ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ
РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ
ЭНЕРГОСИСТЕМ

Обзор экосистемы ПО RISC-V для АСУ ТП

Владимир Карантаев
Научный руководитель
Центра Практической кибербезопасности
НТИ МЭИ

WWW.NTI.MPEI.RU

О Центре экспертизы

ЦЕНТР НТИ МЭИ

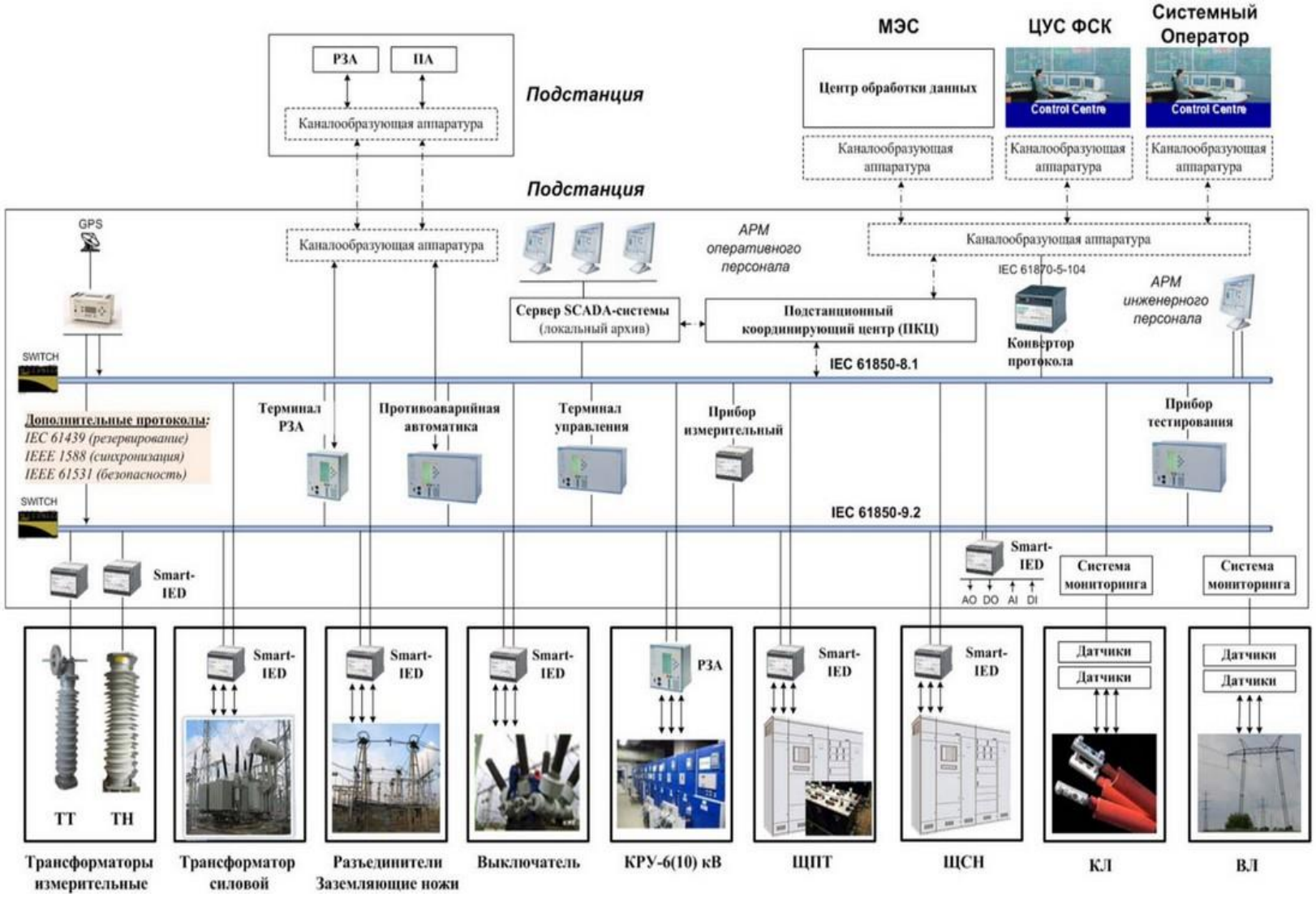
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Первый отраслевой центр по вопросам обеспечения кибербезопасности высокоавтоматизированных объектов электроэнергетики и промышленности.

Состоит из нескольких специализированных лабораторий:

- доверенный искусственный интеллект в электроэнергетике;
- разработка безопасного программного обеспечения;
- применение встраиваемых средств криптографической защиты информации;
- кибербезопасность объектов электроэнергетики.

Архитектура цифровой подстанции



Интеллектуальная система релейной защиты и автоматики (РЗА)

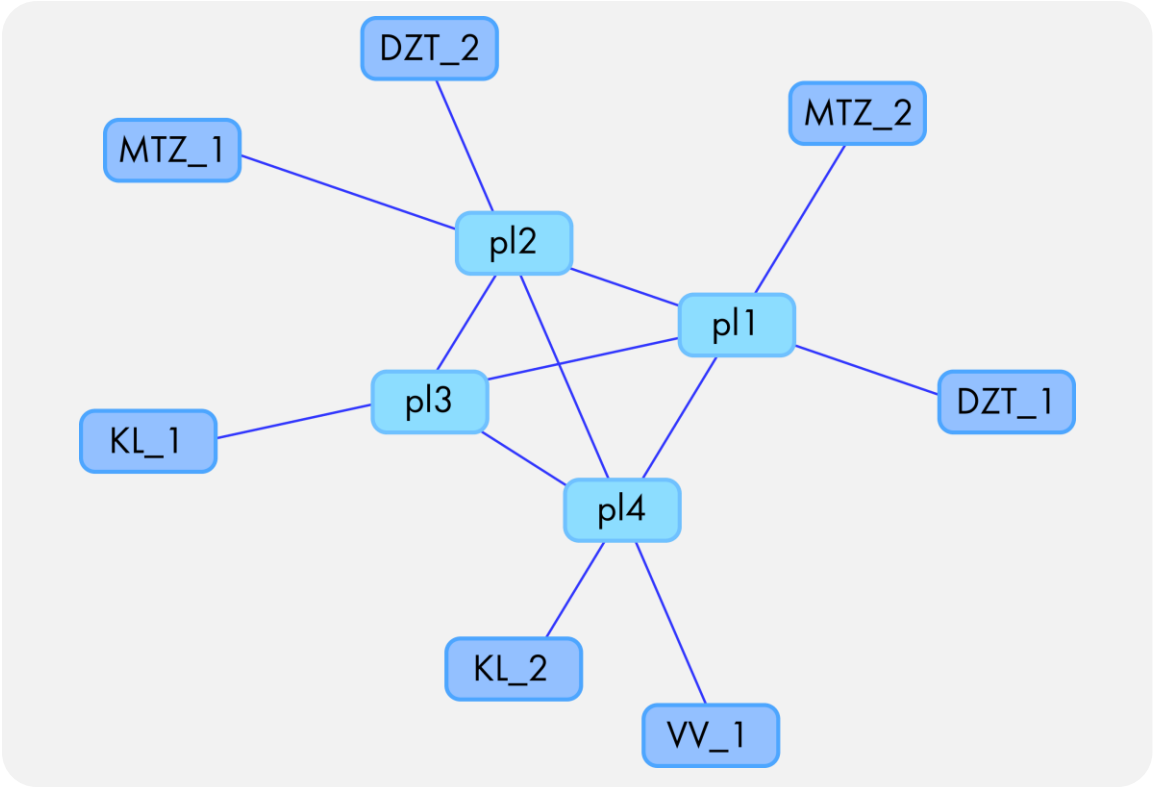
ЦЕНТР НТИ МЭИ

ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

Устройство интеллектуальной системы релейной защиты

Время срабатывания быстродействующих защит: **до 25 мс**

Схема миграции функций между устройствами

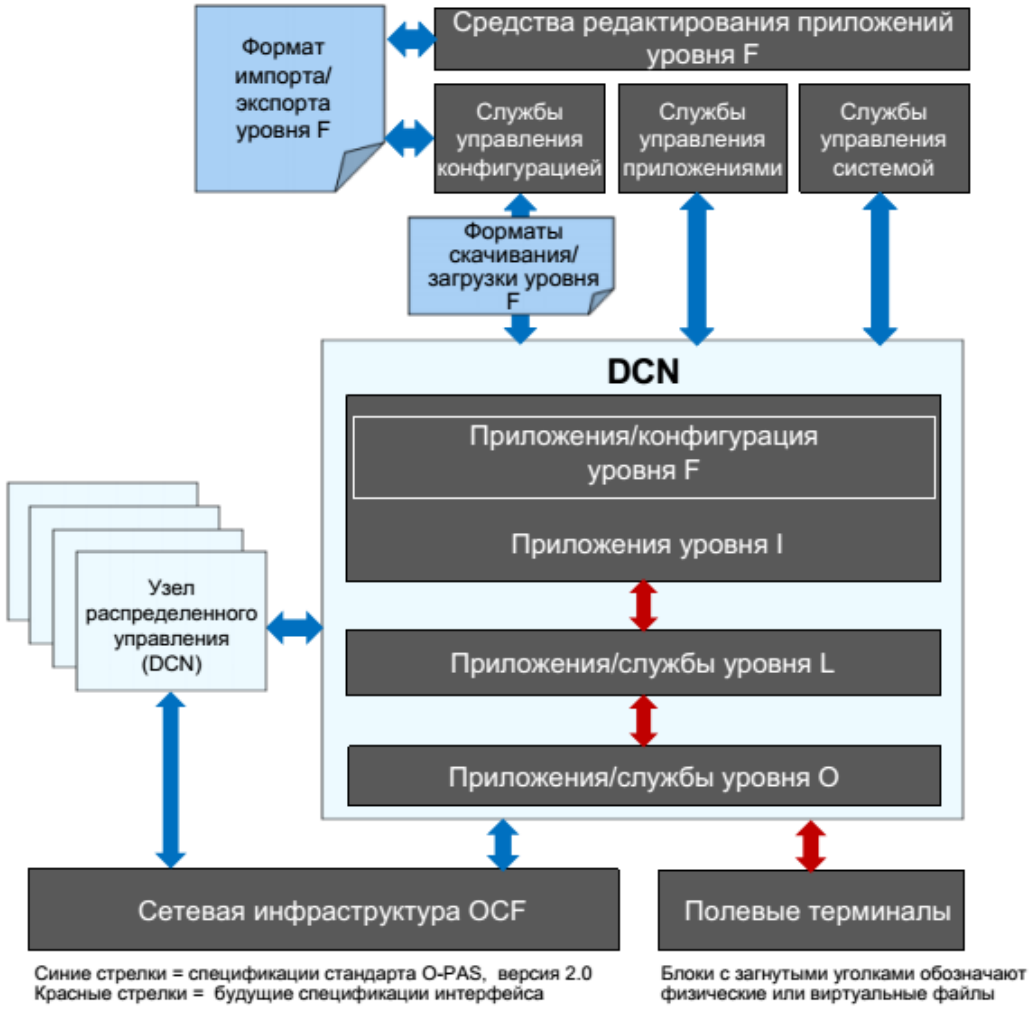


Время миграции функции: **до 80 мс**

Защищенное сетевое взаимодействие по протоколу МЭК 61850-8-1 (GOOSE)

Алгоритм	Длина пакета, байт	Проход по сети	Подписчик	Нормируемое время
		Медиана, мкс	Медиана, мкс	Медиана, мкс
Без криптографических методов	190	1 113	1	**1 114**
	550	1 051	1	**1 052**
	1 450	1 050	2	**1 052**
GOST_3411_12_256_HMAC	190	1 133	13	**1 146**
	550	1 124	17	**1 141**
	1 450	972	25	**997**
GOST_3411_12_512_HMAC	190	1 032	14	**1 046**
	550	1 068	17	**1 085**
	1 450	1 151	25	**1 176**

Структура узла распределенного управления (УРУ)



1. Приложения уровня F:

- Описываются с помощью конфигураций, определенных в OPAS.
- Включают функциональные блоки, программы IEC 61131-3, IEC 61499-1 и др.

2. Приложения уровня I:

- Написаны на языках программирования (C#, C++, Python и др.)
- Предоставляют интерфейсы для исполнения приложений уровня F.

3. Приложения уровня L:

- Библиотеки и сервисные программы на высокоуровневых языках.
- Независимые от платформы в плане двоичного формата.

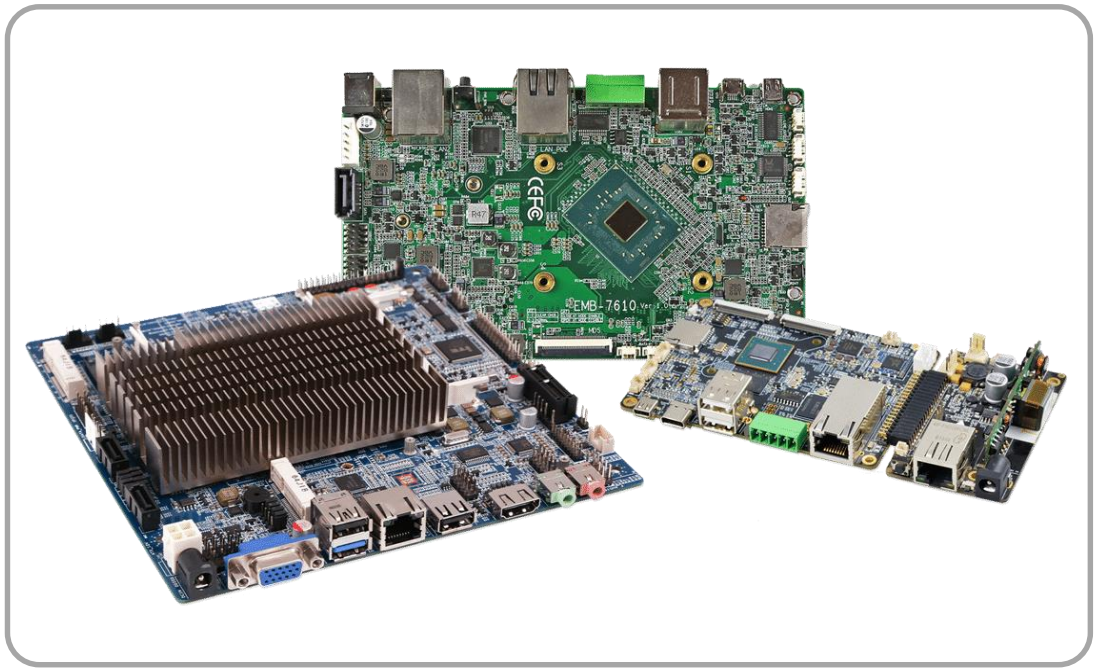
4. Приложения уровня O:

- Являются частью базовой операционной системы.
- Предоставляют среду для выполнения приложений уровней L и I.

Автор: Роман Шестаков
Координатор ТРГ по архитектуре и оркестратору ОАСУ ТП Межотраслевой РГ «Открытая АСУ ТП»

Современное устройство (ИЭУ, ПЛК)

- CPU
- Оперативная память
- Энергонезависимая память (Flash)
- Сетевые интерфейсы Ethernet
- BIOS/UEFI/U-Boot
- Операционная система (например, Linux)
- Системное ПО
- Прикладное ПО
- ЖК-экран



Это ПЛК или не ПЛК?

Пример архитектуры промышленного устройства

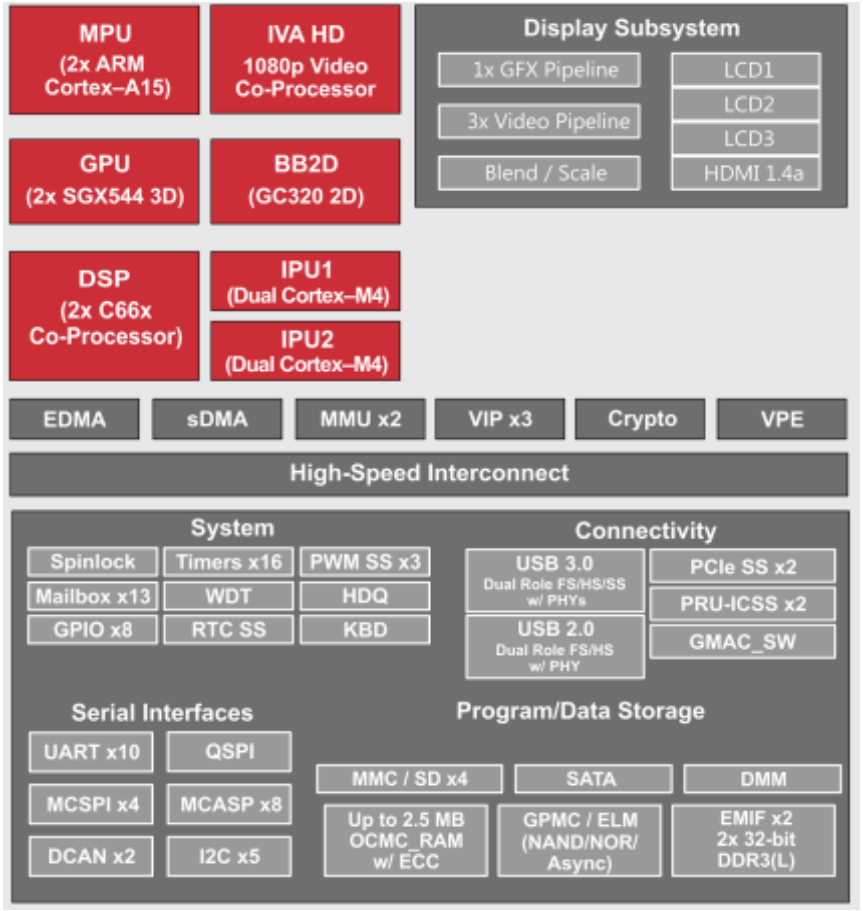
Современное устройство (ИЭУ, ПЛК):

- Компьютерная система.
- Объект критической информационной инфраструктуры.
- Значимый объект критической информационной инфраструктуры.
- Доверенный ПАК.

Пример СнК, используемого в промышленных устройствах

Современное устройство (ИЭУ, ПЛК):

- Может сочетать в себе микропроцессоры и микроконтроллеры.
- Может использовать как ОС жесткого и/или мягкого реального времени, так и ОС общего назначения.
- На соседних вычислителях совместно могут работать разные ОС.
- Жесткие требования к устойчивости к влиянию внешней среды.



Функциональная блок-схема СнК, распространенной в АСУ ТП и РЗА

Причины изучения экосистемы RISC-V для РЗА и АСУ ТП

Практические задачи, которые мы решали:

- Разработать прототип ПЛК открытой АСУ ТП.
- Оценить риски возникновения технологической зависимости.

Связанные задачи:

- Выбор СнК.
- Выбор загрузчика и операционной системы.
- Исследование производительности операционной системы.
- Исследование необходимости векторных расширений в задачах РЗА и АСУ ТП (вычисление тригонометрических функций, матриц и рядов).
- Оценка применимости СнК на базе архитектуры RISC-V для задач РЗА и АСУ ТП.

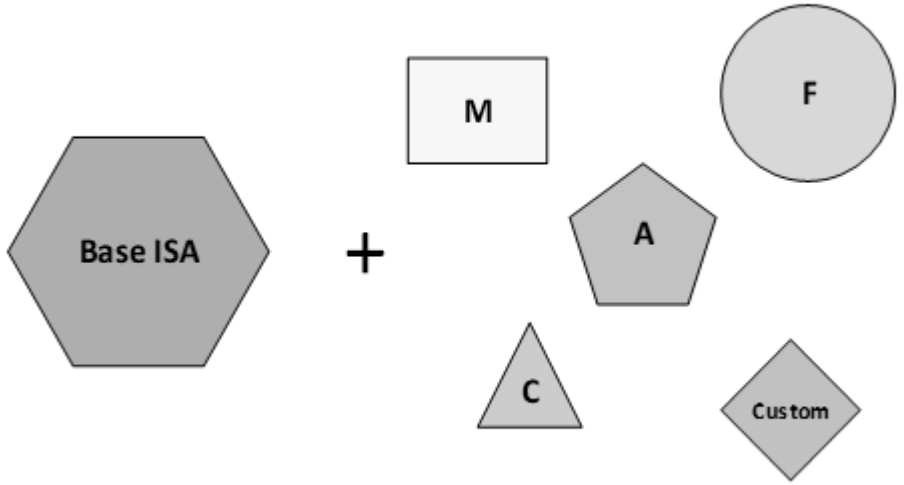
Адаптивность архитектуры для национальных задач

- Модульная – можно исключить всё лишнее

- Расширяемая – и можно добавить своё:

Технологическим комитетом Альянса разработана спецификация криптографических расширений Xkgost

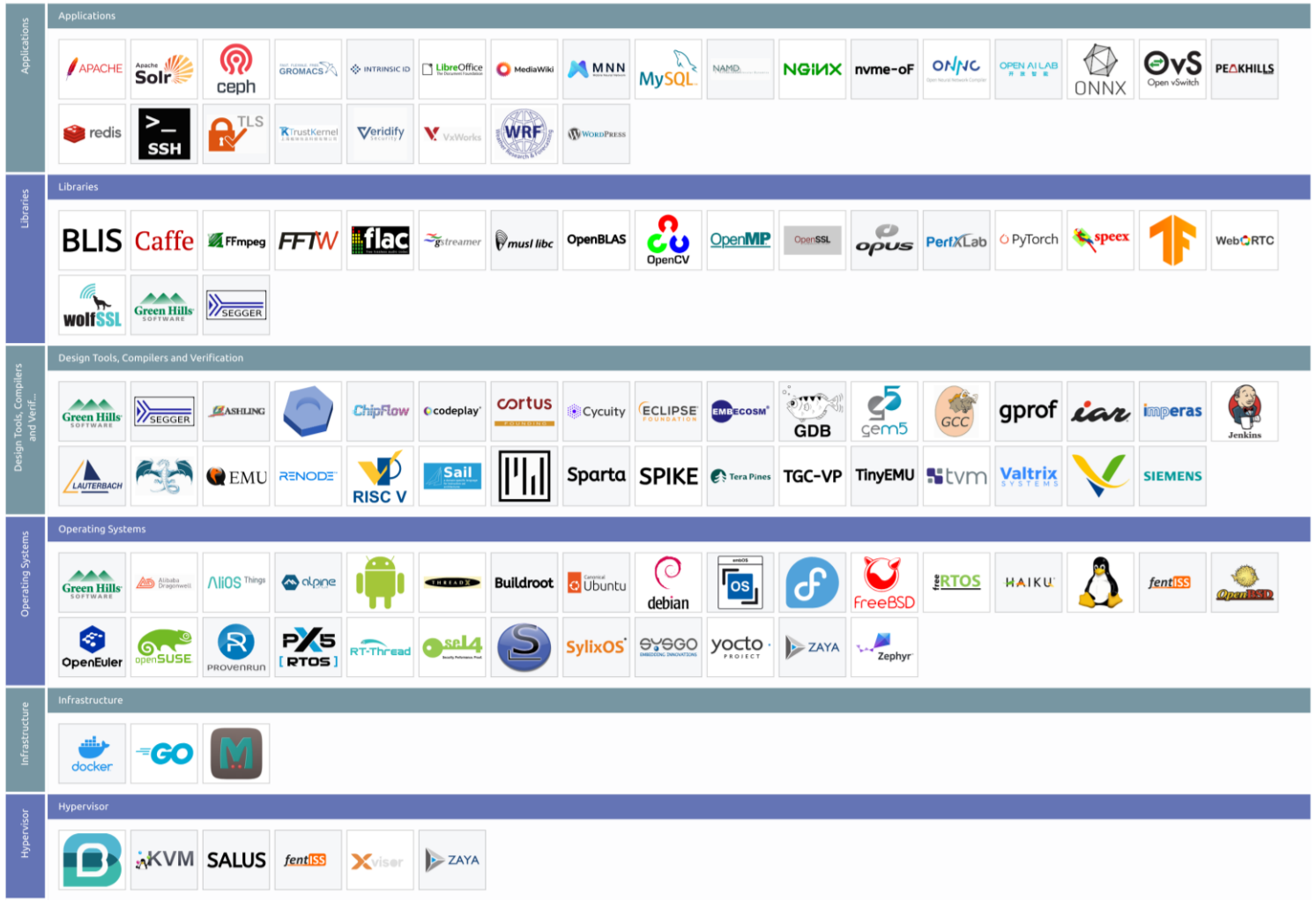
- Открытые проекты показывают возможность реализации корня доверия: OpenTitan



Потребности разработчиков ПАК для РЗА и АСУ ТП

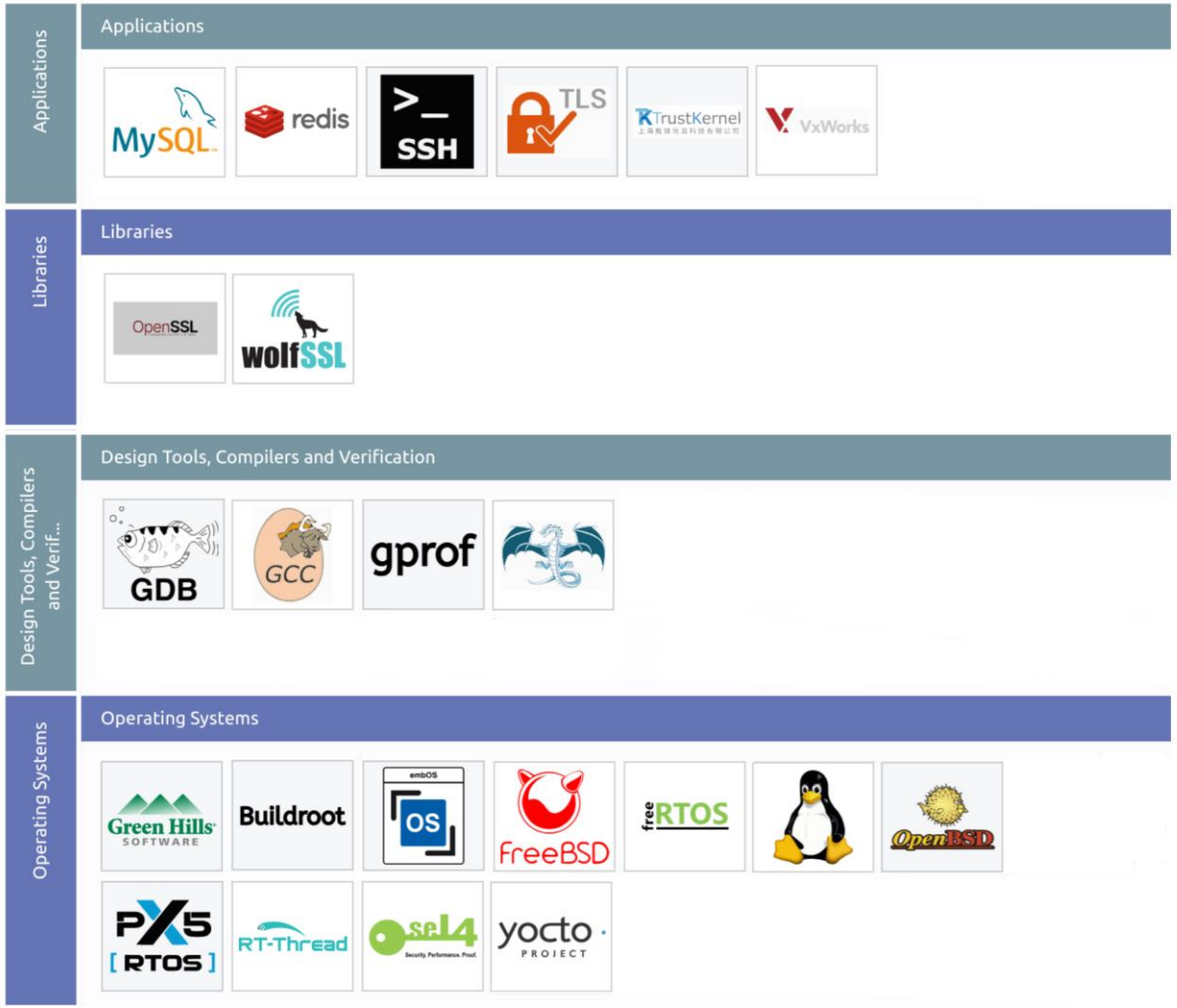
- Производительность СнК (4 ядра от 1,5 ГГЦ).
- Состав периферии (желательно несколько RJ45, GPIO).
- Профили и спецификации ядер СнК (поддержка Linux, векторные расширения).
- Поддержка механизмов доверенной загрузки в СнК.
- Аппаратная поддержка криптографии на уровне СнК (Кузнечик, Магма и Стрибог).
- Доверенные среды исполнения (TEE).
- Защищенная встраиваемая операционная система, обладающая свойствами мягкого реального времени.
- Страна-производитель СнК, не входящая в список недружественных стран.

Какое ПО нужно для промышленных задач?



Источник: riscv.landscape2.io

Какую экосистему ПО чаще всего представляют для АСУ ТП



Источник: riscv.landscape2.io

Операционные системы

Решаемые задачи:

- Работа в режиме жесткого реального времени.
- Работа в режиме мягко реального времени (чаще всего на MPU).

Существующие сложности:

- Отсутствие поддержки доступных СнК на базе RISC-V в отечественных ОСРВ.
- Отсутствие поддержки доступных СнК на базе RISC-V в сертифицированных во ФСТЭК России ОС.
- Отсутствие поддержки большинства одноплатных компьютерах в отечественных ОС.
- Отсутствие отечественных инструментов, позволяющих собирать ОС для встраиваемых систем (аналог Yocto или Buildroot).

Виртуализация и контейнеризация

Решаемые задачи:

- Разработка под целевые аппаратные платформа.
- Реализация программно-определяемых ПЛК.
- Инструментальное определение поверхности атаки с использованием полносистемной эмуляции.

Существующие сложности:

- Отсутствие в открытом доступе образов Qemu для эмуляции интересующих одноплатных компьютеров.
- Отсутствие поддержки в инструментах определения поверхности атаки.

Дальнейшие исследования: вопросы контейнеризации и виртуализации для задач открытой АСУ ТП.

Автоматизация процесса развертывания

Решаемые задачи:

- Автоматизация тестирования.
- Автоматизация развертывания на целевые платформы.
- Реализация программно-определяемых ПЛК.

Криптографические методы защиты информации

Решаемые задачи:

- Реализация механизмов доверенной загрузки (Secure Boot и Encrypted Boot).
- Построение защищенного сетевого взаимодействия по промышленным протоколам передачи данных.
- Реализация механизмов доверенного обновления.

Существующие сложности:

- Отсутствие сертифицированных в ФСБ России средств криптографической защиты информации, работающих на RISC-V.
- Отсутствие отечественной экосистемы ПО для работы с корнем доверия и доверенной загрузкой.

Прикладное программное обеспечение ч.1

Решаемые задачи:

- Работа с сетевым трафиком с высокими требованиями к времени обработки.
- Обработка, хранение и передача информации о технологических процессах.

Существующие сложности:

- Малое количество поддерживаемых DPDK СнК (SiFive U740 SoC и Generic rv64gc ISA).
- Высокая стоимость сертифицированных во ФСТЭК России СУБД.

DPDK
DATA PLANE DEVELOPMENT KIT

PostgreSQL

Прикладное программное обеспечение ч.2

Решаемые задачи:

- Применение интегрированных сред разработки и исполнения, в том числе, Runtime.
- Управление технологическим процессом.

Существующие сложности:

- Малое количество поддерживаемых в Beremiz и Open PLC СнК и их периферии.
- Отсутствие отечественных Runtime, работающих на RISC-V.

Прикладное программное обеспечение ч.3

Решаемые задачи:

- Реализация человеко-машинных интерфейсов.

Существующие сложности:

- Высокая стоимость сертифицированных во ФСТЭК России JDK.

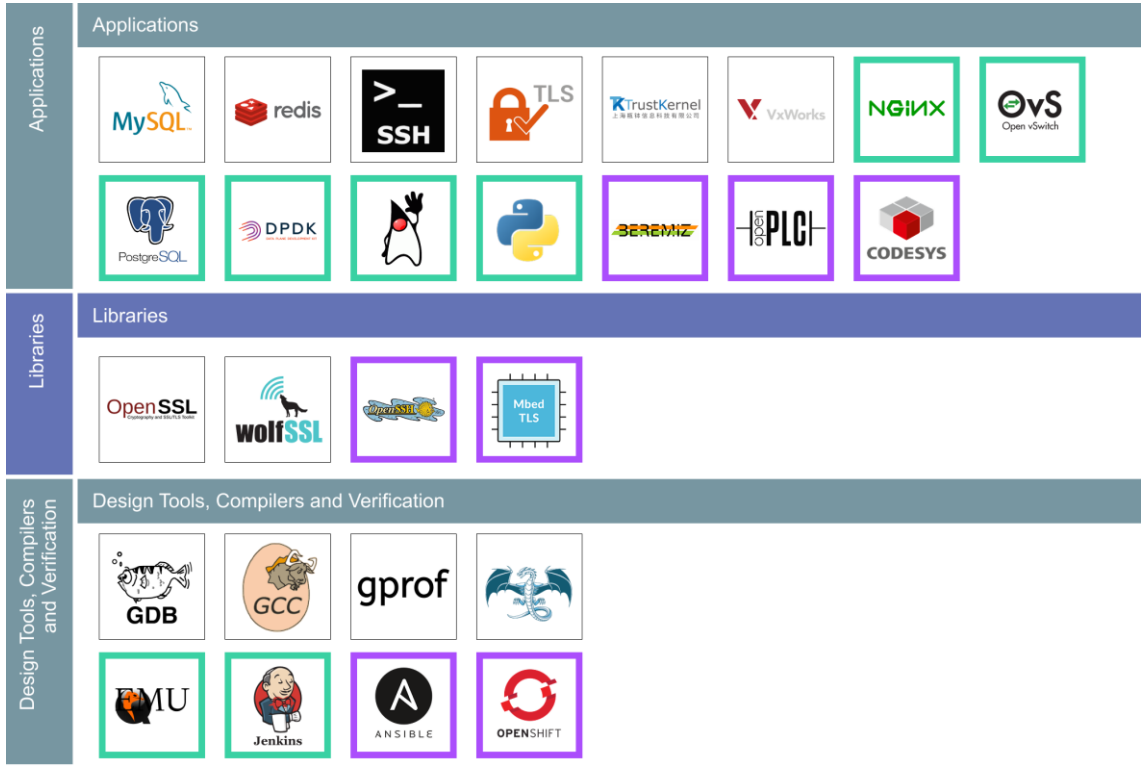
Spring Boot

spring SECURITY

OpenJDK

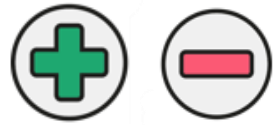
NGINX

Требуемая экосистема ПО для АСУ ТП



- ПО экосистемы RISC-V, которое не ожидают увидеть в АСУ ТП.
- ПО, которого нет в классическом RISC-V Landscape.

Инструменты для разработки безопасного ПО

Безопасный компилятор	
Инструментальное определение поверхности атаки	
Статический анализатор	
Инструменты композиционного анализа	
Динамический анализ и фаззинг-тестирование	

Обзор одноплатных компьютеров для задач АСУ ТП и РЗА

ЦЕНТР НТИ МЭИ
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ

№	Одноплатный компьютер	СнК (ядра)	ОЗУ	ПЗУ	Ethernet	USB	GPIO, pin
1	**OrangePi RV**	**StarFive JH7110 (4 ядра U74 1.5 ГГц)**	**8 ГБ LPDDR4**	**SDCard**	**1 x 1GB**	**2 x USB 3.0**	**40**
2	**StarFive VisionFive 2**	**StarFive JH7110 (4 ядра U74 1.5 ГГц)**	**8 ГБ LPDDR4**	**SDCard**	**2 x 1GB**	**2 x USB 3.0, 2 x USB 2.0**	**40**
3	**Banana Pi BPI-F3**	**SpacemiT K1 (8 ядер X60 1.6 ГГц)**	**8 ГБ LPDDR4**	**eMMC (32 ГБ) + SDCard**	**2 x 1GB**	**4 x USB 3.0**	**26**
4	**BeagleV-Ahead**	**TH1520 (4 ядра T-Head Xuantie C910 2 ГГц)**	**8 ГБ LPDDR4**	**eMMC (16 ГБ) + SDCard**	**1 x 1GB**	**Нет**	**92**
5	CanMV-K230	Kendryte K230 (1 ядро 800 МГц и 1 ядро 1.6 ГГц)	512MB DDR3	SDCard	1 x 100MB	1 x USB 2.0	40
6	Smartfly Kendryte K510	Kendryte K510 (2 ядра 800 МГц и 1 DSP ядро 800 МГц)	512MB DDR3	eMMC (16 ГБ)	1 x 1GB	1 x micro USB 2.0	30
7	**Lichee Pi 4A**	**TH1520 (4 ядра T-Head Xuantie C910 2 ГГц)**	**16 ГБ LPDDR4**	**eMMC (128 ГБ) + TF-Card**	**2 x 1GB**	**4 x USB 3.0**	**10**
8	Smartfly Nezha	Allwinner D1-H (1 ядро T-Head XuanTie C906 1 ГГц и 1 DSP ядро HiFi4 600 МГц)	2 ГБ LPDDR3	eMMC (16 ГБ)	1 x 1GB	1 x USB 2.0, 1 x USB C 2.0	40
9	Milk-V Duo S	SG2000 (1 ядро T-Head XuanTie C906 1 ГГц и 1 ядро T-Head XuanTie C906 700 МГц)	512MB DDR3	eMMC (8 ГБ)	1 x 100MB	1 x USB C 2.0	54
10	BeagleV-Fire	MPFS025T (FPGA 667 МГц, 4 ядра SiFive U54-MC 1,5 ГГц, 1 ядро SiFive E51 1,5 ГГц)	2 ГБ LPDDR4	eMMC (16 ГБ)	1 x 1GB	Нет	98

Технологически задача создания одноплатных компьютеров для АСУ ТП и РЗА решена. - время Российских решений пришло…

ЦЕНТР НТИ МЭИ
АЛЬЯНС
ТЕХНОЛОГИИ ТРАНСПОРТИРОВКИ ЭЛЕКТРОЭНЕРГИИ И РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГОСИСТЕМ
RISC-V

№	Одноплатный компьютер	СнК (ядра)	Профили, спецификации, расширения	
1	OrangePi RV	StarFive JH7110 (4 ядра U74 1.5 ГГц)	RVA20	RV64GC
2	StarFive VisionFive 2	StarFive JH7110 (4 ядра U74 1.5 ГГц)	RVA20	RV64GC
3	**Banana Pi BPI-F3**	**SpacemiT K1 (8 ядер X60 1.6 ГГц)**	**RVA22 + RVV 1.0**	**RV64GCVB**
4	**BeagleV-Ahead**	**TH1520 (4 ядра T-Head Xuantie C910 2 ГГц)**	**RVA20 + RVV 0.7.1**	**RV64GCV**
5	CanMV-K230	Kendryte K230 (1 ядро 800 МГц и 1 ядро 1.6 ГГц)	-	RV64GCB
6	Smartfly Kendryte K510	Kendryte K510 (2 ядра 800 МГц и 1 DSP ядро 800 МГц)	-	RV64GC
7	**Lichee Pi 4A**	**TH1520 (4 ядра T-Head Xuantie C910 2 ГГц)**	**RVA20+ RVV 0.7.1**	**RV64GCV**
8	**Smartfly Nezha**	**Allwinner D1-H (1 ядро T-Head XuanTie C906 1 ГГц и 1 DSP ядро HiFi4 600 МГц)**	**RVA20 + RVV 0.7.1**	**RV64GCV**
9	**Milk-V Duo S**	**SG2000 (1 ядро T-Head XuanTie C906 1 ГГц и 1 ядро T-Head XuanTie C906 700 МГц)**	**RVA20 + RVV 0.7.1**	**RV64GCV**
10	BeagleV-Fire	MPFS025T (FPGA 667 МГц, 4 ядра SiFive U54-MC 1,5 ГГц, 1 ядро SiFive E51 1,5 ГГц)	-	RV64GC (54-MC) RV64IMAC (E51)

Поддержка механизмов безопасности в СнК

№	Одноплатный компьютер	СнК (ядра)	Secure Boot	Аппаратная поддержка криптографии	TEE
1	OrangePi RV	StarFive JH7110 (4 ядра U74 1.5 ГГц)	Да	AES, SHA, DES, 3DES	Нет
2	**StarFive VisionFive 2**	**StarFive JH7110 (4 ядра U74 1.5 ГГц)**	**Да**	**AES, SHA, DES, 3DES**	**Да**
3	Banana Pi BPI-F3	SpacemiT K1 (8 ядер X60 1.6 ГГц)	Да	AES, SHA, RSA	Нет
4	**BeagleV-Ahead**	**TH1520 (4 ядра T-Head Xuantie C910 2 ГГц)**	**Да**	**AES, RSA, SHA, SM2, SM3, SM4**	**Да**
5	CanMV-K230	Kendryte K230 (1 ядро 800 МГц и 1 ядро 1.6 ГГц)	Да	AES, RSA, SHA, HMAC, SM2, SM3, SM4	Нет
6	Smartfly Kendryte K510	Kendryte K510 (2 ядра 800 МГц и 1 DSP ядро 800 МГц)	Нет	AES, SHA-2	Нет
7	**Lichee Pi 4A**	**TH1520 (4 ядра T-Head Xuantie C910 2 ГГц)**	**Да**	**AES, RSA, SHA, SM2, SM3, SM4**	**Да**
8	Smartfly Nezha	Allwinner D1-H (1 ядро T-Head XuanTie C906 1 ГГц и 1 DSP ядро HiFi4 600 МГц)	Нет	-	Нет
9	**Milk-V Duo S**	**SG2000 (1 ядро T-Head XuanTie C906 1 ГГц и 1 ядро T-Head XuanTie C906 700 МГц)**	**Да**	**AES, SHA**	**Да**
10	BeagleV-Fire	MPFS025T (FPGA 667 МГц, 4 ядра SiFive U54-MC 1,5 ГГц, 1 ядро SiFive E51 1,5 ГГц)	Да	AES, SHA, HMAC, RSA, ECDSA	Нет

Важные параметры для задач РЗА и АСУ ТП

Приоритет	Параметр, единицы измерения	Причина измерения	Отраслевые сценарии
1-2	Задержка планирования (scheduling latency), мкс	Исследование детерменированности поведения системы при исполнении rt-процессов.	Требования к детерминированности при выдачи управляющих воздействий.
1-2	Выполнение математических операций: 1. Целочисленные вычисления, MOPS 2. Вычисления с плавающей точкой, MFLOPS 3. Тест условных переходов, MOPS 4. Тест тригонометрических функций, MOPS 5. Операции присвоения, MOPS	Исследование производительности процессора с точки зрения математических операций.	Программная реализация алгоритмов РЗА строится на математических операциях и операторах ветвления. Скорость исполнения данных операций является критичной при реализации алгоритмов.
3	Сетевые взаимодействия: 1. Количество переданных данных, ГБ 2. Скорость передачи данных в сети, МБ/с 3. Потеря пакетов, % 4. Jitter, мс	Исследование возможностей сетевой подсистемы.	Качество работы сетевой подсистемы напрямую влияет на детерминированность и быстроту выполнения функций.
4	Взаимодействие с ОЗУ: 1.Скорость чтения/записи, МБ/с 2.Время доступа к памяти, нс	Исследование влияния различных режимов работы ОС на работу с ОЗУ.	Математические операции, используемые в алгоритмах РЗА и алгоритмах фильтрации токов и напряжений, важным является быстрое чтение и запись в ОЗУ.
5	Взаимодействие с ПЗУ: 1.Скорость чтения/записи, МБ/с 2.Задержки в считывании данных, мс	Исследование влияния режимов работы ОС при выполнении I/O с ПЗУ.	При реализации функций регистрации аварийных событий и журналирования важным является скорость записи в ПЗУ.

Выводы

- Требуются отечественные ядра, сопоставимые по производительности с SiFive U74.
- Требуются отечественные СнК, сопоставимые с Rockchip 3568/3588.
- СнК должны иметь поддержку Linux, возможность реализации доверенной загрузки и поддержка отечественной криптографии.
- Поддержка доступных СнК на базе RISC-V со стороны отечественных разработчиков ОС.
- Формирование отечественных инструментов, позволяющих собирать ОС для встраиваемых систем (аналог Yocto или Buildroot).
- Требуется снижение стоимостей лицензий сертифицированных во ФСТЭК России СУБД и JDK.
- Расширение поддержки RISC-V со стороны отечественных разработчиков инструментов РБПО.

Спасибо!

ул. Красноказарменная, д. 17
Москва, Россия

WWW.NTI.MPEI.RU