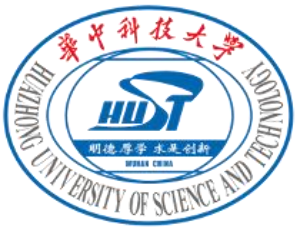


華中科技大學
HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

HUST
OPENATOM CLUB

Rust for QEMU
架构演进、现状分析与贡献指南

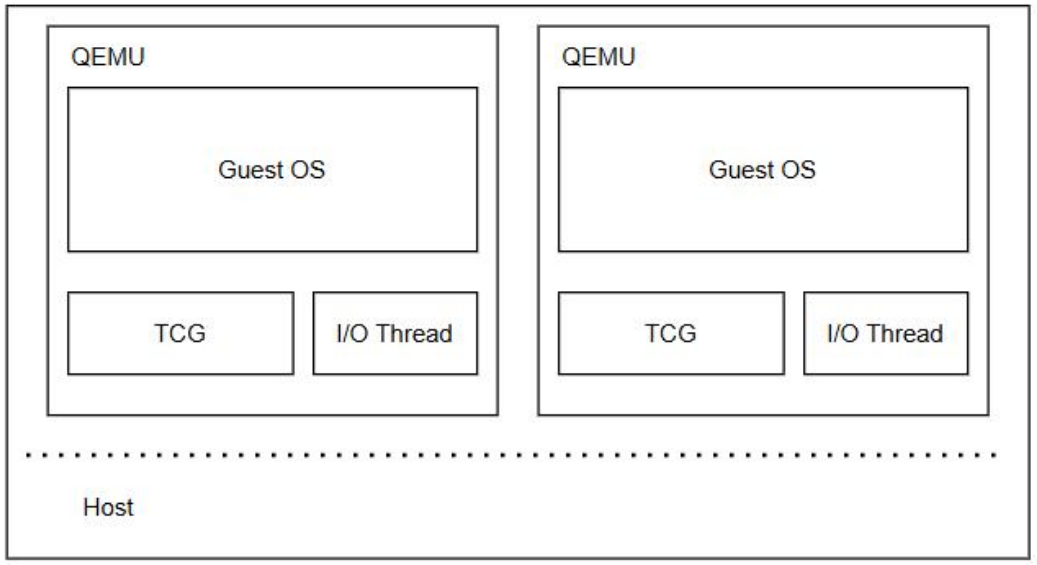
Rust for Linux/QEMU 项目组 泽文

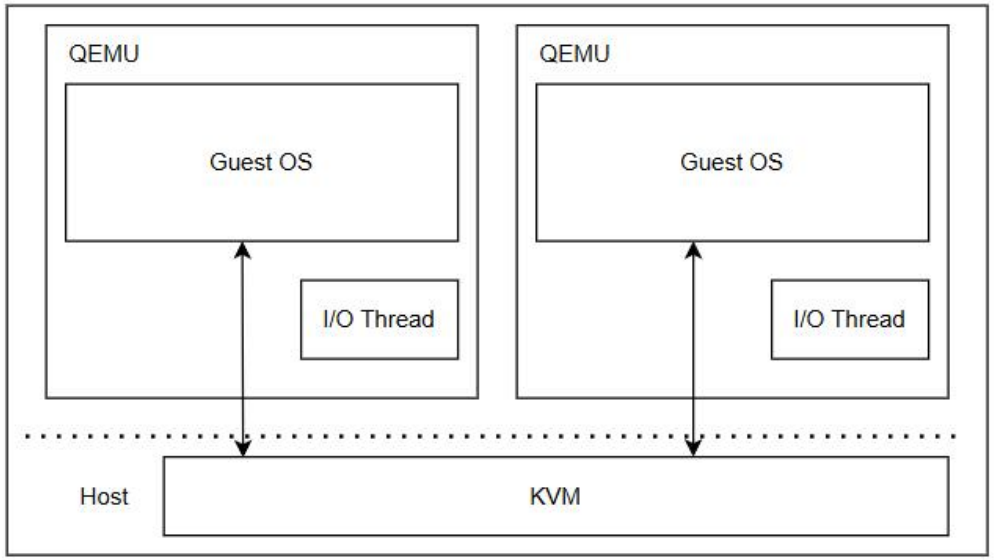
QEMU 基本介绍

HUST OPENATOM CLUB

QEMU（Quick Emulator）是一个通用的开源机器模拟器和虚拟化工具，由 Fabrice Bellard 于 2005 年创建。它支持多种加速器（accelator），比如 KVM 和 TCG。前者利用硬件虚拟化机制，支持同构模拟；后者通过动态二进制翻译技术，支持系统级模拟（System Emulation）和用户模式模拟（User Mode Emulation）。

在系统级模拟（虚拟化）下，QEMU 提供完整的虚拟机环境，包括 CPU、内存和外围设备，允许运行客户操作系统；在用户模式模拟下，QEMU 可以跨架构运行程序，例如在 x86 主机上执行 RISC-V 或 ARM 的二进制文件。





为什么要引入 Rust?

HUST OPENATOM CLUB

QEMU 漏洞根源：

QEMU 多数安全漏洞（如缓冲区溢出、释放后使用等）及可能的非安全漏洞，均源于 C 语言编程错误，安全性受严重影响，可通过 CVE 列表验证。

传统防错方法局限：

QEMU 社区虽用编码规则、静态检查、测试等手段减少 C 语言错误，但仍难杜绝新漏洞，且安全 C 代码对经验要求高，阻碍新手贡献，影响代码质量一致性。

Rust 引入契机：

Rust 通过编译时借用检查、边界检查等设计预防内存安全漏洞，因 QEMU 代码量大难全面转换，可优先在作为主要安全攻击面的设备模拟领域用单独程序实现，为 Rust 应用创造条件。

Rust for QEMU 演进历史

HUST OPENATOM CLUB

- **社区讨论阶段（2020）**

  Why QEMU should move from C to Rust • Stefan Hajnoczi

- **早期开发阶段（2021 - 2023）**

  1. KVM Forum 2021 针对 Rust 展开专题讨论
  2. 确定技术方案以后，在主线外进行早期开发

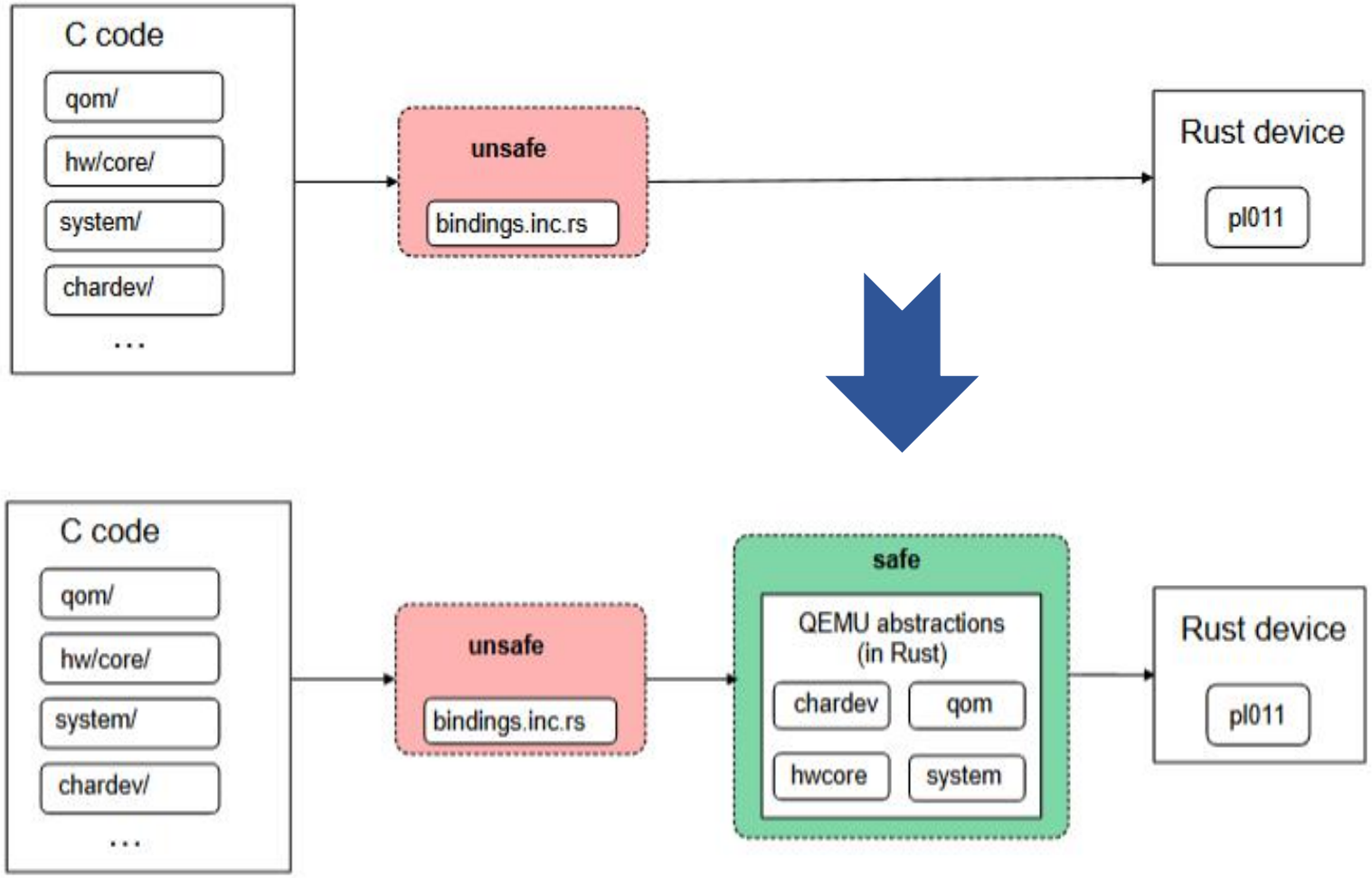
- **主线化阶段（2024）**

  1. QEMU 9.2 首次官方支持 Rust，默认禁用需手动开启，
  2. 引入构建系统支持，核心 Crate，PL011 串口设备

- **功能完善阶段（2025）**

  1. QEMU 10.0 实现了 Rust 相关源码的构建稳定和测试覆盖
  2. 新增 HPET 设备，日志记录、trace、热迁移等核心功能

架构演进：QEMU 9.2

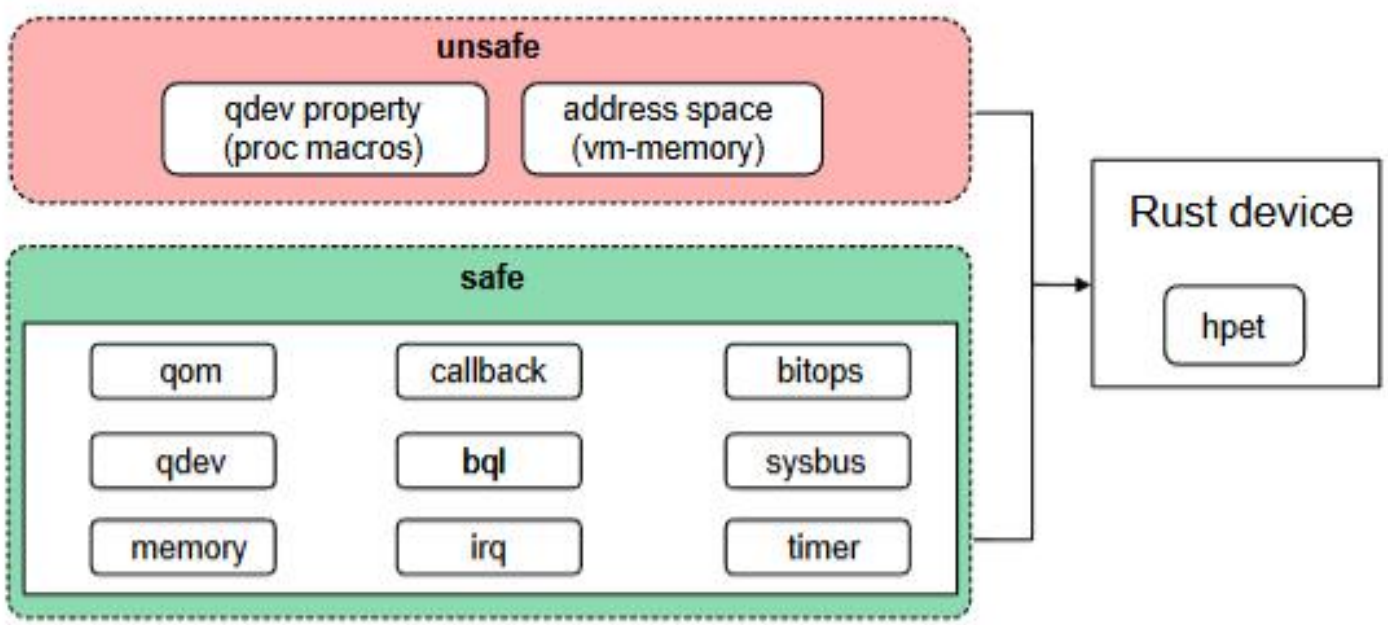


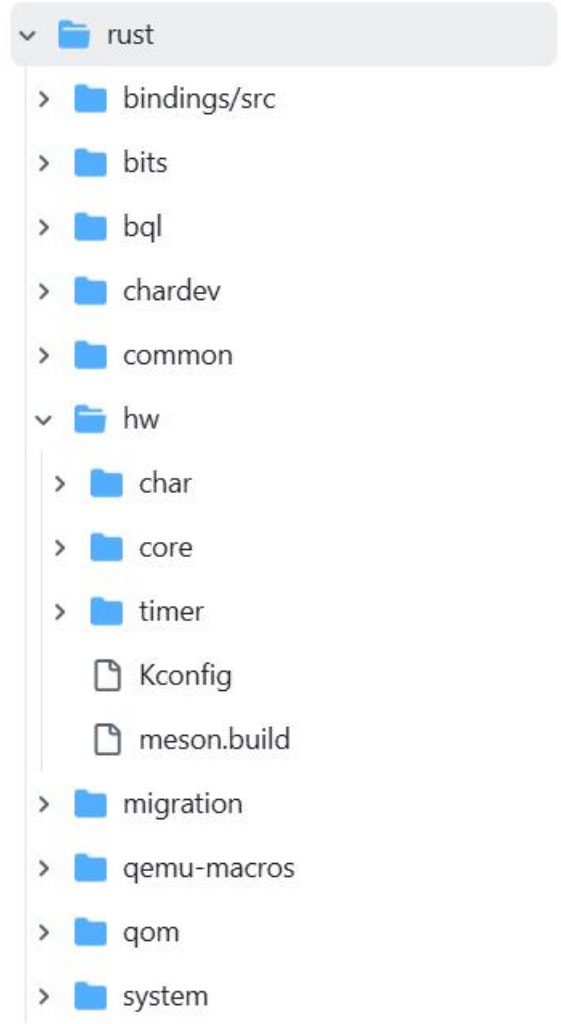
- Meson:支持构建 Rust 源码
- FFI：bindings 导出 C 接口
- usafe：隔离不安全的代码
- safe：提供安全接口
- RAII:符合 QOM 生命周期
- 运行时：BQLRefCell

架构演进：QEMU 10.x

HUST OPENATOM CLUB

- pl011：将不安全代码作为实现绑定的参考依据
- HPET：从头开始编写符合 Rust 安全的设备代码

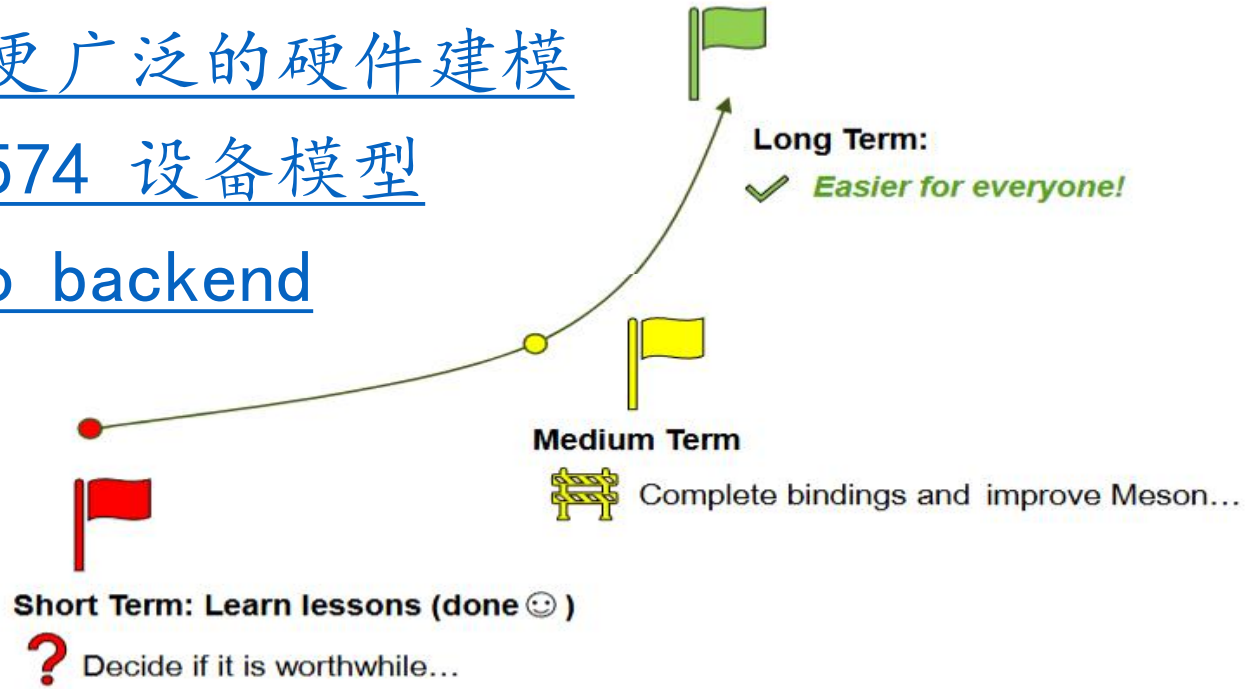




现状分析：初步完善

HUST OPENATOM CLUB

- 提供完整的 QOM of Rust 抽象：设备创建、实例化、销毁
- 支持了 MemoryRegion、IRQ、SysBus 等核心组件
- 完善了设备热迁移、日志调试、错误处理等功能
- RFC：新增 BusClass，支持更广泛的硬件建模
- RFC：新增 I2CBus 和 pcf8574 设备模型
- WIP：新增 GStreamer audio backend



贡献指南

HUST OPENATOM CLUB

- 学习路线：
  - 掌握 QEMU 硬件建模原理及常用 API
  - 掌握 Rust 常用知识：所有权、生命周期、常用 crate
- 贡献指南：
  - 支持 Block Device
  - 清理 Unsafe Code
  - 简化 Meson Build Script
- 参考文档：
  - Learning QEMU Docs：QEMU 硬件建模原理
  - Rust for QEMU Insides：技术文档、博客、上游新闻
  - Rust for QEMU 官方文档：Rust 代码规范、编译流程、开发指南

致谢

- 姓名：泽文
- 邮箱：chao.liu@openatom.club
- Github ID：@zevorn

参考链接：

[1] Rust in QEMU roadmap - Paolo Bonzini

[2] From C to a Rust interface, brick by brick - Zhao Liu, Paolo Bonzini

[3] Rust in QEMU: strengths and challenges - Manos Pitsidianakis

公众号：开源内核安全修炼

微信号：kernel_sec_pratice