Научная статья

DOI: 10.15593/2224-9397/2022.1.03
УДК 681.32

И.В. Бурдышев, С.Ф. Тюрин

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ НАДЕЖНОСТИ ЦИФРОВЫХ УСТРОЙСТВ

В настоящее время цифровые устройства интенсивно развиваются и применяются в различных сферах науки и техники. В частности, они используются в тех областях, где аппаратура подвергается негативным факторам воздействия и где существуют высокие требования по надежности. К негативным факторам можно отнести радиацию, перепады температур, электромагнитные воздействия, скачки напряжения и др. Нарушение функционирования таких систем может повлечь за собой значительные издержки. В статье приводится небольшой исторический обзор основных этапов становления надежности как науки и выделяются ее направления. В начале статьи рассматриваются основные факторы, негативно влияющие на надежность аппаратуры. Далее материал посвящен методам и подходам обеспечения надежности, посредством резервирования, средств контроля, методам защиты от негативного излучения. Также нами предлагается задача оптимального перераспределения интенсивности отказов между подсистемами, которое способствует оптимальному выигрышу в надежности. Решается данная задача с помощью методов оптимизации. Таким образом, **цель исследования** состоит в формулировании принципов решения данной задачи и нахождения оптимального алгоритма ее решения. **Методы решения:** детерминированный алгоритм обобщенного приведенного градиента и эволюционный алгоритм, реализованные с помощью пакета Microsoft Excel. **Результатом** является нахождение набора оптимального перераспределения функций между подсистемами, а также выделение основных достоинств и недостатков применения детерминированных и стохастических алгоритмов в задачах подобного рода. **Практическая значимость** заключается возможности применения принципов данной задачи к задачам увеличения надежности с помощью оптимального распределения объектов.

Ключевые слова: надежность, отказоустойчивость, перераспределение интенсивностей отказов.

I.V. Burdyshev, S.F. Tyurin

Perm National Research Polytechnic University, Perm, Russian Federation

ANALYSIS OF METHODS FOR INCREASING THE RELIABILITY OF DIGITAL DEVICES

Currently, digital devices are being intensively developed and used in various fields of science and technology. In particular, they are used in areas where the equipment is exposed to negative factors of influence and where there are high requirements for reliability. Negative factors include radiation, temperature extremes, electromagnetic effects, voltage surges, etc. Disruption of the functioning of such systems can entail significant costs. The article provides a small historical overview of the main stages of the formation of reliability as a science and highlights its directions. The first chapter of the article discusses the main factors that negatively affect the reliability of the equipment. The second chapter is devoted to methods and approaches to ensure reliability through redundancy, means of control, methods of protection against negative radiation. Also, we propose the problem of optimal redistribution of the failure rate between subsystems, which contributes to the optimal gain in reliability. This problem is solved using optimization methods. Thus, the **purpose** of the study is to formulate the principles for solving this problem and finding the optimal algorithm for its solution. **Solution methods:** deterministic generalized reduced gradient algorithm and evolutionary algorithm by means, implemented using Microsoft Excel. The **result** is finding a set of optimal redistribution of functions between subsystems, as well as highlighting the main advantages and disadvantages of using deterministic and stochastic algorithms in problems of this kind. The **practical significance** lies in the possibility of applying the principles of this problem to the problems of increasing reliability with the help of the optimal distribution of objects.

Keywords: reliability, fault tolerance, reallocating of the failure rates.

Введение

В век информационных технологий цифровые устройства применяются повсеместно. Основу цифровых устройств составляют интегральные схемы (ИС). К наиболее сложным по степени интеграции, т.е. по уровню сложности и числу элементов, относят сверхбольшие интегральные схемы (СБИС). К ним относят микропроцессоры, микроконтроллеры, программируемые логические схемы (ПЛИС) и другие. Также помимо ИС цифровые устройства состоят из диодов, транзисторов, электромагнитных реле, соединительных шин и других составляющих. Данные устройства применяются в атомной, военной, аэрокосмической и других сферах, где они могут подвергаться негативным факторам воздействия и существуют высокие требования по надежности.

Надежность технических средств может пониматься как свойство объекта сохранять работоспособность и выполнять необходимые функции в пределах определенного времени [1]. Надежность является

свойством технических устройств и конструкций. Надежностью как наукой ученые занимались давно. Так еще в XVII веке Галилео Галилей в одной из своих работ дал анализ прочности каната с позиции резервирования нитей [2]. Однако основополагающие принципы и становление теории надежности произошли в XX веке. В послевоенные годы появился ряд работ, в частности, работы Дж. фон Неймана, где он указывает способ повышения надежности путем резервирования элементов системы и формулирует принцип «надежных организмов из ненадежных компонентов» [3, 4]. Данный метод основан на понятии избыточности, которая бывает структурной, функциональной, информационной, временной. Хэмминг в своих работах описал помехоустойчивое кодирование, что послужило толчком к развитию отказоустойчивости в цифровой схемотехнике [5]. Появляются работы Э. Мура по построению надежных устройств, К. Шеннона по кодированию информации, где были рассмотрены вопросы надежности в секретных системах связи. В США в 1954 г. проходит национальный симпозиум по вопросам надежности. В СССР в 60-е гг. прошлого века проводится работа в области теории надежности, которую возглавляет Б.В. Гнеденко [2]. В области надежности первые работы, включающие математические вопросы и прикладные задачи, были осуществлены такими учеными, как Ю.К. Беляев, А.И. Берг, Н.Г. Бруевич, А. Пирс и другими.

Методологию гарантоспособных вычислений предложил в своих работах Алгирдас Авиженис, обладатель премии Эккера – Мокли «за фундаментальный вклад в отказоустойчивую компьютерную архитектуру и компьютерную арифметику» [6]. Выделяют два метода обеспечения надежности. Первый заключается в создании высоконадежных компонентов системы. Данный метод часто экономически не выгоден и не приносит должного результата. Второй способ базируется на понятии отказоустойчивости, т.е. способности объекта сохранять работоспособность при наличии ошибок, отказов, без потери функциональных свойств либо с частичной потерей. Отказоустойчивость обеспечивается введением избыточности в систему [7].

Часто методы повышения надежности (отказоустойчивости) условно делят на два класса – активные и пассивные методы. Пассивные методы характеризуются постоянством структурной, функциональной организации. Вся система или отдельные ее части резервируются. При

этом не требуется время на устранение отказа. Активная отказоустойчивость характеризуется способностью к изменению конфигурации системы. Она требует меньшей избыточности, но при этом требуются средства контроля, время для обнаружения и устранения отказа [8].

1. Анализ неисправностей цифровых устройств

На этапе проектирования цифрового устройства может быть не учтено влияние различных параметров на работу всей схемы. Так, например, к наиболее важным параметрам при проектировании интегральных схем относят пороговое напряжение U0 и длину канала *L* МОП-транзистора. На эти параметры влияют уровень легирования подложки, доза ионной имплантации, толщина оксида под затвором, длина затвора – их отклонения приводят к изменению данных параметров. На этапе производства могут быть выбраны некачественные детали, происходит попадание пыли на кристалл из-за дефектов упаковки. Качественное производство невозможно без контроля дефектов. Поэтому этап проектирования производства имеет значительное влияние на надежность устройств. Все это субъективные факторы, влияющие на надежность, т.е. обусловлены человеческим фактором [2].

Помимо них выделяют и объективные факторы – воздействия окружающей среды [9]. Это может быть радиация, т.е. ионизация, обусловленная α- и γ-излучением или тяжелыми заряженными частицами, что может приводить к одиночным сбоям SEU (Single-Event-Upsets), отказам SEE (Single Event Effect). Может произойти защелкивание транзисторов в пропускающем состоянии SEL (Single Effect Latchup), могут происходить скачки напряжения питания, что приводит к сбоям переключений транзисторов – SET (Single Event Transient) [10, 11]. Например, может происходить сбой в конфигурационной памяти SRAM, что является довольно частым явлением [12]. Также на надежность аппаратуры могут воздействовать перепады температуры, электромагнитные воздействия, перепады напряжения, деградация элементов (например, электромиграция) [13]. Кроме этого частой причиной отказов радиоэлектронной аппаратуры являются электрические перегрузки, воздействие статического электричества. На рис. 2, 3 продемонстрированы последствия воздействия негативных факторов [9].

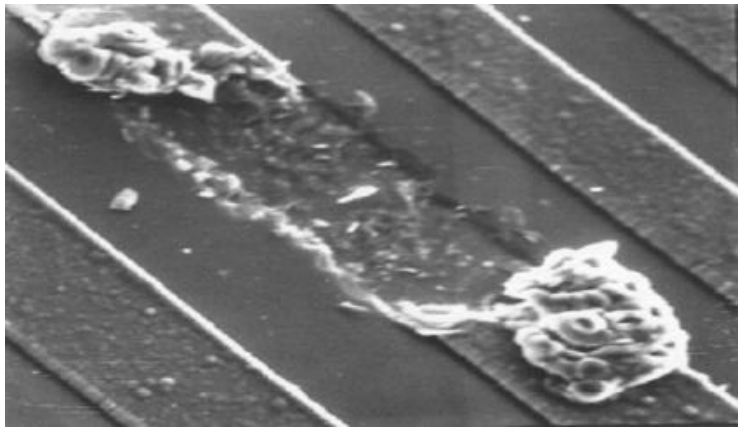

Рис. 1. Следы коррозионного разрушения шины металлизации

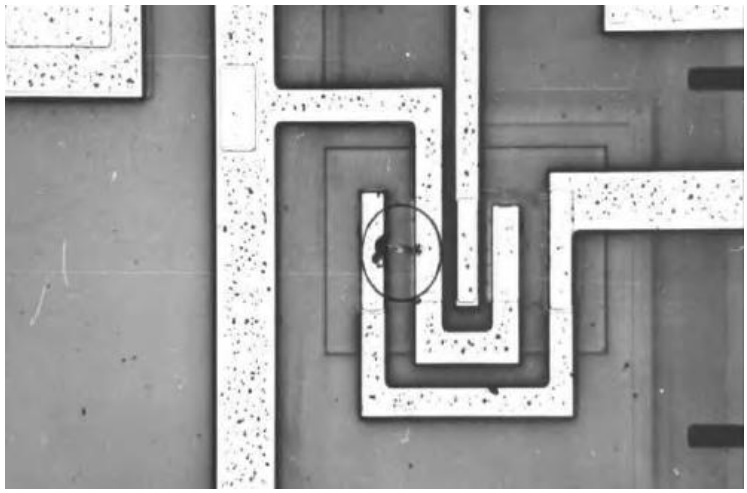

Рис. 2. Пробой *p-n* перехода в интегральной схеме

Для представления поведения устройств при физических дефектах используют упрощения – модели неисправностей. Модели неисправности являются ключевым фактором в тестирования и диагностике неисправностей ИС. Существуют различные модели неисправностей. В модели константных неисправностей считается, что неисправная часть схемы принимает значение логического нуля либо логической единицы. Бывают кратные константные неисправности, при которых несколько узлов микросхемы принимают постоянные значения сигналов. Также бывают и другие модели неисправностей, описывающих разрыв в цепи, задержку прохождения сигнала и др. [2].

2. Методы и подходы обеспечения надежности

На этапе проектирования закладывается фундамент отказоустойчивой системы. То, насколько грамотно это произведено, будет во многом обусловливать ее надежность. Зачастую надежные решения – это старые, проверенные временем устройства. В пример можно привести марсоход Perseverance, который был запущен на планету в 2020 г. В нем установлен процессор PowerPC 750. Это процессор, который был разработан в конце прошлого столетия и устанавливался в компьютеры iMac того времени. Конечно, процессор марсохода отличается особым исполнением RAD750. Также данный процессор работает на марсоходе Curiosity. Такой выбор объясняется тем, что сложные, современные и с огромным количеством элементов микрочипы чувствительны к вредоносным излучениям, которые в Космосе и на Марсе гораздо выше, чем здесь, а также тем, что длительность автономной работы важнее производительности для таких машин [14]. Надежность не означает техническое совершенство системы. Иногда лучше использовать проверенные временем микросхемы.

В зависимости от области применения устройств методы обеспечения надежности для них будут разными. Это связано с требованиями по надежности, с характером вредоносных воздействий, с областью применения аппаратуры и с другими факторами. Например, ремонт космических аппаратов, как правило, невозможен, и требования по надежности, соответственно, будут другие. Хотя есть и редкие исключения, как с телескопом «Хаббл», который неоднократно ремонтировали на орбите экипажи «Спейс Шаттл» [15].

Существует большое количество различных методов борьбы со сбоями. К ним относятся методы кратного резервирования, при котором основная схема копируется некоторое количество раз – это структурное резервирование. Резерв может выполнять те же функции, что и основной элемент, а схема голосования (мажоритирования) определяет истинный результат, т.е. выполняется мажоритирование. Также резервные элементы могут быть не задействованы в работе и заменять основной в случае его отказа. Это может быть скользящее резервирование, при котором помимо основных рабочих элементов есть некоторое число запасных, которые могут заменить любой отказавший элемент системы [16].

Классическим методом мажоритирования является тройное модульное резервирование – TMR (Triple Modular Redundancy), допускающее наличие ошибки в одном из трех элементов (рис. 3) [17, 18]. Система имеет трехкратную избыточность, не считая мажоритарный элемент. Также возможно резервирование с большей кратностью – пять, семь и т. д.

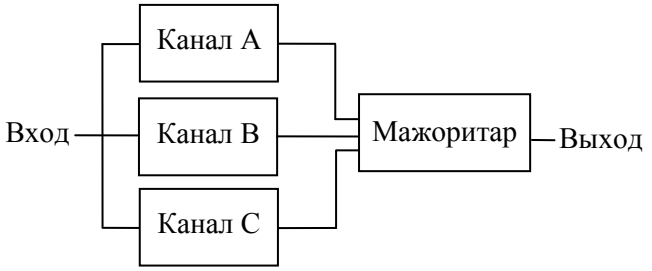

Рис. 3. Метод мажоритарного резервирования TMR

Резервирование увеличивает надежность, показателем которой является вероятность безотказной работы ВБР. Для резервирования TMR она определяется так:

$$P_{TMR} = 3P^2 - 2P^3 = 3e^{-2\lambda t} - 2e^{-3\lambda t}, \quad (1)$$

где λ – интенсивность отказов одного из каналов (или системы), 1/ч. Интенсивность отказов нерезервированной системы равна сумме интенсивностей отказов ее элементов:

$$\lambda_c = \sum_{i=1}^{n} \lambda_i . \quad (2)$$

Методы мажоритирования применяются в программируемых логических интегральных схемах, где могут троироваться триггеры. Несмотря на то, что данный метод обеспечивает надежность, его недостатком является большая избыточность – более чем в три раза. Зачастую применяется резервирование на уровне системы в целом. Например, может применяться дублирование. Может применятся резервирование на уровне крупных элементов системы, например резервирование процессоров [19].

Развивается такое направление в области надежности, как резервирование на транзисторном уровне. Так, в работе [20] представлена разработка библиотеки высоконадежных логических элементов,

имеющих такое резервирование. Данная технология строится на основе функционально-полных толерантных (ФПТ) булевых функций [21]. Метод предполагает резервирование транзисторных цепочек с четырехкратным увеличением транзисторов (рис. 4). Данный метод увеличивает параметры надежности на значительном временном интервале, незначительно увеличивается энергопотребление, но ухудшается быстродействие. В работе [20] логические элементы, разработанные по данной технологии, имеют проблемы с падением напряжения и снижением помехоустойчивости.

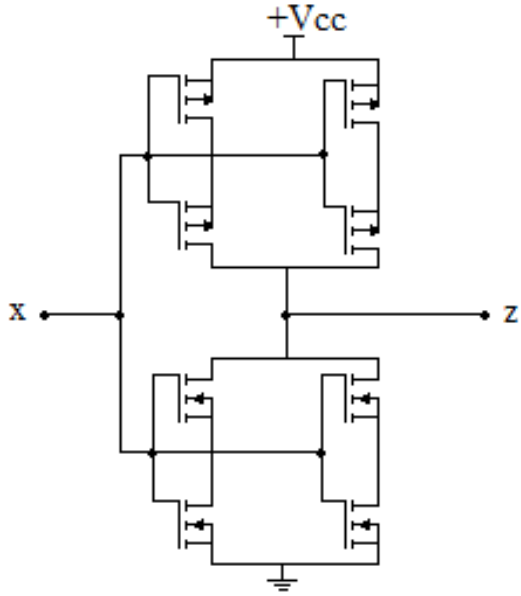

Рис. 4. Схема ФПТ-элемента на основе КМОП-транзисторов

Одним из главных методов обеспечения надежности является подход с применением встроенных средств контроля [22]. Контроль, или диагностирование, может осуществляться в специально отведенное время, вне работы устройства – это тестовый контроль. Либо диагностирование может осуществляться во время работы устройства и называется функциональным контролем. Функциональный контроль (рис. 5) требует дополнительной схемы, которая будет способна обнаружить неисправность. Также бывают схемы, способные исправлять обнаруженную ошибку, но они менее распространены из-за большой структурной избыточности [23].

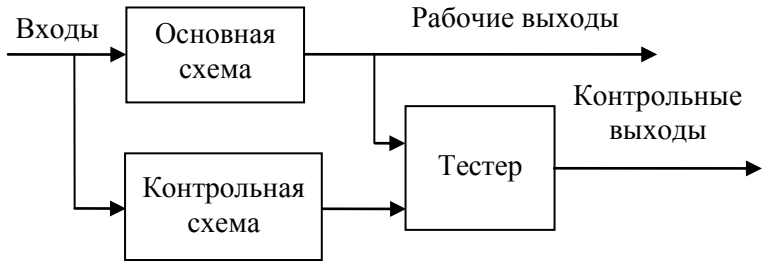

Рис. 5. Схема функционального контроля

Схема контроля состоит из основной схемы, блока контрольной логики и тестера. Контрольным блоком вычисляется набор проверяемых функций. Тестер выдает сигнал ошибки в случае несовпадения рабочих и контрольных функций. Функциональный контроль основан на методах избыточного кодирования, применяющийся при сбоях комбинационных схем, для автоматической коррекции ошибок. Применяют самокорректируемые схемы на базе методов избыточного кодирования. К ним относится код с суммированием (код Бергера), который часто используется при организации функционального контроля [24].

В космической сфере для борьбы с SEU применяется экранирование, что уменьшает поток частиц, но полностью не устраняет его. В прошлом такого решения было достаточно, чтобы избежать ошибок.

Современные электронные схемы становятся все более и более чувствительны к частицам излучения, поэтому одного экранирования недостаточно [25]. Например, неустойчивы к сбоям программируемые логические интегральные схемы, применяемые в космосе. У них могут происходить сбои в ячейках статической памяти под воздействием радиации. Для устранения ошибок применяют очистку конфигурационной памяти, динамическую реконфигурацию [26].

3. Задача повышения надежности с помощью перераспределения интенсивностей отказов

При разработке современных цифровых устройств возникают вопросы, связанные с выбором оптимального конструкторского решения, которое бы обладало наилучшими технико-экономическими показателями. При проектировании систем специального назначения большое значение имеет надежность устройств и поэтому решаются задачи оп-

тимизации, в которых главный вопрос – оптимальное обеспечение надежности путем резервирования при минимальных затратах [27].

Нами ставится задача повышения надежности за счет оптимального распределения интенсивностей отказов. Пусть система состоит из N подсистем, соединенных последовательно. В качестве показателя надежности системы выступает вероятность безотказной работы (ВБР). Для системы с последовательным соединением подсистем этот параметр будет определяться произведением ВБР подсистем:

$$P_c(t) = \prod_{i=1}^{N} P_i(t), \tag{3}$$

где i – номер подсистемы, $i = \overline{1, N}$.

Вероятность безотказной работы подсистемы без резервирования определяется как

$$P_i(t) = e^{-\lambda_i \cdot t}, \tag{4}$$

где λ_i – интенсивность отказов i-й подсистемы.

Предположим, что каждая подсистема выполняет часть основных функций и часть функций, которые можно перераспределить. Интенсивность отказов подсистемы в таком случае

$$\lambda_i = \lambda_{ai} + \lambda_{bi}, \tag{5}$$

где λ_{ai} – интенсивность отказов аппаратуры подсистемы при выполнении основных функций, λ_{bi} – интенсивность отказов при выполнении дополнительных функций, т.е. которые можно перераспределять между подсистемами. Она определяется как

$$\lambda_{bi} = A_i \cdot \lambda_{M[i]}, \tag{6}$$

где A_i – коэффициент, учитывающий сложность устройства подсистемы, характеризующий ее надежность, $\lambda_{M[i]}$ – интенсивность отказов i-й переносимой функции в номинальной подсистеме. Тогда задачу можно представить следующим образом. Необходимо найти вектор $\overrightarrow{M}$, при котором целевая функция $P_c(t) \to \max$. Вектор $\overrightarrow{M}$ представляет собой массив, указывающий распределение функций между подсистемами:

$$\overrightarrow{M} = [x_1, x_2, ..., x_n]. \tag{7}$$

Массив состоит из натуральных чисел $x \in \overline{1,N}$, не равных между собой. Таким образом, ставится оптимизационная задача.

4. Решение задачи

Оптимизация заключается в поиске экстремума математической функции. В данном случае это вероятность безотказной работы, которую необходимо увеличить. Количество перестановок (упорядочиваний) множества элементов массива будет равно факториалу числа подсистем. В нашем примере 6 подсистем, а вариантов решения может быть 720. Исходные данные представлены в табл. 1.

Таблица 1

Исходные данные

Номер подсистемы	1	2	3	4	5	6
$\lambda_{ai} \cdot 10^{-5}$, 1/ч	0,7	0,68	0,5	0,45	0,8	0,85
$\lambda_{M[i]} \cdot 10^{-5}$, 1/ч	0,4	0,52	0,2	0,25	0,1	0,25
A_i	1,1	0,7	0,5	1,7	1,2	0,8

Для решения поставленной задачи была выбрана надстройка «Поиск решений» пакета Microsoft Exel. В качестве детерминированного алгоритма был применен метод обобщенного приведенного градиента, в качестве стохастического алгоритма применен эволюционный алгоритм. Также была разработана программа на языке C#, находящая решение путем перебора всех возможных вариантов. Полученные результаты представлены в табл. 2.

Таблица 2

Полученные результаты

Алгоритм решения	$P_c(t)$	Массив $\overrightarrow{M}$
Детерминированный алгоритм обобщенного приведенного градиента (ОПГ)	0,9454	1,2,6,4,5,3
Эволюционный алгоритм	0,9473	4,1,2,5,3,6
Полный перебор	0,9473	6,1,2,5,3,4

(Алгоритм не всегда сходится к решению – стохастический).

Заключение

В ходе работы были рассмотрены основные факторы, влияющие на надежность, рассмотрены методы повышения надежности. Также была поставлена задача повышения надежности с помощью перераспределения интенсивностей отказов.

В результате работы были получены различные решения. Так, с поставленной задачей лучше справился эволюционный алгоритм оптимизации. Детерминированные алгоритмы оптимизируют целевую функцию, используя определенную комбинацию формул, в связи с чем не всегда точны в подобных задачах, так как могут останавливаться в поиске решения в точке локального экстремума функции. Однако детерминированные алгоритмы достаточно точны, если сравнивать значение целевой функции в разных областях, используя разные точки старта на области координат.

Стохастический алгоритм оказался более успешным в поиске оптимального решения. Это связано с тем, что такие алгоритмы не используют сложных математических вычислений, не гарантируют точного решения. Они во многом основаны на вероятностном подходе, реже попадают в локальные экстремумы и чаще находят глобальные. Поэтому часто прибегают к комбинированному подходу, при котором сочетают детерминированный и стохастический подход.

Таким образом, повышение надежности возможно добиться благодаря грамотному распределению интенсивностей отказов, оптимально распределяя задачи между разными подсистемами.

Библиографический список

1. ГОСТ 27.002–2015. Надежность в технике. Основные понятия. Термины и определения. (Введ. 2017–03–01). – М.: Стандатинформ, 2016. – 23 с.

2. Тимошенков С.П., Симонов Б.М., Горошко В.Н. Основы теории надежности: учебник и практикум. – 1-е изд. – М.: Юрайт, 2015. – 445 с. (Бакалавр. Академический курс).

3. Анализ методов обеспечения пассивной отказоустойчивости цифровых устройств и систем / С.Ф. Тюрин [и др.] // Вестник Пермского национального исследовательского университета. Электротехни-

ка, информационные технологии, системы управления. – 2011. – № 5. – С. 143–153.

4. Neumann J. Von. Probabilistic logic and the synthesis of reliable organisms from unreliable components. Automata studies / C. Shannon and J. McCarthy (eds). – Princeton University Pressio. – 1956. – P. 43–98.

5. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем // Искусственный интеллект. – 2008. – № 4. – С. 253–264.

6. Авиженис А. Отказоустойчивость – свойство, обеспечивающее постоянную работоспособность цифровых систем // Тр. Ин-та инженеров по электротехнике и радиоэлектронике. – 1978. – Т. 66, № 10. – С. 5–15.

7. Avizienis A., Laprie J.-C. Dependable computing: from concepts to application // IEEE Trans. on Computers. – 1986. – № 74 (5). – P. 629–638.

8. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. – М., 2016. – 544 с.

9. Методология проектирования радиационно-стойких микросхем на основе БМК для космических аппаратов / А.С. Басаев [и др.] // Проблемы разработки перспективных микро-и наноэлектронных систем (МЭС): сб. тр. всерос. науч.-техн. конф. – Зеленоград: Изд-во Ин-та проблем проектирования в микроэлектронике РАН, 2008. – № 1. – С. 1–8.

10. Анализ методов обеспечения пассивной отказоустойчивости цифровых устройств и систем / С.Ф. Тюрин [и др.] // Вестник Пермского национального исследовательского университета. Электротехника, информационные технологии, системы управления. – 2011. – № 5. – С. 143–153.

11. Тюрин С.Ф. Статическая оперативная память на основе отказоустойчивой ячейки базового матричного кристалла // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2016. – № 1 (17). – С. 16–27.

12. Тюрин С.Ф. Радиационно-устойчивая ячейка SRAM // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2014. – № 4 (12). – С. 14–30.

13. Дианов В.Н. Диагностика и надежность автоматических систем. – М.: Изд-во МГИУ, 2005. – 160 с.

14. Sparkes Matthew. The Perseverance rover runs on processors used in iMacs in the 1990s. – New Scientist, 2021, 26 Febr.

15. Hecht Jeff. Hubble telescope loses another gyroscope. – New Scientist, 2007, 6 September.

16. Надежность и эффективность в технике: справочник: в 10 т. / ред. совет: В.С. Авдуевский (председат.) [и др.]. – М.: Машиностроение, 1986–1990. – Т. 9: Техническая диагностика. – М.: Машиностроение, 1987. – 352 с.

17. Kshirsagar R.V., Patrikar R.M. Design of a novel fault-tolerant voter circuit for TMR implementation to improve reliability in digital circuits. Microelectron // Reliab. – 2009. – 49. – P. 1573–1577. [CrossRef]

18. Arifeen T., Hassan A.S., Lee J.-A. A fault tolerant voter for approximate triple modular redundancy // Electronics. – 2019. – Vol. 8, № 3. – P. 332.

19. Тюрин С.Ф., Прохоров А.С. Отказоустойчивая программируемая логическая матрица // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2017. – № 23. – С. 45–58.

20. Каменских А.Н. Разработка библиотеки высоконадежных элементов на основе резервирования на транзисторном уровне // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2021. – № 1(37). – С. 153–167.

21. Функционально-полный толерантный элемент / С.Ф. Тюрин [и др.] // Науч.-техн. ведомости Санкт-Петербург. гос. политехн. ун-та. – 2011. – № 115. – С. 24–30.

22. Кон Е.Л., Фрейман В.И. Подходы к тестовому диагностированию цифровых устройств // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2012. – № 6. – С. 231–241.

23. Сперанский Д.В., Скобцов Ю.А., Скобцов В.Ю. Моделирование, тестирование и диагностика цифровых устройств. – М.: ИНТУИТ, 2016. – 439 с.

24. Aranda L.A., Sánchez-Macián A., Maestro J.A. ACME: A tool to improve configuration memory fault injection in SRAM-based FPGAs // IEEE Access. – 2019. – Vol. 7. – P. 128153–128161.

25. Impact of scaling on neutron-induced soft error in SRAMs from a 250 nm to a 22 nm design rule / E. Ibe, H. Taniguchi, Y. Yahagi, K. Shimbo, T. Toba // IEEE Trans. Electron Devices. – Jul. 2010. – Vol. 57, № 7. – P. 15271538.

26. Estimating soft processor soft error sensitivity through fault injection / N.A. Harward, M.R. Gardiner, L.W. Hsiao, M.J. Wirthlin // Proc. IEEE 23rd Annu. Int. Symp. Field-Program. Custom Comput. Mach. (FCCM). – May 2015. – P. 143150.

27. Тюрин С.Ф., Громов О.А., Каменских А.Н. Программный комплекс исследования методов повышения надежности // Вестник ИжГТУ им. М.Т. Калашникова. – 2012. – № 2(54). – С. 153–156.

References

1. GOST 27.002–2015. Nadezhnost' v tekhnike. Osnovnye poniatiia. Terminy i opredeleniia. (Vved. 2017-03-01) [GOST 27.002-2015. Reliability in technology. Basic concepts. Terms and Definitions. (Introduced 2017-03-01)]. Moscow: Standatinform, 2016, 23 p.

2. Timoshenkov S.P., Simonov B.M., Goroshko V.N. Osnovy teorii nadezhnosti: uchebnik i praktikum [Fundamentals of the theory of reliability: Textbook and workshop]. 1nd ed. Moscow: Iurait, 2015, 445 p. (Bakalavr. Akademicheskii kurs).

3. Tiurin S.F. et al. Analiz metodov obespecheniia passivnoi otkazoustoichivosti tsifrovykh ustroistv i sistem [The analysis of methods of passive fault-tolerance in digital computing systems]. *Vestnik Permskogo natsional'nogo issledovatel'skogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2011, no. 5, pp. 143-153.

4. Neumann J. Von. Probabilistic Logic and the Synthesis of Reliable Organisms from Unreliable Components. Automata Studies, C. Shannon and J. McCarthy (eds). Princeton University Pressio, 1956, pp. 43-98.

5. Maslova N.A. Metody otsenki effektivnosti sistem zashchity informatsionnykh sistem [Methods for assessing the effectiveness of information systems protection systems]. *Iskusstvennyi intellekt*, 2008, no. 4, pp. 253-264.

6. Avizhenis A. Otkazoustoichivost' - svoistvo, obespechivaiushchee postoiannuiu rabotosposobnost' tsifrovykh sistem [Fault-toleranct - the characteristic that ensures continuous operation of digital systems]. *Trudy Instituta inzhenerov po elektrotekhnike i radioelektronike*, 1978, vol. 66, no. 10, pp. 5-15.

7. Avizienis A., Laprie J.-C. Dependable Computing: From Concepts to Application. *IEEE Trans. on Computers*, 1986, no. 74 (5), pp. 629-638.

8. Shubinskii I.B. Nadezhnye otkazoustoichivye informatsionnye sistemy. Metody sinteza [Reliable failure-safe information systems. Synthesis methods]. Moscow, 2016, 544 p.

9. Basaev A.S. et al. Metodologiia proektirovaniia radiatsionnostoikikh mikroskhem na osnove BMK dlia kosmicheskikh apparatov [The methodology of radiation tolerant design of ASIC based microsystems for space applications]. *Problemy razrabotki perspektivnykh mikro-i nanoelektronnykh sistem (MES). Sbornik trudov vserossiiskoi nauchnotekhnicheskoi konferentsii*. Zelenograd: Institut problem proektirovaniia v mikroelektronike RAN, 2008, no. 1, pp. 1-8.

10. Tiurin S.F. et al. Analiz metodov obespecheniia passivnoi otkazoustoichivosti tsifrovykh ustroistv i sistem [The analysis of methods of passive fault-tolerance in digital computing systems]. *Vestnik Permskogo natsional'nogo issledovatel'skogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2011, no. 5, pp. 143-153.

11. Tiurin S.F. Staticheskaia operativnaia pamiat' na osnove otkazoustoichivoi iacheiki bazovogo matrichnogo kristalla [Static RAM based on a fault-tolerant cell of the base matrix crystal]. *Vestnik Permskogo natsional'nogo issledovatel'skogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2016, no. 1 (17), pp. 16-27.

12. Tiurin S.F. Radiatsionno-ustoichivaia iacheika SRAM [Radiationresistant SRAM cell]. *Vestnik Permskogo natsional'nogo issledovatel'skogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2014, no. 4(12), pp. 14-30.

13. Dianov V.N. Diagnostika i nadezhnost' avtomaticheskikh sistem [Diagnostics and reliability of automation systems]. Moscow: Moskovskii gosudarstvennyi industrial'nyi universitet, 2005, 160 p.

14. Sparkes Matthew. The Perseverance Rover Runs on Processors Used in iMacs in the 1990s. New Scientist, 2021, 26 Febr.

15. Hecht Jeff. Hubble telescope loses another gyroscope. New Scientist, 2007, 6 September.

16. Nadezhnost' i effektivnost' v tekhnike: spravochnik [Reliability and efficiency in engineering: reference]. Eds V.S. Avduevskii et al. Moscow: Mashinostroenie, 1986-1990, vol. 9. Tekhnicheskaia diagnostika. Moscow: Mashinostroenie, 1987, 352 p.

17. Kshirsagar R.V., Patrikar R.M. Design of a novel fault-tolerant voter circuit for TMR implementation to improve reliability in digital circuits. Microelectron. *Reliab*, 2009, 49, pp. 1573-1577. [CrossRef]

18. Arifeen T., Hassan A.S., Lee J.-A. A fault tolerant voter for approximate triple modular redundancy. *Electronics*, 2019, vol. 8, no. 3, 332 p.

19. Tiurin S.F., Prokhorov A.S. Otkazoustoichivaia programmiruemaia logicheskaia matritsa [Fault-tolerant programmable logic matrix]. *Vestnik Permskogo natsional'nogo issledovatel'skogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2017, no. 23, pp. 45-58.

20. Kamenskikh A.N. Razrabotka biblioteki vysokonadezhnykh elementov na osnove rezervirovaniia na tranzistornom urovne [The development of fault-tolerant logic gate library using transistor-level redundancy method]. *Vestnik Permskogo natsional'nogo issledovatel'skogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2021, no. 1(37), pp. 153-167.

21. Tiurin S.F. et al. Funktsional'no-polnyi tolerantnyi element [The functionally complete tolerant logic element]. *Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo unuversiteta*, 2011, no. 115, pp. 24-30.

22. Kon E.L., Freiman V.I. Podkhody k testovomu diagnostirovaniiu tsifrovykh ustroistv [Approaches to test diagnostics of digital devices]. *Vestnik Permskogo natsional'nogo issledovatel'skogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2012, no. 6, pp. 231-241.

23. Cperanskii D.V., Skobtsov Iu.A., Skobtsov V.Iu. Modelirovanie, testirovanie i diagnostika tsifrovykh ustroistv [Digital Device Modeling, Testing, and Diagnostics]. Moscow: INTUIT, 2016, 439 p.

24. Aranda L.A., Sánchez-Macián A., Maestro J.A. ACME: A tool to improve configuration memory fault injection in SRAM-based FPGAs. *IEEE Access*, 2019, vol. 7, pp. 128153-128161.

25. Ibe E., Taniguchi H., Yahagi Y., Shimbo K., Toba T. Impact of scaling on neutron-induced soft error in SRAMs from a 250 nm to a 22 nm design rule. *IEEE Trans. Electron Devices*. Jul. 2010, vol. 57, no. 7, 15271538 p.

26. Harward N.A., Gardiner M.R., Hsiao L.W., Wirthlin M.J. Estimating soft processor soft error sensitivity through fault injection. *Proc. IEEE 23rd Annu. Int. Symp. Field-Program. Custom Comput. Mach. (FCCM)*. May 2015, 143150 p.

27. Tiurin S.F., Gromov O.A., Kamenskikh A.N. Programmnyi kompleks issledovaniia metodov povysheniia nadezhnosti [Software complex for research of methods of increasing reliability]. *Vestnik Izhevskogo gosudarstvennogo tekhnicheskogo universiteta imeni M.T. Kalashnikova*, 2012, no. 2(54), pp. 153-156.

Сведения об авторах

Бурдышев Иван Васильевич (Пермь, Россия) – аспирант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: iburdyshev@mail.ru).

Тюрин Сергей Феофентович (Пермь, Россия) – заслуженный изобретатель Российской Федерации, доктор технических наук, профессор кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: tyurinsergfeo@yandex.ru), профессор кафедры «Математическое обеспечение вычислительных систем» Пермского государственного национального исследовательского университета (614990, Пермь, ул. Букирева, 15).

About the authors

Sergey F. Tyurin (Perm, Russian Federation) – Honored Inventor of the Russian Federation, Doctor of Technical Sciences, Professor at the Department of Automation and Telemechanics Perm National Research

Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: tyurinsergfeo@yandex.ru), Professor at the Department of Software Computing Systems Perm State National Research University (614990, Perm, 15, Bukireva str.).

Ivan V. Burdyshev (Perm, Russian Federation) – Graduate Student of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: iburdyshev@mail.ru).

Поступила 27.10.2021
Одобрена 13.12.2021
Принята к публикации 20.06.2022

Финансирование. Исследование не имело спонсорской поддержки.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Вклад авторов. Все авторы сделали эквивалентный вклад в подготовку публикации.