Original article
Dependability, vol. 21 no. 1, 2021 https://doi.org/10.21683/1729-2646-2021-21-1-38-44

On the functional safety of a complex technical control system with digital twins

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

Igor B. Shubinsky

Hendrik Schäbe

Efim N. Rozenberg

Abstract. *The* **Aim** *of this paper is to evaluate the advantages of digital twin technology as compared with the conventional approaches to the design of a vital two-channel system.* **Methods.** *The system is described with a Markovian model. This model allows defining the quantitative safety characteristics if the system is affected by right-side failures.* **Results.** *The system's primary quantitative safety indicators were identified as the mean time to wrong-side failure and mean time to right-side failure along with the quantitative relations of the prime and additional costs for a batch of products.* **Conclusion.** *Transforming the initial item into a system with digital twins allows significantly reducing the rate of wrong-side failures. This effect may be obtained not only with the use of digital twins, but also as the result of the system transitioning into the state of right-side failure in each event of discrepancy betwin the initial item and/or the digital twins. It has been established that the mean time to right-side failure under such conditions is not less than the mean time to failure of the initial item. That means that highly efficient measures for safety improvement allow maintaining the system dependability at a level not lower than that of the initial item. The introduction of digital twins into a system is a new, not yet tested way of ensuring system safety. The decision on the benefits of additional costs is taken by the customer and system developer together. At the same time, it must be taken into consideration that in case of large batches of manufactured technical systems, the effect of additional costs is reduced and the effect of significantly improved safety is maintained.*

Keywords: *digital twin, functional safety, control system*

For citation: *Shubinsky I.B., Schäbe H., Rozenberg E.N. On the functional safety of a complex technical control system with digital twins. Dependability 2021;1: 38-44. https://doi.org/10.21683/1729-2646-2021-21-1-38-44.*

Received on: *07.10.2020* / **Upon revision:** *04.02.2021* / **For printing:** *22.03.2021*

1. Introduction

The paper examines a control system that is supposed to operate with a high level of functional safety. Possible solutions for control system design are given in the IEC 61508 standard [1]. In the context of train control and/or protection systems, many recommendations regarding the functional safety of hardware and software are sets forth in the EN 50128 [2] and EN 50129 [3] standards, as well as in [4 – 10, etc.]. The key solutions consist in the application of multichannel hardware and multiversion software, which naturally causes significantly higher costs of the systems and often limits their serial use. We must note certain difficulties in terms of upgrading and modification of such system due to the requirement to redesign its redundant components subject to new needs. In railway transportation, those are due to the system's adaptation to another type of rolling stock, variation of track tonnage, change of line class, etc.

The current problem consists in designing affordable mass-producible train control and protection systems that comply with the stricter requirements for functional safety. In this paper, the feasibility is examined of designing a train control and/or protection system comprising an SIL1 or SIL2 initial item and outer circuit of digital twins designed for attaining the desired level of functional safety.

A digital twin is understood as an entity containing:

– the mathematical model of the initial item;

– the software implementation of the model that performs all the operating functions of the initial item;

– the results of model verification and proof of its adequacy to the initial system, as well as a list of hazardous and potentially hazardous states defining the allowed duration of wrong-side failures of the initial item;

– operational documentation.

As a whole, a digital twin can be represented as a complex diagnostics tool.

2. Architecture of a technical system with a digital twin

The architecture of a digital twin is shown in Fig. 1. It is somewhat similar with the architecture of a complex industrial controlled system suggested in [11], but does not repeat it.

A digital twin is generated as a computer model consisting of three interconnected levels:

• *objective* level containing the computer model of the control system hardware components involved in the implementation of the system's operation algorithm, with associated models of executive and measurement devices;

• *logical* level that contains the simulation model of the operation algorithm of the train control and/or protection system;

• *visual* level where data is visualized, user control commands are generated.

Ensuring the adequacy of the virtual model to the real railway facility is the key element of the design of a train protection system. [12] As an item, let us examine a railway signalling system. The station-based automatic block and power (computer-based) interlocking systems contain sensors that provide information on the track circuit operating parameters (voltages at the receiver inputs). Describing the operation of such sensors is in itself a complicated task, as the aim is to select an optimum out of track occupancy observation modes, broken rail detection, cab signalling strength. However, such processes are well-studied and reduced to standard requirements that ensure traffic safety. Accordingly, for the purpose of virtual modeling, their mathematical description may be used as part of predictive diagnostics of the events that constitute the continuous process of their operation. For the next level of the virtual model that represents the discrete-event operation of the simulated item, it suffices to only have the value of the process parameters exceeding the norms of operability and safety.

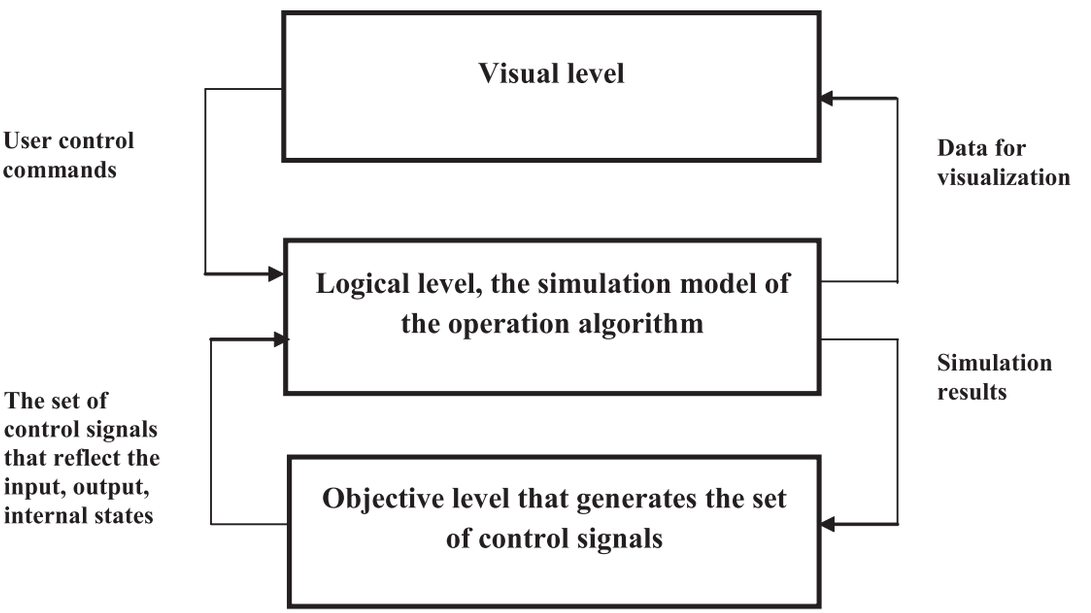

Fig. 1. Architecture of a digital twin

The discrete-event operation in the virtual model is well-represented with a discrete automaton, for which safety criteria have also been developed that are based on the monotonicity of the control functions. Similarly, the virtual model of the operation of individual rolling stock systems can be constructed. Thus, the operation of the brake line of a train in the braking mode comes down to valve opening, which causes the loss of pressure in the line and brake operation. The process itself is described by complex differential equations of airflow propagation throughout the length of the train. Estimating the consequences in terms of safety only requires to have the criteria of pressure drop in the tail car within the specified time. Given that the braking mode itself may be classified as service, full service and emergency, in the virtual model, the respective variants must be generated. It should be noted that the mechanical action of brake blocks against the wheels due to the discharging of the brake line can be described by limiting temporal characteristics that affect the length of braking.

For the next level of the virtual model, i.e., the level of train protection system description, it suffices to have the time marks of the beginning of brake valve opening and end of the train deceleration or its stopping.

Thus, the virtual model of a digital twin combines simplified continuous mathematical models of continuous processes in transformation of information and the associated discrete-event models.

The external circuit of the examined train control and/or protection system is formed by two same-type digital twins according to a dual-channel configuration with independent inputs and outputs and fail-safe comparator. The methods of designing the dual-channel configuration for the purpose of ensuring functional safety are described in the above standards.

The external circuit is connected with the initial single-channel item with an interference-immune and intrusion-protected communication channel (Fig. 2):

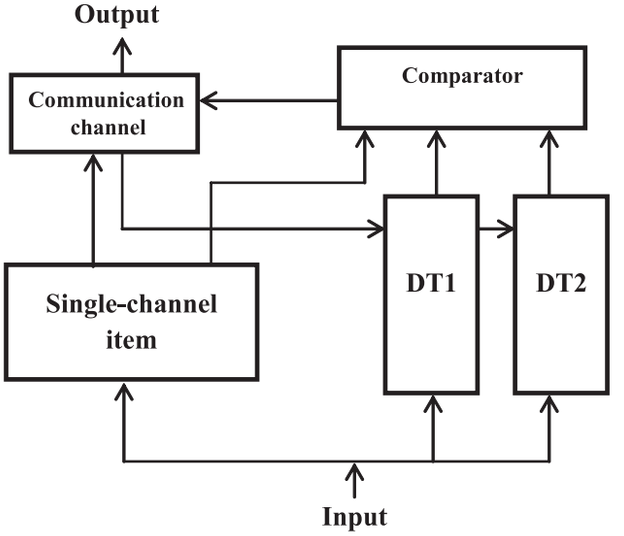

Fig. 2. Summarized structure diagram of a technical system with a digital twin

3. Efficiency estimation of a vital technical system with a digital twin

The system, whose diagram is shown in Fig. 2, falls into the category of vital technical systems (e.g., a train control and/or protection system) that is to comply with stricter requirements for functional safety. The introduction of digital twins into a vital technical system raises concerns and requires a more substantial safety case of such system. IEC 61508 [1] recommends a basic indicator of functional safety of an item, i.e., the rate of wrong-side failures λ. Then, as the indicator of the efficiency of a system with a digital twin we can consider the relation of the rate of wrong-side failures of the initial system λ_S, a single-channel item (Fig. 2), to the probability of wrong-side failure of a system with a digital twin λ_T. The higher is that relation, the more efficient is the application of digital twins in vital systems.

For fixed time intervals, the indicator of efficiency of digital twins is as follows: $E = \lambda_S/\lambda_T$.

In order to identify the rate of wrong-side failures of a system as a whole λ_T, the following prerequisites were adopted:

– a train control and/or protection system operates at a high demand rate;

– the dependability of a single-channel item is defined by the failure rate λ_1;

– the initial item is supervised with the probability of correct failure detection α. The digital twin is also supervised with the probability α. The probability of failure non-detection is $\overline{\alpha}$. The supervision tools are perfectly dependable. The probability of false alarm is negligibly small;

– the adequacy of the digital twin to the initial item is evaluated subject to the results of its verification. It is assumed that both digital twins adequately imitate the operation of the initial item. The corresponding safety integrity level is to be ensured using the IEC 61508 [1] part 3 or EN 50128 [2] standards.

– the dependability of a digital twin is defined by the systematic failures of its software. Failures manifest themselves under certain sets of input data. It is assumed that such sets are varied and random. That implies the feasibility of evaluating the dependability of a digital twin based on the failure rate λ_2. It is also assumed that the dependability of a digital twin is much higher than that of the initial item, i.e., $\lambda_2 << \lambda_1$.

– in case of detection of item failure, a command is issued to replace it by involving two digital twins. At the same time, it is understood that the probability of correct and timely delivery of the command is v;

– the comparator and ruggedized communication node are perfectly dependable (if that assumption is not ensured, the failure rates λ_1 and λ_2 may include respective shares associated with the comparator);

– exponential distributions of failures and recoveries of the item are adopted. That is due to the fact that most train control and/or protection systems include electrical/electronic equipment;

– random failure events of the item and digital twins are mutually independent;

– item failure and digital twin systematic failure restoration rates are equal to μ, as they are performed by a single maintenance crew;

– wrong-side failure restoration rates γ are defined by the duration of hidden (undetected by supervision tools) failures;

– it is assumed that system restoration times are distributed exponentially (that is a common assumption in such cases. However, even if the restoration time distribution function is not exponential, that barely affects the system's steady-state characteristics, see, e.g., Gnedenko and Kovalenko [13]).

Let us examine the model of system safety organization.

Criteria of right-side failure of a system with digital twins:

1. Non-matching performance of the initial item and digital twins caused by an undetected failure of the initial item or one of the digital twins. System restoration.

2. Failure of one of the digital twins. System restoration.

Criterion of wrong-side failure of a system with a digital twin:

Item failure and error in the delivery of the control command to involve the digital twins or failure of the initial item and digital twins.

The state graph of the safety of a technical system with digital twins (see. Fig. 2) according to model 1 is shown in Fig. 3.

Description of states:

1 – perfect state of system;

2 – detected failure of item;

3 – non-matching performance of the item and its digital twins due to an undetected item failure. The cause of non-matching performance is unknown. The system is put into the state of *right-side failure.*The system is restored;

4 – incorrect or untimely delivery of control command to involve the digital twins upon correct detection of item failure, *hazardous failure*. The failure is eliminated upon detection of a hidden failure;

5 – detection of a failure of one of the two digital twins. The system is put into the state of *right-side failure.* The system is restored.

The graph edges in Fig. 3 are marked with the following parameters: **1-2**: $\alpha\lambda_1$ is the detected failure flow of the initial item; **1-3**: $\bar{\alpha}(\lambda_1+2\lambda_2)$ is the non-detected failure flow of the item or digital twins; **1-5**: $\alpha 2\lambda_2$ is the detected failure flow of the digital twins; **4-2:** γ is the rate of hidden wrong-side failure; **2-4:** $\bar{\nu}2\lambda_2$ is the rarefied, with the probability of non-involvement $\bar{\nu}$, failure flow of digital twins; **2-5:** $\nu 2\lambda_2$ is the rarefied, with the probability of involvement ν, failure flow of digital twins; **3-1, 5-4:** μ is the system recovery rate; **5-4.**

The functional safety model of the examined system in Fig. 3 implies the following logic of operation. Initial state 1, all elements in perfect state. In case of detection of failure or fault in the item's operation, transition into state 2 occurs and command to replace it with digital twins is issued for

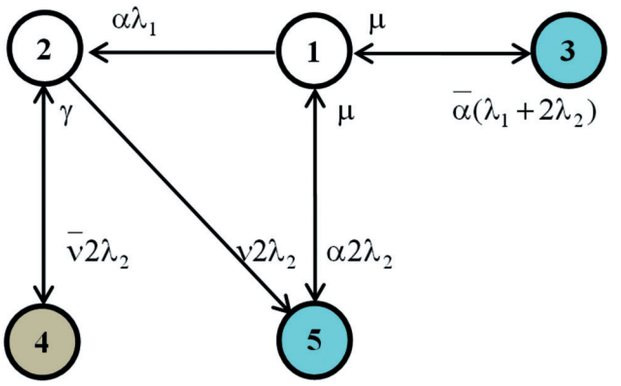

Fig. 3. Safety states graph of a system with digital twins

the period of time not affecting the occurrence of hazardous control actions. In case of actual or potential wrong-side failure, the item's output signals are blocked, as it is shown in patent [12]. If the initial item has failed and the performance of the digital twins does not match, the system is put into the state of right-side failure 3. If a failure of any one of the digital twins is detected and the item is in perfect state, the system goes from state 1 into state 5 of right-side failure. If the item and any one of the digital twins have failed, the system goes from state 2 into state 4 of wrong-side failure (if an error occurred in the process of involvement of the digital twins) or into state 5 in case of faultless digital twin involvement.

Under the adopted exponential distribution laws and, subsequently, constant failure and recovery rates in the examined system there is no consequence. That means that the system behaviour in the future depends on the current state and does not depend on the previous ones. Under the above prerequisites, the system's behaviour is described using a Markovian process.

In order to solve the problem, the input data is predetermined:

– the distribution functions of the system being in the states of the graph in Fig. 3.

$$F_1(t) = 1 - \exp[-(\lambda_1 + 2\lambda_2)t];$$

$$F_2(t) = 1 - \exp(-2\lambda_2 t);$$

$$F_4(t) = 1 - \exp(-\gamma \cdot t);$$

$$F_3(t) = F_5(t) = 1 - \exp(-\mu \cdot t);$$

– the mathematical expectation of the system being in the states of the graph in Fig. 3 according to formula:

$$T_i = \int_0^\infty [1 - F_i(t)]dt;\ T_i = \frac{1}{\lambda_1 + 2\lambda_2};\ T_2 = \frac{1}{2\lambda_2};$$

$$T_4 = \frac{1}{\gamma};\ T_3 = T_5 = \frac{1}{\mu}; \quad (1)$$

- probabilities of transition according to formula: $p_{ij} = \int_0^\infty \lambda_{ij}[1 - F_i(t)]dt$, where λ_{ij} is the rate of system transition from state *i* into state *j*

$$p_{12} = \frac{\alpha\lambda_1}{\lambda_1 + 2\lambda_2};\ p_{13} = \frac{\bar{\alpha}(\lambda_1 + 2\lambda_2)}{\lambda_1 + 2\lambda_2};\ p_{15} = \frac{\alpha \cdot 2\lambda_2}{\lambda_1 + 2\lambda_2};$$

$$p_{24} = \bar{\nu};\ p_{25} = \nu;\ p_{31} = p_{42} = p_{51} = 1; \quad (2)$$

Key safety indicator, i.e., mean time to wrong-side failure T_{WS} can be defined using the topological method [14] according to formula

$$T_{WS} = \frac{T_1 \Delta G^1_{S_{WS}} + \sum_{(k)} \sum_{i,j} l^{ij}_k \Delta G^j_k T_j}{\Delta G_{S_{WS}}}, \quad (3)$$

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 $S_{WS} = \{4\}$ 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 graph resolution without the nodes situated on the k-th path and without node j in the set of non-hazardous states $S_H = \{1, 2, 3, 5\}$.

The resolution weights can be defined using Mason's gain formula [15]

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

where the weights of boundaries are found within the set of non-hazardous states (Fig. 3):

$$C_1 = p_{13} \cdot p_{31} = \frac{\bar{\alpha}(\lambda_1 + 2\lambda_2)}{\lambda_1 + 2\lambda_2};\ C_2 = p_{15} \cdot p_{51} = \frac{2\lambda_2}{\lambda_1 + 2\lambda_2};$$

$$C_3 = p_{12} \cdot p_{25} = \frac{\alpha\nu\lambda_1}{\lambda_1 + 2\lambda_2}.$$

All boundaries intersect, since they have a common node 1. The resolution weights of the graph in Fig. 3.

$$\Delta G^1_{S_{WS}} = 1;$$

$$\Delta G_{S_{WS}} = 1 - C_1 - C_2 - C_3 = 1 - \frac{\bar{\alpha}(\lambda_1 + 2\lambda_2) + 2\lambda_2 + \alpha\nu\lambda_1}{\lambda_1 + 2\lambda_2} \quad (4)$$

According to the graph in Fig. 3 and substituting expressions (1), (2) and (4) into formula (3), we find within the set of non-hazardous states (1.2.5)

$$T_{WS} = \frac{T_1 + p_{12}T_2 + p_{13}T_3 + (p_{15} + p_{12}p_{25}) \cdot T_5}{1 - C_1} =$$

$$= \frac{\mu(\alpha\lambda_1 + 2\lambda_2) + \bar{\alpha}2\lambda_2(\lambda_1 + 2\lambda_2)}{2\lambda_2\mu \cdot [\alpha(\lambda_1 + 2\lambda_2) - \alpha(\lambda_1\nu + 2\lambda_2)]}. \quad (5)$$

Given that the failure rate of the digital twin λ_2 is 2 to 3 orders of magnitude lower than that of the λ_1 initial item and $\mu >> 2\lambda_2\lambda_1$, expression (5) with an error not higher than one order of vanishing, can be transformed as follows:

$$T_{WS} \approx \frac{1}{2\lambda_2\bar{\nu}}.$$

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 [16, 17, 18] a multiply rarified, irregularly simplest failure flow is also a simplest one with constant parameter

$$\lambda_T = 1 / T_{WS} = 2\lambda_2\bar{\nu}.$$

Note. In order to ensure an important assumption, i.e., "the failure rate of a digital twin is 2 or 3 orders of magnitude lower than that of the initial item", it is important that the software was designed using methods that comply with higher safety integrity levels, for instance, 2 of 3 safety integrity levels higher. Alternatively, the failure rate is to be proven statistically [19].

Ensuring the compliance with the EN 50159 [20] requirements for the communication channel safety, implies that the probability of timely and faultless communication of the command to involve the digital twins tends to one. Therefore, a probability $\bar{\nu}$ of incorrect delivery of digital twin control command close to 0 can be achieved. Subsequently, by using digital twins, the safety of the initial item in terms of wrong-side failure rate may be improved by several orders of magnitude. Indeed, let us examine the relation of the wrong-side failure rates of the initial item ($\lambda_O = \lambda_1$) to the wrong-side failure rate of the system: $E = \frac{\lambda_S}{\lambda_T} = \frac{\lambda_1}{2\lambda_2\bar{\nu}}$. As $\lambda_1 >> \lambda_2$ and $\bar{\nu} \to 0$, our assertion is correct.

The above effect may be achieved not only with the use of digital twins, but also as the result of the system transitioning into the state of right-side failure in each event of initial architecture modification. Therefore, the time to system transition into any safe state should be compared to the time to failure of the initial item.

Let us identify the system's mean time to right-side failure. For that purpose, in the state graph in Fig. 3, we must calculate states 3.4.5 (states of wrong-side and right-side failures) together with the adjacent edges. Then, the graph on Fig. 3 modifies into the form shown in Fig. 4.

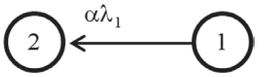

Fig. 4. Graph of the examined system without hazardous and safe states

We find the mean time to right-side failure according to formula (3), where all the expansion weights are equal to 1 due to the absence of boundaries in the graph in Fig. 4:

$$T_{RS} = T_1 + p_{12}T_2 = \frac{1 + \alpha\lambda_1}{\lambda_1 + 2\lambda_2}.$$

Then, the relation of the mean time to right-side failure to the mean time to failure of the initial item subject to correlation $\lambda_1 >> \lambda_2$ is defined as follows:

$$\frac{T_{RS}}{T_1} \approx \frac{1+\alpha\lambda_1}{\lambda_1}. \quad (6)$$

Thus, the mean time to right-side failure is not less than the mean time to failure of the initial item. That means that, within the examined model, provided highly efficient measures for safety improvement are in place, the system dependability is maintained at a level not lower than that of the initial item.

The introduction of digital twins into a system is a new, not yet tested way of ensuring system safety. Naturally, it requires a substantial safety case. That is associated with significant expenditures. On the one hand, there is a significant effect in terms of improved functional safety of the system. On the other hand, significant one-off costs may be required for the development of the digital twin algorithm C_{DTA} and preparation of the system safety case C_{SC}. Given the above, let us evaluate the economic feasibility of this approach.

Let the cost of the initial item be C_1. The cost of a system with digital twins is $C_1 + \Delta C_1$. The size of the batch of manufactured products is m units. The cost of a batch m systems with digital twins is $C_{BAT} = (C_1 + \Delta C_1)m + C_{DTA} + C_{SC}$. The cost of development of such system along with the cost of the safety case are acceptable if the following is true:

$$C_{BAT} - C_1 m \le C_{SC}, \quad (7)$$

where C_{SC} is the acceptable investment in the assurance of the desired level of safety. The effect of additional costs on a batch of products can be estimated using the following expressions:

$$\frac{C_{BAT}}{C_1 m} = \frac{(C_1 + \Delta C_1)m + C_{DTA} + C_{SC}}{C_1 m}. \quad (8)$$

If $m \to \infty$, expression (8) modifies into

$$\lim_{m\infty\to} \frac{C_{BAT}}{C_1 m} = \frac{C_1 + \Delta C_1}{C_1}. \quad (9)$$

As the cost ΔC_1 of series production of digital twins in the system is significantly lower than the cost C_1 of production of the initial item, the expression (9) tends to 1. That means that in case of large batches of manufactured technical systems, the effect of additional costs is reduced.

The decision on the benefits of additional costs is taken by the customer and system developer together based on the requirement to ensure the safety of such system. However, the cost of ensuring a high level of system safety is about 10 to 50 times higher than the cost of the initial single-channel item, whereas the reduction of the rate of wrong-side system failures as compared with the same indicator for the initial item may amount to several orders of magnitude. This circumstance may play a key role in the decision regarding the application of digital twins for the purpose of technical system safety.

4. Conclusion

Transforming the initial item into a system with digital twins allows significantly reducing the rate of wrong-side failures. This effect may be obtained not only with the use of digital twins, but also as the result of the system transitioning into the state of right-side failure in each event of discrepancy between the initial item and/or the digital twins. It has been established that the mean time to right-side failure under such conditions is not less than the mean time to failure of the initial item. That means that highly efficient measures for safety improvement allow maintaining the system dependability at a level not lower than that of the initial item.

The introduction of digital twins into a system is a new, not yet tested way of ensuring system safety. Naturally, it requires a substantial safety case. That is associated with significant additional expenditures. The decision on the benefits of additional costs is taken by the customer and system developer together. At the same time, it must be taken into consideration that in case of large batches of manufactured technical systems, the effect of additional costs is reduced and the effect of significantly improved safety is maintained.

References

1. IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

2. EN 50128, Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems; 2011.

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

4. Schabe H. The Safety Philosophy behind CENELEC Rails Standards. In: Proceedings of ESREL 2002. Lyon; March 19-21, 2002; 788-790.

5. Hirao Y., Watanabe I. Safety technologies and management of railway signalling in Japan. *Signal + Draht* 2000; 5.

6. 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.)

7. Shubinsky I.B., Shaebe H. On the definition of functional reliability. In: Steenbergen et al., editors. Proceedings of the ESREL 2013, Safety, Reliability and Risk Analysis: Beyond the Horizon. Taylor & Francis Group; London; 2014; 3021-3027. ISBN 978-1-138-00123-7.

8. Shubinsky I.B., Shaebe H., Rozenberg E.N. A short study on rebooting safe computers and the impact on safety. In: proceedings of ESREL 2009, Reliability, Risk and Safety;1:175-178.

9. Braband J. A practical guide to safety analysis methods. *Railway Signalling + Telecommunication* 2001;9:41-45.

10. Gulker J., Schaebe H. Physical Principles of Safety. In: Proceedings of ESREL 2006, Safety, Reliability and Risk Analysis; Balkema, Rotterdam;2:1045-1050.

11. Dmitriev V.M., Gandzha T.V., Zaychenko T.N. Technique of stratification and integration of computer models of complex technical controlled system. *Informatika i sistemy upravleniya* 2016;4(50). (in Russ.)

12. Batraev V.V., Kudriashov S.V., Popov P.A., Rozenberg E.N., Rozenberg I.N., Shukhina E.E., Shubinsky I.B. [Dual-channel system for railway vehicle traffic regulation]. Patent RF no. 2726243. 2020. Bul. no. 19. (in Russ.)

13. Gnedenko B.V., Kovalenko B.V. [Introduction into the queueing theory]. Moscow: Nauka, 1987. (in Russ.)

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

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

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

17. Pogozhev I.B. [Estimation of failure flow deviation from the Poisson flow in assessment of multiphase use equipment]. In: [Cybernetics to the benefit of communism. Volume 2]. Moscow: Energia; 1964. (in Russ.)

18. Nazarov A.A., Lapatin I.L. [Asymptotic Poisson MAP flows]. *Tomsk State University Journal* 2010;413:72-78. (in Russ.)

19. Braband J., Gall H., Schäbe H. Proven in use for software: assigning an SIL based on statistics. In: Mahboob Q., Zio E., editors. Handbook of RAMS in Railway systems – Theory and Practice. Boca Raton, Taylor and Francis; 2018. P. 337-350.

20. EN 50159 Railway applications Communication, signalling and processing systems. Safety-related communication in transmission systems; 2010.

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

The author's contribution

Igor B. Shubinsky developed the mathematical model, analyzed the findings.

Hendrik Schäbe developed the system state graph, defined the limits of the proposed model.

Efim N. Rozenberg defined the research problem.

Conflict of interests

The authors declare the absence of a conflict of interests.