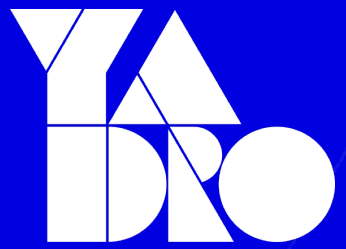


Моделирование процессоров архитектуры RISC-V с помощью QEMU

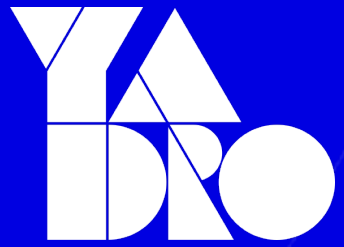
Подготовил Прокопьев Евгений

Содержание

- Что такое QEMU?
- Как QEMU работает?
- С какими вызовами сталкиваемся?
- Обновления QEMU связанные с RISC-V



Что такое QEMU?



QEMU

QEMU (Quick Emulator) — эмулятор с открытым исходным кодом (GPL 2)

Эмулируемые архитектуры

Alpha	LoongArch	PA-RISC	sh4
Arm	m68k	Power	SPARC
AVR	Microblaze	RISC-V	Tricore
Hexagon	MIPS	RX	x86
	OpenRISC	s390x	Xtensa

Поддерживаемые архитектуры

CPU Arch	Accelerators
Arm	hvf, kvm, tcg, whpx, xen
PPC	kvm, tcg
RISC-V	kvm, tcg
s390x	kvm, tcg
SPARC	tcg
x86	hvf, mshv, kvm, nvmm, tcg, whpx, xen

Какие проблемы решаем использованием QEMU

1. Проверка конфигураций платформы.
2. Подготовка поддержки новых инструкций и CSR.
3. Разработка ПО до получения RTL, битстримов и т.д.
    1. Отладка багов в ПО.
    2. Проверка драйверов СнК.
4. Сравнение с RTL и FPGA-прототипом.
5. Автоматизация тестирования (CI).

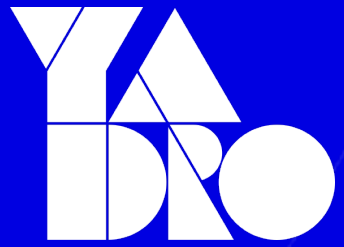


Ограничения модели и риски использования



- **Время и производительность**
  - Кэши, подсчет времени не эмулируются достоверно.
- **Параллелизм**
  - Host система может влиять на результат работы. Решается использованием icount.
- **Перенос на железо**
  - ПО работающее в QEMU необходимо обязательно проверить на реальном железе.

Как QEMU работает?



Режимы работы QEMU

- User TCG (user-mode)
- System TCG (softmmu)
- Гипервизор (KVM)

Параметр	User-mode	System	KVM
Тип гипервизора	—	Тип 2	Тип 1
Хост-ОС	Linux/BSD	Windows, Linux, BSD, MacOS	Linux
Доступ	Обычный пользователь	Обычный пользователь	/dev/kvm
CPU	—	Эмулируется	Тот что в системе
MMIO	—	да	да

QEMU TCG

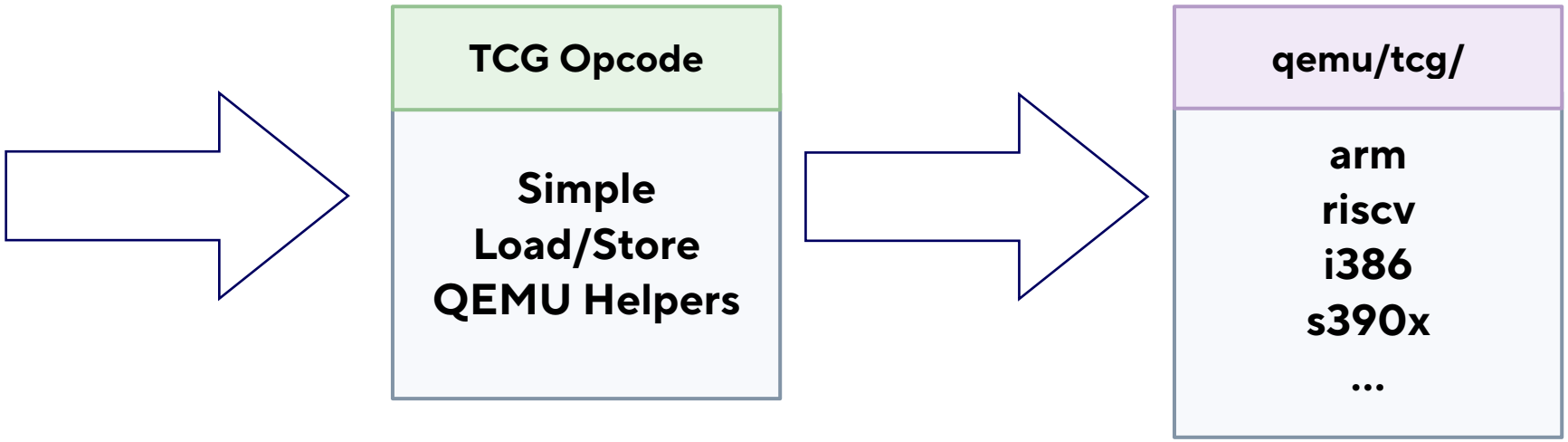
qemu/target/

alpha
arm
avr
hexagon
hippo
i386
loongarch
microblaze
mips
openrisc
riscv
sparc
tricore

TCG (Tiny Code Generator) разновидность Just in Time компиляторов.

qemu/target — трансляторы машинного кода целевой архитектуры в промежуточные инструкции QEMU.

qemu/tcg — трансляторы промежуточных инструкций в машинный код исполняющией архитектуры.

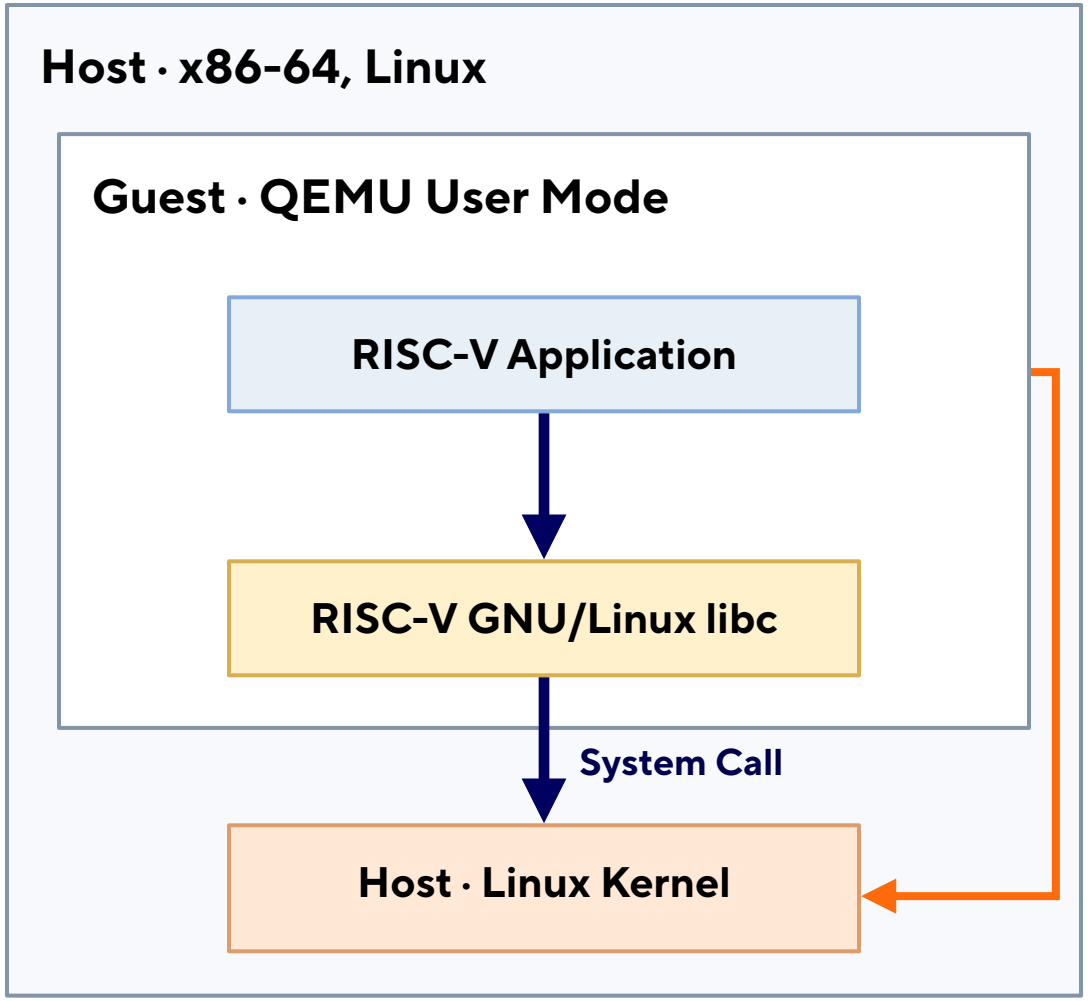


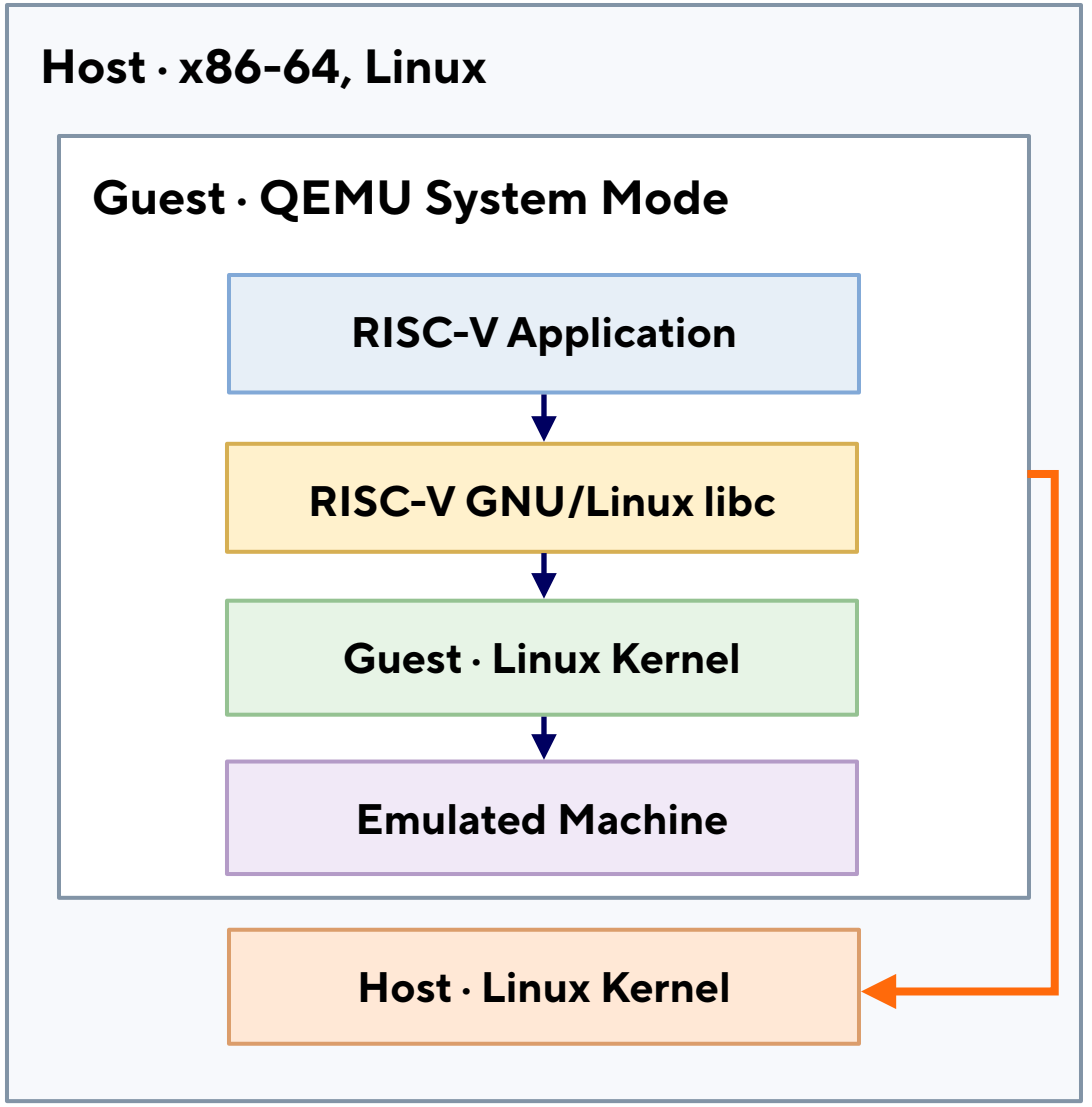
[Статья на habr]

Как обрабатываются инструкции?

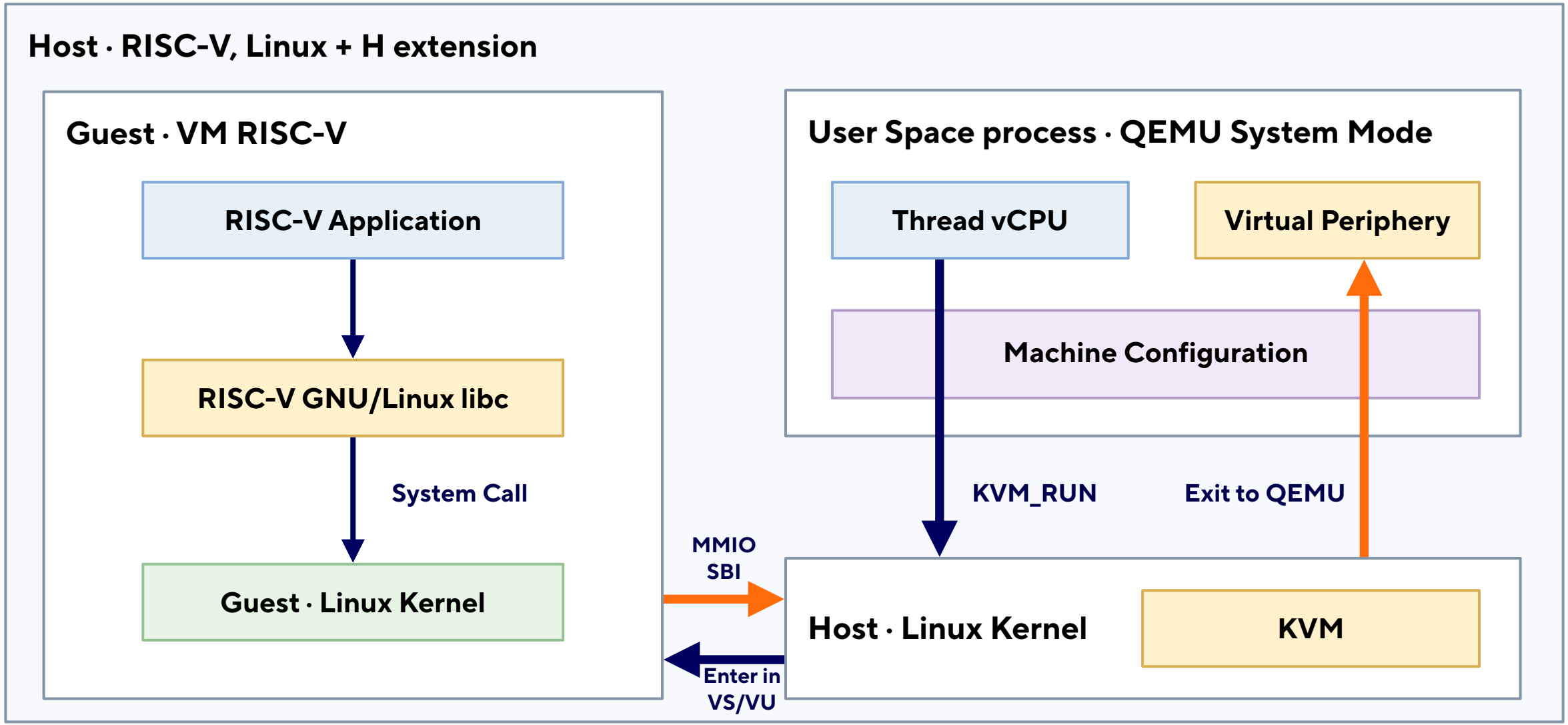


Режимы работы QEMU (TCG)

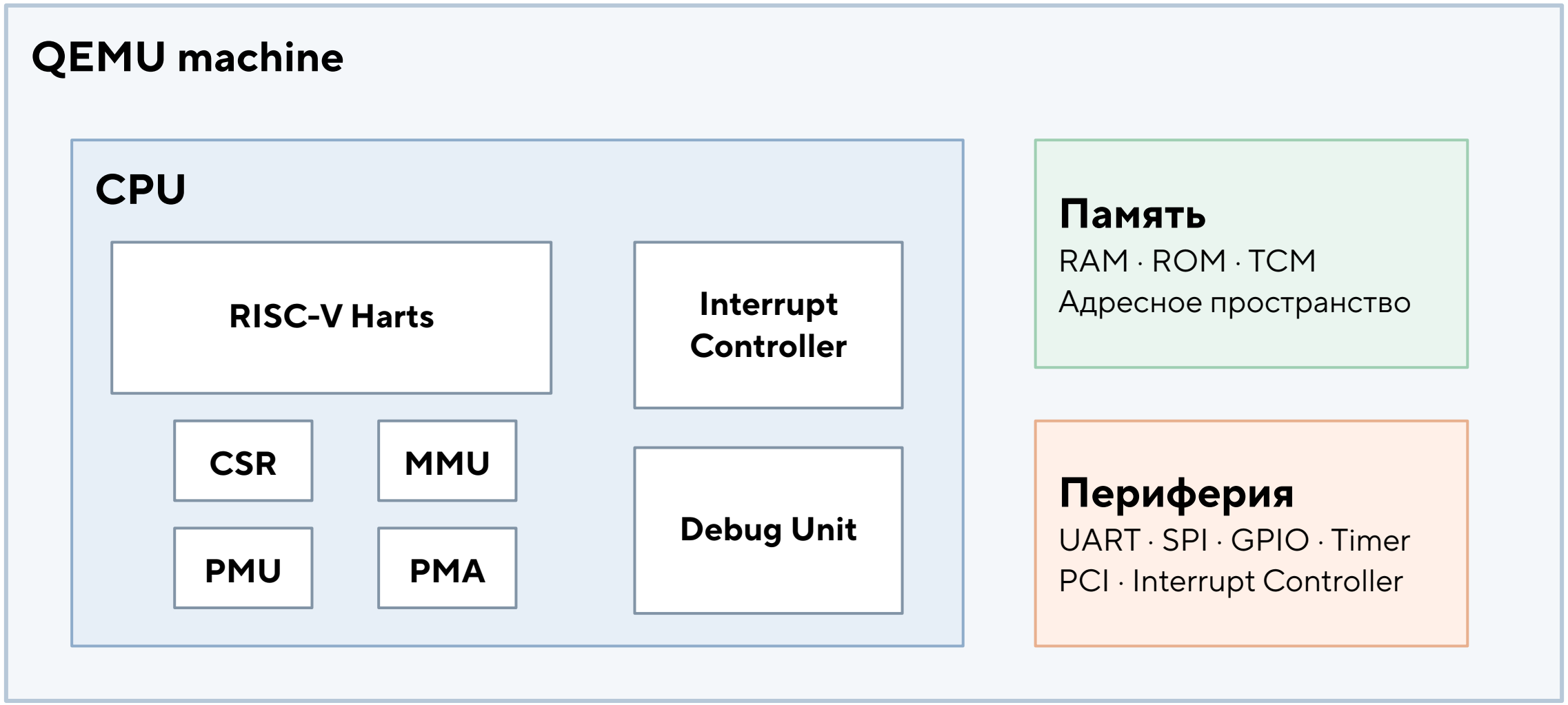




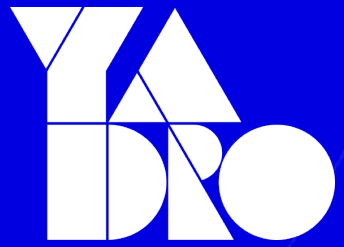
Режимы работы QEMU (KVM)



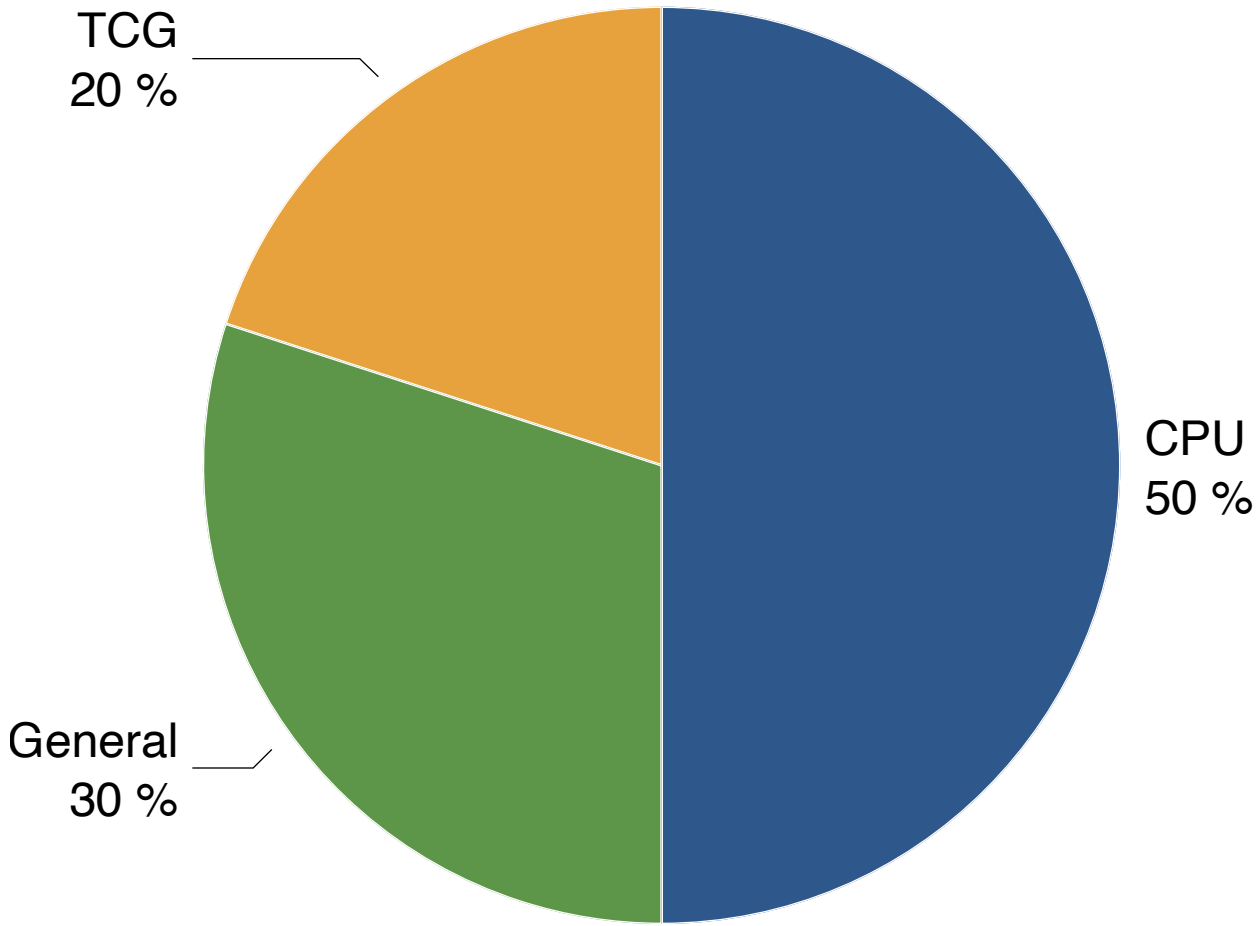
Что входит в состав QEMU модели



Какие проблемы решает команда?

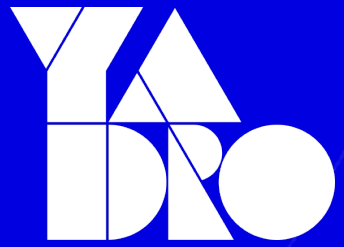


Чем занимается наша команда?

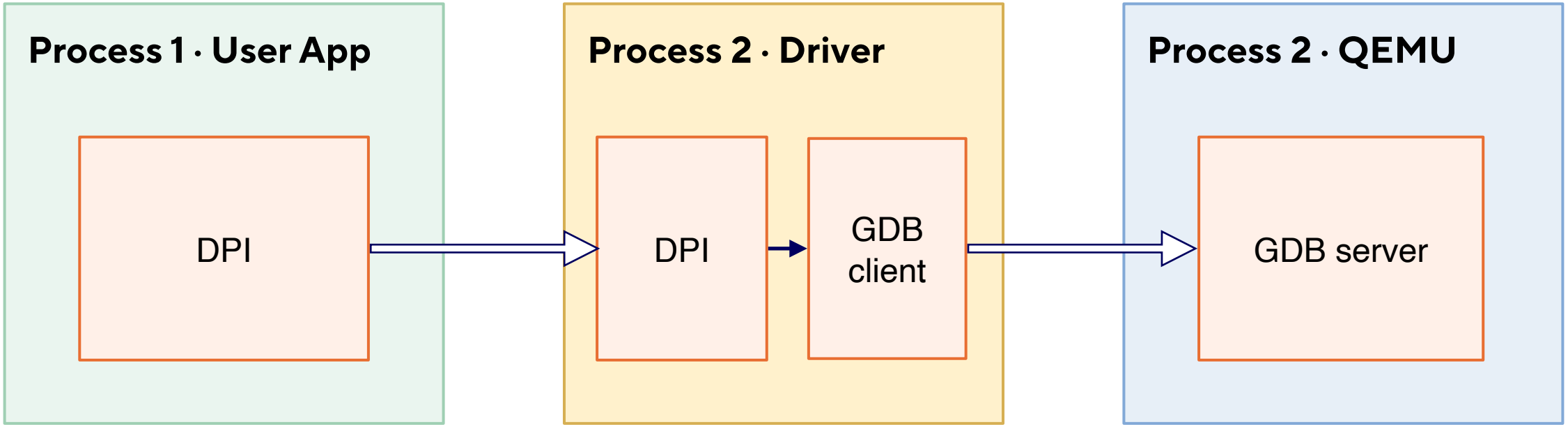


- **CPU**
  - RISC-V harts
  - RISC-V ext
  - SoC components
    - ACLINT, CLIC, PLIC и т.д.
- **TCG**
  - RVV
  - Packed SIMD
  - Bugs
- **General**
  - Lib
  - Heterogeneous systems
  - Upstream

QEMU библиотека

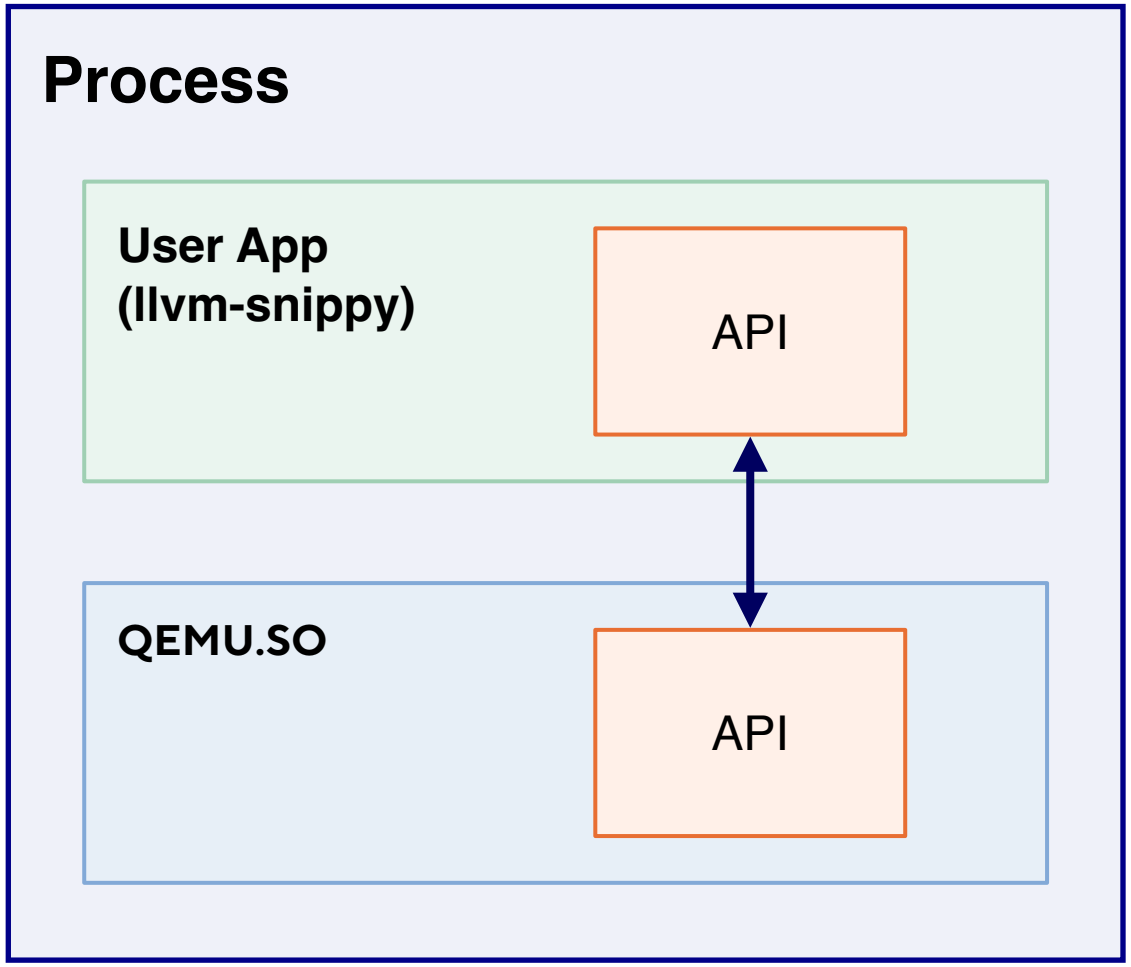


QEMU как библиотека



DPI (Direct Programming Interface) — механизм для взаимодействия между SystemVerilog и другим языком, например C или C++.

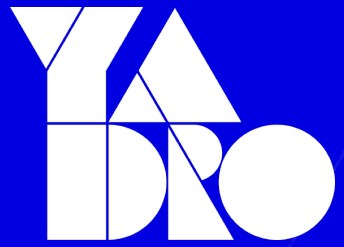
QEMU как библиотека



Области применения:

1. Сравнение с RTL
2. Тестирование
3. Эмуляция гетерогенных систем

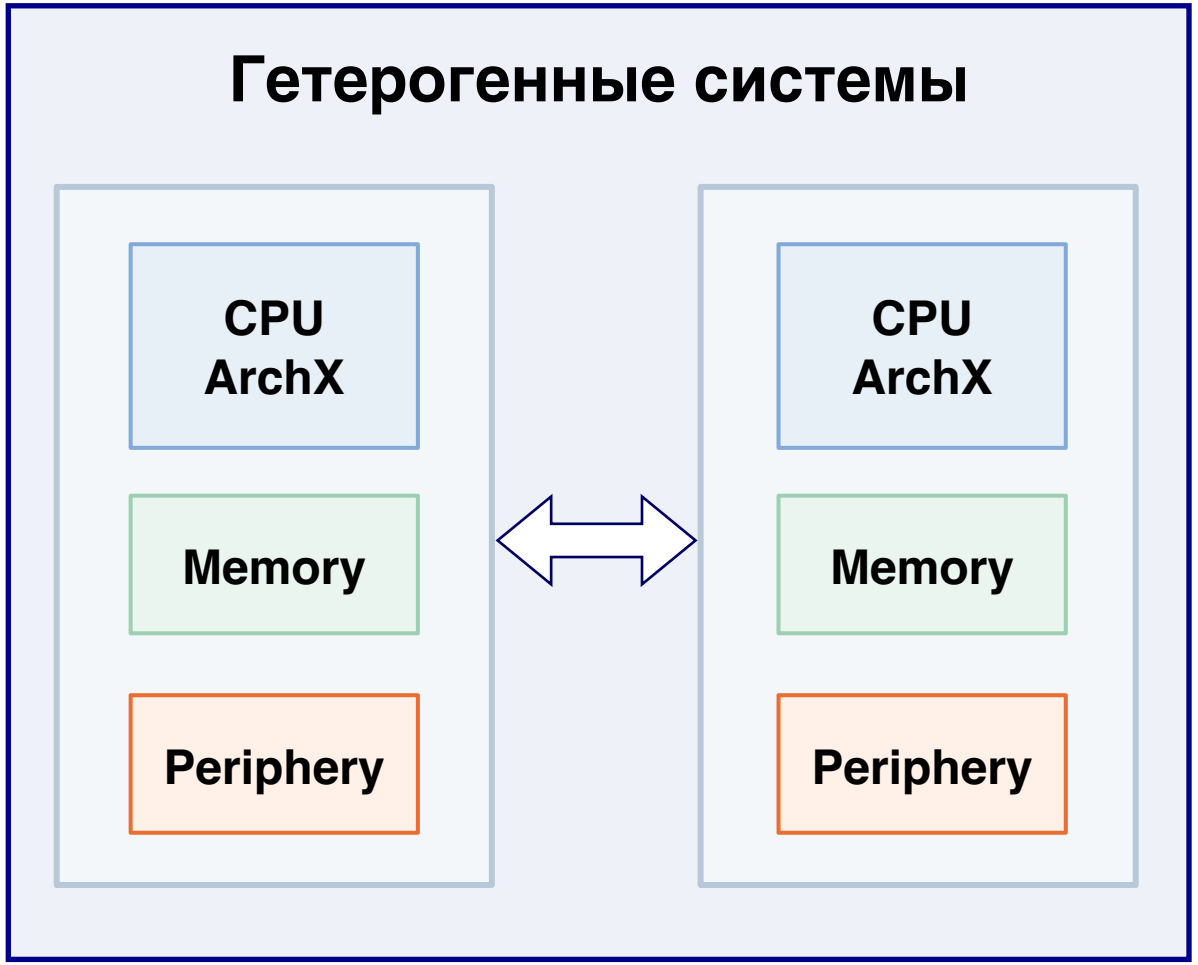
Эмуляция гетерогенных систем



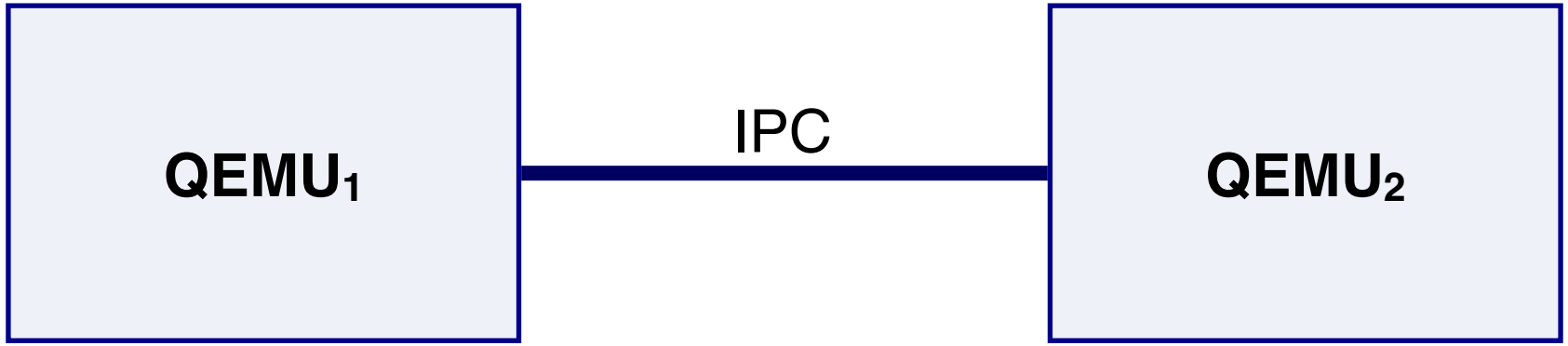
Гетерогенные системы

Эмулируемые архитектуры

Alpha	LoongArch	PA-RISC	sh4
Arm	m68k	Power	SPARC
AVR	Microblaze	RISC-V	Tricore
Hexagon	MIPS	RX	x86
	OpenRISC	s390x	Xtensa



Гетерогенные системы. Вариант №1



Плюсы:

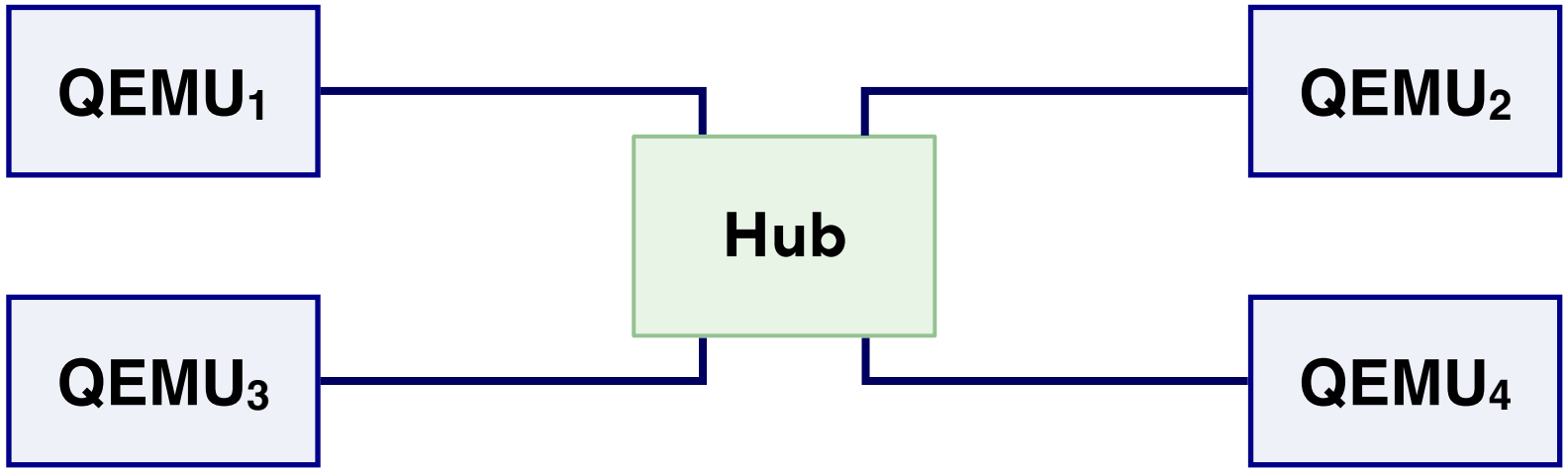
- Простота
- Подходит в ситуациях с раздельной памятью и периферией
- Можно комбинировать разные архитектуры

Минусы:

- Накладные расходы
- Дедлоки
- Сложно масштабировать
- Проблемы с частичным завершением
- Сложность отладки

[Статья на habr]

Гетерогенные системы. Вариант №2



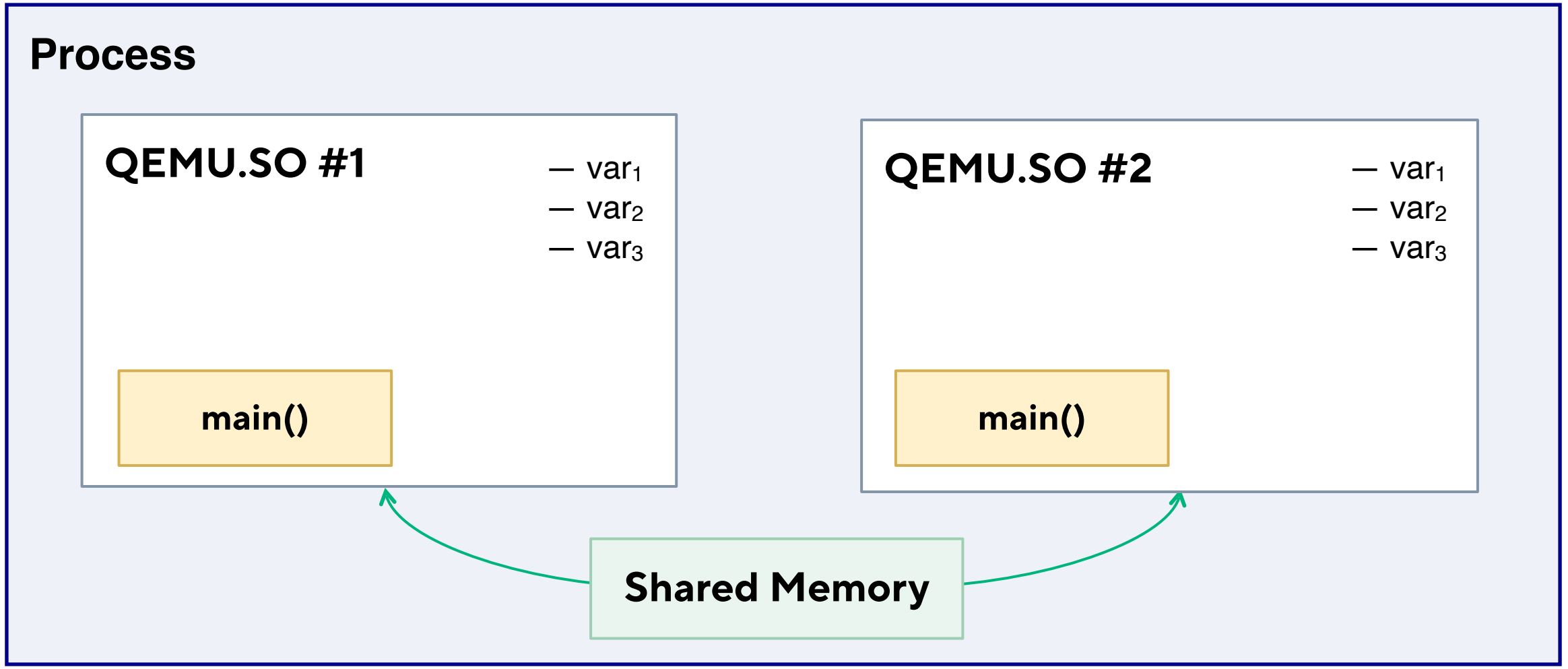
Плюсы:

- Решается проблема масштабирования
- Частично решается проблема с завершением

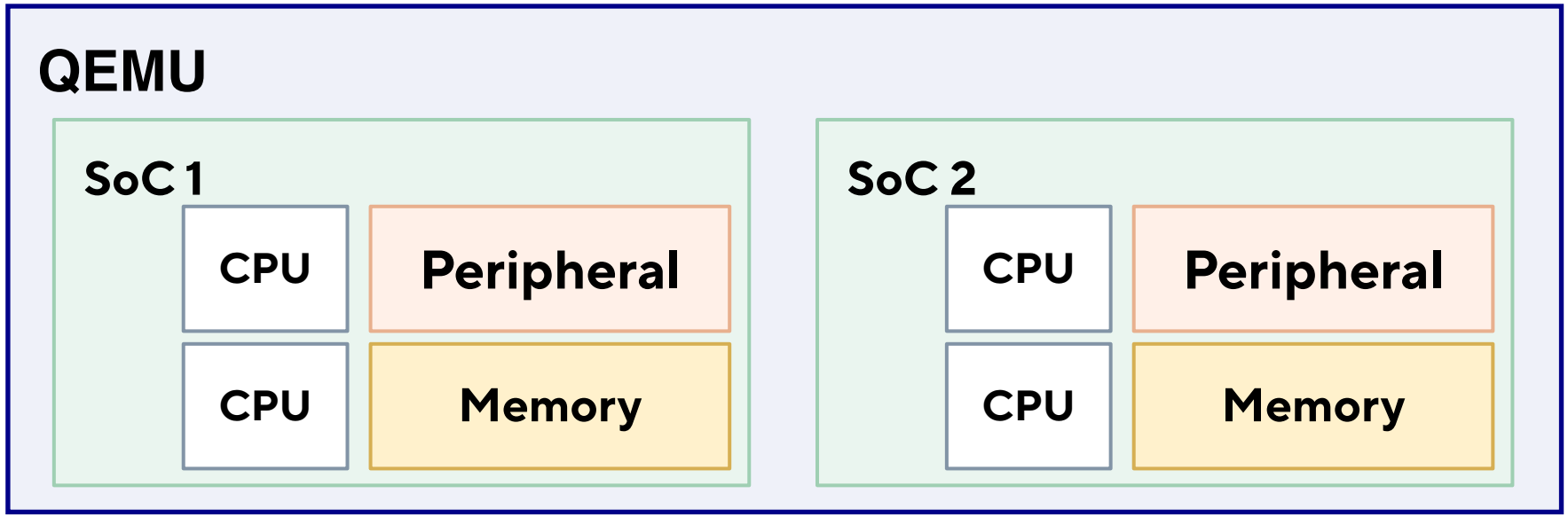
Минусы:

- Накладные расходы
- Дедлоки
- Сложность отладки

Пример реализации Варианта №2.



Гетерогенные системы. Вариант №3



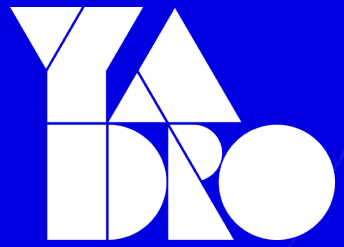
Плюсы:

- Простота отладки
- Простота коммуникации
- Нет накладных расходов
- Подходит в сценариях с общей памятью и периферией
- Нет проблем с частичного завершения

Минусы:

- Плохо подходят сценарии с раздельной памятью и периферией
- Сложности реализации

Обновления QEMU касающиеся RISC-V



Обновления за последний год

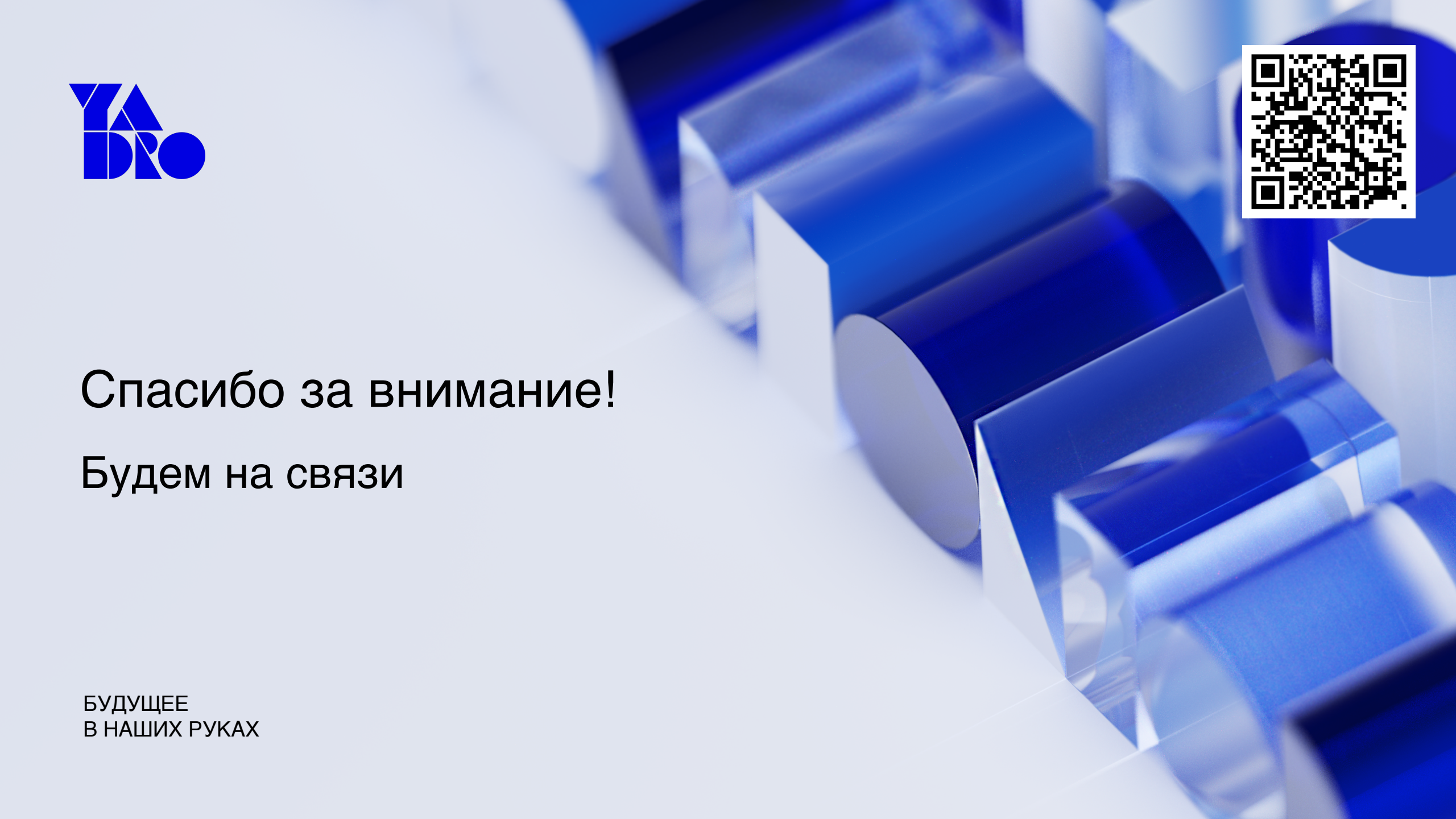
- **RISC-V**
  - **Efficient Trace (E-Trace) и Nexus-based Trace (N-Trace)**

    Аппаратная трассировка исполняемого кода
  - **Обновление Packed SIMD реализации**

    Packed SIMD для DSP; патчи опираются на черновик спецификации v0.21
  - **Обновление и поддержка Debug 1.0 (sdtrig + sdext)**

    Новая модель отладки рядом с прежней 0.13
- **Серия патчей Single Binary**

  Склеивание всех архитектур в один бинарь. В v3 были объединены: ARM (32 и 64), RISC-V (32 и 64), MicroBlaze.



Спасибо за внимание!

Будем на связи

БУДУЩЕЕ
В НАШИХ РУКАХ

Список наших обновлений в апстриме



- N-Trace:
  - [PATCH 00/13] hw/riscv, target/riscv: initial n-trace support
  - [PATCH 0/6] hw/riscv, target/riscv: implement N-Trace messages
  - [PATCH 0/6] hw/riscv, target/riscv: implement initial N-Trace filtering
- [PATCH] target/riscv: add support for the hcontext CSR
- Упрощенный репродьюсер для TCG бага
- [RFC PATCH] accel/tcg/cpu-exec.c: Wake up gdb client after WFI