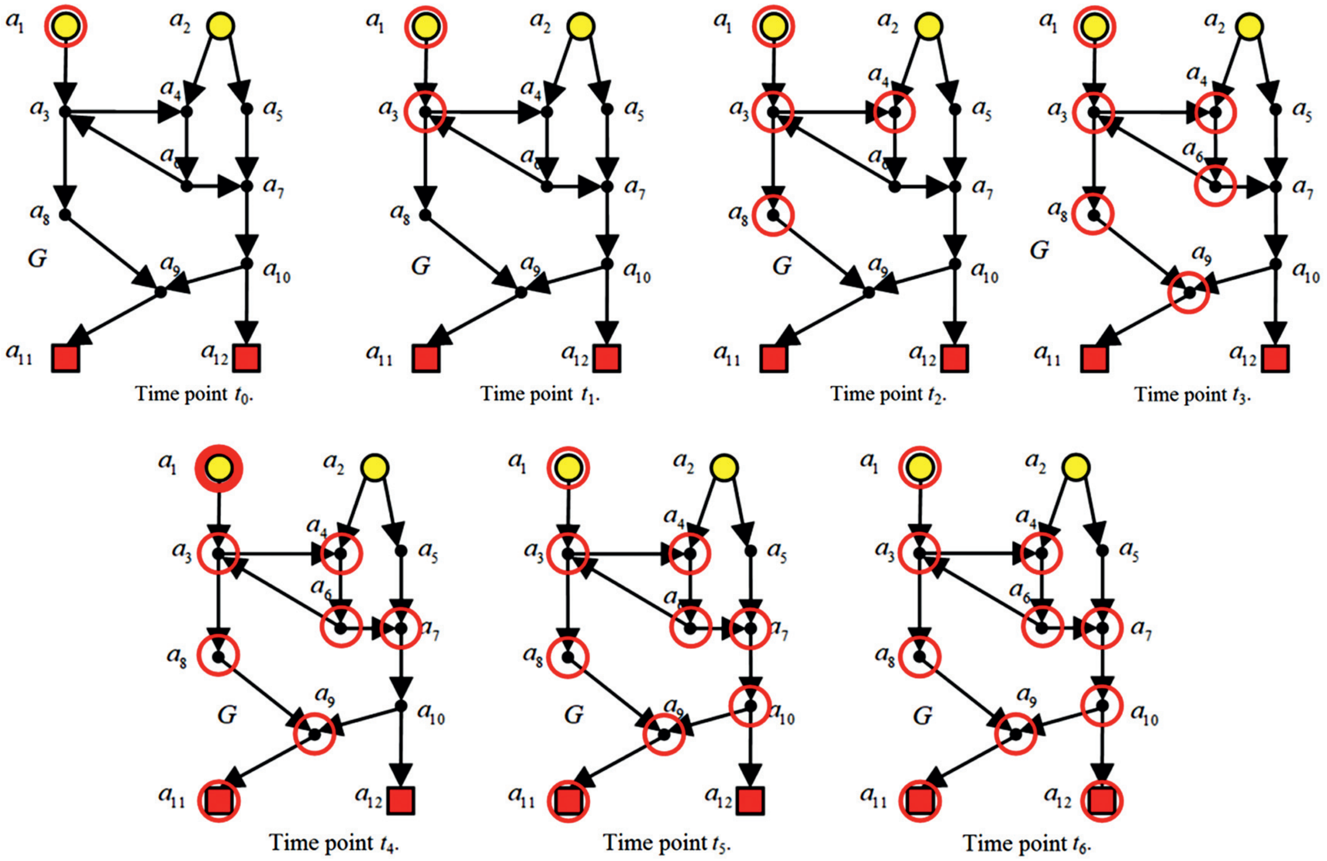
For the purpose of more efficient diagnostics of emergency hazard, a model of application of structurally integrated indicators in railway infrastructure facilities will be considered. The indicator-based approach means that, in addition to the sensors, indicators are integrated within the structure of a technical system immediately delivering the required and sufficient information to the corresponding visualization, dispatching or situational management systems in case of emergency in order to inform the DM (dispatchers, operators, etc.) if increased attention to the situation or direct intervention are required.

The main task is to identify a set of indicators (the concept of "indicator dashboard" generally accepted in organizational management [10] can be used here) with the primary purpose of reducing the information-related stress and concentration of dispatchers' or operators' attention on the processes within a technical system that are most relevant in terms of accident-free and safe operation.

The values of the parameters reflected by the selected indicators should reliably demonstrate the deviations from the normal operation of the system. Thus, within the framework of control, dispatching or situational management, the approach under consideration is to first and foremost provide the decision makers with the necessary and sufficient information on the status of the CTS in visual form, as well as ensure the possibility of operational (including scenario) analysis of alternative ways of emergency situation developing on a specific time horizon. Ultimately, it should improve the efficiency of management decisions on transport safety.

In order to achieve these objectives, the location of the indicators in the CTS structure should allow for informing the DS on the occurrence and development of a potentially dangerous situation at the earliest possible stage. At the same time, it should be noted that at the early stages of a situation's development, the possible (most probable, pessimistic, optimistic, etc.) scenario for an abnormal situation is not always clear. As a result, the set of consequences may be too broad, which does not allow reliably predicting the consequences and making the right decision. In this case, real-time and detailed monitoring of the potentially pre-emergency state of the CTS is required in order to collect additional information to analyze it and decide on the appropriate response.

Naturally, an equally important criterion for choosing a specific placement of indicators is the cost of such placement. Depending on the specific task, it is necessary to take into account not only the number of indicators, but also their weight, volume, physical distance between indicators, sensors, etc. When selecting a set of indicators one should obviously strive to reduce their total number,



Time point t_0.

Time point t_1.

Time point t_2.

Time point t_3.

Time point t_4.

Time point t_5.

Time point t_6.

Figure 2. The process of disturbance propagation in the system

while ensuring the minimum possible reduction in the accuracy and information content of the data they send to the visualization, dispatching or situational management systems.

At the substantive level, the following main criteria for choosing the set of indicators in a complex technical system can be distinguished.

Reliability of consequence evaluation. The selection of the indicator set should allow for making judgment on the nature of the situation development and possible consequences with maximum accuracy based on their readings.

Accuracy of cause identification. Indicators should allow not only for timely detection and consequences assessment of abnormal situations, but also for identification of their causes. For example, indicators should show with which CTS node (element) the spread of the negative impact started, whether the cause of the deviations was external or internal, etc.

Abnormal situation detection time. Indicators' selection and localization in the structure of the CTS should allow for detecting deviation from normal operating at the earliest possible stages of their development in order to maximize the amount of time available for a decision made by system operator.

Cost. Indicators' selection and localization in the structure of the CTS should minimize one-time and current costs.

The proposed criteria are contradictory in a way. For example, in order to determine the cause of an abnormal situation as precisely as possible, strictly speaking, one should place indicators in all elements of the system, but this will increase the cost, the information-related stress on the decision maker, the time required for abnormal situation detection, etc.

To solve the problem of composing a set of indicators, the above graph model of disturbance propagation in the CTS is modified. The concept of edge passing time is introduced expressed as a positive number associated with the edge of the relation graph and meaning the time, during which the disturbance passes from the model element at the beginning of the edge to the element at the end of the edge. To register the edge passing times, the matrix of temporal relations Mt, which is a square matrix $n \times n$, indexed along both axes by the model elements. Positions (i, j), $i, j, \in 1, n$ of the temporal relations matrix contain edge passing time (a_i, a_j), if such edge exists, and infinity sign ∞, if such edge does not exist.

Temporal distances matrix N shall mean a $n \times n$ square matrix indexed along both axes by the set of model elements. Position (i, j), $i, j, \in 1, n$ of this matrix contains temporal distance between graph nodes a_i and a_j. The temporal distance matrix is the result of applying the Floyd-Warshall algorithm for finding the shortest distances between the nodes to the matrix of temporal relations [11].

An optimization problem of placing indicators in a technical system is formulated using a series of definitions introduced below. A subset of indicators will be denoted by $I=\{i_1, i_2, ..., i_{n_I}\}$. The set of time t precedence of element a shall mean a set of model elements $Bef_i(a)$, from which the element a can be reached in a time not exceeding time t. The set of time t precedence of element a shall mean a set of model elements $Bef_i(a)$, from which the element a can be reached in a time not exceeding time t. The set of time t afteraction of element a shall mean a set of model elements $Aft_i(a)$, which can be reached from the element a in a time not exceeding time t.

Indicator coverage of time t precedence shall mean a set of time t precedence sets for all indicators:

$$I_t^{Bef} = \left\{ Bef_t(i_1), Bef_t(i_2), \ldots, Bef_t\left(i_{n_t}\right) \right\}.$$

Indicator set of coverage of time t precedence shall mean the union of the set of model elements included in the indicator coverage of time t precedence, or, what is the same, the union of time t precedence sets for all indicators:

$$\overline{I_t^{Bef}} = \bigcup_{j=n_t} Bef_t\left(i_j\right).$$

Similarly, indicator coverage of time t afteraction shall mean a set of time t afteraction sets for all indicators:

$$I_t^{Aft} = \left\{ Aft_t(i_1), Aft_t(i_2), \ldots, Aft_t\left(i_{n_t}\right) \right\}.$$

Indicator set of coverage of time t afteraction shall mean the union of the set of model elements included in the indicator coverage of time t afteraction, or, what is the same, the union of time t afteraction sets for all indicators:

$$\overline{I_t^{Aft}} = \bigcup_{j=n_t} Aft_t\left(i_j\right).$$

Overall set of coverage precedence shall mean the union of sets of time given for each indicator precedence for all indicators:

$$I_T^{Bef} = \left\{ Bef_{t_1}(i_1), Bef_{t_2}(i_2), \ldots, Bef_{t_{n_I}}\left(i_{n_t}\right) \right\},$$

where $T=\{t_1, t_2, ..., t_{n_T}\}$ is a set of times of precedence sets. Similarly, the concept of overall indicator precedence coverage

$$I_T^{Aft} = \left\{ Aft_{t_1}(i_1), Aft_{t_2}(i_2), \ldots, Aft_{t_{n_I}}\left(i_{n_t}\right) \right\}.$$

Diameter of the overall coverage shall mean the maximum value of all times of a set.

$$T:D\left(I_T^{Bef}\right)=D\left(I_T^{Aft}\right)=\max_{j\le n_I}\left(t_j\right).$$

Similar to the time coverage, the concept of the indicator set of the overall indicator coverage of precedence and afteraction is introduced:

$$\overline{I_t^{Bef}}=\bigcup_{j\le n_t}Bef_t\left(i_j\right),\overline{I_t^{Aft}}=\bigcup_{j\le n_t}Aft_t\left(i_j\right).$$

Let us suppose that the solutions to the indicator localization problem is a subset of model elements $I\subseteq A$. With the introduction of some restrictions on the set of solutions the set of feasible solutions is obtained.

The number of indicators should be limited. This restriction derives from the requirement to reduce the information-related stress on the operator. Mathematically this restriction can be expressed as $|I|=n_I\le N_I$, where N_I is some constant given in a specific task.

The set of indicators shall cover all possible threats known at the current stage of system development. In other words, in terms of the model in question, there should not be a situation in which the disturbance caused by the sensor reaches a critical element before it reaches the indicator. The mathematical interpretation of this restriction can be written as $\forall d\in D:Alf\left(d\right)\bigcap K\ne\varnothing\,\exists i\in I:i\in Aft_S\left(d\right)$

Thus, the region of feasible solutions must satisfy the afteraction requirements:

$$I\subseteq A,$$

$$|I|=n_I\le N_I,$$

$$\forall d\in D:Alf\left(d\right)\bigcap K\ne\varnothing\,\exists i\in I:i\in Aft_S\left(d\right).$$

Optimization criteria for finding the optimal solution among the feasible solutions are formulated.

1. *Criterion of maximizing the allowable time for decision making.* From the system's operational safety and failure prevention point of view the earliest possible threat detection is required. This criterion implies maximizing the time from the moment of activation of the critical element to the critical event. In terms and designations of the model it is written as follows:

$$\min_{d\in D,k\in K}\left(\max_{i\in I\bigcap Alf\left(d\right)}\left(dis^t\left(d,k\right)-dis^t\left(d,i\right)\right)\right)\to\max_I.$$

2. *Completeness of coverage*. For each set of indicators, coverage by precedence and afteraction sets is defined.

In order to judge of the possible causes and consequences of the current situation most accurately, the selected indicators must allow for the precedence and afteraction sets to covers as much of the model elements as possible. Mathematically, it can be expressed as:

$$\left|\overline{I^{Alt}}\right|\to\max_I;\left|\overline{I^{Bef}}\right|\to\max_I.$$

3. *Accuracy of coverage.* In the previous criterion coverage is used without consideration of time. However, to accurately identify the developing situation, the indicators should be "close" to the propagating through the system disturbance in time. For that purpose, the minimal diameter of precedence or afteraction coverage (the set of which covers the whole set of precedence I^{Bef} or afteraction I^{Alt}) must be minimal:

$$\min_{T:\overline{I_T^{Alt}}=\overline{I^{Alt}}}\left(D\left(I_T^{Alt}\right)\right)\to\min_I;$$

$$\min_{T:\overline{I_T^{Bef}}=\overline{I^{Bef}}}\left(D\left(I_T^{Bef}\right)\right)\to\min_I.$$

Let us formulate the task of optimizing the placement of indicators.

Let us suppose that the given model of disturbance propagation through a technical system is: the set of model elements is $A=\{a_1,a_2,...,a_n\}$, the subset of sensors is $D=\{d_1,d_2,...,d_{n_D}\}$, the subset of critical elements is $K=\{k_1,k_2,...,k_{n_K}\}$. The model elements are interconnected in relations graph *G*, edge passing times are given in the matrix of temporal relations *M*.

It is required to find such subset of elements (a set of indicators) $I=\{i_1,i_2,...,i_{n_I}\}$ that would comply with the following conditions:

$$|I|=n_I\le N_I,$$

$$\forall d\in D:Alf\left(d\right)\bigcap K\ne\varnothing\,\exists i\in I:i\in Aft_S\left(d\right).$$

$$\min_{d\in D,k\in K}\left(\max_{i\in I\bigcap Alf\left(d\right)}\left(dis^t\left(d,k\right)-dis^t\left(d,i\right)\right)\right)\to\max_I,$$

$$\left|\overline{I^{Alt}}\right|\to\max_I;\left|\overline{I^{Bef}}\right|\to\max_I,$$

$$\min_{T:\overline{I_T^{Alt}}=\overline{I^{Alt}}}\left(D\left(I_T^{Alt}\right)\right)\to\min_I;$$

$$\min_{T:\overline{I_T^{Bef}}=\overline{I^{Bef}}}\left(D\left(I_T^{Bef}\right)\right)\to\min_I.$$

Due to the orientation to the systems of high dimensional, structural and functional complexity and in light of opposing nature of the criteria formulated above, the precise algorithms for solving the problem in question will have too high computational complexity. Thus this problem is proposed to be solved using a combination of various approximate algorithms that create solutions according to individual criteria, or modify some existing indicator placement created based on other performance criteria [5, 12]. The practical application of this problem algorithms should be carried out using interactive procedures to collaborate with experts or specialists in a given subject area. Such approach can significantly improve the quality of the solution results (variants of indicator placement) in terms of achieving the set goals.

Conclusion

The main aim of the proposed indicator-based approach is to increase the dependability of CTS in operation and to prevent SE through the early diagnostics of the hazard of emergencies in technical systems. The indicator-based approach offers means to reduce the information-related stress and to concentrate dispatchers' or operators' attention on the processes that are most relevant in terms of safety. The approach also allows locating the sources of emergency situations with the required accuracy.

The proposed models of the disturbance propagation in the CTS are the basis for the formulation and development of formalized methods for timely detection of abnormal situations during the CTS operation and preventing SE. The developed indicator-based approach includes a set of models and technologies for analyzing the processes of hazard effect and disturbances propagation in complex technical systems, as well as methods for solving multi-criteria problems of optimal placement of indicators in the structure of the CTS based on criteria of completeness, accuracy and timeliness of detecting failures of various types.

References

[1] Gapanovich V.A. Development and implementation of the URRAN technology on railway transport. Dependability 2013;4:11-17.

[2] Gapanovich V.A., Shubinsky I.B., Rozenberg E.N., Zamyshlyaev A.M. System of adaptive management of railway transport infrastructure technical maintenance (URRAN project). Dependability 2015;2:14-22.

[3] Kulba V.V., Kosyachenko S.A., Shelkov A.B. Methodology of research of railway transport safety problems. Large-Scale Systems Control 2012;38:5-19 [in Russian].

[4] Baranov L.A. Automatic control of metro trains. World of Transport and Transportation. 2018;16(3):156-165 [in Russian].

[5] Kulba V.V., Kononov D.A., Kosyachenko S.A., Kochkarov AA, Somov DS. Ispolzovanie scenarnogo i indikatornogo podhodov dlya upravleniya zhivuchestyu, stojkostyu i bezopasnostyu slozhnyh tekhnicheskih sistem [Use of scenario and indicator-based approaches to controling the survivability, durability and safety of complex technical systems]. Moscow: ICS RAS;2011 [in Russian].

[6] Bykov A.A. O problemah tekhnogennogo riska i bezopasnosti tekhnosfery [On the problems of technology-related risk and safety of the technosphere]. Issues of risk analysis 2012:9(3):4-7 [in Russian].

[7] Shults V.L., Kulba V.V., Shelkov A.B., Chernov I.V., Somov D.S. Upravlenie tekhnogennoy bezopasnostyu na osnove scenarnogo i indikatornogo podhodov. Nauchnoe izdanie [Technogenic safety management using scenario and indicator approaches. A scientific publication]. Moscow: ICS RAS; 2013 [in Russian].

[8] Shults V.L., Kulba V.V., Shelkov A.B., Chernov I.V. Metodologiya upravleniya tekhnogennoy bezopasnostyu obiektov infrastruktury zheleznodorozhnogo transporta na osnove indikatornogo podhoda [Method of technogenic safety management of railway infrastructure facilities using indicator approach]. Trends and management 2013;3:4-23 [in Russian].

[9] Shults V.L., Kulba V.V., editors. Modeli i metody analiza i sinteza scenariev razvitiya socialno-ekonomicheskih sistem [Models and methods of analysis and synthesis of development scenarios of socio-economic systems]. Moscow: Nauka; 2012 [in Russian].

[10] Eckerson W. Performance Dashboards: Measuring, Monitoring, and Managing your Business. Moscow: Alpina Business Books; 2007.

[11] Cormen T., Leiserson C., Rivest R., Stein C. Introduction to Algorithms. Third edition. Moscow: Izdatelstvo Viliams; 2013.

[12] Kulba V.V., Somov D.S., Kochkarov A.A. The use of structure-integrated indicators in complex technical systems monitoring. Izvestiya SFedU. Engineering sciences 2011;3(116):52-65 [in Russian].

About the authors

Leonid A. Baranov, Doctor of Engineering, Professor, Head of Department, Russian University of Transport (MIIT), Russian Federation, Moscow, e-mail: baranov.miit@gmail.com

Vladimir V. Kulba, Doctor of Engineering, Professor, Head of Laboratory, V.A. Trapeznikov Institute of

Control Sciences of the Russian Academy of Sciences, Russian Federation, Moscow, e-mail: kulba@ipu.ru

Alexey B. Shelkov, Candidate of Engineering, Lead Researcher, V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Russian Federation, Moscow, e-mail: abshelkov@gmail.com

Dmitry S. Somov, Chief Analyst, Sberbank, Russian Federation, Moscow, e-mail: somov.dmitry@gmail.com

Received on: 27.02.2019