УДК 681.3

**С.Ф. Тюрин, О.А. Громов, А.В. Сулейманов**

Пермский национальный исследовательский
политехнический университет

**А.В. Греков**

Пермский военный институт внутренних войск МВД РФ

# АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ ПАССИВНОЙ ОТКАЗОУСТОЙЧИВОСТИ ЦИФРОВЫХ УСТРОЙСТВ И СИСТЕМ

*Производится анализ методов обеспечения пассивной отказоустойчивости. Приведен расчет вероятностей безотказной работы для различных методов и показаны графики изменения вероятности безотказной работы. Также дан расчет функции затрат на построение системы с внесенной избыточностью.*

Под безотказностью (Reliability, failure-free operation) как одним из свойств надёжности понимается свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки [1].

При этом событие, заключающееся в нарушении работоспособного состояния объекта, называют отказом (Failure), а самоустраняющийся отказ или однократный отказ, устраняемый незначительным вмешательством оператора, – сбоем (Interruption) [1].

Системы, обладающие свойством функционировать в условиях отказов (сбоев), называют отказоустойчивыми (сбоеустойчивыми). Создание надёжных, отказоустойчивых систем является одной из ключевых задач науки и технологии. Для этого применяют резервирование (Redundancy) – способ обеспечения надежности объекта за счет использования дополнительных средств и (или) возможностей, избыточных по отношению к минимально необходимым для выполнения требуемых функции [2–3], то есть резервирование – это

введение разного рода избыточности – структурной, временной, информационной, алгоритмической, функциональной и пр.

Отказоустойчивые цифровые приборы и вычислительные комплексы впервые были разработаны для военной аппаратуры [4]. Различают пассивную и активную отказоустойчивость [4–6]. При пассивной отказоустойчивости отказы и сбои маскируются системой, которая продолжает функционирование и при возникновении определённого количества отказов. Это требует значительной избыточности – мажоритирования 2 из 3 (парируется 1 отказ – в одном из 3 каналов, то есть отказ 1 канала), 3 из 5 (парируется отказ 2 каналов), 4 из 7 (парируется отказ 3 каналов) и т.д. Пассивная отказоустойчивость применяется там, где недопустимы даже кратковременные перерывы в работе системы.

Активная отказоустойчивость требует времени на обнаружение, локализацию отказов и так называемую реконфигурацию системы, зато выигрышна с точки зрения избыточности. Проанализируем методы обеспечения пассивной отказоустойчивости цифровых устройств и систем.

**Мажоритирование 2 из 3.** В этом случае используется более чем трёхкратная избыточность – 3 канала одного цифрового устройства (рис. 1).

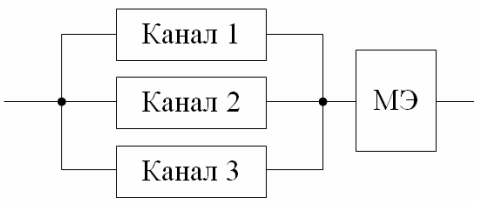



Рис. 1. Мажоритирование

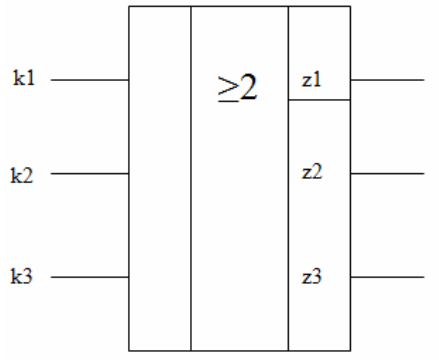



Рис. 2. Мажоритарный элемент с формированием номера ошибки

Мажоритарный элемент с формированием номера отказавшего канала представлен на рис. 2 (интегральные микросхемы, например, 561 ЛП3, 561 ЛП13) и описывается таблицей истинности (табл. 1).

Таблица 1

Таблица истинности мажоритарного элемента
с формированием номера отказавшего канала

| k3 | k2 | k1 | ВС | z1 | z2 | z3 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 2 | 0 | 1 | 0 |
| 0 | 1 | 1 | 3 | 1 | 1 | 1 |
| 1 | 0 | 0 | 4 | 0 | 1 | 1 |
| 1 | 0 | 1 | 5 | 1 | 1 | 0 |
| 1 | 1 | 0 | 6 | 1 | 0 | 1 |
| 1 | 1 | 1 | 7 | 1 | 0 | 0 |

Кроме того, необходимы три источника питания. Без учёта вероятности безотказной работы мажоритарного элемента получаем вероятность безотказной работы мажоритарной системы (м.с) с выбором 2 из 3:

$$P_{\text{м.с}} = p^3 + 3p^2(1-p) = 1-(1-p)^3 - 3p(1-p)^2 = 3p^2 - 2p^3. \qquad (1)$$

Таким образом,

$$P_{\text{м.с}}^{2\ \text{из}\ 3}(t) = 3P^2 - 2P^3. \qquad (2)$$

Например,

$$P = 0{,}9 / P_{\text{м.с}}^{2\ \text{из}\ 3}(t) = 3(0{,}9)^2 - 2(0{,}9)^3 = 0{,}972. \qquad (3)$$

Для экспоненциальной модели отказов:

$$P_{\text{м.с}} = [3e^{-2\lambda t} - 2e^{-3\lambda t}] \qquad (4)$$

где $\lambda$ – интенсивность отказов одного канала.

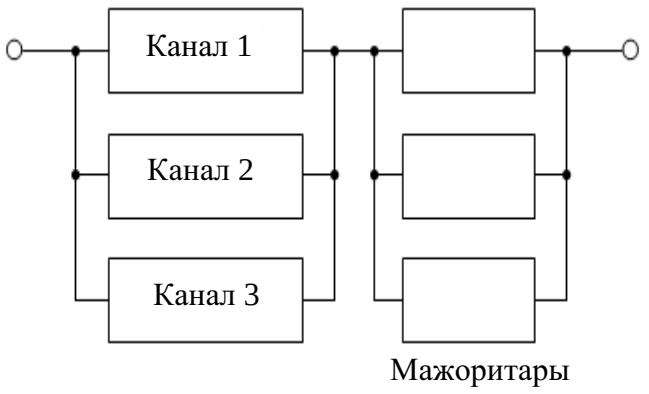



Рис. 3. Мажоритирование мажоритарных элементов

С учётом отказов мажоритарного элемента:

$$P_{\text{м.с}} = [3e^{-2\lambda t} - 2e^{-3\lambda t}]e^{-\lambda_{\text{м.э}} t}, \quad (5)$$

где $\lambda_{\text{м.э}}$ – интенсивность отказов мажоритарного элемента, $t$ – время работы.

Как правило, мажоритарных элементов для отказоустойчивости – тоже три, и каждый выдаёт сигналы в следующий участок схемы (рис. 3).

Тогда получаем

$$P_{\text{м.с}} = [3e^{-2\lambda t} - 2e^{-3\lambda t}][3e^{-2\lambda_{\text{м.э}} t} - 2e^{-3\lambda_{\text{м.э}} t}]. \quad (6)$$

**Мажоритирование 3 из 5.** Известны примеры мажоритирования 3 из 5:

$$P_{\text{м.с}}^{3\text{ из }5}(t) = P^5 + 5P^4(1-P) + 10P^3(1-P)^2. \quad (7)$$

Например,

$$P = 0{,}9 / P_{\text{м.с}}^{3\text{ из }5}(t) = (0{,}9)^5 + 5(0{,}9)^4(0{,}1) + 10(0{,}9)^3(0{,}1)^2 = 0{,}99144. \quad (8)$$

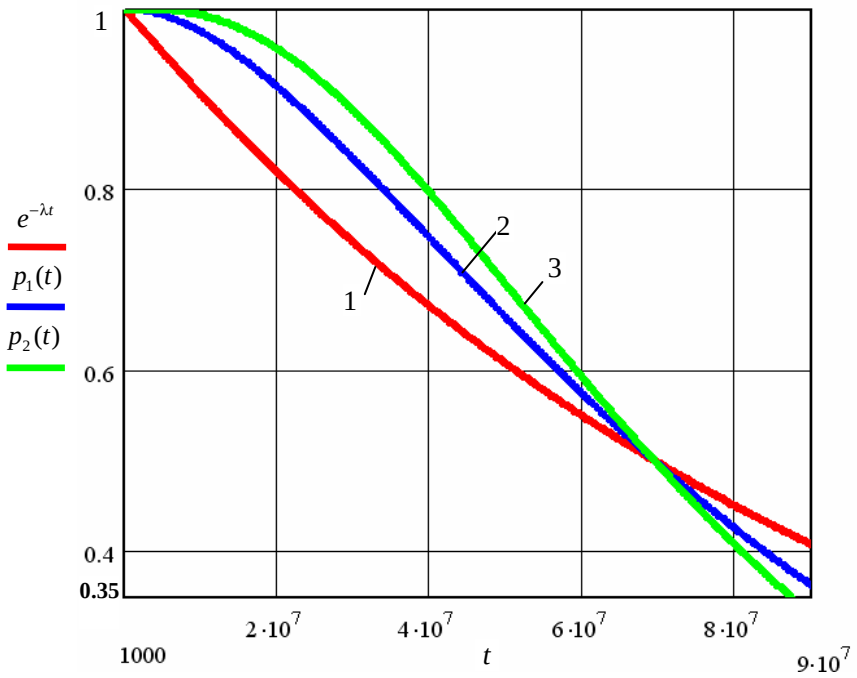



Рис. 4. Сравнение одноканальной цифровой системы с мажоритированием: *1* – $e^{-\lambda t}$ – без резервирования; *2* – $p_1(t)$ – 2 из 3; *3* – $p_2(t)$ – 3 из 5

Для экспоненциальной модели отказов без учёта мажоритарных элементов для схемы 3 из 5:

$$P_{\text{м.с}}^{3\text{из}5}(t) = e^{-5\lambda t} + 5e^{-4\lambda t}(1-e^{-\lambda t}) + 10e^{-3\lambda t}(1-e^{-\lambda t})^2. \quad (9)$$

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

$$P_{\text{м.с}}^{3\text{ из }5}(t) = [e^{-5\lambda t} + 5e^{-4\lambda t}(1-e^{-\lambda t}) + 10e^{-3\lambda t}(1-e^{-\lambda t})^2] \times$$
$$\times [e^{-5\lambda_{\text{м.э}} t} + 5e^{-4\lambda_{\text{м.э}} t}(1-e^{-\lambda_{\text{м.э}} t}) + 10^{-3\lambda_{\text{м.э}} t}(1-e^{-\lambda_{\text{м.э}} t})^2]. \quad (10)$$

На рис. 4 представлены графики изменения вероятности безотказной работы ПЛИС без мажоритирования и с мажоритированием.

**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. Без учёта этой дополнительной аппаратуры и мажоритарных элементов, которые также троируются, получим:

$$P_{\text{м.с1}} = P^3 + 3P^2(1-P) + 3P(1-P)^2 = 1-(1-P)^3. \quad (11)$$

Например,

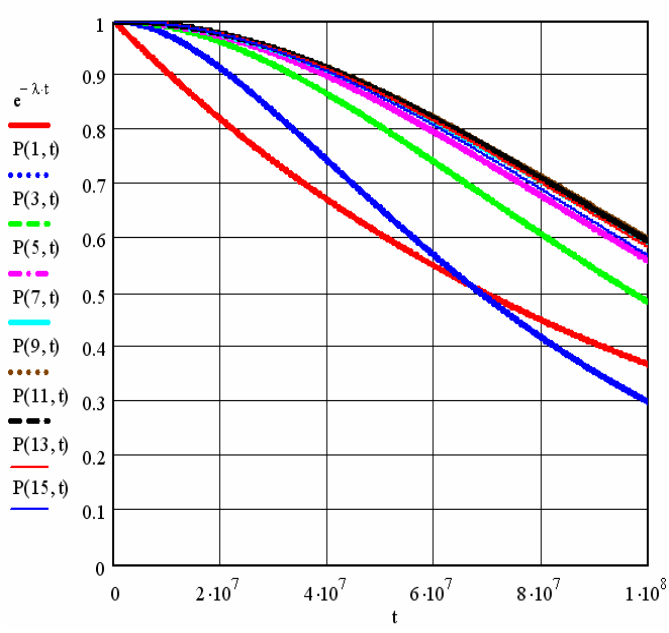
$$p = 0{,}9 / P_{\text{м.с1}} = 1-(0{,}1)^3 = 0{,}999. \quad (12)$$

Как выбрать канал из двух оставшихся, если они начнут выдавать разные результаты?! При отказе одного канала – он блокируется, сравниваются результаты двух оставшихся. В случае несравнения производится оперативное тестирование, канал с ошибкой отключают. Если оперативное тестирование не приводит к обнаружению отказавшего канала, делать нечего, выбирают один из двух случайным образом.

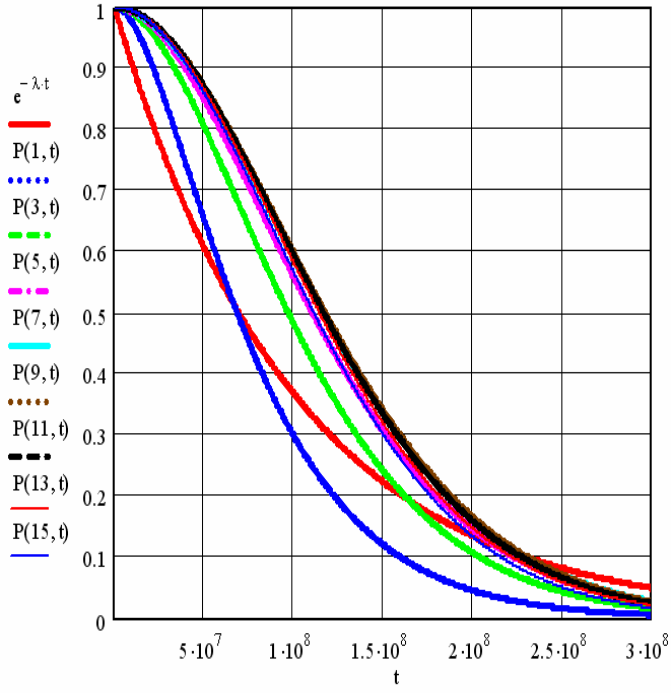
Для экспоненциальной модели отказов с учётом мажоритарных элементов и дополнительной аппаратуры реконфигурации (интенсивность отказов $\lambda_{\text{д}}$)

$$P_{\text{м.с}} = [1-(1-e^{-\lambda t})^3][3e^{-2(\lambda_{\text{м.э}}+\lambda_{\text{д}})t} - 2e^{-3(\lambda_{\text{м.э}}+\lambda_{\text{д}})t}]. \quad (13)$$

Выражение (13) не учитывает вероятности «промаха» в случае, если оперативное тестирование не приводит к обнаружению отказавшего канала.




*а*




*б*

Рис. 5. Графики изменения вероятности безотказной работы системы без мажоритирования, с мажоритированием и с глубоким мажоритированием *к* слоёв $\lambda = 10^{-8}$

**Глубокое мажоритирование.** Мажоритируются отдельные подблоки блоков ПЛИС, например, АЛУ процессора, устройство управления и т.д. Иногда бывает так: ни один канал в «разваленном» состоянии не работает, а в мажоритарном – работа идёт!

Для экспоненциальной модели отказов и троированных мажоритаров

$$P_{\text{г.м}} = \prod_{j=1}^{k}[3e^{-2\lambda_k t} - 2e^{-3\lambda_k t}][3e^{-2\lambda_{\text{м.э}} t} - 2e^{-3\lambda_{\text{м.э}} t}]^k, \qquad (14)$$

где $P_{\text{г.м}}$ – вероятность безотказной работы глубоко мажоритированной структуры из $k$ троированных слоёв, $\lambda_k$ – интенсивность отказов $k$-го троированного слоя, $\lambda_{\text{м.э}}$ – интенсивность отказов мажоритарного элемента, $t$ – время работы.

Необходимо сравнить троирование всей структуры без разбивки на слои с одним троированным мажоритаром:

$$P_{\text{м.с}} = [3e^{-2\lambda t} - 2e^{-3\lambda t}][3e^{-2\lambda_{\text{м.э}} t} - 2e^{-3\lambda_{\text{м.э}} t}], \qquad (15)$$

где $\lambda$ – интенсивность отказов всей структуры, $\lambda_{\text{м.э}}$ – интенсивность отказов мажоритарного элемента, $t$ – время работы.

На рис. 5 представлены графики изменения вероятности безотказной работы ПЛИС без мажоритирования, с мажоритированием и с глубоким мажоритированием.

Примем допущение, что $\lambda$ – интенсивность отказов всей структуры разбивается на $k$ одинаковых частей, тогда

$$P_{\text{г.м}} = [3e^{-2\frac{\lambda}{k}t} - 2e^{-3\frac{\lambda}{k}t}]^k [3e^{-2\lambda_{\text{м.э}} t} - 2e^{-3\lambda_{\text{м.э}} t}]^k. \qquad (16)$$

Так, для $\lambda = 10^{-5}$, $\lambda_{\text{м.э}} = \frac{\lambda}{\alpha_1}, \alpha_1 = 10, t = 10^2, 10^3, 10^4, 10^5, 10^6, 10^7$ получим оптимум для $k = 12$, $t = 10^4$ (рис. 6).

При $\lambda = 10^{-5}$, $\lambda_{\text{м.э}} = \frac{\lambda}{\alpha_1}, \alpha_1 = 100, t = 10^2, 10^3, 10^4, 10^5, 10^6, 10^7$ получим оптимум для $k = 115$, $t = 10^5$ (рис. 7).

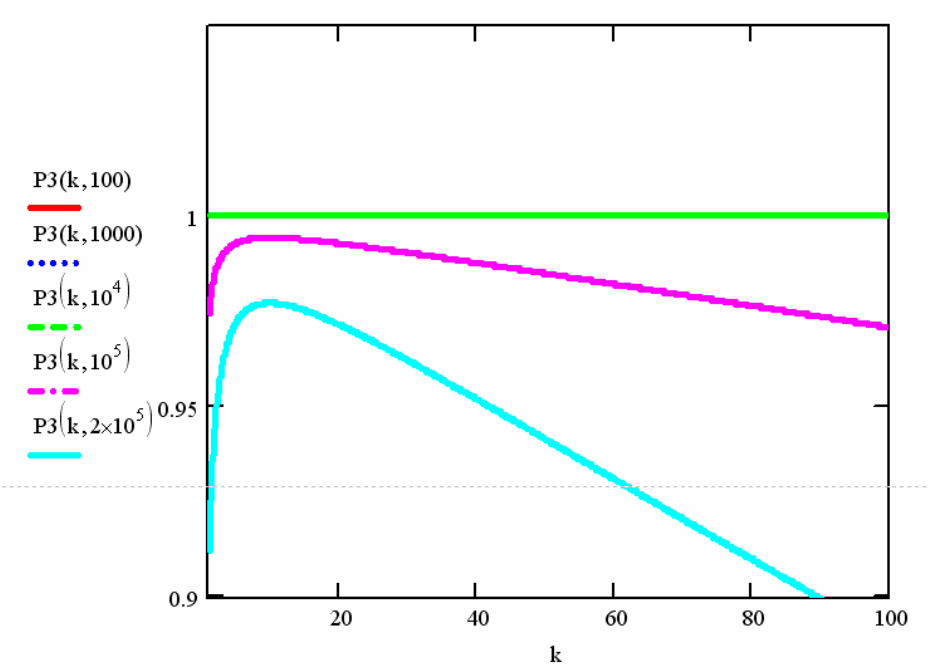



Рис. 6. Оптимум глубокого мажоритирования для $k$ =12, $t = 10^4$

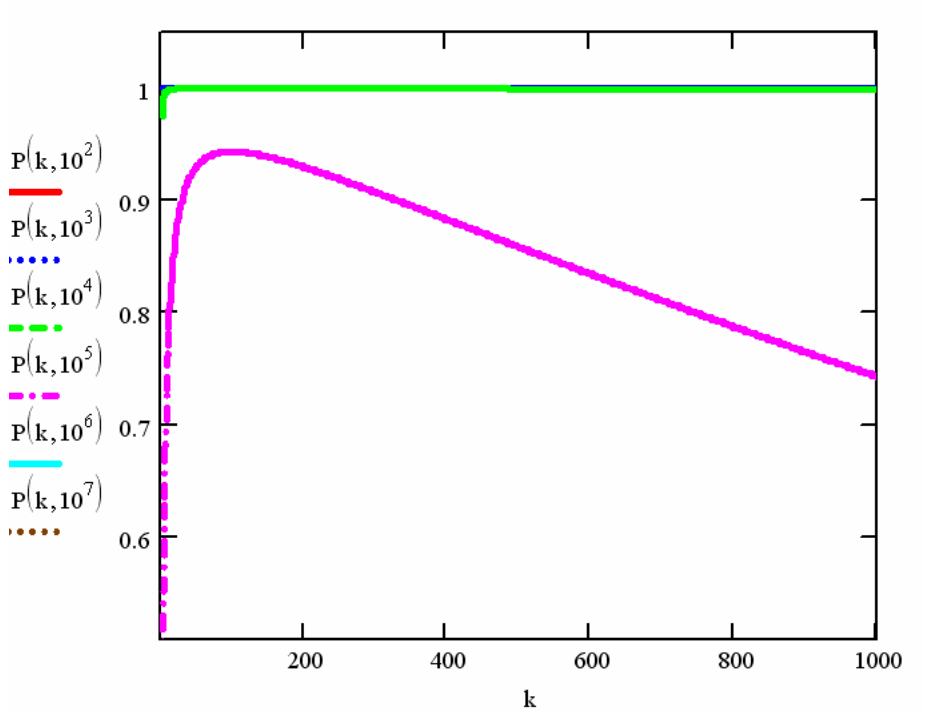



Рис. 7. Оптимум глубокого мажоритирования для $k$ =115, $t = 10^5$

При $\lambda = 10^{-5}$, $\lambda_{\text{м.э}} = \dfrac{\lambda}{\alpha_1}, \alpha_1 = 1000, t = 10^2, 10^3, 10^4, 10^5, 10^6, 10^7$ получим оптимум для $k = 999$, $t = 10^6$ (рис. 8).

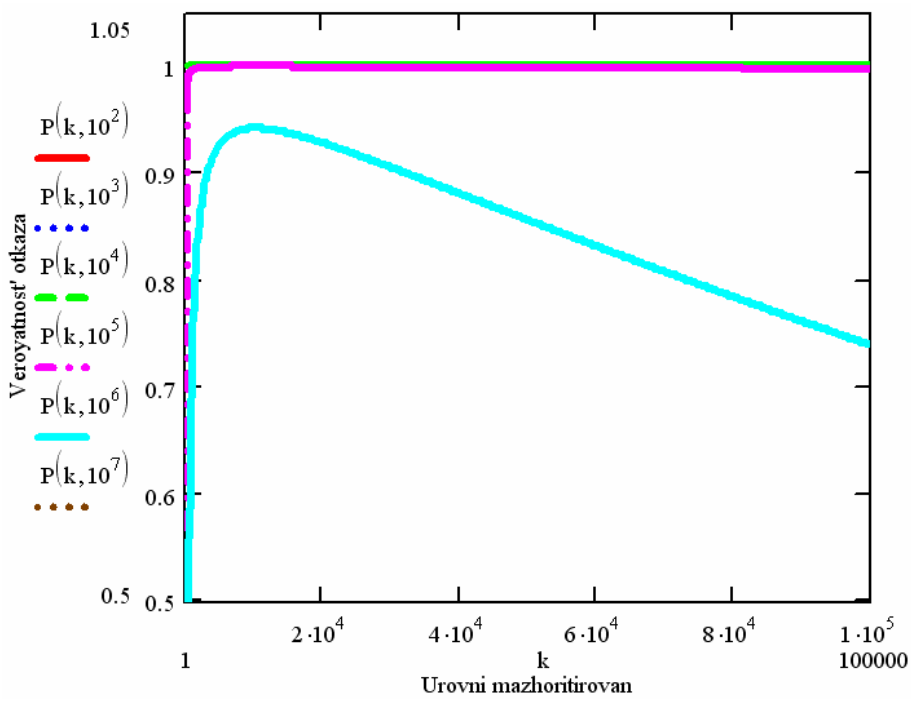



Рис. 8. Оптимум глубокого мажоритирования для $k = 999$, $t = 10^6$

При этом стоимость системы увеличивается по сравнению с обычным мажоритированием:

$$C_{\text{м}} = 3C_{\lambda} + 3C_{\text{м.э}} + 3C_{\text{и.п}}, \qquad (17)$$

где $C_{\lambda}$ – стоимость одного канала, $C_{\text{м.э}}$ – стоимость мажоритара, $C_{\text{и.п}}$ – стоимость источника питания. Задержка прохождения сигнала увеличивается всего на величину задержки одного мажоритара $\tau_{\text{м.э}}$.

В случае глубокого мажоритирования

$$C_{\text{г.м}} = 3C_{\lambda} + 3kC_{\text{м.э}} + 3C_{\text{и.п}}, \qquad (18)$$

а задержка прохождения сигнала увеличивается на величину задержки $k$ мажоритаров $k \cdot \tau_{\text{м.э}}$. Используются три мажоритарных мультиплексора (рис. 9).

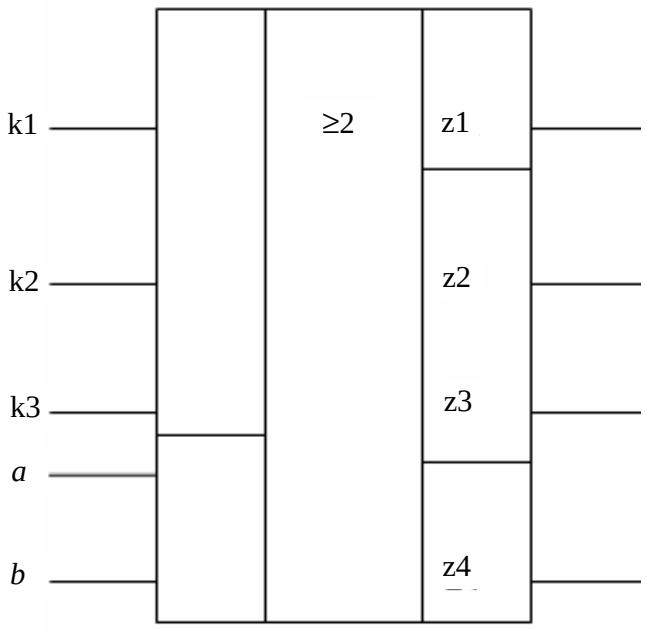



Рис. 9. Мажоритарный мультиплексор
с возможностью «развала» на отдельные каналы

Работа мажоритарного мультиплексора представлена в табл. 2:

Таблица 2

Подключение входов
мажоритарного мультиплексора

| *a* | *b* | z1 |
|---|---|---|
| 0 | 0 | k1 |
| 0 | 1 | k2 |
| 1 | 0 | k3 |
| 1 | 1 | мажоритирование |

Подобные структуры обладают недостатком снижения производительности на 10–15 % за счет введения большого количества мажоритарных схем, однако конструкторы идут на это, компенсируя временные затраты другими методами [4].

Таким образом, наиболее эффективно «глубокое» мажоритирование, но оно является и самым дорогим методом, кроме того, необходимо оценивать допустимое снижение быстродействия.

**Библиографический список**

1. ГОСТ 27.002-89. Надежность в технике Основные понятия. Термины и определения. – М.: Изд-во стандартов, 1990. – 42 с.

2. Надежность и эффективность в технике: справочник: в 10 т. / ред. совет во главе с В.С. Авдуевским (предс.) [и др.] Т.1: Методология. Организация. Терминология / под ред. А.И. Рембезы. – М.: Машиностроение, 1989. – 224 с.

3. Надежность и эффективность в технике: справочник: в 10 т. / ред. совет во главе с В.С. Авдуевским (предс.) [и др.]. Т.2: Математические методы в теории надежности и эффективности / под ред. Б.В. Гнеденко. – М.: Машиностроение, 1987. – 280 с.

4. Отказоустойчивые вычислительные системы / В.А. Бородин [и др.]. – М., 1990. – С. 55.

5. Айзенберг Я.Е., Ястребенецкий М.А. Сопоставление принципов обеспечения безопасности систем управления ракетоносителями и атомными электростанциями // Космічна наука та технологія. – 2002. – № 1. – С. 55–60.

6. Основи надійності цифрових систем: підручник / за ред. В.С. Харченка, В.Я. Жихарева. – Харків, 2004. – 572 с.

Получено 05.09.2011