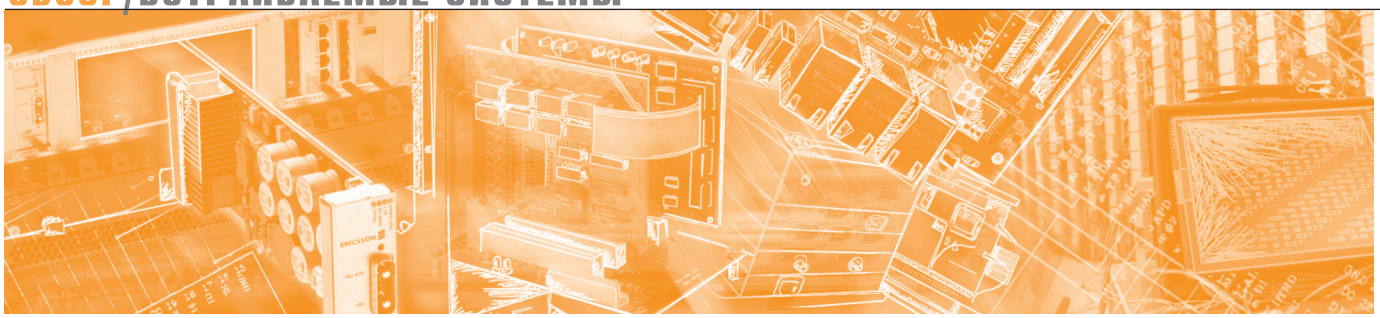


Майкл Хенце

FPGA – гарантия функциональной безопасности

В статье рассматривается вопрос обеспечения функциональной безопасности встраиваемых систем для критически важных приложений. Описан подход компании MEN с применением матриц FPGA, имеющий ряд неоспоримых преимуществ перед традиционными решениями.

Электронные компоненты всегда критически важны для безопасности в тех случаях, когда неисправности или сбои угрожают жизни людей или могут привести к серьёзному экологическому и/или материальному ущербу, поэтому критически важные для безопасности системы всегда должны функционировать надёжно. Необходимой функциональной безопасности можно достичь при помощи логики FPGA (Field Programmable Gate Arrays, или ПЛИС – программируемая логическая интегральная схема).

Зачастую в определённых отраслях промышленности устанавливаются технические требования для критических по безопасности встраиваемых систем, которые соответствуют строгим стандартам. В них нет места ошибкам в аппаратном или программном обеспечении. Типичные применения таких систем – в поездах, автобусах, на кораблях и воздушных судах, они также могут быть составными частями более сложных систем в промышленной автоматизации, медицине, энергетике. В этом контексте фактору функциональной безопасности следует придавать особое значение.

Но возможно ли спроектировать систему таким образом, чтобы она благодаря своей конструкции предусматривала и сводила к нулю все известные риски? Требуется предвидеть также и случайные сбои, вызванные отказами компонентов, влиянием ЭМС или космического излучения, и вероятные ошибки, которых можно избежать при разработке. Можно ли сертифицировать системы в соответствии со стандартами безопасности различных рынков, если на большинство имеющихся стандартных компонентов действие этих стандартов по умолчанию не распространяется?

Самостоятельная проверка обычно занимает очень много времени, особенно если компоненты сложны. Вдобавок иногда она возможна лишь в сотрудничестве с производителем компонентов, что требует погружения в особенности производственных процессов. Но все ли производители компонентов идут навстречу? Зачастую не все, потому что функциональная безопасность является нишевым рынком для большинства поставщиков стандартных компонентов, используемых во встраиваемых компьютерах. Как же разрешить эту дилемму и при этом производить функционально безопасные системы?

Тестирование стандартных компонентов – это дорого

Очень хорошая альтернатива ретроспективному испытанию стандартных компонентов, предусмотренному процедурой сертификации EASA в меморандуме "EASA CM – SWCEH – 001", – это использование матриц FPGA, в которых функции реализованы по-новому и отвечают нормам безопасности соответствующих стандартов. Это решение подходит для точного выполнения критичных по безопасности требований, имеющихся в соответствующих отраслях промышленности. Кроме того, оно позволяет эффективно реализовать специфические потребности клиентов в малых сериях изделий и предлагать их по привлекательным ценам. Данное решение закладывает основу для обеспечения функциональной безопасности в специфических приложениях. Преимущество FPGA заключается в том, что отпадает необходимость перестраивать всю систему. Пересмотру подвергаются по мере необходимости только библиотечные функциональные блоки для построения логики (блоки IP), что позволяет сэкономить как средства, так и время разработки. Такой подход возможен не только для разработки одной специфической FPGA, но и для конструирования платы или системы с несколькими FPGA.

Моделирование ошибок и тестирование корректного поведения

Однако прежде чем критически важная для безопасности конструкция будет подготовлена и сертифицирована, необходимо проанализировать её поведение в критических ситуациях. С инструментами разработки FPGA это сделать сравнительно легко, поскольку для проверки поведения системы в виртуальной

среде разработки FPGA можно моделировать даже серьёзные или сложные ошибки. Такая форма эмуляции является частью процесса разработки FPGA даже в случае, если соответствие требованиям функциональной безопасности не нужно. В этом смысле для FPGA не требуются какие-либо дополнительные усилия. Моделирование также может быть использовано не только для доказательства «правильного» поведения в ошибочных ситуациях, но и для подтверждения корректной реализации требуемой функциональности. Таким образом, на базе эмуляции можно создавать полные отчёты моделирования, которые затем могут быть представлены TÜV или другим сертифицирующим органам.

Расширенные функции мониторинга

Мониторинг надлежащих условий функционирования также играет существенную роль в критически важных для безопасности областях, поскольку это единственный способ обнаружения сбоев и инициирования соответствующих действий. Например, температура и функционирование компонентов или обмен данными должны контролироваться и анализироваться на предмет отклонений от заданных значений, а в аварийной ситуации требуется обеспечить остановку машины или поезда контролируемым образом. Однако готовые компоненты для подключения входных и выходных блоков, такие как последовательные интерфейсы или GPIO (контакты ввода-вывода общего назначения), редко содержат функции мониторинга, необходимые для обеспечения функциональной безопасности, например, в соответствии с EN 50129 для железных дорог или с IEC 61508 для электронных систем с функцией безопасности. Но если нет подходящих микроконтроллеров, такие функции можно очень эффективно реализовать в FPGA. Внедрение функций контроля при помощи FPGA также имеет преимущества перед микроконтроллерами, которые обусловлены свободным конфигурированием и хорошей адаптацией к требованиям конкретного применения.

Долгосрочная доступность и снижение риска морального износа

Высказывание «никогда не изменяйте работающую систему» применимо и к функционально безопасным системам. С одной стороны, расходы на проверку функциональной безопасности в соответствии со стандартами очень большие, и такие проверки должны проводиться повторно каждый раз, когда вносятся изменения, что означает их чрезвычайно высокую стоимость. С другой стороны, при внесении изменений всегда существует риск появления новой ошибки. По этой причине, особенно на железнодорожном транспорте и в авиации, системы используются десятилетиями без изменений. Но это требует наличия стратегии реагирования на старение компонентов, поскольку стандартные компоненты для промышленности редко доступны более 5–10 лет. FPGA и здесь предлагают решающие преимущества. Дело в том, что реализация каждой функции осуществляется не определённым компонентом, а программно. В результате замены компонентов сравнительно безболезненны, ввиду того что программный код можно перенести в новые FPGA, обеспечив идентичную функциональность. Таким образом, продолжительность проекта более чем 30 лет – не проблема, даже если придётся поменять производителя FPGA. Данный подход к тому же обеспечивает независимость от определённого поставщика.

Используя FPGA, всегда можно интегрировать дополнительную функциональность на самой современной платформе, модернизировав систему. Эта гибкость, естественно, имеет значение и в начале жизненного цикла продукта: если некоторые из функций оборудования реализованы в FPGA, то эту часть можно в дальнейшем развивать и модернизировать. Такая стратегия позволяет сэкономить время при последующих пусконаладочных работах и испытаниях всей системы.

Замена компонентов при работе в расширенном температурном диапазоне

Одно из самых общих требований, особенно в критических областях, – поддержка расширенного диапазона рабочих температур, обычно –40...+85°C. Здесь часто возникают проблемы с подбором подходящих стандартных компонентов. Однако в последнее время стало значительно труднее или вообще невозможно найти компоненты для выполнения различных аппаратных функций при работе в сверхширокомдиапазоне –55...+125°C. Надо сказать, что FPGA обеспечивают достаточно широкий диапазон, позволяющий работать и при этих экстремальных температурах.

Лёгкое конструирование систем, невосприимчивых к сбоям

Наиболее важной стратегией снижения риска для системы является избыточность критически важных компонентов, то есть их функционально идентичное умножение. Компонент, отказ которого парализует всю систему, называется единой точкой отказа (SPOF – Single Point of Failure). Любой важный строительный блок системы может превратиться в SPOF. В аэрокосмических приложениях, например, серьёзной проблемой являются ошибки памяти, вызванные космическим излучением. Это приводит к однобитным (SEU – Single Event Upsets) или многобитным (MBU – Multi-Bit Upsets) ошибкам, когда один или несколько битов в элементах памяти меняют состояние от 0 к 1 или наоборот. Если критические компоненты, такие как ЦП, дублированы, это увеличивает функциональную безопасность системы и готовность к работе. Такая избыточность может быть создана с помощью FPGA, преимущество которых в том, что эта логика может быть легко дублирована в каждом экземпляре путём копирования и вставки логических блоков IP. В FPGA это резервирование повторяется и позволяет завершить вычисление, если логика IP FPGA отказывает. В результате на основе флэш-FPGA можно реализовать устойчивую к SEU-ошибкам логику.

Возможности реального времени и гарантированный отклик

В критически важной для безопасности среде в дополнение к надёжности часто требуется предсказуемое время выполнения. Система должна реагировать на внешнее событие за определённое время даже в наихудшем случае. Однако типичные компьютерные архитектуры используют прерывания и топологии DMA (Direct Memory Access), которые могут отрицательно влиять на время исполнения отдельных задач, когда другая задача запрашивает те же ресурсы. Необходимое детерминированное поведение, то есть точно предсказуемое по времени, в этом случае становится труднодостижимым. По этой причине такие решения не используются там, где предъявляются жёсткие требования реального времени. Однако FPGA поддерживают возможности реального времени, поскольку они построены на основе параллельной логики. Это означает, что разные процессы не конкурируют друг

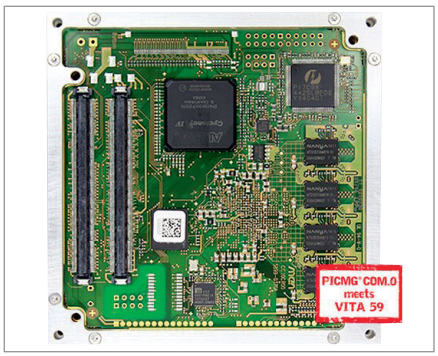


Рис. 1. Матрица FPGA на модуле Rugged COM Express CC10C с процессором ARM i.MX6

с другом, но идут своим собственным предопределённым путём, который не нарушается другими событиями. Это значительно облегчает обеспечение детерминированных возможностей в режиме реального времени с чётко определённым поведением во времени.

Интеграция приложений безопасности

В контексте функциональной безопасности во времена Интернета вещей, Industry 4.0 и Mobility 4.0 рано или поздно возникает проблема безопасности в аспекте защиты от манипуляций. FPGA предлагают множество возможностей для защиты приложения от манипуляций, несанкционированного доступа или дублирования данных. Например, в FPGA может быть запрограммирован уникальный ключ. Там он хранится в зашифрованном виде в энергонезависимой памяти. Этот ключ гарантирует, что доступ к данным смогут получить только приложения и люди, которые его знают. Ключ также может использоваться для идентификации при связи устройства с другими устройствами. Поскольку он прописан аппаратно, им нельзя манипулировать со стороны программного обеспечения, которое всегда однозначно идентифицирует устройство. Код, который реализован в аппаратном обеспечении, не может быть скопирован так же легко, как программное обеспечение. Таким образом, FPGA может добавлять ценные функции безопасности, которые идут намного дальше, чем, например, доверенный платформенный модуль. Мало того, они даже имеют преимущество перед стандартными решениями, потому что, если они запрограммированы индивидуально, они гораздо менее подвержены взлому.

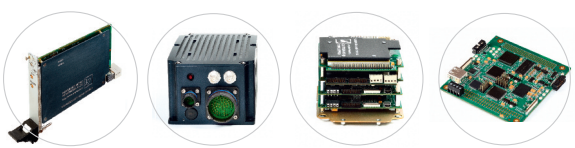
Ограничения FPGA

Несмотря на все перечисленные преимущества, FPGA имеют и ограничения в использовании. С одной стороны, это затраты. FPGA, конечно, дороже, чем стандартные компоненты, производимые крупными партиями. FPGA можно использовать только в ограниченной степени для реализации сложных решений, поскольку, начиная с определённого уровня функциональности, лучше переключиться на комбинацию программного и аппаратного обеспечения: ведь микроконтроллеры и прикладные процессоры уже имеют фундаментальную логику, включая различную функциональность ввода-вывода и интерфейсы, которые для FPGA должны быть разработаны вновь. Тем не менее, конечно, можно сделать многое и с FPGA. Например, в FPGA уже реализована логика x86. Но мы всё ещё далеки от воспроизведения в FPGA всей логики программного обеспечения, которая существует для x86, поэтому преимущества и недостатки должны быть взвешены в зависимости от характера применения и существующих альтернативных стандартных компонентов. В принципе, FPGA пред-

Advanced Micro Peripherals
THE EMBEDDED VIDEO EXPERTS

ADVANCED MICRO PERIPHERALS
20 ЛЕТ ОПЫТА В СФЕРЕ ВСТРАИВАЕМЫХ ВИДЕОРЕШЕНИЙ

- Кодирование в MPEG-4 / H.264 (AVC)
- Захват, запись, вывод на экран и передача многоканальных NTSC/PAL видеопотоков и видеоданных
- Системные решения (COTS) для серверов цифрового видео и цифровых видеомагнитофонов (DVR)
- Специализированные программные комплекты разработчика



PC/104 • PC/104-Plus • PCI/104-Express • CompactPCI • CompactPCI Serial • miniPCI

ProSoft®
ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР
(495) 234-0636
INFO@PROSOFT.RU
WWW.PROSOFT.RU
Реклама

лагают гибкие и безопасные альтернативы практически для всех задач, где на стороне оборудования или программного обеспечения вы давно бы столкнулись с ограничениями развития. Сегодня без логики FPGA не могут обойтись многие приложения, ориентированные на функциональную безопасность (рис. 1).

Разработка функционально безопасных систем

Такие компании, как MEN Mikro Elektronik, специализируются на платформах на базе FPGA для критически важных встраиваемых систем и хорошо знакомы с требованиями конкретных отраслей промышленности. На рис. 2 в качестве примера показана высокопроизводительная плата A25 SBC 6U с 16-ядерным процессором и интерфейсом VME-bus на основе FPGA. Плата используется в большом адронном коллайдере ЦЕРН и считается эталоном безопасности среди разработчиков. В некоторых отраслях промышленности распространена практика, согласно которой разработка FPGA не закреплена в стандартах, но поставщики решений полагаются на результаты моделирования, выполненного с помощью средств разработки FPGA, и документируют их для сертификации. Несмотря на большие усилия, связанные с разработкой, FPGA могут сэкономить значительное время в процессе сертификации, которая иногда более затратна, чем сама разработка. Приносят пользу и уже имеющиеся наработки. Например, у компании MEN есть много функциональных блоков, используемых в сертифицированных приложениях. С одной стороны, они выполняют базовые функции плат, с другой стороны, они реализуют специфические функции ввода-вывода.

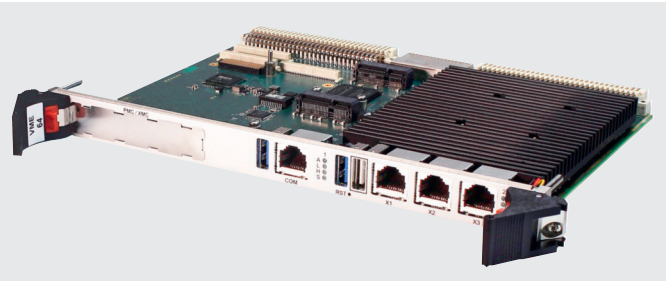
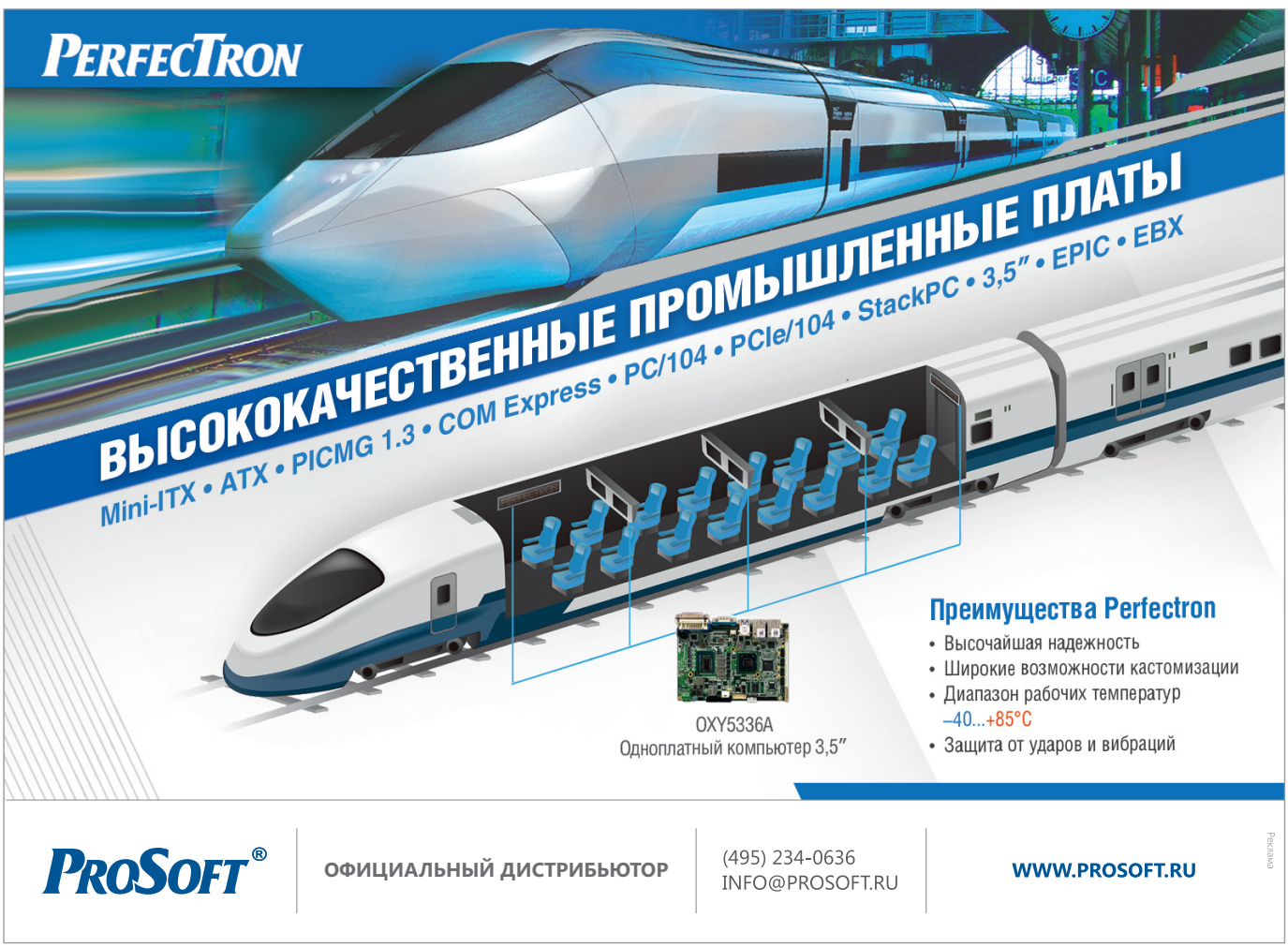


Рис. 2. Высокопроизводительная плата MEN A25 SBC 6U

Строительные блоки IP MEN для FPGA включают:

- графические и сенсорные дисплеи;
- интерфейсы Fieldbus, такие как CAN и MVB;
- различные интерфейсы UART, такие как RS-232 или RS-485;
- интерфейсы Ethernet и HDLC;
- контроллеры SRAM и флэш-памяти;
- GPIO, цифровой ввод-вывод, счётчики, квадратурные декодеры и функции ШИМ.

Все эти IP-блоки могут быть объединены с ядрами, предоставляемыми Altera (Avalon Bus) или сообществом Open Cores Community (Wishbone Bus). Мосты, разработанные MEN, – Wishbone-to-Avalon и Avalon-to-Wishbone – завершают постоянно развивающийся спектр готовых приложений с логикой FPGA, который, конечно же, может быть адаптирован и расширен в соответствии с требованиями заказчика.

Перевод Юрия Широкова
E-mail: textoed@gmail.com