УДК 621.399
Оригинальная статья
Надежность, том 19, №1, 2019 DOI: 10.21683/1729-2646-2019-19-1-4-9

Обеспечение надежности технических средств путем их троирования и расчетверения

Сергей Ф. Тюрин, *Пермский национальный исследовательский политехнический университет, Пермский государственный национальный исследовательский университет, Пермь, Россия*

Сергей Ф. Тюрин

Резюме. *Резервирование, в частности, структурное является одним из основных способов повышения надёжности, обеспечивает отказо и сбоеустойчивость элементов, устройств и систем. Согласно МПК – международной патентной классификации, класс устройств и способов G06F11/18 – «using passive fault-masking of the redundant circuits, e.g. by quadding or by majority decision circuits». У нас это трактуется как «повышение надёжности за счёт использования пассивного маскирования сбоев, например, с помощью расчетверения (quadding) или мажоритарных решающих схем». При этом, очевидно, что «fault-masking» – это маскирование не только сбоев, но и отказов. Мажоритарные решающие схемы или просто мажоритары в минимальном варианте реализуют выбор «2 из 3-х». Принятый термин «расчетверение» на взгляд автора не слишком благозвучный, ибо он может вызвать ассоциацию с четвертованием, но ничего не поделаешь. Такая избыточность согласно выше приведённой формулировки вроде как не требует специальной решающей схемы. Однако, это выполняется не всегда. В случае выдачи результирующего сигнала после учетверённой логики, например, на исполнительный орган, всё равно нужна схема выбора «3 из 4-х». Другой вариант повышения надёжности фиксирует класс G06F 11/20 – «using active fault-masking, e.g. by switching out faulty elements or by switching in spare elements». У нас он переводится как «с использованием маскирования сбоев с помощью замещения, например, выключения сбойных элементов или переключения на резервные элементы». Здесь пропущено слово «активного», таким образом имеем активную и пассивную отказоустойчивость. В статье исследуется пассивная отказоустойчивость, использующая троирование и расчетверение и сравниваются соответствующие вероятности безотказной (бессбойной) работы. При этом используется распределение Вейбулла, которое наиболее адекватно описывает надёжность в смысле радиационной стойкости в условиях воздействия тяжёлых заряженных частиц. Показывается, что в ряде случаев расчетверение имеет меньшую избыточность, чем троирование. Предлагается формула, описывающая условия предпочтительности расчетверения на транзисторном уровне.*

Ключевые слова: *надёжность, резервирование, троирование, расчетверение, отказы, сбои, интенсивность отказов.*

Формат цитирования: *Тюрин С.Ф. Обеспечение надежности технических средств путем их троирования и расчетверения // Надежность. 2019. №1. С. 4-9. DOI: 10.21683/1729-2646-2019-19-1-4-9*

Введение

Резервирование (Redundancy) согласно используемому новому ГОСТ [1] это «способ обеспечения надежности объекта за счет использования дополнительных средств и (или) возможностей, избыточных по отношению к минимально необходимым для выполнения требуемых функции». Особенно важно резервирование для систем, работающих в условиях радиации, например, для систем управления космическими аппаратами. В этой области применяют радиационно-стойкое проектирование (Radiation Hardened by Design, RHBD), включающее, например, троирование (Triple Modular Redundancy, TMR) [2, 3]. Мажоритарное резервирование, при котором отказ или сбой маскируются без особенных временных затрат, указано в ГОСТ [1]. Однако нет соответствующего термина «пассивная» отказоустойчивость. Активная, адаптивная отказоустойчивость [4, 5] обладает меньшей избыточностью, по сравнению с пассивной, но она требует процедур контроля, диагностики, реконфигурации, на что требуется значительное время. Для особо ответственных систем (систем критического применения), работающих относительно короткое время, в том числе в условиях радиации, часто применяют мажоритарное резервирование, требующее более чем 300% избыточности. В то же время иногда может быть применено и так называемое расчетверение (учетверение). Оказывается, в ряде случаев избыточность в 300% может быть затратнее избыточности в 400%, если учитывать дополнительное требуемое оборудование (так называемые «мажоритары»), которые иногда не нужны при расчетверении. Рассмотрим особенности таких вариантов резервирования.

Постановка задачи

При троировании происходит голосование по принципу «два из трёх», то есть в бинарном случае – по большинству единиц. В более широком смысле под мажоритированием понимают выбор

$$(r{+}1) \text{ from } (2r{+}1), \tag{1}$$

где r – число маскируемых (парируемых) отказов.

Вероятность безотказной работы $P(t)$ для экспоненциальной модели Вейбулла [6] имеет вид:

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

где λ – интенсивность отказов одного канала (размерность 1/час); α – коэффициент распределения Вейбулла, $1 < \alpha < 2$; t – время работы в часах; r – число парируемых отказов (сбоев).

Таким образом, избыточность для r отказов (сбоев) путём мажоритирования описывается выражением

$$2r{+}1. \tag{3}$$

То есть, парируются отказы (сбои) в r каналах из возможных $2r + 1$.

При расчетверении парируется один отказ (сбой) в одном из 4-х элементов, которые могут трактоваться и как каналы, и как, например, отдельные КМОП транзисторы.

Более широкая трактовка такого резервирования может быть названа, например, «расквадрением, квадрированием» и требует избыточности

$$(r{+}1)^2. \tag{4}$$

В этом случае парируются отказы (сбои) в r элементах из возможных $(r{+}1)^2$.

Вероятность безотказной работы $P(t)$ при отсутствии необходимости в устройстве голосования имеет вид:

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

Исследуем выражения (1) – (5) с учётом особенностей различной реализации избыточности.

Теоретическая часть

При мажоритировании 2 из 3-х (r = 1) имеем три канала и мажоритарный элемент (МЭ), получаем структурную схему надёжности (рис. 1).

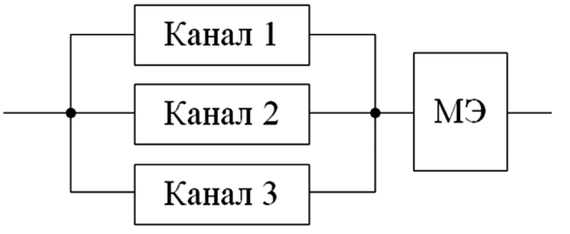


Рисунок 1 – Мажоритирование 2 из 3-х

Получаем с учетом того, что в канале n элементов (например, транзисторов) и сложность МЭ – 12 транзисторов [7]:

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

С целью парирования отказов (сбоев) в МЭ получим структурную схему надёжности (рис. 2).

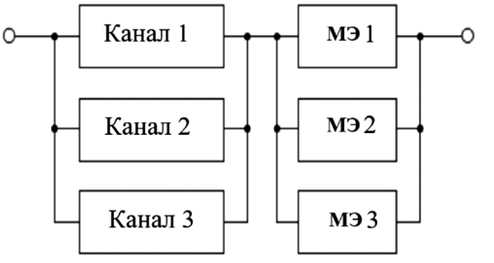


Рисунок 2 – Мажоритирование мажоритарных элементов

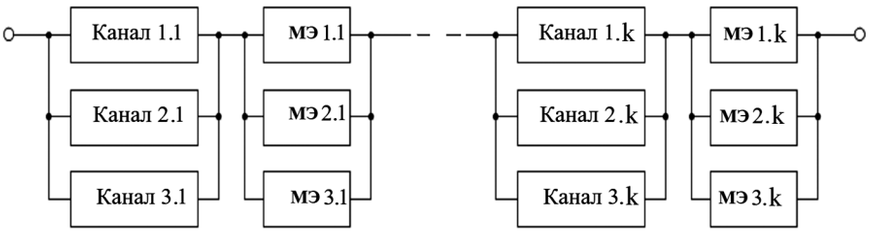


Рисунок 3 – Глубокое мажоритирование

В этом случае получим:

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

Кроме того, необходимы три источника питания. Таким образом, парируется либо отказ одного источника питания, либо отказ одного канала, либо отказ одного мажоритара.

Мажоритирование 3 из 5. Соответственно, необходимо пять мажоритарных элементов «3 из 5»:

$$P_{м.с}^{3\ из\ 5}(t)=e^{-5\cdot\lambda\cdot t^{\alpha}}+5e^{-4\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-\lambda\cdot t^{\alpha}}\right)+10e^{-3\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-\lambda\cdot t^{\alpha}}\right)^{2}\cdot$$
$$\cdot\left[\begin{array}{c}e^{-5\cdot\lambda_{м.э.3/5}\cdot t^{\alpha}}+5e^{-4\cdot\lambda_{м.э.3/5}\cdot t^{\alpha}}\left(1-e^{-\lambda_{м.э.3/5}\cdot t^{\alpha}}\right)+\\+10e^{-3\cdot\lambda_{м.э.3/5}\cdot t^{\alpha}}\left(1-e^{-\lambda_{м.э.3/5}\cdot t^{\alpha}}\right)^{2}\end{array}\right]. \quad (8)$$

Мажоритирование с возможностью работы на одном канале. В этом случае система способна перестраиваться в дублированную и из неё, в случае необходимости, – в одноканальную. Для этого нужна более сложная дополнительная аппаратура. С учётом дополнительной аппаратуры реконфигурации (интенсивность отказов $\lambda_д$) получим:

$$P_{м.с.1}=\left[1-\left(1-e^{-\lambda\cdot t^{\alpha}}\right)^{3}\right]\cdot\left[3e^{-2(\lambda_{м.э}+\lambda_д)t^{\alpha}}-2e^{-3(\lambda_{м.э}+\lambda_д)t^{\alpha}}\right]. \quad (9)$$

Выражение (9) не учитывает вероятности «промаха» в случае, если оперативное тестирование не приводит к обнаружению отказавшего канала.

При так называемом **глубоком мажоритировании** каналы «дробятся» на k частей (рис. 3).

Примем допущение, что λ – интенсивность отказов всего канала – разбивается на k одинаковых частей, тогда получим

$$P_{г.м}=\left[3e^{-2\cdot n\frac{\lambda}{k}t^{\alpha}}-2e^{-3\cdot n\frac{\lambda}{k}t^{\alpha}}\right]^{k}\cdot\left[3e^{-2\cdot12\cdot t^{\alpha}}-2e^{-3\cdot12\cdot t^{\alpha}}\right]^{k}. \quad (10)$$

При расчетверении ($r = 1$) n элементов получим:

$$P_4(t)=\left[e^{-4\cdot\lambda\cdot t^{\alpha}}+4e^{-3\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-\lambda\cdot t^{\alpha}}\right)\right]^{n}. \quad (11)$$

Однако выражение (10) справедливо лишь до ограничения $(r+1)^2 \le q$ в связи с требованиями Мида-Конвей [8] на максимальное число последовательно соединённых транзисторов r в схеме, их не может быть больше q (до и после расчетверения).

Пусть n – количество транзисторов (при соблюдении ограничений Мида-Конвей); m – число выходов схемы. Тогда для $r = 1$, сравнивая рачетверение и троирование, получим:

$$4n \le 3n+12m. \quad (12)$$

Иначе, при выполнении соотношения

$$1 \le 12\frac{m}{n} \quad (13)$$

расчетверение «не дороже» троирования.

В случае расчетверения каналов необходимо устройство голосования «три из четырёх», поэтому получим:

$$P_4(t)=\left[e^{-4\cdot n\cdot\lambda\cdot t^{\alpha}}+4e^{-3\cdot n\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-n\cdot\lambda\cdot t^{\alpha}}\right)\right]^{n}\cdot$$
$$\cdot\left[e^{-4\cdot\lambda\cdot t^{\alpha}}+4e^{-3\cdot\lambda\cdot t^{\alpha}}\left(1-e^{-\lambda\cdot t^{\alpha}}\right)\right]^{m}. \quad (14)$$

Экспериментальная часть

Без учёта вероятности безотказной работы мажоритарного элемента получаем вероятность безотказной работы мажоритарной системы $P_{м.с}^{2\ из\ 3}$ с выбором 2 из 3:

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

Таким образом, например, для $P = 0{,}9$ получаем существенный прирост:

$$P_{м.с}^{2\ из\ 3}(t)=3(0{,}9)^2-2(0{,}9)^3=0{,}972. \quad (16)$$

Мажоритирование 3 из 5 ещё более повышает надёжность:

$$P_{м.с}^{3\ из\ 5}(t)=P^5+5P^4(1-P)+10P^3(1-P)^2. \quad (17)$$

Например,

$$P_{м.с}^{3\ из\ 5}(t)=(0{,}9)^5+5(0{,}9)^4(0{,}1)+10(0{,}9)^3(0{,}1)^2=0{,}99144. \quad (18)$$

Без учёта этой дополнительной аппаратуры и мажоритарных элементов, которые также троируются, в случае мажоритирования с возможностью работы на одном оставшемся канале, получим:

$$P_{м.с1}=P^3+3P^2(1-P)+3P(1-P)^2=1-(1-P)^3. \quad (19)$$

В этом случае вероятность безотказной работы достигает значения

$$P_{м.с1} = 1 - (0,1)^3 = 0,999. \qquad (20)$$

Получим временные графики сравнения выражений вероятности безотказной работы для одноканальной цифровой системы $e^{-\lambda t}$ с мажоритированием: 2 из 3 (5) и 3 из 5 (7) в системе компьютерной математики MathCad (рис. 4).

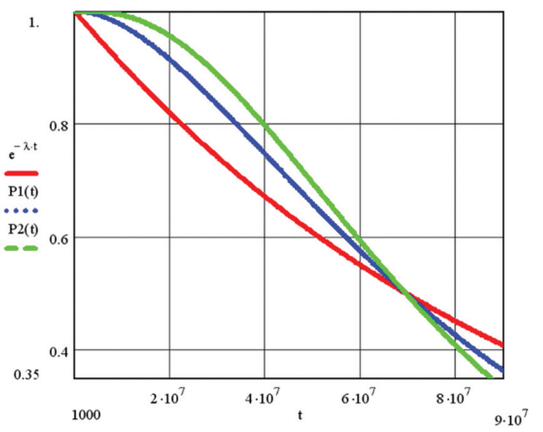


Рисунок 4 – Сравнение одноканальной цифровой системы $e^{-\lambda t}$ с мажоритированием: 2 из 3 ($P_1(t)$ – синяя линия), – 3 из 5 ($P_2(t)$ – зелёная линия) при $\lambda = 10^{-8}$, $\alpha = 1$

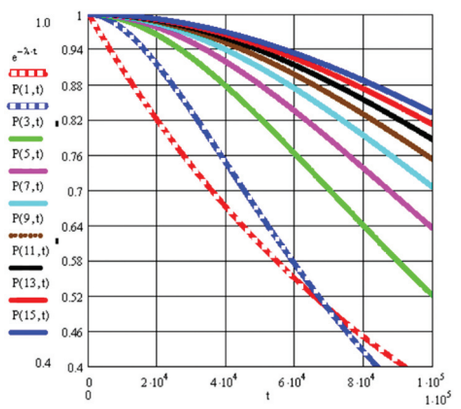


Рисунок 5 – Графики изменения вероятности безотказной работы системы без мажоритирования $e^{-\lambda t}$, с мажоритированием $P_1(t)$ и с глубоким мажоритированием $P_k(t)$ (k слоёв, $k = 3, 5, 7, 9, 11, 13, 15$) при $\lambda = 10^{-8}$

Видим, что мажоритирование как бы «поднимает» экспоненту вверх за точку, соответствующую примерно трети временной оси, но это приводит к «провисанию» в последней трети. После некоторого значения времени вероятность безотказной работы становится менее 0,5 и нерезервированная структура становится лучше резервированной. Ясно, что до такой вероятности доводить дело не стоит. Оценим глубокое мажоритирование (рис. 5).

Видим, что глубокое мажоритирование значительно повышает надёжность по мере увеличения количества k слоёв.

Для $\lambda = 10^{-5}$, $\lambda_{м.э} = \lambda / \alpha_1$, $\alpha_1 = 10$ получим оптимум для $k = 12$, $t = 10^4$ (рис. 6, а). При $\lambda = 10^{-3}$, $\lambda_{м.э} = 10^{-5}$ получим оптимум для $k = 100$ (рис. 6, б).

При этом стоимость системы увеличивается по сравнению с обычным мажоритированием:

$$C_м = 3(C_\lambda + C_{м.э} + C_{и.п}), \qquad (21)$$

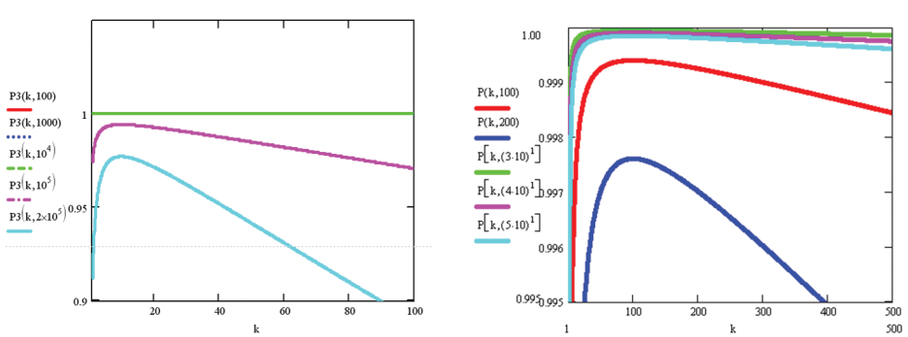
где C_λ – стоимость одного канала, $C_{м.э}$ – стоимость мажоритара, $C_{и.п}$ – стоимость источника питания. Задержка прохождения сигнала увеличивается всего на величину задержки одного мажоритара $\tau_{м.э}$. При этом (21) не учитывает усложнение связей (трассировки). В случае глубокого мажоритирования затраты существенно больше:

$$C_{г.м} = 3(C_\lambda + kC_{м.э} + C_{и.п}), \qquad (22)$$

а задержка прохождения сигнала увеличивается на величину задержки k мажоритаров $k \cdot \tau_{м.э}$. Обычно на это идут в случае необходимости обеспечения высокой надёжности, а снижение производительности компенсируют алгоритмическими методами.

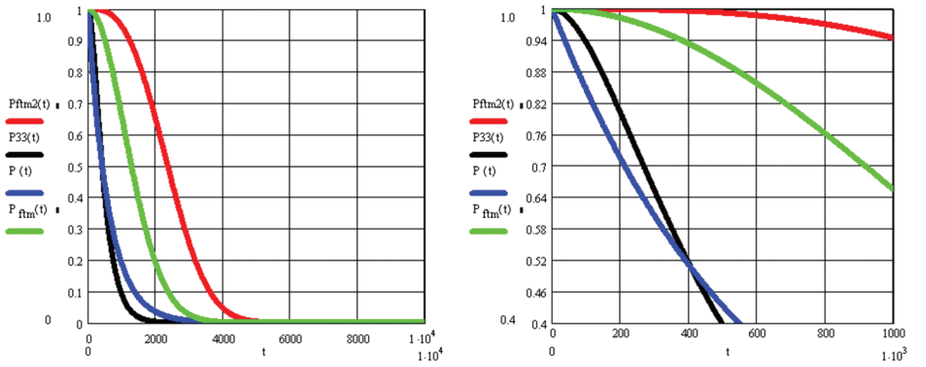
Получим графики сравнения потранзисторного расчетверения схемы с мажоритированием. Парирование отказа одного любого транзистора в каждой транзисторной структуре – в каждой четвёрке транзисторов – требует четырёхкратной избыточности [9] и описывается выражением:

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



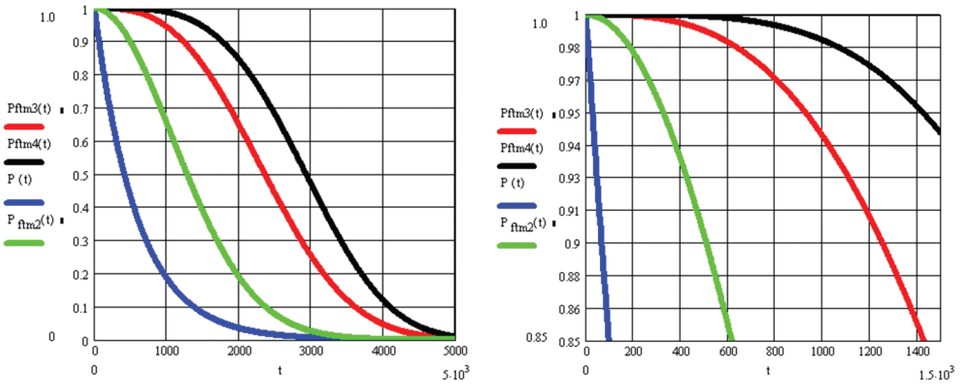
а) б)

Рисунок 6 – Оптимум глубокого мажоритирования: а) $k = 12$, б) $k = 100$.



а) б)

Рисунок 7 – Графики изменения вероятностей безотказной работы нерезервированной схемы $P(t)$; расчетверённой схемы, парирующей один отказ $P_{ftm}(t)$; троированной схемы с тремя мажоритарными элементами $P_{33}(t)$ и схемы, парирующей два отказа $P_{ftm2}(t)$ при интенсивности отказов 10^{-5} 1/час; а) в диапазоне вероятности от 1 до 0; б) в диапазоне вероятности от 1 до 0,4



а) б)

Рисунок 8 – Графики изменения вероятностей безотказной работы нерезервированной схемы $P(t)$; расчетверённой схемы, парирующей один отказ $P_{ftm2}(t)$; схемы, парирующей два отказа $P_{ftm3}(t)$ и схемы, парирующей три отказа $P_{ftm4}(t)$ при интенсивности отказов 10^{-5} 1/час; а) в диапазоне вероятности от 1 до 0; б) в диапазоне вероятности от 1 до 0,4

Парирование отказа любых двух транзисторов в каждой транзисторной структуре требует девятикратной избыточности и описывается выражением:

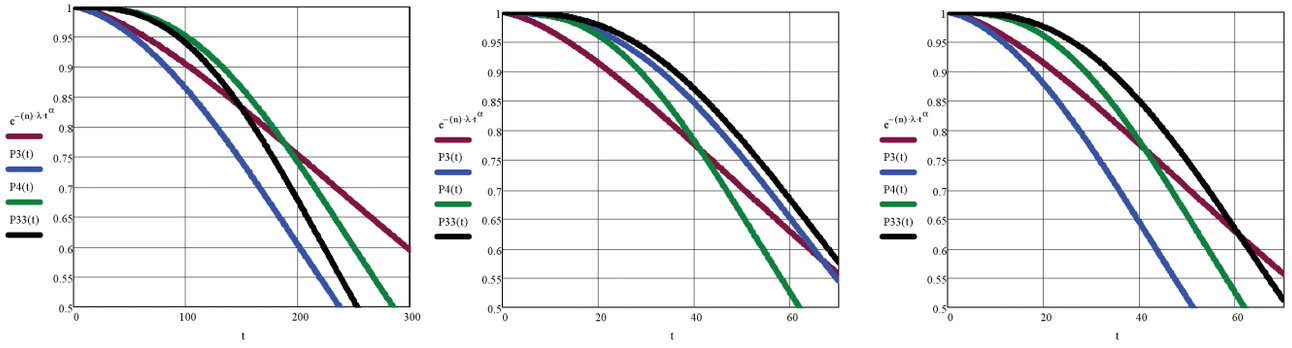
$$P_{fmt2}(t)=e^{-(9)\cdot\lambda\cdot t}+9\cdot e^{-8\cdot\lambda\cdot t}\left(1-e^{-1\cdot\lambda\cdot t}\right)+36\cdot e^{-7\cdot\lambda\cdot t}\left(1-e^{-1\cdot\lambda\cdot t}\right)^2. \quad (24)$$

Соответствующие графики изображены на рис. 7.

Парирование отказа любых трех транзисторов в каждой транзисторной структуре требует шестнадцатикратной избыточности и описывается выражением:

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

Графики изменения вероятностей безотказной работы нерезервированной схемы $P(t)$; схемы FCTLUT, парирующей один отказ $P_{ftm2}(t)$; схемы FCTLUT, парирующей два отказа $P_{ftm3}(t)$ и схемы FCTLUT, парирующей три отказа $P_{ftm4}(t)$ при $n = 4$ изображены на рис. 8.



а) б) в)

Рисунок 9 – Расчетверение канальное: а) $n = 10$, $m = 1$; б) $n = 100$, $m = 1$; в) $n = 100$, $m = 10$

Сравнение расчетверения канального $P_4(t)$ с нерезервированной структурой и троированием $P_3(t)$; $P_{33}(t)$ представлено на рис. 9.

Заключение

С целью проектирования радиационно-стойкой цифровой аппаратуры наиболее эффективно расчетверение на транзисторном уровне. Оно позволяет получить более высокую вероятность безотказной работы, чем троирование, причём на всём временном диапазоне. В ряде случаев избыточность расчетверения меньше троирования, если учитывать мажоритарные элементы. Для парирования любого одного отказа в каждой транзисторной структуре необходима четырёхкратная избыточность. Для парирования любых двух отказов в каждой транзисторной структуре необходима девятикратная избыточность, позволяющая достичь более существенной вероятности безотказной работы расчетверённой схемы, но и её превосходит на всём временном интервале расшестнадцатерённая схема, парирующий отказы любых трёх транзисторов в каждой транзисторной структуре, для реализации которой требуется шестнадцатикратная избыточность. С целью парирования отказов блока питания возможно использовать его дублирование в расчетверённой схеме, например, так, как предложено в [10].

Библиографический список

1. ГОСТ 27.002–2015. Надежность в технике Основные понятия. Термины и определения [Текст]. – Введ. 2017–03–01. – М.: Старнартинформ, 2016. – 23 с.

2. Shankarnarayanan Ramaswamy, Leonard Rockett, Dinu Patel and others. A Radiation Hardened Reconfigurable FPGA [Электронный ресурс]. – URL: https://pdfs.semanticscholar.org/57f8/ff540360eadceafc062797b7a01065f6f9cc.pdf (дата обращения 30.03.2018).

3. Борисов Ю.И. О выборе архитектуры отказоустойчивых вычислительных комплексов для космических аппаратов [Текст] / Ю.И. Борисов // Надежность. – 2004. – № 2(21). – С.46-51.

4. Шебе Х. Предельная надёжность структурного резервирования [Текст] / Х. Шебе, И.Б. Шубинский // Надежность. – 2016. – № 1(56). – С.3-8.

5. Carl Carmichael. Triple Module Redundancy Design Techniques for Virtex FPGAs [Электронный ресурс]. – URL: https://www.xilinx.com/support/documentation/application_notes/xapp197.pdf (дата обращения 30.03.2018)

6. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза [Текст]: методы синтеза / И.Б. Шубинский. – М: Журнал «Надежность», 2016. – 544 с.: ил., табл.; 23 см.; ISBN 978-5-7572-0399-7 : 500 экз.

7. Васильев Н.П. Аналитическая оценка вероятности успешной адаптации к отказам модульных вычислительных систем с многоуровневой активной защитой [Текст] / Н.П. Васильев, И.Б. Шубинский // Известия высших учебных заведений. Приборостроение. – 1994. – Т. 37. – № 3-4. – С. 47.

8. Тарасов А.А. Минимизация времени функциональной реконфигурации распределенной отказоустойчивой системы [Текст] / А.А. Тарасов // Надежность. – 2010. – № 2(37). – С.24-29.

9. Тюрин С.Ф. Скользящее резервирование толерантных элементов [Текст] / С.Ф. Тюрин // Надежность. – 2017. – Т. 17. – № 1(60). – С.17-21.

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

11. Carver A. Mead. Introduction to VLSI Systems / Carver A. Mead, Lynn Conway [Электронный ресурс]. – URL: https://www.researchgate.net/publication/234388249_Introduction_to_VLSI_systems (дата обращения 30.03.2018).

Сведения об авторе

Сергей Ф. Тюрин – доктор технических наук, профессор, профессор кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (www.pstu.ru),

профессор кафедры Математического обеспечения вычислительных систем ПГНИУ (www.psu.ru), Пермь, Россия, e-mail: tyurinsergfeo@yandex.ru

Поступила 25.04.2018