麒麟信安嵌入式操作系统基于分区虚拟化的技术实践

麒麟信安操作系统工程师 邱文博

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

目录

混合关键性系统（MCS）

MCS系统

定义：（混合）运行着不同关键性应用（任务）的软硬件系统。

关键性：系统异常是否会导致严重后果

动机：

- 运行关键性任务的系统需要漫长的测试验证其安全性
- 关键性任务往往存在非关键性的部分
- 拆分运行任务的关键性与非关键性部分可以简化关键性任务的设计与验证流程
- 减少系统整体使用的组件

常见应用：飞控， 车机

现状分析

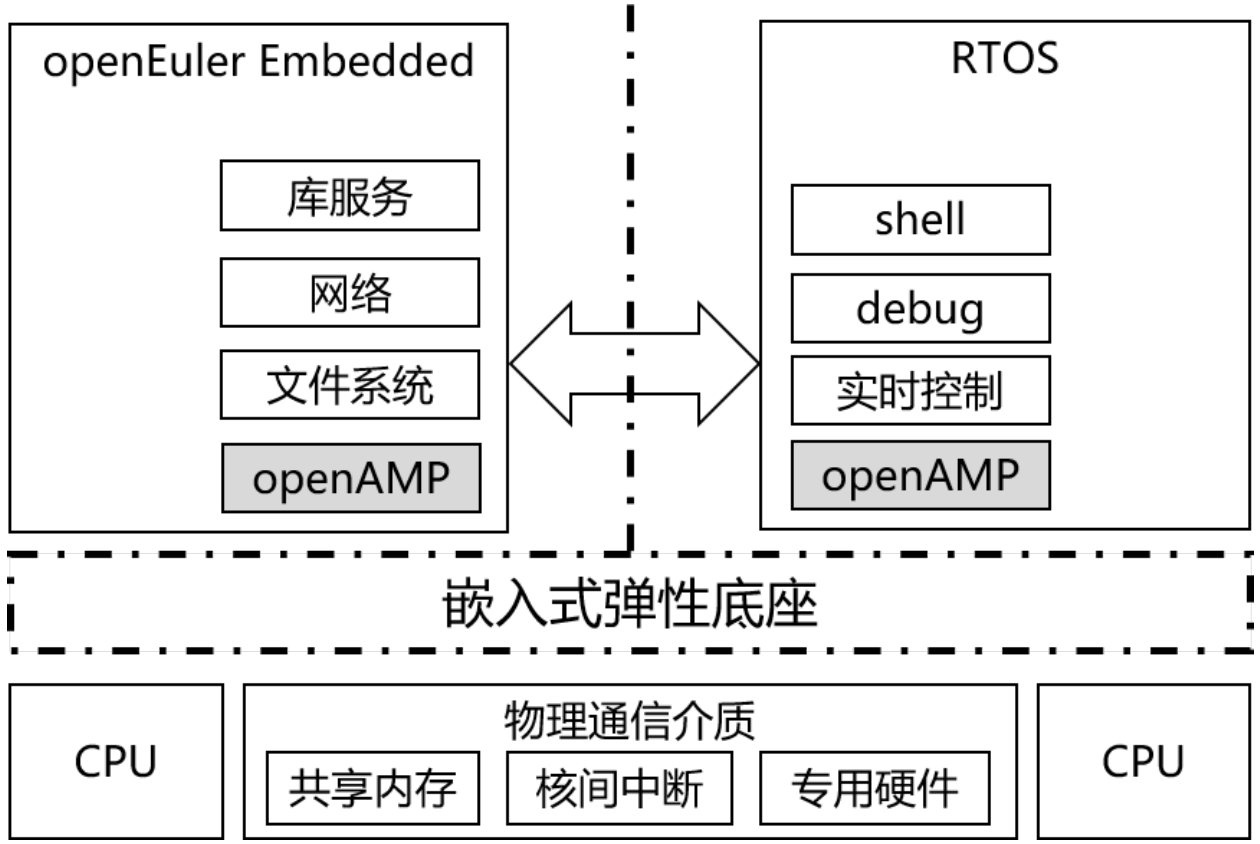
现状：管理能力、丰富生态、高实时、高可靠、高安全要求不能同时满足。

传统方案：采用一颗性能较强的处理器运行Linux负责富功能，一颗微控制器/DSP/实时处理器运行实时操作系统负责实时控制或者信号处理。两者之间通过I/O、网络或片外总线的形式通信。

缺陷问题：集成度不高、通信速度受限、灵活性差、可维护性成本高。

openEuler Embedded MCS框架

- **高效地混合部署问题：**高效地实现多OS协同开发、集成构建、独立部署、独立升级。
- **高效地通信与协作问题：**系统的整体功能由各个域协同完成，高效地实现不同域之间可扩展、实时、安全的通信。
- **高效地隔离与保护问题：**高效地实现多个域之间的强隔离与保护，使得出故障时彼此不互相影响，以及较小的可信基（Trust Compute Base）。
- **高效地资源共享与调度问题：**在满足不同目标约束下（实时、功能安全、性能、功耗），高效地管理调度资源，从而提升硬件资源利用率。

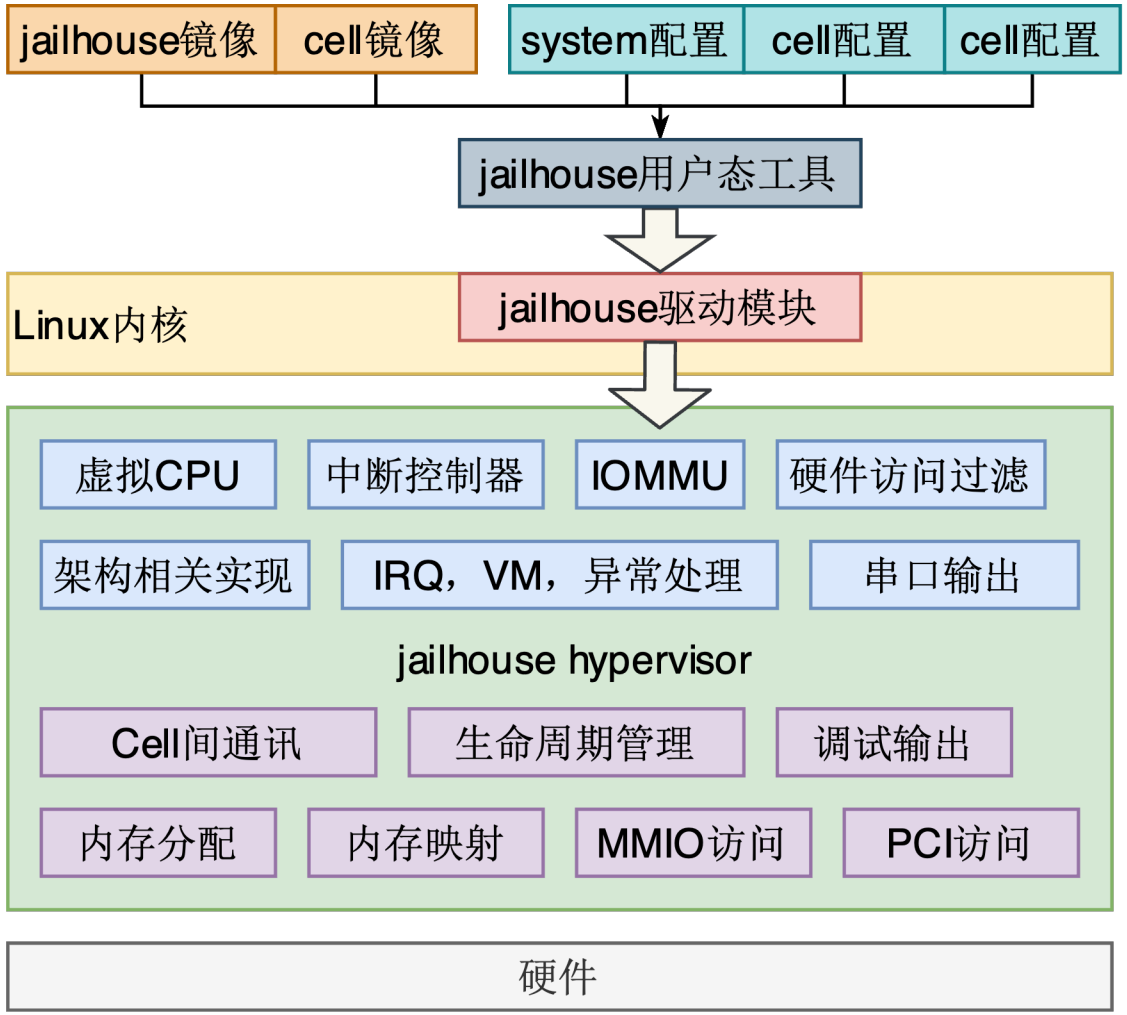


jailhouse软件架构

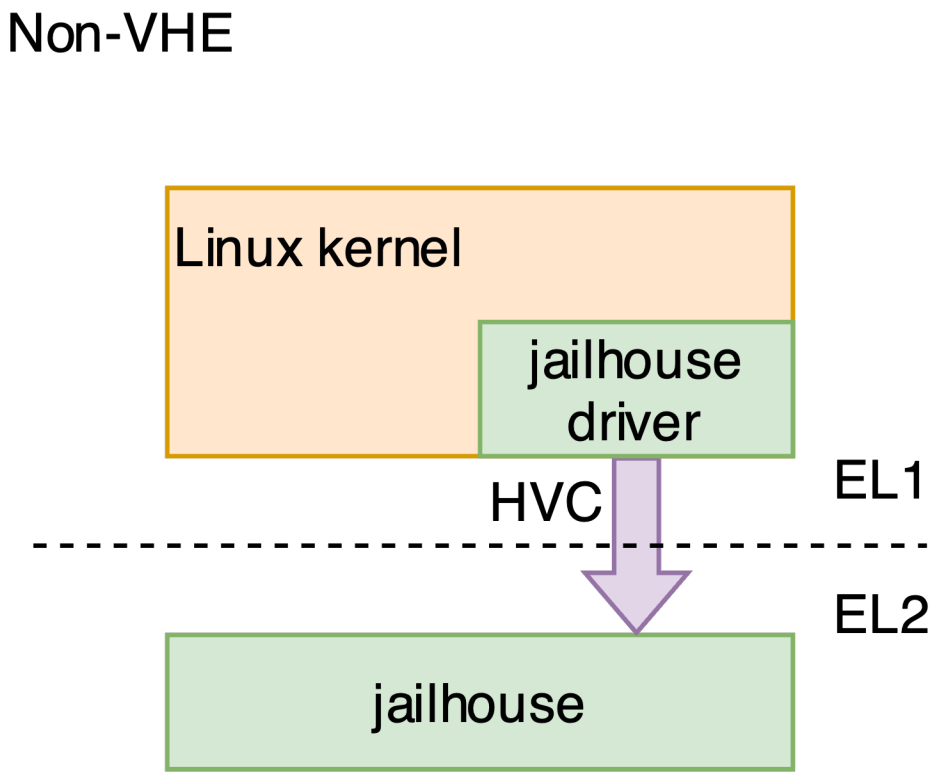
一个开源的分区虚拟化系统，提供轻量级、高性能的硬件资源分割和隔离，适用于嵌入式和实时应用场景。

特点：

- 基于分区虚拟化的MCS系统实现
- 静态分区虚拟化
- 无资源调度器实现
- 1比1资源分配
- 尽量不进行设备模拟
- 运行时最小化
- 硬实时支持，额外开销最小化
- 考虑隔离安全性，支持IOMMU等硬件特性

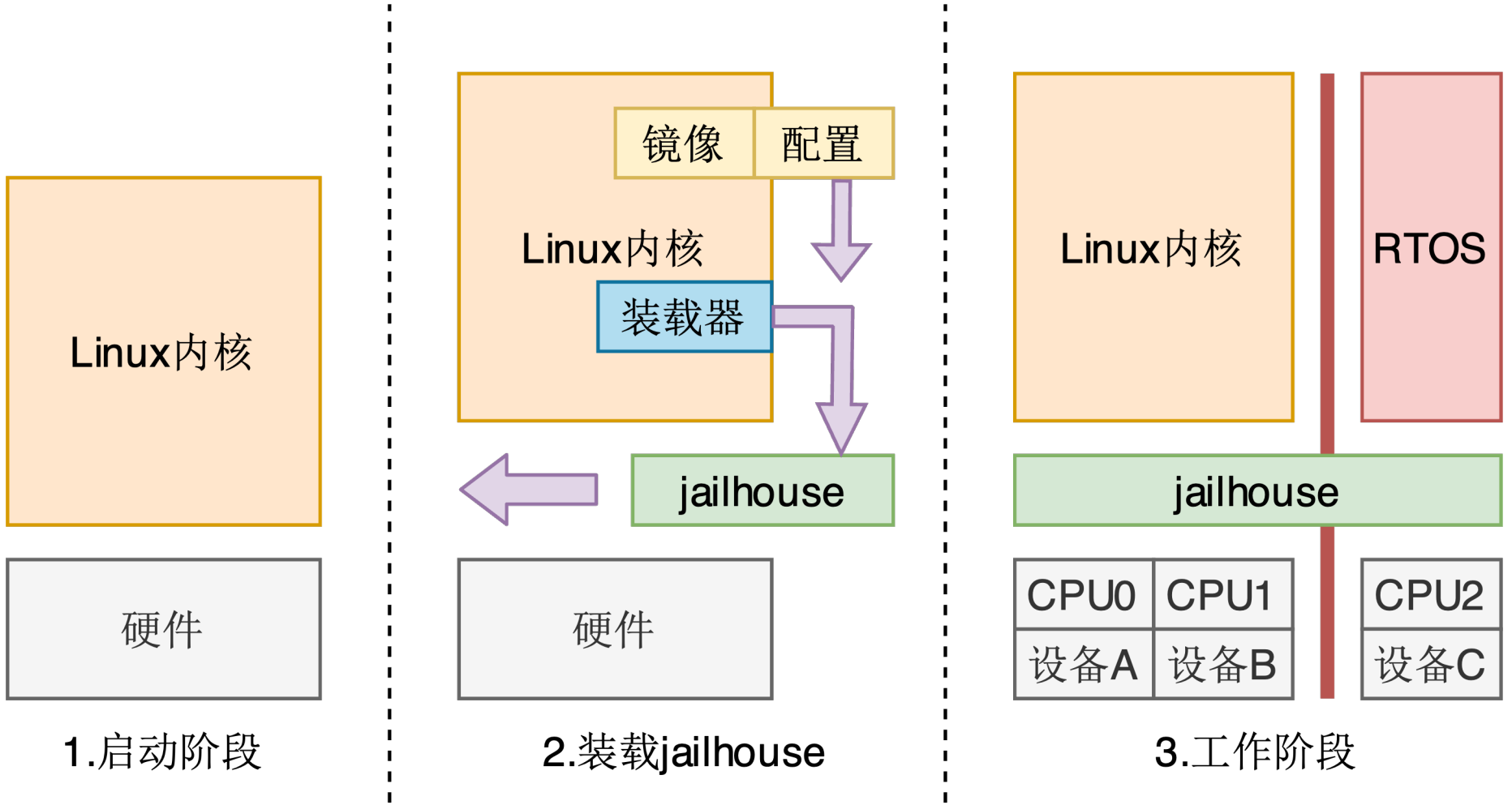


Linux内核Hypercall调用



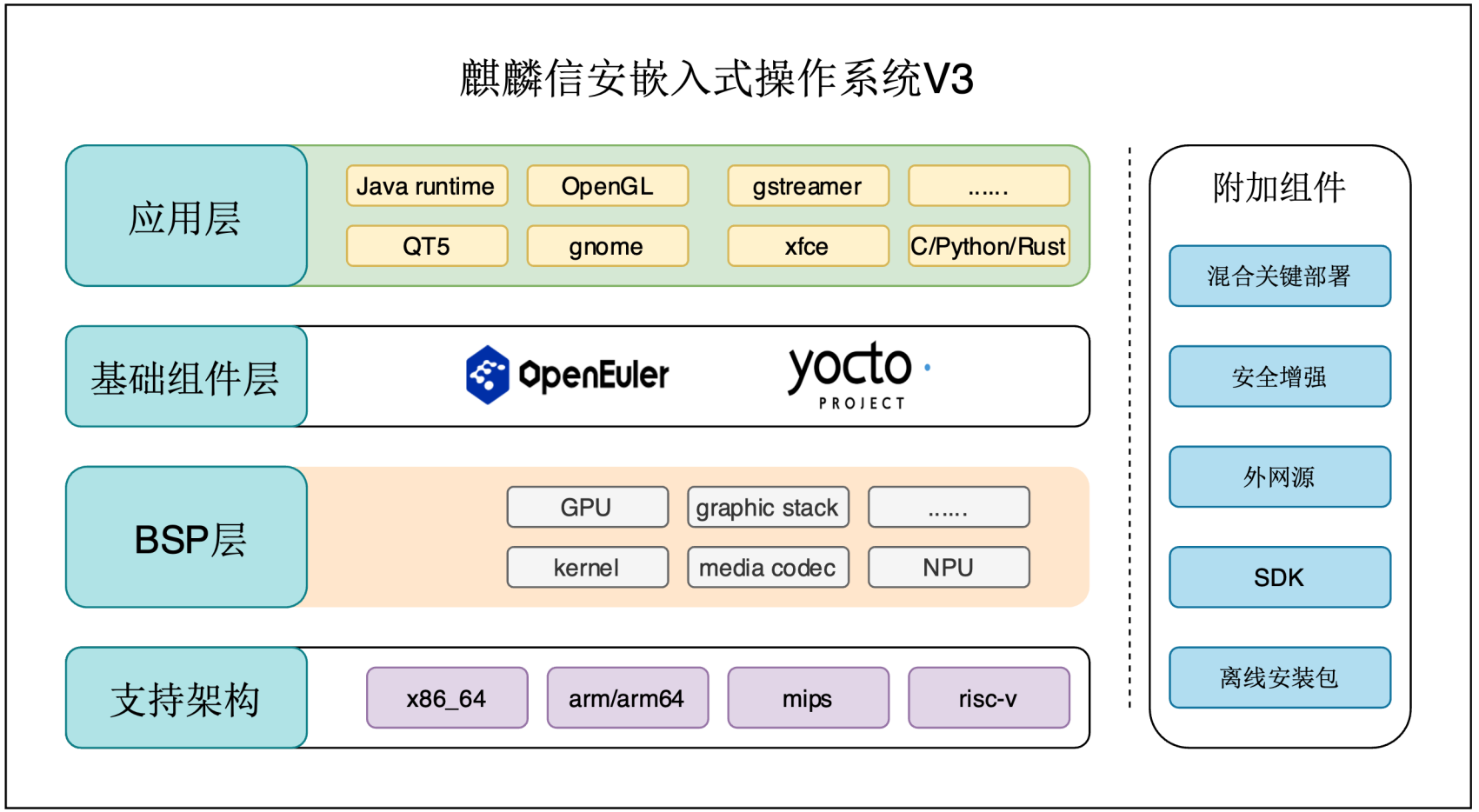
- debug console putc
- cpu get info
- disable
- cell destroy
- cell create
- cell get state
- cell set loadable
- hypervisor get info
- cell start

jailhouse工作流程



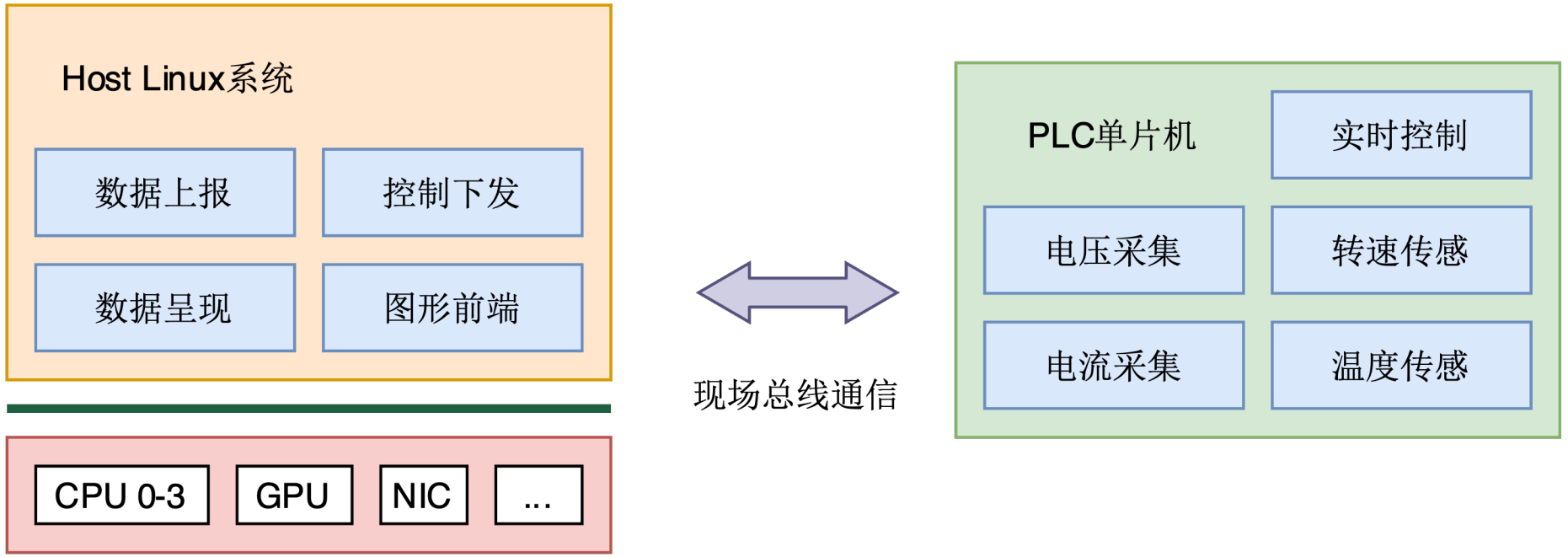
麒麟信安嵌入式Linux系统

- 基于openEuler Embedded的商业发行版
- BSP - 更多嵌入式板卡支持
- 附加桌面组件支持
- 开源/闭源图形栈支持
- wayland/X11双图形栈支持
- 安全增强策略



电网应用案例（原方案）

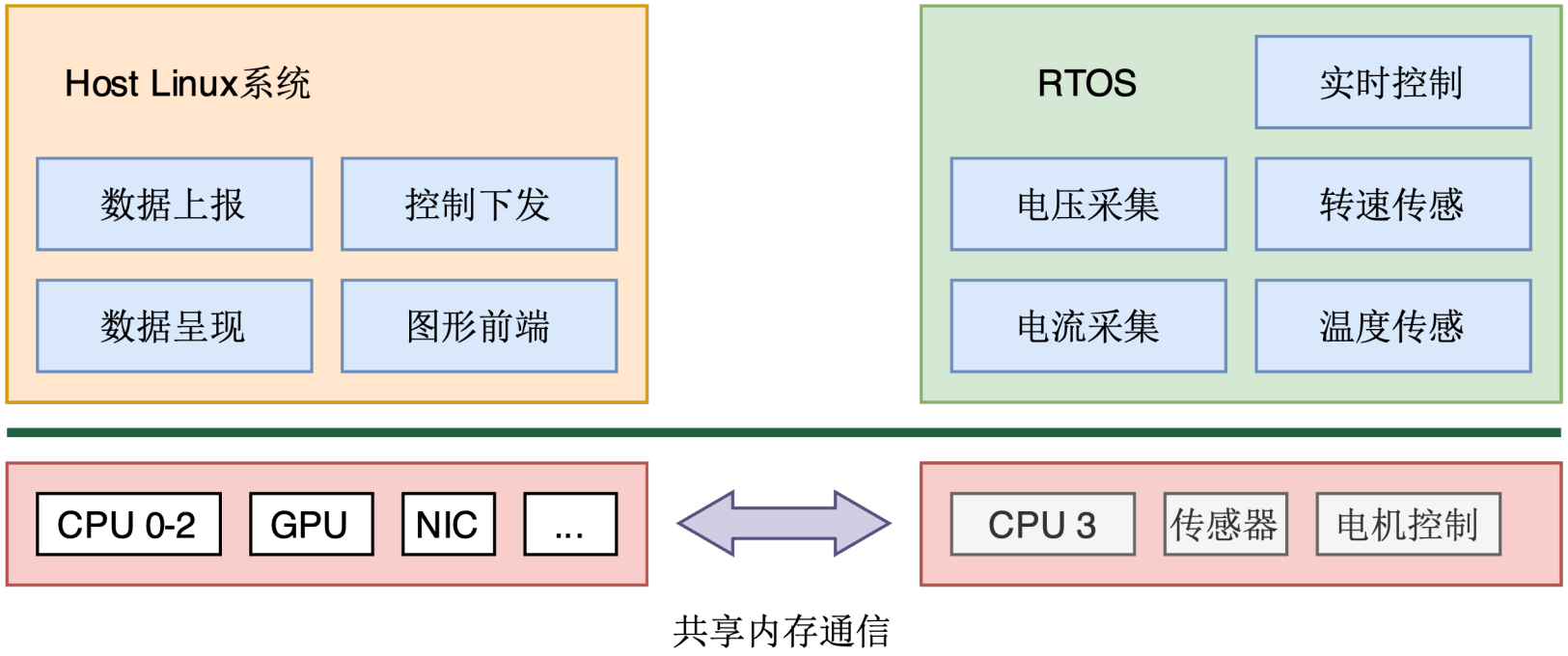
- 嵌入式系统由Linux控制端与PLC单片机组成
- 两端通过现场总线进行通信
- PLC端进行数据采集与控制
- Host Linux系统端进行数据上报与控制下发



电网应用案例（分区虚拟化）

- PLC替换为高性能ARM-A核心
- 相关设备分区到RTOS虚拟化资源Cell
- 基于共享内存的数据通信

- 使用分区虚拟化与RTOS替代原PLC功能
- 使用同一硬件实现原有两个独立硬件的功能



THANKS