УДК 621.382+621.396.6 DOI: 10.22184/NanoRus.2019.12.89.282.286

ПРОГРАММНО-АППАРАТНЫЕ МЕТОДЫ ЛОКАЦИИ ОШИБОК И СБОЕВ ДЛЯ РЕЗЕРВИРОВАННЫХ И МНОГОКАНАЛЬНЫХ СФ-БЛОКОВ

SOFTWARE AND HARDWARE METHODS OF LOCATING ERRORS AND FAILURES FOR REDUNDANT AND MULTI-CHANNEL IP-BLOCKS

АНТОНОВ АНДРЕЙ АЛЕКСАНДРОВИЧ[1]

ПРОЗОРОВА АЛЕКСАНДРА ГЕННАДИЕВНА[1]

СОЛОВЬЕВА ЛЮДМИЛА АЛЕКСЕЕВНА[1]

КРАСНЮК АНДРЕЙ АНАТОЛЬЕВИЧ[1,2]
aakrasnyuk@mephi.ru
aakr@cs.niisi.ras.ru

[1] *ФГУ ФНЦ НИИСИ РАН*
117218, Москва, Нахимовский просп., 36, к. 1
[2] *Национальный исследовательский ядерный университет «МИФИ»*
115409, Россия, г. Москва, Каширское ш., 31

ANTONOV ANDREY A.[1]

PROZOROVA ALEKSANDRA G.[1]

SOLOVYEVA LYUDMILA A.[1]

KRASNYUK ANDREY A.[1,2]
aakrasnyuk@mephi.ru
aakr@cs.niisi.ras.ru

[1] *SRISA RAS*
bld. 1, 36 Nakhimovskiy Ave., Moscow, 117218
[2] *National Research Nuclear University MEPhI,*
31 Kashirskoe Highway, Moscow, 115409, Russia

Представлены выводы о схемотехнических и методологических решениях для определителей (локаторов) ошибок и сбоев, реализуемых как специализированные узлы микропроцессоров.
Ключевые слова: СФ/IP-блоки; SEC-DED-кодеки; System Chain of Trust; Root of Trust.
The paper presents conclusions about circuit and methodological solutions for determinants (locators) of errors and failures implemented as specialized components of microprocessors.
Keywords: IP blocks; SEC-DED encoders; System Chain of Trust; Root of Trust.

Задачи обнаружения, локализации, исправления и защиты от ошибок, сбоев, отказов в микроэлектронных системах являются основополагающими и фундаментальными проблемами как при разработке программного обеспечения, так и при аппаратной реализации микроэлектронных систем, включая сложно-функциональные (СФ) блоки и системы на их основе. Традиционно терминология «локация ошибок» относилась именно к направлениям разработки, верификации и характеризации программного обеспечения и, например, топологической и физической реализации интегральных схем и систем на их основе. Вопросы программно-аппаратной реализации данных решений возникли из необходимости построения многоканальных, многопоточных и резервированных систем, устойчивых к внешним деструктивным воздействиям, таким как высокая температура или радиационные факторы космического пространства. В этом случае актуальной задачей становятся определение и возможное исправление нестационарных ошибок и сбоев, появление которых не связано с ошибками конструирования и проектирования. В данной работе рассматриваются и систематизируются те решения данной проблемы, которые могут быть реализованы при разработке многоканальных и резервированных элементов СБИС.

ПРИНЦИПЫ МНОГОКАНАЛЬНОСТИ И РЕЗЕРВИРОВАНИЯ В СФ-БЛОКАХ

Сложно-функциональные СФ/IP-блоки, по своему определению, являются комбинацией программной и аппаратной составляющих проекта. Цифровая часть проекта — Soft-IP формируется на основе RTL-описания безотносительно привязки к конкретной технологии. К конкретному технологическому процессу привязаны так называемые PHY — физические (топологические) блоки, разработанные под определенный техпроцесс. Система на кристалле из разных СФ/IP-блоков должна верифицироваться на функциональном уровне с помощью VIP-блоков, которые поставляются разработчиком Soft-IP. Функциональная верификация может вестись на любом САПР. По данным TSMC IP Alliance, современные проекты по нормам 14 нм и ниже могут использовать от 220 и выше различных СФ/IP-блоков [1]. Стандарты — основа формализации СФ/IP-блоков. СФ/IP принципиально не может выходить за пределы стандарта. Поэтому обеспечение определенных степеней свободы при проектировании схем на основе различных СФ/IP-блоков так или иначе требует введения функциональной избыточности, что наиболее просто реализуется именно на принципах многоканальности и дублирования унифицированных узлов, рис. 1.

В общем случае требования к управлению политикой контроля и защиты от ошибок и сбоев включают в себя защиту не только от внешних и внутренних программных атак, но и от физических деструктивных воздействий. Наиболее критическими направлениями для многоканальных и многоядерных систем являются программные модули политики кеширования, записи и чтения в памяти, менеджеров когерентности и др., как показано на рис. 2 [3]. Введение в архитектуру

процессоров отдельных модулей безопасности, аналогичных модулям watchdog, представляет интерес лишь с точки зрения повышения производительности систем, но требует обоснования их собственной безусловной устойчивости к внешним и внутренним ошибкам и сбоям. Более обоснованными для многоканальных и многоядерных вычислительных систем должны стать и более простые традиционные решения для элементов управления и памяти, например на основе резервированных конечных цифровых автоматов.

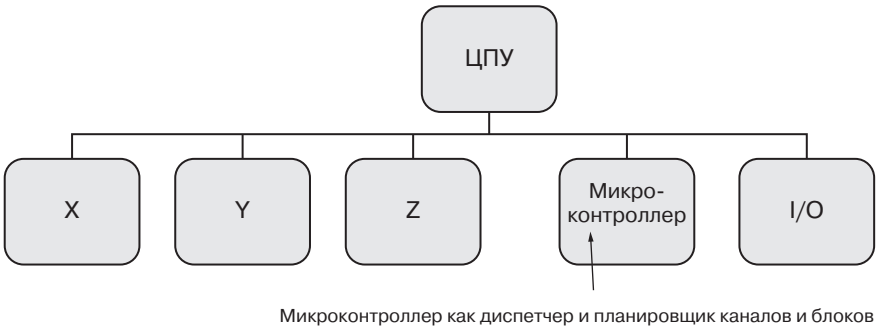


Рис. 1. Пример принципа многоканальности в реализации СФ/IP-блоков аппаратных ускорителей проектов RISC-V [2]

ПРОГРАММНО-АППАРАТНАЯ ЛОКАЦИЯ ОШИБОК ПО ХЭММИНГУ

Методы помехоустойчивого кодирования по Хэммингу и Риду — Соломону являются наиболее известными примерами реализации программно-аппаратных методов локации нестационарных ошибок и сбоев. Надо отметить, что локация ошибок по Хэммингу является в равной мере уникальным по красоте решением как в программной, так и в аппаратной части своей реализации [4]. На рис. 3 приведен классический [5] пример локации одиночных ошибок по Хэммингу. Необходимым условием исполнения данного алгоритма является формирование кодового слова из информационных и контролирующих бит. Соответствующая аппаратная реализация относится к классу SED-DEC-кодеков (single-error-detection double-error-correction), которые позволяют однозначно исправлять однократные и детектировать двукратные ошибки в кодовом слове.

Рис. 2. Контроль ошибок и защита данных СнК на программном уровне [2]

Практическая аппаратная реализация данного алгоритма для элементов памяти, описанная в работе [4], предполагает использование метода дополнительных столбцов [6]. Метод заключается в том, что при проектировании схем памяти в массив вводятся дополнительные столбцы и мультиплексоры, позволяющие при возникновении кратных сбоев в каком-либо столбце заменять его дополнительным. Этот схемотехнический метод дополняется алгоритмическим: дополнительные столбцы, пока они не используются для замены, применяются как элементы хранения дополнительных контролирующих битов кодового слова. При проектировании элементов памяти (пример функциональной схемы приведен на рис. 3) наиболее распространенные размерности информационных слов (16, 32, 64 и т. д.) не являются оптимальными для кодов, вследствие чего возникает избыточность, выражающаяся в том, что SED-DEC-код может детектировать часть ошибок кратности больше двух.

Эту избыточность можно также использовать для исправления двукратных смежных ошибок, преобразовав уже существующий SED-DEC-код в SED-DAEC (double-adjacent-error-correction) код. Для этого столбцы проверочной матрицы SED-DEC-кода необходимо переставить так, чтобы суммарные синдромы ошибок в любых двух смежных битах не совпадали друг с другом [6]. Сравнительный анализ различных методов локации

№ п/п	1	2	3	4	5	6	7
Исходное слово	0	1	0	0	1	1	1
Информационные биты			0		1	1	1
Контрольные биты	A	B		C			
a = (0 + 1 + 1)%2 = 0 = A			0		1		1
b = (0 + 1 + 1)%2 = 0 ≠ B			0		1	1	
c = (1 + 1 + 1)%2 = 1 ≠ C					1	1	1
Вычисление позиции бита ошибки							
		2	+	4		=6	
Исправление ошибки	0	1	0	0	1	0	1

Рис. 3. Пример алгоритма локации и исправления ошибки данных по Хэммингу [5]

ошибок по Хэммингу подтверждает эффективность аппаратной реализации данного метода лишь при наличии предварительного кодирования и представления данных.

МАЖОРИРОВАНИЕ И ОПРЕДЕЛЕНИЕ ОТСУТСТВИЯ ОШИБОК И СБОЕВ

Метод и алгоритм дополнительных столбцов в общем случае относится к классу резервированных устройств и элементов, в котором механизм дублирования и резервирования используется для определения и локации не ошибок, а наоборот, их отсутствия, правильности кодовых слов. Существенным достоинством стратегии резервирования является безотносительность принимаемых решений от предварительного кодирования данных и команд. В качестве референсного источника анализируемых данных были использованы троированные ячейки памяти на базе двухуровневых трехтактных триггеров (рис. 5*а*). В данной ячейке памяти предполагаются три основных выхода. В зависимости от информации, записанной в триггере, на одном из выходов должна быть единица (в соответствии с заданной для анализа таблицей истинности).

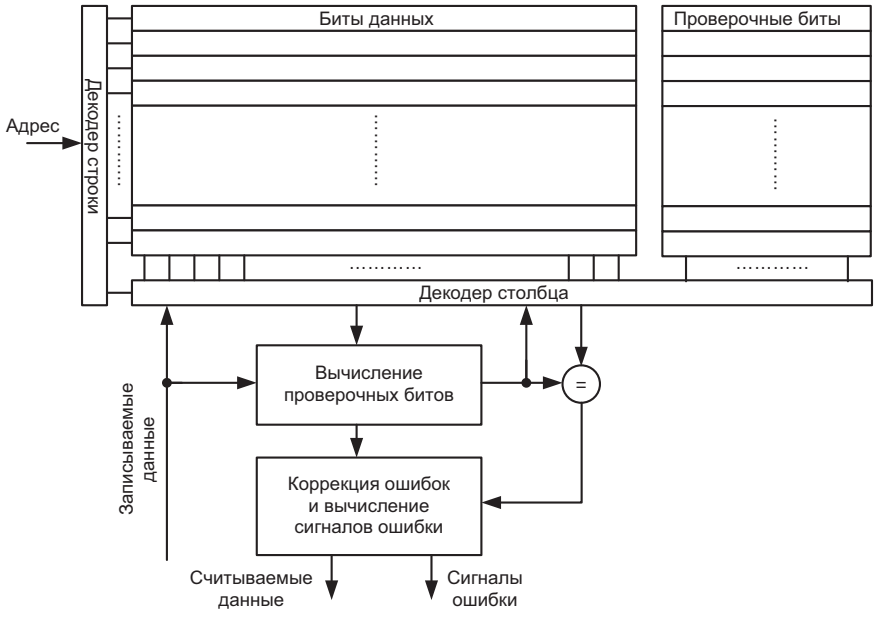
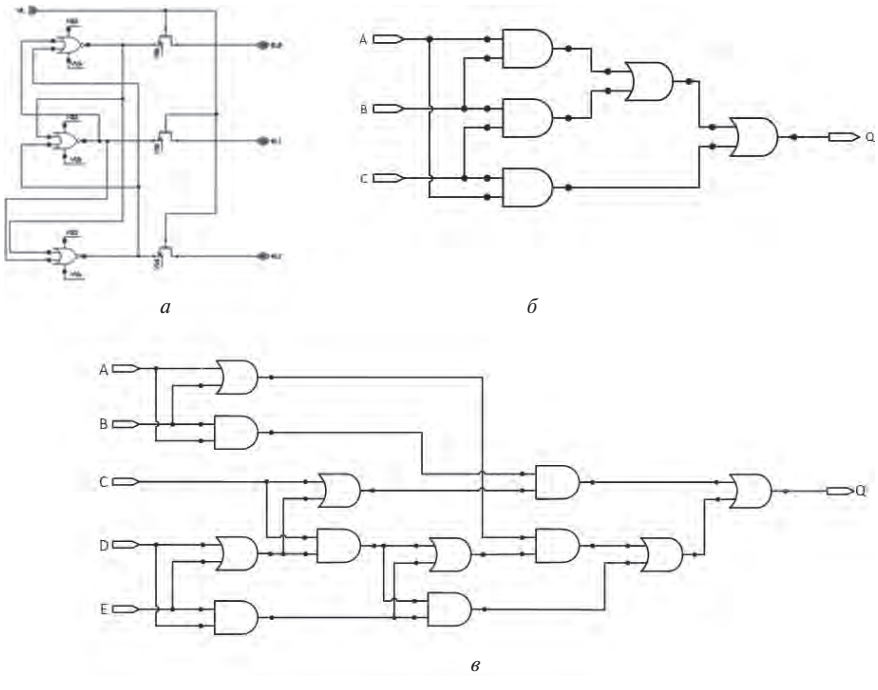


Рис. 4. Функциональная схема использования SED-DEC-кодов для локации и исправления ошибок



а *б* *в*

Рис. 5. Модельное описание: а) троированная ячейка памяти на базе двухуровневых трехтактных триггеров; б) и в) вотеры на базе мажоритарных элементов «2 из 3» и «3 из 5» соответственно

Признаком ошибки определяется невыполнение условия $Q = A \cdot B + B \cdot C + A \cdot C$ для комбинации данных на выходах ячейки памяти [7].

При моделировании сигналы с выходов ячеек памяти подавались на входы схемы мажорирования, или вотеры. В исследовании рассмотрены случаи с использованием схем мажорирования «2 из 3» и «3 из 5» (рис. 5*б* и рис. 5*в*) [8].

Алгоритм исправления (перезаписи) данных основывается на изменении состояния ячеек памяти в локализованных сбоем ячейках памяти по команде воутера. Данный подход обеспечивает максимальное быстродействие при исправлении одиночных сбоев резервированных ячеек памяти. Как отмечалось ранее, сопряженные с воутером ячейки памяти имеют три информационных выхода, комбинация которых соответствует хранимой информации. Помимо элемента мажорирования каждый выход подается на схему перезаписи. Также на схему идет выход вотера, а выход самой схемы заводится обратной связью на выход ячейки памяти (количество ячеек определяется количеством входов схемы мажорирования). Пример аппаратной реализации данного алгоритма приведен на рис. 6. Рассмотренные решения основаны на стандартных библиотечных моделях вентилей и сопряженных с ними триггерных ячейках памяти для основных планарных технологий (28 нм, 65 нм, 180 нм). Анализ влияния температурных и радиационных воздействий показал устойчивость и стабильность работы подобных структур [7, 8].

КОНЦЕПЦИИ COT И ROT И КОНЕЧНЫЕ ЦИФРОВЫЕ АВТОМАТЫ

Стратегии и концепции System Chain of Trust (CoT) и Root of Trust (RoT) в настоящее время уделяется большое внимание, в частности в системах

самодиагностики проектов RISC-V [9]. Во многом данная концепция построения микропроцессорных СФ/IP-блоков развивает теорию трасс для цифровых конечных автоматов [10], которая позволяет определять при определенных ограничениях как самое слабое звено в цепи исполнителей команд (CoT), так и необходимую позицию для самого надежного элемента в цепи (RoT), способного удержать систему от падения при наличии ошибки или сбоя. Для локации и исправления ошибок при данной стратегии моделирования тестируемая система аппроксимируется системой конечных автоматов (КА). Состояния автомата соответствуют состояниям этой системы, входной алфавит — набору возможных воздействий на систему (стимулов), выходной алфавит — набору возможных реакций системы, а начальное состояние — состоянию, в котором тестируемая система находится (или в которое приводится) в начале теста. Задача определения и локации ошибок при этом сводится к анализу трасс — набора путей на графе переходов анализируемой системы и соответствующих выпадений на трассе переходов от ожидаемых значений.

Определение, локация ошибок осуществляются на основе достаточно простых формальных спецификаций (требований) к системе. То есть каждый раз после применения очередного стимула полученные от тестируемой системы реакции анализируются на соответствие спецификации. Несоответствие наблюдаемой реакции описанным в спецификации требованиям или расхождения между ожидаемым и наблюдаемым состоянием целевой системы считается ошибкой. Ключевым достоинством данной стратегии по отношению к резервированным и многоканальным элементам СФ/IP-блоков является то, что стимулы и результаты реакции могут быть общими для всех составляющих и выходной алфавит при отсутствии ошибок должен совпадать для всех каналов. Несовпадение требований спецификации трасс и результатов прохождения ее однозначно указывает самое слабой звено или канал в анализируемой системе [10]. В рамках данного исследования были разработаны тестовые структуры зависимых триггерных цепочек и проведен анализ наиболее уязвимых топологических узлов этих схем. Выбор решений определялся по возможности оценки критического заряда в плечах триггеров, образуемого, например, при наличии однократных помех.

Тестовые структуры разработаны на стандартных библиотечных элементах по технологическим нормам КМОП 65 нм. Моделирование производились при типичных условиях для моделей класса typical. Анализировалась реакция триггерных цепочек при инжекции токовой помехи в различные узлы трассы. Целью исследований была проверка концепции о наиболее стабильных

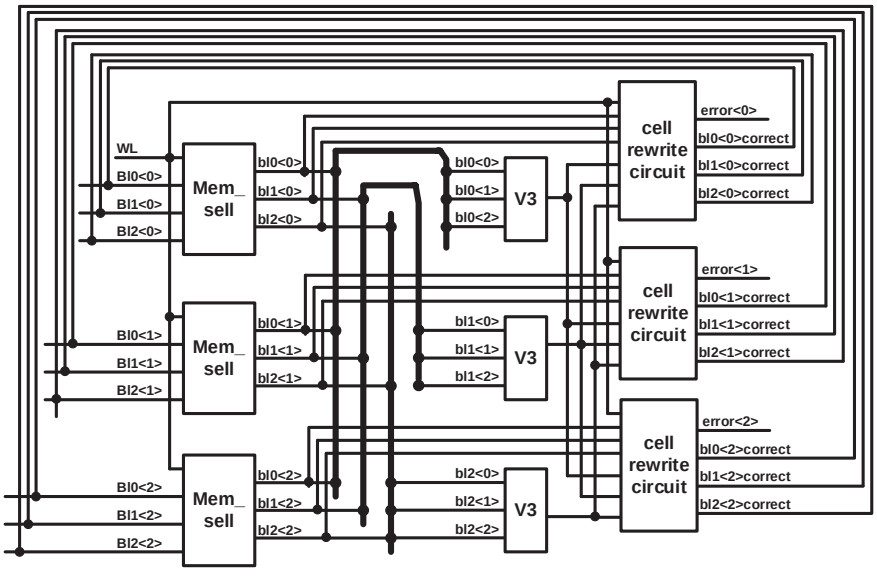


Рис. 6. Троированная схема с решающим вотером «2 из 3», применимая для задач локации и исправления ошибок

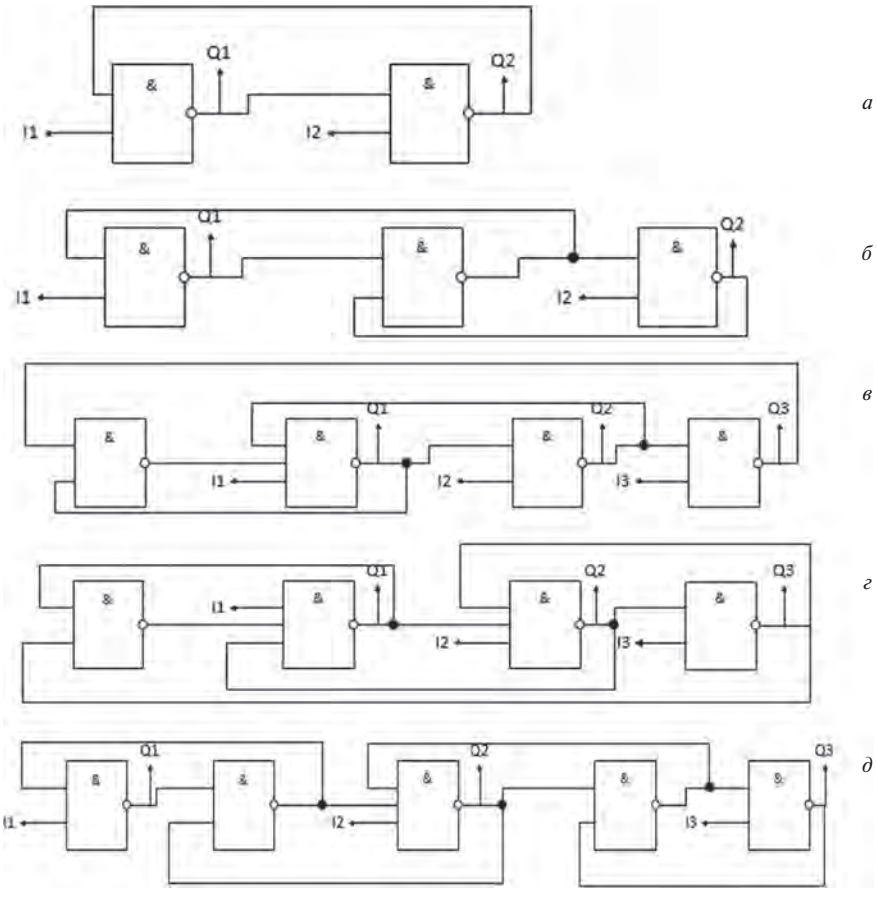


Рис. 7. Тестовые структуры триггерных цепочек для моделирования концепции RoT

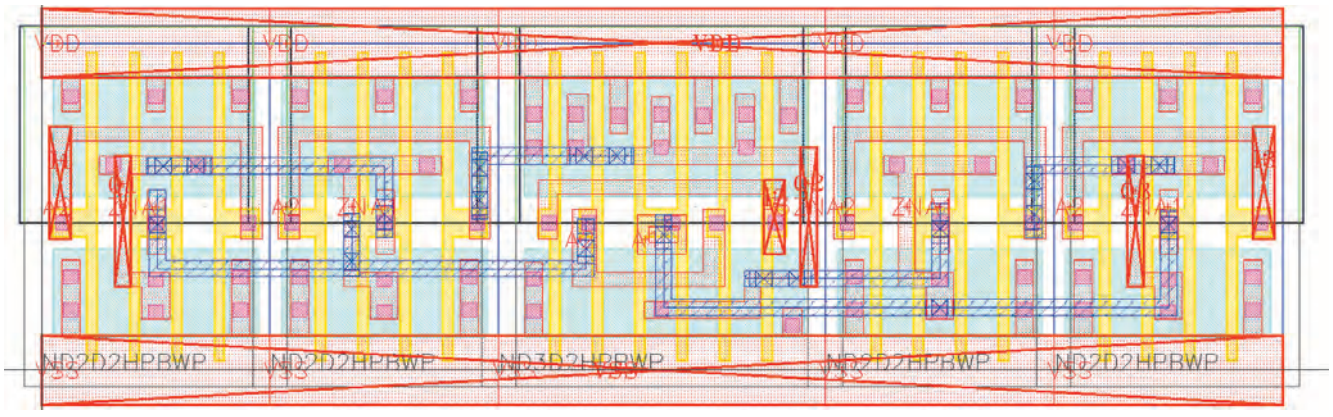


Рис. 8. Пример топологии триггерной цепочки, показанной на рис. 7д

узлах цепочек, способных удерживать всю цепочку от падения при наличии внешнего физического воздействия. Изменялась только величина поданной помехи.

Было рассмотрено четыре симметричных триггерных цепочки, за референсную топологию которых был взят RS-триггер (рис. 7*а*). Для того чтобы оценить устойчивость узлов триггера, на каждый узел была подана вариативная помеха в виде короткого импульса с эквивалентной величиной заряда. Для каждого узла получено семейство графиков, демонстрирующих поведение данного узла в зависимости от величины поданной на него помехи. На основе этих зависимостей можно выделить наиболее слабые и наиболее устойчивые узлы отдельных триггеров, а также можно рассчитать количественно критический заряд, при котором происходит сбой. При топологической и схемотехнической симметрии схем наибольшую устойчивость показали центральные узлы схем с нечетным числом вентилей (рис. 7*б* и рис. 7*д*). Критический заряд ошибки для цепочек на рис. 7*в* и на рис. 7*г* почти в два раза ниже, чем в узле Q2 схемы на рис. 7*д* (рис. 8).

Данный эффект можно объяснить тем, что в случае четного числа инверторов их центральный узел может быть узлом конкуренции плечей цепочки, а в случае нечетного числа вентилей состояния входов-выходов центрального вентиля являются взаимодополняющими для плечей цепочки и взаимно скомпенсированными. Поэтому ошибка в одном из плечей не перебрасывает состояние всей цепочки. В целом это подтверждает концепцию RoT о значимости и необходимости коренных узлов в цепочках КА.

ЗАКЛЮЧЕНИЕ

Авторы считают, что в данной работе новыми являются следующие положения и результаты:

- на примере задач, стоящих перед разработчиками микропроцессорных СФ/IP-блоков, представлены выводы о схемотехнических и методологических решениях для определителей (локаторов) ошибок и сбоев, реализуемых как специализированные узлы микропроцессоров;
- рассмотрены вопросы корреляции концепций System Chain of Trust (CoT) и Root of Trust (RoT) и их аппаратной реализации на уровне исследования тестовых триггерных цепочек, сформирована методика определения слабого и наиболее важного звена при наличии нестационарных ошибок и сбоев;
- приведенные рекомендации могут быть реализованы на отечественных КНИ и КМОП технологических процессах.

Публикация выполнена в рамках государственного задания ФГУ ФНЦ НИИСИ РАН (проведение фундаментальных научных исследований) по теме №0065-2019-0004.

ЛИТЕРАТУРА:

1. The TSMC IP Alliance Program // http://www.tsmc.com/english/dedicatedFoundry/services/tsmc9000.htm.
2. Matt Cockrell. *Evaluation of RISC-V for Pixel Visual Core* // RISC-V Workshop in Barcelona Proceedings. 7–10 May, 2018.
3. Cybersecurity software increases vulnerability and ruins performance. Dover microsystems // RISC-V Workshop in Barcelona Proceedings. 7–10 May, 2018.
4. Краснюк А.А., Петров К.А. Особенности применения помехоустойчивого кодирования в суб-100 нм микросхемах памяти для космических систем // Микроэлектроника, 2012. — Т. 41. — № 6. — С. 450–456.
5. Крис Касперски. Могущество кодов Рида—Соломона или информация, воскресшая из пепла // Системный администратор — http://www.insidepro.com/kk/027/027r.shtml.
6. Kim I. *et al. Built in self repair for embedded high density SRAM*. Proc. of International Test Conf., 1998. P. 1112–1119.
7. Antonov A.A., Gorbunov M.S., Danilov I.A. *SET Tolerance of 65 nm CMOS Majority Voters: a Comparative Study* // Proceedings of RADECS, 2013.
8. Краснюк А.А., Прозорова А.Г., Соловьева Л.А., Кириченко П.Г. и др. Исследование высокочастотных схем мажорирования для применения в троированных системах // Proceedings of the 28th International Conference CriMico, 2018.
9. Danny Ybarra. *CoT, RoT, RISC-V & High Volume Application* / CTO organization Storage Device Security Architect April 25, 2018 // RISC-V Workshop in Barcelona Proceedings. 7–10 May, 2018.
10. Грошев С.Г. Локализация ошибок методом сокращенного воспроизведения трассы // Труды Института системного программирования РАН, 2008. — № 1. — Т. 14. — 13 с.