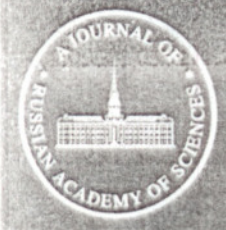
Volume 43, Number 1
January–February 2004

ISSN: 1064-2307



JOURNAL OF COMPUTER AND SYSTEMS SCIENCES INTERNATIONAL

(A Journal of Optimization and Control)

English Translation of *Izvestiya Rossiiskoi Akademii Nauk. Teoriya i Sistemy Upravleniya*

Editor-in-Chief
Evgenii A. Fedosov

http://www.maik.ru

The Journal Publishes the Results of Investigations on All Aspects of Modern Control Theory and Its Applications

Russian Academy of Sciences

МАИК "НАУКА/INTERPERIODICA" PUBLISHING

Journal of Computer and Systems Sciences International, Vol. 43, No. 1, 2004, pp. 145–151.
Translated from Izvestiya Akademii Nauk. Teoriya i Sistemy Upravleniya, No. 1, 2004, pp. 155–162.

COMPLEX TECHNICAL CONTROL SYSTEMS AND INFORMATION CONTROL COMPLEXES

Functional Reliability of Information Control Systems for Federal Railway Transport

A. S. Misharin and I. B. Shubinskiĭ

Russian Research Institute of Control for Railway Transport, Ministry of Railways of the Russian Federation, Nizhegorodskaya ul. 27, Moscow, 109029 Russia

Received March 31, 2003

Abstract—In this paper, the goals and problems, as well as the object and the subject, of the study of the theory of functional reliability of information control systems as a part of general reliability theory are discussed. The definition of a functional failure of these systems is given, a set of indices of the correctness of implementing computational and information processes in these systems for federal railway transport is proposed, and a flexible strategy for providing functional reliability of information control systems is considered.

INTRODUCTION

Information control systems (ICSs) for federal railway transport (FRT) are multifunction hardware and software complexes that gather, convert, accumulate, process, and transmit information, as well as exert control (or make decisions for the control) over subordinate objects [1].

On the basis of ICSs of a lower hierarchical level, ICSs of higher hierarchical levels are built. These ICSs are charged with a large number of functions and more important problems. So, using local networks, distributed databases, and workstations (WKSs) as the base, centers of rail control at the federal and regional levels are organized; these centers are connected with one another by digital data-transmission networks (information networks). On the basis of local area networks, operating–technological digital and combined data transmission networks, and the WKSs of train dispatchers, networks of dispatcher control are built.

Despite the wide variety of ICSs for FRT, they have a number of common features. The main commonalities are the following:

Problem solving on a real time basis.

The necessity of information interchange with a large number of users.

The relative invariability of a complex of executed programs for the whole operating time.

Large amounts of information in each control cycle.

Stiffly prescribed terms of solving given problems under the randomness of external actions.

The structure of ICSs is rapidly rebuilt in accordance with solved problems.

The amount of compound software is comparable with the amount of hardware (and in a number of cases exceeds it).

The majority of ICSs for FRT are critical systems (for them, the cost of errors in the results of the execution of specified tasks is great).

Errors in the results of operating an ICS are caused, mainly, by errors in a complex of algorithms and programs, malfunctions, operator errors, and input-information errors. To a significantly lesser extent, errors in the results depend upon digital-equipment failures, especially on small time intervals of the task execution. The functional reliability of ICSs is directly dependent on the information load, i.e., the parameters of request flows.

The methods of classical reliability theory give no way to estimate the faultlessness of executing computational and information processes in an ICS and the correctness of the results of given processes. Solving these problems is the subject of this paper.

1. OBJECT AND SUBJECT FOR THE STUDY OF THE FUNCTIONAL RELIABILITY OF ICSs

The object of the study of modern reliability theory is a product (a technical device or a technical system). **The subject** of the study are processes of failures and restoration of the product. Therefore, according to *GOST* (State Standard) *27.002–89*, the following basic reliability parameters of a product are taken: mean operating time to a failure, the failure rate, the reliability function (the survival function), mean restoration time, the (instantaneous) availability function, the operational availability function, and the efficiency ratio (for a multifunctional product subject to failures). These indices allow one to predict, calculate, and estimate the total time needed for repairing the product over a given long operating period, as well as calculate the number of failures and restorations, the failure probability, etc. On the whole, the classical methods of reliability theory reduce to designing irredundant and

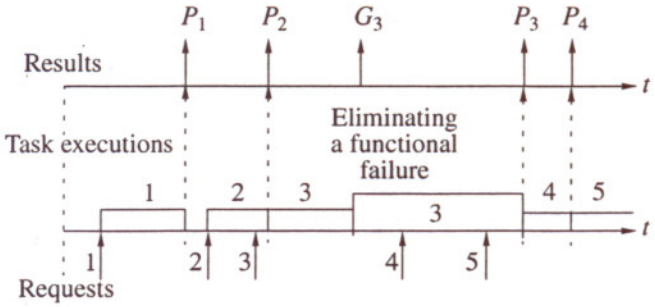


Fig. 1. Task executions in accordance with received requests, as well as generating correct output results.

redundant systems and making it possible to determine a rational strategy for providing the reliability and restorability of a product [2, 3].

The known methods of reliability theory are not intended for estimating the correctness of intermediate and output results in computational and information networks, the correctness of implementing computational and information processes in ICSs, and the efficiency of using methods for error protection.

Figure 1 demonstrates two random processes and the output results of their correct implementation. The first process is a random sequence of requests 1–5 for solving given problems. The second process is a time sequence of task executions (request servicing) and elimination of incorrect results. The output results are the probabilities of correct task execution (P_1, P_2, P_3, ...) or the functional-failure probability (G_3).

On the basis of the common features of ICSs and the analysis of failures, malfunctions, operator errors, input-information errors, and program errors presented in [4], we can assert that providing the reliability of ICSs refers, mainly, to the problems of determining and providing the correctness of functional task executions (Fig. 1) and not to determining and providing hardware reliability and restorability, as in other technical systems. Hence, within the limits of general reliability theory, a theory of functional reliability of ICSs for FRT should be developed.

The object for the study of the functional reliability is a multifunctional hierarchical information system.

The subject for the study is defined as processes of occurring, detecting, and eliminating errors in intermediate and output results of the system operation that are caused by its own errors and introduced errors related to parameters of request flows (that come for servicing, i.e., for executing given functional tasks).

2. DEFINITION OF A FUNCTIONAL FAILURE OF AN ICS

Assume that, at a particular instant, an ICS solves q functional problems. Each problem is implemented by a single program or a group of programs and is described by a set of parameters. A set of possible parameter values of the ith problem ($i \in q$, where q is the number of solved problems) we denote by r_i. The set r_i contains the subset x_i of reliability parameters of the hardware that is used for solving the ith problem, as well as the subset y_i of reliability parameters of the software that provides implementation of this problem, i.e., $x_i \subset r_i$ and $y_i \subset r_i$.

The set $\mathbf{R} = (r_1, r_2, \ldots, r_q)$ of parameter values of all problems that are solved at the current instant represents an instantaneous pattern of the computing environment of the ICS; this pattern describes its operation at the instant considered. The pattern can be processed in different ways. A typical way of processing is to find the centroid $\hat{\mathbf{R}}$ of the pattern. In the simplest case, the centroid can be found by calculating the weighted average value of the instantaneous characteristics r_i. The coordinates of the centroid $\hat{\mathbf{R}}$ of the pattern define the functioning state of the computing environment of the ICS. They depend on possible parameter values $\mathbf{X} = (x_1, x_2, \ldots, x_q)$ of the hardware that is used for the current solution of n problems and on the possible parameter values $\mathbf{Y} = (y_1, y_2, \ldots, y_q)$ of the implemented software.

Due to error occurrence and elimination in solving any one of q functional problems, the coordinates of the centroid vary with time: a random process $\hat{\mathbf{R}}(\mathbf{t})$ takes place. Individual realization of this process will be called a trajectory g of the process of states changing, and the set of the trajectories will be denoted by $\mathbf{G}$, i.e., $g \in \mathbf{G}$. The absence of errors in solving any functional problem on the entire time interval t corresponds to the trajectory g_0.

Consider the set $\mathbf{U} = (i_1, i_2, \ldots, i_l)$ of parameter values of an information process that is running in the ICS at the current instant. These parameters are the information transmission speed, distortions of information sending through the noise, the number of bits in messages, time delays in information interchange, etc. The information process is a random process $\mathbf{U}(\mathbf{t})$.

Along with patterns $\mathbf{R}$ and $\mathbf{U}$, which describe the properties of the functional reliability of computational and information processes in the ICS, one should take into account the parameters of external factors, whose values depend on the influence of the environment on the system. Among them are parameters of request flows that at random instants of the reception determine the required amount of hardware for request servicing and messaging channels, the parameters of information processing and transmission speed, etc. The totality of possible parameter values of the jth external factor ($j \in m$, where m is the number of considered external factors) will be denoted by Z_j. The vector $\mathbf{Z} = (Z_1, Z_2, \ldots, Z_m)$ describes parameter values (of external factors) that are known at the current instant.

Let us introduce the serviceability function $F(\mathbf{R}, \mathbf{U}, \mathbf{Z}, t)$, which describes the capacity of the ICS for cor-

rect solution of different groups of compound functional problems at a time t, as well as for correct reception and transmission of messages during this time in accordance with time-varying parameters of external factors.

The set of states S of the system is divided into two subsets: $S_f \cup \overline{S}_f = S$. Here, S_f is the subset of functioning states of the ICS and $\overline{S}_f$ is the subset of states having serviceability levels of the ICS that are lower than a permissible level. The subset S_f is also divided into two subsets: $S_0 \cup S_1 = S_f$. Here, S_0 are states in which the nominal serviceability of the ICS is provided, since all requested problems have been solved correctly and completely, with all the given information also having been received and transmitted correctly (this is explained by the absence of errors in the system or, at least, in the operation of the facilities that have been used for solving the requested problems), and S_1 are states of the reduced serviceability of the ICS. The states S_1 can also be divided into groups of subsets; for this purpose, they should be ordered by decreasing the serviceability levels

$$S_{11} \supset S_{12} \supset S_{13} \ldots \supset S_{1z}.$$

Here, S_{11} and S_{1z} are subsets of states (bordering the subsets S_0 and $\overline{S}_f$, respectively) of reduced serviceability. In this case, the subsets of states S_{1k} and S_{1j} $(k < j)$ are intermediate between the subsets of states S_{11} and S_{1z}.

In these terms, *a functional failure* of an ICS is the transition of the processes $\hat{\mathbf{R}}(\mathbf{t})$ and (or) $\mathbf{U}(\mathbf{t})$ from one subset S_{1k} into another S_{1j} $(S_{1j} \subset S_{1k})$ (or even into $\overline{S}_f$) having worse values of the serviceability function: $F_j < F_k$. The level of the nominal serviceability F_0 is matched by the subset of states S_0.

Partial functional failures take place in the cases where the processes $\hat{\mathbf{R}}(\mathbf{t})$ and (or) $\mathbf{U}(\mathbf{t})$ transit from one subset into another one having a lowered serviceability level within the set S_f.

A total functional failure of an ICS takes place in its transition from the subset of states $S_i \subset S_f$ into the subset of states $S_j \subset \overline{S}_f$, when the serviceability level of the system is lower than the permissible one: $F_j < F_{per}$.

Hence, the functional reliability of an ICS is its capacity for correctly solving given goal problems under the interaction with external objects.

3. INDICES OF THE FUNCTIONAL RELIABILITY OF ICSs

The indices of the functional reliability are intended to determine the capacity of ICSs for correctly solving given problems in the operation process. These indices are subdivided into the indices of the correctness of the execution of computational and information processes.

The correctness indices of the execution of computational processes:

Probability of no-failure solving a problem is the probability that no functional failure occurs while solving the problem.

Probability of no-failure run of computational processes during a time t is the probability of no-failure run of process flows and task flows that are imbedded in them during the time t.

Probability of correct run of computational processes during a time t is the probability that failures will not take place or will be prevented by a fail-safe system.

Mean operating time to a functional failure of an ICS in implementing computational processes.

Mean restoration time of a computational process.

The correctness indices of the execution of information processes:

Probability of the error occurrence in a message transfer.

Probability of no-failure run of information processes during a time t.

Probability of correct run of information processes during a time t.

Functional-failure rate while running information processes.

Mean operating time to a functional failure of an ICS in information processes.

Mean restoration time of an information process in an ICS.

Integrated indices of the functional reliability of an ICS:

The *functional-availability factor of an ICS* is the probability that, at any instant, the ICS is available for executing given computational and information processes.

The *operational functional-availability factor of an ICS* estimates the availability for operating at an arbitrary instant and the correctness in a required time of running specified tasks of information processing and transmission in accordance with given algorithms.

4. METHODS FOR PROVIDING THE FUNCTIONAL RELIABILITY OF ICSs

There exist different ways for increasing the reliability of technical devices and systems. Among these are, primarily, hardware redundancy and time redundancy. The attainment of the efficiency of a structural redundancy, as applied to the functional reliability, is problematic. This is explained by the following. Errors in a computational process cannot be eliminated by change-over if these errors are caused by random malfunctions, a program error, input-information errors, etc. Current errors in an information process are elimi-

nated by information redundancy (e.g., by noiseproof message coding), but without using a structural reserve. A time redundancy can significantly increase the functional reliability; however, it is impermissible to use the majority of traditional methods of double and triple computations in real time systems (to which ICSs are related) due to the limitations of real time.

These considerations imply the necessity of a complex applying flexible strategies of providing functional fail-safe operation of ICSs. Among these strategies is the introduction of check points in computational and information processes. This approach is known; however, if time intervals between check points are chosen so that, on time intervals between requests, the detection and the elimination of partial functional failures are provided, then the content and the efficiency of such a strategy radically change. Another efficient strategy of increasing the functional reliability can be the use of natural time, functional, information, and structural redundancy in ICSs. This redundancy is present to a greater or lesser extent in any technical system, even more in an information system (e.g., computational capabilities of computing facilities are employed not fully, not all given problems are implemented with the same intensity, an information-transmission channel capacity is used incompletely, etc.). We can also relate other nontraditional strategies of increasing the functional reliability of ICSs.

To jointly employ the strategies in question, special mechanisms for the rational use of redundancy for preventing functional failures are introduced. We shall call them adaptive mechanisms for providing the functional fail-safe operation. Together with redundant facilities, these mechanisms are facilities for providing the functional fail-safe operation (FPF).

Functions of FPF are as follows: detection of the presence of an error in a program or in hardware operation, fault localization, fault classification, decision making concerning the nature of the fault and interruption of task execution, detection of the location of the fault, reconfiguration of the ICS and (or) fault masking, and the restoration of task execution.

Hence, FPF are intended for providing the adaptation of ICSs to functional failures. A number of methods and engineering solutions concerning the design of FPF are described in [4].

The efficiency index of FPF is the probability β of successful adaptation of an ICS with FPF to these failures

$$\beta = P\{\Omega \le \Omega_g\}.$$

Here, Ω is a resource (structural, time, etc.) that can be used without sacrificing other efficiency indices of the ICS for failure protection and Ω_g is the permissible resource consumption with which one or several efficiency indices of the ICS reach the minimum permissible value.

For example, if the resource is time and the permissible resource consumption is, in the particular case, a fixed permissible pause in operating the ICS t_g, then we have

$$\beta = P\{V \le t_g\} = \int_0^{t_g} f_v(t)dt.$$

Here, V is the time interval from the instant of the fault occurrence to the fault elimination and the restoration of the computational process of problem solving, whereas $f_v(t)$ is the distribution density of the random time V.

If the permissible time of a pause in operating the system is random (V_g) and is distributed by the exponential law with parameter ρ_g, then, by the formula of total probability, we obtain

$$\beta = \int_0^\infty P\{V \le V_g\}\rho_g e^{-\rho_g t}dt = \int_0^\infty f_v(t)e^{-\rho_g t}dt$$
$$= [f_v^*(S)]_{S=\rho_g},$$

where $f_v^*(S)$ is the Laplace transform of function $f_v(t)$.

Let us estimate the probability that, during the task execution, functional failures will not occur or partial functional failures that occurred will be successfully neutralized by the FPF discussed above on the basis of permissible consumption of redundant resources. We denote the probability of no-failure task execution by p_p and the probability that functional failures in the FPF did not occur during the task execution by p_1. Then, the probability of no-failure task execution under the protection of the FPF is estimated by the relation

$$p_{p1} = p_p p_1 + (1 - p_p)p_1\beta_1 = 1 - g_p - g_1 + g_p g_1$$
$$+ \beta_1(g_p - g_p g_1).$$

Here, β_1 is the probability of successful adaptation of the first protective level (the protection of problem solving without the protection by the FPF), $g_1 = 1 - p_1$; and $g_p = 1 - p_p$.

Since $g_1 \ll 1$ and $g_p \ll 1$, with an error that does not exceed the second-order smallness, the following condition is fulfilled:

$$p_{p1} = 1 - g_1 - g_p(1 - \beta_1). \quad (4.1)$$

There exists a direct relationship between the probability of successful adaptation of an ICS to functional failures β_1, on the one hand, and the probabilities g_1 and g_p of functional failures of FPF and the problem, on the other hand. By analogy with [5], we take $\beta_1 = 1 - \exp[-\delta\zeta]$, where the normalization factor $\delta \cong 5$–10; $\zeta = \frac{g_1}{g_p + g_1}$. Using this relation, the influence of the failure probability (and, therefore, also an amount) of the hard-

ware and software of the FPF on the efficiency of adapting the ICS to the functional failures is simulated.

Let us estimate by formula (4.1) and the relation presented above, the type of decrease in the probability of functional failure as a result of using the protection. The plots in Fig. 2 demonstrate comparative probability values of functional failures of the ICS in the runs of computational processes without using FPF (g_p) and using protection facilities ($1 - p_{p1}$) for limiting values of the normalization factor δ.

The obtained results are curious: they testify that, for a moderate amount of protection facilities ($g_1/g_p \le 0.5$), the protection efficiency is the highest (it means the proportional relationship between the failure probability in problem solving g_p or the failure probability in operating the protection facilities g_1 and the amounts of the problems and the FPF, respectively, i.e., $g_p \equiv W_p$ and $g_1 \equiv W_1$). As the amount of protection facilities grows, the probability of successful adaptation to functional failures increases. However, its increase is opposite to the increase in the probability of functional failures in the FPF. From this, for $g_1/g_p \ge 1$, the number of failures that are eliminated by the FPF becomes less than the number of functional failures that are introduced by the FPF. Therefore, it is necessary to solve the problem of determining the permissible unreliability of facilities for protecting ICSs from functional failures.

Let us determine the permissible limits of the unreliability of protection facilities (and this also implies permissible amounts of protection facilities) in accordance with their efficiency and the unreliability of basic facilities of process execution.

First, we consider one-level protection. It has meaning only in the case where the condition

$$p_{p1} > p_p$$

is fulfilled. Here, p_{p1} is the probability of correct problem solving with the use of the one-level failure protection and p_p is the probability of correct problem solving without the use of the protection (coincides with the probability of no-failure task execution). With consideration of (4.1), this condition is transformed into the inequality

$$g_1 < g_p\beta_1. \qquad (4.2)$$

Inequality (4.2) is of fundamental significance in designing FPF. First, it specifies that the amount of FPF must not exceed the amount of hardware and software of ICSs that solve the given problem. Really, we have $\beta_1 < 1$, $g_1 \equiv W_1$, and $g_p \equiv W_p$, where W_1 and W_p are the amounts of FPF and the facilities for problem solving, respectively. Hence, from inequality (4.2), it follows that $W_1 < W_p\beta_1$. From this inequality it also follows that, the larger the amount of a solved problem, the more ramified and efficient the FPF must be. Hence, if $\beta_1 \longrightarrow 1$, then $W_1 \longrightarrow W_p$.

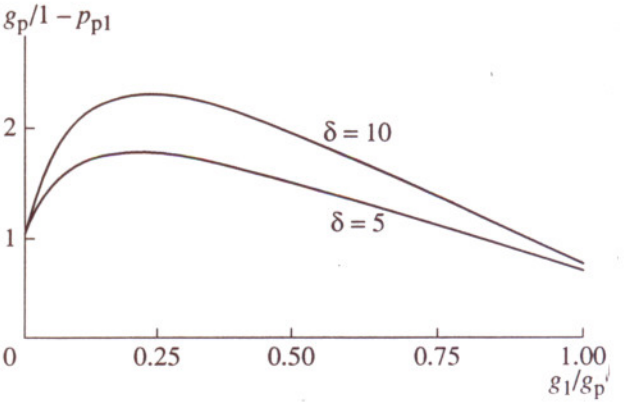


Fig. 2. Comparative probability values of functional failures of an ICS while running computational processes without the use of facilities for providing functional fail-safe operation (g_p) and using protection facilities ($1 - p_{p1}$) for limiting values of the normalization factor δ.

In turn, if FPF are inefficient ($\beta_1 \longrightarrow 0$), then, evidently, it makes no sense to use them ($W_1 \longrightarrow 0$).

Let us solve the problem of protecting the protection facilities from functional failures, which is known as the "how to guard the guard" problem.

Assume that an ICS has two levels of protection from functional failures: the first level protects facilities for problem solving and operates with the probability of correct operation $p_1 = 1 - g_1$, whereas the second level protects the facilities of the first protective level (the FPF of the first protective level) with the probability of the adaptation to failures β_2 and operates with the probability of correct operation $p_2 = 1 - g_2$. Here, the second level operates without protection by protection facilities. Then, the index of correctness of problem solving is determined as follows:

$$p_{p2} = p_p p_2(p_1 + g_1\beta_2) + (1 - p_p)p_2(p_1 + g_1\beta_2)\beta_1$$
$$= p_2(p_1 + g_1\beta_2)(p_p + g_p\beta_1).$$

Example. Suppose that the probability of correct problem solving by an ICS $p_p = 0.9$ does not satisfy the requirements of a user. For protection from functional failures at the first level, efficient steps that provide a high probability of adapting the ICS to failures $\beta_1 = 0.99$ are taken. Here, the ramified protection facilities of the first level (FPF1) have a deficient functional probability $p_1 = 0.95$. To protect FPF1 from functional failures, the second protective level (FPF2) is introduced. This level provides an insufficiently high probability of adapting to the failures of FPF1 $\beta_2 = 0.9$, but its operation is reliable ($p_2 = 0.99$).

Under these conditions, the correctness index of problem solving is evaluated as follows: $p_{p2} = p_2(p_1 + g_1\beta_2)(p_p + g_p\beta_1) = 0.98$.

Note that, if, in the statement of this problem, we retain only one protective level, then, in accordance

with (4.1), the correctness index of problem solving is evaluated as follows: $p_{p1} = 1 - g_1 - g_p(1 - \beta_1) = 0.95$ (i.e., $p_{p1} < p_{p2}$). This implies the advisability of introducing the second protective level.

With n protective levels, the correctness index of problem solving is calculated by the relation

$$\begin{aligned} p_{pn} &= p_n(p_{n-1} + g_{n-1}\beta_n) \\ &\times (p_{n-2} + g_{n-2}\beta_{n-1})\ldots(p_1 + g_1\beta_2)(p_p + g_p\beta_1) \\ &= (1 - g_n)\prod_{i=0}^{n-1}(p_i + g_i\beta_{i+1}), \end{aligned} \quad (4.3)$$

where $p_0 = p_p$ and $g_0 = g_p$.

It is evident that, at each protective level, the following condition, which results from inequality (4.2), must be fulfilled:

$$g_i < g_{i-1}\beta_i. \quad (4.4)$$

Here, $i = \overline{1, n}$.

From (4.4), we obtain the new inequality

$$g_i < g_p\prod_{j=1}^{i}\beta_j, \quad (4.5)$$

where $g_0 = g_p$. This inequality determines the limits of the advisability of constructing multilevel protection.

Proposition. If condition (4.5) is fulfilled, then it is permissible to introduce auxiliary hardware and software into the ICS for constructing several protective levels (for error checking, diagnostics, and correction); this brings about not a decreasing, but an increasing probability of correct problem solving.

Proof. In accordance with (4.3), we have

$$\begin{aligned} p_{pn} &= (1 - g_n)\prod_{i=0}^{n-1}(p_i + g_i\beta_{i+1}) \\ &= (1 - g_n)\prod_{i=0}^{n-1}[1 - g_i(1 - \beta_{i+1})]. \end{aligned}$$

From (4.5), we obtain

$$g_n < g_p\prod_{i=0}^{n}\beta_i; \quad g_i < g_p\prod_{j=0}^{i}\beta_{j+1}.$$

After substituting these relations into the previous formula, we obtain

$$p_{pn} > \left(1 - g_p\prod_{i=0}^{n}\beta_i\right)\prod_{i=0}^{n-1}\left[1 - g_p(1 - \beta_{i+1})\prod_{j=0}^{i}\beta_{j+1}\right].$$

Let us introduce the notation

$$g_p(1 - \beta_{i+1})\prod_{j=0}^{i}\beta_{j+1} = A_i,$$

where $A_i < 1$.

The series

$$\prod_{i=0}^{n-1}[1 - A_i] = 1 - \sum_i A_i + \sum_{ij} A_{ij} - \ldots + (-1)^{n-1}\prod_{i=1}^{n-1}A_i$$

for $A_i < 1$ is alternating. According to the Leibniz criterion for alternating series, this series converges, since its terms tend to zero and the remainder of the series R_p has the same positive sign as does the first omitted term $\sum_{ij} A_{ij}$ and is less than this term in magnitude. Therefore, with an error that does not exceed the second order of smallness, the following condition is fulfilled:

$$p_{pn} > \left(1 - g_p\prod_{i=0}^{n}\beta_i\right)\left[1 - g_p\sum_{i=0}^{n-1}(1 - \beta_{i+1})\prod_{j=0}^{i}\beta_{j+1}\right]. \quad (4.6)$$

Here, the probability p_{pn} is underestimated.

The proposition is valid if $p_{pn} > p_p$; formula (4.6) implies that this condition holds if $p_{pn} > 1 - B$, where $B < g_p$, i.e., where

$$\begin{aligned} g_p\Bigg[&\prod_{i=1}^{n}\beta_i + \sum_{i=0}^{n-1}(1 - \beta_{i+1})\prod_{j=0}^{i}\beta_{j+1} \\ &- g_p\sum_{i=0}^{n-1}(1 - \beta_{i+1})\prod_{j=0}^{i}\beta_{j+1}\prod_{i=1}^{n}\beta_i\Bigg] < g_p. \end{aligned}$$

In this case, it is sufficient to testify that the value of the expression in square brackets is less than one. Really, since the probabilities β_i, β_{i+1}, and β_{j+1} are always less than one, the value of the expression in square brackets

$$\left[\prod_{i=1}^{n}\beta_i + \sum_{i=0}^{n-1}(1 - \beta_{i+1})\prod_{j=0}^{i}\beta_{j+1}\right]$$

is also always less than one.

Thus, under inequality (4.5), the introduction of auxiliary hardware and software into an ICS for constructing several protective levels (for error checking, diagnostics, and correction) brings about not a decreasing, but an increasing probability of correct problem solving.

CONCLUSIONS

The presented propositions of the functional reliability of ICSs for federal railway transport are intended for calculations, prediction, and statistical estimation of the correctness of obtaining intermediate and output results in computational and information networks, the correctness of the execution of computational and information processes in the ICSs, and the efficiency of using some methods for protection from

malfunctions and program errors, as well as errors in information channels.

These materials agree with the requirements and materials of CENELEC EN 50159-1 and CENELEC EN 50159-2 European standards for closed and open data transmission systems for railway transport, as well as with the materials of the MEK/IEC 61508 International standard for functional safety.

The questions of determining and calculating some of the introduced indices of functional reliability have been solved by a number of researchers. This is true, primarily, for the following indices: the probability of failure-free problem solving, mean restoration time of a computational process, the probability of an error while transmitting a message, and the mean operating time to a failure of an ICS in relation to computational or information processes. At the same time, defining and calculating other simple indices of the functional reliability of ICSs require special-purpose investigations. This is related, in full measure, to the integrated indices of functional reliability of ICSs. In order to determine them, it is necessary to design models of combined flows of functional failures in systems jointly executing computational and information processes.

To protect ICSs from functional failures, it is proposed to employ in the ICSs facilities for providing the functional fail-safety (FPF) that are intended to make the efficient use of its natural and artificially introduced resources. The problems of providing the efficiency of FPF have been set, and the corresponding indices have been presented. The introduced auxiliary hardware and software, in turn, require protection. The boundary conditions that determine the permissibility of introducing several levels of protecting the ICSs from functional failures have been found.

REFERENCES

1. P. A. Kozlov and A. S. Misharin, Izv. Ross. Akad. Nauk, Teor. Sist. Upr., No. 5 (2002) [J. Comp. Syst. Sci. Interh. **41**, 803 (2002)].
2. G. N. Cherkesov, *Reliability of Engineering Systems with Time Redunduncy* (Sov. Radio, Moscow, 1975) [in Russian].
3. I. V. Panfilov and A. M. Polovko, *Computational Systems* (Sov. Radio, Moscow, 1980) [in Russian].
4. I. B. Shubinskiĭ, V. I. Nikolaev, S. K. Kolganov, *et al.*, *Active Failure Protection for Control Module Computational Systems*, Ed. by I. B. Shubinskiĭ (Nauka, St. Petersburg, 1993) [in Russian].
5. N. D. Putintsev, *Hardware Inspection of Control Digital Computers* (Sov. Radio, Moscow, 1966) [in Russian].