Юрий Широков

Платформы SIL 4 для критически важных приложений

Сегодня электроника вездесуща. Не обходится без неё ни поезд, ни самолёт. Как создать компьютер таким образом, чтобы его можно было сертифицировать для работы в ответственных приложениях, какие препятствия существуют на этом пути, и есть ли способ сделать компьютер, подобный этому, модульным типовым продуктом? О принципах построения надёжных схемотехнических решений для критически важных приложений рассказано в этой статье.

Безопасность, надёжность и конкурентоспособность: цели достижимы

Везде, где ошибки или сбои могут привести к гибели людей или серьёзному ущербу для окружающей среды, а также имущества, используемая электроника критически важна для безопасности. Подобные системы следуют строгим стандартам, предписывающим свои критерии безопасности для каждого рынка. Вы можете увидеть примеры таких систем в поездах, автобусах, кораблях и самолётах. Аппаратное и программное обеспечение здесь должно работать надёжно, поскольку права на ошибку нет. К электронике на транспортных средствах предъявляются дополнительные требования. Она должна быть не только безопасной, но и чрезвычайно надёжной. Эти два аспекта увеличивают стоимость таких систем по сравнению с коммерческой электроникой. Тем не менее их цена не должна становиться чрезмерной, поскольку, в конечном счёте, расходы несут потребители. Если не соблюсти этот принцип, то транспортные средства и, следовательно, их поставщики (особенно это верно для общественного транспорта) утратят конкурентоспособность. В области встраиваемых систем снизить затраты помогает модульность. Классическими примерами модульных систем являются 19-дюймовые шинные системы CompactPCI и VMEbus. Оба стандарта разрабатывались и совершенствовались на протяжении многих лет в различных приложениях, включая бортовые системы самолётов. Большое количество производителей предлагает для них стандартные карты, многие из которых спроектированы для суровых условий окружающей среды. Несмотря на это, аспект функциональной безопасности остаётся отдельной проблемой, особенно если принимать во внимание особенности построения вычислительного ядра системы. Можете ли вы спроектировать компьютер, на аппаратном уровне защищённый от ошибок в вычислениях, происходящих по вине случайных сбоев, отказа компонентов, влияния электромагнитных помех или жёсткого космического излучения? Надо учесть и возможные ошибки на этапе проектирования, которых можно избежать, используя соответствующие технологии. Специалисты компании MEN Mikro Elektronik решили эти проблемы.

Далее мы расскажем о том, что необходимо учитывать, когда вы хотите сделать компьютер безопасным, и какие именно решения нашла фирма MEN.

Основы безопасности жизнедеятельности компьютеров

Наиболее действенной стратегией придания надёжности системам является дублирование (или резервирование) их значимых компонентов. Компонент, сбой в работе которого останавливает работу системы, называется единой точкой отказа (SPOF – Single Point of Failure). Если реализовать избыточность критических компонентов, таких как ЦПУ, то доступность и/или надёжность возрастает. В зависимости от преследуемой цели можно выбирать различные конфигурации резервирования. Для этого нужно планировать функциональность, которая должна быть в рабочем состоянии даже в случае сбоя (M), по сравнению с общим количеством избыточных функций (N), то есть получаем систему “M из N”, или сокращённо MooN (M out of N). Например, конструкция 1oo2 увеличивает доступность системы и, как следствие, среднее время между отказами (MTBF – Mean Time Between Failures). Система 1oo2 (рис. 1) может продолжать работать, даже если один из двух процессоров выйдет из строя. Это называется отказоустойчивостью. MTBF такой системы увеличивается в 1,5 раза. Для обеспечения безопасности резервирования

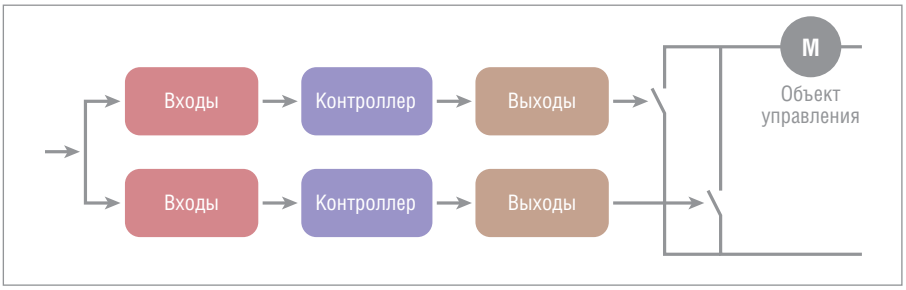

Рис. 1. Система 1oo2

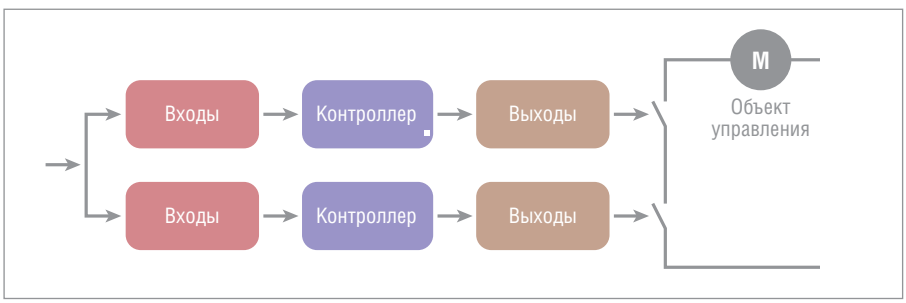

Рис. 2. Система 2oo2

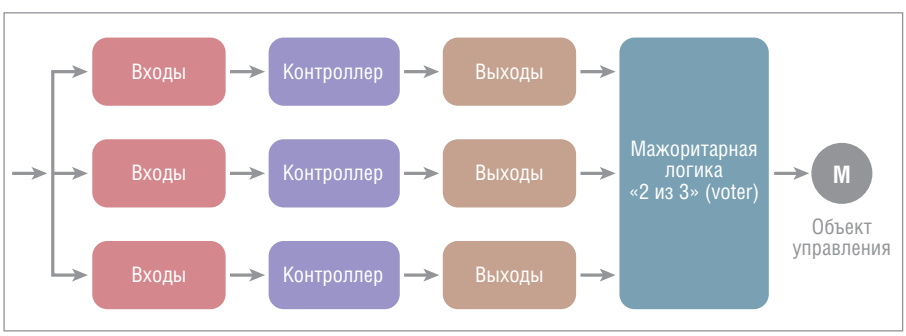

Рис. 3. Система 2oo3

все компоненты также должны обеспечивать идентичные результаты вычислений, чтобы можно было посредством сравнения обнаруживать ошибки. В простейшем случае это реализовано в примере системы 2oo2 (рис. 2). Эта схема гарантирует, что обе части системы работают одинаково в любое время. К сожалению, такая конструкция в 0,5 раза[1] снижает доступность (MTBF). Например, в случае ошибки системы управления подвижны́м составом поезд должен полностью остановиться, после чего система переходит в безопасное состояние, то есть она является отказоустойчивой. Однако вопрос правильного выбора типа резервирования не в том, нуждаетесь ли вы в бо́льшей безопасности или доступности. Невозможно просто отключить критически важную функцию на борту самолёта. Она должна быть доступна и постоянно, и безопасно. Поэтому, если нужна высокая степень избыточности, необходимо создать систему 2oo3 или 2oo4 (рис. 3).

При таком уровне сложности неотъемлемой частью системы является механизм мажоритарного голосования (*voter, или воутер*). Он постоянно сравнивает и анализирует результаты вычислений. В случае отклонения он выявляет и изолирует засбоивший ЦП, но система может продолжать работу с использованием двух других исправных компонентов. Принцип 2oo3 часто используется именно потому, что он повышает безопасность и доступность до статистически достаточной и разумной степени, сохраняя приемлемыми сопутствующие накладные расходы. MTBF при этом возрастает с коэффициентом около 1,2. Тем не менее, управление такой системой сложно: три подсистемы должны быть синхронизированы и должны обмениваться данными – это особенно непростая задача для программного обеспечения. Более того, в результате такого преобразования может снизиться производительность. Модульные системы, основанные на стандартных сменных картах, позволяют относительно легко настроить описанную избыточность: вам просто надо «утроить» все карты. Но это имеет свои недостатки: трём параллельным системам требуется пространство, а также тройной запас мощности источника питания, и реализация программного обеспечения и воутера для трёх компьютеров может оказаться сложной. Вот почему компания MEN пошла путём реализации избыточности на уровне платы. Помимо тройного резервирования процессора на плате ЦП имеется резервная основная память, локальное питание, тактовые генераторы и флэш-память. Воутер реализован в виде IP-ядра внутри программируемой вентильной матрицы FPGA. В случае отказа одного из процессоров воутер изолирует его и сохраняет в состоянии сброса. Он также уведомляет программное обеспечение о сбое и продолжает контролировать работу исправных процессоров. Пока не выйдет из строя один из оставшихся процессоров, система полностью сохраняет функциональность. Это решение требует значительно меньше энергии и места, чем три отдельные платы. Тот факт, что при этом значительно облегчаются проблемы с программным обеспечением, также важен. Три ЦПУ работают в архитектуре, называемой lockstep (жёсткая параллельная работа, в которой процессоры полностью синхронизированы). Для программного обеспечения они являются единым целым, поскольку вопросы управления избыточностью становятся для ПО непрозрачными. На практике это означает, что от самого программного обеспечения управление избыточностью уже не требуется. Это значительно сокращает затраты на интеграцию ПО, а вместе с этим и общие затраты на разработку. Код, необходимый для синхронизации трёх процессоров, довольно прост. Поэтому даже модификация существующих систем, рассчитанных на работу с одним процессором, не потребует больших усилий.

TMR как основа радиационно-стойкой электроники

Как было упомянуто ранее, любой важный компонент может стать единой точкой отказа. В бортовых приложениях авионики и космонавтики особенно часты ошибки памяти, вызванные косми-

[1]В системе MooN для сохранения функциональности системы должны работать M из N каналов. В нашем примере системной функцией будет включение двигателя. В первом примере (рис. 1) достаточно работы одного канала; во втором примере (рис. 2) для включения двигателя должны быть работоспособны оба канала.

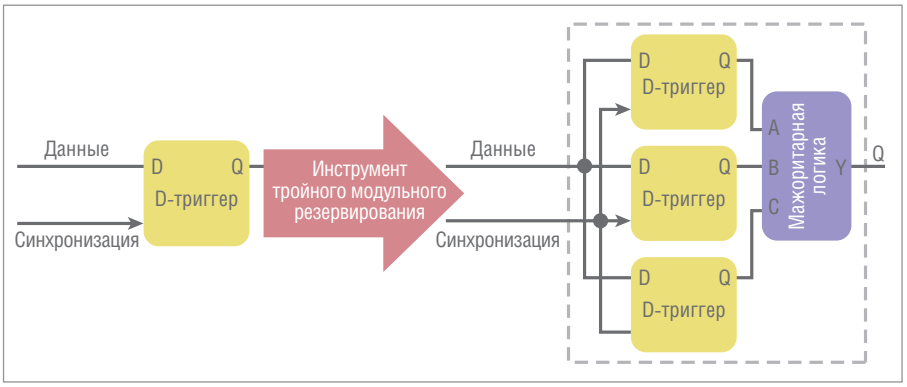

Рис. 4. Строенный триггерный блок TMR в матрице FPGA

ческим излучением. К ним относятся такие эффекты, как SEU (Single Event Upsets – одиночные сбои) или MBU (Multi-Bit Upsets – множественные сбои), когда один или несколько битов в триггерах или ячейках ОЗУ инвертируются, то есть случайным образом меняются с 0 на 1 или наоборот. Это особенно касается компонентов памяти и FPGA, играющих важную роль в разработках MEN. FPGA (или ПЛИС) не только являются частью воутеров для процессоров, но и контролируют банки оперативной памяти. С целью автоматического выявления и исправления битовых ошибок можно вместо одного установить три банка памяти, то есть использовать тройное модульное резервирование (TMR – Triple Modular Redundancy). Все операции чтения и записи будут выполняться параллельно и одновременно во всех банках. Воутер анализирует данные, считанные из ячеек памяти, по принципу приоритета большинства (мажоритарная логика). Вся память,таким образом, периодически контролируется в фоновом режиме – одно слово с каждым циклом обновления. Мажоритарное значение записывается обратно во все ячейки. Этот предотвращающий накопление «перевёрнутых» битов механизм называется очисткой памяти. Аналогичным образом разработчики ИС также сделали более надёжными триггеры в регистрах ПЛИС. Случайное переключение триггеров может привести к нескольким различным эффектам ошибок на интерфейсах ПЛИС, от искажённых выходных данных до полностью ошибочного поведения. Инструмент для синтеза безопасных компонентов позволяет преобразовать один триггер в блок из трёх триггеров, объединённых по выходам мажоритарной логикой 2oo3 (рис. 4). Частота отказов таких блоков TMR составляет примерно 0,000001 FIT (Failure in Time – отказ в единицу времени), что делает их (по сравнению с вероятностью других отказов в системе) практически абсолютно надёжными. IP-ядра внутри FPGA были разработаны в соответствии со стандартом авионики DO-254 (Design Assurance Guidance for Airborne Electronic Hardware – руководство по безопасному проектированию бортового электронного оборудования). В итоге можно использовать стандартные компоненты FPGA такой конструкции даже в безопасном компьютере. При своей устой-

чивости к радиации они гораздо более дешёвые и гибкие, чем специально разработанные для аэрокосмической промышленности компоненты. Поскольку в критически важных для безопасности приложениях долгосрочная доступность тоже является важным фактором, использование FPGA защищает конструкцию также и от устаревания компонентов. В долгосрочной перспективе это может снизить затраты на разработку, особенно если речь идёт о чрезвычайно сложной функциональности. Одним из примеров является интерфейс AFDX (Avionics Full Duplex Switched Ethernet – полнодуплексный коммутируемый Ethernet для авиации). Этот тип Ethernet обеспечивает связь между системами самолёта. Он основан на стандарте Ethernet и дополнительно определяет высокую целостность данных, избыточность и детерминированное поведение. Реализация функциональности AFDX потенциально требует большого объёма разработок, окупающихся в приложениях только через длительный период времени. Проектирование этого интерфейса на основе FPGA является обоснованным и экономичным подходом.

Предсказуемость – залог безотказности

Детерминированность, являющаяся свойством AFDX, применима и ко всей системе в целом. Наряду с безопасностью в плане отказов критически важные задачи также требуют предсказуемого расчётного времени выполнения. Даже в наихудших условиях система должна реагировать на внешние события в течение определённого времени. Типичные компьютерные архитектуры используют прерывания и структуры DMA (Direct Memory Access – прямой доступ к памяти). Однако эти механизмы могут отрицательно влиять на время реакции. В таком случае трудно достичь требуемого детерминированного, то есть предсказуемого поведения. Вот почему нужно избегать упомянутых общих механизмов. Вместо этого инженеры должны подробно рассмотреть возможное поведение и его последствия на ранней стадии подготовки к реальному проектированию. Точный и максимально полный анализ различных ошибочных сценариев и ситуаций в сочетании с детерминированным в момент возникновения ошибок поведением компьютера приводит к высокому уровню предсказуемости. Основной целью здесь является обнаружение ошибок до того, как они смогут причинить вред всей системе. С точки зрения аппаратного обеспечения и прошивки, для этого используются компоненты BITE (Built-in Test Equipment – встроенная тестовая функциональность). Важную роль играют также методы обработки ошибок, такие как ECC (Error-Correcting Code – код коррекции ошибок) или мониторинг внутренних напряжений. Если говорить о программном обеспечении, самый важный вопрос здесь – какую использовать операционную систему. Нуждающиеся в детерминированном поведении системные интеграторы выбирают системы реального времени типа VxWorks или PikeOS. Эти ОС оптимизированы для минимизации задержек управления памятью и задачами, так что система всегда остаётся предсказуемой. Везде, где возможны перебои в электроснабжении, очень важно также короткое время запуска. По этой причине разработчики MEN оптимизировали свои платы для быстрой за-

грузки. Загрузочный образ объёмом всего 8 МБ позволяет достичь времени запуска 500 мс, то есть практически сразу после включения.

Кластеризация и диверсификация избыточности

Разнообразие избыточности и кластеризация делают системы ещё более безопасными, потому что не только обеспечивается избыточность, но и дополнительно используется распределённый принцип построения. Для одинаковых подсистем (гомогенная избыточность) вероятен одновременный выход из строя по одинаковым причинам. Можно противостоять этому, создавая различия, снижающие подверженность единообразным сбоям CMF (Common Mode Failures) и сбоям по общей причине CCF (Common Cause Failures).Например, можно запускать в подсистемах различные, независимо разработанные программные приложения. С аппаратной точки зрения можно использовать разные интерфейсы ввода/вывода, в которых однотипные функции реализованы по-разному. В конце концов, две разные настройки должны привести к одинаковому результату, но разными путями. Такое разнообразие возможно даже на одной плате: управление памятью процессоров в конструкции MEN позволяет разделить ресурсы, что, в свою очередь, поддерживается операционными системами реального времени, такими как PikeOS. Разделам назначены определённые области памяти, а внутри них могут выполняться совершенно различные приложения и задачи (рис. 5). Возможно также объединение двух сборок, формирующих в данном случае компьютерный кластер. В такой конфигурации каждый канал, будучи сам по себе избыточным, работает независимо, но активен в любой момент времени только один из них. Если активный канал выходит из строя, система автоматически переключается на другой. Платы могут быть объединены с использованием выделенных последовательных интерфейсов UART (DEX), предназначенных специально для межканальной связи. Переключение с активного на неактивный канал контролируется платой управления BMCX (Board Management Controllers, рис. 6). На рис. 7 показано, как эта идеология была реализована на плате с тройным резервированием.

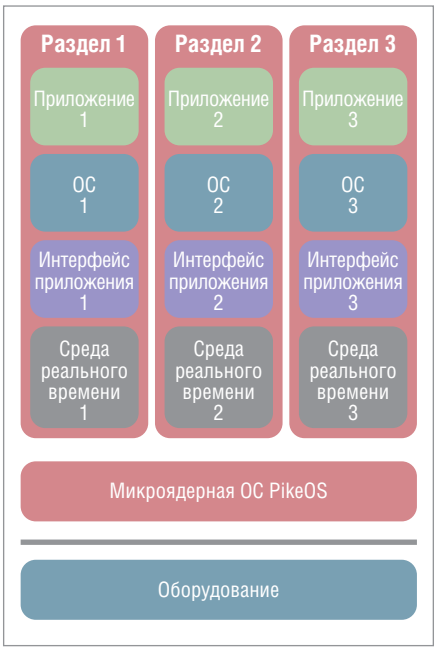

Рис. 5. Организация независимых разделов в PikeOS

Безопасность зависит не только от компьютера

Стандарты безопасности

Общий стандарт функциональной безопасности описан в документе МЭК 61508 Международной электротехнической комиссии. Он охватывает основные вопросы функциональной безопасности в электронных системах и определяет уровни безопасности от SIL 1 до SIL 4. Производители обязаны определять требуемый уровень SIL для систем или функций, связанных с безопасностью, путём проведения анализа опасности и рисков. Определённый уровень диктует степень эффективности функций безопасности и выражается вероятностью сбоя жизненно важных функций. Различные сценарии соответствуют определённой шкале числовых значений. Впо-

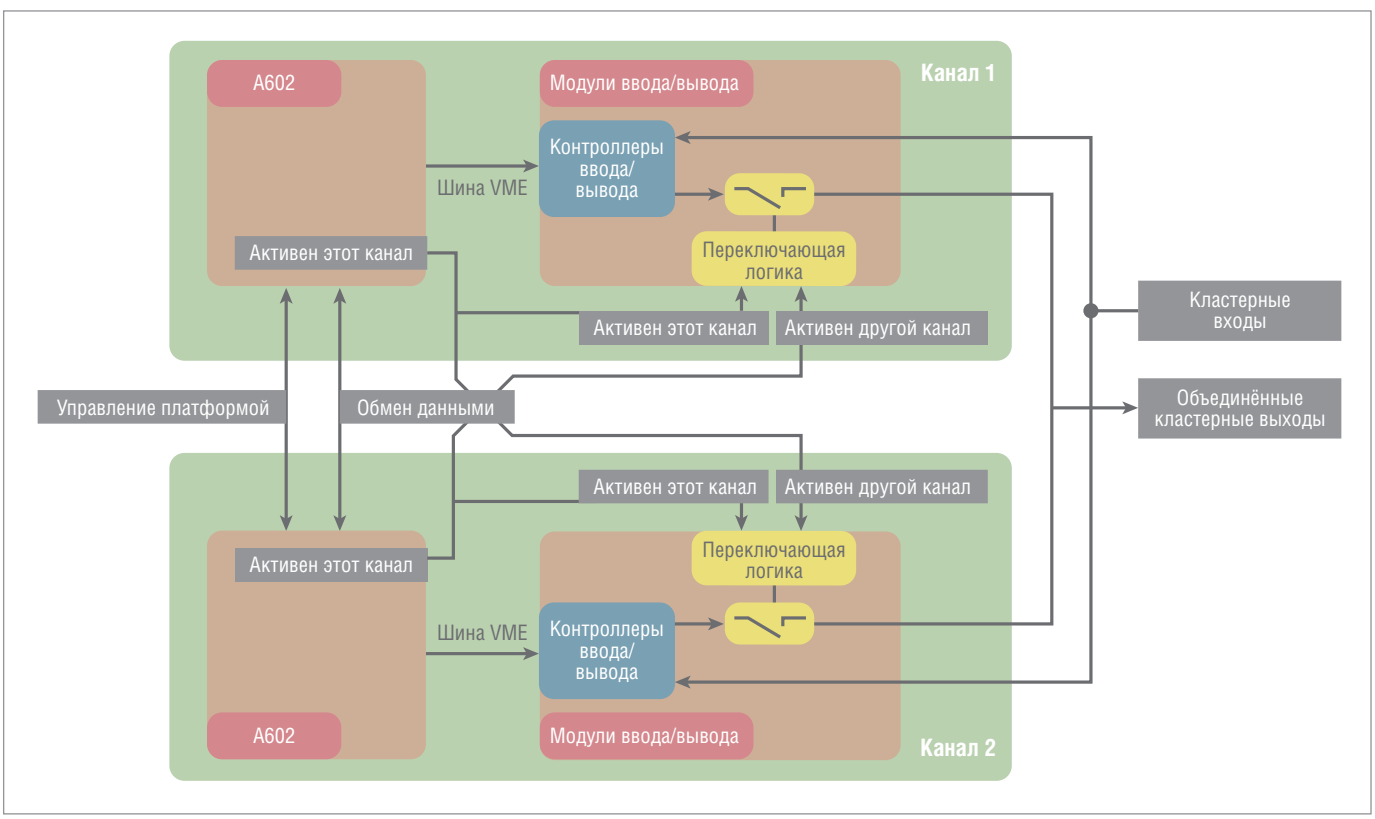

Рис. 6. Две платы VMEbus в виде кластера с одним активным и одним неактивным каналом

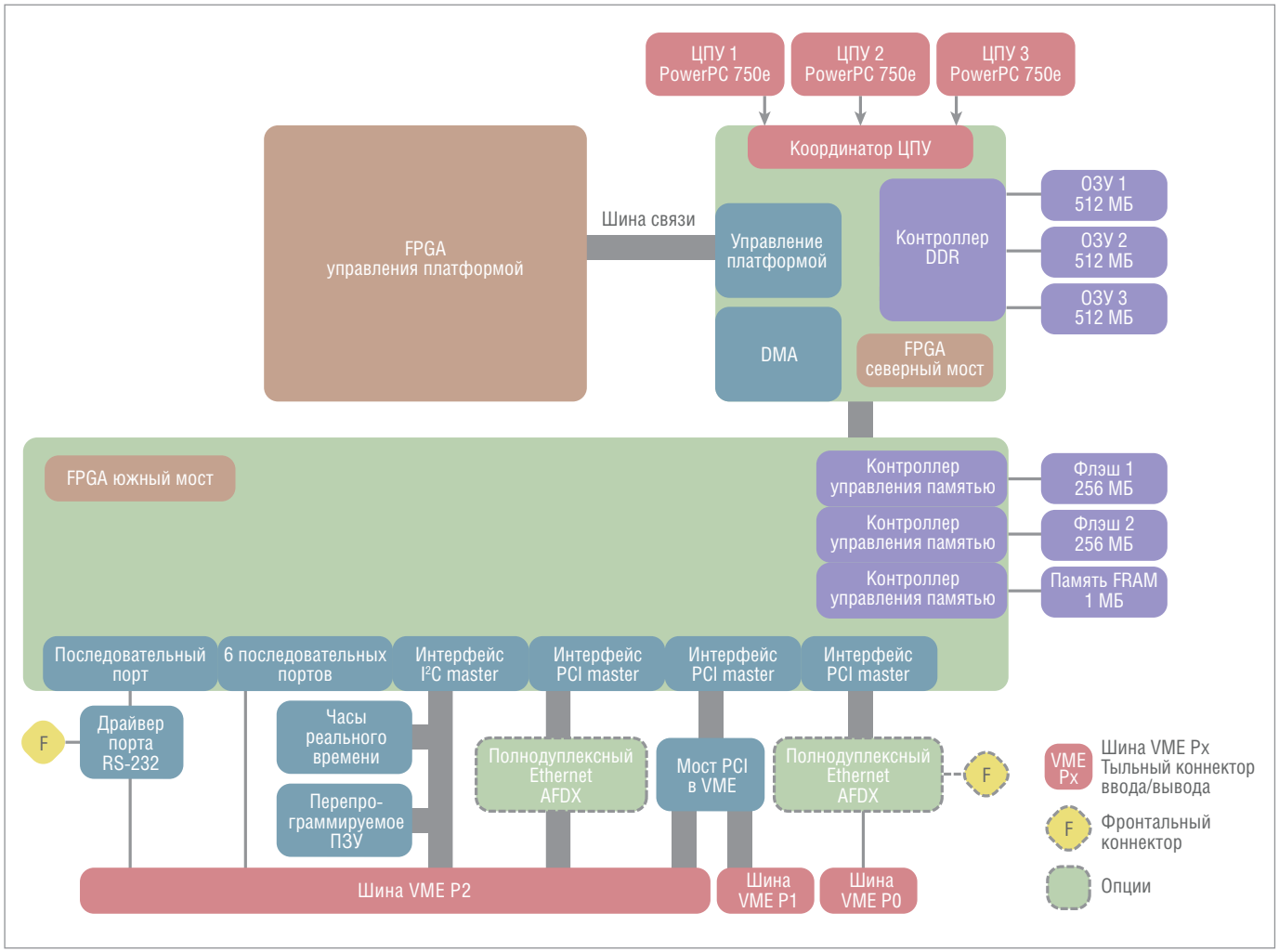

Рис. 7. Внутреннее устройство отказоустойчивой платы с тройным резервированием (2oo3)

следствии в стандарт было добавлено несколько конкретных спецификаций для различных отраслей и областей применения. Соответствующие документы для железных дорог выпустил Европейский комитет по электротехнической стандартизации (CENELEC). К ним относятся EN 50126 RAMS (надёжность, доступность, ремонтопригодность и безопасность железнодорожных систем), EN 50128 (программное обеспечение для систем управления и защиты железных дорог) и EN 50129 (электронные системы безопасности для сигнализации). EN 50129 также содержит точное определение уровней SIL в области железнодорожных применений. Соответствующий уровень SIL выводится из допустимого уровня опасности (THR – Tolerable Hazard Rate) в час и на каждую функцию. Диапазоны значений этой величины составляют для SIL 4 10^{-9}...10^{-8}, а для SIL 1 это 10^{-6}...10^{-5}. В авиационной промышленности стандарты RTCA DO-254 и RTCA DO-178B (EUROCAE ED-12B, руководство по обеспечению качества проектирования бортового электронного оборудования и безопасность программного обеспечения при сертификации бортовых систем и оборудования) определяют пять уровней безопасности, называемых уровнями обеспечения проектирования DAL (Design Assurance Levels) для бортового аппаратного и программного обеспечения. Уровни от DAL-A (самый высокий) до DAL-E в основном перекликаются с уровнями SIL от 4 до 0 (SIL 0 – небезопасные устройства), а также связываются с возможными повреждениями в случае неисправности.

Два примера – железнодорожный транспорт и авиация – очень хорошо представляют крайне жёсткие требования в области безопасности. Они являются одними из самых критичных в этом смысле рынков. Но в любом случае при проектировании электроники разработчики должны учитывать все применимые стандарты, что требует экспертного опыта производителя и его соответствия стандартам качества.

Требования к производителю

Стандарт управления качеством ISO 9001 прочно вошёл в нашу жизнь: ему стараются соответствовать даже небольшие и средние компании. Для квалификации производителей в области требовательных отраслей существуют стандарты, основанные на ISO 9001, но в то же время выходящие далеко за его рамки. Стандарт EN/AS 9100 берёт на себя эту роль для авионики, в то время как международный стандарт железнодорожной промышленности IRIS (International Railway Industry Standard) охватывает железнодорожный рынок. Оба предполагают периодические интенсивные проверки производителей.В идеале, чтобы соответствовать высоким требованиям указанных стандартов качества, производитель должен иметь многолетний опыт работы с соответствующими проектами и готовую необходимую инфраструктуру. Проверки включают анализ всех шагов во всей цепочке создания продуктов. Система оценки поставщиков и управления устареванием компонентов при закупках, прослеживаемость компонентов в производстве, управление рисками в целом – вот лишь некоторые аспекты аудита производителей. Инспекцион-

ные отделы регулярно используют такие методы испытаний, как ускоренный тест срока службы HALT (Highly Accelerated Life Test) и стресс-тест при повышенных нагрузках HASS (Highly Accelerated Stress Screening). Тем не менее, одним из самых серьёзных этапов остаётся разработка. Функциональная безопасность требует наивысшего уровня качества процессов проектирования, позволяющих распознавать и устранять ошибки на ранней стадии создания продукта. Команды разработчиков должны быть полностью вовлечены в борьбу за аспект безопасности, поскольку невозможно сделать разработку безопасной в ретроспективе. Метод проектной работы, называемый V-моделью, поддерживает эту идеологию, регламентируя определённые шаги в соответствии с фиксированной схемой: от требований к спецификации архитектуры на уровне системы и компонентов и через разработку к интеграции и тестированию всех компонентов и системы в целом. Методология также обеспечивает отслеживание и документирование выполнения всех пунктов требований. В течение нескольких лет компания MEN была сертифицирована как по EN 9100, так и по IRIS, и при проектировании описанных здесь продуктов соблюдались все инструкции по авионике (DO-254) и железнодорожному транспорту (EN 50129). Благодаря этому продукты сертифицируются в соответствии с самыми строгими уровнями безопасности: SIL 4 для железных дорог или DAL-A для авионики.

Сертификация компонентов и систем

Сертификация критически важных приложений – это процедура, включающая множество деталей – составных компонентов системы, и, следовательно, является задачей системного интегратора. Если на уровне платы были соблюдены все применимые стандарты и требования и если это было соответствующим образом задокументировано, производитель может облегчить жизнь системному интегратору, предоставив данную документацию. Для интегратора это означает снижение затрат и ускорение выхода на рынок при высоком уровне качества. MEN в настоящее время сертифицирует свой дизайн в соответствии с SIL 4 в сотрудничестве с немецкой организацией TÜV SÜD. На железных дорогах такая сертификация возможна даже для одной платы. Основными стандартами для неё являются EN 50128 (FPGA) и EN 50129 (аппаратные средства).

Клиенты, интегрирующие карту в целостную систему, могут использовать пакет, который включает в себя все необходимые документы по безопасности для этого компонента. Вместе с описанием безопасных условий эксплуатации заказчик получает требуемую стандартом документацию и затем может интегрировать компонент в своё приложение с требуемым уровнем безопасности. Подобный вид сертификации на уровне бортового оборудования невозможен в авионике, где всегда сертифицируется система целиком. Тем не менее, продукты MEN создавались с учётом авиационных регламентов и уже сертифицированы по DAL. Это даёт хорошую основу для дальнейших разработок с их участием. Платы CPU компании MEN поддерживают Sysgo PikeOS и Wind River VxWorks – две сертифицируемые системы реального времени, специально предназначенные для критически важных приложений. Для VxWorks Wind River предлагает платформы, сертифицируемые до DAL-A или SIL 4.

Положить все яйца в одну корзину тоже можно безопасно

Подход с размещением отказоустойчивого компьютера с тройным резервированием на одной плате, которую можно использовать в существующих стандартных системах 6U, является уникальным в отрасли. MEN удалось удовлетворить как высокие требования своих целевых рынков железных дорог и авионики, так и спрос на модульные решения. Платы имеют все функции безопасного компьютера. Благодаря реализации типовых механизмов безопасности на одной плате требуются значительно меньшие программные издержки для переноса приложений, написанных для одного ЦП, или для согласования со встроенным воутером. В сочетании с ноу-хау и комплексным управлением качеством MEN и с оптимальной поддержкой в сертификации эти продукты помогают снизить затраты на создание систем в критически важных для безопасности приложениях. ●

Статья подготовлена по материалам компании MEN Mikro Elektronik

E-mail: textoed@gmail.com

Доломант

ЗАО «НАУЧНО-ПРОИЗВОДСТВЕННАЯ ФИРМА «ДОЛОМАНТ»

ОТВЕТСТВЕННАЯ ЭЛЕКТРОНИКА ДЛЯ ЖЕСТКИХ УСЛОВИЙ ЭКСПЛУАТАЦИИ

100% РОССИЙСКАЯ КОМПАНИЯ

ЗАКАЗНЫЕ РАЗРАБОТКИ

Разработка электронного оборудования по ТЗ заказчика в кратчайшие сроки

- Модификация КД существующего изделия
- Разработка спецвычислителя на базе COM-модуля
- Конфигурирование модульного корпусированного изделия
- Сборка магистрально-модульной системы по спецификации заказчика
- Разработка изделия с нуля

КОНТРАКТНОЕ ПРОИЗВОДСТВО

Контрактная сборка электроники уровней: модуль / узел / блок / шкаф / комплекс

- ОКР, технологические консультации и согласования
- Макеты, установочные партии, постановка в серию
- Полное комплектование производства импортными и отечественными компонентами и материалами
- Поддержание складов, своевременное анонсирование снятия с производства, подбор аналогов
- Серийное плановое производство
- Тестирование и испытания по методикам и ТУ
- Гарантийный и постгарантийный сервис

(495) 232-2033 • WWW.DOLOMANT.RU • (495) 739-0775