ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

СЮЗАННА БОРНШЛЕГЛ (SUSANNE BORNSCHLEGL)
MEN Mikro Elektronik

ПЕРЕВОД: АЛЕКСЕЙ ПЯТНИЦКИХ
info@prosoft.ru

Ошибки и неисправности оборудования на транспорте могут привести к угрозам для жизни, серьезным загрязнениям окружающей среды и значительным экономическим потерям. К используемым на железнодорожном (ж/д) транспорте электронике и компьютерной технике предъявляются повышенные требования. Компания MEN, имеющая большой опыт в разработке оборудования для ж/д отрасли, выпустила плату F75P в формате 3U CompactPCI, которая демонстрирует новый уровень функциональной безопасности.

Основным способом повышения надежности систем, а также обеспечения их функциональной безопасности является резервирование (дублирование, троирование). Важной причиной широкого применения стандарта CompactPCI для ж/д транспорта является возможность резервирования в рамках системы. Существует много вариантов реализации этой функции в зависимости от требований безопасности и надежности. Возможность «горячей» замены стандартных плат позволяет построить надежные, удобные в обслуживании системы по приемлемой цене. Можно создать систему с дублированием, троированием процессорных плат, связанных между собой сетевыми интерфейсами. Несмотря на пропорционально увеличивающиеся объем, вес и потребление электроэнергии, суммарные затраты такого решения лежат 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 дорого. При этом надежная работа сетевого оборудования является неотъемлемым требованием обеспечения функциональной безопасности. Таким образом, разработчикам часто приходится идти на определенные 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 — F75P в формате 3U CompactPCI (рис. 1) — спроектирована с использованием трех процессоров: два из них служат для организации резервирования, тре-

РИС. 1. ▶
Процессорная плата F75P компании MEN

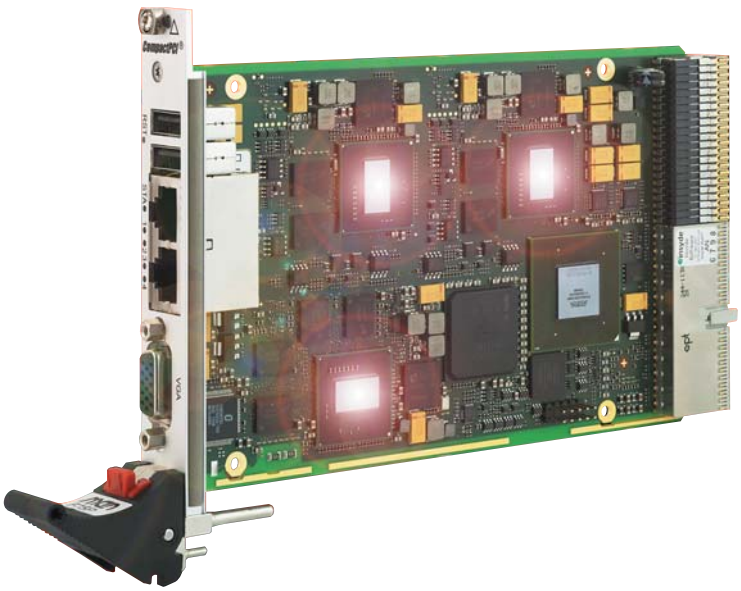
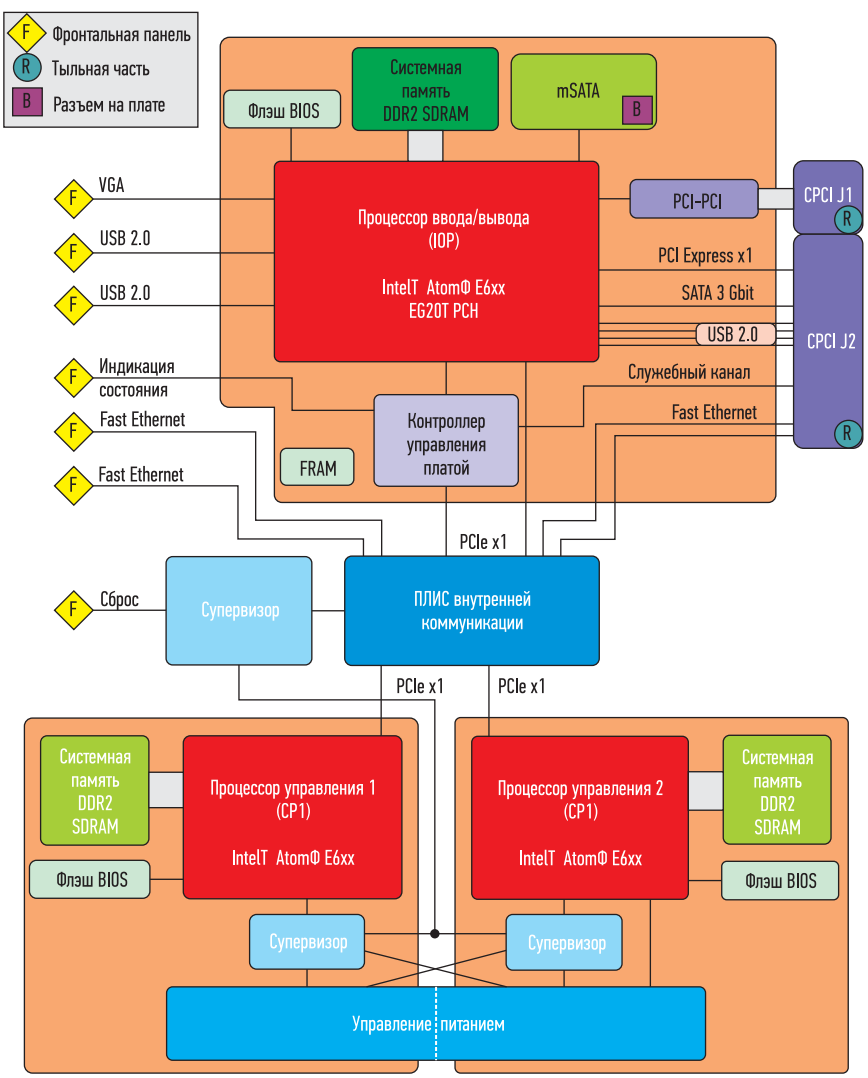


РИС. 2. ▼
Блок-схема процессорной платы F75P с двумя резервируемыми процессорами и одним процессором ввода/вывода



тий — 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 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 (ПО): можно использовать уже готовые стандартные программы, которые будут работать под разными или одинаковыми операционными системами на каждом процессоре. К процессору ввода/вывода можно подключать датчики, а также реализовать функционально небезопасные приложения, например вывод графической информации.

Отметим, что, в дополнение к преимуществам применения трех процессоров, новая 3U-плата F75P 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 неис-

правности 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. Также они регистрируют ошибки каждого процессора. Каждый супервизор, а также ПО процессоров могут переводить платы в безопасный режим. Для быстрого поиска неисправности и ее устранения ведется журнал событий в энергонезависимой памяти FRAM. Записи в журнале обычно регистрируют аппаратные события, но ПО, 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 ПО.

Полная информация о поведении компонентов системы применительно к критическим задачам важна, так как их поведение должно быть предсказуемым. Инженерам следует рассматривать наихудшие сценарии еще на ранней стадии проектирования, поскольку ошибки необходимо фиксировать еще 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.

РЕЖИМ «КЛАСТЕР» ДЛЯ УВЕЛИЧЕНИЯ НАДЕЖНОЙ 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 не должно отключаться при аварийной остановке поезда в туннеле. Чтобы получить высокий коэффициент доступности системы, можно создать кластерную систему путем ее 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.

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 (Board Management Controller, BMC), которые могут переключать плату в активный или резервный режим работы.

СЕРТИФИЦИРУЕМЫЙ ПРОДУКТ

При реализации функций безопасности системным интеграторам не придется во всех случаях изобретать велосипед. Наоборот, многие определенные в стандартах требования характерны для различных рынков. Как правило, чем более критичны вопросы функциональной безопасности, тем более полны и требовательны отраслевые стандарты. На ж/д транспорте электроника должна быть сертифицирована по определенному 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 ж/д транспорте, строящих проекты на базе F75P, важно, что плата поставляется с полным набором документов, в том числе с сертификатом соответствия SIL4 от German TU V SU D 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 является преимуществом по сравнению со стандартными коммерческими платами.

ЗАКЛЮЧЕНИЕ

Имея сертификат IRIS (International Railway Industry Standard — международный стандарт для железных дорог), компания MEN постоянно улучшает процессы разработки и производства своей продукции. Перспективный дизайн платы F75P в формате CompactPCI вкупе с хорошей документированностью делают этот инновационный компьютер пригодным 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" системы CompactPCI, а также использоваться для реализации новых проектов. Это решение также может быть востребовано в таких отраслях, как медицина и автоматизация, где все более и более возрастают требования к функциональной безопасности. Не менее важен и тот факт, что применение F75P позволяет снизить издержки при построении систем для ответственных применений. ⬣

РИС. 3. ▼ Организация кластерной системы