Original article
DOI: 10.21683/1729-2646-2017-17-1-17-21
Dependability, vol. 17 no.1 2017 УДК 621.399

Moving redundancy of tolerant elements

Sergey F. Tyurin, *Perm National Research Polytechnic University, Perm, Russia, e-mail: tyurinsergfeo@yandex.ru.*

Sergey F. Tyurin

Abstract. *Redundancy is one of the primary ways of improving dependability. In particular, structural redundancy is used. In such cases fail-safe operation of elements, devices and systems can be ensured. Fail-safety can enable mitigation of both faults and failures. The paper examines the matter of increasing dependability by means of the so-called sliding redundancy that ensures the health of systems of n elements with m redundant elements that can replace any of the main elements. It is proposed to improve sliding redundancy through recovery of elements out of a number of failed elements that have retained some functionality (basis). For example, the basis of the logical (Boolean) function in terms of Post's theorem is available if such function is not a zero-preserving function, not a one-preserving function, not a self-dual function, not a line function, not a monotone function. Previously, the author proposed the so-called functionally complete tolerant logical functions (FCTF) that do not only possess functional completeness but retain it under the specified failure model. Then even a failed element remains functionally complete, yet with reduced capabilities, e.g. becomes a 2OR-NOT, though the FCTF can be implemented with an element 2AND-2OR-NOT. In this case the recovery of the original function requires several 2OR-NOT elements. However, the diagnostics of such elements and their reconfiguration in case of failure are problematic. This approach can be interpreted with logic recovery of programmable logic devices (PLD) that is based on the so-called Look Up Tables (LUT) that are memory devices based on 16:1 multiplexers. The circuit is a transmitting transistor tree. If they fail, the healthy half of LUT can be used. By means of reconfiguration using standard PLD facilities that contain local and global connections matrix, such "semi-LUTs" can be transformed into LUTs whose functions are equivalent to initial ones. That equals to an increase of the number of redundant elements. Sliding redundancy with recovery of elements out of several failed ones that retained the basis can be used in critical system applications when repair or replacement of elements is impossible. The article proposes a formula that takes such recovery into consideration, analyzes the special features of such redundancy and evaluates the advantages for dependability.*

Keywords: *dependability, redundancy, sliding redundancy, recovery, failures, fault tolerance, failure rate.*

For citation: *Tyurin S.F. Moving redundancy of tolerant elements. Dependability, 2017, vol. 17, no. 1, pp. 17-21. (in Russian) DOI: 10.21683/1729-2646-2017-17-1-17-21*

Introduction

System dependability can be achieved through redundancy. Standby redundancy is often used when the functions of the main element are transferred to the standby element only upon failure of the main one [1]. In case of majority redundancy, a failure or fault is disguised. However, that requires a high level of redundancy. A lesser structure redundancy is typical to adaptive fault tolerance [2, 3, etc.] that includes procedures for supervision, reconfiguration and automatic replacement of failed modules by available redundant ones. In case of sliding redundancy a group of main elements is backed up by one or more redundant elements each of which can replace any of the failed elements of the group [1]. If the number of main elements is n and the number of backup elements is m, sliding redundancy ensures operability if subset of elements R is operational with the power of $|R| \geq n$. Without regard to the complexity and diagnostics and recovery time, for the exponential failure model the probability of no-failure for a system with sliding redundancy is described with the formula:

$$P_{SMR}(n,m,t) = \sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot \left[1 - e^{-\lambda\cdot t}\right]^{n+m-i}. \quad (1)$$

In formula (1) P_{SMR} is the probability of no-failure of a system with sliding redundancy (SMR), t is time, hours. Graphs of (1) change in MathCad are given in Fig. 1.

In case of an element's failure, a switch device (SD) enables the remaining backup ones (the so-called reconfiguration is performed); taking into account the SD failure rate λ_{sd} and the assumption of ideality of supervision of the main and backup elements, we deduce:

$$P_{SMR}(n,m,t) = \sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot \left[1 - e^{-\lambda\cdot t}\right]^{n+m-i} \cdot e^{-\lambda_{sy}\cdot t}. \quad (2)$$

The graph of dependency of P_{SMR} (2) from the number of backup elements for n =10 if $\lambda = 10^{-5}$ (1/h), $\lambda_{sd} = 10^{-7}$ (1/h) is given in Fig. 2.

Problem definition

Let us not consider the recovery by means of replacement or repair of failed elements. Let us suggest using the

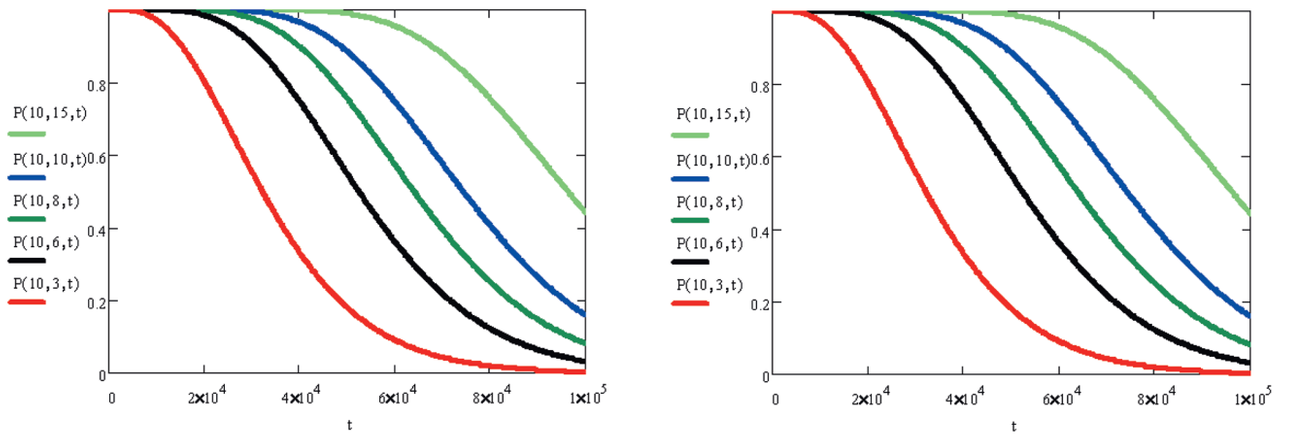

Figure 1. Dependence of P_{SMR} on the number of backup elements m, main elements n, time t (h) if $\lambda = 10^{-5}$ (1/h) with no regard to failure rate of a switch device

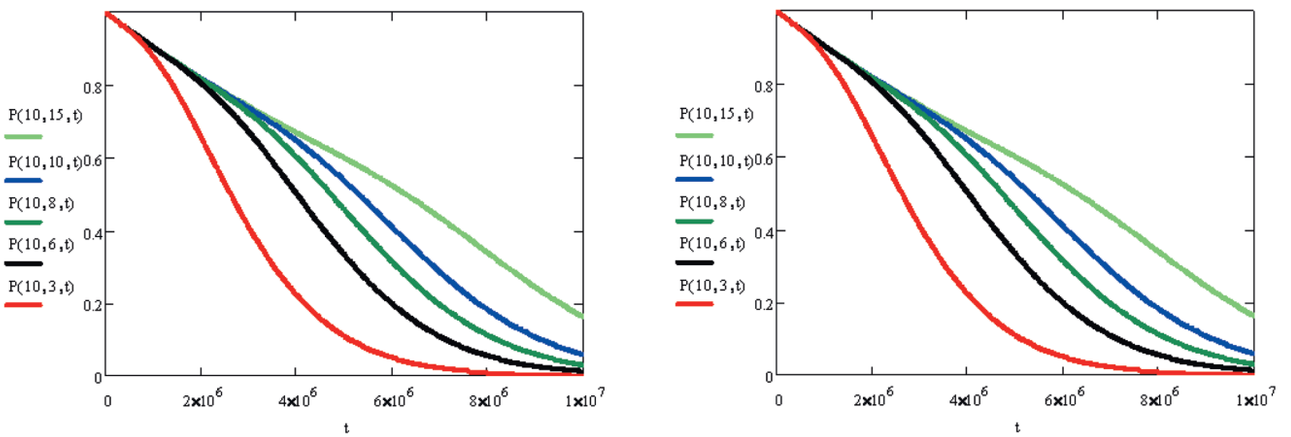

Figure 2. Dependence of P_{SMR} on the number of backup elements m, main elements n, time t (h) if $\lambda = 10^{-5}$ (1/h) with regard to failure rate of a switch device $\lambda_{sd} = 10^{-7}$ (1/h)

capabilities of the failed elements, i.e. a kind of "internal" redundancy [4]. In this case the failed elements of the system with sliding redundancy remain in backup if they retain at least some functionality (basis) and can be used, but in order to supplement the initial element more than one of them will be required. This concept conforms with state-of-the-art programmable logic devices (PLDs) of the type FPGA (field-programmable gate array) that contain a large number of logical devices (Look Up Table, LUT) [5] in case of single failures of which it is sometimes possible to use a LUT with a smaller number of variables [6-7]. Normally, a PLD does not use all the logical devices (according to some evaluations, 70% or even less). Therefore, the remaining elements can constitute the backup for the sliding redundancy. After proper diagnostics, reconfiguration can be performed remotely (e.g. for a spacecraft, using commands from mission control). However, in case of LUT starvation, the PLD stops being operational. For critical systems in which the PLD cannot be replaced that is not acceptable.

Theoretical part

The recovery of failed main (backup) elements is equivalent to their increase given that they recover as failures occur. However, in order for one element to recover, a number of them must have failed. The premises of the proposed approach to elements recovery out of failed ones lay in the modern trends of introducing built-in diagnostics units into PLDs and systems on a chip, in-built maintenance service with test generators in accordance with the IEEE 1500 standards [8]. Those units can also be backed-up, e.g. according to the technology used by Xilinx in the Virtex PLD [9], which allows assuming the ideality of supervision of main and backup elements.

Let us consider a LUT with two variables that is described with the following formula:

$$z = a\bar{x}_2\bar{x}_1 \vee b\bar{x}_2x_1 \vee cx_2\bar{x}_1 \vee dx_2x_1. \qquad (3)$$

If a failure occurs in one half of this LUT, it can for instance be represented with the following formula:

$$z_1 = a\bar{x}_1 \vee bx_1. \qquad (4)$$

If there are such «half» elements with functions z_1, z_2, z_3, then the following formula can be recovered from them by means of the required variable (reconfiguration) (3):

$$z = z_3 = (a\bar{x}_1 \vee bx_1 = z_1)\bar{x}_2 \vee (c\bar{x}_1 \vee dx_1 = z_2)x_2. \quad (5)$$

In general, for various abstract bases the following formula will be in place:

$$\nu = \left\lfloor \frac{m}{r} \right\rfloor, \quad (6)$$

where r is the maximum number of failed elements required for recovery of the initial function, $\lfloor \cdot \rfloor$ is the closest lowest whole natural number (ceil). For instance, m=5; r=4; v=1. I.e. a sixth failure can be additionally countered. The remainder will be:

$$w = m - r\left\lfloor \frac{m}{r} \right\rfloor. \quad (7)$$

In our case w=1.

$$1 \le w \le r - 1. \quad (8)$$

The remainders may become useful later when failures occur in the elements out of the number n.

If we do not count the remainders, then the number $v_1 = \left\lfloor \frac{m}{r} \right\rfloor$ is used to counter v_1 failures additionally to m. For instance, m=18; r=4; v=4. That means that if four elements fail, one more element can be recovered from them, i.e. the following number of additional failures will be countered:

$$v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor. \quad (9)$$

In principle, the "nesting" of the fractions can be high, but the number of countered additional failures does not exceed n. We believe that elements that failed more that once do not recover (though in some cases that is possible, e.g. transition of three-element basis into a two-element one). We deduce the following:

$$m;\ v_1 = \left\lfloor \frac{m}{r} \right\rfloor;\ v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor;\ v_3 = \left\lfloor \frac{\left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor}{r} \right\rfloor \ldots \quad (10)$$

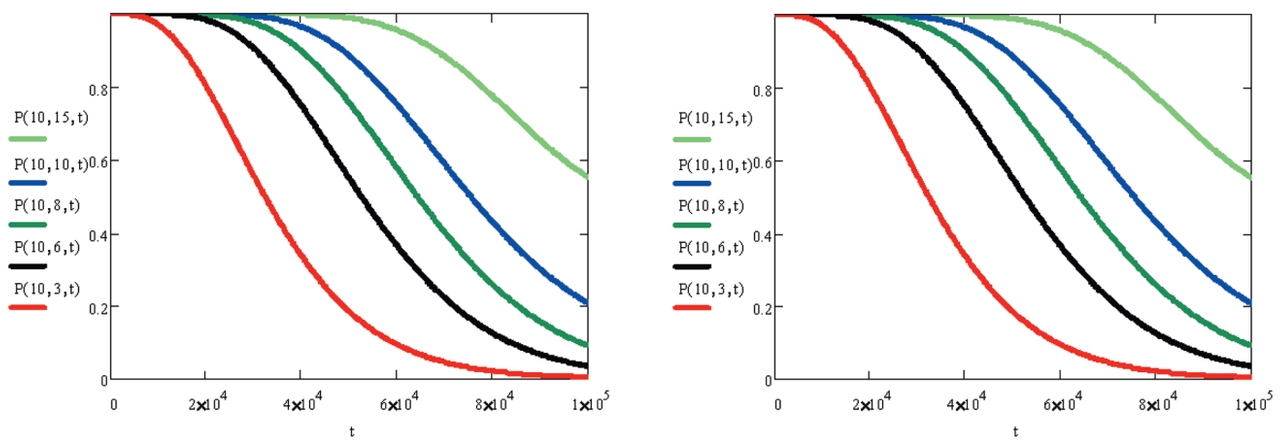

Figure 3. Dependence of P_{SMR} with partial recovery on the time t (h), number of backup elements m, main elements n if $\lambda = 10^{-5}$ (1/h) and r=3 with no regard to failure rate of a switch device

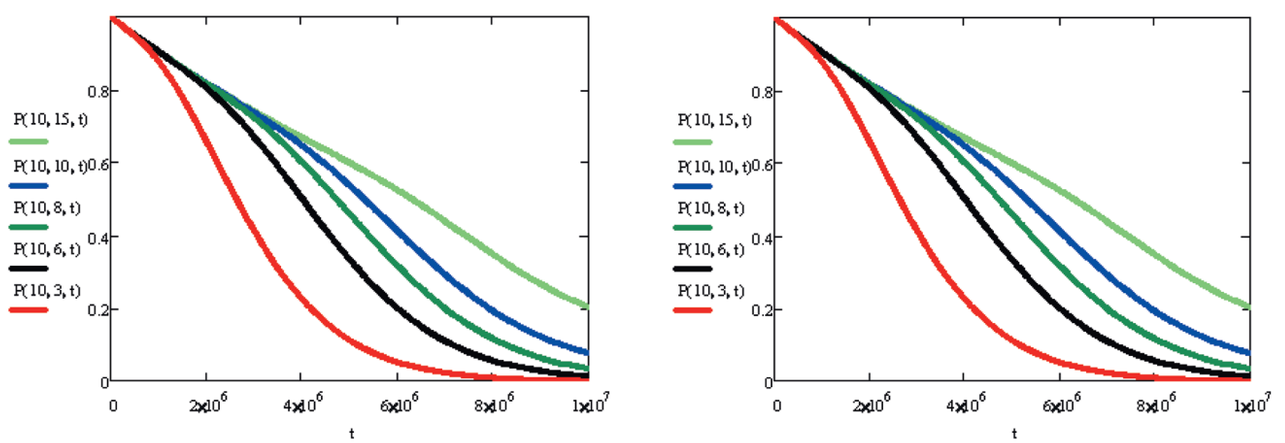

Figure 4. Dependence of P_{SMR} with partial recovery on the number of backup elements m, main elements n, time t (h) if $\lambda = 10^{-5}$ (1/h) and r=3 with regard to failure rate of a switch device $\lambda_{sd} = 10^{-7}$ (1/h)

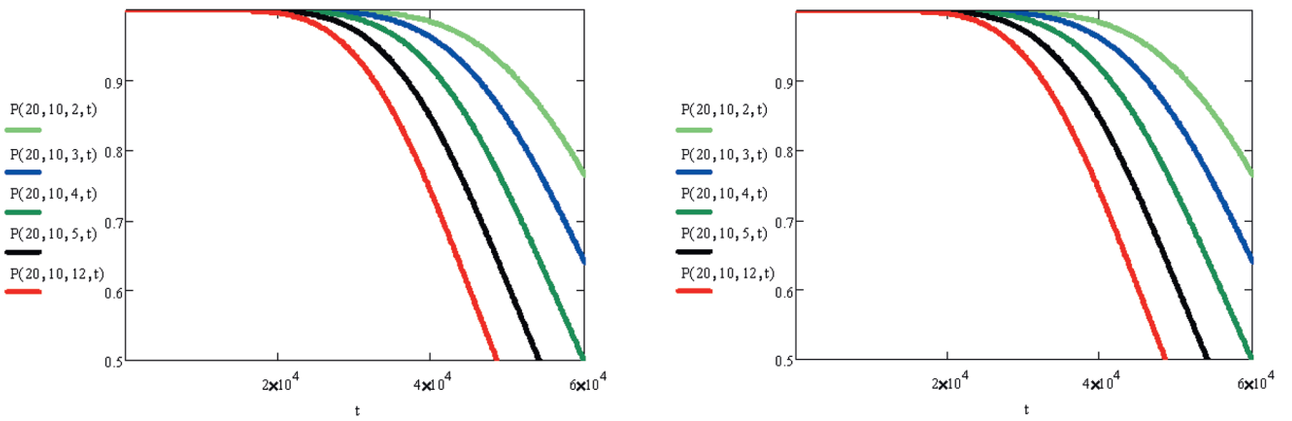

Figure 5. Dependence of P_{SMR} with partial recovery on the number of backup elements m, main elements n, time t (h) if $\lambda = 10^{-5}$ (1/h) and various r with regard to failure rate of a switch device $\lambda_{sd} = 10^{-7}$ and cost of recovery equipment $\lambda_r = 10^{-8}$ (1/h)

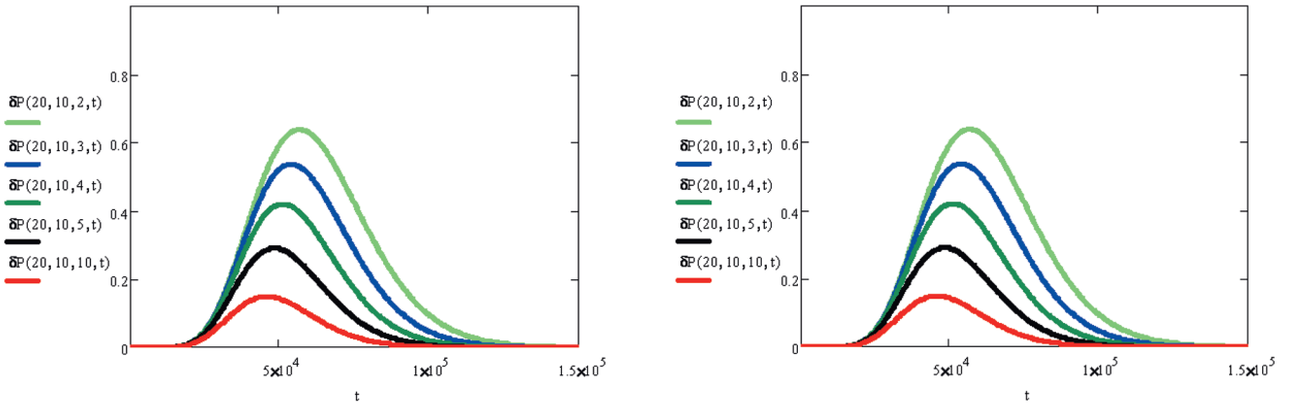

Figure 6. Dependence of $\delta P(n, m, r, t)$ with partial recovery on the number of backup elements m, main elements n, number of failed elements r required for recovery of one element, time t (h) if $\lambda = 10^{-5}$ (1/h) with regard to the failure rate of a switch device $\lambda_{sd} = 10^{-7}$ (1/h), $\lambda_{rec} = 10^{-8}$ (1/h)

This is none other than a geometrical progression, yet with truncation.

$$\sum_i v_i = \theta \le n. \qquad (11)$$

This sum shows the additional number of countered failures with no regard to the "remainders".

If regard is given to the "remainders", then:

$$v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor + m - r\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor;$$

$$v_3 = \left\lfloor \frac{\left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor + \left\lfloor \frac{m}{r} \right\rfloor (1-r) + m - r\left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor}{r} \right\rfloor. \qquad (12)$$

Experimental part

As a first approximation (for recovery out of m failed elements of a system) we deduce for v_1:

$$P_{SMR}(t) = \sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} \cdot e^{-\lambda_{sd}\cdot t} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda t} (1-e^{-\lambda t})^{m+j} e^{-\lambda_{sd} t}. \qquad (13)$$

Respective (13) graphs without and with regard to failure rates of a switch device are given in Fig. 3 and 4:

In case of additional expenditures for the recovery of the failed λ_{rec} we deduce:

$$P_{SMR}(t) = \sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} \cdot e^{-\lambda_{sd}\cdot t} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda t} (1-e^{-\lambda t})^{m+j} e^{-(\lambda_{sd}+\lambda_{rec})t}. \qquad (14)$$

Graphs of change (14) are given in Fig. 5.

We deduce the value of gain δP:

$$\delta P = [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} + \\ + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda t} (1-e^{-\lambda t})^{m+j}] e^{-(\lambda_{ny}+\lambda_{e})t} - \\ -[\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\lambda t} (1-e^{-\lambda t})^{n+m-i}] e^{-\lambda_{ny} t}. \quad (15)$$

The results of calculation of formula (15) in MathCad are given in Fig. 6.

Out of formula (15) let us deduce the conditions of gain under given λ_{rec}. Let us reconstruct (15) in order to identify λ_{rec}:

$$\delta P_{mp} + [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} (1-e^{-\lambda t})^{n+m-i}] e^{-\lambda_{ny} t} = \\ = [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} + \\ + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda\cdot t} (1-e^{-\lambda t})^{m-j}] e^{-(\lambda_{ny}+\lambda_{e})t}. \quad (16)$$

By dividing the left part of the formula (16) by the right part without the member that takes into consideration λ_{rec} and taking the logarithm we will deduce l_{rec}:

$$-\frac{1}{t} \ln \frac{\{\delta P_{mp} + [\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\lambda t} (1-e^{-\lambda t})^{n+m-i}] e^{-\lambda_{ny} t}}{\left([\sum_{i=n}^{n+m} C_{n+m}^{i} \cdot e^{-i\cdot\lambda\cdot t} \cdot (1-e^{-\lambda t})^{n+m-i} + \right.} = \lambda_{e}. \quad (17)$$
$$\left. + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j)\lambda\cdot t} (1-e^{-\lambda t})^{m+j}] e^{-\lambda_{ny} t} \right\}$$

Conclusion

The proposed sliding redundancy with recovery of elements out of several failed ones that retain the basis ensures a significant growth of dependability. In some cases the probability of no-failure under condition of perfect diagnosis grows 15-20% of the maximum possible gain. This approach can be used for systems in which the maintenance is impossible, e.g. spacecraft in orbit, in flight or in operation on other planets. Later, the matter of recovery time recording should be considered with the use of the mathematical tools of Markov chains, and the matters of supervision and diagnostics should be analyzed in further detail. Recording of slowdown of the elements built out of failed elements is of interest as well.

References

1. GOST 27.002-89. Industrial product dependability. General concepts. Terms and definitions. Moscow: Izdatelstvo standartov; 1990.

2. Shubinsky IB. Nadiozhnye otkazoustoychivye informatsionnye systemy. Metodi sinteza [Dependable failsafe information systems. Synthesis methods]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2016.

3. Vasiliev NP, Shubinsky IB. Analiticheskaya otsenka veroiatnosti ouspeshnoy adaptatsii k otkazam modulnykh vychislitelnykh sistem s mnogourovnevoy aktivnoy zashchitoy [Analytical evaluation of the probability of successful adaptation to failures of modular computer systems with multilevel active protection]. Izvestia vysshykh ouchebnykh zavedeniy. Priborostroenie [Journal of higher educational establishments. Instrument engineering]. 1994; 37: 3 – 4. Russian.

4. Tyurin SF. Problema sokhranenia funktsionalnoy polnoty boulevykh funktsiy pri "otkazakh" argumentov [The problem of maintaining the functional completeness of Boolean functions in case of argument "failure"]. Avtomatika i telemekhanika [Automation and remote control]. 1999; 9: 176 – 186. Russian.

5. Strogonov A, Tsybin S. Programmiruemaia kommutatsia PLIS: vzgliad iznutri [Software switching of FPGA: a look from the inside]. Available from: http://www.kit-e.ru/articles/plis/2010_11_56.php (accessed 16.10.2016).

6. Tyurin SF, Gromov OA. A residual basis search algorithm of fault-tolerant programmable logic integrated circuits. Russian Electrical Engineering. 2013; 84 (11): 647 – 651. DOI: 10.3103/S1068371213110163

7. Tyurin SF, Grekov AV. Functionally Complete Tolerant Elements. International Journal of Applied Engineering Research. 2015; 10 (14): 34433 – 34442.

8. Parfentiy AN, Khakhanov VI, Litvinova EI. Modeli infrastruktury servisnogo obsluzhivania tsifrovykh sistem na kristallakh [Models of infrastructure of digital systems on a chip maintenance service]. ASU i pribory avtomatiki [ACS and automatic devices]. 2007; 138: 83 – 99. Russian.

9. Carmichael C. Triple Module Redundancy Design Techniques for Virtex FPGAs. Available from: https://www.xilinx.com/support/documentation/application_notes/xapp197.pdf (accessed 07.12.2016).

About the author

Sergey F. Tyurin, Doctor of Engineering, Professor, Honored Inventor of the Russian Federation, Professor of Automation and Remote Control, Perm National Research Polytechnic University, Perm, Russia, e-mail: tyurin-sergfeo@yandex.ru

Received on 21.11.2016