*Original article*
*DOI: 10.21683/1729-2646-2017-17-1-46-52*

# Evaluation of safety and reliability parameters of supervision and control systems

**Oleg L. Makoveev**, *Radioavionica, Saint Petersburg, Russia, e-mail: makoveev38@mail.ru*
**Sergey Yu. Kostyunin**, *Radioavionica, Saint Petersburg, Russia, e-mail: kostyunin.sergey@gmail.com*

*Oleg L. Makoveev*

*Sergey Yu. Kostyunin*

**Abstract. The aim** *of this article is the analytical evaluation of dependability and reliability indicators of vital facility supervision and control systems. Such indicators include: probability of no-failure, collective failure rate, wrong-side and right-side failure rate, average service life. The article considers systems with different redundancy rates (2-oo-2, 2-oo-3, 2-oo-2-by-2) ensuring recovery of failed equipment (channels) without interruption of operation. The paper covers such safety and reliability mechanisms as interchannel data comparison, mutual channel blocking and protection against negative failure development by mutual channel blocking.* **Methods.** *For the purpose of achieving the set goal, the article suggests a mathematical functional model based on absorbing homogenous Markovian continuous-time chains. The states of this chain reflect the number of good channels of the system, while state transition rates are identified based on the equipment failure rates of each channel and repair rates (subject to the mechanisms of interchannel data comparison and failed channel blocking). The absence of protection can be caused by such events as non-detection of failure by supervision facilities, disability of blocking mechanisms, protection tripping delay. In such case the failure of a channel (channels) causes the failure of the whole system and forces the Markovian chain into the absorbing state. The probabilities of transition into the absorbing state are divided into the probabilities of transition into state of right-side failure and state of wrong-side failure. As a failure occurrence in a situation of absent guaranteed protection against its possible negative consequences in a system that continues operating may cause undue inputs to the system's executive mechanisms and on the assumption of the worst case scenario we deem such failure to be a wrong-side one. The used methods allow finding the probabilities of each state of the chain by solving a system of Kolmogorov-Chapman differential equations. Based on the given probabilities, the collective failure rate and average service life are identified along with the right-side and wrong-side failure rates. In order to ensure the usability of the presented methods, the authors provide approximate formulas of failure rates and approximation errors.* **Results.** *A mathematical model of operation of a multichannel microprocessor system has been developed. Formulas for calculation of system state probabilities, average service life, wrong-side and right-side failure rates have been obtained that allow evaluating the safety and fault tolerance of various systems with hot standby and in-operation operability recovery capabilities. The given formulas for calculation of system state probabilities allow increasing the number of safety and reliability indicators, if needed. The article presents the feasibility of simplified calculation of failure rates.* **Conclusions.** *The formulas given in the article can be used for evaluation of reliability, safety and longevity indicators of microprocessor-based supervision and control circuits of vital facilities (ship-borne technical facilities, trackside equipment in railway stations and open lines, fixed power facilities, etc.). In the development process they allow finding the rational system organization by means of comparative evaluation of performance of structures with various degrees of redundancy. In the context of system adaptation for application in various facilities as well as its modernization the formulas in question enable analytical calculation of the above indicators.*

**Keywords:** *functional safety, reliability, supervision, diagnostics, wrong-side failure, right-side failure, failure rate.*

**For citation:** *Makoveev O.L., Kostyunin S.Yu. Evaluation of safety and reliability parameters of supervision and control systems. Dependability, 2017, vol. 17, no. 1, pp. 46-52. (in Russian) DOI: 10.21683/1729-2646-2017-17-1-46-52*

Vital facility supervision and control systems are expected to meet reliability and safety requirements [1]. High levels of reliability and safety are ensured by multichannel architectures of computer-based systems, supervision and diagnostics.

It is suggested to use the following indicators for quantitative evaluation of such systems [2, 3, 4]:

– in terms of reliability: probability of no-failure and failure rate (collective failure rate);

– in terms of longevity: average service life;

– in terms of safety: wrong-side and right-side failure rates.

The standard for functional safety of equipment [4] sets forth a formula that serves as the foundation for deduction of wrong-side and right-side failure rates.

$$\Lambda = \Lambda_S + \Lambda_D, \tag{1}$$

where $\Lambda$ is the collective failure rate;

$\Lambda_S$ is the right-side failure rate;

$\Lambda_D$ is the wrong-side failure rate.

The same formula shows the connection between dependability and safety.

In order to highlight the importance of protection of the considered systems against the negative consequences of failures of railway automation equipment, safe failures are conventionally called right-side failures.

There is a number of Russian and foreign computer-based systems, whose safety and reliability [4, 5] are based on hardware and software redundancy and automatic engineering supervision and diagnostics. Under identical safety and reliability requirements, the structure of such systems significantly depends on the operation conditions. Thus, in systems whose operation conditions do not allow replacement of failed equipment in operation, the required safety and reliability characteristics are achieved through significant redundancy of hardware and software facilities [5].

A noticeably smaller redundancy in hardware and software facilities is required for systems of which the operation conditions do allow replacement of failed equipment in operation. In this case the most common solutions are the 3-channel “2-oo-3” and 4-channel “2-by-2-oo-2” hot standby with recovery, as well as combinations of the above (different levels of redundancy for different devices of the system). It should be noted that in a number of cases 2-channel “2-oo-2” devices are used, in which each channel is secure.

In such systems, on-line inspection and testing allow localizing malfunctions with subsequent replacement of failed modules or redundant channels without interruption of operation (“smooth” replacement). On-line inspections are based on interchannel comparisons and checks per a limited number of parameters over the system’s operation cycle. Diagnostic tests are performed routinely in the background in order to eliminate failure accumulation. Checks are performed on all hardware ever used regardless of the current facility management program.

The distinctive feature of such systems is the continuation of normal operation after one failure and transition to limit state after the second failure. Two types of limit state exist that correspond to the two types of failure consequences [2], namely:

– state upon wrong-side failure, that causes the emergence of hazard to human life and/or significant material and/or moral damage;

– state upon safe failure that does not cause hazardous situations.

In case of failures in order to eliminate the possibility of hazardous situations as best possible, based on the results of supervision and diagnostics, the system is automatically transferred into state of safe failure, i.e. the system is protected against potential negative consequences of a wrong-side failure.

Among system components responsible for providing protection against possible negative consequences of wrong-side failures are system state supervision and diagnostics facilities, as well as failed component and whole product operation blocking mechanism. Designing secure and reliable systems with all types of redundancy involves maximal possible elimination of wrong-side failures, while maintaining a required level of operability. For that purpose, it is required to ensure high reliability of supervision and diagnostics with a dependable and fast-operating blocking mechanism.

In order to ensure product recovery in operation, malfunction reporting is specific to replacement modules, while replacement of failed equipment is performed with the power on.

As a failure in a situation of absent protection against its possible negative consequences in a system that continues operating may cause undue inputs to the system’s executive mechanisms and on the assumption of the worst case scenario, we deem such failure to be a wrong-side one (WSF).

The absence of protection may be due to such unrelated events as non-detection of failure by the supervision facilities, failure of the blocking mechanism or the time between failures being longer than the protection operation time. Therefore, the probability of non-availability of protection ($q_1$,$q_2$) can be identified as follows:

in case of first failure:

$$q_1 = q_{1C} + q_{1b}, \qquad (2)$$

where: $q_{1C}$ is the probability of control facilities did not detect the system failure,

$q_{1b}$ is the probability of blocking mechanism failure.

in case of second failure:

$$q_2 = (1 - q_{2\tau})\,(q_{2C} + q_{2b}) + q_{2\tau}, \qquad (3)$$

where: $q_{2C}$ is the probability of control facilities did not detect the system failure,

$q_{2b}$ is the probability of blocking mechanism failure;

$q_{2\tau}$ is the probability of the time between failures being shorter than the protection operation delay (we assume that the protection mechanisms are guaranteed to operate within time $\tau$).

For the purpose of malfunction detection, over each operation cycle the on-line inspection checks primary procedures data (data input, calculations, supervision, data output, diagnostics, etc.).

The list of such procedures is specific and permanent to each system.

In 3 and 4-channel systems on-line inspection is based on interchannel comparison, and in those double checking is possible up to the second failure. In 2-channel systems, blocking per first failure is also based on interchannel comparison. Additionally, the integrity of data batches received and transmitted by users (external systems) is verified by beans of redundant coding. The reliability of supervision under double verification is quite high. It declines if interchannel comparison is performed by means of convolutions and signatures [6, 7].

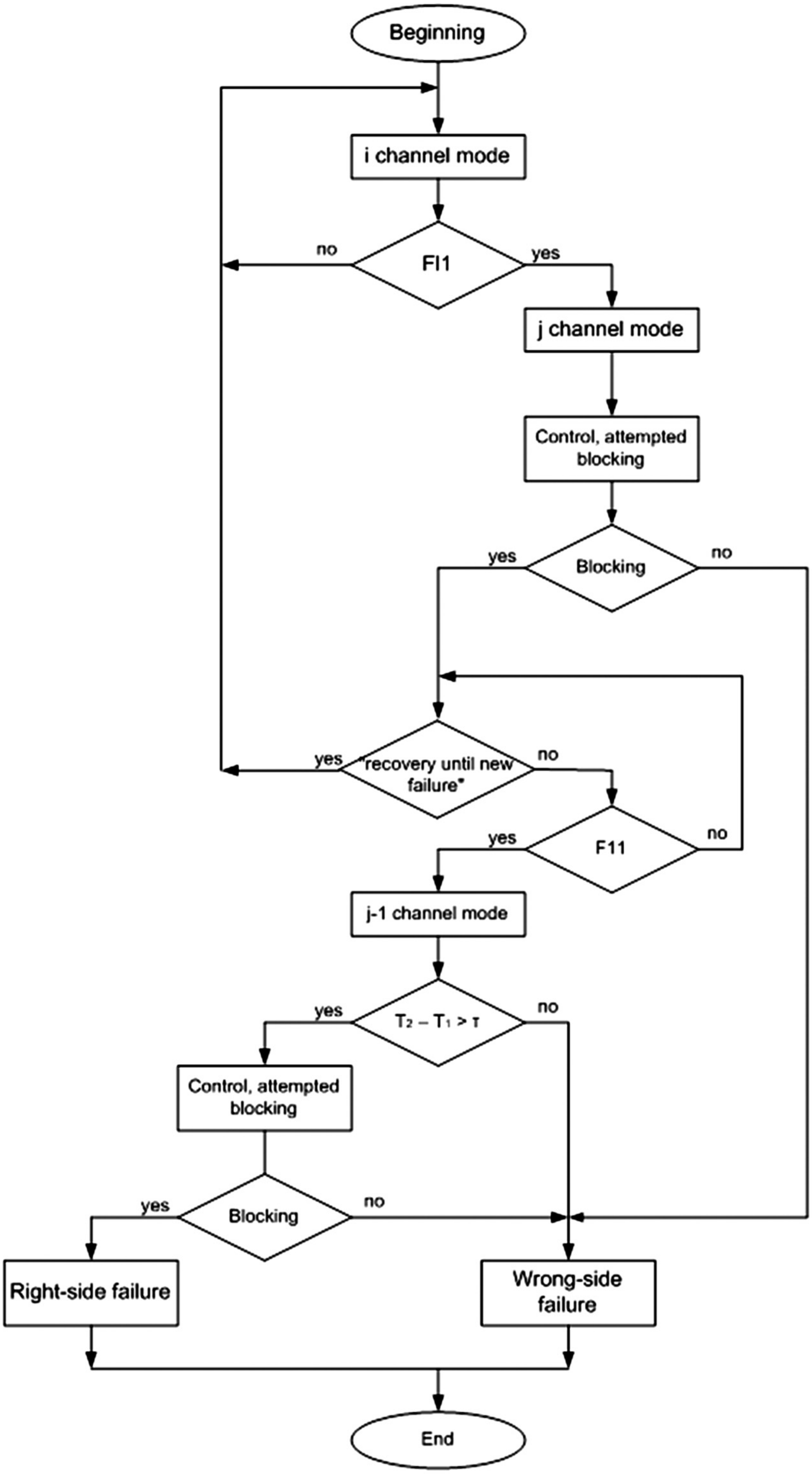

Figure 1. Block diagram of system state change

After the second failure, in 3 and 4-channel systems a single check is done. For this case, the most typical supervision reliability limitations are due to failures with identical consequences in different channels (non-detectable by interchannel comparison). Most probably, identical failure consequences may take place in case of practically simultaneous occurrence (within one operation cycle) of same-type failures of elements with identical reference designations in two channels.

In 2-channel systems, after blocking per first failure operation may continue if safety facilities are available for each channel [8] or through external checking. That is a serious limiting factor of such systems' application.

Given the above, let us consider the operation of a system in case of failures.

At the initial start the system is in fully operational state. After the first failure (event F1) the system passes into state in which malfunction detection is performed. In case of malfunction detection and protection operation (with the probability $1 – q_1$), as well as in the absence of the second failure during recovery, the failed channel is excluded from operation without loss of function. After failure recovery the system passes onto the initial state.

If protection is not available (with the probability $q_1$), the first failure is considered a wrong-side one.

If within time before recovery of a failed channel the second failure occurs (event F2), the system passes into state of complete failure under the following circumstances:

1) the second failure occurred sometime after the protection operation for the consequences of the first failure, and during that time the protection was implemented (with the probability $1 – q_2$). However, due to depleted reserves (number of good channels) recovery causes the loss of function. In other words, the event F1 was followed by the event "protection of device with loss of function", i.e. the so-called right-side failure (RSF);

2) the second failure occurred in absence of protection (with the probability $q_2$), but the operation continues, which allows considering such failure a wrong-side one.

Figure 1 shows a diagram of system state change with failures and recoveries based on the results of condition supervision.

In Figure 1, some states are referred to by the number of good channels at a specific moment in time according to Table 1, where:

– initial state is «i channel mode» (all channels operational);

– state after the first failure (event F1) is «j channel mode»;

– state after the second failure (event F2) is «(j-1) channel mode»;

Each type of the considered systems (type of redundancy) is characterized by two parameters, i.e. *i* and *j*, that are different type to type, which allows using *"i j"* as a designation of belonging to a specific type.

Transition from state to state occurs in the following cases:

– in case of recovery of a failed channel, return into the initial state;

– if $T_2 – T_1 > \tau$ (time between failures is longer than the protection operation delay), transition to control and, in case of detected malfunction, blocking of the failed channel;

– in case of failures (F1 and F2) and operation and failure to operate of protection, transitions in (j-1) channel mode into states of "right-side failure" and "wrong-side failure".

For the purpose of evaluation of secure fail-safe supervision and control systems, let us consider a Markovian process with a discrete set of states and continuous time represented as a graph of model transition from state to state.

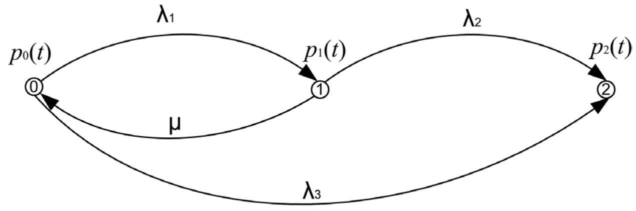

Figure 2. Transition graph

The states of the model reflect the changes related to product failures and recoveries, while the transitions are defined by the failure and recovery rates.

The model has the following features:

the failure flow of individual redundant channels is most simple with the rate of i λ or j λ.

Here, the *i* and *j* are presented as multipliers of λ, while in Table 1 they were designations of belonging to a specific type of system, in which there is no contradiction.

2) the recovery flow is adopted as the simplest, of which the rate $\mu = 1/T_r$ , where $T_r$ is the time of recovery;

3) the probabilities of states are as follows:

– $p_0(t)$ is the probability of initial state (after initial start or recovery, when all *i* channels are good);

– $p_1(t)$ is the probability of state, at which one channel has failed with the rate of *i*λ (following an event F1), while *j* channels are good;

**Table 1**

| ***i* channel system<br>(*i, j*)** | **Number of good channels** | | |
|---|---|---|---|
| | **in initial state, *i*** | **after first failure, *j*** | **after second failure, *j*-1<br>(right-side or wrong-side failure)** |
| 2 channel system – (2,1) | 2 | 1 | 0 |
| 3 channel system – (3,2) | 3 | 2 | 1 |
| 4 channel system – (4,2) | 4 | 2 | 1 |

– $p_2(t)$ is the probability of absorbing state, at which a second channel has failed with the rate of $j\lambda$ (following an event F2) and the whole device enters the state of right-side failure (operation is impossible) or the state of wrong-side failure, when operation continues with a malfunction.

F0, F1 and F2 represent exhaustive events, therefore:

$$p_0(t) + p_1(t) + p_2(t) = 1. \tag{4}$$

Based on the transition graph, with known λ and μ a system of differential equations (Kolmogorov equations) is constructed:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = -\left(\lambda_1 + \lambda_3\right) p_0(t) + \mu\, p_1(t) \\ \dfrac{dp_1(t)}{dt} = -\left(\mu + \lambda_2\right) p_1(t) + \lambda_1\, p_0(t) \\ \dfrac{dp_2(t)}{dt} = \lambda_3\, p_0(t) + \lambda_2\, p_1(t) \end{cases} \tag{5}$$

Solving the system allows finding the probabilities of model states, rates of right-side and wrong-side failures, as well as mean time to failure.

The following formulas are used:

$\Lambda(t) = f(t)/(1 - F(t))$ is the system's overall failure rate,

where: $f(t)$ is time to failure density function;

$F(t)$ is the distribution function.

Due to the fact that beside the overall failure rate of the system we need to find the wrong-side and right-side failure rates subject to the type of the system let us introduce the following notations:

Λ(t) is the collective failure rate of the system;

$\Lambda(t)_{\mathrm{WSF}}$ is the wrong-side failure rate;

$\Lambda(t)_{\mathrm{RSF}}$ is the right-side failure rate.

Under the introduced notations:

$$\Lambda(t) = \frac{\dfrac{dp_2(t)}{dt}}{1 - p_2(t)}, \tag{6}$$

2) the rates of transition from state to state in case of failures depend on parameters *i* and *j*, as well as availability or non-availability of protection:

$$\lambda_1 = i\left(1 - q_1\right)\lambda,\ \lambda_2 = j\left(1 - q_2\right)\lambda + j\,q_2\,\lambda = j\,\lambda,\ \lambda_3 = i\,q_1\,\lambda;$$

for the systems under consideration the time to failure is as follows

$$T_{cp} = \int_0^\infty t\, p_2'(t)\, dt \approx \frac{\mu}{ij\,\lambda^2}. \tag{7}$$

4) an event "time between failures is shorter than the protection operation delay" is equivalent to the event "occurrence of second failure over the time period not exceeding τ". The probability of the second event is identified as follows:

$$q_{2\tau} = 1 - e^{-\lambda_2 \tau} \approx j\,\lambda\tau. \tag{8}$$

The formulas for identifying the probabilities of duration of various system states deduced by solving the differential equations, as well as other parameters are given in Table 2.

**Table 2**

| Parameters | Formulas |
|---|---|
| $P_0(t)$ | $\dfrac{1}{k_1 - k_2}\left[\left(\mu + j\lambda + k_1\right)e^{k_1 t} - \left(\mu + j\lambda + k_2\right)e^{k_2 t}\right]$ |
| $P_1(t)$ | $\dfrac{\lambda_1}{k_1 - k_2}\left(e^{k_1 t} - e^{k_2 t}\right)$ |
| $P_2(t)$ | $\dfrac{1}{k_1 - k_2}\left[\left(iq_1\lambda + k_2\right)e^{k_1 t} - \left(iq_1\lambda + k_1\right)e^{k_2 t}\right] + 1$ |
| $T_{cp}$ | $\dfrac{1}{k_1 k_2\left(k_1 - k_2\right)}\left[\left(k_2 - k_1\right)\lambda_3 + k_2 k_1 - k_1 k_1\right] \approx \dfrac{\mu}{ij\,\lambda^2}$ |

Here $k_1$ and $k_2$ are the roots of the characteristic equation for the differential equations system (5):

$$k_1 = \frac{-\left(\mu + (i+j)\lambda\right) + \sqrt{\left(\mu + (i+j)\lambda\right)^2 - 4\left(ij\lambda^2 + iq_1\lambda\mu\right)}}{2} \approx$$

$$\approx -\lambda\left(\frac{ij\lambda}{\mu} + iq_1\right). \tag{9}$$

$$k_2 = \frac{-\left(\mu + (i+j)\lambda\right) - \sqrt{\left(\mu + (i+j)\lambda\right)^2 - 4\left(ij\lambda^2 + iq_1\lambda\mu\right)}}{2} \approx -\mu. \tag{10}$$

The absolute approximation error of $k_1$ and $k_2$ are found using the formula:

$$\Delta = \frac{i\lambda\left(j\lambda + q_1\mu\right)}{\mu^2}. \tag{11}$$

In accordance with (6) the collective failure rate equals to:

$$\Lambda(t) = \frac{k_1\left(iq_1\lambda + k_2\right) - k_2\left(iq_1\lambda + k_1\right)e^{(k_2 - k_1)t}}{\left(iq_1\lambda + k_1\right)e^{(k_2 - k_1)t} - \left(iq_1\lambda + k_2\right)}. \tag{12}$$

As $|k_2| >> |k_1|$ and $|k_2| >> iq_1\lambda$, we obtain

$$\Lambda(t) \approx \left(\lambda_3 + k_1\right)e^{(k_2 - k_1)t} - k_1. \tag{13}$$

If Λ(t) is found as the specified service life $T_S$, where, for instance, $T_S \approx 10^5$ hours, then

$$\Lambda(t) \approx \frac{ij\lambda^2}{\mu} + iq_1\lambda. \tag{14}$$

Let us find the wrong-side and right-side failure rates.

Under the notations used in this article, formula (1) is as follows:

$$\Lambda(t) = \Lambda(t)_{RSFI} + \Lambda(t)_{WSFI}\,. \tag{15}$$

Consequently:

$$\Lambda(t) = \Lambda(t)\,p(t)_{RSFI} + \Lambda(t)\,p(t)_{WSFI}\,. \tag{16}$$

$$p(t)_{RSFI} + p(t)_{WSFI} = 1, \tag{17}$$

where $p(t)_{\mathrm{RSF}}$, $p(t)_{\mathrm{WSF}}$ are the probabilities of right-side and wrong-side failures.

In order to identify $p(t)_{\mathrm{RSF}}$ and $p(t)_{\mathrm{WSF}}$,we should deduce the formula for probability of absorbing state $p_2(t)$. That is done by integrating $\frac{dp_2(t)}{dt} = \lambda_3\, p_0(t) + \lambda_2\, p_1(t)$ (from differential equation system (5). Here, $\lambda_3 = iq_1\lambda$ is the rate of transition from the initial state to the absorbing state in absence of protection (with the probability $q_1$), i.e. transition to the wrong-side failure, $\lambda_2 = j(1-q_2)\lambda + jq_2\lambda$ is the rate of transition from the state after the first failure to the absorbing state in presence of protection (with the probability $1 - q_2$) and in the absence of protection (with the probability $q_2$), i.e. transition to right-side and wrong-side failure respectively.

Thus, the probabilities of transition to wrong-side failure and right-side failure are divisible, i.e.:

$$p_2(t) = p_{2,\,WS}(t) + p_{2,\,RS}(t), \tag{18}$$

therefore,

$$p(t)_{RSFI} = \frac{p_{2,\,RS}(t)}{p_2(t)},\; p(t)_{WSFI} = \frac{p_{2,\,WS}(t)}{p_2(t)}. \tag{19}$$

If $p_2(t)$ is written as

$$p_2(t) = \frac{\lambda_3}{k_1 - k_2}\left[\frac{1}{k_1}(\mu+\lambda_2+k_1)e^{k_1 t} - \frac{1}{k_2}(\mu+\lambda_2+k_2)e^{k_2 t}\right] + \\ + \frac{\lambda_3(\mu+\lambda_2)}{k_1 k_2} + \frac{\lambda_1\lambda_2}{k_1 - k_2}\left(\frac{1}{k_1}e^{k_1 t} - \frac{1}{k_2}e^{k_2 t}\right) + \frac{\lambda_1\lambda_2}{k_1 k_2},$$

then after substitution of values of transition rate we deduce the divided formula

$$p_2(t) = \frac{iq_1\lambda}{k_1 - k_2}\left[\frac{1}{k_1}(\mu + j\lambda + k_1)e^{k_1 t} - \frac{1}{k_2}(\mu + j\lambda + k_2)e^{k_2 t}\right] + \\ + \frac{i(1-q_1)\lambda\, jq_2\lambda}{k_1 - k_2}\left(\frac{1}{k_1}e^{k_1 t} - \frac{1}{k_2}e^{k_2 t}\right) + \\ + \frac{i\lambda(\mu q_1 + jq_1\lambda + jq_2\lambda - jq_1q_2\lambda)}{k_1 k_2} + \\ + \frac{i(1-q_1)\lambda\, j(1-q_2)\lambda}{k_1 k_2 (k_1 - k_2)}\left(k_2 e^{k_1 t} - k_1 e^{k_2 t} + k_1 - k_2\right),$$

where

$$p_{2,WS}(t) = \frac{iq_1\lambda}{k_1 - k_2}\left[\frac{1}{k_1}(\mu + j\lambda + k_1)e^{k_1 t} - \frac{1}{k_2}(\mu + j\lambda + k_2)e^{k_2 t}\right] + \\ \frac{i(1-q_1)\lambda\, jq_2\lambda}{k_1 - k_2}\left(\frac{1}{k_1}e^{k_1 t} - \frac{1}{k_2}e^{k_2 t}\right) + \\ + \frac{i\lambda(\mu q_1 + jq_1\lambda + jq_2\lambda - jq_1q_2\lambda)}{k_1 k_2}, \tag{20}$$

$$p_{2,RS}(t) = \frac{i(1-q_1)\lambda\, j(1-q_2)\lambda}{k_1 k_2 (k_1 - k_2)}\left(k_2 e^{k_1 t} - k_1 e^{k_2 t} + k_1 - k_2\right). \tag{21}$$

In order to simplify formulas for $p(t)_{\mathrm{RSF}}$ and $p(t)_{\mathrm{WSF}}$ by using approximate values $k_1$ and $k_2$ (9), (10) and that μ>>λ, we deduce:

$$p(t)_{RSFI} = \frac{p_{2,\,RS}(t)}{p_2(t)} \approx (1-q_1)(1-q_2), \tag{22}$$

$$p(t)_{WSFI} = \frac{p_{2,\,RS}(t)}{p_2(t)} \approx 1 - (1-q_1)(1-q_2). \tag{23}$$

Given the value Λ($t$) (15) we have:

$$\Lambda(t)_{RSFI} \approx \lambda\left(\frac{ij\lambda}{\mu} + iq_1\right)(1-q_1)(1-q_2), \tag{24}$$

$$\Lambda(t)_{WSFI} \approx \lambda\left(\frac{ij\lambda}{\mu} + iq_1\right)\left[1 - (1-q_1)(1-q_2)\right]. \tag{25}$$

## Conclusion

The article presents formulas that allow evaluating the safety and fault tolerance of various systems with the hot standby capability. Those systems operate normally up to two failures in different channels and provide for condition-monitored recovery without interruption of operation.

Advanced supervision and diagnostics enable condition-based operation of the presented systems.

## References

1. Gapanovich VA, Rozenberg EN, Shubinsky IB. Nekotorye polozheniya otkazobezopasnosti i kiberzashhishhennosti sistem upravleniya [Some concepts of fail-safety and cyber protection of control systems]. Dependability. 2014; 2: 88 – 100. Russian

2. GOST R 27. 002-89. Industrial product dependability. General concepts. Terms and definitions. Russian.

3. GOST R 51901.5-2005 (IEC 60300-3-1:2003). Guide for application of analysis techniques for dependability. Russian.

4. GOST R IEC 62061-2013. Safety of machinery. Functional safety of safety-related electrical, electronic, programmable electronic control systems. Russian.

5. Theeg G, Vlasenko S, editors. Sistemi avtomatiki i telemekhaniki na zheleznykh dorogakh mira [Railway Signalling & Interlocking. International Compendium]. Moscow: Inteks; 2010. ISBN 978-5-89277-098-9. Russian.

6. Avakian AA. Sozdanie sverkhnadyozhnykh ehlektronnykh sistem dlya aehrokoosmicheskoj tekhniki [Development of fail-safe electronic systems for aerospace structures]. Kontrol. Diagnostika [Testing. Diagnostics]. 2013; 2: 67 – 75. Russian

7. Novik GH. O dostovernosti signaturnogo analiza [On the integrity of signature analysis]. Avtomat. i telemekh. [Automation and remote control]. 1982; 5: 157 – 159. Russian.

8. Goldshtein VB, Mironov SV. Khesh-funktsii dlya sokrashheniya diagnosticheskoj informatsii [Hash functions for reduction of diagnostics information]. Izvestia Saratovskogo universiteta. Novaia seria. Seria Matematika. Mekhanika. Informatika. [Journal of the University of Saratov. New series. Mathematics. Mechanics. Information technologies Series]. 2007; 2 (7). Russian.

9. Iyudu KA. Nadiozhnost, kontrol i diagnostika vychislitelnykh mashin i sistem [Dependability, supervision and diagnostics of computer systems]. Moscow: Vyshaya shkola; 1989. Russian.

## About the authors

**Oleg L. Makoveev**, Candidate of Engineering, Science Adviser, Radioavionica. Troitskiy pr., 4, building B, Saint-Petersburg, Russia 190005, e-mail: makoveev38@mail.ru

**Sergey Yu. Kostyunin**, Candidate of Physics and Mathematics, Head of Unit, Radioavionica. Troitskiy pr., 4, building B, Saint-Petersburg, Russia 190005, e-mail: kostyunin.sergey@gmail.com

**Received on 29.09.2016**