

Методы повышения стойкости ПЛИС со статическим ОЗУ к воздействию ионизирующего излучения

А. Строгонов, д. т. н.¹, С. Цыбин, к. т. н.², П. Городков³

УДК 621.3.049.774 | ВАК 05.27.01

Проблема сбоев в работе БИС, в частности ПЛИС, в результате ионизирующего излучения становится все более актуальной для разработчиков аппаратуры космического назначения. При непрерывном уменьшении технологических проектных норм ошибки, вызванные излучением, стали оказывать существенное влияние на надежность БИС. Основными источниками одиночных сбоев БИС могут быть как высокоскоростные нейтроны, которые генерируются при столкновении космических лучей с молекулами воздуха в атмосфере Земли, так и вторичные альфа-частицы, испускаемые, например, материалом корпуса ИС. Воздействию высокоэнергетических частиц подвергаются даже БИС, работающие на уровне Земли, что может приводить к отказам радиоэлектронной аппаратуры, используемой повсеместно. Рассмотрим основные аппаратные и программные методы защиты современных ПЛИС со статическим ОЗУ от влияния сбоев, вызванных ионизирующим излучением.

Одиночные события, приводящие к случайным отказам или сбоям (Single Event Effects – SEE), – причина как устранимых, или программных, ошибок (soft error) в работе ПЛИС, так и катастрофических, или постоянных (невосстанавливаемых), отказов (hard error) [1]. По классификации компании Intel к одиночным событиям (SEE) относят одиночные сбои ячеек памяти, что проявляется в обратимом изменении их состояния (Single Event Upset – SEU); одиночные сбои переключения, которые приводят к кратковременному изменению состояния выхода логического элемента (Single Event Transient – SET); и одиночные события радиационного защелкивания, под которыми понимается тиристорный эффект, когда КМОП-транзисторы ПЛИС переходят в состояние с высоким потреблением тока (Single Event Latchup – SEL).

Если не принимать специальных мер для предотвращения одиночных сбоев, они могут приводить к серьезным последствиям, таким как потеря информации, сбои

в функционировании или потеря контроля, например ошибочное исполнение прикладной программы [2]. По мере уменьшения геометрических размеров транзисторов в современных БИС возникает вероятность того, что одна падающая частица будет воздействовать на несколько транзисторов, создавая множественные сбои ячеек в массивах памяти (Multiple Cell Upset – MCU). Если поврежденные биты (бит) принадлежат одному слову памяти, то такие ошибки называют многобитовыми сбоями в логическом слове (Multiple Bit Upset in a Logical Word – MBU). Могут возникать также однобитовые сбои в логическом слове (Single Bit Upset – SBU). MBU особенно критичны, поскольку снижают эффективность применения кодирования с исправлением ошибок (Error Correcting Codes – ECC).

К катастрофическим отказам, вызванным ионизирующим излучением, относят, как правило, отказы двух типов: одиночные пробой подзатворного диэлектрика МОП-транзистора (Single Event Gate Rupture – SEGR) и одиночные пробой сток/истоковых областей МОП-транзистора (Single Event Burnout – SEB) [1, 2].

Основные методы защиты БИС от случайных сбоев, вызванных ионизирующим излучением, рассмотрим на примере ПЛИС со статическим ОЗУ, выпускаемых различными компаниями. Эти устройства содержат матрицу конфигурируемых логических блоков (КЛБ), трассировочные ресурсы, встроенные блоки ОЗУ, блоки цифровой обработки сигнала, набор управляющей и контролирующей логики. КЛБ состоят из таблиц преобразований (LUT), которые реализуют

¹ Воронежский государственный технический университет, профессор кафедры полупроводниковой электроники и нанoeлектроники, тел. +7 (4732) 43-76-95, andreistrogonov@mail.ru.

² АО «Конструкторско-технологический центр «ЭЛЕКТРОНИКА», генеральный директор, тел. +7 (4732) 02-00-22, tsybin@edc-electronics.ru.

³ Воронежский государственный технический университет, аспирант кафедры полупроводниковой электроники и нанoeлектроники, тел. +7 (4732) 43-76-95, gorodkoff@gmail.com.

комбинационную логику, и D-триггеров, отвечающих за последовательностную логику. Структура трассировочных ресурсов может быть очень сложной, насчитывать миллионы предустановленных соединений, которые настраиваются с помощью мультиплексоров и коммутаторов для обеспечения требуемой маршрутизации сигналов.

Конфигурация КЛБ, блоков ОЗУ, ЦОС-блоков, модулей ввода-вывода, а также маршрутизация сигналов задается с помощью битов конфигурационной памяти (СRAM). Например, в САПР Intel Quartus Prime конфигурация проекта хранится в файле с расширением sof, загружаемом в конфигурационную память ПЛИС. С помощью sof-файла происходит настройка логики и маршрутизации [1].

Конфигурационные ячейки памяти, которые хранят битовый поток, или прошивку, ПЛИС, образуют массив статического ОЗУ. Возникновение SEE в конфигурационной памяти ПЛИС на основе статического ОЗУ может спровоцировать инвертирование битов, что станет причиной изменения маршрутизации сигналов, конфигурации LUT или триггера в КЛБ и в результате приведет к изменениям в логике работы. Это может иметь катастрофические последствия для проекта пользователя, поскольку SEE изменяет его функциональность [2].

Следует отметить, что если SEU воздействует на конфигурационный бит памяти, который не используется в проекте, то эффект может быть безвредным. Многие биты конфигурации только управляют логикой конфигурирования и маршрутизацией сигналов в ПЛИС. Как правило, в проекте используется до 40% всех битов СRAM. Это означает, что только эти биты можно рассматривать как критичные, восприимчивые к сбоям [1].

Установлено, что нормированная чувствительность к сбоям конфигурационной памяти софт-процессора MicroBlaze компании Xilinx на 26% выше, чем у процессора LEON3 компании Aeroflex Gaisler. Более высокая восприимчивость к SEU процессора MicroBlaze по сравнению с процессором LEON3 объясняется особенностями синтеза этих устройств. В процессоре MicroBlaze в качестве базовых элементов используются LUTRAM и SRL, процессор LEON3 преимущественно архитектурно не зависит от ПЛИС, за исключением базовых элементов, которые применяются для организации блоков ввода-вывода, устройств управления синхронизацией и памятью. LEON3 использует большее количество синтезируемой логики, чем MicroBlaze, что приводит к меньшей функциональной плотности и, как следствие, к меньшей чувствительности к сбоям [2].

Конфигурационную память ПЛИС можно защитить от SEU с помощью очистки и/или методами обнаружения и исправления ошибок (Error Detection and Correction – EDAC) [2, 4]. Очистка конфигурационных ячеек – важный элемент любой высоконадежной системы на основе ПЛИС, используемой в агрессивной радиационной среде. Очистка предусматривает периодическую запись

конфигурационных данных в ПЛИС для устранения сбоев в ячейках памяти. Для этого требуются внешнее запоминающее устройство и аппаратные средства для управления процессом очистки.

В ПЛИС со статическим ОЗУ также нужно предусмотреть защиту от SEU триггеров КЛБ (регистров пользователя) для реализации последовательностной логики (например, конечных автоматов) и блоков памяти ОЗУ, применяемых в проектах пользователя. Наиболее распространенный метод защиты памяти пользователя в проектах – тройное модульное резервирование (TMR), которое сводится к утраиванию ресурсов проекта и применению схем голосования для получения корректного результата. TMR обеспечивает защиту от всех однобитовых и некоторого числа многобитовых ошибок. Различают локальный вариант TMR, когда применяется тройное дублирование только триггеров; и глобальный TMR, также известный как XTMR, когда три раза дублируется вся комбинационная и последовательностная логика. Возможно также использование различного тройного модульного резервирования (Diverse TMR), в этом случае каждый дублирующий модуль отличается от остальных архитектурой [2].

Недостаток TMR – увеличение аппаратных ресурсов и, следовательно, повышение стоимости оборудования. Минимизировать стоимость можно путем использования TMR только для наиболее важных частей проекта [2]. Тем не менее считается, что ошибки в конфигурационной памяти ПЛИС (уровень конфигурации), вызванные SEE, значительно более вероятны, чем ошибки в регистрах пользователя (уровень приложений) [4].

В настоящее время многие зарубежные компании выпускают радиационно-стойкие ПЛИС, например, Virtex-5QV от Xilinx с конфигурационными ячейками памяти на статическом ОЗУ или структурированные ПЛИС серии RT ProASIC3 от Microsemi с ячейками на основе флеш-памяти, а также ПЛИС серии RTAX с токопроводящими перемычками (antifuse). ПЛИС Virtex-5QV обеспечивают высокий уровень защиты от SEU, SET, MBU, защелкиваний (SEL), выдерживают высокие дозы ионизирующего излучения (TID) [2].

ООО
СМП



ИНТЕРНЕТ-МАГАЗИН
www.SMD.ru

электронные **КОМПОНЕНТЫ**

для поверхностного

монтажа

НОВОЕ В ПРОГРАММЕ ПОСТАВОК

- Микромощный ТСХО генератор на 32.768КГц
- Мосты на диодах Шоттки TS140S и TS240S



Москва, Ленинградский пр., 80 к. 32. e-mail: sale@smd.ru
 Тел.: (499) 158-7396, (495) 943-6234, (499) 943-8780

Устойчивость к одиночным сбоям в радиационно-стойких ПЛИС обеспечивается специальными схемотехническими методами проектирования (Rad-Hard by Design – RHBD) и особыми технологическими приемами (Rad-Hard by Process – RHBP). RHBD предполагает использование тройного модульного резервирования (TMR) конфигурации и управляющей логики JTAG-интерфейса, двойных триггеров в конфигурационных ячейках памяти, двойных триггеров-защелок и SET-фильтров на всех входах триггеров конфигурируемых логических блоков, встроенных схем обнаружения и исправления ошибок в блочной памяти (ECC, SECDED – код с исправлением одиночных и обнаружением двойных ошибок).

Для поддержки радиационно-стойких ПЛИС компания Xilinx разработала программно-аппаратную платформу (XRTC Virtex-5) для оценки устойчивости конфигурационных ячеек памяти ПЛИС с soft-процессорами к SEU и SET методом ввода ошибок (Fault Injector) [2].

Следует отметить, что радиационно-стойкие ПЛИС по своим функциональным возможностям уступают коммерческим (COTS) БИС, таким как ПЛИС класса «система-на-кристалле» серии Zynq-7000 компании Xilinx. Поэтому в последние годы в РЭА с длительным сроком активного использования широко применяются доступные в свободной продаже коммерческие ПЛИС, что позволяет создавать инновационные решения, которые отличаются невысокой стоимостью. Однако нужно учитывать, что коммерческие ПЛИС не разрабатывались специально для обеспечения стойкости к воздействию радиации [2].

Большая часть ПЛИС компании Xilinx поддерживает частичную динамическую реконфигурацию (DPR), которая выполняется во время работы системы через внутренний порт доступа к конфигурационным ячейкам (ICAP).

DPR часто используется в различных интеллектуальных системах, в частности в аэрокосмической промышленности, для изменения их функциональности и локализации сбоев [2]. Динамическая частичная реконфигурация выполняется с применением встроенного soft-ядра процессора, такого как MicroBlaze, или аппаратного процессора с жесткой системой команд, например PowerPC для управления ICAP [2].

Примером высокотехнологичных коммерческих (COTS) ПЛИС служат устройства серий Cyclone 10 и Stratix 10 от Intel, которые изготавливаются по 14-нм технологическому процессу Tri-Gate (FinFET). Они содержат два или четыре процессорных ядра (ARM Cortex-A9 или ARM Cortex-A53), конфигурируемые блоки встроенной памяти M20K, аппаратные ЦОС-блоки с переменной точностью для вычислений с плавающей точкой, аппаратные IP-блоки (высокоскоростные трансиверы, контроллеры внешней памяти, контроллеры PCI Express Gen1-3), а также аналоговые блоки (Cyclone 10). Блоки памяти M20K и eSRAM-блоки поддерживают коды коррекции ошибок (ECC). Для блока M20K применение ECC позволяет исправлять для 32-разрядного слова не только одиночные, но и две-три смежные ошибки [5].

Специальная встроенная схема ПЛИС Intel Stratix 10 дает возможность обнаружить и исправить в конфигурационной памяти одиночную или две смежные ошибки, обнаружить до восьми ошибок типа MBU, если они объединяются в прямоугольную область размерами 8×1, 1×8, 4×2 или 2×4 [5].

САПР Intel Quartus Prime предлагает программное ядро для обнаружения и исправления последствий SEU (Advanced SEU Detection IP core), а также позволяет оценить влияние воздействия SEU на проекты пользователя, реализуемые в базе ПЛИС (рис. 1). Данная стратегия

получила название On-Chip Lookup Sensitivity Processing. Для исправления последствий SEU можно также подключить внешний микропроцессор, который для поиска месторасположения ошибки использует очередь сообщений об ошибках (Off-Chip Lookup Sensitivity Processing) [5].

В очереди сообщений об ошибках ПЛИС Stratix 10 хранятся сообщения об обнаруженных ошибках SEU – максимум четыре сообщения. Каждое из них содержит информацию об их количестве в очереди, адресе сектора, типе и месторасположении ошибки. Содержимое очереди сообщений об ошибках можно получить с использованием инструментов модуля ввода ошибок (Fault Injection Debugger) либо программного IP-ядра Advanced

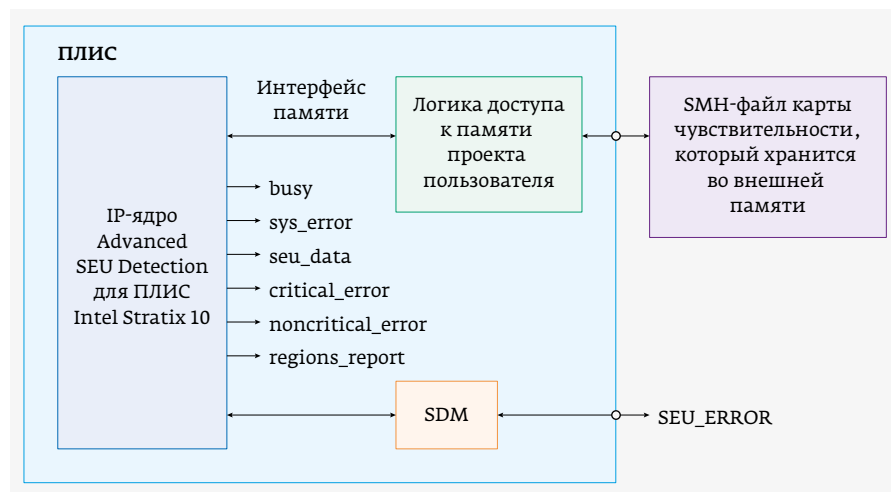


Рис. 1. Использование IP-ядра Advanced SEU Detection для ПЛИС Intel Stratix 10 с целью обнаружения и исправления последствий SEU с применением стратегии On-Chip Lookup Sensitivity Processing

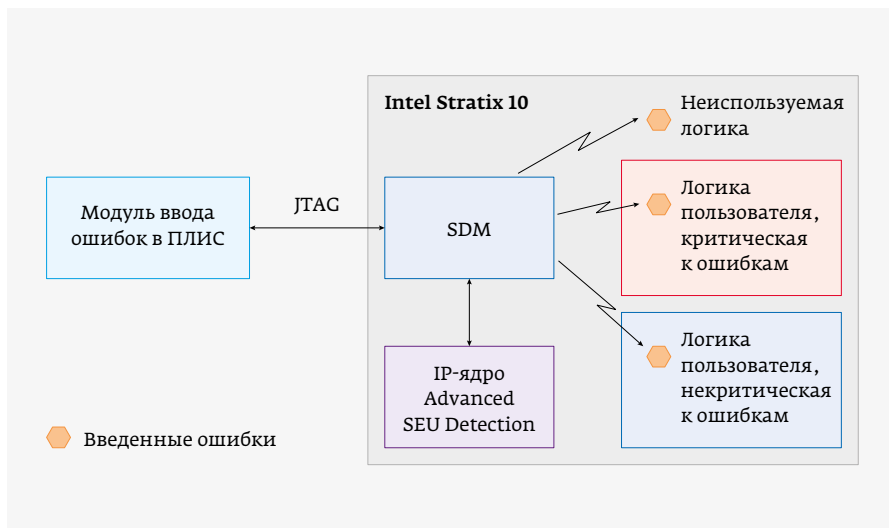


Рис. 2. Специальный модуль для ввода ошибок в СРАМ с целью выявления критической и некритической логики проекта пользователя к SEU посредством JTAG-интерфейса

SEU Detection IP core. SMN-файл карты чувствительности содержит, в частности, хэш настроек битов СРАМ проекта и сохраняется во внешнюю память.

IP-ядро работает совместно с менеджером Secure Device Manager (SDM) для обнаружения SEU, отправки или получения команды или ответа от SDM в случае обнаружения ошибки SEU. Совместное использование менеджера SDM и модуля ввода ошибок в конфигурационную память (Fault Injection Debugger) посредством JTAG-интерфейса в САПР Intel Quartus Prime позволяет выявить критические биты СРАМ, изменение которых приводит к сбоям в логике проекта пользователя (рис. 2). С помощью САПР Intel Quartus Prime можно также отследить, как ПЛИС, работающая в составе системы, будет обнаруживать и исправлять сбои SEU. Ввод ошибок осуществляется случайным образом, при этом можно задать месторасположение ошибки – случайное или в указанной области (ASD Region). Для внесения сбоев в указанную область необходимо сгенерировать SMN-файл [5].

ЗАКЛЮЧЕНИЕ

Практически все современные ПЛИС со статическим ОЗУ ведущих производителей (Intel Altera, Xilinx) содержат внутренние аппаратные средства защиты конфигурационной памяти от последствий SEU. Кроме того, обнаруживать и исправлять последствия SEU помогают реализованные в САПР программные функции, например программное ядро Advanced SEU Detection IP core в САПР Intel Quartus Prime для проектов на базе ПЛИС серии Stratix 10.

Для ПЛИС, начиная с серий Virtex-6, Spartan-6 и Spartan-7, компания Xilinx разработала IP-ядро для устранения сбоев SEU – SEM-контроллер. IP-ядро применяется вместе

с проектами пользователя и использует внутренний порт доступа к конфигурации (ICAP) для обнаружения, исправления и определения типа устранимых ошибок в конфигурационной памяти ПЛИС. Для более эффективной реконфигурации можно применять IP-ядро управления процессом частичной динамической реконфигурации ПЛИС (DPRM – DPR Manager core IP).

Для защиты от SEU регистров пользователя подходит тройное модульное резервирование (TMR). Некоторые компании, такие как Synopsys и Xilinx, предоставляют автоматизированные способы создания TMR-проектов, при этом автоматически тиражируются назначенные функции и синтезируется необходимая логика голосования.

ЛИТЕРАТУРА

1. WP-01206-1.0. Introduction to Single-Event Upsets. September 2013 Altera Corporation.
2. ПЛИС и параллельные архитектуры для применения в аэрокосмической области. Программные ошибки и отказоустойчивое проектирование / Под ред. Кастеншмидт Ф., Реха П.; пер. с англ. и научная редакция Цыбина С. А, Быстрицкого А. В, Строгонова А. В., Городкова П. С. – М.: ТЕХНОСФЕРА, 2018. 326 с.
3. WP-01207-1.0. Understanding Single Event Functional Interrupts in FPGA Designs. September 2013 Altera Corporation.
4. Application Note 357. Error Detection and Recovery Using CRC in Altera FPGA Devices. July 2008, Version 1.4 Altera Corporation. AN-357-1.4.
5. Intel Stratix 10 SEU Mitigation User Guide. Updated for Intel Quartus Prime Design Suite: 18.0. UG-S10SEU2018.08.07.

Санкт-Петербург, Россия
ул. Матроса Железняка,
д. 57, лит. А, пом. 126-Н
Телефон: 7-812-3259792

Москва, Россия
Лужнецкая набережная, 2/4,
строение 19, офис 119
Телефон: 7-095-7477590

VITAL-IC

Поставки электронных компонентов
широкой номенклатуры
Системы RFID: поставка и консультации

XILINX **Mini-Circuits**
ALTERA