Сюзанна Борншлегл

Функциональная безопасность в стандарте CompactPCI 3U

В статье рассматривается новый подход к построению функционально безопасных систем на основе процессорной платы F75P компании MEN, выполненной на базе трёх процессоров. Данная плата соответствует высшему уровню безопасности SIL 4 и поставляется с полным набором документации, необходимой для сертификации готовой системы. Описанный подход позволяет снизить стоимость и время выхода готового решения на рынок.

Введение

Сейчас в стандарте CompactPCI инновационные продукты достаточно редки. Большинство производителей процессорных плат идут по пути наращивания производительности и увеличения скорости передачи данных в используемых интерфейсах. В отличие от традиционного подхода сейчас появился и новаторский, который реализует скрытые возможности применительно не только к железнодорожным приложениям, но и к другим отраслям.

Ошибки и неисправности оборудования на транспорте могут привести к угрозам для жизни, серьёзным загрязнениям окружающей среды и значительным экономическим потерям. С переходом от аналоговых технологий к современным компьютерным вопросы функциональной безопасности играют всё более серьёзную роль при проектировании электронных систем. Каждый рынок, от автобусного и железнодорожного транспорта до авиации и судоходства, имеет свои собственные критерии функциональной безопасности, опирающиеся на соответствующие стандарты. Компьютерная техника и программное обеспечение должны работать на транспорте надёжно. При этом они должны быть функционально безопасными и устойчивыми к воздействию внешних факторов, таких как воздействие высоких и низких температур, вибрации и т.д. В связи с этим у поставщиков оборудования для транспорта возникает дилемма: с одной стороны, чтобы быть конкурентоспособными, они должны предлагать современные решения, с другой стороны, новые технологии могут значительно увеличивать стоимость продукции, что ведёт к росту тарифов за перевозку и проезд и, в свою очередь, снижает конкурентоспособность данного решения.

Системы в стандарте CompactPCI 3U завоевали популярность на железнодорожном транспорте, так как позволяют получить требуемую функциональность по разумной цене. Модульность, компактные размеры готовых коммерческих плат и их способность работать в жёстких условиях эксплуатации в сочетании с ценовой привлекательностью поддерживают постоянный спрос. На их базе можно строить надёжные и защищённые системы в рамках отраслевых стандартов. Другой причиной широкого применения CompactPCI является возможность реализации резервирования в рамках системы. Существует много вариантов реализации этой функции в зависимости от требований безопасности и надёжности. Возможность «горячей» замены стандартных плат позволяет построить надёжные, удобные в обслуживании системы по приемлемой цене. Можно создать систему с дублированием, троированием процессорных плат, связанных между собой сетевыми интерфейсами. Для определённого уровня требований это может быть хорошим решением. Несмотря на пропорционально увеличивающиеся объём, вес и потребление электроэнергии, суммарные затраты такого решения могут находиться в допустимых пределах. Слабым звеном в этом случае может стать организация сетевого обмена данными. Сети подвержены неисправностям и требуют обслуживания. Грамотная кабельная проводка, а также сами кабели стоят до-

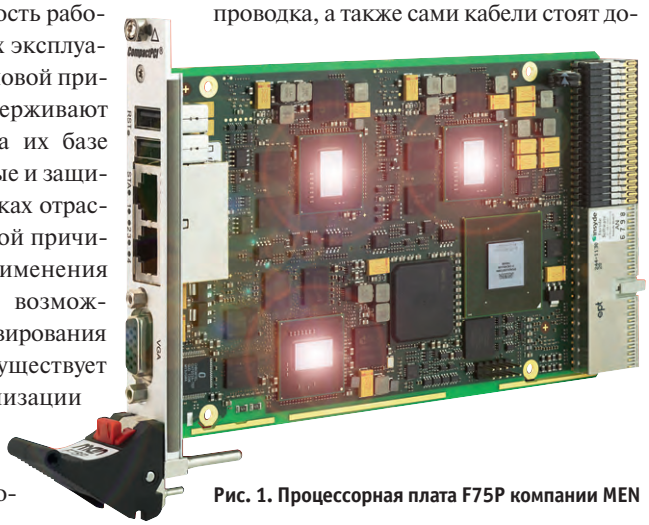

Рис. 1. Процессорная плата F75P компании MEN

рого. При этом надёжная работа сетевого оборудования является неотъемлемым требованием обеспечения функциональной безопасности. Таким образом, разработчикам часто приходится идти на определённые компромиссы в выборе оборудования и архитектуры для обеспечения требований функциональной безопасности.

F75P – процессорная плата для задач с высоким уровнем функциональной безопасности

Новая плата компании MEN в формате 3U CompactPCI способна помочь уйти от компромиссов к новому уровню функциональной безопасности электроники. Защищённое исполнение, высокая надёжность, компактные размеры, модульная конструкция и невысокая цена – эти классические атрибуты получают новые возможности вместе со встроенным резервированием. Процессорная плата **MEN F75P** (рис. 1) спроектирована с использованием трёх процессоров: два из них служат для организации резервирования, а третий – для организации функций ввода-вывода. Блок-схема процессорной платы F75P представлена на рис. 2. Внутренние соединения по Ethernet позволяют сократить количество кабелей. На переднюю панель выводятся интерфейсы Ethernet, USB и графики, на задней панели доступны все интерфейсы в соответствии со стандартом PICMG 2.30 (CompactPCI Plus IO). За всеми внешними атрибутами скрывается главная ценность платы: она оптимизирована для обеспечения функциональной безопасности.

Типовым вариантом использования двух процессоров является запуск одной и той же логики приложения на каждом из них. Оба процессора формируют выходные данные, значения которых сравниваются между собой для определения расхождений. Но возможности платы не ограничиваются описанной стратегией сравнения данных. Системный интегратор имеет полную свободу действий, правда, это означает и увеличение работы по программированию функции арбитра. С другой стороны, гибкость позволяет снизить затраты: можно применять разные алгоритмы арбитража на базе одной и той же электроники. Для обеспечения более низкого уровня безопасности **SIL** (Safety Integrity Level) можно применять более простые алгоритмы, в то время как для обеспечения максимального уровня **SIL 4** надо использовать более сложные и комплексные алгоритмы. Гибкость также проявляется и в выборе программного обеспечения: можно использовать уже готовые стандартные программы, которые будут работать под разными или одинаковыми операционными системами на каждом процессоре. Плата F75P поддерживает операционные системы реального времени, такие как VxWorks и PikeOS, применяемые для ответственных задач, а также стандартную ОС Linux. К процессору ввода-вывода можно подключать датчики, а также реализовать функционально небезопасные приложения, например, вывод графической информации. Для комфортного программирования графических приложений этот процессор поддерживает операционную систему Windows.

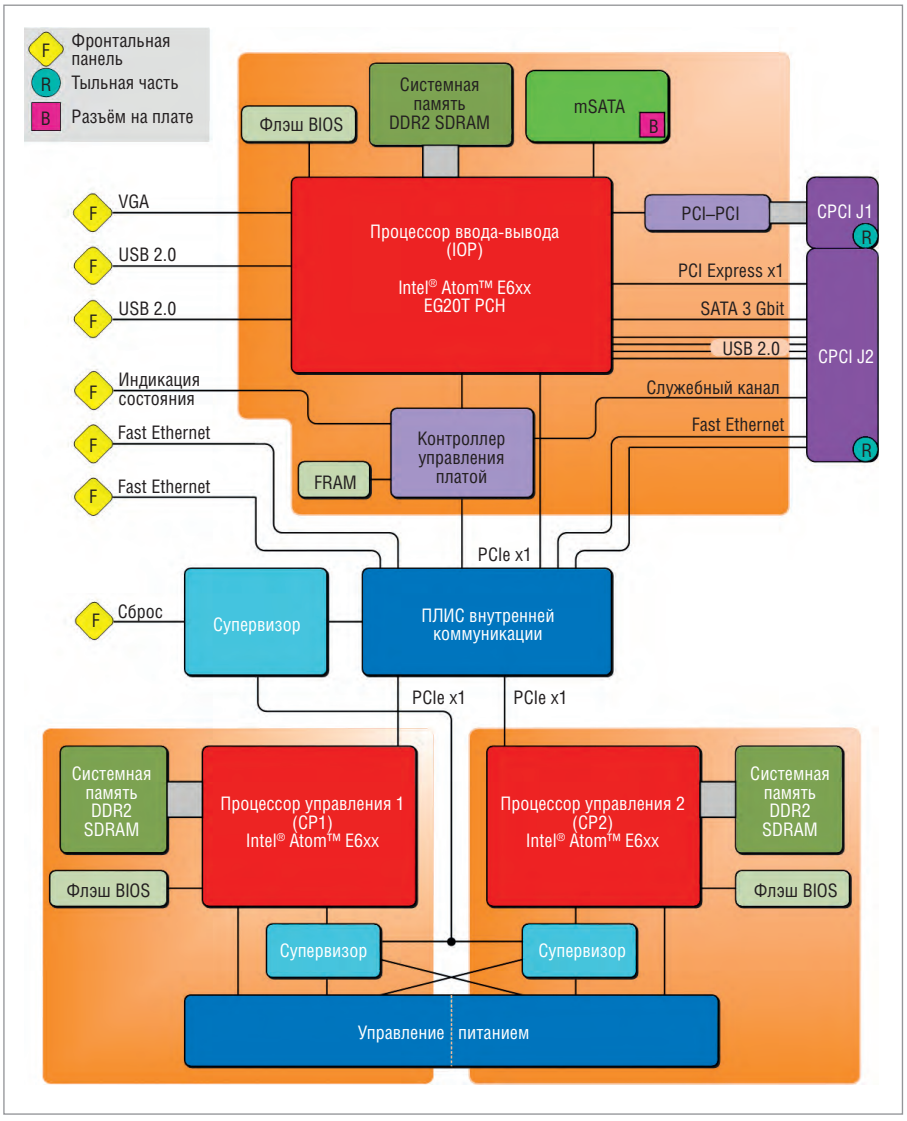

Рис. 2. Блок-схема процессорной платы F75P с двумя резервируемыми процессорами и одним процессором ввода-вывода

В дополнение к преимуществам применения трёх процессоров можно сказать, что новая 3U-плата F75P имеет ряд функциональных особенностей, обеспечивающих необходимый уровень функциональной безопасности. Для начала укажем на то, что процессорная плата может полностью отключаться. Это очень важно. При возникновении ошибки система должна быть отказоустойчивой или иметь режим «остановка без уведомления», то есть переходить в безопасное состояние, что означает полное отключение процессоров. Многие стандартные процессорные платы в случае возникновения неисправности либо переходят в состояние сброса, либо перезагружаются. Плата F75P способна выполнять любое из этих действий, в зависимости от конфигурации аппаратных средств.

Кроме того, имеются независимые супервизоры для каждого процессора. Они проверяют, чтобы такие параметры, как напряжение питания, температура, рабочая частота были в допустимых диапазонах. Они регистрируют

также ошибки каждого процессора. Каждый супервизор, а также программное обеспечение процессоров могут переводить платы в безопасный режим. Для быстрого поиска неисправности и её устранения ведётся журнал событий в энергонезависимой памяти FRAM. Записи в журнале обычно регистрируют аппаратные события, но программное обеспечение, в свою очередь, может инициировать запись других событий, что позволяет сделать протокол более полным и удобным, ведь ошибки дополнительного оборудования, которые могут привести к отключению системы, могут быть зарегистрированы только программным обеспечением.

Полная информация о поведении компонентов системы применительно к критическим задачам важна, так как их поведение должно быть предсказуемым. Инженеры должны рассматривать наихудшие сценарии ещё на ранней стадии проектирования. Ошибки должны быть обнаружены до того, как они смогут нанести вред системе. Следовательно, для достижения необходимого уровня безопасности коммерческая процессорная плата должна быть детерминированной. Для F75P это был вызов, так как она выполнена на базе процессоров Intel Atom E6xx, поддерживающих существующую популярную архитектуру x86. Для достижения требований по точному определению времени исполнения программного кода, были заблокированы такие технологии, как Hyper Threading и SpeedStep. Они позволяют обрабатывать несколько операций параллельно, кроме того, изменяют частоту процессора. Функции прерывания также заблокированы. Как упоминалось ранее, плата предназначена для работы с операционными системами жёсткого реального времени VxWorks или PikeOS, гарантирующими детерминированное поведение. Среди прочего в них оптимизирован процесс работы с памятью и выполнения команд для получения минимальной задержки, так что система остаётся полностью предсказуемой.

Режим «кластер» для увеличения надёжной работы системы

В то время как все описанные ранее меры направлены на повышение уровня функциональной безопасности, схема организации резервирования не приводит к увеличению доступности системы. Но необходимо соблюдение требования доступности в случае, если система не должна отключаться полностью при возникновении неисправности. Например, освещение поезда не должно отключаться при аварийной остановке поезда в туннеле. Чтобы получить высокий коэффициент доступности системы, можно создать кластерную систему путём её удвоения, делая вторую систему доступной в качестве резервного блока: одна система доступна, в то время как другая находится в режиме ожидания. Если активный канал неисправен, то система переключается на второй. Такая организация кластерной системы представлена на рис. 3.

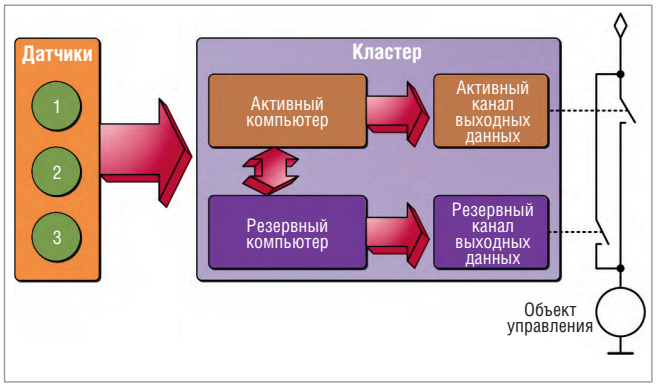

Рис. 3. Организация кластерной системы

Для получения данного функционала в F75P заложена логика управления ролями при совместной работе двух плат. В этом случае процессорные платы общаются через кросс-панель CompactPCI без использования дополнительных кабелей. Они используют интерфейс RS-422 для связи между двумя контроллерами управления платами (BMC – Board Management Controller), которые могут переключать плату в активный или резервный режим работы.

Сертифицируемый продукт

При реализации функций безопасности системным интеграторам не придётся во всех случаях изобретать велосипед. Наоборот, многие определённые в стандартах требования характерны для различных рынков. Как правило, чем более критичны вопросы функциональной безопасности, тем более полны и требовательны отраслевые стандарты. На железнодорожном транспорте электроника должна быть сертифицирована по определённому уровню безопасности SIL, для самого высокого из которых SIL 4 предусмотрена низкая вероятность отказа в соответствии со стандартом EN 50129. Соответствующее требование является одним из немногих элементов данных, которые необходимы системным интеграторам при сертификации. Вся процедура состоит из множества деталей. Для системных интеграторов на железнодорожном транспорте, строящих проекты на базе F75P, важно, что плата поставляется с полным набором документов, в том числе и сертификатом соответствия SIL4 от German TÜV SÜD и требуемым обоснованием безопасности. Плата разработана в соответствии с IEC 61508, EN 50129 и EN 50128 и полностью соответствует стандарту EN 50155 для электроники, применяемой на железных дорогах. Таким образом интеграторы получают более низкую стоимость работ по сертификации и уменьшение времени выхода на рынок конечного продукта с высоким качеством– безусловно, это уникальное преимущество по сравнению со стандартными коммерческими платами.

Поддержка операционных систем

Обеспечение функциональной безопасности в полной мере невозможно без поддержки соответствующих сертифицированных операционных систем. На данный момент доступны стандартные инструментальные средства для разработки встраиваемого ПО (BSP) для QNX и PikeOS. Для снижения затрат на разработку приложений в стандартную поставку входит комплект поддержки процессорной платы BSP (Board Support Package) для безопасной ОС QNX. При работе с безопасной операционной системой (Safe QNX Kernel) гарантируется, что неправильная информация с неисправного процессора не пройдёт к исполнению (режим «остановка без уведомления»), а также система в целом будет отключена при возникновении неисправности, например, во время работы поезда (отказоустойчивость). Процессор ввода-вывода не работает с безопасной операционной системой. Он расположен внутри так называемого чёрного канала. Протоколы коммуникации, разработанные в соответствии с EN 50159, позволяют сделать безопасной коммуникацию между управляющим блоком и периферийными устройствами. F75P поставляется вместе с пакетом сертификации для оборудования и операционной системы (QNX + BSP),

который удостоверяет соответствие требованиям SIL 4 и включает в себя отчёт об оценке, обоснование безопасности, руководство пользователя по безопасности и сертификат TÜV SÜD.

Для PikeOS доступен тестовый комплект BSP. Полный комплект BSP доступен у поставщика операционной системы – компании Sysgo. Комплекты BSP для других операционных систем: Wind River VxWorks Cert и Green Hills INTEGRITY – доступны по запросу. Поддержка Linux осуществляется без BSP, но с предоставлением адаптированных драйверов и документации, подробно описывающей функционал платы.

Заключение

MEN имеет большой опыт в разработке оборудования для железнодорожной отрасли. Имея сертификат IRIS (International Railway Industry Standard – международный стандарт для железных дорог), MEN постоянно улучшает процессы разработки и производства своей продукции. Кроме того, многолетний опыт разработки систем в стандарте CompactPCI придал дополнительный импульс менеджерам MEN по развитию продуктовой линейки. Новая плата F75P в формате CompactPCI как раз и служит хорошим доказательством этого. Перспективный дизайн платы вкупе с хорошей документированностью делают этот инновационный компьютер готовым к работе на подвижном составе. Ноу-хау поставщика и оптимальная поддержка в сертификации, компактные размеры компьютера и возможность гибкого резервирования позволяют системным интеграторам реализовать новые идеи по построению функционально безопасных систем.

Плата может интегрироваться в существующие 19-дюймовые системы CompactPCI, а также использоваться для реализации новых проектов. С этим решением также можно идти в такие отрасли, как медицина и автоматизация, где всё более и более возрастают требования к функциональной безопасности. Но самое главное, применение F75P позволяет снизить издержки при построении систем для ответственных применений. ●

Автор – сотрудник MEN Mikro Elektronik
Авторизованный перевод Алексея Пятницких, сотрудника фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Новости ISA

Указом Президента Российской Федерации от 14.08.2014 года № 568 «О государственных наградах Российской Федерации» президент ГУАП, глава представительства ISA в Российской Федерации, доктор технических наук, профессор Анатолий Аркадьевич Оводенко за большой вклад в развитие науки, образования, подготовку квалифицированных специалистов и многолетнюю плодотворную деятельность награждён орденом Александра Невского. Члены Российской секции ISA сердечно поздравили главу представительства ISA в Российской Федерации, почётного члена ISA А.А. Оводенко с высокой государственной наградой.

В сентябре 2014 года впервые в истории ISA прошли Интернет-выборы в руководящие органы ISA. Каждый член ISA получил возможность проголосовать через Интернет. Результаты голосования опубликованы 9 октября 2014 года. Президентом-секретарём избран господин James W. Keaveney (Emerson Process Management, США), набравший 62,5% от общего числа голосов. Членами Исполкома ISA избраны двое представителей округа 12: господин Brian Curtis (DPS Engineering Ltd, Корк, Ирландия) и господин William D.Walsh (Университет Корка, Ирландия).

В октябре прошли выборы президента-секретаря Российской секции ISA. В результате голосования на этот пост избрана проректор ГУАП Любовь Александровна Тимофеева. Она вступит в должность президента секции 1 января 2016 года.

Международное общество автоматизации ISA приобрело современный популярный электронный информационный ресурс Automation.com. По статистике, популярный сайт посещают более 100 000 пользователей в месяц.

В связи с семидесятилетием со дня рождения Президент Российской секции ISA Юлия Анатольевна Антохина вручила двум профессорам ГУАП, докторам технических наук, активным членам Российской секции ISA Леониду Андрониковичу Осипову и Анатолию Павловичу Ястребову памятные медали «20 лет ISA в России».

Почётным дипломом ISA в связи с 75-летием награждён секретарь Российской секции ISA, доцент ГУАП, кандидат технических наук Михаил Александрович Волохов. ●