Original article
Dependability, vol. 19 no.1, 2019 DOI: 10.21683/1729-2646-2019-19-1-4-9

Ensuring the dependability of technical facilities through triplication and quadrupling

Sergey F. Tyurin, *Perm National Research Polytechnic University, Perm State National Research University, Perm, Russia*

Sergey F. Tyurin

Abstract. *Redundancy, e.g. structural redundancy, is one of the primary methods of improving the dependability, ensures failsafety and fault tolerance of components, devices and systems. According to the International Patent Classification (IPC), the class of systems and methods G06F11/18 is defined as «using passive fault-masking of the redundant circuits, e.g. by quadrupling or by majority decision circuits». Obviously, «fault-masking» masks not only faults, but failures as well. The majority decision circuits (MDC) in the minimal configuration implements a «2-out-of-3» choice. According to the above definition, such redundancy should not require a special decision circuit. However, that is not always the case. In cases when the resulting signal out of a quadruple logic is delivered to, for instance, an executive device, a «3-out-of-4» selection circuit is required anyway. Another dependability-improving solution is defined by class G06F 11/20, «using active fault-masking, e.g. by switching out faulty elements or by switching in spare elements». The word «active» is missing here, thus we have active and passive fault tolerance. The paper examines passive fault tolerance that uses triplication and quadrupling and compares the respective probabilities of no-failure.The Weibull distribution is used that most adequately describes dependability in terms of radiation durability under the effects of heavy ions. It shows that in a number of cases quadrupling has a lower redundancy than triplication. A formula is proposed that describes the conditions of preferability of quadrupling at transistor level.*

Keywords: *dependability, redundancy, triplication, quadrupling, failures, faults, failure rate.*

For citation: *Tyurin SF. Ensuring the dependability of technical facilities through triplication and quadrupling. Dependability 2019;1: 4-9. DOI: 10.21683/1729-2646-2019-19-1-4-9*

Introduction

Redundancy, according to the new GOST [1] is "the method of guaranteeing the dependability of an item through the use of additional means and/or capabilities redundant as regards those minimally required for the performance of the desired function". Redundancy is especially important for systems whose operation is affected by radiation, e.g. spacecraft control systems. In this area the principle of radiation hardened by design (RHBD) is employed that involves, for example, triplication (triple modular redundancy, TMR) [2, 3]. Majority redundancy, whereas a failure or a fault are masked with no significant time expenditure, is indicated in the GOST [1]. However, the associated terms "passive" fault tolerance is not specified. Active, adaptive fault tolerance [4, 5] has a lower redundancy as compared to passive fault tolerance, but it requires procedures for supervision, diagnostics, reconfiguration that take significant time. In critical systems with relatively short time of operation, including those affected by radiation, majority redundancy of 300 percent or more is frequently used. At the same time, so-called quadrupling is also applicable. As it turns out, in some cases 300-percent redundancy can be more costly than 400-percent redundancy, if we take into consideration the required additional equipment that sometimes is not required in case of quadrupling. Let us examine the special features of such redundancy solutions.

Problem definition

Triplication involves "2-out-of-3" voting, i.e., in the binary case, the majority of entities. More generally, majority voting means the choice

$$(r+1)\text{–}out\text{–}of\text{–}(2r+1), \qquad (1)$$

where r is the number of masked (countered) failures.

The probability of no-failure $P(t)$ for Weibull's exponential model [6] is as follows:

$$P_{(r+1)from(2r+1)}(t)=\sum_{i=0}^{r} C_{2r+1}^{i+1}\left\{e^{-[(2r+1)-i]\cdot\lambda\cdot t^{\alpha}}\cdot\left(1-e^{-\lambda\cdot t^{\alpha}}\right)^{i}\right\}, \qquad (2)$$

where λ is the failure rate of one channel (the dimensionality is 1/h); α is the Weibull distribution coefficient, $1 < \alpha < 2$; t is the time of operation in hours; r is the number of countered failures (faults).

Thus, the redundancy for r failures (faults) by means of majority voted redundancy is described by formula

$$2r+1. \qquad (3)$$

I.e. failures (faults) are countered in r channels out of possible $2r + 1$.

In case of quadrupling, one failure (fault) is countered in one of the 4 elements that can be regarded both as channels and, for instance, separate CMOS transistors.

A broader interpretation of such configuration requires the following redundancy

$$(r+1)^2. \qquad (4)$$

In this case failures (faults) are countered in r channels out of possible $(r+1)^2$.

The probability of no-failure $P(t)$, if voting is not required, is as follows:

$$P_{(r)from(r+1)^2}(t)=\sum_{i=0}^{r} C_{(r+1)^2}^{i}\left\{e^{-[(r+1)^2-i]\cdot\lambda\cdot t^{\alpha}}\cdot\left(1-e^{-\lambda\cdot t^{\alpha}}\right)^{i}\right\}. \qquad (5)$$

Let us examine formulas (1) to (5) taking into account the special features of various implementations of redundancy.

Theoretical part

In case of a "2-out-of-3" majority voted redundancy ($r = 1$) we have three channels and majority elements (ME) and obtain the structure diagram of dependability (Fig. 1).

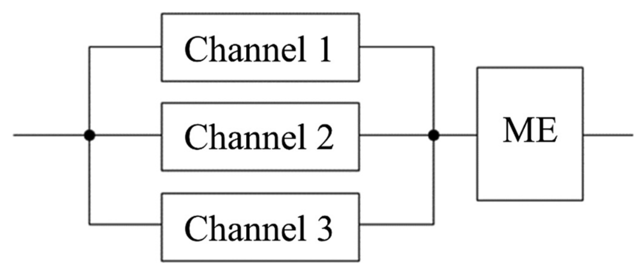


Figure 1. "2-out-of-3" majority voted redundancy

Given that the channel has n elements (e.g. transistors) and the complexity of ME is 12 transistors we obtain [7]:

$$P_{*3}=\left(3e^{-2\cdot(n)\cdot\lambda\cdot t^{\alpha}}-2e^{-3\cdot(n)\cdot\lambda\cdot t^{\alpha}}\right)e^{-(12)\cdot\lambda\cdot t^{\alpha}}. \qquad (6)$$

For the purpose of countering failures (faults) in ME, let us obtain the structure diagram of dependability (Fig. 2).

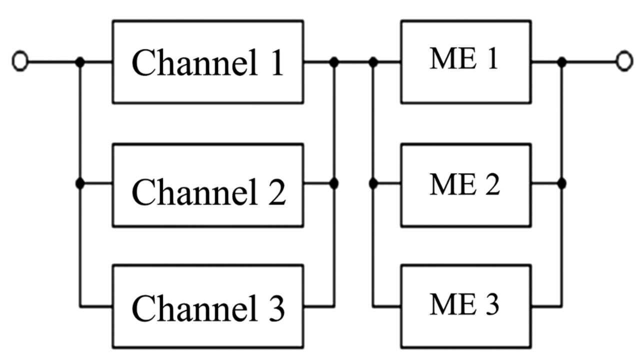


Figure 2. Majority voted redundancy

In this case we obtain:

$$P_{*33}=\left(3e^{-2\cdot(n)\cdot\lambda\cdot t^{\alpha}}-2e^{-3\cdot(n)\cdot\lambda\cdot t^{\alpha}}\right)\cdot\left(3e^{-2\cdot(12)\cdot\lambda\cdot t^{\alpha}}-2e^{-3\cdot(12)\cdot\lambda\cdot t^{\alpha}}\right). \qquad (7)$$

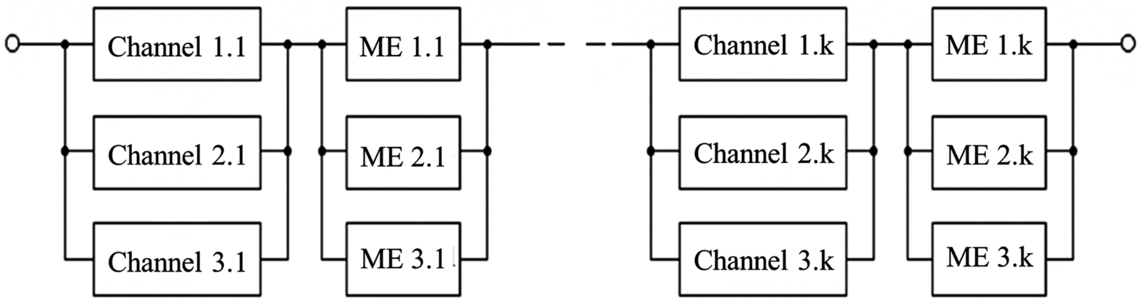


Figure 3. Deep majority voted redundancy

Furthermore, three power supplies are required. Thus, either the failure of one power supply, or the failure of one channel, or the failure of one majority element is countered.

“3-out-of-5” majority voted redundancy. Accordingly, five “3-out-of-5” majority elements are required:

$$P_{mvr}^{3\,oo\,5}(t)=e^{-5\cdot\lambda\cdot t^{\alpha}}+5e^{-4\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-\lambda\cdot t^{\alpha}}\right)+10e^{-3\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-\lambda\cdot t^{\alpha}}\right)^{2}\cdot$$
$$\cdot\begin{bmatrix} e^{-5\cdot\lambda_{me.3/5}\cdot t^{\alpha}}+5e^{-4\cdot\lambda_{me.3/5}\cdot t^{\alpha}}\left(1-e^{-\lambda_{me.3/5}\cdot t^{\alpha}}\right)+ \\ +10e^{-3\cdot\lambda_{me.3/5}\cdot t^{\alpha}}\left(1-e^{-\lambda_{me.3/5}\cdot t^{\alpha}}\right)^{2} \end{bmatrix}. \tag{8}$$

Majority voted redundancy that enables operation with one channel. In this case the system is capable of rearranging itself into a doubled configuration and further into a single-channel configuration, if necessary. That requires more complex additional equipment. Taking into account the additional equipment for reconfiguration (the failure rate is $\lambda_{д}$) we will obtain:

$$P_{mvr1}=\left[1-\left(1-e^{-\lambda\cdot t^{\alpha}}\right)^{3}\right]\cdot\left[3e^{-2(\lambda_{me}+\lambda_{\partial})t^{\alpha}}-2e^{-3(\lambda_{me}+\lambda_{\partial})t^{\alpha}}\right]. \tag{9}$$

Formula (9) does not take into consideration the probability of “oversight” in case real-time testing does not detect the failed channel.

The so-called **deep majority voted redundancy** involves “splitting” channels into k parts (Fig. 3).

Let us assume that λ, the failure rate of the entire channel, is split into k identical parts, then we obtain

$$P_{dm}=\left[3e^{-2\cdot n\frac{\lambda}{k}t^{\alpha}}-2e^{-3\cdot n\frac{\lambda}{k}t^{\alpha}}\right]^{k}\cdot\left[3e^{-2\cdot 12\cdot t^{\alpha}}-2e^{-3\cdot 12\cdot t^{\alpha}}\right]^{k}. \tag{10}$$

If n elements are quadrupled (r = 1), we obtain:

$$P_{4}(t)=\left[e^{-4\cdot\lambda\cdot t^{\alpha}}+4e^{-3\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-\lambda\cdot t^{\alpha}}\right)\right]^{n}. \tag{11}$$

However, formula (10) only holds for restriction $(r+1)^2\leq q$ in connection with the Mead-Conway requirements [8] on the maximum number of series-connected transistors r in a circuit that cannot be more than q (before and after quadrupling).

Let n be the number of transistors (while observing the Mead-Conway restriction) and m be the number of the circuit’s outputs. Then for r = 1 by comparing the quadrupling and triplication, we will obtain:

$$4n\leq 3n+12m. \tag{12}$$

Otherwise, if the following formula is correct

$$1\leq 12\frac{m}{n} \tag{13}$$

quadrupling is not “costlier” than triplication.

In the case of channel quadrupling “3-out-of-4” voting is required, therefore we will obtain:

$$P_{4}(t)=\left[e^{-4\cdot n\cdot\lambda\cdot t^{\alpha}}+4e^{-3\cdot n\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-n\cdot\lambda\cdot t^{\alpha}}\right)\right]^{n}\cdot$$
$$\cdot\left[e^{-4\cdot\lambda\cdot t^{\alpha}}+4e^{-3\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-\lambda\cdot t^{\alpha}}\right)\right]^{m}. \tag{14}$$

Experimental part

With no regard to the probability of no-failure of the majority element we obtain the probability of no-failure of a majority system P_{mvr}^{2oo3} with a “2-out-of-3” selection:

$$P_{м.с}^{2\,из\,3}=p^{3}+3p^{2}(1-p)=$$
$$=1-(1-p)^{3}-3p\left(1-p^{2}\right)=3p^{2}-2p^{3}. \tag{15}$$

Thus, for example, if P = 0,9 we obtain a significant increase:

$$P_{mvr}^{2oo3}(t)=3(0.9)^{2}-2(0.9)^{3}=0.972. \tag{16}$$

A “3-out-of-5” majority voted redundancy improves the dependability even more:

$$P_{mvr}^{3oo5}(t)=P^{5}+5P^{4}(1-P)+10P^{3}(1-P)^{2}. \tag{17}$$

For example,

$$P_{mvr}^{3oo5}(t)=(0.9)^{5}+5(0.9)^{4}(0.1)+10(0.9)^{3}(0.1)^{2}=0.99144. \tag{18}$$

With no regard to this additional equipment and majority elements, that can also be triplicated, in the case of majority voted redundancy that enables operation with one remained channel, we will obtain:

$$P_{mvr1}=P^{3}+3P^{2}(1-P)+3P(1-P)^{2}=1-(1-P)^{3}. \tag{19}$$

In this case the probability of no-failure reaches the value

$$P_{mvr1} = 1 - (0.1)^3 = 0.999. \quad (20)$$

Let us obtain in MathCad the time curves of comparison of the formulas for the probability of no-failure for a single-channel digital system $e^{-\lambda t}$ with majority voting redundancy of "2-out-of-3" (5) and "3-out-of-5" (7) (Fig. 4).

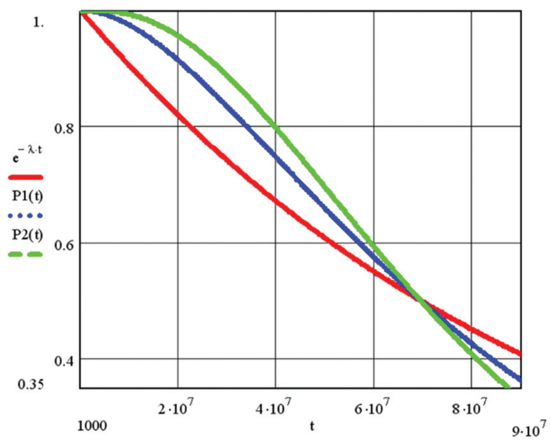


Figure 4. Comparison of a single-channel digital system $e^{-\lambda t}$ with a majority voted redundancy: "2-out-of-3" ($P_1(t)$, blue line), "3-out-of-5" ($P_2(t)$, green line) if $\lambda = 10^{-8}$, $\alpha = 1$

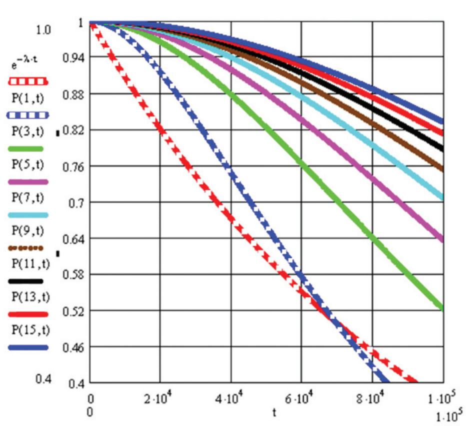


Figure 5. Probability of no-failure curves of a system without majority voted redundancy $e^{-\lambda t}$, with majority voted redundancy $P_1(t)$ and deep majority voted redundancy $P_k(t)$ (k layers, $k = 3, 5, 7, 9, 11, 13, 15$) if $\lambda = 10^{-8}$

We see that the majority voting redundancy "raises" the exponential curve beyond the point that corresponds to approximately a third of the time axis, but this causes a "slack" in the last third. After a certain value of time the probability of no-failure becomes less than 0.5 an the non-redundant configuration becomes better that a redundant one. It is clear that such probability should not be allowed to happen. Let us evaluate the deep majority voted redundancy (Fig. 5).

We can see that the deep majority voted redundancy considerably improves the dependability as the number of layers k grows.

If $\lambda = 10^{-5}$, $\lambda_{me} = \dfrac{\lambda}{\alpha_1}$, $\alpha_1 = 10$ we obtain the optimum for $k = 12$, $t = 10^4$ (Fig. 6, a). If $\lambda = 10^{-3}$, $\lambda_{me} = 10^{-5}$ we obtain the optimum for k = 100 (Fig. 6, b).

The cost of the system increases in comparison with ordinary majority voted redundancy:

$$C_m = 3(C_\lambda + C_{me} + C_{ps}), \quad (21)$$

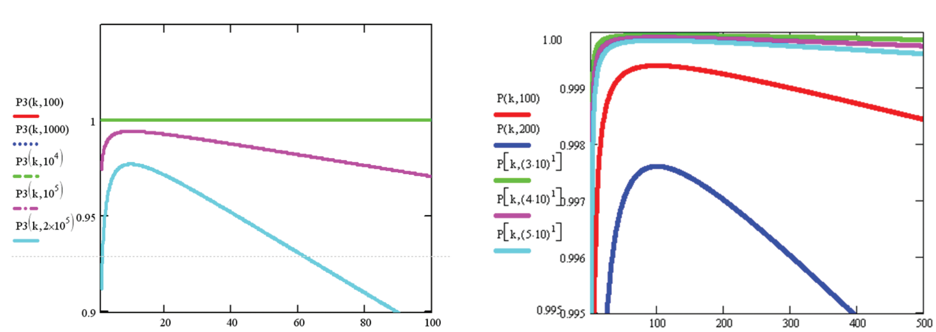
where C_λ is the cost of one channel, C_{me} is the cost of the majority element, C_{ps} is the cost of the power supply. The signal propagation delay only increases by the delay of one majority element τ_{me}. In (21), the growing complexity of routing is not taken into consideration. In case of deep majority voted redundancy, the costs are significantly higher:

$$C_{dm} = 3(C_\lambda + kC_{me} + C_{ps}), \quad (22)$$

while the signal propagation delay is increased by the delay k of the $k \cdot \tau_{me}$ majority elements. Normally, that is done if high dependability must be ensured, while the reduced performance is compensated by algorithmic methods.

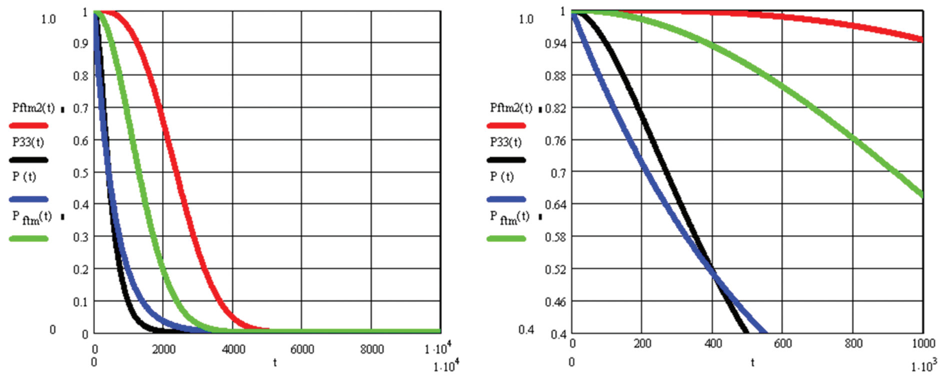
Let us obtain comparison graphs for transistor-for-transistor circuit quadrupling with majority voted redundancy. Countering a failure of any single transistor in each transistor configuration (each group of four transistors) requires quadruple redundancy [9] and is described with formula:

$$P_{fmt}(t) = e^{-(4)\lambda \cdot t} + 4 \cdot e^{-3 \cdot \lambda \cdot t}\left(1 - e^{-1 \cdot \lambda \cdot t}\right). \quad (23)$$



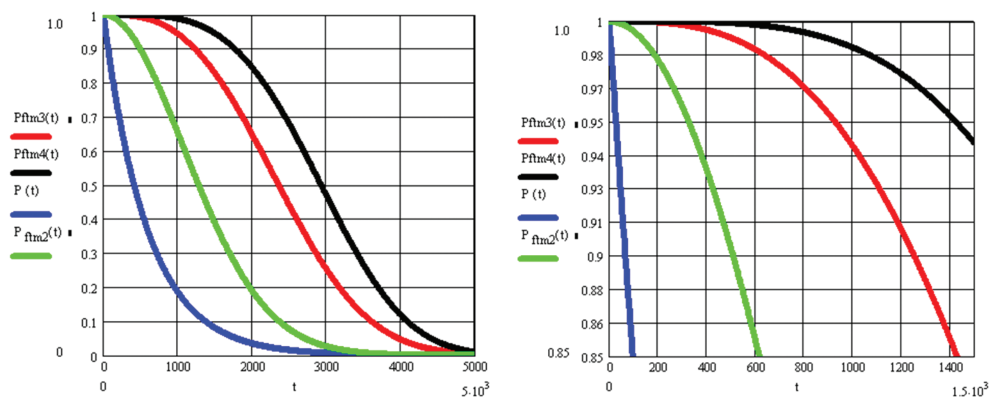
a) b)

Figure 6. Optimum of deep majority voted redundancy: a) $k = 12$, b) $k = 100$



a) b)

Figure 7. Change graphs of the probability of no-failure of a non-redundant circuit $P(t)$; a quadruple circuit that counters one failure $P_{ftm}(t)$; a triplicated circuit with three majority elements $P_{33}(t)$ and a circuit that counters two failures $P_{ftm}2(t)$ if the failure rate is 10^{-5} 1/h; a) within probability range from 1 to 0; b) within probability range from 1 to 0.4



a) b)

Figure 8. Change graphs of the probability of no-failure of a non-redundant circuit $P(t)$; a quadruple circuit that counters one failure $P_{ftm}2(t)$; a circuit that counters two failures $P_{ftm}3(t)$ and a circuit that counters three failures $P_{ftm}4(t)$ if the failure rate is 10^{-5} 1/h; a) within probability range from 1 to 0; b) within probability range from 1 to 0.4

Countering a failure of any two transistors in each transistor configuration requires nonuple redundancy and is described with formula:

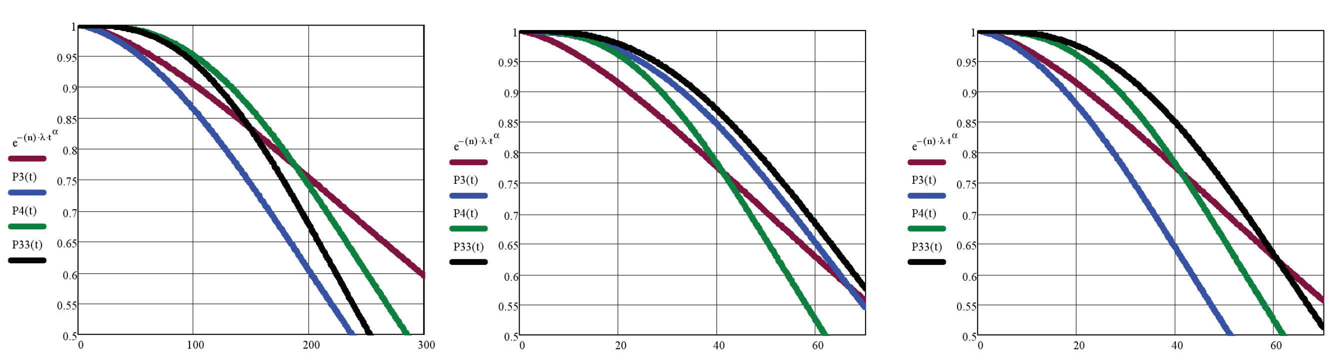
$$P_{fmt2}(t)=e^{-(9)\cdot\lambda\cdot t}+9\cdot e^{-8\cdot\lambda\cdot t}\left(1-e^{-1\cdot\lambda\cdot t}\right)+36\cdot e^{-7\cdot\lambda\cdot t}\left(1-e^{-1\cdot\lambda\cdot t}\right)^2. \quad (24)$$

The respective graphs are shown in fig. 7.

Countering a failure of any three transistors in each transistor configuration requires sixteen-fold redundancy and is described with formula:

$$P_{fmt3}(t)=e^{-(16)\lambda\cdot t}+16\cdot e^{-15\cdot\lambda\cdot t}\left(1-e^{-1\cdot\lambda\cdot t}\right)+$$
$$+120\cdot e^{-14\cdot\lambda\cdot t}\left(1-e^{-1\cdot\lambda\cdot t}\right)^2+560\cdot e^{-13\cdot\lambda\cdot t}\left(1-e^{-1\cdot\lambda\cdot t}\right)^3. \quad (25)$$

Change graphs of the probabilities of no-failure of a non-redundant circuit $P(t)$; a FCTLUT circuit that counters one failure $P_{ftm}2(t)$; a FCTLUT circuit that counters two failures $P_{ftm}3(t)$ and a FCTLUT circuit that counters three failures $P_{ftm}4(t)$ if $n = 4$ are shown in in fig. 8.



a) b) c)

Figure 9. Channel quadrupling: a) $n = 10$, $m = 1$; b) $n = 100$, $m = 1$; c) $n = 100$, $m = 10$

Comparison of channel quadrupling $P_4(t)$ with a non-redundant circuit and triplication $P_3(t)$; $P_{33}(t)$ is shown in fig. 9.

Conclusion

Quadrupling at transistor level is the most efficient solution in terms of designing radiation-resistant digital equipment. It enables higher probability of no-failure as compared to triplication throughout the timeframe. In some cases the redundancy of quadrupling is lower than that of triplication, if majority elements are taken into account. Countering any single failure in each transistor configuration requires quadruple redundancy. Countering any two failures in each transistor configuration requires nonuple redundancy that enables a higher probability of no-failure of a quadruple circuit, yet it is outperformed throughout the timeframe by a sixteen-fold redundant circuit that counters the failures of any three transistors in each transistor configuration whose implementation required sixteen-fold redundancy. Countering powers supply failures can be done by doubling it as part of a quadruple circuit, e.g. as it is proposed in [10].

References

[1] GOST 27.002-2015. Dependability in technics. Terms and definitions. Moscow: Standartinform; 2016 [in Russian].

[2] Ramaswamy S, Rockett L, Patel D et al. A Radiation Hardened Reconfigurable FPGA, <https://pdfs.semanticscholar.org/57f8/ff540360eadceafc062797b7a01065f6f9cc.pdf, 2018 [accessed 30.03.2018].

[3] Borisov YuI. O vybore arkhitektury otkazoustoychivykh vychislitelnykh kompleksov dlya kosmicheskikh apparatov [On the selection of the architecture of failsafe computer systems for spacecraft]. Dependability 2004;2(21):46-51 [in Russian].

[4] Schäbe H, Shubinsky IB. Limit reliability of structural redundancy. Dependability 2016;16(1):9-13.

[5] Carl Carmichael. Triple Module Redundancy Design Techniques for Virtex FPGAs, <https://www.xilinx.com/support/documentation/application_notes/xapp197.pdf>, 2018 [accessed 30.03.2018].

[6] Shubinsky IB. Nadiozhnie otkazoustoychivie informatsionnie sistemy. Metody sinteza [Dependable failsafe information systems. Synthesis methods]. Moscow: Dependability Journal; 2016 [in Russian]. ISBN 978-5-7572-0399-7.

[7] 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]. Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie. 1994;37(3-4):47 [in Russian].

[8] Tarasov AA. Minimizatsiya vremeni funktsionalnoy rekonfiguratsii raspredelennoy otkazoustoychivoy sistemy [Minimizing the time of functional reconfiguration of a distributed failsafe system]. Dependability 2010;2(37):24-29 [in Russian].

[9] Tyurin SF. Moving redundancy of tolerant elements. Dependability 2017;17(1):17-21.

[10] Weibull W. A statistical distribution function of wide applicability. Journal of Applied Mechanics, Transactions of ASME 1951;18:293–297.

[11] Mead CA, Conway L. Introduction to VLSI Systems, <https://www.researchgate.net/publication/234388249_Introduction_to_VLSI_systems>, 2018 [accessed 30.03.2018].

About the author

Sergey F. Tyurin, Doctor of Engineering, Professor, Professor of Automation and Remote Control, Perm National Research Polytechnic University (www.pstu.ru),

Professor of Computer Software, Perm State National Research University (www.psu.ru), Perm, Russia, e-mail: tyurinsergfeo@yandex.ru

Received on 25.04.2018