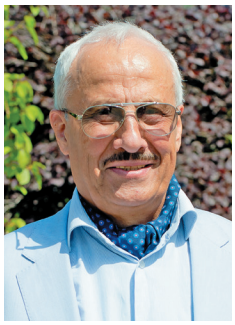
Original article
https://doi.org/10.21683/1729-2646-2021-21-4-31-37

On the safety assessment of an automatic train operation system

Igor B. Shubinsky[1]*, Hendrik Schäbe[2], Efim N. Rozenberg[1]
[1]JSC NIIAS, Moscow, Russian Federation
[2]TÜV Rheinland, Germany, Cologne
**igor-shubinsky@yandex.ru*


Igor B. Shubinsky


Hendrik Schäbe


Efim N. Rozenberg

Abstract. *The paper examines the automatic train operation system as part of the locomotive control and protection system, the remote supervision centre's means for control of onboard and trackside machine vision facilities. The focus is on the dependence of the system's safety and dependability on the dependability characteristics of its components and adverse weather effects. The criteria of a system's wrong-side and right-side failures were defined, the graph models were constructed of the safety and dependability states of an automatic train operation system. The Markovian graph method of calculating the safety and dependability of complex systems was substantiated. That allowed defining such key safety indicators of an automatic train operation system as the mean time to wrong-side failure, probability of wrong-side failure, wrong-side failure rate. The study established that the safety of an automatic train operation system primarily depends on the dependability of machine vision facilities. The growth of the system's wrong-side failure rate is limited to half the failure rate of machine vision facilities. It was also established that the dependability of an automatic train operation system is defined by the failure rate of a locomotive control and protection system and the failure rate of machine vision facilities. The conducted analysis allows concluding that in order to achieve an acceptable level of safety of an automatic train operation system, efforts should focus on machine vision redundancy, ensuring the SIL4 functional safety of on-board and trackside machine vision facilities, as well as regular comparison of the outputs of on-board and trackside machine vision facilities, redundant output comparison, integration of the outputs in motion. Additionally, adverse weather effects are to be countered by improving the efficiency of machine learning of the machine vision software.*

Keywords: *automatic train operation system, machine vision, safety, dependability, Markovian model, state graph, hazardous failure, right-side failure.*

For citation: *Shubinsky I.B., Shäbe H., Rozenberg E.N. On the safety assessment of an automatic train operation system. Dependability 2021;4: 31-37. https://doi.org/10.21683/1729-2646-2021-21-4-31-37*

Received on: *27.07.2021* / **Revised on:** *16.11.2021* / **For printing:** *14.12.2021.*

1. Introduction

Ensuring the safety of a complex technical system, in which information is processed using neural networks, requires special methods of safety case preparation [1].

The primary problem associated with the development of such method consists precisely in the fact that the above computer system is unstable in terms of the structure of the information processing algorithm, and classical methods of probabilistic estimation in the form of two and more independent hardware and software information processors, application of different software products in the processors, etc. [2] are difficult to use as part of the safety case preparation.

That is why redundant information processors in the form of onboard machine vision cameras for safe obstacle detection are unlikely to achieve the required safety level due to the unknown testing time of such self-trained, i.e., ever-changing, system for vital information processing.

Braband and Shäbe [1] intended to use statistical methods for safety case preparation, as well supposed the obligatory inclusion in the processing system of an additional device, whose safety could be proven by conventional means due to its unchanging structure.

Shubinsky and Rozenberg [3, 4] proposed using the so-called multi-level structures for safety case preparation that allow integrating safe systems and information systems with the introduction of the information processing criterion subject to the safety requirements. This approach has shown good results in the development of advanced onboard and trackside safety systems. An extremely important property of system safety evaluation was also used, i.e., obtaining reliable information on a facility's background in terms of safety.

For the purpose of safety case preparation of an intelligent system with a neural network, the principles of multi-level safety system should be used. The difference is that, in this case, the focus should be not on an individual intelligent device, i.e., an onboard machine vision camera, but on an entire system of technical assets within the locomotive's area of operation.

Indeed, the operation of a locomotive camera with a pre-designed software for processing obstacle information depends not only on the prior measures aimed at training the neural network, but also on specific factors that affect the operation of the camera hardware, software faults, etc. In addition, it should be noted that the effects of the external environment, i.e., snow, fog, rain, cause changes within the obstacle acquisition area, which directly affects safety, as it is associated with the length of the trains' braking path.

In this context, the situation ahead of the train is additionally monitored from the special control centre, where an operator driver supervises several locomotives [5].

The difficulty of this method consists in the fact that the critical component is the operator driver's response that, in turn, depends on the stability of the video image transmission from the onboard camera and the dependability of the broadband radio communications in a particular location.

On the other hand, dividing the information processing into two sub-processes (in the form of internal intelligent processing of information onboard for the purpose of decision-making on the track vacancy and in the form of communication of the original visual information to the operator driver for decision-making) allows improving safety. The criterion in this case is that the onboard system should have a high probability of false alarm, while the operator driver can rectify this situation using a special command transmitted to the locomotive by radio. In practice, if this principle was not used, driverless systems would stop, for instance, because of a plastic bag on the track.

It should be noted that the system includes trackside devices that supervise track vacancy in places with poor visibility [5]. Information from those trackside systems is communicated to the locomotive in real time, which greatly improves train safety. Thus, the used model is simplified, but it enables an analytical study of the problem. That constitutes the superiority of this approach to the construction of the research model as compared to more complex models. An interesting feature of the interaction between trackside and onboard machine vision assets is that, under the same environmental conditions, they can see the same objects either in the line of sight, or from different, including inverse, observation points.

The existence of objects acquired by two independent systems allows using this feature for cross-supervision of intelligent equipment, especially for the purpose of development of correct solutions by onboard intelligent systems that operate in more severe operating conditions (speed of movement, visibility limitations, etc.). The object comparison output can have the form of a comparison of images processed by trackside and onboard cameras represented as pre-processed image models, or it can contain an assumed inversion of the image of the same object if it is aimed by machine vision cameras from opposite points. This predefined feature of the output comparison safety system enables an improved independence of information processing. Each technical asset, including video cameras, contains elements of internal testing as a prerequisite factor when calculating their level of safe operation. Given that a comprehensive testing of an intelligent system with a neural component is a difficult matter, self-diagnosis using predefined observation objects should be employed. For instance, near the railway tracks, within the area covered by machine vision cameras or lidars, there are traffic lights, control cabinets, power and communication masts that are clearly associated with the linear coordinates, moreover if the locomotive uses a 3D map of the infrastructure assets.

Thus, the acquisition of such assets actually allows testing onboard cameras and sensors taking into account the parameters of detection distance and type of asset identification. If the rate of acquisition of such objects is high enough, then, for the distance of the locomotive's movement between these points, the probability of no failure or distortion of the information processing algorithm onboard can be calculated. The advantage of such method is the completeness of information

processing, when, along the internal hardware testing, the required level of system safety can be achieved. The system itself in this case is a "black box", but with absolutely known outputs within an absolutely known space coordinate.

2. Conceptual safety model of an automatic train operation system

An automatic train operation system includes the following key facilities:

- onboard train control and protection equipment;
- supervision centre equipment;
- trackside machine vision facilities;
- onboard machine vision facilities.

The conceptual safety model of an automatic train operation system contains a description of the dependability and safety states of the system's component facilities, their interrelations, as well as the effects of adverse weather conditions. This model is presented in the form of a system safety state graph (Fig. 1).

For the purpose of system safety model construction, the following criterion of **wrong-side failure** is adopted: the failure of machine vision facilities and the remote supervision centre or undetected failure of the locomotive's control and protection system. Criterion of **right-side failure**: the failure of trackside machine vision facilities, remote supervision centre and adverse weather effects or detected failure of the locomotive's control and protection system.

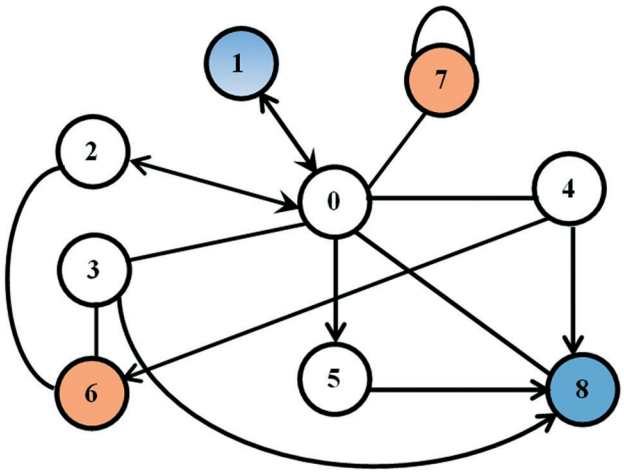


Fig. 1. State graph of the safety of an automatic train operation system

Graph states:

0 – good state, no adverse weather effects;

1 – detected failure of the locomotive control and protection system – **right-side failure;**

2 – failure of remote supervision centre equipment;

3 – failure of trackside machine vision facilities;

4 – failure of onboard machine vision facilities;

5 – adverse weather effects;

6 – failure of all machine vision facilities and the supervision centre – **wrong-side failure** of the automatic train operation system;

7 – undetected failure of the locomotive control and protection system – **wrong-side failure;**

8 – failure of trackside machine vision facilities, supervision centre and adverse weather effects – **right-side failure.**

The whole set of system states – according to the state graph in Fig. 1 – is divided into the following subsets:

– subset of up states S_U={0, 2, 3, 4, 5};

– subset of protective states S_P={1, 8};

– subset of hazardous states S_H={6, 7};

The up and protective states form the set of good states.

Given below are the model's good state transitions that need clarification: 1-0, 2-0, 3-0, 8-0, equipment restorations after failure; 3-8, failure of the supervision centre equipment on condition of failure of trackside machine vision facilities; 4-8, failure of the supervision centre equipment on condition of failure of onboard machine vision facilities; 7-8, failure of trackside machine vision facilities on condition of adverse weather effects.

The mathematical description of the model will be based on the following considerations. The system is new and unique, no statistical information about it is available. Therefore, the system's random values distribution laws are not established. Based on the existing experience in railway control systems, it can be safely assumed that failures of such electronic devices, as the locomotive control and protection system, supervision centre equipment and machine vision facilities, are exponentially distributed. This assumption does not apply to random values of time to device restoration after failures, much less to random adverse weather effects. The problem of disturbing effects was theoretically examined by Schäbe and Viertl in [6]. Those models are also applicable to adverse weather effects. In order to ensure adequate results, the authors were forced to use a complex mathematical description of the random process of adverse effects on the locomotive's control system. The above circumstances complicate their practical application in mathematical simulation of the safety of the automatic train operation system.

In the absence of practical information, it is very difficult to predict the quantitative safety indicators of the automatic train operation system. In this paper, in the context of great uncertainty, we aim to identify the most significant factors affecting the system's safety. The assumption of the simplest flows of random events in the automatic train operation system fits this purpose. The simplest flows are ordinary, stationary and have no aftereffect. Due to the great uncertainty of the initial conditions their application, on the one hand, does not favour an accurate prediction of the safety characteristics of the system's behaviour. On the other hand, the resulting outputs can be considered as prerequisites guaranteed from below (as the worst case) to the construction of a safe automatic train operation system through neutralization of the most significant identified negative factors. Thus, the used model is simplified, but it enables the analysis of the problem. That constitutes the advantage of this approach over more complex models.

Based on the above assumptions, let us adopt an exponential distribution of failures $F_i(t)$ and restorations $Q_i(t)$ of equipment components:

$$F_i(t) = 1–\exp(–\lambda_i t),\ i = 1...4;\ Q_i(t) = 1–\exp(–\mu_j t),$$

where λ_1 is the failure rate of the locomotive control and protection system;

λ_2 is the failure rate of the supervision centre equipment;

λ_3 is the failure rate of the trackside machine vision facilities;

λ_4 is the failure rate of the onboard machine vision facilities;

μ_1 is the restoration rate of the locomotive control and protection system;

μ_2 is the restoration rate of the supervision centre equipment;

μ_3 is the restoration rate of the onboard machine vision facilities;

μ_4 is the restoration rate of the trackside machine vision facilities and supervision centre equipment.

It is assumed that a failure of the locomotive control and protection system is detected with the probability of correct detection α. A possibility of non-detection of a failure of the locomotive's system exists and is $\bar{\alpha} = 1-\alpha$. The probability of false detection is negligible.

Based on the above assumptions, let us assume that the law of distribution of random adverse weather conditions has the form of $H(t)=1–\exp(–\gamma t)$, where γ is the rate of their effect on the safety of the automatic train operation system.

Under the above assumptions, the safety-specific behaviour of the automatic train operation system is represented by a Markov process.

For that purpose, we find the input parameters of the system safety model in the subsets of good (up and protective) states according to the graph in Fig. 1.

The distribution functions of the unconditional good time of the system presented with the state graph in Fig. 1 are as follows:

$$F_0(t) = 1-\exp\left(-\left[\gamma + \sum_{i=1}^{4}\lambda_i\right]\cdot t\right);\ F_1(t)=1–\exp(–\mu_1 t);$$

$$F_2(t)=1–\exp(–[\lambda_3+\mu_2]\cdot t);\ F_3(t)=1–\exp(–[\lambda_2+\lambda_4+\mu_3]\cdot t);$$

$$F_4(t)=1–\exp(–[\gamma+\lambda_2]\cdot t);$$

$$F_5(t)=1–\exp(–\lambda_4 t);\ F_8(t)=1–\exp(–\mu_4 t). \qquad (1)$$

Hazardous states 6 and 7, as well as the edges that are part of those states, are excluded from the mathematical description as the study covers the behaviour of the automatic train operation system before it enters hazardous states.

The mathematical expectations of the system's good times are as follows:

$$T_0 = \int_0^\infty \left(1-F_0(t)\right)dt = \frac{1}{\gamma + \sum_{i=1}^{4}\lambda_i};\ T_1 = \int_0^\infty e^{-\mu_1 t}dt = \frac{1}{\mu_1};$$

$$T_2 = \int_0^\infty e^{-\lambda_3 t}e^{-\mu_2 t}dt = \frac{1}{\lambda_3+\mu_2};$$

$$T_3 = \int_0^\infty e^{-\lambda_2 t}\cdot e^{-\lambda_4 t}\cdot e^{-\mu_3 t}dt = \frac{1}{\lambda_2+\lambda_4+\mu_3};$$

$$T_4 = \int_0^\infty e^{-\gamma t}e^{-\lambda_2 t}dt = \frac{1}{\gamma+\lambda_2};$$

$$T_5 = \int_0^\infty e^{-\lambda_4 t}dt = \frac{1}{\lambda_4};\ T_8 = \int_0^\infty e^{-\mu_4 t}dt = \frac{1}{\mu_4}. \qquad (2)$$

The probability of transitions between states i, j of the system is identified using formula $p_{ij} = \int_0^\infty \lambda_{ij}[1-F_i(t)]dt$, where λ_{ij} is the rate of the system's transition from state i to state j. For example, the rate of transition from initial state 0 to state 1 (Fig. 1) of detected failure of the locomotive control and protection system is $\lambda_{01}=\alpha\cdot\lambda_1$, whereas the rate of transition from state 0 to state 7 of the system's undetected failure (hazardous system failure) is calculated as $\lambda_{07} = \bar{\alpha}\cdot\lambda_1$.

Thus,

$$p_{01} = \frac{\alpha\lambda_1}{\gamma + \sum_{j=1}^{4}\lambda_j};\ p_{0i} = \frac{\lambda_i}{\gamma + \sum_{j=1}^{4}\lambda_j},\ i = 2,3,4;$$

$$p_{05} = \frac{\gamma}{\gamma + \sum_{j=1}^{4}\lambda_j};\ p_{10} = p_{58} = p_{80} = 1;\ p_{20} = \frac{\mu_2}{\lambda_3+\mu_2};$$

$$p_{30} = \frac{\mu_3}{\lambda_2+\lambda_4+\mu_3};\ p_{38} = \frac{\lambda_2}{\lambda_2+\lambda_4+\mu_3};\ p_{48} = \frac{\gamma}{\lambda_2+\gamma}. \qquad (3)$$

3. Results of the analysis of the safety indicators of the automatic train operation system

Using Shubinsky's Markovian graph method of calculating the safety of complex systems [7], such key safety indicators of an automatic train operation system as the mean time to wrong-side failure T_{WS}, the probability of wrong-side failure $G_{WS}(t)$, wrong-side failure rate λ_{WS} can be identified.

The key safety indicator, mean time to wrong-side failure T_{WS} is identified using method [8] according to formula

$$T_{WS} = \frac{T_1\Delta G^1_{S_{WS}} + \sum_{(k)}\sum_{i,j} l^{ij}_k \Delta G^j_k T_j}{\Delta G_{S_{WS}}}, \qquad (4)$$

where $\Delta G^1_{S_{WS}}$ is the weight of the expansion of the graph without the initial node 1 and set of hazardous states $S_{WS}=\{6,7\}$ and associated graph edges; $\Delta G_{S_{WS}}$ is the weight of the expansion of the graph without the set of hazardous states and associated graph edges; l^{ij}_k is the weight of the k-th path from node i to node j; ΔG^j_k is the weight of the expansion of the graph without the nodes situated on the

k-th path and without node *j* in the set of non-hazardous states $S_{NH}=\{0,1,2,3,4,5,8\}$.

The expansion weights can be defined using Mason's gain formula [8]

$$\Delta G = 1 - \sum_i C_i + \sum_{ij} C_i C_j - \sum_{ijk} C_i C_j C_k + ...,$$

where the weights of boundaries are found within the set of non-hazardous states (Fig. 1)

$$C_1=p_{01}{:}p_{10};\ C_2=p_{02}{:}p_{20};\ C_3=p_{03}{:}p_{30};\ C_4=p_{03}{:}p_{38}{:}p_{80};$$
$$C_5=p_{04}{:}p_{48}{:}p_{80};\ C_6=p_{05}{:}p_{58}{:}p_{80}. \quad (5)$$

All boundaries intersect, since they have a common node 0.

According to the graph in Fig. 1 and substituting expressions (1), (2), (3) into formula (4), we find within the set of non-hazardous states $S_{NH}=\{0,1,2,3,4,5,8\}$

$$T_{\text{WS}} = \frac{T_0 + \sum_{i=1}^{5} p_{0i} T_i + (p_{03}p_{38} + p_{04}p_{48} + p_{05}p_{58}) \cdot T_8}{\Delta G_{S_{\text{WS}}}}, \quad (6)$$

where the expansion weight of the graph without the hazardous states $\Delta G_{S_{\text{WS}}} = 1 - \sum_{i=1}^{6} C_i$ and the weight of the boundaries is calculated using formula (5).

Since, in actual control systems, between the rates of restorations and failures of electronic equipment the correlation is $\lambda_i << \mu_i$, with an error not exceeding the first order of smallness, the explicit expressions of the model's initial parameters can be significantly simplified. It is to be taken into account that the recovery rates of such trackside electronic assets as the supervision centre and machine vision facilities, are almost identical and deviations of tens of percentage points do not significantly affect the final results in the context of the above ratio between the failure and restoration rates. Then, $\mu_2=\mu_4=\mu$ and $\mu_1=\mu_3=k\mu$, $(0<k\leq 1)$, where *k* is the coefficient of logistical delays of restoration of onboard assets of the automatic train operation system.

The above changes in the initial parameters apply to the distribution functions $F_1(t) \cong 1-\exp(-k\mu \cdot t)$, $F_2(t) \cong 1-\exp(-\mu \cdot t)$, $F_3(t) \cong 1-\exp(-k\mu \cdot t)$, expectations $T_2 \cong \frac{1}{\mu}$ and $T_1 \cong T_3 \cong \frac{1}{k\mu}$, transition probabilities $p_{20} \cong p_{30} \cong 1$, $p_{38} \cong \frac{\lambda_2}{k\mu}$.

Indeed, according to NPRD-2011 camera sub-assembly [9], the failure rate of the machine vision facilities is to be $\lambda_2 = \lambda_4 = 2{,}3 \cdot 10^{-5}$ and $\lambda_3 = 2{,}8 \cdot 10^{-5}$ for the supervision centre. According to EN 50129 [10], the failure rate of the locomotive control and protection system must be SIL4, i.e., $\lambda_1 \leq 10^{-8}$. According to IEC 61508-2 (A4, first line) [12], the probability of non-detection of failure is to be less than $\overline{\alpha} \leq 0{,}01$. In most cases, the restoration rate of the electronic programmable equipment of the automatic train operation system exceeds $\mu \geq 2$, which is higher than the failure rate by four or more orders of magnitude. This allows – within an acceptable margin of error – excluding from the explicit expression those terms of the sum that are several orders of magnitude smaller than the other terms.

The above considerations allow developing the explicit expression (6) of the mean time to wrong-side failure of the automatic train operation system to an acceptable applied mathematical expression

$$T_{\text{ws}} = \frac{\frac{k\mu + \alpha\lambda_1 + \lambda_3 + k(\lambda_2+\lambda_4)}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)k\mu} + \frac{\gamma}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)\lambda_4} + \left[\frac{\lambda_3 \cdot \lambda_2}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)k\mu} + \frac{\lambda_4 \cdot \gamma}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)(\lambda_2+\gamma)} + \frac{\gamma}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)}\right] \cdot \frac{1}{\mu}}{\Delta G_{S_{\text{WS}}}},$$

where

$$\Delta G_{S_{\text{WS}}} = 1 - p_{01}p_{10} - p_{02}p_{20} - p_{03}p_{30} - p_{03}p_{38}p_{80} - p_{04}p_{48}p_{80} - p_{05}p_{58}p_{80} \cong 1 - \frac{\alpha\lambda_1 + \lambda_2 + \lambda_3 + \gamma}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)} - \frac{\lambda_3}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)}\frac{\gamma}{(\gamma+\lambda_2)} - \frac{\lambda_4}{\left(\gamma + \sum_{i=1}^{4}\lambda_i\right)}\frac{\lambda_2}{k\mu}. \quad (7)$$

Upon transformation of formula (7), we deduce that – with an error not exceeding the first order of smallness – the mean time to wrong-side failure of the automatic train operation system can be represented as

$$T_{\text{WS}} \cong \frac{\lambda_4(\gamma + \lambda_2 + \lambda_4) + \gamma \cdot (\gamma + \lambda_2)}{\lambda_4(\overline{\alpha} \cdot \lambda_1 + \lambda_4)(\gamma + \lambda_2)}, \quad (8)$$

The limit value of the time to wrong-side failure of an automatic train operation system occurs in the absence of adverse weather effects ($\gamma \to 0$) and when compliance with IEC 61508-2 [11] ($\alpha \to 0$) is ensured. By substituting these values into formula (8), we deduce the output of the mathematical simulation. It indicates that the safety of an automatic train operation system primarily depends on the dependability of the machine vision facilities, i.e.,

$$T_{\text{LIM}} \leq \frac{\lambda_2 + \lambda_4}{\lambda_2\lambda_4} = \frac{1}{\lambda_4} + \frac{1}{\lambda_2}.$$

If the failure rate values of the trackside and onboard machine vision facilities are close, this expression modifies into

$$\lambda_2 \cong \lambda_4 = \lambda; \text{ therefore } T_{\text{LIM}} \leq \frac{2\lambda}{\lambda^2} = 2 \cdot T,$$

where *T* is the mean time to failure of the machine vision facilities.

As the system's flow of wrong-side failures is multiply rarefied in relation to the right-side failure flow of the initial

item that is a simplest one, then, according to [12, 13] a multiply rarefied, irregularly simplest failure flow is also a simplest one with constant parameter

$$\lambda_{WS} = 1/T_{WS} = \frac{\lambda_4(\bar{\alpha}\cdot\lambda_1 + \lambda_4)(\gamma + \lambda_2)}{\lambda_4(\gamma + \lambda_2 + \lambda_4) + \gamma(\gamma + \lambda_2)}. \quad (9)$$

In the limit, the rate of wrong-side failures of the automatic train operation system tends to

$$\lambda_{WS} \to \frac{\lambda_2 \cdot \lambda_4}{\lambda_2 + \lambda_4} \cong \frac{\lambda}{2}(\lambda_2 \approx \lambda_4), \quad (10)$$

i.e., half of the failure rate of the machine vision facilities.

The probability of wrong-side failure with an error not exceeding the first order of smallness is defines as

$$G_{WS}(t) \cong \lambda_{WS} \cdot t \to \frac{\lambda}{2}t.$$

4. Results of the analysis of the dependability indicators of the automatic train operation system

The dependability model of the automatic train operation system is transformed from the conceptual safety model of such system (Fig. 1) by eliminating hazardous states and associated edges. The state graph of the dependability model is shown in Fig. 2.

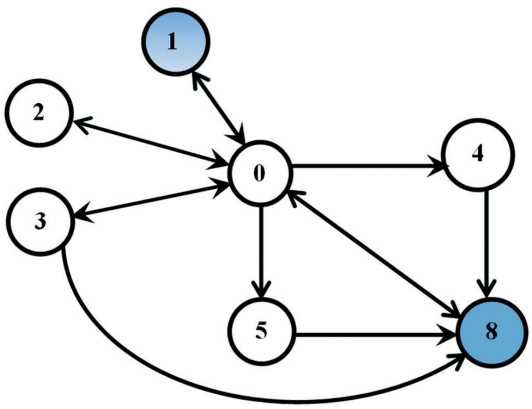


Fig. 2. State graph of the dependability of an automatic train operation system

For the purpose of the system's dependability analysis, let us restrict ourselves to the definition of the mean time of it being in the set of up states $S_U = \{0, 2, \rightleftarrows 3, 4, 5\}$. This indicator is none other than the system's mean time to right-side failure. This indicator is to be analysed due to the fact that improving safety involves bringing the system into the safe (non-operational) state in every alarm case, whenever possible. It is therefore important to identify which factors affect the dependability of a system with machine vision in the course of its design according to this architecture.

Using the graph in Fig. 2 and method [7] we deduce

$$T_{RS} = \frac{T_0 + p_{02}T_2 + p_{03}T_3 + p_{04}T_4 + p_{05}T_5}{1 - p_{02}p_{20} - p_{03}p_{30}}.$$

Under the assumptions of Items 2 and 3, this expression transforms into

$$T_{RS} = \frac{(\lambda_2 + \gamma)(\lambda_4 + \gamma) + \lambda_4^2}{\lambda_4(\lambda_2 + \gamma)(\lambda_1 + \lambda_4 + \gamma)} + \frac{\lambda_2\mu_3 + \lambda_3\mu_2}{\mu_2\mu_3(\lambda_1 + \lambda_2 + \gamma)}. \quad (11)$$

As noted above in Item 2, in accordance with NPRD-2011 camera sub-assembly [9], the failure rate of the machine vision facilities is to be $\lambda_2 = \lambda_4 = 2{,}3\cdot10^{-5}$ and that of the supervision centre is to be $\lambda_3 = 2{,}8\cdot10^{-5}$. Therefore, $\lambda_2 \cong \lambda_3 \cong \lambda_4 = \lambda$ can be assumed without noticeable loss of evaluation accuracy. In addition, the machine vision and supervision centre equipment overwhelmingly contain electronic assets whose restoration rate is about the same $\mu \geq 2$. Therefore, we can assume that $\mu_2 \cong \mu_3 = \mu$ and expression (11) modify into

$$T_{RS} = \frac{(\lambda + \gamma)^2 + \lambda_4^2}{\lambda(\lambda + \gamma)(\lambda_1 + \lambda + \gamma)} + \frac{2\lambda}{\mu(\lambda_1 + \lambda + \gamma)}. \quad (12)$$

As with the system's safety assessment, let us assume that the limit value of time to right-side failure of the automatic train operation system takes place in the absence of adverse weather effects ($\gamma \to 0$). Then, formula (12) will modify into

$$T_{RS} \to \frac{2}{\lambda_1 + \lambda}\left(1 + \frac{\lambda}{\mu}\right).$$

As noted in Item 2, for the purpose of the problem at hand, $1 >> \frac{\lambda}{\mu}$. Given the above, we deduce the marginal estimate of dependability of the automatic train operation system in terms of mean time to right-side failure:

$$T_{RS} \to \frac{2}{\lambda_1 + \lambda}. \quad (13)$$

Consequently, the dependability of an automatic train operation system is defined by the failure rate of the locomotive control and protection system (λ_1) and the machine vision facilities (λ). These components of the automatic train operation system must be the focus of attention in the context of ensuring an acceptable level of the system's dependability.

5. Conclusion

The above analysis allows concluding that in order to achieve an acceptable level of safety of the automatic train operation system, the efforts should focus on the following:

– redundancy of machine vision facilities;

– ensuring the SIL4 functional safety of onboard and trackside machine vision facilities (dual channel and dual versioning of software, use of independent channels, etc.);

– regular comparison of the outputs of onboard and trackside machine vision facilities, redundant output comparison, integration of the outputs in motion.

Additionally, it is required to ensure compliance with EN 50129 in terms of SIL4 functional safety of the locomotive control and protection system. Adverse weather effects should also be countered by increasing the efficiency of machine learning of the machine vision software.

The study confirmed that the reliability of the locomotive control and protection system has a decisive effect on the dependability of the automatic train operation system.

References

1. Braband J., Shäbe H. On safety assessment of artificial intelligence. *Dependability* 2020;20(4):25-34.

2. Sapozhnikov V.V., Sapozhnikov Vl.V., Khristov Kh.A., Gavzov D.V. Sapozhnikov Vl.V., editor. [Design methods of vital computer-based railway automatics]. Moscow: Transport; 1995. (in Russ.)

3. Shubinsky I.B. [Dependable failsafe information systems. Synthesis methods]. Moscow: Dependability Journal; 2017. (in Russ.)

4. Rozenberg E.N. [Multi-level train control and protection system: Doctor of Engineering thesis]. Moscow State University of Railway Engineering (MIIT). Moscow; 2004. (in Russ.)

5. Mylnikov P.D., Okhotnikov A.P., Popov P.A. Patent 2742960. Russian Federation, IPC B61L 25/02. [Onboard information system]: no. 2020131633; application 25.09.2020; published 12.02.2021; bulletin no. 5. (in Russ.)

6. Schäbe H., Viertl R. An Axiomatic Approach to Models of Accelerated Life Testing. Eng. Fract. Mechanics 1995;50(2):203-217.

7. Shubinsky I.B. [Structural dependability of information systems. Analysis methods]. Moscow: Dependability Journal: 2012. (in Russ.)

8. Mason S.J. Feedback theory – Further properties of signal flow graphs: Proceedings of the IRE;44:920-926. doi:10.1109/jrproc.1956.275147.

9. NPRD-2011. Nonelectronics Parts Reliability Data. Reliability Information analysis. Expert Center; 2011.

10. EN 50129 Railway applications – Communication, signalling and processing system – Safety related electronic systems for signalling; 2018.

11. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. Parts 1 – 7; 2011.

12. Grigelionis B.I. [On the accuracy of Poisson approximation of a composition of recovery processes]. *Litovsky matematichesky sbornik* 1962;2(2):135-143. (in Russ.)

13. Nazarov A.A., Lopatin I.L. [Asymptotic Poisson MAP flows]. *Tomsk State University Journal* 2010;4(13):72-78 (in Russ.)

About the authors

Igor B. Shubinsky, Doctor of Engineering, Professor, Deputy Director of Integrated Research and Development Unit, JSC NIIAS. Address: 27, bldg 1 Nizhegorodskaya St., 109029, Moscow, Russian Federation, phone: +7 (495) 786 68 57, e-mail: igor-shubinsky@yandex.ru.

Hendrik Schäbe, Dr. rer. nat. habil., Head of Risk and Hazard Analysis, TÜV Rheinland InterTraffic, Cologne, Germany; e-mail: schaebe@de.tuv.com.

Efim N. Rozenberg, Doctor of Engineering, Professor, First Deputy Director General, JSC NIIAS. Address: 27, bldg 1 Nizhegorodskaya St., 109029, Moscow, Russian Federation, e-mail: info@vniias.ru.

The authors' contribution

Shubinsky I.B. developed and solved the safety and dependability models of the automatic train operation system, analysed the results.

Shäbe H. analysed publications dedicated to the safety of automatic train operation systems, prepared experimental data, participated in the development of safety and dependability models of an automatic train operation system and analysis of the findings.

Rozenberg E.N. defined the research problem, participated in the development of the safety model of an automatic train operation system, participated in the analysis of the findings.

Conflict of interests

The authors declare the absence of a conflict of interests.