

УДК 621.382:004.052.2

## Отказоустойчивые самосинхронные схемы

© 2022 г. А. А. Зацаринный<sup>1</sup>, Ю. А. Степченков<sup>1</sup>✉, Ю. Г. Дьяченко<sup>1</sup>,  
Ю. В. Рождественский<sup>1</sup>, Л. П. Плеханов<sup>1</sup>

<sup>1</sup> Федеральний исследовательский центр  
«Информатика и управление» Российской академии наук,  
ул. Вавилова, д. 44, корп. 2, Москва, 119333, Российская Федерация

✉ Автор для переписки: YStepchenkov@ipiran.ru

**Аннотация.** Статья исследует проблему создания отказоустойчивых самосинхронных (СС) схем. Использование избыточного СС-кодирования и двухфазной дисциплины работы обеспечивает более высокую сбоеустойчивость СС-схем в сравнении с синхронными аналогами. Использование дублирования канала обработки данных вместо традиционного для синхронных схем троирования позволяет сократить избыточность СС-схем в отказоустойчивом исполнении и обеспечивает более высокий уровень надежности в сравнении с синхронными аналогами.

**Ключевые слова:** самосинхронные схемы, логический сбой, отказ, отказоустойчивость, парафазный сигнал, индикация

**Для цитирования:** Зацаринный А.А., Степченков Ю.А., Дьяченко Ю.Г., Рождественский Ю.В., Плеханов Л.П. Отказоустойчивые самосинхронные схемы. *Известия высших учебных заведений. Материалы электронной техники.* 2022; 25(4): 298—304. <https://doi.org/10.17073/1609-3577-2022-4-298-304>

## Fault-tolerant self-timed circuits

A. A. Zatsarinny<sup>1</sup>, Yu. A. Stepchenkov<sup>1</sup>✉, Yu. G. Diachenko<sup>1</sup>,  
Yu. V. Rogdestvenski<sup>1</sup>, L. P. Plekhanov<sup>1</sup>

<sup>1</sup> Federal Research Center «Computer Science and Control»  
of the Russian Academy of Sciences,  
44-2 Vavilova Str., Moscow 119333, Russian Federation

✉ Corresponding author: YStepchenkov@ipiran.ru

**Abstract.** The article considers the problem of developing synchronous and self-timed (ST) circuits that are tolerant to faults. Redundant ST coding and two-phase discipline ensures that ST circuits are more soft error tolerant than synchronous counterparts. Duplicating ST channels instead of tripling reduces the fault-tolerant ST circuits' redundancy and retains their reliability level compared to synchronous counterparts.

**Keywords:** self-timed circuits, soft error, fault, voting, dual-rail signal, indication

**For citation:** Zatsarinny A.A., Stepchenkov Yu.A., Diachenko Yu.G., Rogdestvenski Yu.V., Plekhanov L.P. Fault-tolerant self-timed circuits. *Izvestiya vuzov. Materialy elektronnoi tekhniki = Materials of Electronics Engineering.* 2022; 25(4): 298—304. <https://doi.org/10.17073/1609-3577-2022-4-298-304>

## Введение

В синхронных схемах проблема отказоустойчивости неразрывно связана с проблемой сбоеустойчивости. Отсутствие встроенных средств проверки корректности текущего состояния делает невозможным различие логических сбоев, длительность которых превышает один период тактового сигнала, и отказов.

Под сбоем понимается изменение логического состояния входа или выхода элемента, вызванное одиночным событием (пролетом ядерной частицы, шумовой наводкой и т. д.), не приводящим к потере переключательных свойств активных компонентов (в современной технологии комплементарный металл–диэлектрик–полупроводник (**КМДП**) — транзисторов) [1]. В комбинационной схеме сбой сам собой исчезает со временем за счет рассасывания индуцированного избыточного заряда под действием драйверов внутренних сигналов. Но в схемах с памятью сбой может привести к инверсии хранимого бита информации и может быть исправлен только перезаписью памяти.

Отказом считается изменение функции, выполняемой элементом, вследствие выхода из строя одного или нескольких транзисторов [1] из–за высокоэнергичного электромагнитного импульса, пролета ядерной частицы или накопления дозы радиации в процессе работы схемы. Устранение отказа возможно только путем замены неисправного логического элемента или функционального блока аналогичным работоспособным компонентом.

Наиболее распространенная причина сбоев и отказов в микроэлектронике — пролет ядерных частиц через тело микросхемы [2–3]. При этом область поражения определяется эффективным диаметром трека частицы, углом падения частицы на поверхность микросхемы и пробегом частицы в объеме кристалла микросхемы. Диаметр трека и длина пробега определяются энергией частицы и величиной линейной передачи энергии (**ЛПЭ**), которая зависит от материала кристалла микросхемы. Величина ЛПЭ, приводящая к сбою, падает с уменьшением технологических норм: от нескольких десятков  $\text{МэВ}\cdot\text{см}^2/\text{мг}$  для микронных норм до единиц  $\text{МэВ}\cdot\text{см}^2/\text{мг}$  для глубокого субмикрона [4].

Парирование отказа в синхронных схемах обеспечивается с помощью сбоеустойчивых кодов [5],

эффективных лишь при небольших интенсивностях сбоев, или одновременной обработки входных данных несколькими параллельными идентичными устройствами с последующим вотированием правильного результата [6].

Вотирование обеспечивает надежное маскирование любого количества сбоев или отказов, возникших в минорном подмножестве параллельных каналов. Обычно применяется принцип «два из трех» [6], который гарантирует надежную работу схемы в условиях, когда в каждый момент времени наблюдается не более одного логического сбоя. При большей плотности потока сбоев существует вероятность одновременных сбоев в мажорном числе каналов, ведущих к критической ошибке. Кроме того, остается проблема сбоя в схеме вотирования.

Безусловным преимуществом схемы с вотированием является принятие решения «на лету» и продолжение корректной работы при однократном логическом сбое или отказе в любом канале. Она также обеспечивает защиту от любого числа отказов в одном канале.

Самосинхронные (**СС**) цифровые схемы обладают более высокой естественной устойчивостью к логическим сбоям [7–8], чем их синхронные аналоги, благодаря изначальной аппаратной избыточности, двухфазному режиму работы и индицированию завершения переключения схемы в каждую текущую фазу. Они детектируют любой отказ (константную неисправность) и останавливают свое функционирование в этом случае. Благодаря этому **СС**–схемы, построенные по методу вотирования, даже при множественном сбое, поразившем мажорное число параллельных каналов одновременно, способны продолжить штатную работу по окончании сбоя без потери данных. Синхронная же схема в такой ситуации исчерпает свои резервы и выдаст диагностику о наличии неисправимой ошибки. Тройирование **СС**–схемы обеспечивает уровень защиты от логических сбоев и отказов не хуже, чем синхронные схемы. Но аппаратные затраты при этом тоже утраиваются и становятся еще более избыточными.

В то же время, существуют более экономичные способы построения отказоустойчивых **СС**–схем. Данная статья посвящена исследованию возможностей и способов построения отказоустойчивых **СС**–схем.

---

Статья подготовлена по материалам доклада, представленного на VI–й международной конференции «Математическое моделирование в материаловедении электронных компонентов», Москва, 24–26 октября 2022 г.

© 2022 National University of Science and Technology MISiS.

This is an open access article distributed under the terms of the Creative Commons Attribution License (CC-BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

---

### Детектирование отказа в СС–схеме

СС–схемы используют избыточное кодирование информации. Наиболее распространенным является парафазное кодирование, при котором каждый информационный сигнал  $X$  представляется парой связанных сигналов  $\{X, XB\}$ , имеющей одно спейсерное состояние («00» — нулевой спейсер или «11» — единичный спейсер) и два рабочих состояния («01» и «10»). Четвертое состояние, противоположное спейсеру (антиспейсер), является запрещенным. Но оно может появиться в результате логического сбоя или отказа. Работа СС–схемы представляет собой последовательное строгое чередование рабочей и спейсерной фаз.

Окончание переключения СС–схемы в очередную фазу подтверждается индикаторной подсхемой. Переключение индикаторного выхода в рабочее (спейсерное) значение разрешает предыдущей СС–схеме начать переключение в спейсерную (рабочую) фазу. Ортогональность подмножеств рабочих и спейсерных состояний СС–схемы облегчает индикацию и обеспечивает обнаружение константных неисправностей (отказов). Отказ в СС–схеме означает «залипание» парафазного сигнала в фиксированном значении. «Залипание» в спейсерном значении обнаруживается при индикации рабочей фазы, а «залипание» в рабочем значении индицируется в спейсерной фазе.

Таблица 1 показывает возможные сбои парафазного сигнала с нулевым спейсером. Строки 1, 4 и 7 отображают появление антиспейсера. Строки 5 и 8 иллюстрируют сбойное переключение парафазного сигнала в противоположное рабочее состояние, когда обе компоненты парафазного сигнала переключаются в противоположное значение. Теоретически это возможно, если источник сбоя поразил выходы обеих ячеек, формирующих парафазный сигнал. Однако, на практике для случаев пролета одиночной ядерной частицы эти ситуации можно предотвратить. Достаточно в топологии кристалла разнести соответствующие ячейки на расстояние, превышающее максимальный ожидаемый (вероятный) эффективный диаметр трека ядерной частицы, который в условиях ближнего космоса и наземного базирования оценивается как 2,0—2,5 мкм [9], и длину ее пробега в теле полупроводника. Тогда сбой может произойти только в одной компоненте парафазного сигнала.

Основным преимуществом действительно СС–схем является функциональная корректность их работы при любых задержках формирования и распространения внутренних и выходных сигналов. Это означает, что быстроедействие СС–схемы всегда соответствует текущим условиям окружающей среды, поскольку оно определяется причинно–следственными отношениям, а не глобальным

тактовым сигналом. Уменьшение напряжения питания и/или повышение окружающей температуры замедляет работу СС–схемы, но не нарушает корректности выполняемого ею алгоритма обработки данных. СС–схемы свободны от любых «гонок» сигналов. С одной стороны, это свойство является безусловным преимуществом СС–схем. С другой стороны, оно затрудняет задачу обнаружения отказа, так как задержки срабатывания элементов и схемы оказываются не регламентированными.

### Варианты отказоустойчивых СС–схем

Самый простой способ построения отказоустойчивой СС–схемы – дублирование [10], при котором два идентичных канала обрабатывают одинаковые наборы входных данных. Решение о работоспособности каналов принимается на основе сравнения информационных и индикаторных выходов.

Выбор корректного результата из двух информационных на основе только индикаторного выхода не годится, так как индикатор может сработать преждевременно из–за сбоя или отказа в самой индикаторной подсхеме. Кроме того, отказ может появиться после успешной индикации завершения переключения сбойного парафазного сигнала.

Решение о выборе корректного результата в дублированной схеме неизбежно основывается на допущениях о времени появления сбоя и предшествующих ему условиях. Кроме того, какие бы ни были способы решения задачи обеспечения отказоустойчивости, всегда будет существовать проблема «последней мили»: если отказ произойдет в последнем каскаде схемы сравнения и контроля, то

Таблица 1

**Сбойные состояния парафазного сигнала с нулевым спейсером**  
[Failure states of the dual–rail signal with zero spacer]

№	Исходное состояние		Сбойное состояние		Фаза обнаружения
	X	XB	X'	XB'	
1	0	0	1	1	Рабочая
2	0	0	1	0	Спейсерная
3	0	0	0	1	Спейсерная
4	0	1	1	1	Рабочая
5	0	1	1	0	Спейсерная
6	0	1	0	0	Рабочая
7	1	0	1	1	Рабочая
8	1	0	0	1	Спейсерная
9	1	0	0	0	Рабочая

он окажется не обнаруженным. Поэтому можно говорить только о степени защищенности от отказов.

Дублированная СС–схема обладает следующими свойствами:

- обеспечивает контроль работоспособности обоих каналов,
- гарантирует детектирование не более двух отказов,
- парирует первый отказ в любом из дублированных каналов,
- останавливает обработку данных при выявлении второго отказа.

Средства обеспечения сбое- и отказоустойчивости могут быть *пассивными* или *активными*. В *пассивном* варианте схема просто ждет, пока информационные и индикаторные выходы обеих половин совпадут, т.е. когда сбой сам собой закончится, в предположении, что это сбой, а не отказ. В *активном* варианте нужно быстро (в течение одного рабочего цикла) локализовать неисправность и замаскировать ее или заменить отказавший фрагмент СС–схемы.

Борьба с отказами не может быть полностью пассивной, т.к. отказ сам собой не исправится. Но на первом этапе выявления сбоя ждать какое-то время необходимо, чтобы классифицировать неисправность (константная или нет) и принять правильное решение: продолжить или ремонтировать. Здесь требуются счетчики–таймеры, определяющие ожидаемую для данной СС–схемы и данной технологии максимальную суммарную длительность рабочей и спейсерной фазы в наихудшем случае. Использование таймера нарушает концептуальный принцип «независимости от задержек». Таймер накладывает ограничение на задержки элементов, но в разумных пределах.

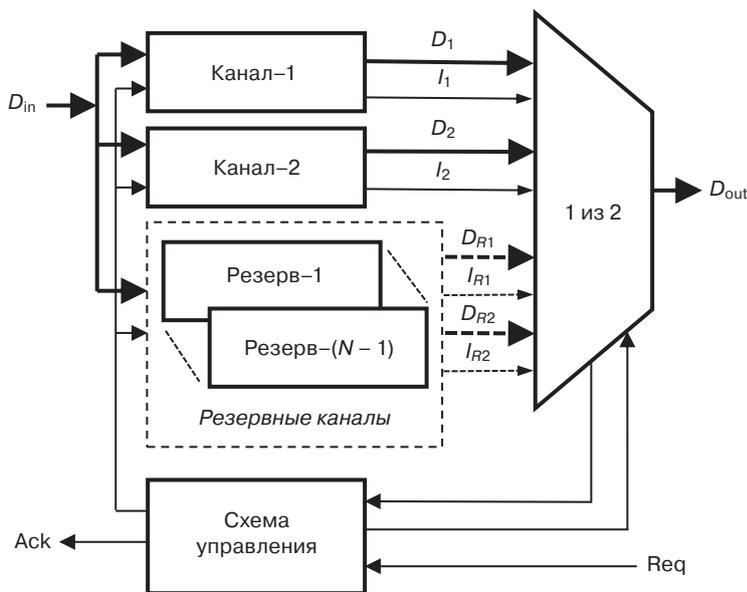


Рис. 1. СС–схема, устойчивая к  $N$  отказам  
Fig. 1. ST circuit resistant to  $N$  failures

Сбой, проявляющийся как «зависание» одного из индикаторных выходов, вызывает ожидание, отсчитываемое таймером в схеме управления. По окончании ожидания на выход схемы мультиплексируется выход того канала, чей индикаторный выход переключился в правильное значение.

Сбой, проявляющийся как несовпадение информационных выходов в рабочей фазе при правильном переключении индикаторов, требует дополнительной проверки состояний информационных выходов по окончании времени работы таймера. Корректным будет тот результат, который не содержит спейсерных и антиспейсерных состояний в рабочей фазе или рабочих состояний в спейсерной фазе. Он и мультиплексируется на выход схемы.

Пусть значение логического нуля индикаторного сигнала отражает спейсерное или антиспейсерное состояние индицируемого парафазного сигнала, а значение логической единицы — его рабочее состояние. Тогда для проверки наличия спейсерных и антиспейсерных состояний в составе информационного выхода в рабочей фазе достаточно объединить его поразрядные индикаторы простой схемой логического «И» (функция WI). Для проверки наличия рабочих состояний в составе информационного выхода в спейсерной фазе достаточно объединить его поразрядные индикаторы простой схемой логического «ИЛИ» (функция SI). Признаком наличия отказа в состоянии информационного выхода — единичное значение функции  $F_{S0}$ :

$$F_{S0} = (\overline{SP} \wedge \overline{WI}) \vee (SP \wedge SI),$$

где SP — признак текущей спейсерной ( $SP = 1$ ) или рабочей ( $SP = 0$ ) фазы.

Для обеспечения устойчивости к  $N$  последовательным отказам, каждый из которых воспринимается и детектируется как однократный отказ, простую дублированную схему нужно дополнить  $(N - 1)$  резервными каналами (рис. 1). Обнаружение первых  $(N - 1)$  отказов запускает процесс замещения сбойного канала идентичным резервным. Последний  $N$ -й отказ вынуждает схему управления оставить один работающий канал.

Сигналы  $D_{R1}$ ,  $D_{R2}$  (информационные выходы задействованных резервных каналов) и  $I_{R1}$ ,  $I_{R2}$  (индикаторные выходы задействованных резервных каналов) замещают собой сигналы  $D_1$ ,  $D_2$ ,  $I_1$ ,  $I_2$  в выходной схеме выбора рабочего канала по мере необходимости.

Схема управления на рис. 1 включает в себя таймер ожидания окончания гарант–интервала, длительность которого

соответствует времени гарантированного переключения СС-схемы в рабочую и в спейсерную фазу в наихудших условиях при наличии входных сигналов, разрешающих такое переключение, и превышает максимальное время самоликвидации логического сбоя в предполагаемых условиях эксплуатации.

### Таймер ожидания

Таймер ожидания переключения СС-схемы в текущую фазу идеологически может быть реализован различными способами как СС-схема, работающая в режиме автономного замыкания с СС-сбросом.

Аппаратные затраты в схеме на рис. 1 складываются из аппаратных затрат  $(N + 1)$  рабочих и резервных каналов, схемы управления, включающей таймер ожидания, и выходной схемы сравнения и выбора. В первом приближении можно считать, что схема управления и выходная схема сравнения и выбора в совокупности имеют сложность, сравнимую со сложностью одного канала обработки данных. Тогда общую сложность отказоустойчивой СС-схемы можно оценить как  $A_{C,ST}(N + 2)$ , где  $A_{C,ST}$  — сложность одного СС-канала обработки данных.

Синхронная схема, обеспечивающая защиту от  $N$  однократных отказов, может быть реализована в двух вариантах:

- 1) схемой вотирования « $(N + 1)$ -из- $(2N + 1)$ » — вариант С-1,
- 2) схемой вотирования «2-из-3» с  $(N - 1)$  резервными каналами и блоком адаптивной коммутации резервных каналов, представляющим собой синхронный вариант схемы управления на рис. 1 — вариант С-2.

Аппаратные затраты первого варианта в первом приближении можно оценить как  $A_{C,S}(2N + 2)$ , где  $A_{C,S}$  — сложность одного синхронного канала обработки данных, а сложность второго варианта — как  $A_{C,S}(N + 4)$ .

Сравнение аппаратных затрат на реализацию вариантов отказоустойчивых синхронных и

СС-схем показано на рис. 2. Аппаратные затраты всех вариантов приведены к аппаратным затратам первого синхронного варианта С-1.

Здесь учтено соотношение аппаратных затрат СС и синхронных реализаций типовых цифровых схем — конвейеров обработки данных: СС-конвейер оказывается сложнее синхронного аналога примерно в 2,4 раза, т.е.  $A_{C,ST}/A_{C,S} = 2,4$ .

Из диаграммы видно, что при увеличении степени защищенности, т.е. числа отказов, парируемых отказоустойчивой схемой, ее СС-реализация становится менее избыточной в сравнении с традиционным синхронным решением. Вместе с тем, устойчивость СС-реализации к множественным логическим сбоям остается выше в несколько раз [10], чем у обоих синхронных аналогов, если сбои происходят одновременно в нескольких каналах. В совокупности с другими преимуществами СС-схем в сравнении с синхронными аналогами (независимость работоспособности от актуальных задержек элементов и от условий эксплуатации) это делает СС-схемы привлекательным базисом для реализации сбое- и отказоустойчивых цифровых устройств.

### Заключение

1. Вотированные синхронные схемы ( $N$ -из- $M$ ) обеспечивают защиту не от всех видов сбоев и отказов. Например, часто повторяющиеся одиночные сбои и множественные одновременные сбои маскируются не гарантированно.
2. Топологические методы способны сократить число типов сбоев в СС-схемах. В частности, сделать нереализуемыми сбой типа «переключение парафазного сигнала из корректного рабочего состояния в инверсное рабочее состояние».
3. Дублированная СС-схема обладает устойчивостью к множественным логическим сбоям и однократным отказам, но при этом необходим таймер, работающий от внешнего синхросигнала.
4. При увеличении степени защищенности, т.е. числа отказов, парируемых отказоустойчивой

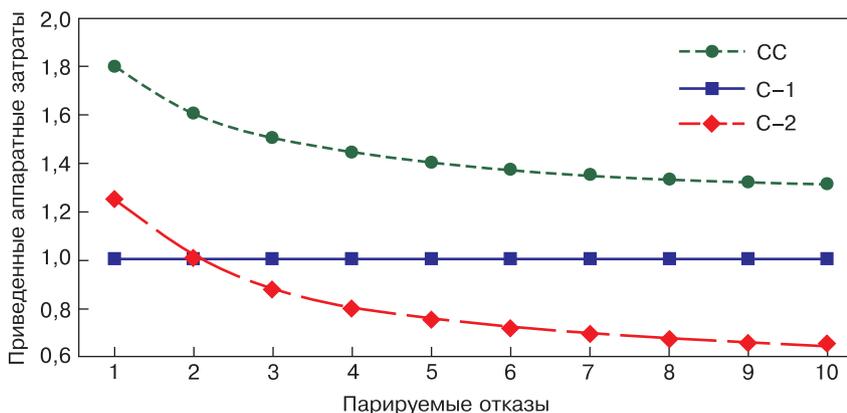


Рис. 2. Сравнение отношений аппаратных затрат СС-варианта (СС) и двух синхронных вариантов (С-1 и С-2) цифровой схемы  
Fig. 2. Comparison of the ratios of hardware costs of the ST-case (CC) and two synchronous variants (C-1 and C-2) of the digital circuit

схемой, ее СС–реализация становится менее избыточной в сравнении с традиционным синхронным решением.

### Библиографический список

1. Викторова В.С., Лубков Н.В., Степанянц А.С. Анализ надежности отказоустойчивых управляющих вычислительных систем. М.: ИПУ РАН; 2016. 117 с. [https://www.ipu.ru/sites/default/files/card\\_file/VLS.pdf](https://www.ipu.ru/sites/default/files/card_file/VLS.pdf) (дата обращения: 08.08.2022).
2. Байков В.Д., Герасимов Ю.М., Петричкович Я.Я., Раннев Н.Ю. Повышение сбоеустойчивости КМОП СФ–блоков смешанного сигнала. *Наноиндустрия*. 2021; 14(S7(107)): 368—369. <https://doi.org/10.22184/1993-8578.2021.14.7s.368.369>
3. Hasegawa M., Mori S., Ohsugi T., Kojima H., Taketani A., Kondo T., Noguchi M. Radiation damage at silicon junction by neutron irradiation. *Nuclear Instruments and Methods in Physics Research*. 1989; (A277): 395—400. [https://doi.org/10.1016/0168-9002\(89\)90768-7](https://doi.org/10.1016/0168-9002(89)90768-7)
4. Бондарь О.Г. Проектирование радиационно–устойчивых электронных средств: методические указания к практическим занятиям. Курск: Юго–Зап. гос. ун–т; 2018. 52 с. [https://swsu.ru/sveden/files/MU\\_Proektirovanie\\_radiacionno-ustoychivyx\\_elektronnyx\\_sredstv\\_PZ.pdf](https://swsu.ru/sveden/files/MU_Proektirovanie_radiacionno-ustoychivyx_elektronnyx_sredstv_PZ.pdf)
5. Шавенько Н.К. Основы теории информации и кодирования. М.: Изд–во МИИГАиК; 2012. 125 с. <https://miigaik.ru/vtiaoi/tutorials/10.pdf>
6. Song W., Zhang G. Fault–tolerant asynchronous circuits. In: *Asynchronous On–Chip Networks and Fault–Tolerant Techniques*. Boca Raton: CRC Press; 2022. 380 p. <https://doi.org/10.1201/9781003284789-5>
7. Zakharov V., Stepchenko Y., Diachenko Y., Rogdestvenski Y. Self–timed circuitry retrospective. *Inter. conf. engineering and computer science (EnT 2020)*. Moscow, June 24–27, 2020. IEEE; P. 58—64. <https://doi.org/0.1109/EnT48576.2020.00018>
8. Stepchenko Y.A., Kamenskih A.N., Diachenko Y.G., Rogdestvenski Y.V., Diachenko D.Y. Improvement of the natural self–timed circuit tolerance to short–term soft errors. *Advances in Science, Technology and Engineering Systems Journal*. 2020; 5(2): 44—56. <https://doi.org/10.25046/aj050206>
9. Emel'yanov V.V., Vatiev A.S., Useinov R.G. Impact of heavy ion energy on charge yield in silicon dioxide. *IEEE Transactions on Nuclear Science*. 2018; 65(8): 1496—1502. <https://doi.org/10.1109/TNS.2018.2813669>
10. Зацаринный А.А., Степченко Ю.А., Дьяченко Ю.Г., Рождественский Ю.В. Сравнение сбоеустойчивых синхронных и самосинхронных схем. В сб.: *Матер. III Междунар. конф. «Математическое моделирование в материаловедении электронных компонентов»*

(MMMЭК–2021). 25–27 октября 2021 г., Москва. М.: МАКС Пресс; 2021. С. 154—156. <https://doi.org/10.29003/m2498.MMMSEC-2021/154-156>

### References

1. Viktorova V.C., Lubkov N.V., Stepanyants A.S. Reliability analysis of fault–tolerant control computing systems. Moscow: IPU RAN; 2016. 117 p. (In Russ.). [https://www.ipu.ru/sites/default/files/card\\_file/VLS.pdf](https://www.ipu.ru/sites/default/files/card_file/VLS.pdf) (accessed: 08.08.2022).
2. Baikov V.D., Gerasimov Yu.M., Petrichkovich Ya.Ya., Rannev N.Yu. Increasing the fault tolerance of CMOS mixed signal IP–modules. *Nanoindustry*. 2021; 14(S7(107)): 368—369. (In Russ.). <https://doi.org/10.22184/1993-8578.2021.14.7s.368.369>
3. Hasegawa M., Mori S., Ohsugi T., Kojima H., Taketani A., Kondo T., Noguchi M. Radiation damage at silicon junction by neutron irradiation. *Nuclear Instruments and Methods in Physics Research*. 1989; (A277): 395—400. [https://doi.org/10.1016/0168-9002\(89\)90768-7](https://doi.org/10.1016/0168-9002(89)90768-7)
4. Bondar' O.G. Designing radiation–resistant electronic devices: guidelines for practical classes. Kursk: Yugo–Zap. gos. un–t; 2018. 52 p. (In Russ.)
5. Shaven'ko N.K. Fundamentals of information theory and coding. Moscow: Izd–vo MIIGAiK; 2012. 125 p. (In Russ.). <https://miigaik.ru/vtiaoi/tutorials/10.pdf>
6. Song W., Zhang G. Fault–tolerant asynchronous circuits. In: *Asynchronous On–Chip Networks and Fault–Tolerant Techniques*. Boca Raton: CRC Press; 2022. 380 p. <https://doi.org/10.1201/9781003284789-5>
7. Zakharov V., Stepchenko Y., Diachenko Y., Rogdestvenski Y. Self–timed circuitry retrospective. *Inter. conf. engineering and computer science (EnT 2020)*. Moscow, June 24–27, 2020. IEEE; P. 58—64. <https://doi.org/0.1109/EnT48576.2020.00018>
8. Stepchenko Y.A., Kamenskih A.N., Diachenko Y.G., Rogdestvenski Y.V., Diachenko D.Y. Improvement of the natural self–timed circuit tolerance to short–term soft errors. *Advances in Science, Technology and Engineering Systems Journal*. 2020; 5(2): 44—56. <https://doi.org/10.25046/aj050206>
9. Emel'yanov V.V., Vatiev A.S., Useinov R.G. Impact of heavy ion energy on charge yield in silicon dioxide. *IEEE Transactions on Nuclear Science*. 2018; 65(8): 1496—1502. <https://doi.org/10.1109/TNS.2018.2813669>
10. Zatsarinnyi A.A., Stepchenko Yu.A., D'yachenko Yu.G., Rozhdestvenskii Yu.V. Comparison of fault–tolerant synchronous and self–synchronous circuits. In: *Proceed. of the Inter. conf. «Mathematical modeling in materials science of electronic components» (ICM3SEC–2021)*. October 25–27, 2021, Moscow. Moscow: MAKS Press; 2021. P. 154—156. (In Russ.). <https://doi.org/10.29003/m2498.MMMSEC-2021/154-156>

### Информация об авторах / Information about the authors

**Зацаринный Александр Алексеевич** — доктор техн. наук, главный научный сотрудник, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, ул. Вавилова, д. 44, корп. 2, Москва, 119333, Российская Федерация; <https://orcid.org/0000-0002-8872-2774>; e–mail: AZatsarinny@ipiran.ru

**Alexander A. Zatsarinny** — Dr. Sci. (Eng.), Chief Researcher, Federal Research Center «Computer Science and Control» of the Russian Academy of Sciences, 44–2 Vavilova Str., Moscow 119333, Russian Federation; <https://orcid.org/0000-0002-8872-2774>; e–mail: AZatsarinny@ipiran.ru

**Степченко Юрий Афанасьевич** — канд. техн. наук, руководитель отдела, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, ул. Вавилова, д. 44, корп. 2, Москва, 119333, Российская Федерация; <https://orcid.org/0000-0003-4784-7519>; e-mail: YStepchenkov@ipiran.ru

**Дьяченко Юрий Георгиевич** — канд. техн. наук, старший научный сотрудник, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, ул. Вавилова, д. 44, корп. 2, Москва, 119333, Российская Федерация; <https://orcid.org/0000-0003-0212-4931>; e-mail: diaura@mai.ru

**Рождественский Юрий Владимирович** — канд. техн. наук, ведущий научный сотрудник, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, ул. Вавилова, д. 44, корп. 2, Москва, 119333, Российская Федерация; e-mail: YRogdest@ipiran.ru

**Плеханов Леонид Петрович** — канд. техн. наук, старший научный сотрудник, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, ул. Вавилова, д. 44, корп. 2, Москва, 119333, Российская Федерация; e-mail: lplekhanov@inbox.ru

**Yury A. Stepchenko** — Cand. Sci. (Eng.), Head of Department, Federal Research Center «Computer Science and Control» of the Russian Academy of Sciences, 44–2 Vavilova Str., Moscow 119333, Russian Federation; <https://orcid.org/0000-0003-4784-7519>; e-mail: YStepchenkov@ipiran.ru

**Yury G. Diachenko** — Cand. Sci. (Eng.), Senior Researcher, Federal Research Center «Computer Science and Control» of the Russian Academy of Sciences, 44–2 Vavilova Str., Moscow 119333, Russian Federation; <https://orcid.org/0000-0003-0212-4931>; e-mail: diaura@mai.ru

**Yury V. Rogdestvenski** — Cand. Sci. (Eng.), Leading Researcher, Federal Research Center «Computer Science and Control» of the Russian Academy of Sciences, 44–2 Vavilova Str., Moscow 119333, Russian Federation; e-mail: YRogdest@ipiran.ru

**Leonid P. Plekhanov** — Cand. Sci. (Eng.), Senior Researcher, Federal Research Center «Computer Science and Control» of the Russian Academy of Sciences, 44–2 Vavilova Str., Moscow 119333, Russian Federation; e-mail: lplekhanov@inbox.ru

*Поступила в редакцию 29.11.2022; поступила после доработки 13.12.2022; принята к публикации 23.12.2022  
Received 29 November 2022; Revised 13 December 2022; Accepted 23 December 2022*