УДК. 629.7.05.017.1:681.5.09:004

А.А. УШАКОВ[1], А.В. ЖЕЛТУХИН[1], В.В. СКЛЯР[2], Б.В. ОСТРОУМОВ[3], В.С. ХАРЧЕНКО[1]

[1] ***Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина***
[2]***Государственный научно-технический центр по ядерной и радиационной безопасности, Украина***
[3] ***НТ СКБ "ПОЛИСВИТ" ГНПП "Объединение Коммунар", Украина***

АНАЛИЗ РИСКОВ ПРОЕКТИРОВАНИЯ И ЭКСПЛУАТАЦИИ ЦИФРОВЫХ СИСТЕМ НА ПЛИС

Рассмотрен опыт применения цифровых систем в аэрокосмической технике и атомной энергетике, построенных на ПЛИС. Дана модель специфических рисков ПЛИС-технологии, включающих риски разработки и верификации проектов и риски схемотехнических решений. Детально представлены результаты анализа рисков схемотехнических решений.

ПЛИС-технолгия, отказоустойчивость, риски технологии проектирования, схемотехнические риски

Введение

Анализ проблем применения ПЛИС в критических приложениях. Наиболее значимыми и масштабными примерами ПЛИС-реализации встроенных систем управления [1] можно назвать вычислитель (High Performance Computer – HPC-I, HPC-II) системы управления австралийского научного спутника FedSat, разработанного совместным исследовательским центром спутниковых систем (Cooperative Research Centre for Satellite Systems), включающим университет Джона Хопкинса и его лабораторию прикладной физики, а также центром космических полетов Goddard NASA.

Другие проекты, разработанные центром, включают систему мониторинга и детектирования катастроф (DDMS) зондирующего спутника, автономную систему навигации спутника (ASNS). На основе ПЛИС была разработана система обработки и выработки курса спутника WIRE, которая выполняла функции стабилизации спутника в трехмерном пространстве и наведения: захват цели, прием блоком электроники контроля курса информации от датчиков, прием блоком вычислительной системы космического корабля информации от датчиков, определение сферических координат, сбор информации о положении звезд, наведение по звездам, обнаружения ухода координат и их коррекции. Последними совместными разработками концерна NASA и лаборатории реактивного топлива (Jet Propulsion Laboratory) стала система управления двигателем исследовательского вездехода Spirit миссии MARS2003, его рулевым управлением, манипуляторами и камерами, а также системы управления ответственными пиротехническими операциями при его спуске и приземлении. Эта же усовершенствованная система управления используется в вездеходе Opportunity следующей исследовательской миссии Марса. Еще одним примером применения технологии стала система приема, обработки сигналов от наземного оборудования и выдачи команд оборудованию гибридного коммерческо-оборонного спутника Optus C1, созданного фирмой Raytheon по заказу Mitsubishi Electric Corporation для военных сил Австралии. ПЛИС получили широкое применение в военных системах управления: радиоэлектронной борьбы, управления запуском и наведением ракет, управления радарами и сонарами (ABRAMS,

ERINTS, LAMPS, PATRIOT, THAADS, AGM–130, HELLFIRE, LANTIRN, SEAWOLF, TOMAHAWK, AIM9-X HARPOON и т.д.); а также в аэрокосмических системах управления (737, 777, APACHE, ARIANE 5, ATF (F-22), A-10, B-52, B-1B, C17A, EUROFIGHTER, F-14, P-3, FEDSAT, F-15, RAFAEL, F-16, HC-130, SKYBRIDGE, F-18, JSF, SPACE SHUTTLE, COMANCHE, F-111, OPTUS, TORNADO). В последнее время опыт создания высоконадежных систем управления на ПЛИС переносится от высокотехнологичной оборонной промышленности к системам управления автомобилем, решающим задачи управления двигателем, обеспечения безопасности, навигации, коммуникации. Примером может стать система управления двигателем, разработанная BMW WilliamsF1, для гоночных автомобилей. К сожалению, отечественные разработки не отличаются большой номенклатурой СОК-реализаций ВСУПЛ. В качестве попыток применения подхода можно привести следующие системы: управления общесамолетным оборудованием самолета Ан-70; противообледенительную, управления двигателем и кондиционирования воздуха самолета Ан-140.

Технология ПЛИС дополняет технологию микропроцессоров и микрокотроллеров. Современные микросхемы реализуются как симбиоз программно настраиваемой микропроцессорной части и цифровой ПЛИС-обвязки. Однако обе технологии имеют как общие, так и свойственные только им источники, причины и механизмы отказов.

Цель статьи – анализ источников и последствий отказов ПЛИС для цифровых систем. Основное внимание уделено отказам элементной базы с учетом возможной области применения.

1. Сущность риск-ориентированного подхода к анализу применения ПЛИС-технологий. Модель (структура) рисков

Целью риск ориентированного анализа является выявление потенциально опасных элементов технологии проектирования цифровых систем на ПЛИС с возможностью дальнейшего их устранения и повышения, таким образом, надежности системы. В дальнейшем при необходимости сравнения элементных баз и выбора наилучшей может быть выделен класс общих рисков.

2. Анализ рисков применения ПЛИС в надежных системах управления

2.1. Риски, связанные с процессами разработки и верификации. Технология проектирования цифровых устройств на ПЛИС сходна с технологией проектирования микропроцессорных драйверов и программных продуктов. Исходными данными проекта является структурное или поведенческое описание устройства на языках описания аппаратуры. Таким образом, возможными источниками дефектов проектирования могут быть как ошибки, вносимые проектировщиком, так и ошибки, вносимые САПР на этапе синтеза проекта. Далее синтезированный список соединений проходит итерационный этап верификации и исправления ошибок посредством тестовых векторов.

Риски нарушения технологии проектирования. **Проблема спецификаций.** Отсутствие четко сформулированного технического задания затрудняет проектирование системы более чем одной командой проектировщиков. В этом случае тестирование используется скорее для проектирования, а не для верификации проекта. В свою очередь необходимо иметь спецификацию и на программу тестирования.

В связи с этим возможность многократного перепрограммирования структуры ПЛИС рассматривается как значительное преимущество, так как стоимость перепроектирования очень высока. Такое перепроектирование сопровождается и проблемой документирования внесенных изменений.

Существуют риски, связанные с **описанием конечного автомата**. При анализе конечных состояний для схемотехнических автоматов

необходимо протестировать все возможные состояния и доказать, что все переходы выполняются должным образом [2]. При этом тест должен включать состояния, отличные от номинальных. При исполнении же части конечного автомата, ответственной за хранение состояния с помощью встроенной памяти, возможен ряд неописанных состояний, которые являются тупиковыми. Обязательно должно быть описано начальное состояние, в которое переводится автомат по включению питания. Отличие стратегии анализа конечных состояний для автоматов на языках описания аппаратуры от предыдущего случая заключается в том, что САПР-системы могут автоматически генерировать описания автоматов [3]. В результате можно столкнуться с рядом проблем: появлением запирающих состояний, непреднамеренным дублированием триггеров, компилированием проекта при нежелательном и специфичном стиле. Кодирование конечных автоматов с помощью языков описания аппаратуры позволяет описать и проверить логику работы, но не раскрывает физику работы. Т.е. конкретное решение в ПЛИС каждого автомата в значительной степени зависит от настроек компилятора, а не от начального описания на языке. Существует набор рисков, связанных с размножением триггеров [2, 4]. Резервирование возможно в том случае, если разговор идет об обеспечении надежности. Размножение же не ограничивается вопросами обеспечения надежности. Это может быть и постановка дополнительных буферных элементов, и разветвление цепи питания, тактирования, и так далее. В случае неустойчивой неисправности и размножения триггеров возможна ситуация, когда к разным частям конечного автомата может передаться различная информация. Существует набор рисков, связанных с детектированием и коррекцией ошибок [2]. Необходимо производить проверку любой комбинационной функции, которая является входной для микросхем памяти. В случае исполнения конечного автомата необходимо контролировать, чтобы комбинационная логика не выдавала переходов в неверные состояния.

Риски, связанные с применением ранее разработанных проектов. Существуют риски, которые являются следствием **несоблюдения правил составления и именования всех элементов**, входящих в проект, и последующей трудностью изменения проекта [2]. Множество САПР-систем в случае наличия неименованной переменной сами выполняют эту операцию. Однако такие проекты трудны для понимания и последующей корректировки. В результате правилом хорошего тона стало именование всех переменных, входящих в проект. Существуют риски, связанные со **значительным изменением проекта при внесении незначительных изменений в исходный код**. Обычно этот эффект наблюдается при изменении настроек синтеза проекта. Для избежания недопонимания в этом вопросе необходимо хранить весь пакет документов проекта и отчетов компиляции.

Риски, связанные с применением инструментальных средств разработки. **Отказы, обусловленные дефектами программных средств.**

Расфазировка синхронизирующих импульсов. Несмотря на довольно богатые функции, предоставляемые системами автоматического проектирования, система не всегда понимает, что от нее желает проектировщик. Оптимизационная фаза компиляции проекта, производимая с функцией обновления информации, определяет, что использование избыточных буферов, иногда применяемых для решения проблемы расфазировки, оставит логику проекта без изменений и займет меньшее число ресурсов [4, 5]. Однако, сам проект все же будет изменен синтезатором САПР и проектировщик не будет знать об этом.

Решением этой проблемы является возможность использования опции сохранения части проекта без изменений.

Описание интерфейсов. Интерфейс блока по стандарту языка VHDL описывается в разделе entity.

Поведение же блока описывается в разделе architecture. Очевидно, что если в разделе интерфейсов описывается сигнал типа Boolean, а в разделе architecture он принимает то или иное значение, то мы все же не знаем, какое значение сигнала соответствует какому уровню [3]. Будучи правильным описанным по стандарту VHDL, сигнал, в зависимости от типа логического синтезатора, может принимать то или иное значение.

Высокоуровневые системы автоматизированного проектирования имеют множество опций настройки типа синтеза.

Тиражирование и временная оптимизация. Современные ПЛИС-микросхемы имеют достаточно сложную и мощную систему трассировки. Выводы одного блока могут быть трассируемы по совершенно разным техникам: использование тиражирования для комбинаторных схем или использование выходных триггеров для последовательных схем. Если такие схемы логически эквивалентны, то электрически – нет [2]. Особенно их реакция будет отличаться при учете внезапных отказов. Системы же проектирования не привносят в проект автоматические средства контроля и диагностирования. Поэтому эффект тиражирования должен быть исключен путем настройки синтезатора.

Описание всех состояний автомата (используемых и не используемых). Один из вариантов создания конечных автоматов – использование триггера для описания одного состояния. Такая цепочка может иметь неиспользуемые и тупиковые наборы [2, 3]. В результате внешнего воздействия возможен переход в эти неиспользуемые состояния. Невозможно обобщить, как средства САПР будут выполнять задачу назначения состояния и генерации конечного автомата. Результат значительно зависит от того, какие средства используются и какие введены установки синтеза.

Риски, связанные с неполнотой верификации. Одной из доступных методик верификации проекта является использование симуляторов. Причем, симуляторы для ПЛИС-технологий используют связку моделей: модель логики работы микросхемы и модель языка высокого уровня. Качество результата в значительной степени зависит от точности и адекватности обоих моделей. На сегодняшний день средства САПР, как правило, предлагают функциональную верификацию, статический временной анализ и определение возможных минимальных временных задержек. В связи с этим существует следующий набор проблем при имитации: ограничение на время выполнения теста, ограничение на количество тестовых векторов, генерация правильного набора тестовых векторов, тесты для всех рабочих режимов, моделирование дополнительной внешней схемы, ограничения средств САПР.

Процесс верификации наиболее трудоемкий в течение всего процесса проектирования и должен занимать от 40 до 75% всех трудозатрат.

2.2. Специфические риски, связанные с реализацией схемотехнических решений на базе ПЛИС

Риски, связанные с хранением проекта ПЛИС в отдельной микросхеме. Это риски, характерные для нерезервированных систем, связанные с ошибками хранимой информации и конфигурации.

Отказ логики пользователя – это воздействие на биты, которые являются динамическими (изменяемыми) при функционировании ПЛИС. Набор возможных проявлений: повреждение единственного бита или кластера временных данных; повреждение состояния элементарной ячейки ПЛИС (триггера логической ячейки, входной/выходной ячейки, ячейки ОЗУ, таблицы перекодировки). Катастрофичность отказа зависит от структуры проекта и времени появления отказа.

Отказы нерезервированной части ПЛИС. Это отказы в элементах контроля ПЛИС (внутренней памяти программ, цепи конфигурации JTAG, цепи контроля JTAG TAP, контроллера Power-on Reset,

цепи питания, цепи синхронизации и системы автоматической подстройки частоты DLL). Это неконтролируемые, недетектируемые, катастрофичные отказы [2].

Отказы выводов. Все отказы выводов делятся на: отказы настраивающих и специальных выводов, отказы входов/выходов, тактирующих входов [2].

Отказы настраивающих и специальных выводов. Все современные микросхемы ПЛИС содержат набор специальных выводов. Они могут выполнять различные функции: перевод устройства в различные режимы (например, режим конфигурации), разрешение отладки, программирование, определение стандарта интерфейса и так далее. Как правило, набор этих выводов уникален для каждого производителя и отдельных семейств. В то же время существуют наиболее общие выводы как, например, выводы стандарта IEEE 1149.1, который может быть использован как для граничного сканирования, так и для конфигурации микросхемы. В качестве основных групп выводов выделяют следующие: выводы, ответственные за режим устройства, интерфейса JTAG, неиспользуемые, тестового интерфейса, конфигурационные, настраиваемые пользователи. Во многих случаях неправильно подсоединенная оконечная нагрузка или отсутствие ее вообще может привести к случаю, когда устройство правильно функционирует при тестировании, но при работе в реальных условиях отказывает. Также требуют необходимой оконечной нагрузки неиспользуемые выводы.

Отказы входов/выходов. Существует ограничения на число выходных выводов, которые могут одновременно переключаться. Такую информацию можно найти в спецификациях на микросхемы и записках по применению. Выводы должны иметь надлежащую оконечную нагрузку. Это касается, во-первых, сигналов тактирования, которые могут быть ошибочными. Во-вторых, это касается сохранения условий для гарантирования распространения сигнала на определенную длину. В-третьих, это касается своевременной установки оконечных резисторов. В-четвертых, это касается ограничений для различных интерфейсов, с целью уменьшения шумов. Следующие риски связаны с надлежащей работой шин с тремя состояниями. Нельзя допустить совместной активной работы устройств на шине. Существует набор рисков, связанных со временем переходного процесса входного сигнала. Не сохранение этого времени может привести к колебанию сигналов, размножению сигналов тактирования и просто повреждению устройства. Для решения этой проблемы используют дополнительные схемы-защёлки. Существует риск, связанный с замыканием (соединением) выводов вместе. Такую ситуацию необходимо избегать, если скорости переключения не совпадают, а также нет возможности протестировать такую избыточную топологию. Объединение возможно в том случае, если эти два сигнала от одной интегральной схемы и производителем разрешается такая ситуация. Существует риск, связанный с ошибкой назначения выводов. Этот риск касается разводки сигнала тактирования, требующего размещения как можно ближе к выводам земли, и так далее. Существует риск, связанный со смешанным напряжением питания, совместимости с постоянным током, запасом помехоустойчивости. Существует риск, связанный с переключением в электроэнергетической системе. При проектировании системы с отдельно питаемыми блоками с целью обеспечения необходимой избыточности или сохранения энергии необходимо быть особенно внимательным. Некоторые КМОП устройства при отключении питания обладают низким импедансом через внутренние диоды или диоды снятия электростатического заряда, другие – высоким входным импедансом.

Отказы тактирующих входов. Существуют риски, связанные с использованием логики с **расфазировкой синхронизирующих импульсов.** Наиболее приоритетно для программируемой логики –

использование внутренних глобальных синхронизирующих импульсов. В случае использования нескольких уровней тактирования существует необходимость анализа таких сигналов. Существуют риски, связанные с **распространением сигнала от одной микросхемы к другой**. Как правило, симулирующие программы позволяют моделировать внутрисхемные задержки, но не позволяют моделировать межсхемное распространение сигнала тактирования. Существуют риски, связанные с **ветвлением дерева тактирования**. Микросхемы ПЛИС обладают схемами фазовой автоподстройки частоты. Каждая ветвь тактового сигнала, а особенно в случае деления частоты, должна быть проверена на наихудшее значение. Каждый генератор должен иметь только одну линию подачи тактового сигнала в схему. Также необходимо контролировать пересекающиеся линии тактирования.

К числу рисков, связанных со **сбросом**, можно отнести риски, связанные с логической схемой сброса (переходный режим и режим устойчивого состояния), разветвлением схемы сброса, несоответствием времен сброса и запуска микросхемы и тактового генератора, защитой сигналов от ложного срабатывания.

Существует вероятность статических и динамических рисков. При статическом риске происходит переключение сигнала за короткий промежуток времени из 0 в 1 и затем обратно в 0. При динамическом риске происходит переключение из 0 в 1, затем в 0 и в конце концов в 1. Эти риски обычны для комбинационных схем. Например, для мажоритарной системы.

Отказ при конфигурировании системы, который будет описан далее в соответствующем разделе.

Риски при подаче питания. При **подаче питания** существуют риски, связанные с последовательностью подачи питания системы, связанные с сигналами при выключенном питании, переходными процессами при включении питания, обходом и распределением сигнала питания. Некоторые современные микросхемы требуют подачи двух или более питающих напряжений. Для ряда устройств необходимо подавать питающее напряжение для вычислительного ядра и второе питающее напряжение – для обеспечения стандарта входа/выхода. Второй стандарт питания может понадобиться как для системы фазовой автоподстройки частоты, так и для стандарта питания и так далее. Порядок подачи питания может воздействовать на надежность всей схемы. Для некоторых устройств неправильная подача питания может привести к повреждению. Проблема сигналов при выключенном питании существует для КМОП микросхем. У некоторых микросхем при выключенном питании выходной сигнал представляет собой низкий импеданс, а для некоторых – высокий. Переходные процессы при включении питания. Величина тока является функцией от времени, температуры, уровня сигнала питания при его нарастании, историей внешнего воздействия, последовательности подачи питающих напряжений. Как правило, уровень, а также время подачи тока должны быть ограничены. Обходом и распределением сигнала питания. Для современных сверхбольших интегральных микросхем существует задача распределения питающего напряжения. Многие микросхемы требуют обвязки множеством развязывающих конденсаторов. Интерфейс JTAG также должен быть должным образом обрамлен. Многие отказы связаны с простым несоблюдением требований разработчиков по обрамлению микросхемы.

Существует группа рисков, связанных с **процессами в ячейках памяти**. Переходные процессы в ячейках памяти при включении/ выключении питания. Существует риск ввести ячейки памяти в режим стирания при подаче неправильного напряжения. Второй режим, который должен быть подвергнут проверкам, является режим записи при выключении питания. Запись должна быть обязательно верно закончена до выключения

питания. Повреждения информации при выключении питания может произойти не только при выключении питания, но и при воздействии агрессивной среды и других факторов. Возможны переходные процессы и шум для микросхем памяти не связанные с включением/выключением питания, а связанные с неправильно выполненной оконечной нагрузкой и с несоблюдением времен циклов. Для микросхем с ограниченным числом циклов стирания и записи существует риск превышения этого числа. Для таких микросхем необходимо оптимизировать число циклов, так как запись одной элементарной ячейки и запись всей памяти приводит к одному и тому же циклу перезаписи и эквивалентны по воздействию на микросхему.

Риски, связанные с избыточностью системы с целью обеспечения отказоустойчивости. Любая кодовая избыточность или схемы коррекции ошибок влечет за собой соответствующую схему. Во-первых, схемы коррекции рассчитываются на определенную кратность отказов и могут быть бессмысленны при непредусмотренных типах отказов. Во-вторых, при проектировании и отладке необходимо контролировать интерфейсы, уровни сигналов и оконечную нагрузку, так как любя дополнительная схема вносит помехи.

Любая избыточность, связанная с переключением на альтернативные конфигурации системы, хранимые в памяти, или с использованием другого интерфейса конфигурирования, влечет за собой необходимость проверки самой альтернативной конфигурации, то есть микросхемы памяти, и вспомогательного интерфейса, и возможной постановки контроллера конфигурации. Также потенциально опасными являются режимы релаксации микросхемы и регенерации, поскольку большинство отказов, связанных с фиксацией ошибочной информации, происходит именно в момент записи.

Риски при конфигурировании. **Отказ при конфигурировании системы** (записи управляющей программы) происходит при сбоях записи конфигурации в цепях и контроллере конфигурирования. Набор возможных проявлений: никаких повреждений, если не повреждена конфигурация/программа, отвечающая за функциональную область; повреждение трассировки и межсоединений; повреждение данных в таблицах перекодировки и логических ячейках. Отказы катастрофичны.

Риски асинхронного проекта. **Асинхронные схемы.** Большинство современных методологий проповедуют синхронные схемы подключения [4 – 6]. Эти методологии настаивают на том, что триггеры должны быть тактированы одним синхроимпульсом с малой расфазировкой и по одному фронту импульса. Использование же асинхронных входов триггера, таких как асинхронный сброс, должно быть сведено к единственному глобальному сигналу сброса микросхемы.

Риски гонки сигналов. **Расфазировка синхронизирующих импульсов** представляет собой событие, связанное с разницей во времени прихода активного фронта синхроимпульса между двумя последовательно соединенными регистрами [4 – 6]. Разница прихода синхроимпульсов зависит от задержки распространения сигнала, скорости нарастания сигнала синхронизации и порога приемника. При этом два последних связанных параметра могут значительно изменяться в зависимости от условий эксплуатации устройства.

Риски метастабильного состояния. **Метастабильное состояние.** Предполагается, что триггер всегда находится в одном из состояний: «0» или «1». Однако работа триггера зависит от таких параметров как: время установки, время удержания, ширина синхросигнала. В случае, если эти параметры не отвечают требованиям, триггер переходит в метастабильное состояние [5]. При этом ошибочные схемы трудно выявить по средствам тестов. Они могут не проявляться из-за низкого времени тестирования. При соответствующем времени установления сигнала ожидаемое время до

отказа для хорошо спроектированной системы с асинхронными входами может быть очень малым и приемлемым.

Риски расположения проекта в кристалле. Дефекты проектирования в микросхеме ПЛИС проявляются так называемым **кластерным отказом**, т.е. множественным отказом логических элементов, причем эти ячейки являются соседними. К кластерным отказам приводят и различные физические воздействия. В то же время существует зависимость между конфигурацией кластерного отказа, определяющей число соседних отказавших ячеек в кластере и их пространственное расположение, его кратностью и расположением проекта в кристалле, выражаемая в различном уровне вероятности сохранения работоспособного состояния. Расположение проекта в микросхеме, а также самой микросхемы в устройстве или в блоке влияет на температурный режим, питание, а, следовательно, и на **временные характеристики структурных элементов**. В результате необходимо тестирование наихудших временных характеристик и определения запаса изменения параметров.

Риски при нарушениях в электрических интерфейсах. **Логические блоки сопряжения.** Иногда требуется сопрягать различные логические блоки, питающиеся от различных источников [2, 3]. Примерами могут быть случаи изоляции избыточных блоков, режимы энергосбережения и так далее. Примером может стать проблема КМОП устройств. При отсутствии питания их выводы сохраняют низкий импеданс между выводами и V_{DD} шиной через защитные или пассивные диоды. Также существует проблема одновременного включения и выключения нескольких источников для предотвращения загрузки блока от не своего источника.

Сопряжение границ напряжения. Корректное сопряжение ТТЛ и КМОП микросхем было проблемой 1980-х. КМОП устройства имели логический высокий входной порог (V_{IH}) равный 70 % от V_{DD} или типично 3,5 В [2, 3]. Примеры также включают ТТЛ-совместимые генераторы и «ТТЛ-совместимые» КМОП микросхемы. При этом «ТТЛ-совместимость» определяется как совместимость с 2,5 В для логического высокого входного уровня V_{IH}.

Направленность современных технологий на уменьшение размеров элементов микросхем привело к понижению питающих напряжений и уменьшению порогов колебаний выходных напряжений. Последние 0,18 μm технологии привели к стандарту питания 1,8 В.

Риски при сопряжении проекта, расположенного в различных микросхемах. Риски, связанные с **выходом сигналов за допустимые пределы**. Такая ситуация может проявиться при отсутствии контроля выхода информации, передаваемой между блоками вещественной арифметики. Также примером может быть наличие шумов при снятии информации с аналогово-цифрового преобразователя. Риски при **недублированных интерфейсах.** Для избежания ситуации, связанной с обрывом интерфейса, необходимо резервировать его и контролировать текущее состояние. В случае, если это линии питания, необходимо их разносить на значительное расстояния для минимизации влияния соседней линии.

Суммирующая классификационная таблица рисков приведена в табл. 1.

2.3. Специфические риски, связанные с применением ПЛИС в аэрокосмических системах. Воздействие космического излучения в космической электронике принято классифицировать на три следующие категории [7]: полная доза ионизирующего излучения (**TID** – Total Ionizing Dose), неионизирующее радиационное воздействие (**DDD** – Displacement Damage Dose), воздействие от единичного события (**SEE** – Single Event Effect). Хотя последствия воздействий (отказ) проявляется в единовременном событии, оба воздействия различны из-за природы и методик ослабления. Рассмотрим все возможные воздействия

согласно классификации по характеру воздействия.

Таблица 1

Классификация рисков

Риск	Детализация проблем, связанных с риском		
Риски, связанные с процессами разработки и верификации:			
Риски нарушения технологии проектирования	Проблема спецификаций		
	Проблема описания конечного автомата	Описание состояний для схемотехнического проекта FSM	
		Описание состояний для проекта FSM на языке	
		Размножение триггеров	
		Переход в неверное состояние	
Риски применения инструментальных средств	Проблема повторного использования проекта	Несоблюдения правил составления схем и именования элементов	
		Значительное изменение проекта при внесении незначительных изменений в код	
	Дефекты САПР	Расфазировка синхроимпульсов, вносимая САПР	
		Описание интерфейсов на уровне логики работы без описания физики ПЛИС	
		Проблема тиражирования и временной оптимизации, выполняемой компилятором	
		Генерация тупиковых состояний автомата	
Риски, связанные с неполнотой верификации	Несоответствие модели логики работы микросхемы и модели проекта		
	Неполнота процесса верификации		
Риски, связанные с применением системного и других видов коммерческого ПО			
Риски, связанные с применением прерываний			
Специфические риски, связанные с реализацией схемотехнических решений (в зависимости от места проявления отказа)			
Риски отказа логики пользователя	Отказы, связанные с процессами в ячейках памяти	Переходные процессы при включении/выключении	
		Повреждение хранимой информации при включении питания от внешних воздействий	
		Шумы при неправильной загрузке	
		Превышение ограничения числа циклов стирания/записи.	
		Избыточность	
	Отказы логических ячеек	Выполняющих комбинационные функции	
		Выполняющих функцию последовательной логики	
Риски отказа нерезервированной части	Отказы конфигурации		
	Отказы нерезервированных выводов (смотри ниже)		
Отказы выводов	Отказы входов/выходов, настраиваемых пользователем	Ограничение на число одновременно переключаемых выводов	
		Несоблюдение правил подключения оконечной нагрузки	Отсутствие резисторов
			Ограничения на интерфейсы
		Статические и динамические риски	
		Неправильный арбитраж шин	
		Несоблюдение времени переходного процесса входного сигнала	
		Ошибочное замыкание выводов	
		Ошибки назначения выводов	
		Выход значения сигналов за допустимые пределы	
		Недублированных интерфейсов	
	Отказы специальных и настраивающих выводов	Электрических интерфейсов при обвязке одной микросхемы	Ошибки схемотехники интерфейсов
			Переходные процессы
			При выключении питания
			Распределение питающих напряжений
		Электрических интерфейсов при реализации проекта на нескольких микросхемах	Ошибочные переключения в электроэнергетических системах
			Ошибки логики работы блоков сопряжений
			Сопряжение границ различных интерфейсов
		Отказы в специальных интерфейсах (загрузки, тестирования и т.д.)	
		Оконечная нагрузка тактирующих выводов (внешняя синхронизация)	Несоблюдения ограничений на сигнал тактирования
			Ошибки распространения сигнала от микросхемы к микросхеме
		Внутренняя синхронизация	Неправильное ветвление дерева синхронизации
			Асинхронизм схем
			Расфазировка синхросигналов
			Метастабильное состояние
		Ошибочный сброс	Неправильная схема сброса
			Ветвление схемы сброса
			Защита от ложного срабатывания
			Несоответствие времен сброса и запуска
		Статические и динамические риски	
		Несанкционированный доступ	

TID (предельная накапливаемая доза (ПНД)) – долговременная деградация из-за накопления энергии. Воздействие приводит к параметрическим или функциональным отказам. Источниками данного воздействия в космической среде могут быть захваченные электроны, захваченные протоны или солнечные протоны.

DDD часто имеет подобную долговременную природу деградации, но отличается физическим механизмом. Приводит к деградации свойств материала, являющейся результатом смещения атомов в материале из устойчивых положений в кристаллической решетке. Первичными источниками воздействия являются захваченные протоны, солнечные протоны, нейтроны радиоизотопного термоэлектрического генератора, захваченные электроны.

SEE происходит при соударении единичного иона и материала. При этом ион передает энергию как от непосредственного соударения (прямая ионизация), так и при помощи вторичной эмиссии (непрямая ионизация из-за протонов). Множество типов SEE может быть разделено на две категории: сбои (восстанавливаемые отказы) и отказы.

Мягкий отказ происходит при переходном импульсе или переключении бита в устройстве, вызывая ошибку информации, детектируемую на выходе. **Невосстанавливаемые отказы** могут быть, но не обязательно, физически разрушительными для ПЛИС. Они вызывают функциональные и параметрические отказы.

Приведем классификацию воздействий по единичному событию, приводящих к отказам ПЛИС в условиях космической радиации.

Некатастрофичный отказ (сбой) по единичному событию (**SEU** – Single Event Upset) – изменение состояния или переходной процесс, вызванный энергетической частицей. Может происходить в цифровых, аналоговых и оптических компонентах или в схеме интерфейса (подмножество отказов известных как переходной процесс по единичному событию, SET – Single Event Transient). По сбросу или перезаписи устройство переходит в нормальный режим функционирования.

Устойчивый отказ по единичному событию (**SHE** – Single Hard Error) представляет собой подвид SEU, который приводит к постоянным изменениям работы системы. Примером может быть константный отказ (залипание) бита памяти.

Защелкивание по единичному событию (**SEL** – Single Event Latchup) – приводит к потере функциональности системы из-за предшествующего превышения тока. SEL может как вызывать, так и не вызывать устойчивый отказ.

Выгорание по единичному событию (**SEB** – Single Event Burnout) – событие, которое может вызвать разрушение элементной базы системы из-за превышения тока в мощном транзисторе.

Пробой вентиля по единичному событию (**SEGR** – Single Event Gate Rupture) – событие, которое приводит к формированию проводящего канала в МОП-транзисторе.

Все отказы по источнику появления идентичны. Высокоэнергетичный ион проходит через кристалл. При взаимодействии с кристаллом по пути прохождения создает пары электрон-дырка. В электрическом поле эти пары начинают дрейфовать в противоположные направления и собираются у соответствующего источника поля, создавая токовый переходной процесс. При этом, критичный заряд необходимый для того, чтобы вызвать отказ, уменьшается как квадрат размера технологии изготовления транзистора. Существует критическая ширина переходного процесса. При ширине переходного процесса больше критической, вызванный ошибочный сигнал воспринимается как нормальный. Переходной процесс по единственному событию выделяют из некатастрофичных отказов по месту проявления.

Если рассмотреть любой СОК-проект как последовательность триггеров и комбинаторной логики, то переходной процесс по единственному событию может возникать на выходе комбинаторной логики и на входе триггера. Сбой же происходит в триггере. При этом переходной процесс по единственному событию может произойти только на срезе тактовой частоты, когда триггер производит считывание нового состояния с входа и переходит в режим хранения (удержания). Поэтому переходной процесс по единственному событию линейно зависит от частоты переключения триггера (некатастрофичный отказ от частоты не зависит).

По количеству отказывающих элементарных структур за одно событие отказы делят на **единичные** и **множественные** отказы. Кратность отказа зависит от угла атаки ионизирующей радиации. Самая большая вероятность при атаке в плоскости кристалла. При этом возможно создание так называемого кластерного отказа, пространственная конфигурация которого описывается набором соседних ячеек.

Программируемая логика на основе RAM, EPROM и EEPROM технологий основана на хранении заряда. Хранимый заряд является чувствительным к деградации от радиационного воздействия. Технология Actel на основе антипрожигаемых перемычек antifuse создает жесткий контакт и не зависит от хранимого заряда. В результате микросхемы Actel имеют значительную устойчивость к радиационному воздействию.

Выводы

Предложенная структура рисков позволяет осуществлять качественную оценку надежности и безопасности ПЛИС-проектов для тех приложений, где задаются жесткие нормативные требования к этим свойствам, выполнение которых сложно верифицировать при применении количественных методов.

Рассмотренные отказы характерны для универсальных структур ПЛИС (триггеров, межсоединений, комбинаторной логики) с учетом всего жизненного цикла проекта.

Литература

1. Xilinx Solutions for Aerospace & Defense Applications. – [Электрон. ресурс]. – Режим доступа: http://www.xilinx.com.

2 Katz R., Barto R., Erickson K. Logic Design Pathology and Space Flight Electronics. // Proceedings of MAPLD Conference. – 1999. – 28 p. – [Электрон. ресурс]. – Режим доступа: http://www.klabs.org.

3 Cohen B. Minimizing HDL Design Errors. VHDL Cohen Publishing. – [Электрон. ресурс]. – Режим доступа: http://www.vhdlcohen.com.

4 Хоровиц П., Хилл У. Искусство схемотехники: В 2-х т. Пер. с англ. – М.: Мир, 1983. – Т. 1. – 598 с.

5 Metastability in Altera Devices. Application Note 42. Ver. 4. – 1999. – P. 845 – 854.

6 Erickson K. Asynchronous FPGA Risks // Proceedings of MAPLD Conference. – 2000. – 6 p. – [Электрон. ресурс]. – Режим доступа: http://www.klabs.org.

7 LaBel K. Single Event Critical Analysis. Sponsored by NASA. Code QW. – 1996. – [Электрон. ресурс]. – Режим доступа: http://radhome.gsfc.nasa.gov.

Поступила в редакцию 14.03.2006

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.