Технологии QNX и
ЗОСРВ «Нейтрино» в России

Москва, 19 апреля 2016

«Функциональная безопасность для железнодорожного транспорта с применением QNX»

Алексей Пятницких, ООО Прософт

СВД Встраиваемые Системы

ProSoft® 25 лет

Уникальное сочетание модульности и безопасности

- Открытая модульная компьютерная платформа для железнодорожного транспорта
  - Базируется на стандартных программных и аппаратных компонентах
  - Свободно программируемая

- Сертифицируема до SIL 4
  - Соответствие EN5012x, EN 50155 и EN 50121-4 железнодорожным стандартам
  - Масштабируемость безопасность уровня - определяется исключительно требованиями приложения
  - Поставляется с сертификационным пакетом с сертификатами от TÜV SÜD

Инновации MTCS – Ваши преимущества

Для подвижного и наземного применения	Синергетический эффект
Нет фиксированного применения	Приложение на стороне заказчика
Разные приложения на одной платформе	Снижение цены и затрат на установку
Открытый интерфейс программирования	Высокая гибкость программирования
Использование открытых стандартов	Функциональная совместимость, независимо от одного поставщика
Сертифицированное ПО и аппаратная часть	Низкие риски, снижение времени и затрат
Концепция семейства	Длительный жизненный цикл
Real-time Ethernet	Безопасный и быстрый ввод-вывод
Удаленные системы ввода-вывода	Уменьшение кабелей, большие возможности расширения

Гнаться за двумя зайцами – MTCS для подвижного транспорта и наземных задач

Подвижный транспорт

ATO / ATP – Автоматическая система управления/защиты (для ETCS, PTC, CTCS, Klub-U)

TCMS – Система управления поездом

CBTC – Система коммуникации в поезде

Синергетический эффект

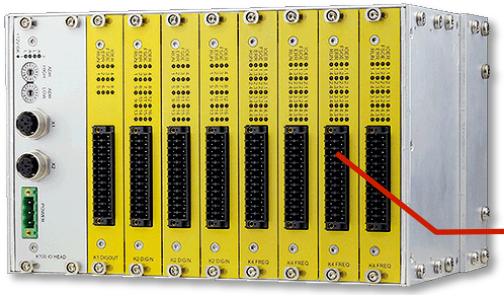
MTCS предназначена для всех функционально безопасных приложений

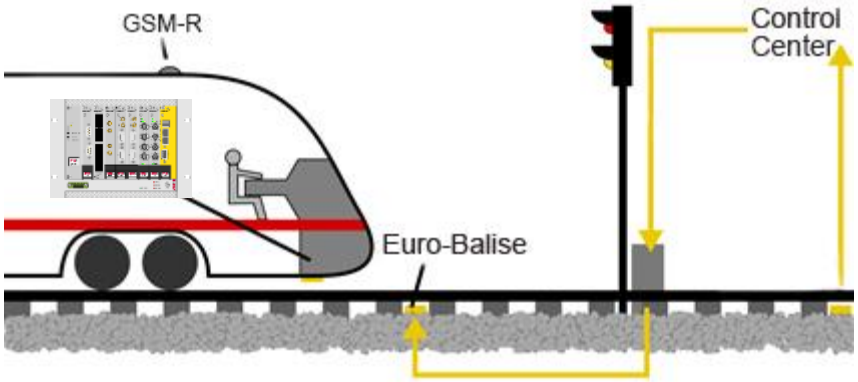
Снижение затрат и времени реализации проекта

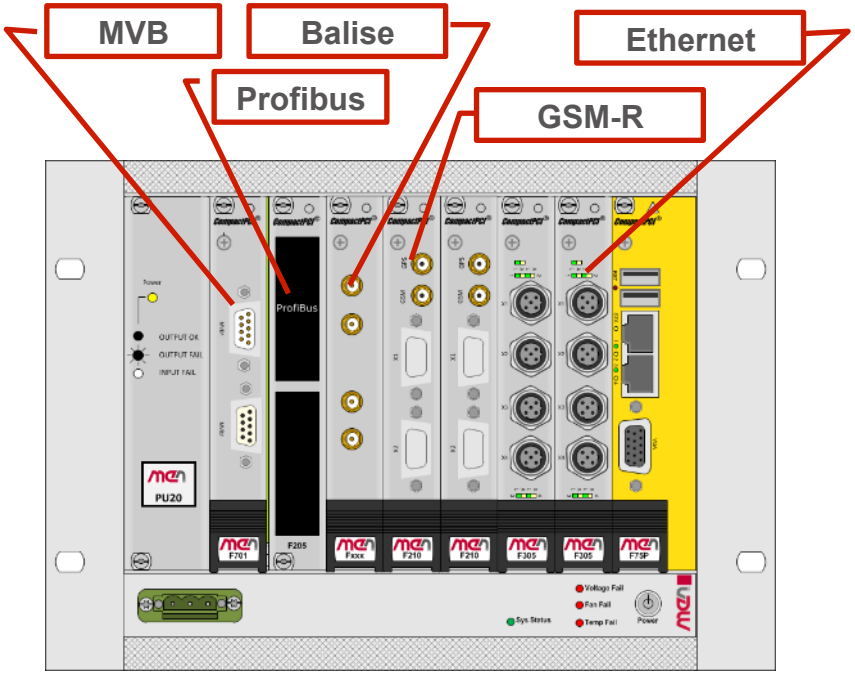
Наземное оборудование

CBI – автоматической управление стрелками

Типовое применение – для ETCS







- ETCS система защиты поездов
  - Разделение поезда или предотвращение столкновения
  - Превышение скорости (аварийный тормоз)
  - Временные скоростные ограничения
- MTCS предоставляют все основную функциональность для EVC (European Vital Computer)
  - GSM-R связь
  - ETCS компьютер приложения
  - Интерфейсы для другого ETCS оборудования
  - Интерфейсы для поезда

Ключ к вариациям – разделение управления и приложения

Сделано MEN

Сертифицированная аппаратная платформа

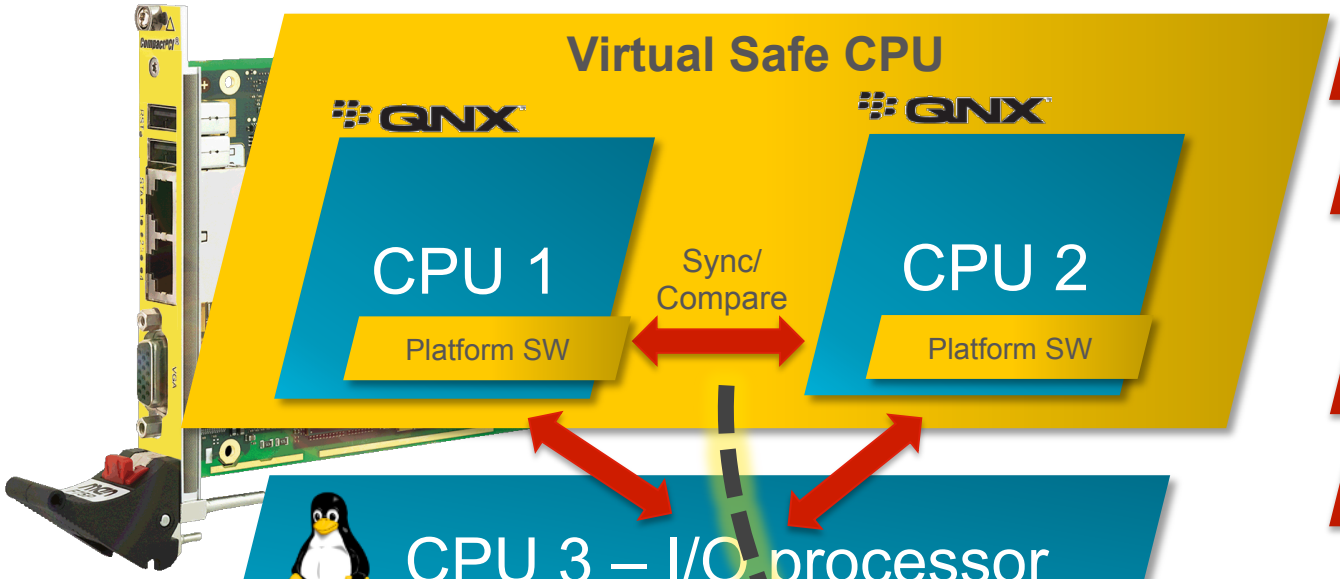
Сертифицированная программная платформа

Сделано заказчиком

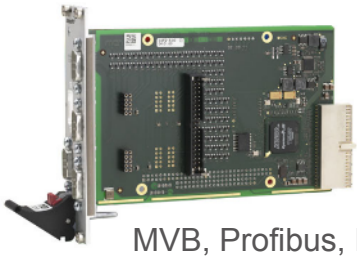
Приложение

- Одна платформа для множества задач
- Преимущества через полное управление
- Лучшее использование преимуществ частей

Безопасный и ввода-вывода уровни

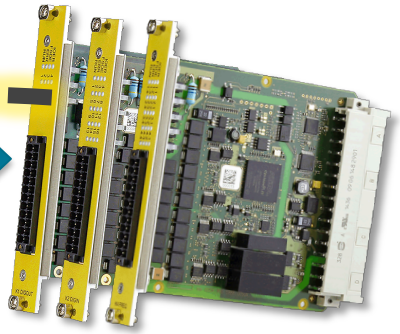


- Отказоустойчивая архитектура
- Безопасная связь через черный канал
- Облегчение программирования безопасного приложения
- Ускорение разработки ПО



MVB, Profibus, Ethernet…

Black Channel



Safe I/O

Программная архитектура изнутри – Безопасный и ввода-вывода уровни

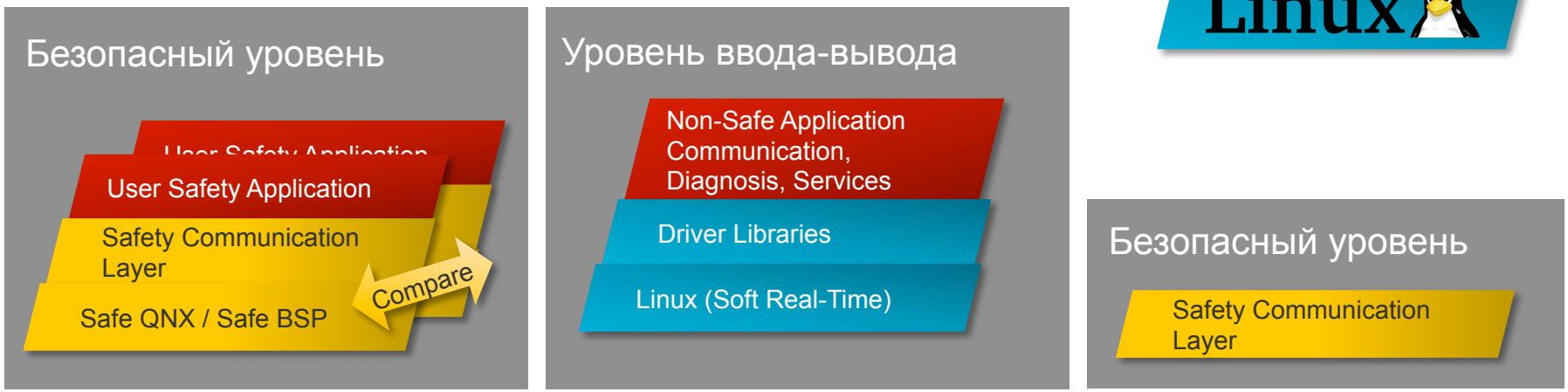
- Разделение между безопасной частью (QNX) и связью (Linux)
- Дублирование выполнения программы на 2-х процессорах
  - Синхронизация и сравнение 2-х ЦПУ и уровень связи
  - Различные приложения в безопасной части благодаря производительным процессорам и QNX структуризации

Приложение независимо от аппаратной части

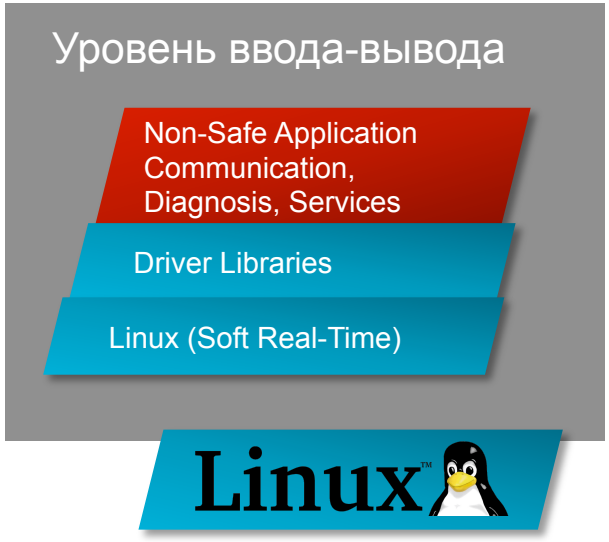
Программа ввода-вывода заменяема без пересертификации

Разные приложения на одной платформе – снижение затрат

Сертифицированная программная платформа



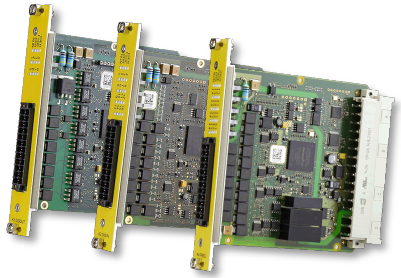
Программные возможности



- Высокая гибкость
- Снижение затрат
- Перспективная архитектура
- Запланированы замещающие продукты
- Снижение затрат на программирование

- Стандартные программные компоненты (open API) и операционные системы
- Стандартный интерфейс программирования POSIX
- Программирование безопасных приложений:
  - C
  - Model-based (e.g. SCADE)
  - Soft PLC
  - Ada

MTCS продуктовая линейка



- Модуль контроллера MH50C, на основе процессорной платы F75P
  - До 6 плат ввода-вывода (либо безопасный ввод-вывод, либо Ethernet, Wi-Fi, GPS, MVB и т.д..)
  - Источники питания переменного и постоянного тока
- Платы ввода-вывода для дискретных и частотных сигналов *(остальные в разработке)*
  - Для использования в модуле контроллера и для удаленного ввода-вывода
- Системы удаленного ввода-вывода

  До 4, 6, 8 плат ввода-вывода
  - Интерфейс связи Real-time Ethernet

Компакнтый размер

Гибкая конфигурация

Расширяемость до 63 систем ввода-вывода

Масштабируемость уровней безопасности

Практически бесконечное расширение

Близкое расположение к датчикам и исполнительным устройствам

Улучшение целостности сигнала

Связь через Real-Time Ethernet

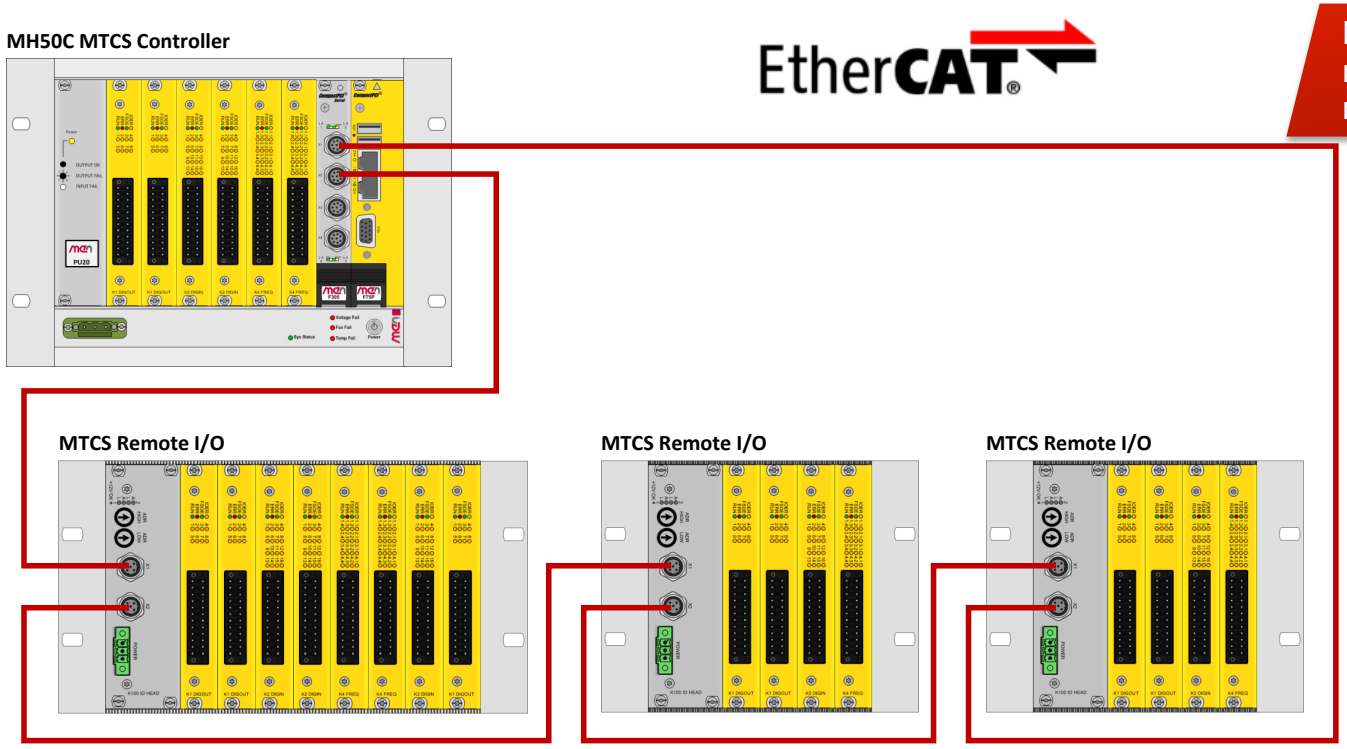
- Все модули ввода-вывода подключены через real-time Ethernet ”EtherCAT“
- Связь защищена протоколом Safety через EtherCAT (FSOE)
- Соединение по топологии кольцо
  - Защита от единичных неисправностей, как обрыв кабеля

Удаленный ввод-вывод снижает количество кабелей

Безопасный и быстрый ввод-вывод черезSafety over EtherCat

Не нужны коммутаторы Ethernet

Высокая доступность с небольшим количеством кабелей



MTCS компоненты с гарантированной безопасностью

Сертификация снижает время и затраты

Низкие риски по проекту для заказчика

Процессорная плата F75P

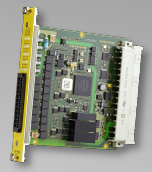
QNX

F75P
QNX
BSP

TÜV Сертификат

TÜV экспертный отчёт

Ввод-вывод



QNX

QNX Drivers

Техническое обоснование безопасности

Руководство пользователя

Открытая и модульная система

- Независимость от одного поставщика
- Легкая интеграция сторонних компонентов
- Легкая замена недоступных компонентов

Стандартные аппаратные компоненты, X86 процессоры

Стандартный Ethernet

CompactPCI промышленный стандарт

Стандартные ОС (QNX, Linux)

Стандартный POSIX

MTCS полностью базируется на открытых стандартах в аппаратной и программной части, а так же в коммуникации

Соответствие стандартам рынка

- Требования по безопасности
  - EN 50126: Железные дороги. Требования и подтверждение надежности, пригодности к эксплуатации, ремонтопригодности и безопасности. (RAMS)
  - EN 50128: Системы телекоммуникационные, сигнализационные и системы для обработки данных, применяемые на железных дорогах. Программное обеспечение для систем управления и защиты на железных дорогах
  - EN 50129: Дороги железные. Системы телекоммуникационные, сигнализационные и системы для обработки данных. Электронные сигнализационные системы обеспечения безопасности
- Требования по воздействию окружающей среды
  - Соответствие EN 50155
  - Расширенный температурный диапазон
  - Устойчивость к вибрации и ударным нагрузкам
  - Защитное покрытие
  - ЭМС по EN 50121-4

Готова к работе на железной дороге

Протестирована на надежную работу

Концепция семейства и управление жизненным циклом

- Гарантируемая доступность в течении 10 лет для каждого продукта
- Документ анализа эффекта изменения дает полную прослеживаемость в случае редизайна
- Легкая замена отдельных частей на основе открытых стандартов
- Запланирован рост семейства аппаратных компонентов, включая и программные пакеты, до 2050 года

Длительный жизненный цикл

Рост семейства продуктов для индивидуальных требований

Уникальное решения для железнодорожного рынка

- Применима к большому числу железнодорожных приложений благодаря модульности
- Полностью базируется на стандартных компонентах, что снижает стоимость жизненного цикла каждого проекта
- Значительное снижение времени разработки и затрат благодаря сертифицированным программным и аппаратным компонентам
- Сертификационный пакет с сертификатами от TÜV SÜD
- Соответствие всем необходимым стандартам по безопасности и воздействию окружающей среды

Typically

Always reliable. Always ahead.