



ОСОБЕННОСТИ ТРЕБОВАНИЙ К ВСТРАИВАЕМОЙ ИНДУСТРИАЛЬНОЙ ОС

OS DAY 2020

ПАРЬЕВ СЕРГЕЙ

Обо мне



- Окончил МФТИ, кафедру математического моделирования в ядерной физике
- Более 20 лет опыта в отрасли разработки коммерческого ПО в различных должностях от системного программиста до руководителя отдела разработки, главного конструктора, менеджера продукта
- Работал как в небольших компаниях-стартапах, так и в компаниях с мировыми брендами, в том числе иностранных
- ПО в основном было встраиваемое. Использовался широкий спектр ОС и аппаратных платформ. Довелось столкнуться как с распространенными встраиваемыми устройствами (мобильные устройства, программируемые логические контроллеры, принтеры и др.), так и с довольно экзотическими (криптомодули)
- Участвовал в разработках встраиваемой RTOS и специализированного дистрибутива Linux
- В последние годы специализируюсь на вопросах кибербезопасности и надежности встраиваемых промышленных систем

Применение различных типов ОС

- Рабочие станции – (клиентская) ОС общего назначения
- Сервера – (серверная) ОС общего назначения
- Встраиваемые (embedded) устройства
 - Встраиваемые и промышленные компьютеры – ОС общего назначения
 - Мобильные устройства, носимая электроника – мобильная ОС
 - **Индустриальные устройства – индустриальная встраиваемая ОС**
 - “Малые” устройства – “малая” встраиваемая ОС, монитор, firmware



Индустриальные встраиваемые устройства

- Интеллектуальное промышленное оборудование
 - УСПД
 - ПЛК, контроллеры PCU
 - РЗА терминалы
 - Интеллектуальные счетчики
 - Станки с ЧПУ
 - IoT Edge, IoT GW
 - ... (сотни других типов)
- Автоматизация зданий и сооружений
- Телекоммуникационное оборудование
- Медицинская техника
- Робототехнические устройства
- Транспорт (бортовые и объектовые системы)
- Спецтехника
- ...



Особенности промышленных встраиваемых устройств

- Ограниченный круг решаемых задач
- Сильная ограниченность аппаратных ресурсов
- “Полевые условия” – колебания температур (-30°C , $+50^{\circ}\text{C}$), ЭМ помехи, вибрации, пыль, вода и др.
- Ограниченные возможности по обслуживанию (например, раз в год)
- Долгие (10+, 20+, 50+ лет) сроки эксплуатации
- Автономная работа продолжительное время
- Массо-габаритные требования
- Требования по питанию (в том числе по автономному)
- Специализированные сетевые (в том числе шинные) интерфейсы
- Оборудование по обработке сигналов
- Требования по безопасности (safety + cybersecurity)



Особенности аппаратного обеспечения

- Аппаратные архитектуры – ARM, MIPS, PowerPC, ...
- Высоко интегрированные SoC-и
- Flash (JFFS2, UBIFS, ...)
- Интерфейсы – UART, I2C, SPI, USB
- Поддержка специализированного сетевого оборудования (и протоколов)
- Расширенные функции управления питанием
- Поддержка оборудования для сбора и преобразования сигналов
- MMU, MMU-less, MPU
- Растет заинтересованность в multi-core (SMP)
- Растет заинтересованность в аппаратной поддержке виртуализации



Ограниченный круг решаемых (специализированных) задач

- ОС общего назначения, мобильные ОС – выполняют (неопределенно) широкий круг клиентских задач (через запуск приложений)
- Встраиваемое устройство (и встраиваемая ОС, установленная на нем) предназначено для исполнения конкретной целевой функции
- **Влияние на требования к ОС**
 - зафиксированный список оборудования (для сборки ОС)
 - заранее определенный список процессов (и других ресурсов ОС)
 - зафиксированное или заранее просчитываемое распределение памяти
 - зафиксированные сетевые конфигурации
 - часто требования real-time (hard, soft) из-за интенсивной работы с периферией и критичности исполняемой целевой функции



Сильная ограниченность аппаратных ресурсов

- Влияние на требования к ОС

- отдается предпочтение к оптимизированным (например, под специализированное оборудование) модулям по отношению к универсальным
- требования сильной кастомизируемости (в том числе на уровне сборки) компонентов ОС
- высокая модульность (причем на уровне сборки ОС)
- жесткий контроль использования аппаратных ресурсов и ресурсов ОС
 - процессорное время
 - постоянная память
 - оперативная память
 - открытые файлы, кэши
 - временные файлы, логи
- часто требуется compile-time распределение ресурсов
- из аппаратного обеспечения “выжимается” максимум



Высокая модульность ОС

- Влияние на требования ОС
 - Встраиваемая промышленная ОС представляет собой “конструктор”, из которого собираются “сборки” ОС
 - Под каждую аппаратную плату (линейку) собирается своя сборка ОС
 - BSP (board support package)
 - сборка осуществляется либо разработчиком ОС, либо предоставляются возможности для сборки уже разработчиком устройства
 - В сборке исключаются (гораздо реже отключаются конфигурированием) лишние модули
 - это делается в том числе по требованиям безопасности (и safety и security)
 - Часто готовятся (полу)готовые сборки ОС под отраслевые задачи для облегчения работы разработчику устройства
 - “Industrial Grade”, “Carrier Grade”, “Military Grade”, “IoT Ready”

Примеры объектов собранных из данного конструктора



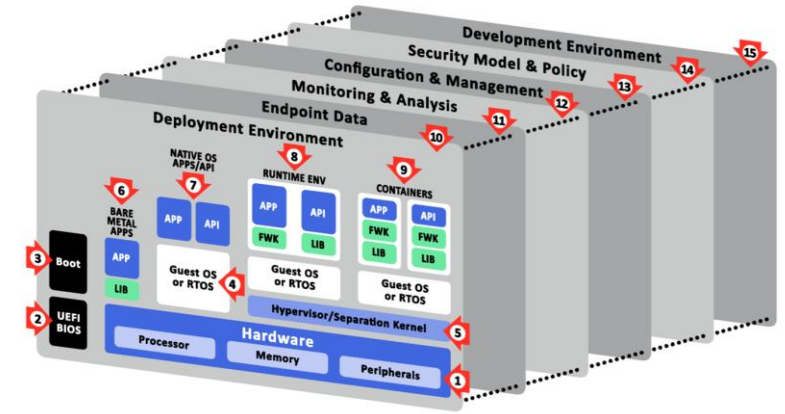
Безопасность (safety)

- Safety - основное требование к встраиваемому устройству после требования выполнять заданную целевую функцию
- Большая часть safety функций находится в ОС (меньшая в прикладном ПО)
- Влияние на требования к ОС
 - дополнительные требования к процессу разработки ПО
 - дополнительные требования к отсутствию программных ошибок
 - возможности широкой внешней диагностики и само-диагностики (а также реагирования) на небезопасные состояния (сбои аппаратуры, неправильность данных, программные ошибки и др.)
 - поддержка Safe режимов
 - возможности резервирования
 - выполнение сертификационных требований (МЭК 61508 (safety), МЭК 61511 (промышленность), МЭК 62304 (медицина), ISO 26262 (автотранспорт), EN 50128 (жд транспорт), авионика, военная техника)
 - могут быть требования использования ограниченных сетов языков (Misra-C)



Безопасность (cybersecurity)

- Нарастающие угрозы кибербезопасности
- Необходимость встроенных механизмов защиты
- Развитие нормативных требований (НПА и НТД)
- Влияние на требования к ОС
 - процессы разработки безопасного ПО (+вендорский CERT, PSIRT)
 - реализация встроенных механизмов защиты в ОС
 - часть функций пересекается с функциями safety
 - поддержка специализированного оборудования (SecEl, TPM, security storage)
 - использование криптографических механизмов
 - соответствие сертификационным требованиям к ОС ФСТЭК России (и зарубежных)
 - соответствие сертификационным требованиям по кибербезопасности встраиваемых устройств МЭК 62443 (-4-1, -4-2), профили защиты по common criteria



IIC Security Framework,
https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Кто основной потребитель ОС?

- ОС общего назначения, мобильная ОС
 - основной потребитель - конечный пользователь компьютера (мобильного устройства)
- Встраиваемая промышленная ОС
 - **основной потребитель – разработчик встраиваемого устройства**
 - не редко промежуточным потребителем выступает производитель HW
 - опосредованный потребитель – конечный пользователь устройства
- **Влияние на требования к ОС**
 - **основные требования к встраиваемой промышленной ОС выдвигает разработчик устройства**
 - конечный пользователь устройства ничего не знает о встроенной в устройство ОС
 - требования конечного пользователя (к устройству) опосредовано, через призму их понимания разработчиком устройства, попадают в требования к ОС

Способы взаимодействия с пользователями

- ОС общего назначения, мобильная ОС
 - постоянное взаимодействие с конечным пользователем
 - устройство большую часть времени находится под контролем конечного пользователя
 - необходимо полноценное GUI
- Встраиваемая промышленная ОС
 - в большинстве случаев необходимы (а часто и только возможны) редкие администраторские действия
 - большую часть времени устройство находится в автономном режиме
 - часто устройство не имеет возможности для ввода (немного реже и вывода) буквенно-цифровой информации
- Влияние на требования к ОС
 - в большинстве случаев не требуется полноценный GUI
 - вся система администрирования должна быть построена на редком вмешательстве
 - большую значимость имеет удаленное (сеть, UART) администрирование



Особенности разработки под встроенную ОС

- Возможности по сборке ОС
 - compile-time кастомизация состава и параметров модулей ОС
 - BSP (board support package)
- Средства разработки и отладки
 - кросс-платформенный toolchain
 - средства удаленной (сеть, UART) отладки
 - средства сборки ОС (прошивки)
 - средства профилирования
- Загрузчик
 - сборка и кастомизация
- **Широкая поддержка со стороны разработчика ОС**



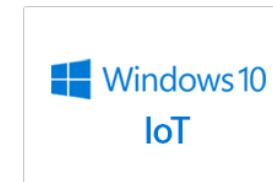
Особенности лицензирования

- Основные потребители – компании, разработчики встраиваемых промышленных устройств
- Реже – компании, разработчики аппаратных или программно-аппаратных платформ
- Часто нет технической возможности контролировать лицензию на устройстве
- Часто нет технической возможности контролировать количество выпущенных устройств
- **Используемые схемы:**
 - “royalty” – определенная сумма (или %) с каждого устройства с ОС
 - “prepaid” – выплачивается фиксированная сумма вперед, которая затем “расходуется” по мере продажи устройств с ОС
 - платная поддержка (сама ОС – условно-бесплатная)
 - дополнительные платные сервисы



Примеры встраиваемых промышленных ОС

- QNX
- ThreadX (MS, Asure OS)
- FreeRTOS (Amazon)
- ZephyrOS
- Wind River WxWorks
- Green Hills Integrity
- Embedded Linux дистрибутивы – CIP Linux, OpenWRT, Linaro, Wind River Linux
- Windows IoT, Windows Embedded
- ARM Mbed



Итоги

- Есть **принципиальные отличия** как в технических, так и не технических требованиях к встроенной промышленной ОС по сравнению с ОС общего назначения
- **Основные потребители** встроенной ОС – компании, **разработчики встраиваемых промышленных устройств**
- Встраиваемая ОС – это **конструктор** для создания сборок под конкретные платформы (линейки)
- Все ресурсы аппаратуры и ОС должны быть направлены на реализацию **целевой функции устройства**
- **Безопасность (safety)** – всегда вопрос N1 (после вопроса о возможности реализовать целевую функцию) к встраиваемой ОС
- **Безопасность (cybersecurity)** – набирающая актуальность тема, без поддержки которой невозможно представить современную встраиваемую ОС





СПАСИБО ЗА ВНИМАНИЕ

OS DAY 2020

ПАРЬЕВ СЕРГЕЙ

E-MAIL: SERGEY.PARIEV@MAIL.RU