Fault-tolerant satellite computing with modern semiconductors

Fuchs, C.M.

Резюме на Русском Языке

Современные полупроводниковые технологии позволяют создавать миниатюризированные спутники, запуск которых дёшев, и недорогие платформы для широкого круга научных и коммерческих инструментов. В особенности это касается наименьших и легчайших спутников, позволяющих организовать космические миссии, которые ранее были технически невозможны, непрактичны и просто неэкономичны. Спутники, сконструированные как Кубсат, могут создаваться быстро и дёшево, в условиях ограниченных ресурсов, характерных для академической среды. Однако такие спутники в настоящее время характеризуются низкой надёжностью. Следовательно, вплоть до последнего времени их использовали в основном для некритичных и малобюджетных миссий, где такие риски приемлемы.

Сегодня многие сложные научные и коммерческие применения могут быть реализованы в форм-факторе миниатюризированных спутников, желательно с намного большей длительностью активного существования. Теоретически, в настоящее время такой спутник мог бы быть использован в критических и сложных многофазных миссиях, а также в высокоприоритетных научных проектах по изучению Солнечной системы и астрономических применениях. Однако из-за своей низкой надёжности эти аппараты до сих пор использовались только как сопутствующие системы для выполнения вторичных задач.

Современная электроника составляет значительную часть таких космических аппаратов и определяет несколько их наиболее критических подсистем. Учитывая их меньший вес, электроника должна быть легче, меньше и предоставлять лучшее соотношение производительности на 1 Ватт мощности, по сравнению с традиционными компонентами космического класса. Таким образом, все наиболее сложные спутники Кубсат сегодня используют передовые промышленные разработки, пришедшие с рынков встроенных систем и мобильных устройств. При минимальной стоимости обеспечивается избыток производительности, малое энергопотребление и лёгкость использования, по сравнению с электроникой космического класса, имеющей длительную историю применения.

Однако для обычных вычислителей на базе систем на кристалле также требуется сбое- и отказоустойчивость, как и для бортовых систем больших космических аппаратов. В соответствующих работах подсистемы, использовавшие эти компоненты признаны ответственными за большинство отказов после того, как аппарат был запущен и выведен на заданную орбиту. Из-за требований ограниченных бюджета миссии, массы, энергии и объёма миниатюризированных спутников существующие решения со сбоеустойчивыми вычислителями для больших аппаратов не могут быть приняты.

По состоянию на 2019 год, не существует архитектур сбоеустойчивых вычислителей, которые могли бы быть использованы в наноспутниках, использующих электронную компонентную базу из применений на мобильных рынках и рынках встроенных систем без нарушений фундаментальной концепции дешёвого, простого, энергоэффективного и лёгкого спутника, который может серийно производится и имеет низкую стоимость запуска. Разработчики малых аппаратов, таким образом, имеют только следующие варианты:

Апскейлинг: (повышение качества) использование традиционных компонентов космического класса. Обычно это приводит к созданию спутника большего форм-фактора, т.к. компонентам нужно больше энергии и они обеспечивают меньшую функциональность, гибкость и производительность. На практике такой подход резко повышает стоимость, требования к рабочей силе и время разработки спутника. Таким образом, этот подход является неконструктивным для большинства концепций новых миссий, концентрирующихся на спутниках, которые разрабатываются быстро, имеют малый размер, способность к расширению и низкую стоимость.

SpareSats: (Спаренные спутники) Уменьшение риска раннего отказа с помощью выведения одного или нескольких SpareSat для замены Кубсат, как только тот отказал. На практике это не только увеличивает стоимость, но и также увеличивает вероятность отказа, поскольку общее количество запущенных компонентов удваивается. Таким образом, данный подход становится реализуемым только если достигнут достаточный уровень надёжности. На сегодняшний день подход может быть реализован только для спутниковых созвездий, где поколения спутников постоянно заменяются в быстром темпе (например, Planet Lab), и для индивидуальных спутников с исключительно большим бюджетом (например, MarCo).

Принятие: Принять недостаток надёжности. Оставить миссию скоротечной в надежде достичь всех главных задач до того, как космический аппарат в произвольный момент откажет. Для будущих миниатюризированных космических миссий с большими сроками активного существования такие факторы как надежда, вера и удача не должны использоваться в качестве инженерной базы.

Когда была написана эта диссертация, разработчики большинства миниатюризированных спутников были вынуждены следовать этому третьему варианту. Для очень простых и быстрых Кубсат миссий этот подход приводил к успеху чаще, чем к неудаче, но тем не менее – к большому числу ранних отказов. Однако, игры со временем и попытки зацепиться за надежду «авось в этот раз пронесёт» — неприемлемы и вызывают всё меньше понимания у правительств, космических агентств и инвесторов. Для обеспечения успеха современных долгоиграющих Кубсат миссий требуются лучшие и более надёжные системные архитектуры. Таким образом, нужны те сбое- и отказоустойчивые концепции, которые подходят для бортовых компьютеров на основе современных полупроводниковых приборов.

Настоящая диссертация и её результаты

В данной диссертации представлена в деталях новая архитектура сбоеустойчивого вычислителя, призванная преодолеть технологический дефицит, который сегодня влияет на использование очень маленьких спутников. Эта технология подходит для интеграции даже в лёгкие научные Кубсат, базирующиеся на современной коммерческой электронной компонентной базе.

Для развития архитектуры, представленной в этой диссертации, использованы результаты и концепции из широкого круга научных и инженерных областей, и потребовавшийся опыт лежит за пределами только науки или только инженерии. Вместо этого мы объединяем лучшее из обоих этих миров: мы интегрируем научные достижения, концептуальное знание и теоретические изыскания с практической реализацией и тщательным тестированием, являющимся стандартом для областей космоса и электронного машиностроения.

Чтобы сделать материалы диссертации доступными для учёных и инженеров, Главы 2 и 3 посвящены неформальному введению и определению рассматриваемой модели сбоев. В Главе 2 содержится краткий обзор сегодняшних ключевых аспектов космического полёта для читателей, незнакомых с данной темой. Он служит в качестве мотивации для данной диссертации. Глава также представляет концепции, относящиеся к проектированию сбоеустойчивого компьютера. Для разработки и развития действительно эффективной и действенной архитектуры сбоеустойчивого бортового компьютера необходимо понимать, как космическое пространство влияет на вычислитель. Глава 3 детализирует эти эффекты, ограничения для разработчика космической электроники, операционные вопросы космических миссий, такие как времена коммуникации, и небесная механика.

В Главе 4, основываясь на материале предыдущих глав, мы представляем архитектуру сбоеустойчивого бортового компьютера, которая включает программно-реализованные концепции на ПЛИС с реконфигурацией и смешанной критичностью. Далее это объединяется с несколькими другими, более традиционными способами обеспечения сбоеустойчивости и исправления ошибок. Сбоеустойчивость в этой архитектуре реализована как несколько взаимосвязанных стадий, позволяющих бортовому компьютеру «стареть изящно».

Для обеспечения этой функциональности мы используем программно-реализованное синхронизированное пошаговое выполнение, описанное в Главе 4. Эта функциональность сама по себе предоставляет широкие возможности обеспечения сбоеустойчивости, но может быть недостаточной для долгих миссий, поэтому в Главе 5 мы описываем, как реконфигурируемая логика может использоваться для восстановления дефективной системы из широкого круга возможных сбоев. Мы используем реконфигурацию ПЛИС для гарантии целостности проекта системы на кристалле, чтобы увеличить сроки функционирования бортового компьютера и максимизировать потенциальное покрытие сбоев и совместно используемые ресурсы.

В космических миссиях с очень долгим сроком выполнения дефективные блоки ПЛИС в конечном счёте перестанут восстанавливаться с помощью реконфигурации, т.е. количество доступной неиспорченной программируемой логики в бортовом компьютере со временем уменьшается. В Главе 6 мы показываем, как смешанная критичность может помочь вычислителю адаптироваться к деградации, вместо того, чтобы внезапно отказывать, как это происходит в традицион-

ных системах. Мы можем использовать эту функциональность для того, чтобы выторговать производительность за энергосбережение и надёжность автономно во время работы. Это позволяет сберечь ядро бортовой программной функциональности при возникновении сбоя, достигая «изящного старения» и используя совместные ресурсы для максимизации выживаемости.

Вся эта функциональность присутствует в виде программного обеспечения. Оно исполняется на мультипроцессорной системе на кристалле, реализованной на ПЛИС. Программное обеспечение, информация о полезной нагрузке и логика, программируемая в ПЛИС, — это данные, целостность которых должна быть обеспечена в течение всей космической миссии. В Главе 7 представлены концепции защиты для различных технологий памяти, используемой на борту современных спутников. Ранее предложенные программные концепции обеспечения сбоеустойчивости, применимые к современным полупроводниковым технологиям, часто звучат привлекательно в теории, однако оказываются непрактичными для реализации в реальном мире. На сегодняшний день не существует такой сбоеустойчивой архитектуры, реализованной и верифицированной на практике, хотя это критический шаг. Мы делаем этот критический шаг в Главах с 8 по 10 данной диссертации.

Функциональность синхронизированного пошагового выполнения, используемого в нашей архитектуре, верифицирована с помощью инжекции (внесения) сбоев в Главе 8. В Главе 9 мы описываем проект мультипроцессорной системы на кристалле, реализованный в ПЛИС, которая служит идеальной платформой для данной архитектуры. Глава 10 посвящена практической реализации концепций и проектов, описанных в предыдущих главах. Таким образом, мы показываем, как может выглядеть бортовой компьютер с этой архитектурой в реальном мире, используя для проверки концепции макеты, сконструированные на основе отладочных плат. Это было сделано для следующих 6-ти ПЛИС фирмы Xilinx:

- Kintex UltraScale KU60,
- Kintex UltraScale+ KU11p, KU3p, KU5p из отладочной платы KCU116 и
- Virtex UltraScale+ VU9P из отладочной платы VCU118.

Для трёх из этих ПЛИС: KU60, KU11p и KU3p – мы представили детальные данные по мощности и утилизации.

Заключение

В начале этой диссертации мы поставили вопрос:

«Может ли архитектура сбое- и отказоустойчивого компьютера основываться на технологиях современного рынка встроенных и мобильных применений, без нарушения ограничений массы, размера, сложности и бюджета, характерных для миниатюризированных спутников?»

Спустя три года, множество опубликованных исследовательских статей и несколько катастроф, можно ответить на этот вопрос следующим образом:

*«**Да.** Сбое- и отказоустойчивая архитектура для миниатюризированных спутников технически реализуема с помощью современных технологий потребительского и промышленного уровня. Будучи однажды полностью реализована в качестве прототипа, она может быть использована для значительного увеличения сроков активного существования современных Кубсат, позволяя тем самым использовать их для длительных космических миссий.»*

Программные компоненты архитектуры, представленные в настоящей диссертации, могут быть реализованы «неинвазивным» способом. Они предоставляют защиту существующих применений без необходимости специализированных изменений в них для поддержки этой архитектуры. Используя обычное программное обеспечение, мы показываем, что эти механизмы могут детектировать сбои и отказы быстро и с большой вероятностью и что мы можем успешно восстанавливаться после сбоев, в большинстве случаев – при малых вычислительных потерях. Мы демонстрируем, что вычислительная стоимость этой архитектуры экономична и остаётся эффективной даже при работе в исключительно жёстких радиационных условиях космоса.

С современными коммерческими электронными компонентами проект системы на кристалле, который служит идеальной платформой для этой архитектуры, может быть реализован даже на наименьшей Ultrascale+ ПЛИС с потреблением всего лишь 1,94 Вт. Следовательно, архитектура бортового компьютера может быть применена к спутникам размером с 2U Кубсат.

При технологическом масштабировании, прогресс в полупроводниковой технологии в следующем поколении ПЛИС сделает этот подход даже более желательным и удобным для защиты меньших космических аппаратов. Он может повысить эффективность и масштабируемость при применении на борту более тяжёлого космического аппарата, который мы используем сегодня для высокоприоритетных научных задач и для исследования Солнечной системы. И можно выразить надежду на то, что когда-нибудь в будущем мы сможем исследовать и то, что находится за её пределами.