Original article
DOI: 10.21683/1729-2646-2019-19-2-28-32

Model of efficiency assessment of diagnostic tools of onboard equipment

Efim N. Rozenberg, *JSC NIIAS, Russian Federation, Moscow*
Alexander S. Korovin, *JSC NIIAS, Russian Federation, Moscow*
Natalia G. Penkova, *JSC NIIAS, Russian Federation, Moscow*

Efim N. Rozenberg

Alexander S. Korovin

Natalia G. Penkova

Abstract. *The* **Aim** *of this paper is to show that the development, deployment of new diagnostic tools and improvement of the existing diagnostic tools in onboard equipment enables better operational characteristics and reduced probability of transition of intelligent railway systems into a forbidden state.* **Method.** *In the context of intelligent railway systems, the construction of the analytical model of probability evaluation is of principal interest due to the feasibility of demonstrating the factors that are taken into consideration by such a model. Forbidden events that cause inoperability of intelligent railway systems are random; they can be represented as a random process. A random process of system development, transition from an allowed state into a forbidden state, system state changes in time can be described with a semi-Markovian process. When assessing the probability of system transition into a forbidden state, the question arises as to the selection of a method of calculation. The paper shows the feasibility of representation and solution of a semi-Markovian model with the help of a coupled graph model [3, 5] that has a high level of visualization and is a well-formalized method of identification of the probability of a system's transition into a forbidden state. The set of system states and their connections are represented with a directed state graph with defined topological concepts [3]. In order to identify the effect of the introduction of new diagnostic tools and improvement of the existing diagnostic tools in onboard equipment on the probability of transition of intelligent railway systems into a forbidden state, the authors use the theorem of identification of the probability of system's transition from the initial unhazardous state into a hazardous state and set forth the formula to calculate this probability.* **Results.** *The graph method implemented in this paper shows that the use of additional diagnostic tools reduces more than twice the probability of a system's transition into a forbidden state, i.e. a state when the failure will not be detected by the inbuilt or additional diagnostic tools.*

Keywords: *onboard train protection systems, display unit, functional dependability, graph model*

For citation: *Rozenberg EN, Korovin AS, Penkova NG. Model of efficiency assessment of diagnostic tools of onboard equipment. Dependability 2019;2: 28-32. DOI: 10.21683/1729-2646-2019-19-2-28-32*

Introduction

Simulation is widely used in the railway industry for planning of forbidden state handling. In case of intelligent systems, mathematic simulation is advantageous. Methods of mathematic simulation are subdivided into two groups: analytical and simulation modeling. Due to certain shortcomings of simulation modeling [1], in the context of intelligent railway systems, the construction of the analytical model of probability evaluation is of principal interest due to the feasibility of demonstration of the factors that are taken into consideration by such model. Forbidden events that cause inoperability of intelligent railway systems are random; they can be represented as a random process. A random process of system development, transition from an allowed state into a forbidden state, system state changes in time can be described with a semi-Markovian process. In general, the construction and solution of semi-Markovian models comes down to building a system of homogenous differential equations. This procedure always involves mathematical difficulties. For this reason the paper shows the feasibility of representation and solution of semi-Markovian models with a coupled graph model [3, 5]. Such models are highly visual, allow formalizing the wanted system states, as well as paths of transition from allowed into hazardous states, does not require the use of complex mathematics in the preparation of measures of forbidden event handling.

Problem definition

Currently, the Russian railway industry employs the following intelligent onboard systems: KLUB-U (standardized integrated onboard train protection system), BLOK (vital integrated onboard system) and BLOK-M (scalable vital integrated onboard system). The KLUB-U, BLOK and BLOK-M systems have their own display units equipped with man-machine interfaces. A display unit is a hardware and software system. This system is to ensure information display to the driver, assistant driver, operator in case of driverless operation, service personnel in case of locomotive driving and pre-trip diagnostics.

The display of information on the permitted speed, target speed, actual speed, track profile, distance, stopping point ahead, train schedule, train ahead, stop aspect enables safe locomotive driving in terms of observation of speed limits in normal operation and prediction of safe mode of locomotive driving.

In the process of operation, system operability may be disrupted due to a random hardware failure, manifestation of a systematic failure in its software, driver's error while interacting with the system, input data error. Any disruption of system operability is regarded as its failure. This causes the display of incorrect information and wrong decisions by the driver in terms of safety of locomotive driving.

That is why great attention is paid to the development and application of diagnostic tools that allow minimizing the probability of the display unit transitioning into a forbidden state that causes disruption of display unit operability. A forbidden state, in this case, is understood as a hidden (not detected by diagnostic tools) failure.

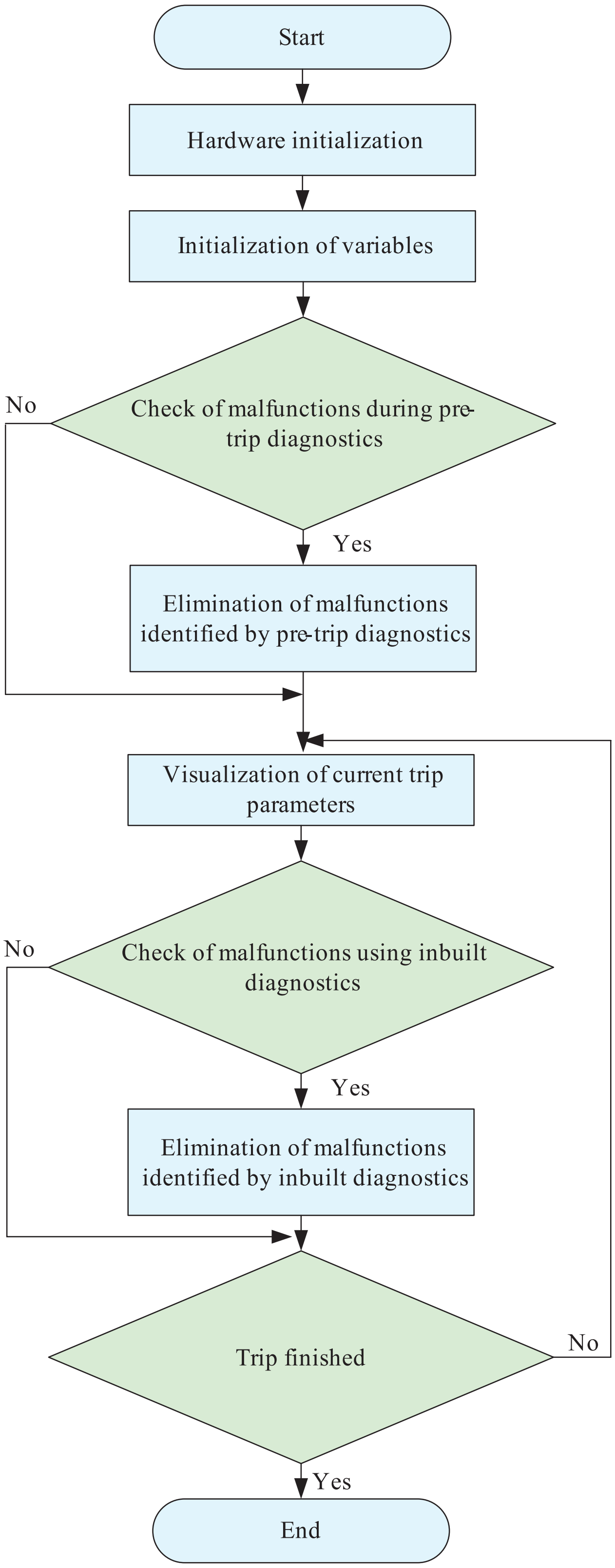
Start
Hardware initialization
Initialization of variables
Check of malfunctions during pre-trip diagnostics
No
Yes
Elimination of malfunctions identified by pre-trip diagnostics
Visualization of current trip parameters
Check of malfunctions using inbuilt diagnostics
No
Yes
Elimination of malfunctions identified by inbuilt diagnostics
Trip finished
No
Yes
End

Figure 1. Flow diagram of the operation algorithm of a display unit with inbuilt diagnostic tools and pre-trip diagnostics

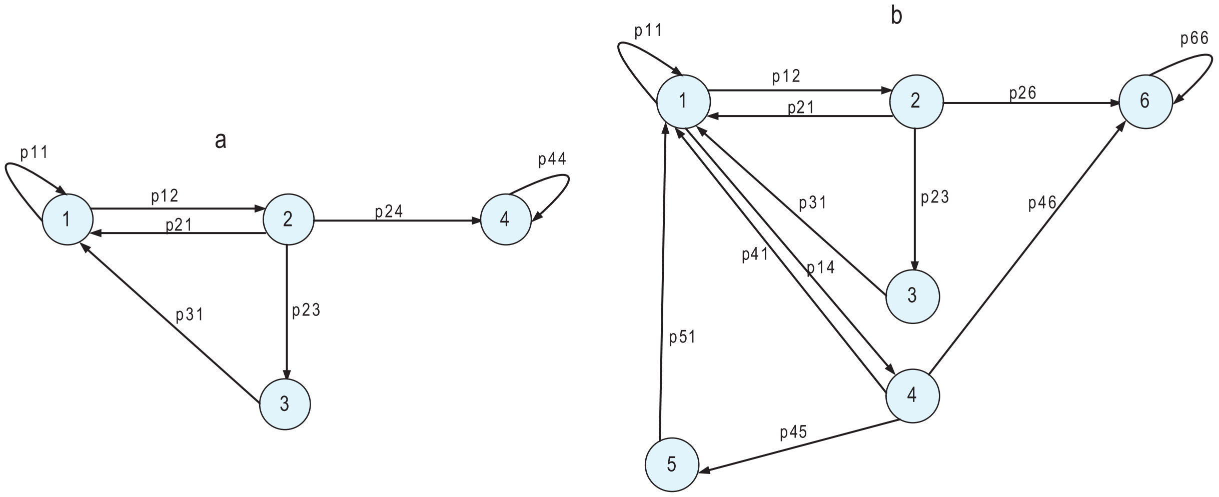

Figure 2. State graph: a) with inbuilt diagnostic tools, b) with inbuilt diagnostic tools and added pre-trip diagnostics of the display unit by the driver or service personnel.

The display unit has inbuilt diagnostic tools that verify the operability of the display unit with a level of diagnostic coverage that is sufficient to ensure safety.

Inbuilt diagnostic tools are able to detect a number of irregularities in the display unit operation. In order to extend the list of detectable errors, it is proposed to introduce additional pre-trip diagnostics by the driver or service personnel to be conducted before each trip. Among other things, that will allow preventing locomotives with faulty safety devices to be cleared for operation.

The aim of this paper is to show the efficiency of diagnostic tools in man-machine interaction in the context of onboard systems. It is also to demonstrate that the development, deployment of new diagnostic tools and improvement of the existing diagnostic tools enables better operational characteristics of the display unit and reduced probability of its transition into a forbidden state.

Models description

Let us represent the operation algorithm of a display unit with inbuilt diagnostic tools and pre-trip diagnostics in the form of a flow diagram (figure 1).

Let us construct the graph of the operation algorithm of the display unit shown in Figure 1.

Events of irregularities of display unit operation are random in their nature. Let us represent the considered operation algorithms of the display unit with a directed state graph *G(S, H)*, where *S* is the finite set of system states; *H* is the finite set of edges between nodes *i, j* (states s_i, s_j). The states of display unit operation can be described as follows: if the display unit is in state s_i, then with probability p_{ij} it can transition into state s_j.

Figure 2a shows a state graph in which only the inbuilt diagnostic tools are used for detection of display unit failure. Figure 2b shows a state graph in which the detection of system failures involves not only the inbuilt display unit diagnostic tools, but additional pre-trip diagnostics of the display unit by the driver or service personnel. In order to attain the goal of this paper, let us consider the graph in Figure 2b. The graph has the following states:

State *S*1, display of the current operational situation by the display unit software;

State *S*2, testing for failures by inbuilt diagnostic tools (software check for CAN errors, software check for controller freeze by watchdog timer switching, software check of display unit being present in the configuration);

State *S*3, elimination by the display unit of failures detected by the inbuilt diagnostic tools (software reboot of CAN interface, hardware controller reboot by means of watchdog timer, hardware reboot of display unit software);

State *S*4, testing for failures by means of pre-trip diagnostics of display unit (correctness of command processing, correctness of operational situation display, correctness of installed version of software, correctness of parameter values of constant characteristics);

State *S*5, elimination by the driver or service personnel of failures detected by means of pre-trip diagnostics (immediate elimination of detected errors, display unit software update input of correct parameter values of constant characteristics);

State *S*6, i.e. display unit being in a state with a hidden failure.

S is the complete set of states, *S* = {*S*1, *S*2, *S*3, *S*4, *S*5, *S*6};

S_p is the subset of non-forbidden states, S_p = {*S*1, *S*2, *S*3, *S*4, *S*5};

$\overline{S}_p$ is the subset of forbidden states, $\overline{S}_p$ = {*S*6}.

Provided that the display unit's inbuilt and pre-trip diagnostic tools are operable, the existence of failure in the display unit is identified and the system is put into failure elimination mode.

It is assumed that in case of failure detection the system is restored. In case of non-detection of failure by the inbuilt and pre-trip diagnostic tools of the display unit due to their failure or insufficient efficiency the system is put into hidden failure mode (forbidden state).

States $S1$ and $S2$ are allowed and belong to the set “normal operation of display unit during intended operation”. The values of transition probability $p11$ and $p12$ were selected based on the ratio of the part of the program that implements the function of current operational situation display and function of failure detection by inbuilt diagnostic tools. A trip lasts 10 hours (i.e. every 10 hours the state a pre-trip diagnostics is to be initiated).

The value $p21$ is selected based on the actual dependability of the display unit in the course of its operation. Statistically, a failure of the display unit is a low-probability event (70 failures were registered in 2018 throughout the railway network based on operational data, the total number of systems being 11740). The fact that a failure has not been registered in the course of operation does not mean that the unit is operational the whole time. It may have been in a forbidden state of hidden failure for some period of time. The values of probabilities of transitions $p23$ and $p26$ were distributed based on the efficiency of the internal diagnostic tools implemented in the unit. The failure detectivity by the inbuilt diagnostic tools implemented in the display unit are at 0.5 in accordance with GOST R 61508-7-2012.

Table 2 shows the values of probabilities of one-step transitions from the i-th state to state j (p_{ij}).

Table 1. Transition probabilities matrix

		State						
		1	2	3	4	5	6	∑
State	1	0,72	0,18	0	0.1	0	0	1
	2	0,85	0	0,075	0	0	0,075	1
	3	1	0	0	0	0	0	1
	4	0.7	0	0	0	0,15	0,15	1
	5	1	0	0	0	0	0	1
	6	0	0	0	0	0	1	1

The problem consists in the identification of the effect of introduction of pre-trip diagnostics on the probability of display unit transitioning into a forbidden state during intended operation, when only in-built diagnostic tools are used.

In order to solve this problem, let us use theorem that states that the probability of system transition from the specific i-th initial non-hazardous state into any hazardous state f is defined by formula [5]

$$b_{if} = \frac{\sum_{f\in\bar{S}p}\sum_{k} l_k^{if}\,\Delta G_k^f}{\Delta G_{\bar{S}p}},$$

where l_k^{if} is the k-th path leading from a non-hazardous state of graph i into a hazardous state f;

ΔG_k^f is the weight of graph resolution without the f-th node and graph nodes situated on the k-th path;

$\Delta G_{\bar{S}p}$ is the weight of graph resolution without the nodes of the hazardous state set.

Let us set forth the following topological concepts used in mathematical simulation [3]:

- *path* is a chain of series-connected unidirectional edges with the beginning in the state i and the end in the state j, the path weight being

$$l_k^{ij} = \prod_{i,r,j\in S} p_{ir}\,p_{rj},$$

where p_{ir} is the probability of one-step transition from state i into state r;

p_{rj} is the probability of one-step transition from state r into state j;

- *closed circuit* is a chain of series-connected unidirectional edges, in which the output of the final node in the circuit is connected to the initial node of the circuit. The weight of the j-th circuit is identified by the formula:

$$C_j = \prod_{i,j\in S} p_{ij}\,p_{ji};$$

- *loop* is a case of closed circuit, in which the incoming and outgoing edges merge into one edge, the weight of a loop is $C_j = p_{ij}$;

- *graph resolution* is a part of a graph that does not contain defined nodes and connected edges; the weight of resolution ΔG^i is calculated subject to the exclusion of node i and connected edges out of the graph; the weight of resolution $\Delta G_{\bar{S}p}$ is calculated subject to the additional exclusion of nodes of set $\bar{S}_p$ and connected edges out of the graph; the weight of resolution ΔG_k^f is calculated subject to the exclusion of node f out of the graph, as well as the nodes situated in the k-th path from the initial node to f and connected edges;

- the *weight of resolution* is found using Mason’s formula:

$$\Delta \mathrm{G} = 1 - \sum_{j} C_j + \sum_{rj} C_r \cdot C_j - \sum_{irj} C_i \cdot C_r \cdot C_j + \dots$$

In order to evaluate the efficiency of introducing pre-trip diagnostics, let us calculate the conditional probability of transition from the initial state “1” into the forbidden state “6”, provided that the inbuilt diagnostic tools (internal diagnostics) are disabled (paths $S1 \rightarrow S2 \rightarrow S6$ and $S1 \rightarrow S2 \rightarrow S3$).

In accordance with the theorem for evaluation of the probability of system transition from the initial allowed state into a forbidden state, the conditional probability of transition from $S1$ to $S6$ is defined with the formula:

$$b_{16/\bar{S}_{126}} = \frac{\sum_{f\in\bar{S}p}\sum_{k} l_k^{16}\,\Delta G_k^6}{\Delta G_{\bar{S}p}}.$$

As it can be seen in the graph in Figure 2b, the number k of transition paths from $S1$ to $S6$ - provided that display unit failure detection relies only on pre-trip diagnostics of the display unit by the driver or service personnel - equals 1.

Identification of path weights: $l_1^{16} = S1 \rightarrow S4 \rightarrow S6 = p14 \cdot p46$.

Identification of circuit weights:

$C1$: $S1 \rightarrow S1$, circuit weight is $p11$;

$C2$: $S1 \rightarrow S2 \rightarrow S1$, circuit weight is $p12 \cdot p21$;

$C3$: $S1 \rightarrow S2 \rightarrow S3 \rightarrow S1$, circuit weight is $p12 \cdot p23 \cdot p31$;

$C4$: $S1\to S4\to S1$, circuit weight is $p14\cdot p41$;

$C5$: $S1\to S4\to S5\to S1$, circuit weight is $p14\cdot p45\cdot p51$;

$C6$: $S6\to S6$, circuit weight is $p66$.

For the considered case, the weight of graph resolution without the nodes of the forbidden state set equals: $\Delta G_{\bar{S}p} = 1 - (C1+C2+C3+C4+C5)$.

The weight of resolution accounting for the exclusion of node "6" out of the graph, as well as the nodes situated in the k-th path from node "1" to node "6" and connected edges equals to: $\Delta G_1^6 = 1$.

By substituting data from Table 1 we obtain the conditional probability of transition from state $S1$ to state $S6$:

$$b_{16/\bar{S}_{126}} = \frac{\sum_{f\in\bar{S}p}\sum_k l_k^{16}\Delta G_k^6}{\Delta G_{\bar{S}p}} =$$

$$= \frac{p14 * p46 * \Delta G_1^6}{1 - C1 - C2 - C3 - C4 - C5} = 0,53.$$

As the considered models describe a complete group of events, the probability of hitting the only forbidden state is in both cases 1. Thus, based on the calculated value of conditional probability $b_{16/\bar{S}_{126}}$, we conclude that adding pre-trip diagnostics of the display unit by the driver or service personnel allows reducing the probability of the display unit transitioning into a forbidden state during the trip more than twice (from 1 to 0.47).

Conclusion

This paper shows the efficiency of adding pre-trip diagnostics of the display unit by the driver or service personnel to the inbuilt tools for diagnosing failures in the display unit. Thus, the probability of a system's transition into a forbidden state, i.e. a state when the failure will not be detected by the inbuilt or additional diagnostic tools, will be reduced more than twice.

Acknowledgement

The authors express their gratitude to Prof. Igor B. Shubinsky, Doctor of Engineering, for his assistance, valuable advice and observations that contributed to this paper.

References

[1] Ivnitsky V.A. Modelirovaniye informatsionnykh sistem zheleznodorozhnogo transporta. Uchebnoye posobiye [Simulation of information systems of the railway industry. Study guide]. Moscow: MIIT; 2011 [in Russian].

[2] Shubinsky I.B. Funktsionalnaya nadezhnost informatsionnykh sistem: Metody analiza [Functional dependability of information systems. Analysis methods]. Moscow: Dependability Journal; 2012 [in Russian].

[3] Shubinsky I.B. Nadiozhnie otkazoustoychivie informatsionnie sistemy. Metody sinteza [Dependable failsafe information systems. Synthesis methods]. Moscow: Dependability Journal; 2016 [in Russian].

[4] Shubinsky I.B. O poniatii funktsionalnoy nadezhnosti [On the concept of functional dependability]. Dependability 2012;4:74-84 [in Russian].

[5] Shubinsky I.B. Methods of software functional dependability assurance. Dependability 2014;4:95-101.

[6] Shubinsky I.B., Zamyshlyaev A.M., Pronevich O.B. Graph method for evaluation of process safety in railway facilities. Dependability 2017;17(1):40-45.

[7] Pronevich O.B., Shved V.E. Algorithm of calculation and forecasting of functional safety indicators of railway power supply systems. Dependability 2018;18(3):46-55.

[8] Rozenberg E.N., Penkova N.G., Korovin A.S. Functional dependability of the display unit software of the BLOK system. Dependability. 2017;17(2):36-40.

[9] Shukhina E.E., Astrakhan V.I. Bezopasny lokomotivny obiedinenny kompleks BLOK [BLOK vital integrated onboard system]. Moscow; 2013 [in Russian].

[10] Zorin V.I., Astrakhan V.I. Unifitsirovannoe kompleksnoe lokomotivnoe ustroystvo bezopasnosti (KLUB-U) [Standardized integrated onboard train protection system (KLUB-U)]. Moscow: Training and Methodology Centre for Railway Transport; 2008 [In Russian].

[11] GOST R IEC 61508–7–2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 7. Techniques and measures. Moscow: Standartinform; 2014 [in Russian].

About the authors

Efim N. Rozenberg, Professor, Doctor of Engineering, First Deputy Director General, JSC NIIAS Russia, Moscow, e-mail: info@vniias.ru

Alexander S. Korovin, Chief Specialist of Computer-Based Devices Development Sector, JSC NIIAS, Russia, Moscow, e-mail: A.Korovin@vniias.ru

Natalia G. Penkova, Deputy Head of Safety and Algorithmic Support, JSC NIIAS, Russia, Moscow, e-mail: N.Penkova@vniias.ru

Received on 08.04.2019