



Открытая системная архитектура для управления поездами

Открытые стандарты несут массу выгод в различных областях автоматизации. Особо заметны они, когда речь идёт о проектировании надёжных и безопасных систем, в частности, автоматики для подвижных составов и путей сообщения железных дорог. На примере модульной платформы *openTCS* в статье рассказано о преимуществах подхода к конструированию систем для железнодорожного транспорта на основе предварительно сертифицированных стандартных блоков.

Применение открытых стандартов для электронных систем управления в поездах позволяет сделать аппаратное и программное обеспечение независимыми от поставщика и, таким образом, даёт свободу выбора поставщиков и технических решений. Кроме того, открытые технологии помогают избежать возможных проблем с функциональной совместимостью и являются решающим фактором в предотвращении серьёзных проблем, вызванных старением, то есть гарантируют достаточно долгий жизненный цикл систем. Основная идея применения открытых отраслевых стандартов – вытеснение старых проприетарных систем, все ещё доминирующих на рынке железных дорог.

Внедрение в Европе ETCS (European Train Control System – Европейская система управления движением поездов) вкупе со стандартизированной системой передачи данных GSM-R (глобальная система мобильной связи на железных дорогах) должно положить конец пестроте технических реализаций систем управления поездами. Но даже здесь широта интерпретации спецификаций ETCS приводит к таким различиям в реализации у поставщиков, что цель трансграничной функциональной совместимости всё ещё не достигнута.

И здесь возникает проект *openETCS*, инициированный компанией Deutsche Bahn. Цель проекта *openETCS* – обеспечить стандартизованную среду разработки для моделирования, тестирования и валидации, а также упростить внедрение будущих систем ETCS.

В то время как ETCS и *openETCS* продвигают стандартизацию в отноше-

нии внедрения, программного обеспечения и коммуникаций, аппаратные средства разных поставщиков систем по-прежнему в основном остаются проприетарными, а значит, несовместимыми между собой.

Это приводит к тому, что компьютерные системы не только требуют высоких первоначальных затрат на разработку, но они также дороги в эксплуатации в течение всего жизненного цикла. Операторы привязаны к поставщикам системы, а расширения или запасные части доступны только у одного поставщика.

Использование стандартных, открытых и предварительно сертифицированных компьютерных модулей поможет как поставщикам систем, так и операторам. Поставщики систем всё ещё могут оградить себя от конкуренции за счёт создания собственных систем и программного обеспечения, однако им больше не нужно будет заботиться о совместимости оборудования. При этом они могли бы ускорить выход своей продукции на рынок. А вот операторам (владельцам) систем это даст ещё больше преимуществ: они смогут приобретать запасные части и расширения системы у разных поставщиков, если те соответствуют стандарту. Таким образом, расходы на запасные части, а вместе с ними и общие затраты на жизненный цикл систем будут уменьшаться.

ОБЯЗАТЕЛЬНОСТЬ СОБЛЮДЕНИЯ СТАНДАРТОВ

Итак, необходимо новое поколение критически важных для безопасности модульных систем управления и конт-

роля, основанных на открытых отраслевых стандартах. Как и ранее созданные системы, они должны быть очень надёжными, рассчитанными на работу в течение многих лет в суровых условиях, характерных для железнодорожного сектора.

Как проектировать такие системы, частично описано, например, в стандарте EN 50155. Он предусматривает требуемую устойчивость к экстремальным температурам и быстрым её изменениям, вибрации, ударным нагрузкам и электромагнитным помехам, но этого недостаточно.

СТАНДАРТЫ SIL

Системы, в которых ошибка или отказ могут нести опасность для жизни человека или для окружающей среды, или вызывать большие финансовые потери, должны соответствовать особым требованиям к функциональной безопасности. (SIL – Safety Integrity Level, или уровень полноты безопасности рассматривает опасные ситуации отказов, которые приводят к авариям, катастрофам и человеческим жертвам. – *Прим. пер.*) К таким системам относятся и компьютеризированные системы для безопасного управления поездами, которые должны соответствовать обширным международным требованиям безопасности EN 50128/IEC 62279 для программного обеспечения и EN 50129/IEC 62425 для аппаратного обеспечения.

Обеспечение доказательств соблюдения этих требований не является ни простой, ни быстрой задачей для производителя.

СЕРТИФИКАЦИЯ – «УБИЙЦА ПРОЕКТОВ»

В новом проекте разработка необходимой документации на соответствие стандартам безопасности может удвоить или даже утроить финансовые затраты, а также продолжительность его выполнения. Соответствующие спецификации функциональной безопасности на железнодорожном рынке включают критерии RAMS (надёжность, доступность, управляемость, безопасность) EN 50126/EN 50128 для программного обеспечения и EN 50129 для аппаратного обеспечения. Все они требуют больших усилий по документированию, которые поставщики решений предпочитают свести к минимуму.

ПРЕДВАРИТЕЛЬНАЯ СЕРТИФИКАЦИЯ ОБОРУДОВАНИЯ

Стратегическим ходом для значительного сокращения усилий по документированию является использование предварительно сертифицированного оборудования, поскольку оно в значительной степени основано на стандартизированных технологиях.

Таким образом, если предположить, что существует поставщик решений с конкретными знаниями о требованиях соответствия стандартам 501xx, можно было бы делегировать эту часть документации непосредственно поставщику.

Вследствие этого у вас появятся два преимущества: во-первых, это позволит снизить расходы на производство внутренней документации, во-вторых, это сэкономит драгоценное время, которое в конкурентной борьбе за самые инновационные решения является одним из наиболее важных факторов, – тот, кто первым выходит на рынок, имеет самые большие рыночные возможности, пользуется эксклюзивностью и может диктовать ключевые стандарты.

Внимание здесь должно быть сосредоточено на открытых и модульных системах: именно они позволяют реализовать гибкие конфигурации для различного использования в поездах или на железных дорогах. Заменяя лишь отдельные модули, а не полные системы, вы снижаете также затраты на техническое обслуживание, поэтому открытые стандарты, безусловно, являются существенным вспомогательным фактором и для поддержания уже сертифицированной системы в рабочем состоянии как можно дольше.

COMPACTPCI – ХОРОШЕЕ РЕШЕНИЕ

Модульные платформы COTS, основанные на стандарте CompactPCI от PCI Industrial Manufacturing Group (PICMG), которые поддерживаются с 1997 года и специально спроектированы для разработки чрезвычайно прочных модульных конструкций с пассивными объединительными панелями, в целом соответствуют требованиям надёжности. Тем не менее, стандарт описывает только основные технологии и не включает в себя сертификацию и документацию, предусмотренные EN 50155 и EN 50126, EN 50128 и EN 50129. Несмотря на это от использования таких модульных COTS-платформ поставщики решений получают большую выгоду, поэтому существует необходимость распространить этот стандарт на железнодорожные технологии.

СИСТЕМА УПРАВЛЕНИЯ MEN TCS: БЕЗОПАСНОСТЬ И СТАНДАРТИЗАЦИЯ

Хорошим примером стандартизованного решения является новая модульная система контроля поездов menTCS, совместимая с EN 50155 и основанная на CompactPCI. Она предлагает все преимущества, которые имеют признанные отраслевые стандарты. Решение хорошо подходит для критически важных железнодорожных приложений и предварительно сертифицировано до SIL 4 в соответствии с EN 50126, EN 50128 и EN 50129. Благодаря своей модульной конструкции оно может быть адаптировано для любых типов применений. Например, в подвижном составе menTCS – отличное решение

для автоматического управления поездом (ATO), автоматической защиты поездом (ATP) или точного управления поездом (PTC) и усиленного контроля поездом (ETC). В путевых приложениях оно может использоваться для управления сигналами и переключениями до уровня безопасности SIL 4 (рис. 1).

Архитектура системы menTCS

Сердцем системы является центральный контроллер MN50C. Он обеспечивает основную логику управления в виде предварительно сертифицированной многопроцессорной платы на базе CompactPCI и может быть настроен на использование до 6 карт расширения в зависимости от требований приложения. Кроме того, доступно до 63 модульных ячеек ввода/вывода menTCS для подключения удалённых входов/выходов к центральному контроллеру. Это важно для установок в высокоскоростных поездах, где каждому пассажирскому вагону нужен свой блок ввода/вывода для подключения датчиков и приводов. Концепция модульного расширения также удобна для таких устройств, как системы сигнализации, где модули ввода/вывода menTCS могут использоваться для управления определёнными участками железной дороги по мере необходимости.

В этом случае устройства ввода/вывода menTCS подключаются через шину кольцевой топологии на основе Ethernet. Это не только упрощает соединение, но и значительно повышает надёжность, поскольку используется избыточный канал связи.

Компоненты модульной концепции семейства, сертифицируемые отдельно,



Рис. 1. Сертифицированная система управления движением SIL 4 MEN основана на открытом стандарте CompactPCI

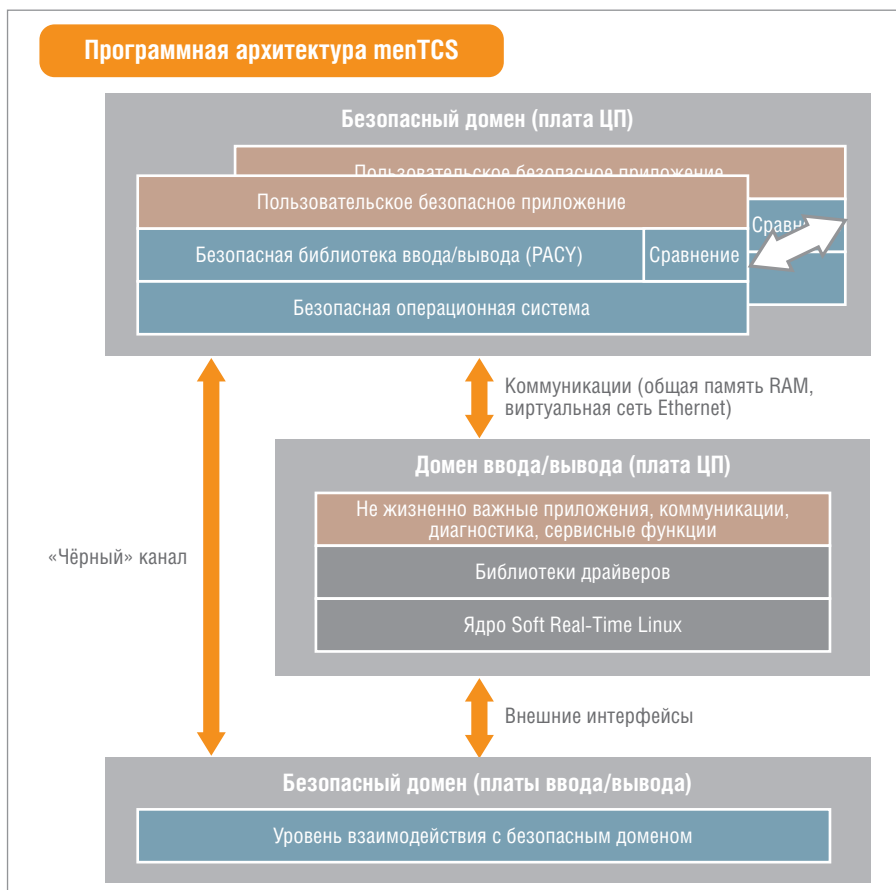


Рис. 2. Платформа menTCS является первой в мире системой, не зависящей от конечного приложения

при необходимости могут упростить разработку полностью сконфигурированных 19-дюймовых систем.

Гибкость расширения и интерфейсов

Модульная концепция ввода/вывода стандартизированной архитектуры menTCS обеспечивает разработчикам большую гибкость и позволяет им посредством карт стандарта CompactPCI легко оснастить контроллер и удалённые блоки ввода/вывода коммуникационными интерфейсами. Для подключения к сети TCN можно использовать интерфейсные платы MVB. Дополнительные бортовые компоненты и блоки управления могут быть подключены через RS-485, CAN, ProfiNet и другие полевые шины. Для подключения IoT доступны WLAN, GSM-R, GPS, GLONASS или Galileo, а также возможна работа через стандартные маршрутизаторы и коммутаторы Ethernet.

Масштабируемая безопасность

Поскольку все критически важные для безопасности модули menTCS предварительно сертифицированы на самый высокий уровень безопасности SIL 4 в соответствии с EN 50128 и EN 50129,

они отвечают всем требованиям, которые могут возникать в критически важных для железных дорог приложениях, от SIL 2 для систем АТО до SIL 4 для сигнализации. Это позволяет разработчикам сосредоточиться исключительно на программном обеспечении, избавляя от забот об аппаратной части. В зависимости от конечного приложения уровень безопасности оборудования может быть определён в любое время и без дополнительных инженерных усилий.

Безопасные домены упрощают разработку программного обеспечения

Аппаратная платформа menTCS разработана таким образом, что программное обеспечение для управления безопасностью строго изолировано от периферийного программного обеспечения, не относящегося к сертификации. Это достигается благодаря выполнению критически важных функций управления в отдельных безопасных доменах. Тем самым обеспечивается их обособленность от общих некритических функций ввода/вывода. Эта изоляция выполняется как на аппаратном, так и на программном уровне. Благодаря такому строгому разделению более сложное и критически важное для безопасности

программирование ограничивается исключительно безопасными доменами, что облегчает разработку программного обеспечения, а также упрощает и ускоряет сертификацию по SIL. В дополнение к сокращению объёмов аппаратной документации это второй важный фактор, способствующий значительной экономии средств во внутренних разработках (рис. 2).

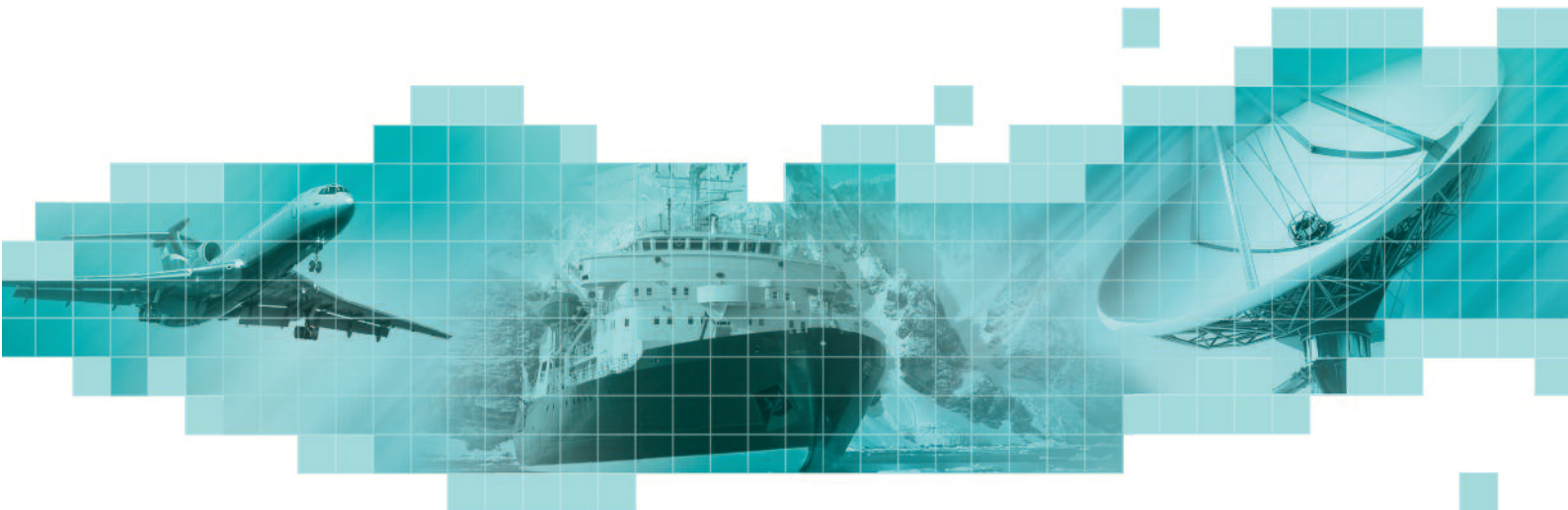
Высокопроизводительные контроллеры уровня SIL 4

В основе контроллера menTCS МН50С лежит процессорная плата F75P CompactPCI PlusIO SBC, сертифицированная по SIL 4. Это одноплатный компьютер, объединяющий три процессора Intel Atom E680T. Два процессора в нём выполняют критически важные функции управления. Они связаны с PCIe через FPGA (ПЛИС – программируемая логическая интегральная схема), которая обеспечивает синхронизацию контрольных точек приложения с SIL 4 для требуемой избыточности 2oo2 (2 out of 2 voting – мажоритарная схема 2 из 2). Третий процессор отвечает за общий ввод/вывод. Благодаря широкой распространённости и многолетнему рыночному опыту работы с этими процессорами все известные критически важные ошибки уже известны и документированы. Поэтому, если соблюдаются известные правила проектирования плат, систематические ошибки, которые могут повлиять на поведение безопасности, исключаются.

Безопасный домен с QNX Neutrino

Для исполнения критически важных приложений контроллер menTCS МН50С имеет предустановленную операционную систему реального времени QNX Neutrino, специально адаптированную к интегрированному оборудованию. По сравнению с проприетарными операционными системами эта интеграция сама по себе экономит разработчикам и OEM-производителям около двух миллионов евро в расходах по проекту и позволяет им избежать всех рисков, связанных с сертификацией. Пакет поддержки платы для разработок под QNX Neutrino также является сертифицированным по SIL 4 на платформе menTCS и, следовательно, с самого начала обеспечивает наивысшую степень надёжности.

QNX Neutrino использует микроядерную архитектуру, которая строго изоли-



CompactPCI ■ Компьютеры специального назначения

Блочные корпуса с различными механическими характеристиками, в том числе с ударпрочностью до **25g**

Эффективное электромагнитное экранирование

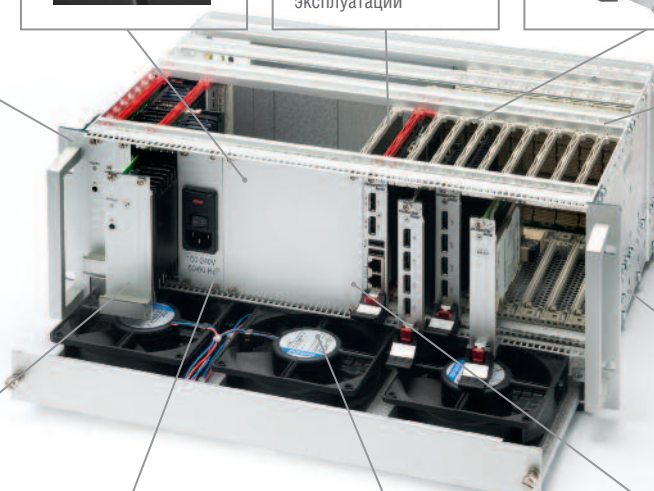
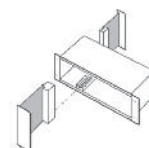


Процессорные модули PICMG 2.0, 2.16, 2.30; CPCI-S.0 (Serial) на различных процессорных платформах AMD и Intel для работы в жёстких условиях эксплуатации

Кросс-платы и модули расширения PICMG 2.0, 2.16, 2.30, CPCI-S.0 (Serial)



Подключение модулей тыльного ввода-вывода



Источники питания одинарные или резервированные: встраиваемые или в виде сменных блоков



Панели ввода с клеммами заземления и разъёмами питания разных типов



Вентиляторы с возможностью «горячей» замены. Система охлаждения, в том числе с кондуктивным отводом тепла



Лицевые панели универсальные и заказные для вставных блоков



Различные габариты и варианты компоновки



рует программные процессы, что не позволяет им взаимно влиять на производительность и поведение друг друга. Это, в свою очередь, гарантирует, что система всегда остаётся в безопасном состоянии, поскольку даже вредоносные программы не могут влиять на критически важные для безопасности процессы. Кроме того, QNX Neutrino поддерживает разделение и гибкую настройку использования ресурсов процессора. Критически важные для безопасности приложения могут быть запрограммированы на языках C или Ada, а также на основе платформы SCADA или Soft PLC (программно реализованный ПЛК). Разработчики могут использовать знакомую среду разработки, что сводит к минимуму дорогостоящую повторную сертификацию. По запросу доступны и другие операционные системы, такие как INTEGRITY от Green Hills, PikeOS от Sysgo или VxWorks от Wind River.

Унифицированный ввод/вывод

Чтобы упростить обработку ввода/вывода в безопасном домене, компания MEN Mikro Elektronik интегрировала

инфраструктуру ввода/вывода PACY (PACY – безопасная среда для приложений и данных, абстрагирующая их от аппаратной платформы) в безопасный домен, что обеспечивает прозрачный уровень абстракции между безопасным доменом и доменом ввода/вывода. Это означает, что идентичные функции в одном домене всегда адресуются одинаково и становятся независимыми от аппаратной реализации входов и выходов. Для PACY не имеет значения, обращается ли команда к реле или к цифровому вводу/выводу. Это делает интеграцию менTCS гораздо более простой и гибкой. Системы для поездов и путей с различными датчиками и исполнительными механизмами для реализации одинаковых функций теперь можно оснащать идентичными системами управления, значительно упрощающими модернизацию.

Среда PACY реализована как структура на модульной основе, что обеспечивает гибкое расширение с помощью отдельных клиентских модулей, а также связывание с любым C-приложением. В будущем разработчики смогут определять функциональные блоки PACY, объеди-

няющие несколько задач в одну макрокоманду. Таким образом, часто используемые процессы, такие как функция экстренного торможения, могут быть просто активированы как стандартные процедуры без необходимости программировать их в каждом случае. Связь между безопасным управлением и безопасным торможением осуществляется посредством домена ввода/вывода (рис. 3).

Домен ввода/вывода с Linux

Поскольку третий процессор Intel Atom обрабатывает аппаратный ввод/вывод совершенно отдельно от безопасного домена, гарантируется, что домен ввода/вывода никогда не будет влиять на логику безопасного управления. MEN Mikro Elektronik использует для данной цели интегрированную и предварительно сертифицированную ОС Linux. Это даёт клиентам доступ к полностью развитой и проверенной экосистеме с готовыми инструментами и драйверами, доступными для использования «из коробки». Дополнительная ОС предоставляется по запросу.

Связь между безопасной системой и картами ввода/вывода контроллеров

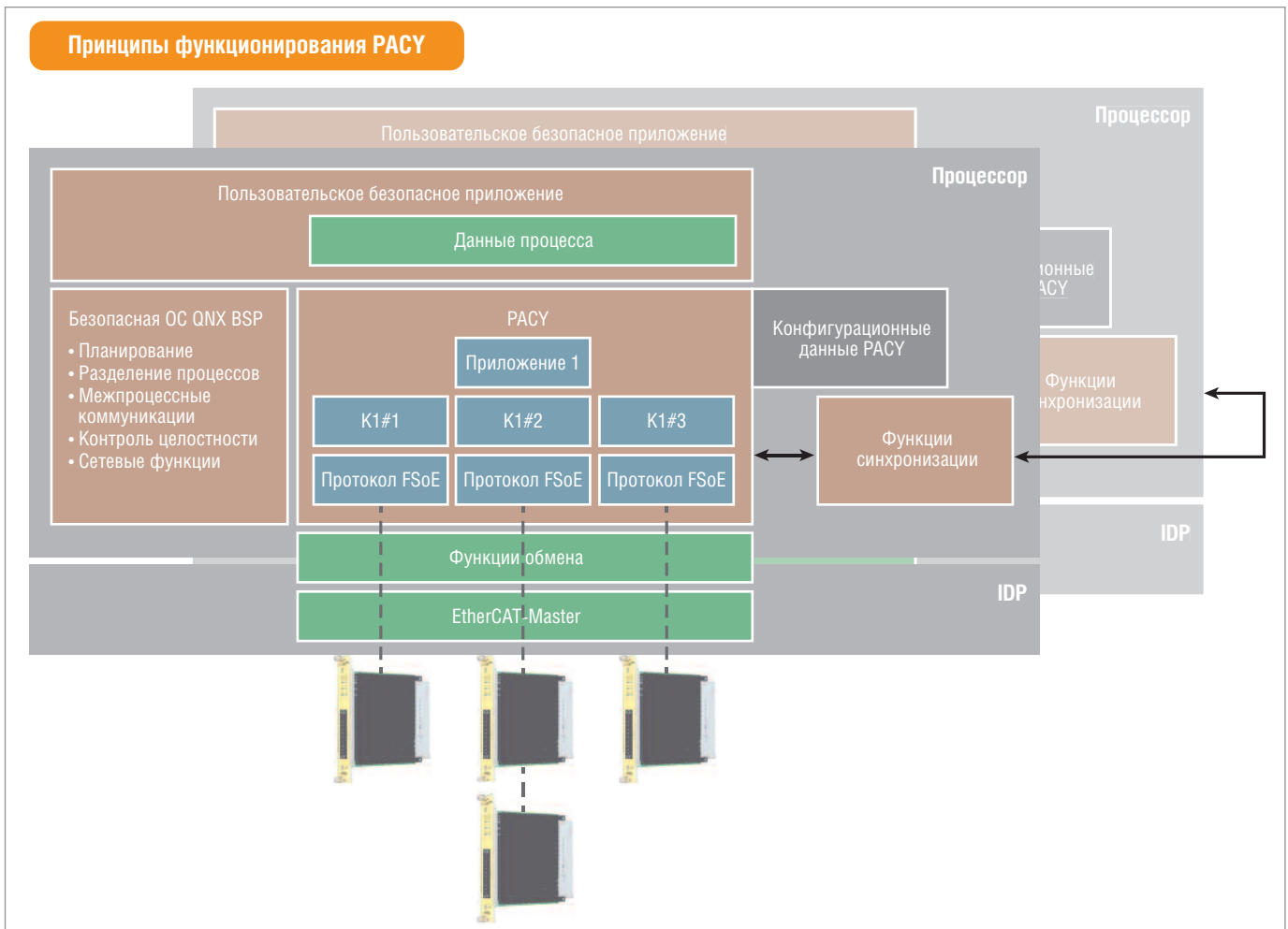


Рис. 3. Структура безопасного ввода/вывода PACY

menTCS, а также модулями ввода/вывода реализована по протоколу EtherCAT. EtherCAT – это Ethernet-стандарт реального времени с гарантированными циклами реального времени менее 5 микросекунд, отвечающий всем требованиям безопасной связи с компонентами menTCS. EtherCAT не требует коммутаторов, поскольку он поддерживает кольцевую топологию с резервированием каналов связи. Для надёжного обнаружения изменённых, дублированных или потерянных пакетов данных в EtherCAT используется протокол функциональной безопасности FSoE (Fail Safe over EtherCAT). Таким образом, весь канал связи ввода/

вывода функционирует как «чёрный» канал, обеспечивая необходимую функциональную безопасность связи.

Вывод: НЕ БОЙТЕСЬ ГОТОВЫХ СИСТЕМ

Платформа menTCS хорошо подходит для всех критически важных железнодорожных применений и демонстрирует возможности и преимущества систем управления поездом, основанных на открытых стандартах.

Она предлагает операторам поездов и путей, а также сторонним поставщикам решений автоматизации много преимуществ, которые сегодня являются уникальными на рынке Smart Railways.

Крупные OEM-производители, в настоящее время доминирующие на рынке SIL-сертифицированных приложений, как и более мелкие компании, будут только в выигрыше от использования инновационной платформы menTCS, позволяющей быстро создавать IoT-совместимые приложения и интеллектуальные железнодорожные решения.

Таким образом, предлагаемое аппаратное обеспечение является хорошей альтернативой для построения стандартизованных систем управления ETCS. ●

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

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Аддитивное производство – важный компонент Industry 4.0

Аддитивное производство (*Additive Manufacturing, AM*) – общее название всех технологических процессов, которые позволяют создавать трёхмерные объекты, добавляя слой за слоем материал: пластик, металл, бетон, в будущем даже человеческую ткань.

Общим для всех AM-технологий является использование цифровой 3D-модели из программы автоматизированного проектирования (САПР), специального оборудования и наслаиваемого материала. Как только схема готова, оборудование AM считывает данные из архива САПР и спекает или последовательно добавляет слои жидкости, порошка или листового материала, послойно изготавливая 3D-объект.

Сфера применения технологии *Additive Manufacturing* безгранична. Первоначально она использовалась для ускоренного создания опытных образцов (визуализации прототипов), и в настоящее время она применяется для изготовления готовых деталей в авиационной, стоматологической, имплантологической, автомобилестроительной и даже при создании коллекций prêt-à-porter.

В то время как принцип послойного добавления материала достаточно прост, его практическая реализация зависит от того, где технология применяется:

- в качестве инструмента визуализации в дизайне;
- как средство для создания персонализированных продуктов потребительского класса;
- в промышленном производстве;
- для производства небольших партий деталей;
- для производства органов человека в недалёком будущем.



Иллюстрация с сайта progress.online

В некоторых случаях AM понимается как дополнительный компонент субтрактивного процесса (удаление материала, высверливание, фрезеровка) и в меньшей степени в качестве формирующего (ковка, штамповка). В общем, аддитивное производство может предложить профессионалам и потребителям среду создания, моделирования и/или ремонта любого продукта и в процессе своего развития переопределит ныне действующую модель производства.

Аддитивные технологии изменят мир так же, как изменил в своё время Интернет, возможно, спектр их применения выйдет далеко за пределы существующих потребностей человека. ●

По материалам valve-industry.ru

Информационная граница на замке: начались поставки компьютеров AdvantiX со специальной проверкой

Компания «Авантикс» – ведущий отечественный производитель электроники для ответственных применений – объявляет о новой возможности для заказчиков – купить компьютерное оборудование AdvantiX, прошедшее специальную проверку и специальное исследование.

Приобретение компьютера государственными органами или учреждениями, работающими с секретной информацией, иногда требует особого подхода. В определённых случаях этим структурам необходимо иметь стопроцентную гарантию того, что процесс обработки данных исключает их утечку.

Для обеспечения уверенности заказчика в отсутствии «прослушивающих закладок» в электронном оборудовании компания начала продажу своих изделий в комплексе с услугами «Специальная проверка» (СП) и «Специальное исследование» (СИ).

Спецпроверка и специсследование компьютера могут быть необходимы организации, если в её информационном потоке присутствуют персональные данные и конфиденциальные сведения. А в случае обработки информации, содержащей служебную или государственную тайну, проведение СП и СИ обязательно.

Спецпроверка позволяет обнаружить внутри оборудования устройства для скрытого считывания информации или подтвердить их отсутствие. Часто такие устройства называют «жучками».

Специсследование оборудования проводят для измерения радиуса распространения электромагнитного излучения, в котором возможно несанкционированное считывание информации, а также для определения необходимых мер по предотвращению хищения данных.

Подводя итог, отметим, что купив компьютер AdvantiX и дополнительные услуги по его проверке, заказчики из государственных структур смогут получить не только желаемую технику, но и уверенность в её безопасности, подкреплённую соответствующими документами от компетентных органов. ●