Внутреннее устройство эмулятора процессора на архитектуре RISC-V для портирования, разработки и отладки ПО

ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

IP-BLOCKS

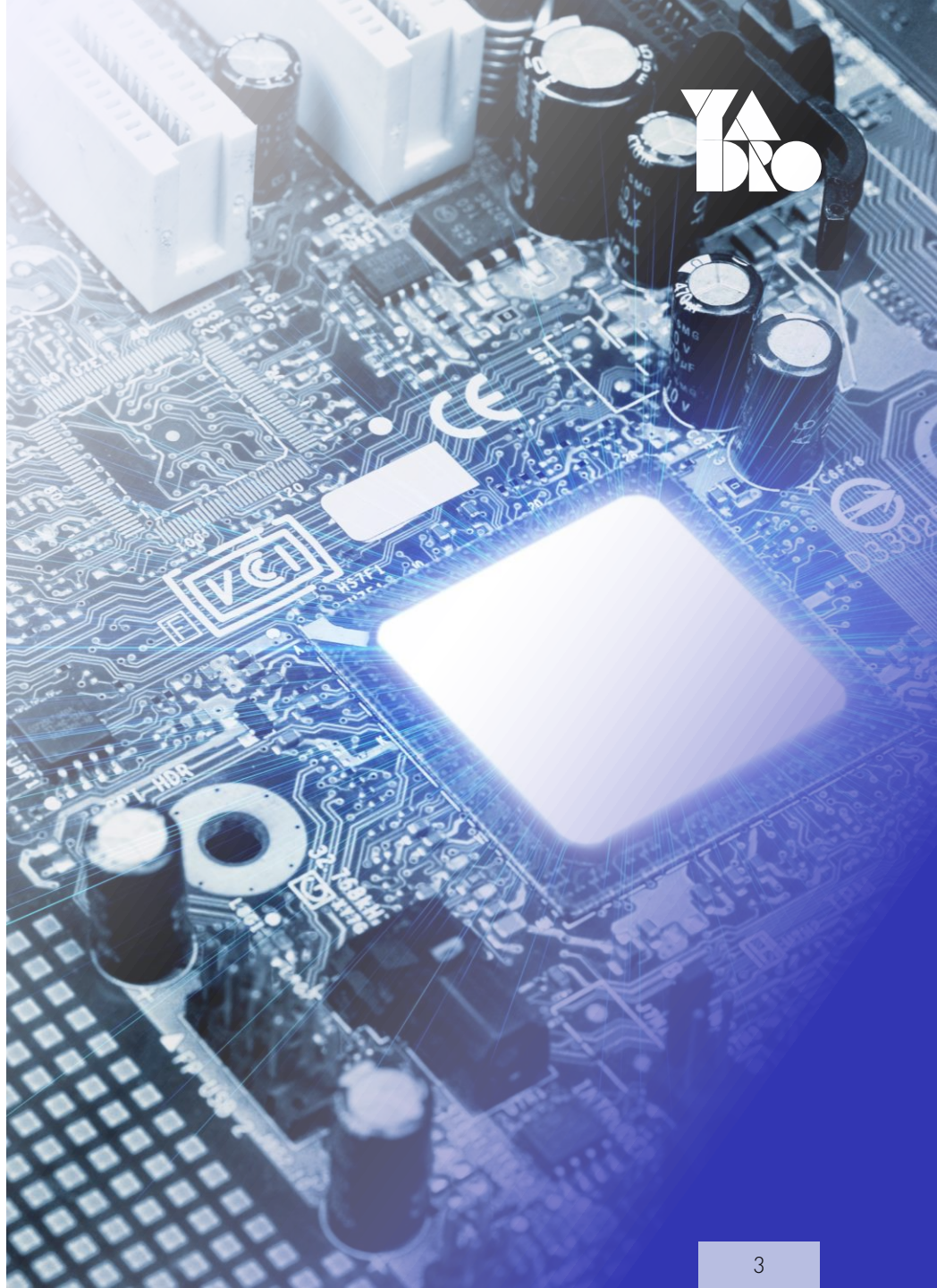
ВЕРИФИКАЦИЯ

CO-SIMULATION

- ПОДХОДЫ К ОТЛАДКЕ
- REMOTE PORT
- REMOTE PORT DPI
- HARDWARE CO-SIMULATION

Введение

- Разработка программируемых микросхем – сложный и длительный процесс
- Как отлаживать ПО в отсутствие аппаратуры?



ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

IP-BLOCKS

ВЕРИФИКАЦИЯ

CO-SIMULATION

- ПОДХОДЫ К ОТЛАДКЕ
- REMOTE PORT
- REMOTE PORT DPI
- HARDWARE CO-SIMULATION

Имитация: симуляция и эмуляция

Симулируются свойства, поведение, функции объекта

Эмулируется сам объект с сохранением принципов работы

Абстрагировано от аппаратных средств

Физическая машина — хост, эмулируемая система — гость

ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

IP-BLOCKS

ВЕРИФИКАЦИЯ

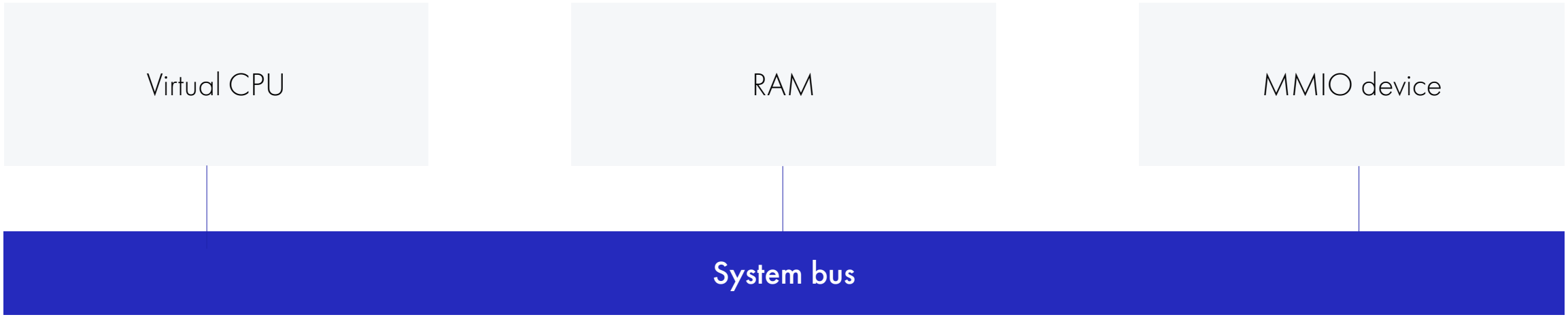
CO-SIMULATION

- ПОДХОДЫ К ОТЛАДКЕ
- REMOTE PORT
- REMOTE PORT DPI
- HARDWARE CO-SIMULATION

QEMU (Quick EMUlator)

- Полная эмуляция компьютера со всем оборудованием
- Может загружать различные ОС
- Может эмулировать различные процессорные архитектуры
- Бесплатный с открытым исходным кодом
- Может эмулировать практически любое устройство
- Поддерживается большим активным сообществом

QEMU overview



- Эмуляция CPU: Tiny Code Generator (динамическая двоичная трансляция)
- RAM: используется host-RAM
- Устройства: Memory Mapped I/O devices
- Sysbus моделируется

- QEMU API: Объектная модель, наследование
- Динамические и статические устройства
- Главный цикл QEMU: main loop

ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

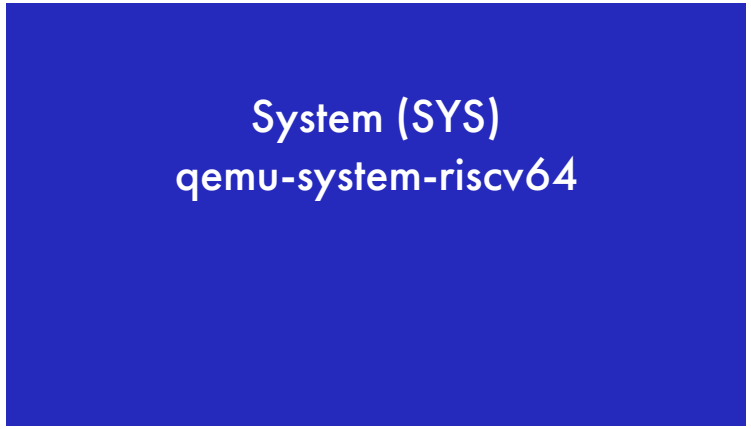
IP-BLOCKS

ВЕРИФИКАЦИЯ

CO-SIMULATION

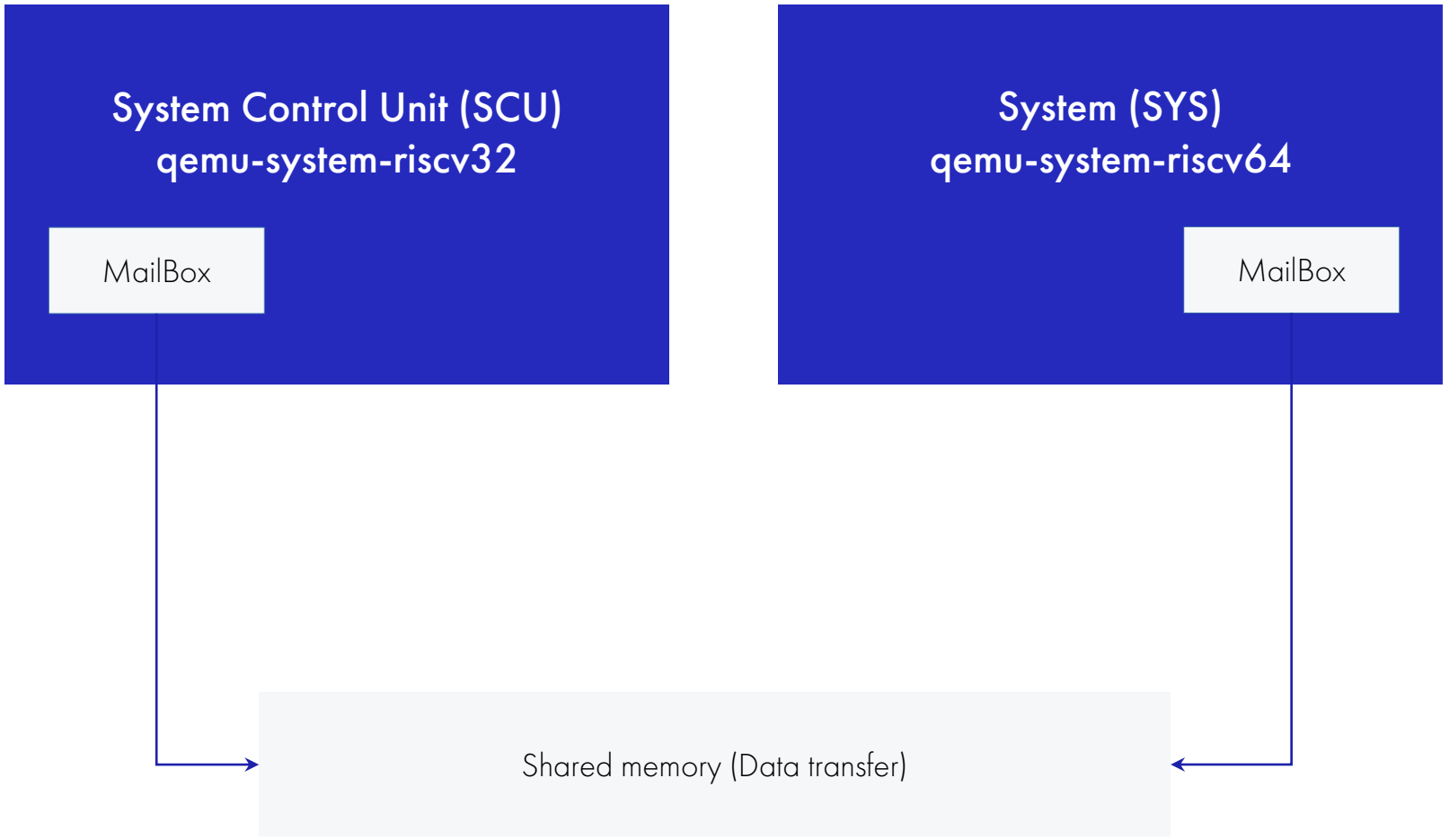
- ПОДХОДЫ К ОТЛАДКЕ
- REMOTE PORT
- REMOTE PORT DPI
- HARDWARE CO-SIMULATION

SCU – SYS (RISC-V)



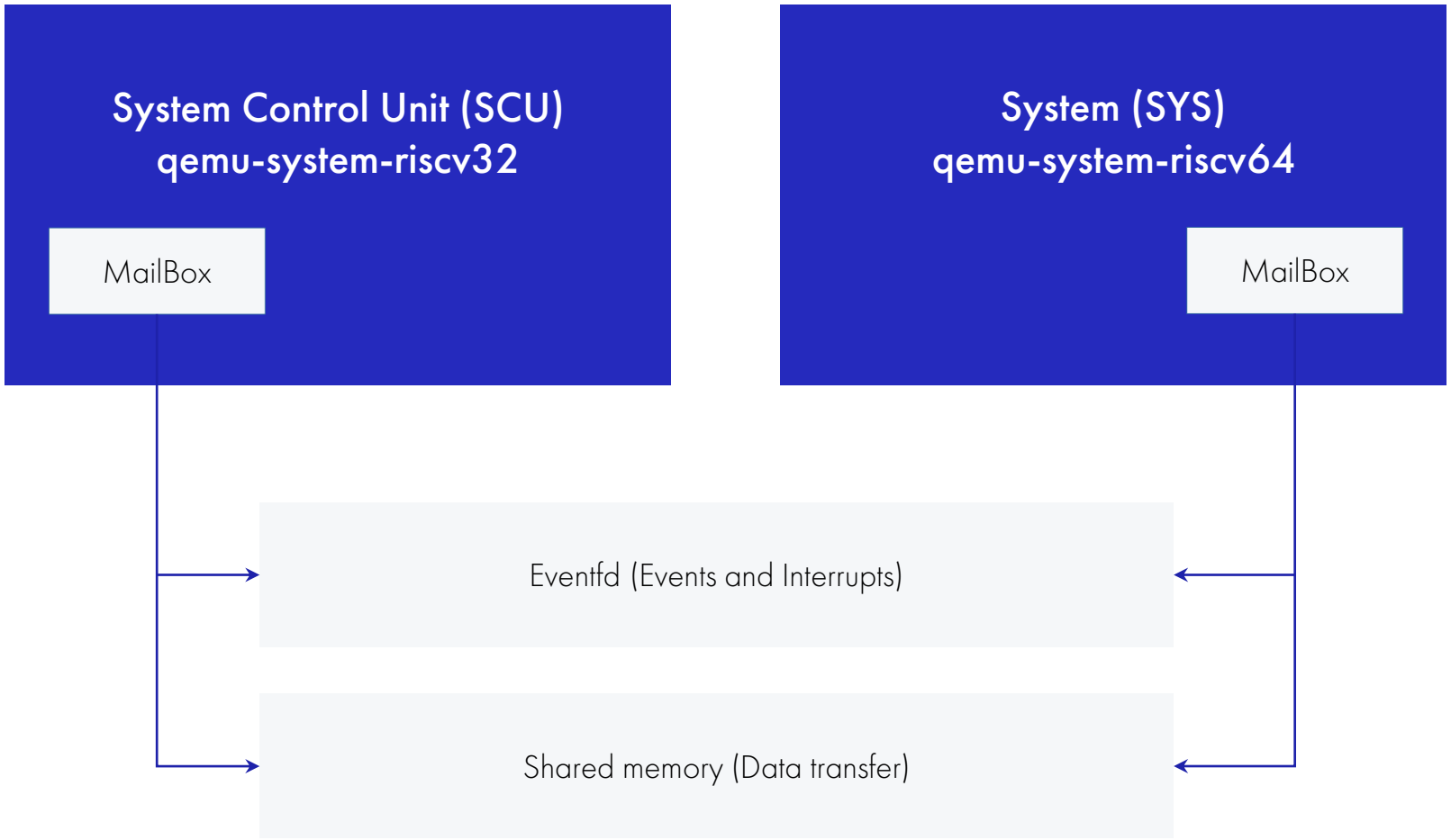
- SCU и SYS – запускаются как два отдельных процесса
- Mailbox: shared memory, куда оба процесса могут писать/читать
- Для сообщения о событии используется eventfd
- Interconnect: обмен файловыми дескрипторами через сокет
- Обработка событий регулируется главным циклом QEMU (main loop)

SCU – SYS (RISC-V)



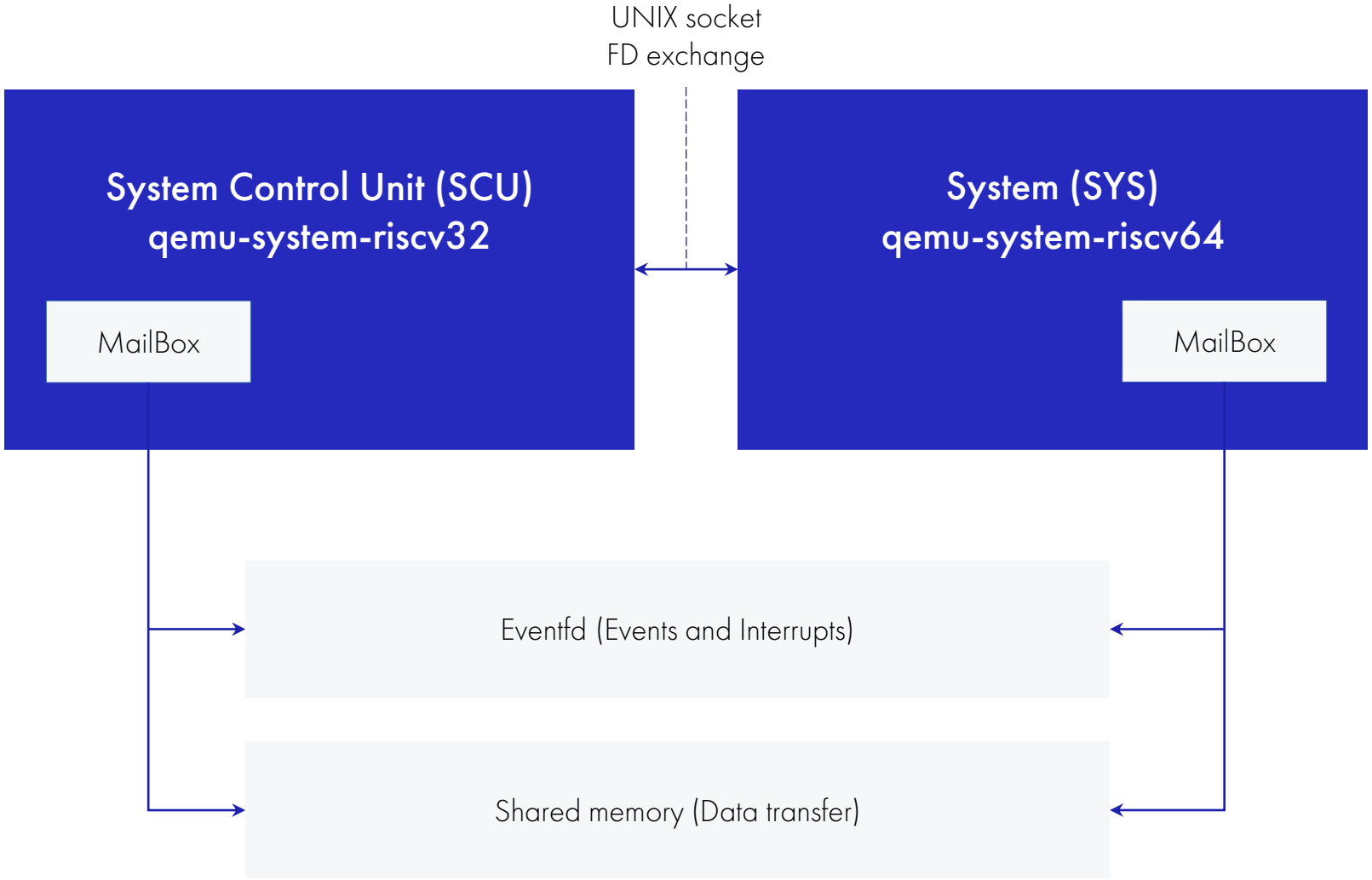
- SCU и SYS – запускаются как два отдельных процесса
- Mailbox: shared memory, куда оба процесса могут писать/читать
- Для сообщения о событии используется eventfd
- Interconnect: обмен файловыми дескрипторами через сокет
- Обработка событий регулируется главным циклом QEMU (main loop)

SCU – SYS (RISC-V)



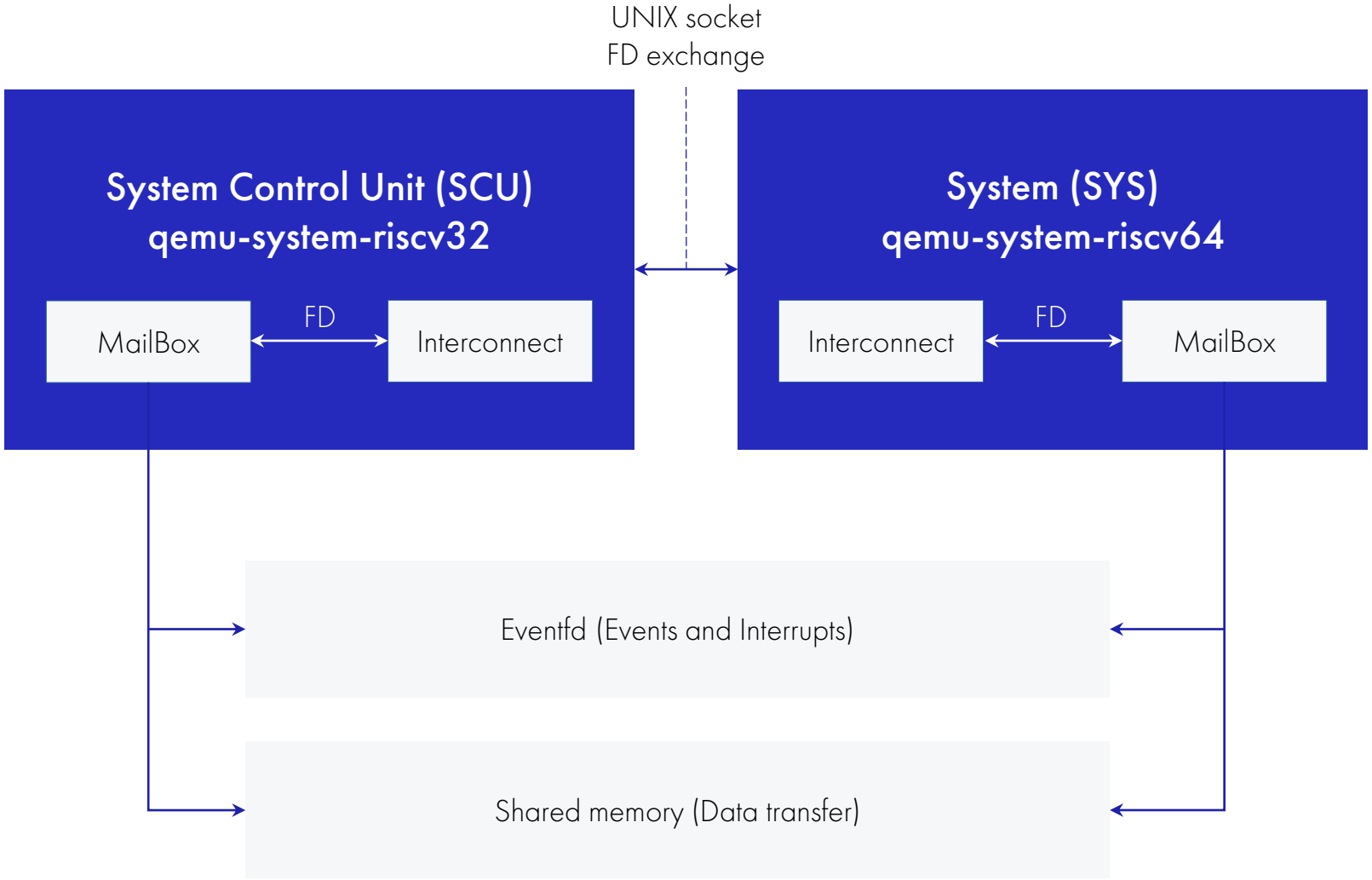
- SCU и SYS – запускаются как два отдельных процесса
- Mailbox: shared memory, куда оба процесса могут писать/читать
- Для сообщения о событии используется eventfd
- Interconnect: обмен файловыми дескрипторами через сокет
- Обработка событий регулируется главным циклом QEMU (main loop)

SCU – SYS (RISC-V)



- SCU и SYS – запускаются как два отдельных процесса
- Mailbox: shared memory, куда оба процесса могут писать/читать
- Для сообщения о событии используется eventfd
- Interconnect: обмен файловыми дескрипторами через сокет
- Обработка событий регулируется главным циклом QEMU (main loop)

SCU – SYS (RISC-V)



- SCU и SYS – запускаются как два отдельных процесса
- Mailbox: shared memory, куда оба процесса могут писать/читать
- Для сообщения о событии используется eventfd
- Interconnect: обмен файловыми дескрипторами через сокет
- Обработка событий регулируется главным циклом QEMU (main loop)

ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

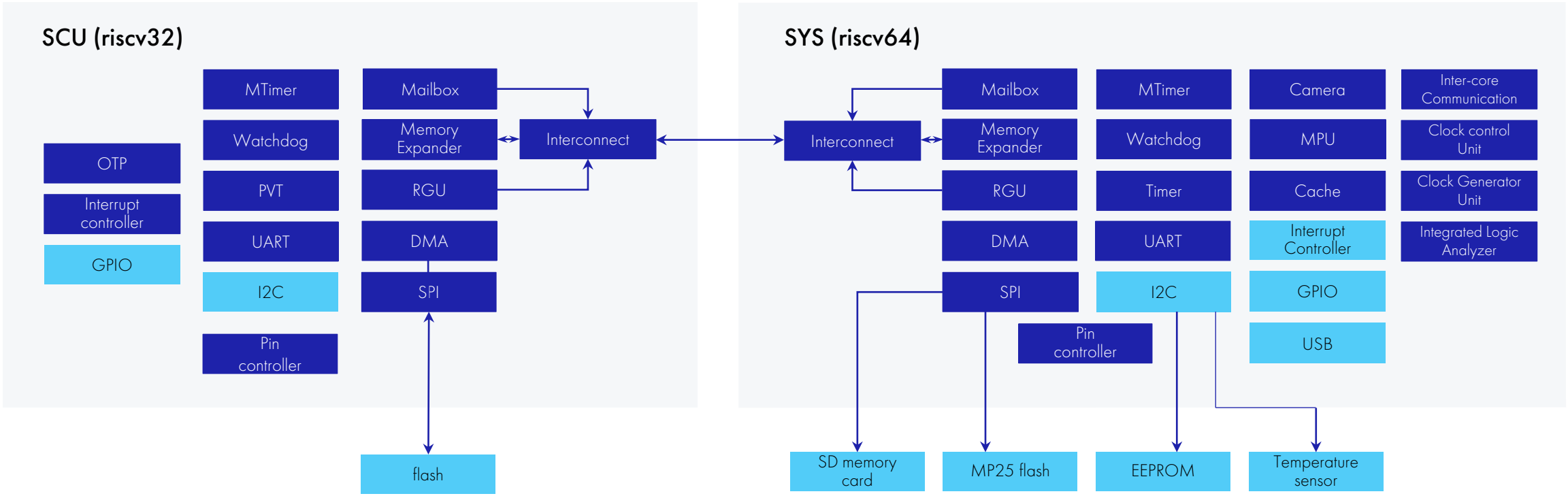
IP-BLOCKS

ВЕРИФИКАЦИЯ

CO-SIMULATION

- ПОДХОДЫ К ОТЛАДКЕ
- REMOTE PORT
- REMOTE PORT DPI
- HARDWARE CO-SIMULATION

IP-blocks



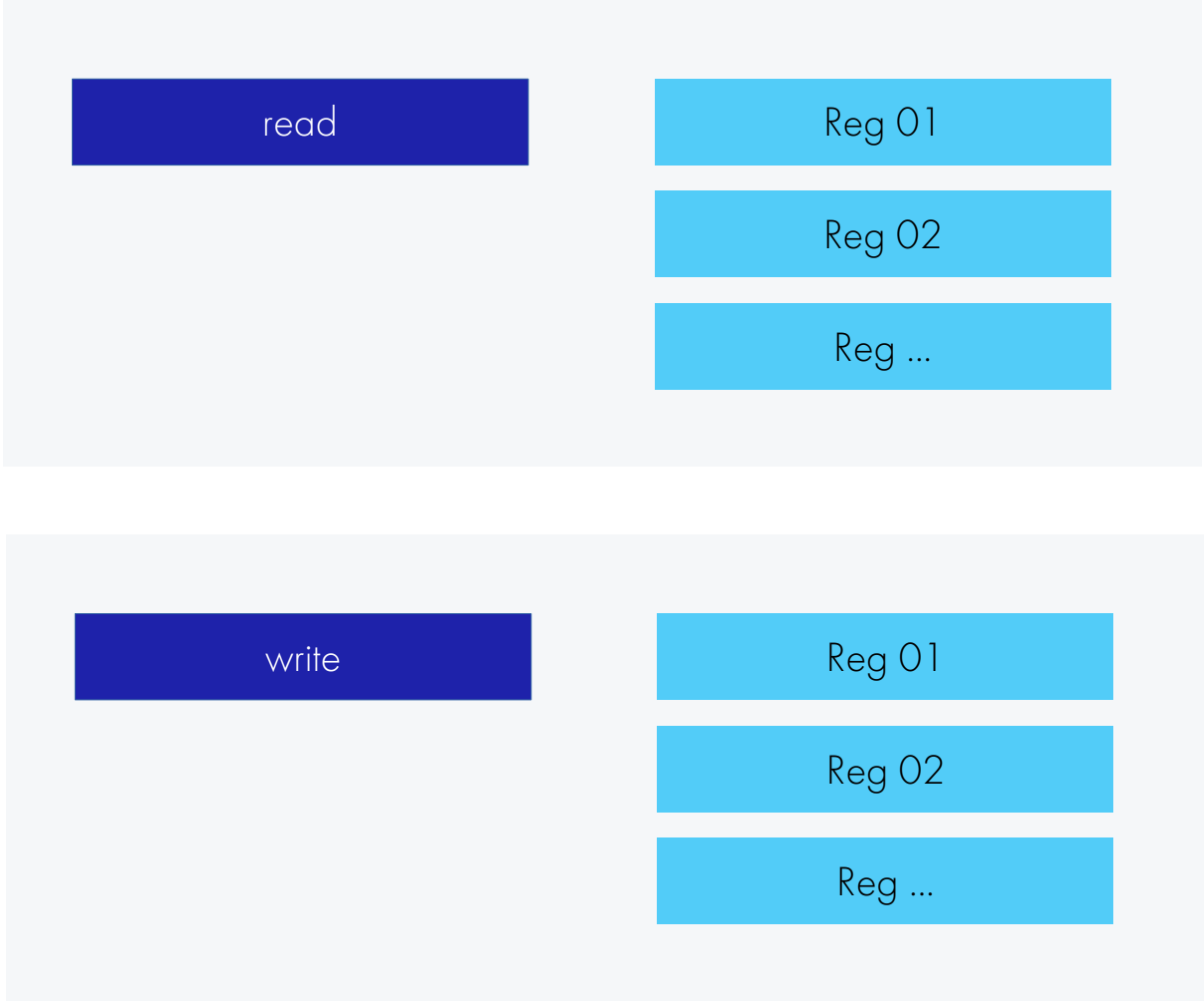
- Моделируются IP-блоки внутри чипа и периферия: наша разработка и QEMU-сообщество
- Полнота функционала зависит от требований целевого ПО

Наша разработка

QEMU-сообщество

Реализация устройств в QEMU

- Привязка к участку памяти
- Релазация callback функций read/write
- Определение регистров и их оффсетов
- Интерпретация чтения/записи в регистры



ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

IP-BLOCKS

ВЕРИФИКАЦИЯ

CO-SIMULATION

- ПОДХОДЫ К ОТЛАДКЕ
- REMOTE PORT
- REMOTE PORT DPI
- HARDWARE CO-SIMULATION

Верификация

Модели IP-блоков: функциональные тесты на Си и Ассемблере

Эмулятор: регрессионное тестирование

Тесты: тест должен давать одинаковые результаты на модели в QEMU и на RTL-модели

Аппаратная часть совместно с ПО: эмулятор + потактовый симулятор или FPGA

ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

IP-BLOCKS

ВЕРИФИКАЦИЯ

CO-SIMULATION

ПОДХОДЫ К ОТЛАДКЕ

REMOTE PORT

REMOTE PORT DPI

HARDWARE CO-SIMULATION

ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

IP-BLOCKS

ВЕРИФИКАЦИЯ

CO-SIMULATION

ПОДХОДЫ К ОТЛАДКЕ

REMOTE PORT

REMOTE PORT DPI

HARDWARE CO-SIMULATION

QEMU

Плюсы:	Минусы:
Высокая скорость симуляции	Сложность разработки моделей некоторых устройств (кодеки, GPU) для которых есть готовый RTL
Возможность запуска Linux	Сложность подключения внешней периферии (камеры, экраны)

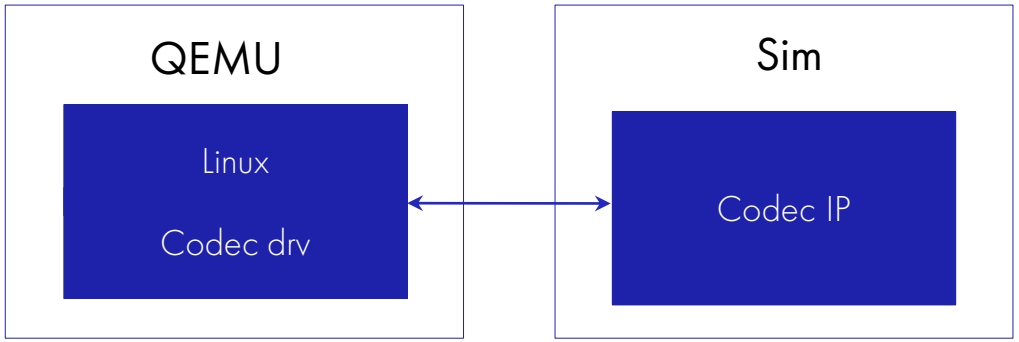
Потактовый симулятор

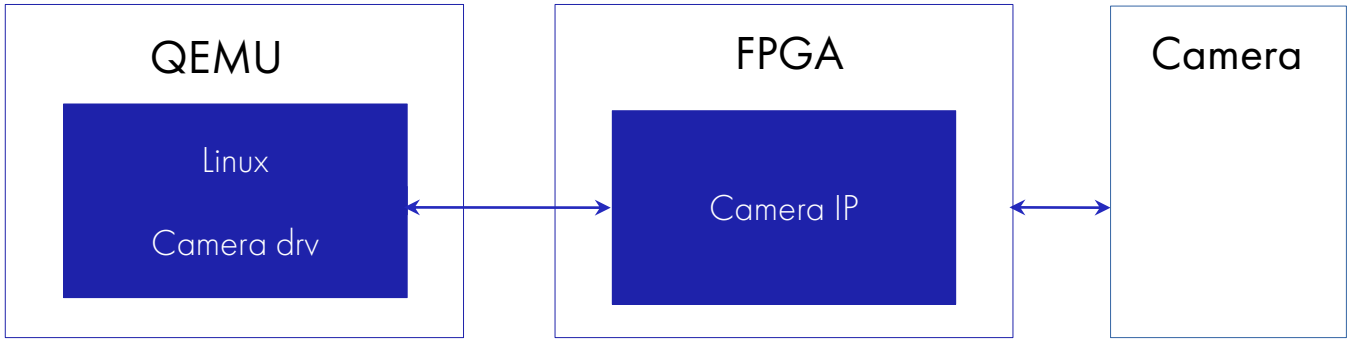
Плюсы:	Минусы:
Возможность точной симуляции	Низкая скорость симуляции
Наличие готовых моделей RTL	Невозможно запустить Linux

FPGA-прототип

Плюсы:	Минусы:
Возможность подключить внешнюю периферию	Дорого (over 300k $);
Возможность симулировать чип целиком	Долго (пересборка дизайна > 12 часов);
	Низкие тактовые частоты (50-100 MHz);
	Проблема partitioning (разделение дизайна на несколько FPGA)

Co-simulation





Программная:

- QEMU + simulator (VSC, SystemC, etc...)

Аппаратно-программная:

- QEMU + FPGA

ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

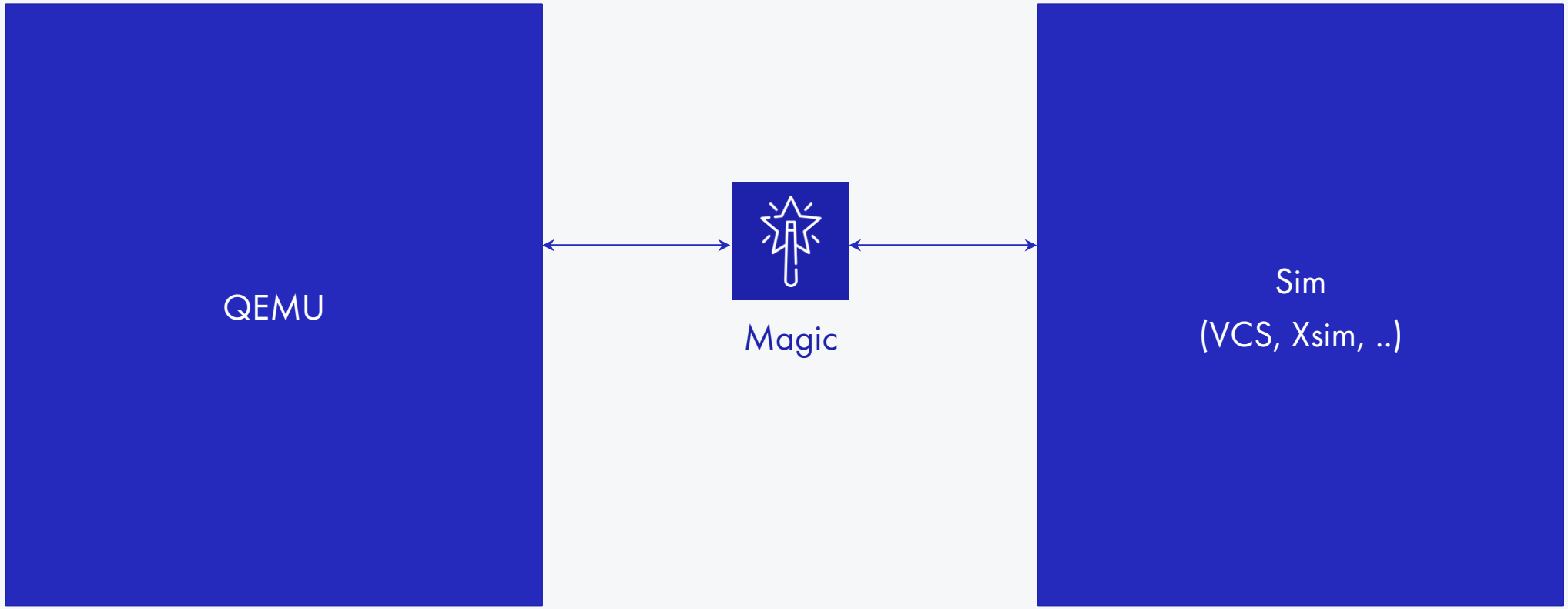
IP-BLOCKS

ВЕРИФИКАЦИЯ

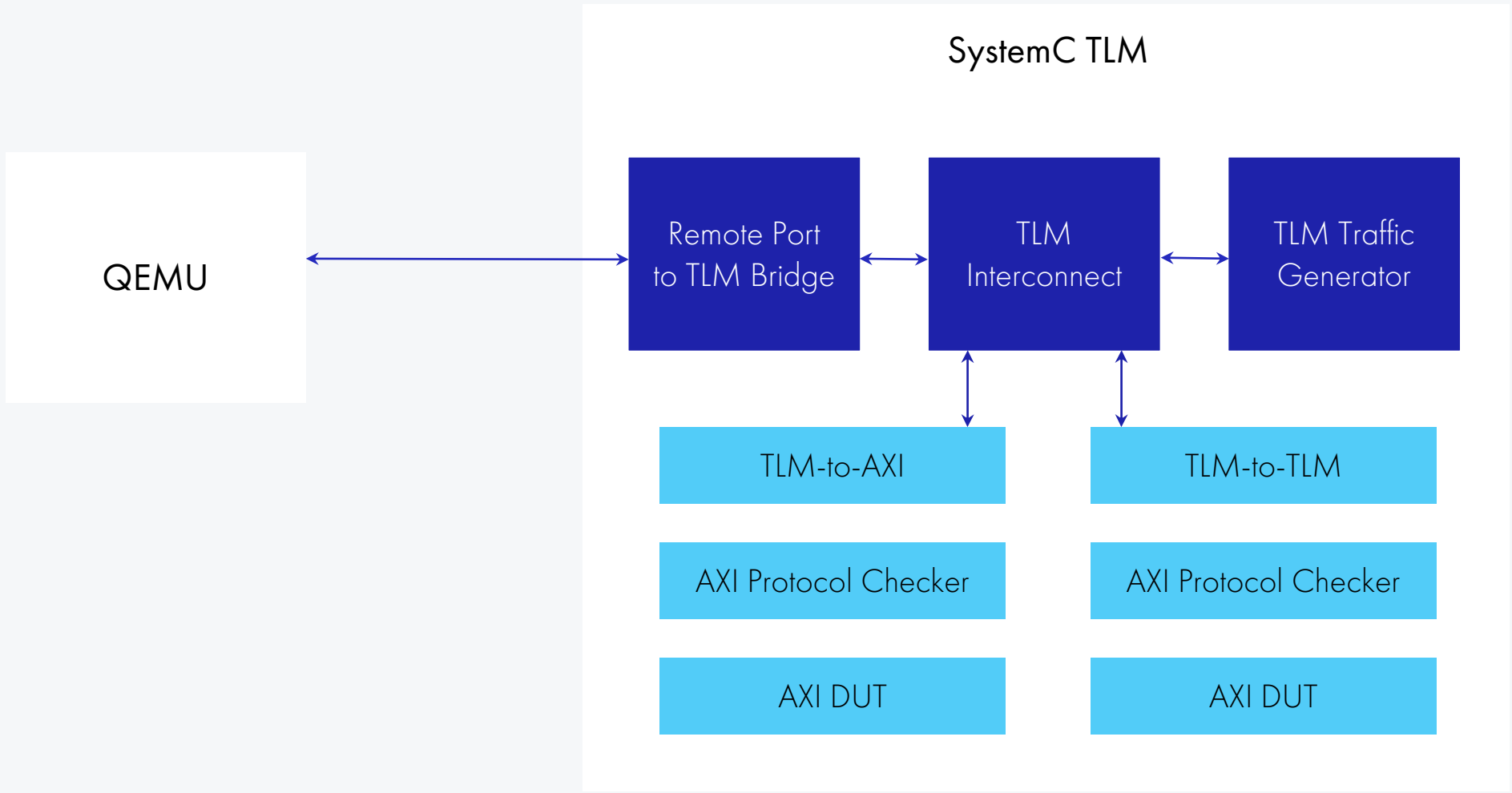
CO-SIMULATION

- ПОДХОДЫ К ОТЛАДКЕ
- **REMOTE PORT**
- REMOTE PORT DPI
- HARDWARE CO-SIMULATION

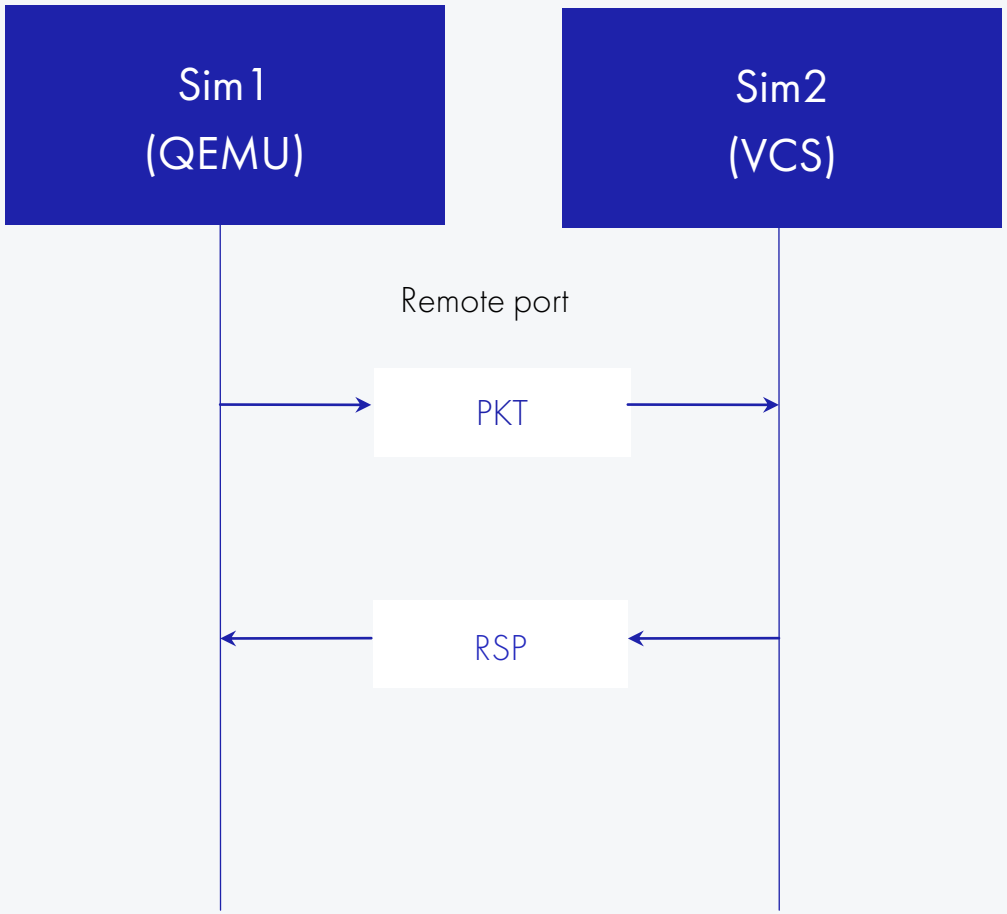
Architecture



Remote Port TLM



RP transactions



- Hello
- CFG
- Read
- Write
- Interrupt
- Sync
- ATS request
- ATS invalidate

RP packets

Base:

- Command
- Length
- ID
- Flags
- Device

Read/write data:

- Address
- Data
- Length
- Width
- Byte Enable
- Timestamp

ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

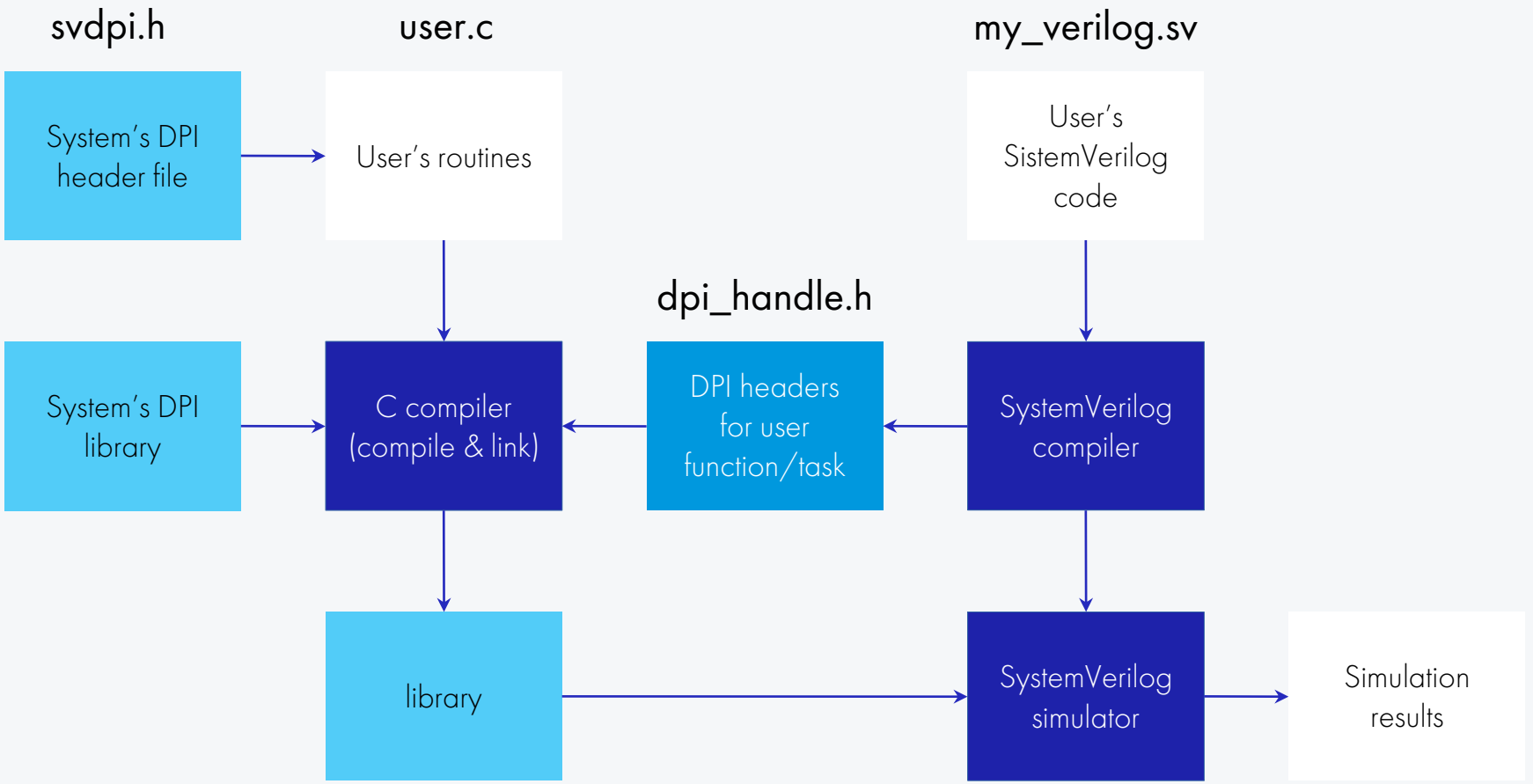
IP-BLOCKS

ВЕРИФИКАЦИЯ

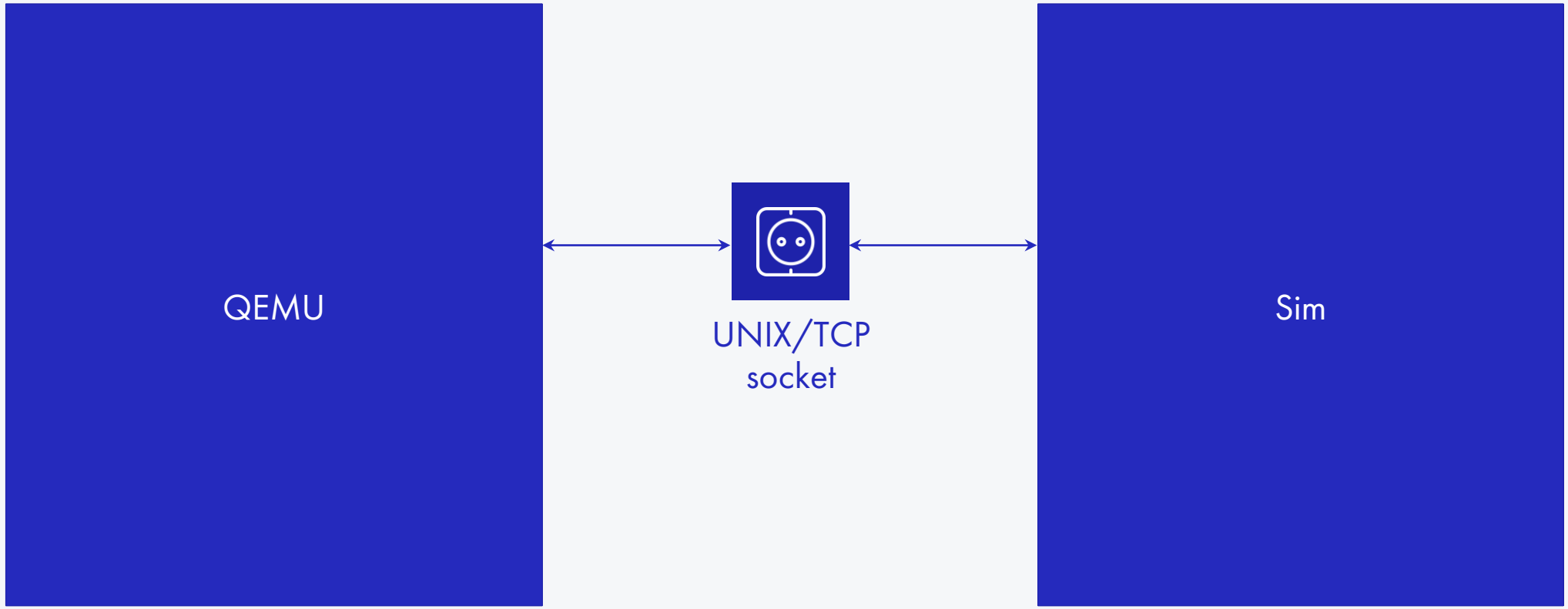
CO-SIMULATION

- ПОДХОДЫ К ОТЛАДКЕ
- REMOTE PORT
- **REMOTE PORT DPI**
- HARDWARE CO-SIMULATION

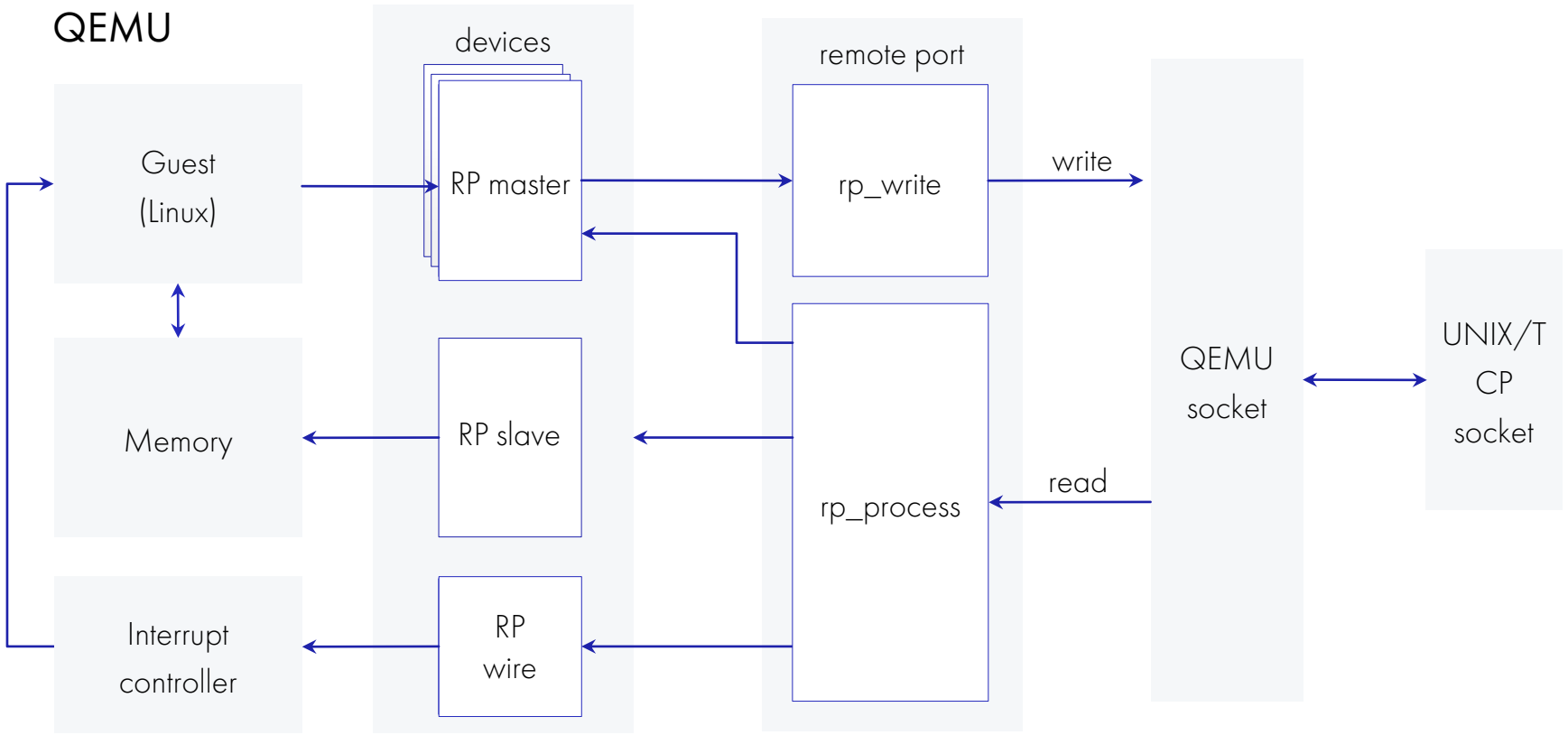
System Verilog DPI



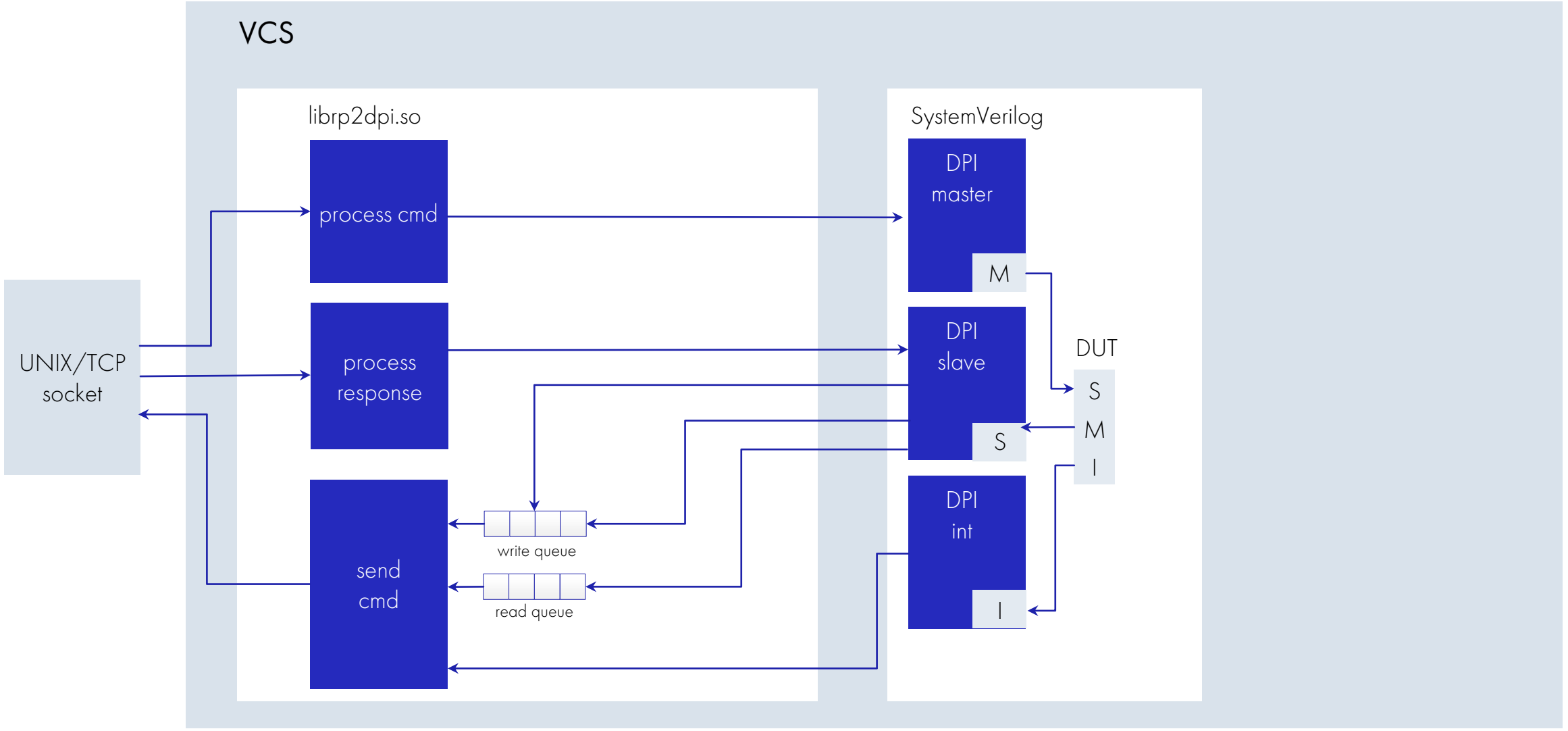
Architecture



Architecture (QEMU part)



Architecture (Sim part)



ВВЕДЕНИЕ

ИМИТАЦИЯ

QEMU

INTERCONNECT

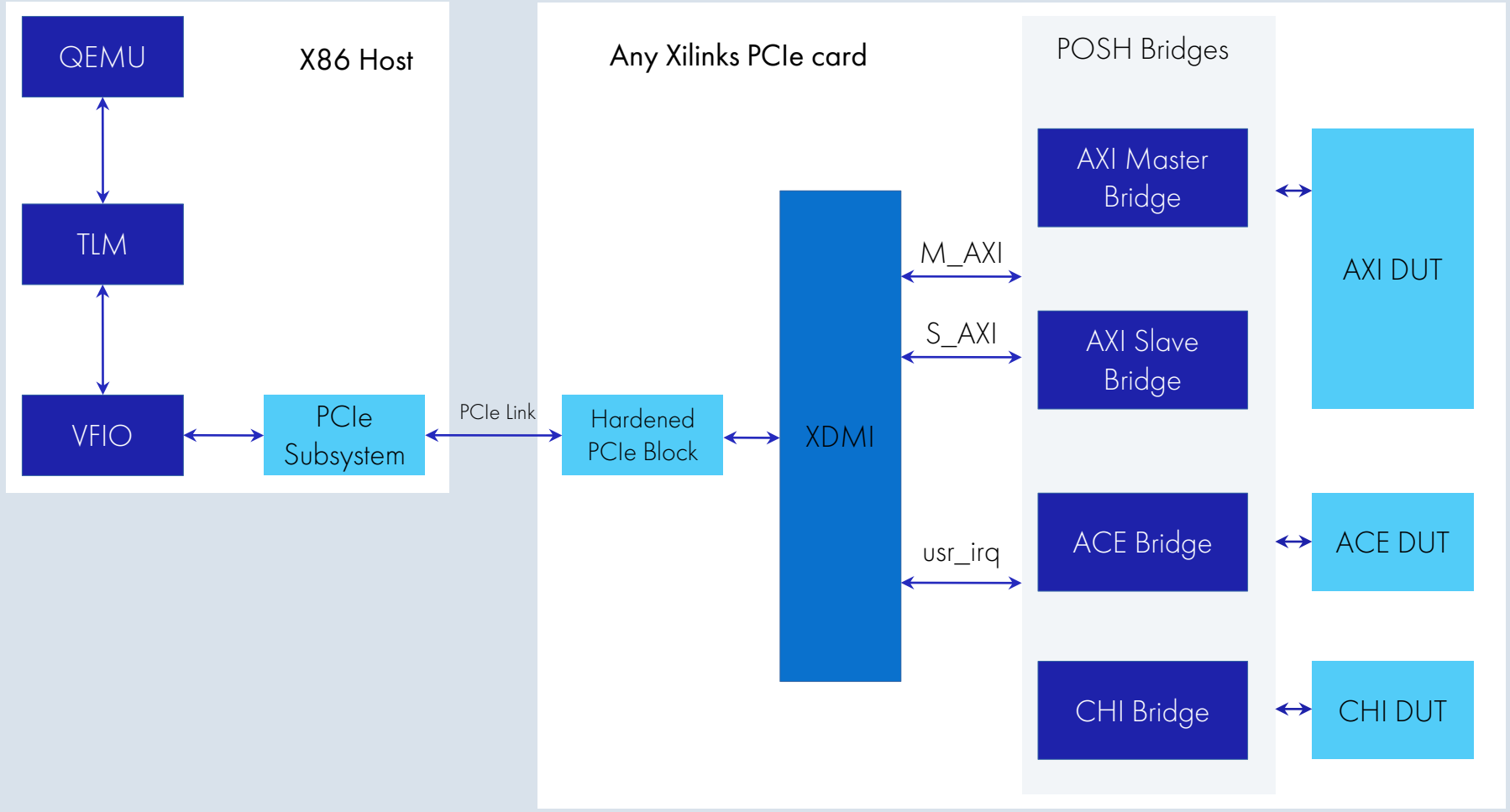
IP-BLOCKS

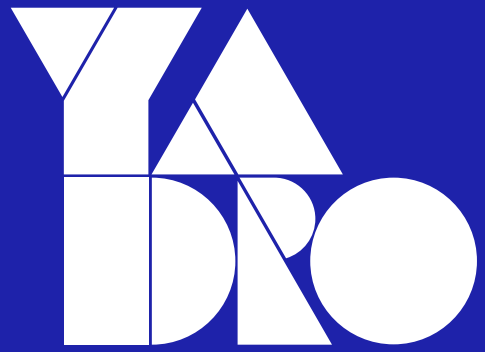
ВЕРИФИКАЦИЯ

CO-SIMULATION

- ПОДХОДЫ К ОТЛАДКЕ
- REMOTE PORT
- REMOTE PORT DPI
- **HARDWARE CO-SIMULATION**

Hardware co-simulation





Москва,
ул. Рочдельская, 15, стр. 13
+7 800 777-06-11

yadro.com