ЭРЕМЕКС

ИННОВАЦИОННЫЙ ПОДХОД К РАЗРАБОТКЕ ЭЛЕКТРОНИКИ

Разработка надёжных встраиваемых систем с операционной системой FX-RTOS

Сергей Пилкин
заместитель генерального директора
ЭРЕМЕКС

WWW.EREMEX.RU

Надёжность встраиваемого ПО

- Надёжность = 1 - p(failure)
- Типы отказов
  - Нет нужных ресурсов (память, время)
  - Эксплуатация уязвимостей
- ОСРВ как фактор надёжности
  - Резервирование ресурсов
  - Гарантия времени реакции
  - Изоляция ПО с разной ответственностью
  - Минимизация доверенной базы
  - Компонентная архитектура

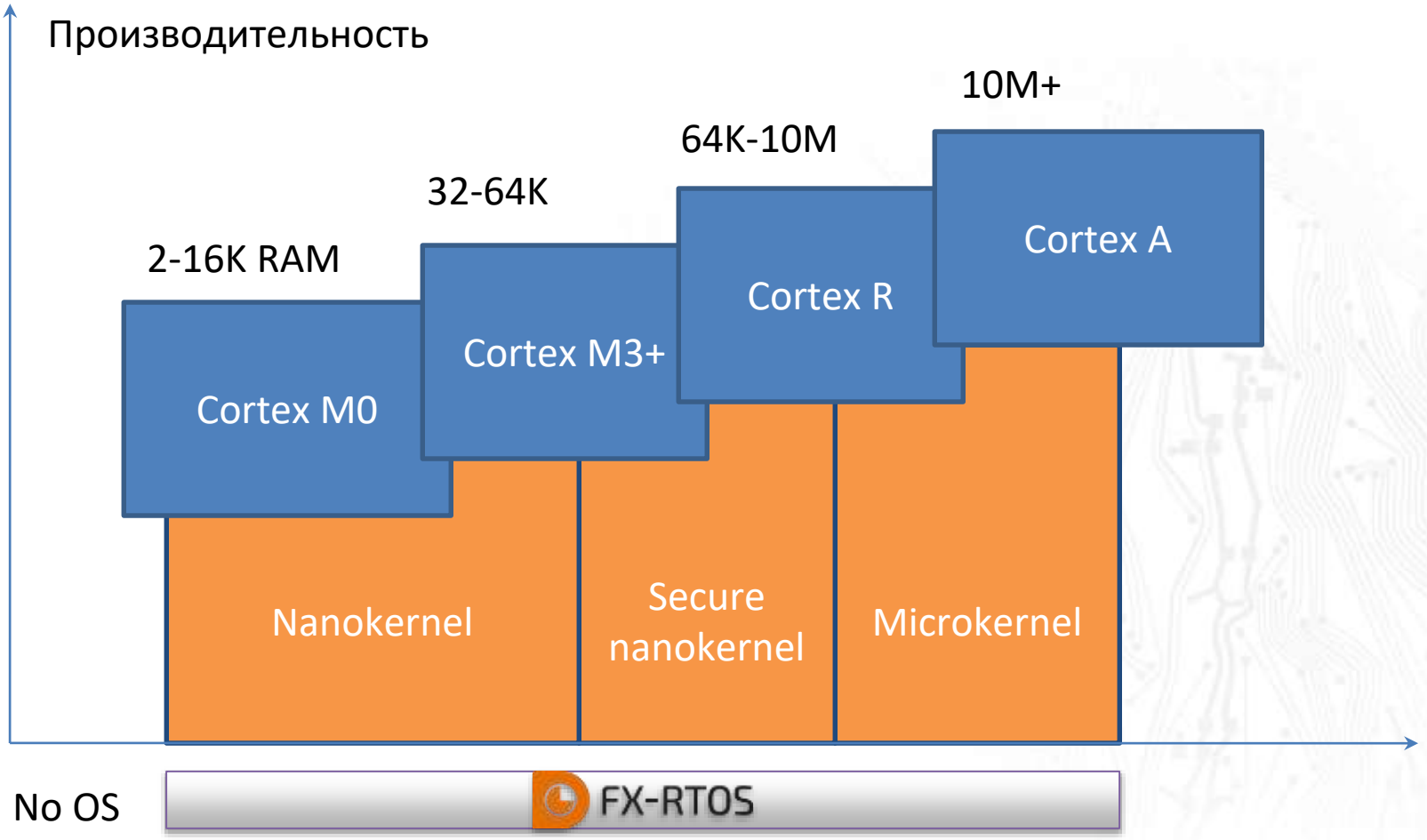
Цели разработки FX-RTOS

- Надёжность и безопасность
- Масштабируемость
  (поддержка разных платформ)
- Параллелизм и многопроцессорность
- Работа в реальном времени
  - Предсказуемость времени реакции
  - Приоритетное планирование
  - Защита от инверсии приоритета

Стандартные конфигурации

FX-RTOS	Потоки	Разделение режимов	Процессы	IPC	SMP
Nanokernel	✓				✓
Secure nanokernel	✓	✓			✓
Microkernel	✓	✓	✓	✓	✓

Позиционирование



FX-RTOS Nanokernel

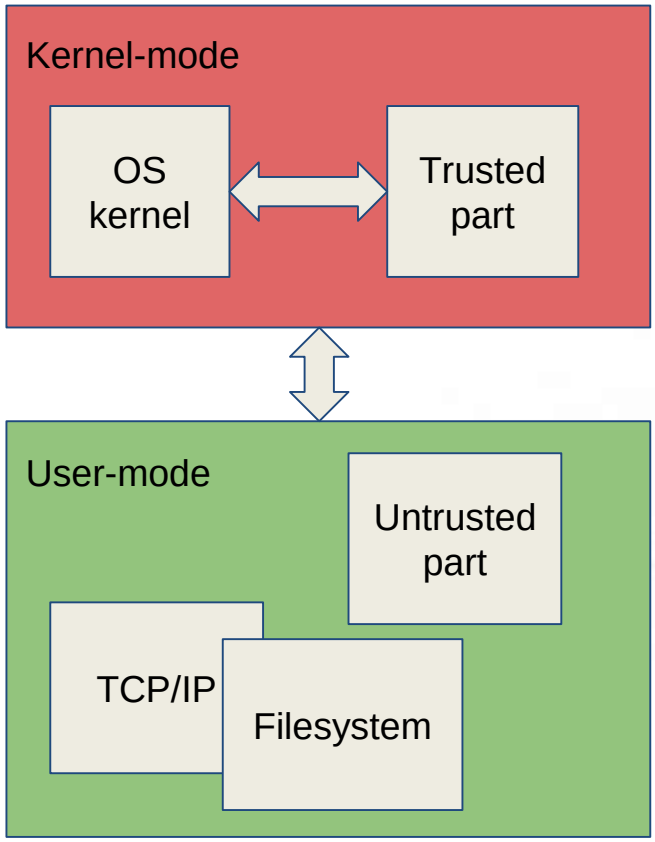
- Статическая библиотека (*.h + *.lib)
- Поддержка всех основных платформ (ARM, PIC32, AVR32, MSP430) и инструментов (IAR, Keil, GCC и др.)
- Ключевые особенности
  - Широкие возможности настройки
  - Изменяемая архитектура без изменения API
  - Конфигурации с низкой латентностью прерываний
  - Фиксированное время реакции
- Используется в устройствах Fastwel с 2012 года
  - Требования к времени реакции < 5 мкс на 100MHz MCU

Secure Nanokernel

- Распространение IoT и автономных устройств
- Растет сложность микроконтроллеров
- Разделение кода по уровням ответственности
- Последствия эксплуатации уязвимостей
  - Активация code read protection через IAP
  - Перехват управления
- Конфиденциальные данные в устройствах
- Трудно детектировать вредоносное ПО

FX-RTOS Secure Nanokernel

Архитектура



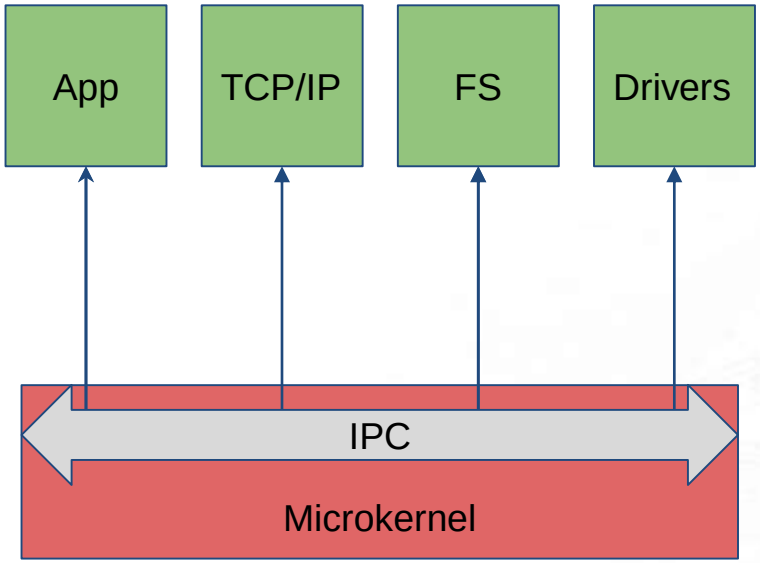
- Два домена защиты
- Механизм системных вызовов
- Идентификаторы объектов
- Контроль доступа к памяти
  - Память ядра недоступна
  - Изоляция устройств
  - Раннее выявление ошибок
- Сокращение доверенной базы
- Подмножество основного API
- Расширяемый интерфейс ядра

Использование Linux во встроенных системах

- Доверенная база = ядро + драйверы
- Драйверы содержат уязвимости
- Встроенные системы редко обновляются
- Модель безопасности для многопользовательских систем (есть суперпользователь «root»)
- Отсутствие детерминизма
  - Оптимистические алгоритмы
  - Copy-on-write
  - Непредсказуемые задержки
- Глобальные ресурсы

FX-RTOS Microkernel

Архитектура



- Мультисерверная микроядерная архитектура
- Использование стандартных инструментов
- POSIX-подобный интерфейс
- Модель безопасности на основе ролей
- Отсутствует концепция «суперпользователя»
- Поддержка ARM, Intel x86

FX-RTOS Microkernel: системы реального времени

- Предсказуемое время реакции
- Надёжность
  - Статическое задание процессов
  - Резервирование ресурсов
  - Изоляция серверов
  - Драйверы в пользовательском режиме
  - Перезапуск процессов по ошибке
  - Квоты приоритета для каждого процесса
- Масштабируемость в многоядерных системах
  - Многопоточные серверы
  - Отсутствие глобальных блокировок

Выводы

ОСРВ для надёжных систем:

- Обеспечивает защиту памяти и устройств
- Изолирует недоверенный код от доверенного
- Имеет минимальную доверенную базу
- Реализует модель безопасности, соответствующую сценарию применения
- Обеспечивает время реакции, не зависящее от действий приложений
- Гарантирует наличие ресурсов

EREMEX

Спасибо за внимание!

подробности на сайте fxrtos.ru