第五届国产嵌入式操作系统技术与产业发展论坛

操作系统内生安全技术与应用

报 告 人： 蒋 金 虎

FUDAN UNIVERSITY
1905
復旦大學
FUDAN UNIVERSITY

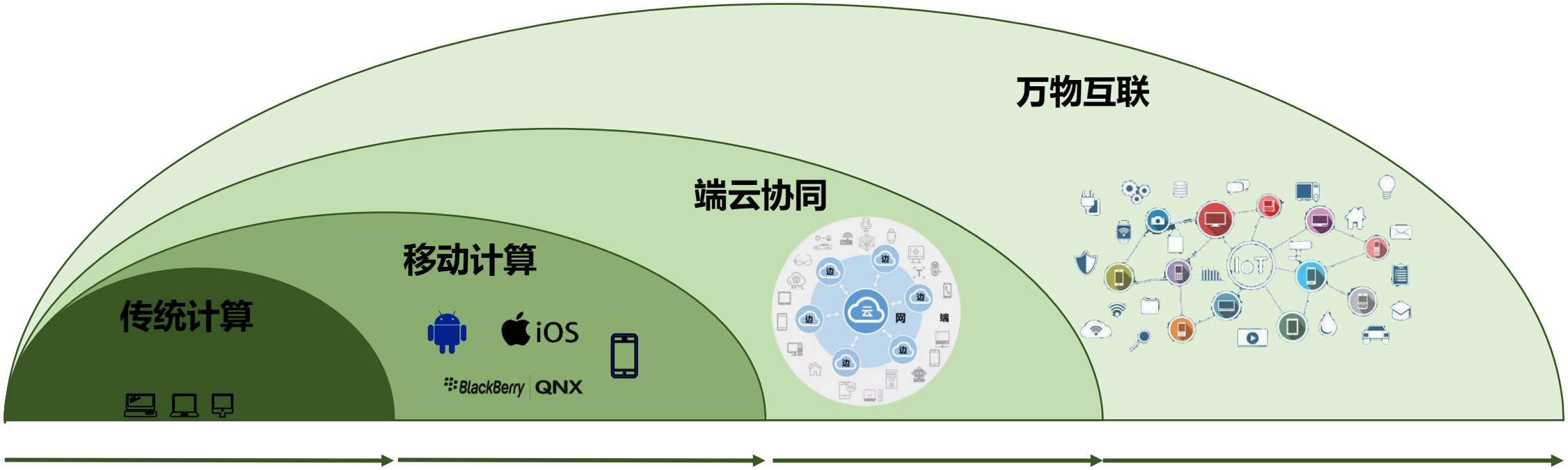
2023年8月12日

目录

- 背景和现状
- 问题和挑战
- 系统设计
- 应用案例

计算应用领域不断扩展

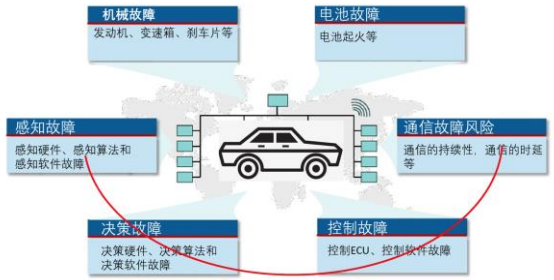
智能设备与物联网的结合，开启了万物互联的时代



安全形势严峻

设备的智能化、网络化，功能安全与网络安全日益交织叠加，安全问题突出

功能安全

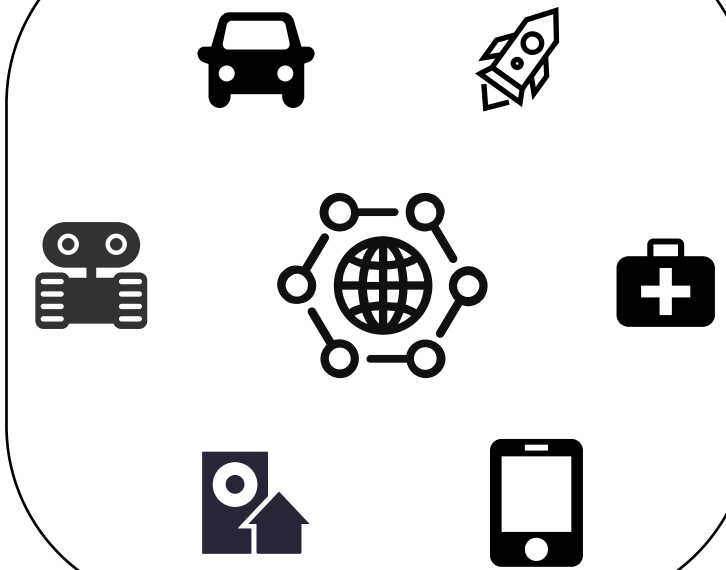


自动驾驶功能故障

工业设施功能隐患

容忍随机的物理故障

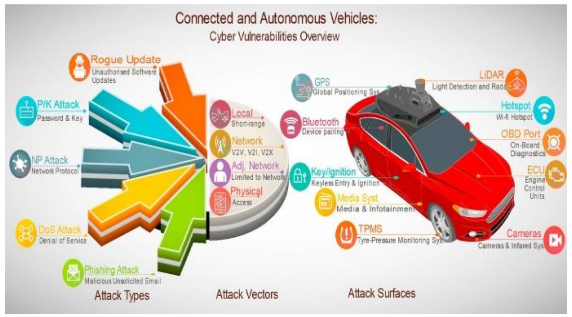
智能化设备



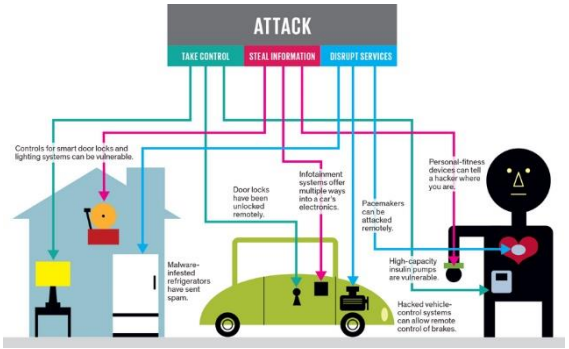
内生安全问题

难以消除的未知设计缺陷极大增加了恶意攻击的安全风险，网络安全问题迅速渗透到传统的功能安全领域

网络安全



自动驾驶网络攻击



智能家居网络攻击

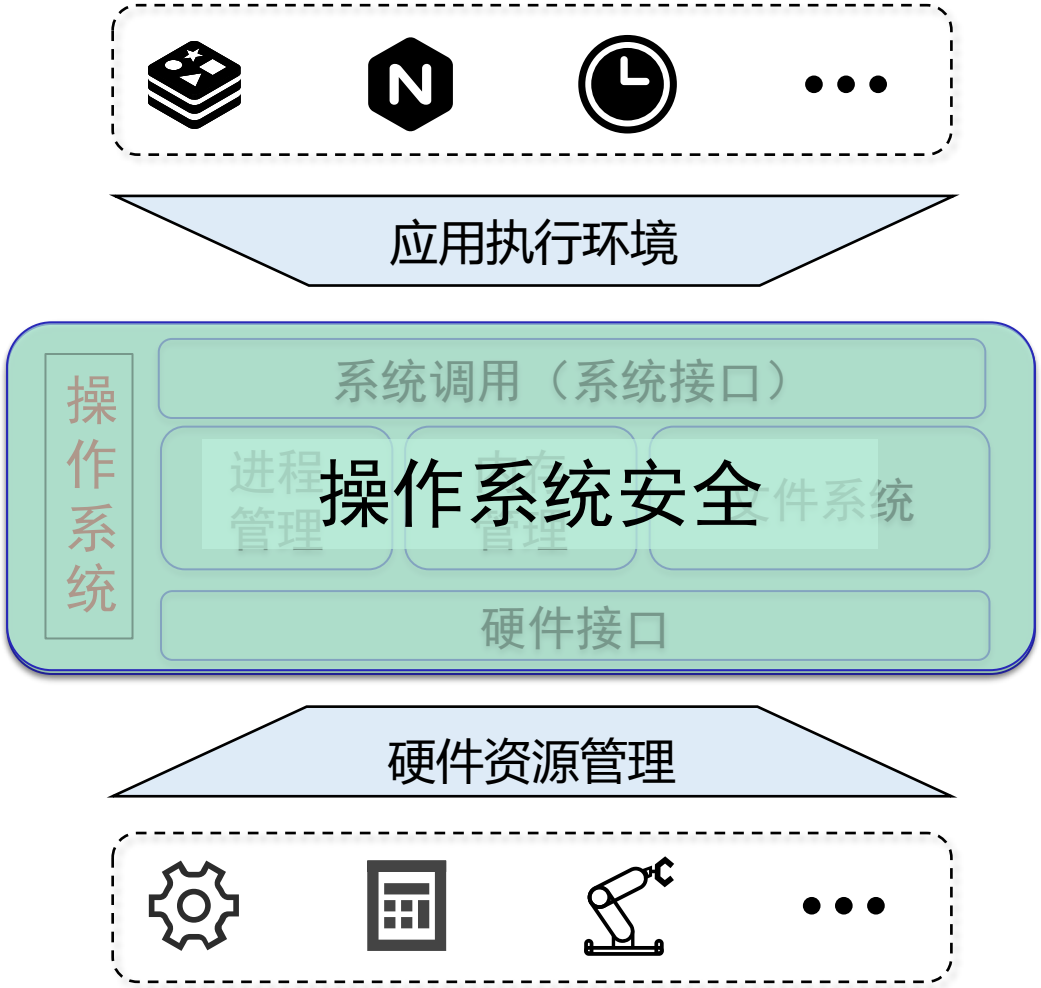
防御未知的网络攻击

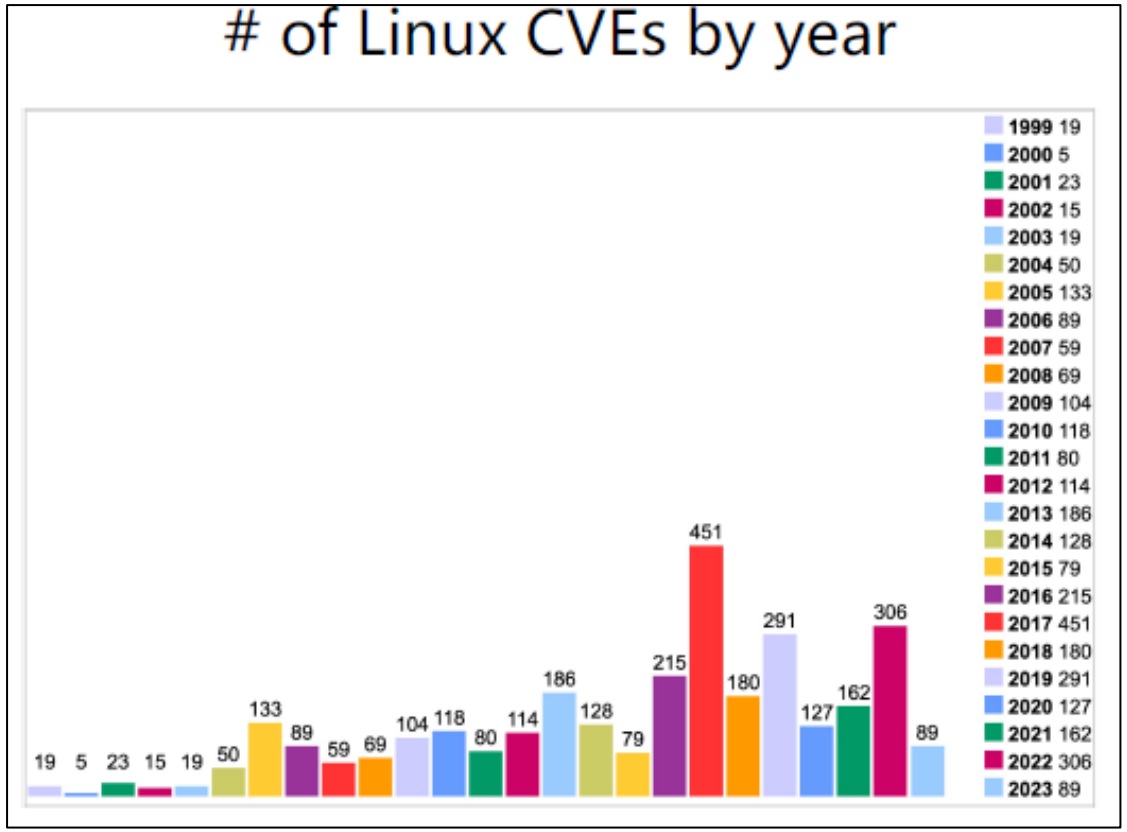
目录

- 背景和现状
- **问题和挑战**
- 系统设计
- 应用案例

问题和挑战

操作系统是软件架构基石，面临着巨大的安全挑战

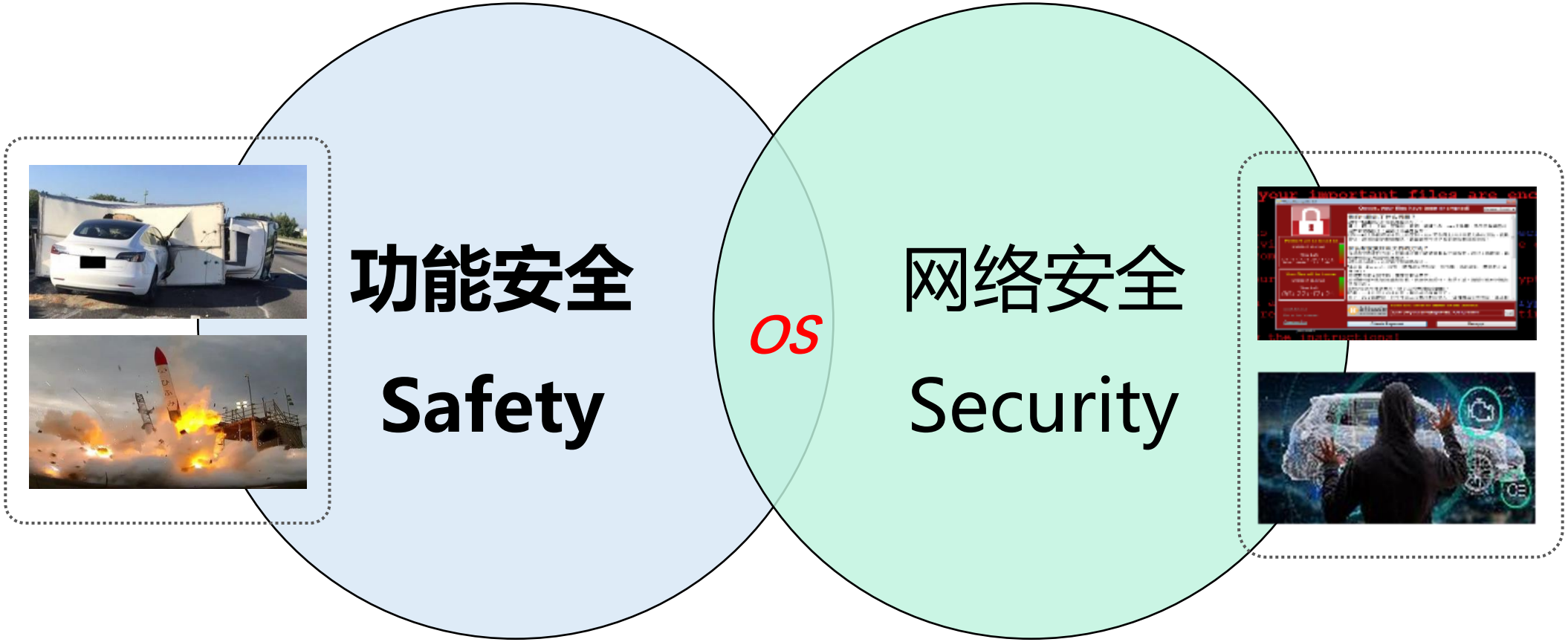




https://cvedetails.com

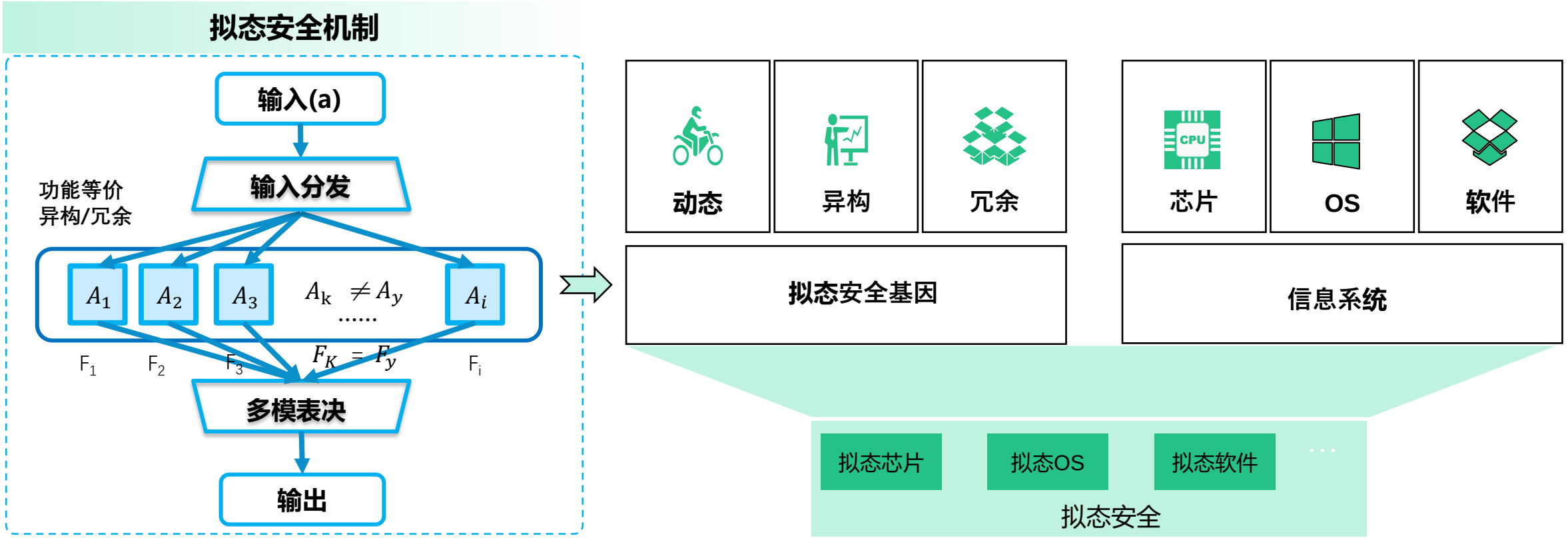
问题和挑战

操作系统需要具有功能安全和网络安全双重安全属性



问题和挑战

鄔江兴院士提出拟态安全，通过动态异构冗余（DHR）特性，为内生安全问题提供综合解决方案



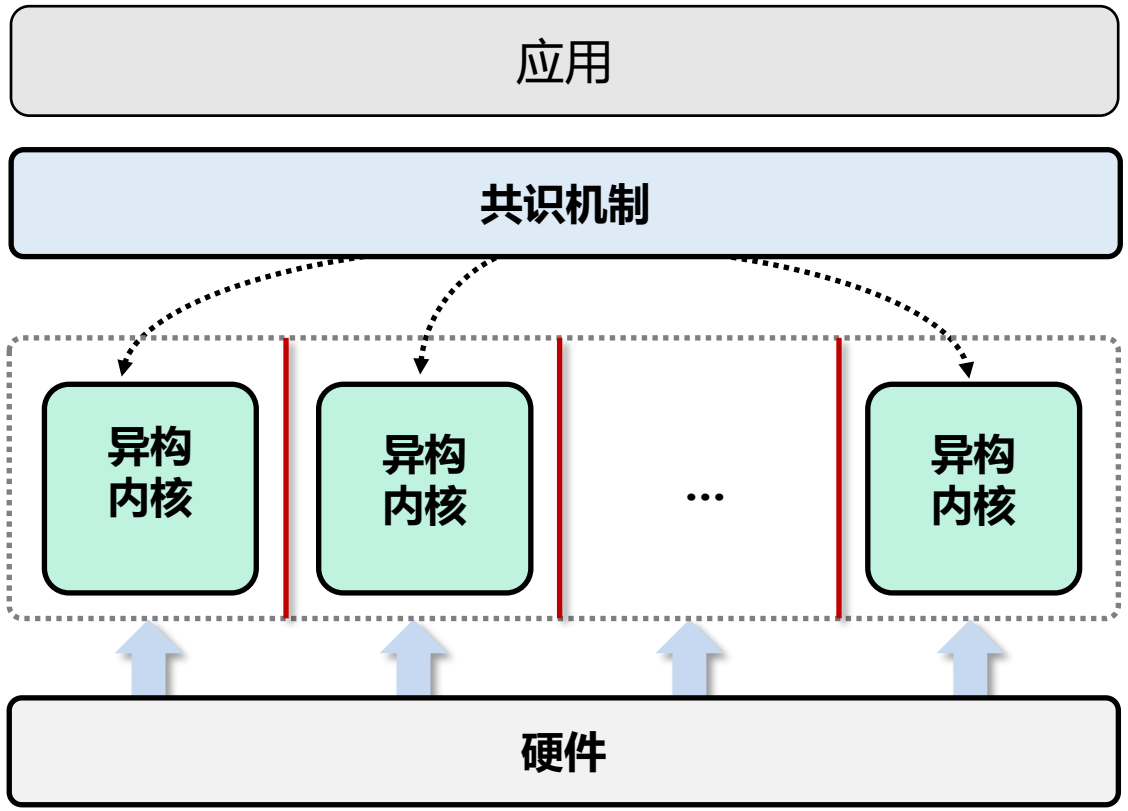
操作系统内生安全是必不可少的一环

目录

- 背景和现状
- 问题和挑战
- **系统设计**
- 应用案例

内生安全的多内核操作系统设计

多内核操作系统架构通过内核级动态异构冗余实现拟态安全

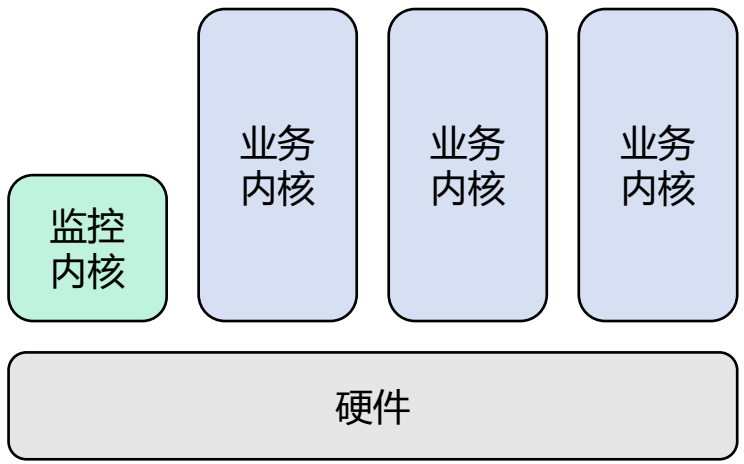


架构特性

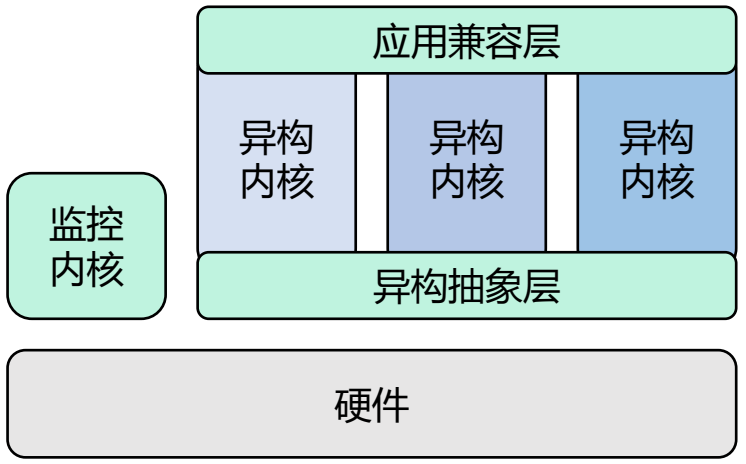
- 同时运行多个内核
- 内核可具备同构或异构属性
- 内核间通过共识机制协同工作

内生安全的多内核操作系统设计

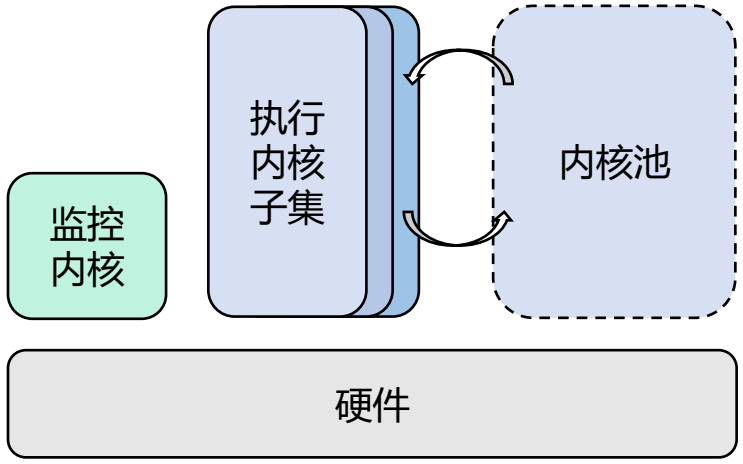
以现有流行系统内核为蓝本，以多内核架构实现动态异构冗余特性



冗余性



异构性

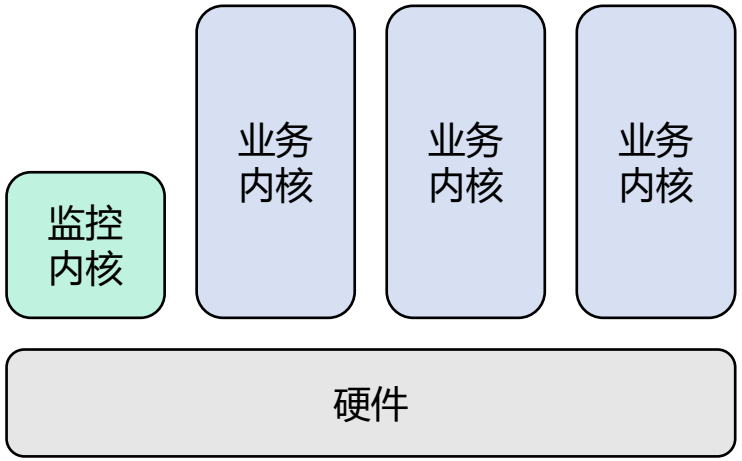


动态性

内生安全的多内核操作系统设计

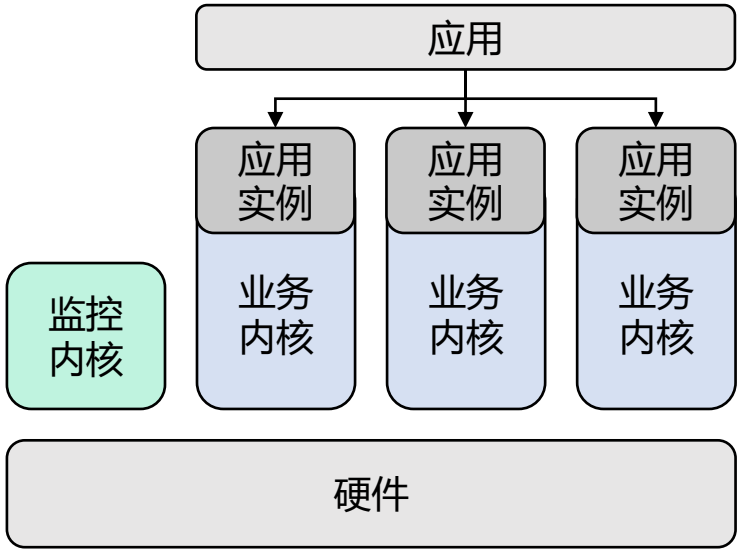
- 冗余内核特性

冗余内核架构



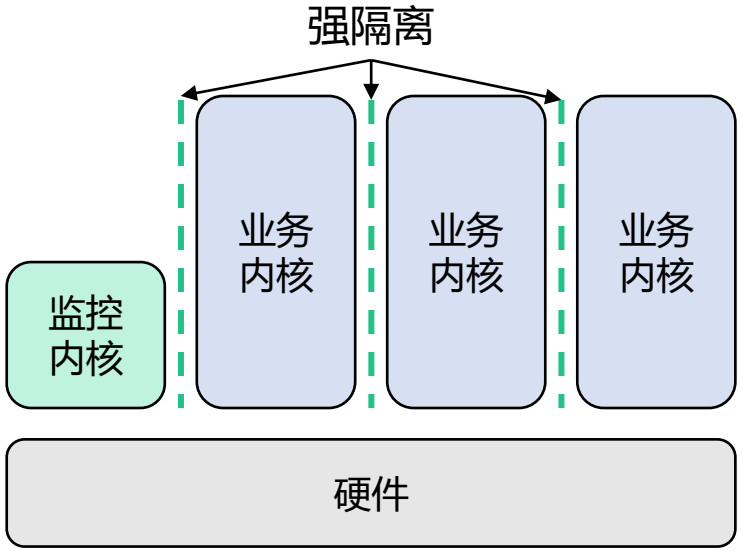
监控内核统摄全局、业务内核独立运行的冗余容错架构

多路径执行



应用透明、语义一致的冗余内核副本以支持应用的多路径独立执行

内核间隔离

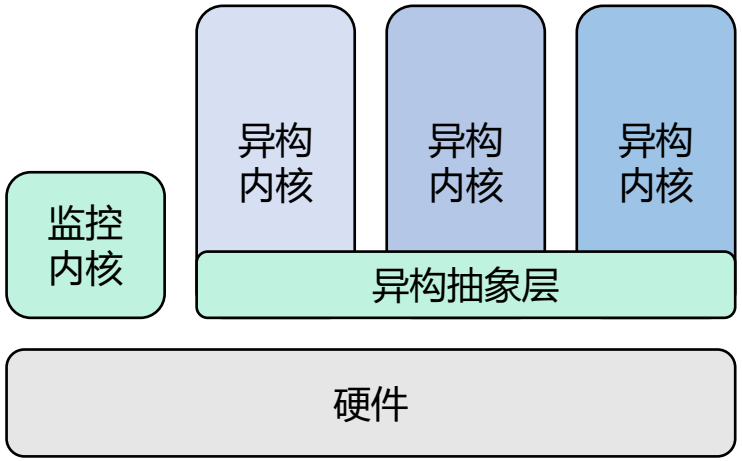


防止功能故障扩散、网络攻击渗透的内核级容错能力

内生安全的多内核操作系统设计

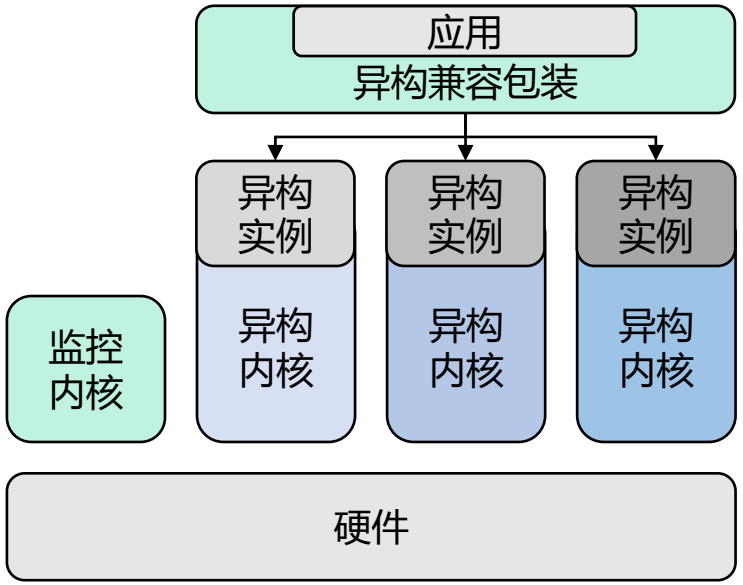
- 异构内核特性

异构内核架构



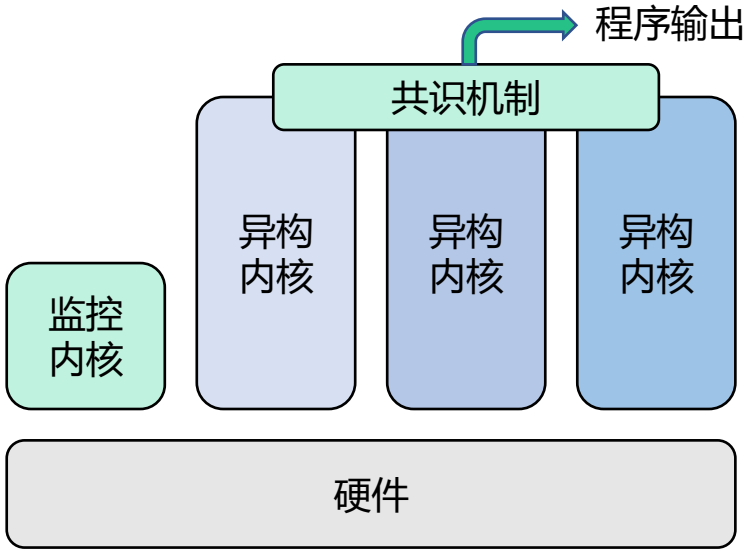
支持异构内核共存的全局数据结构、异构资源接口等抽象层

异构执行机制



异构内核兼容的执行文件格式和异构知晓的应用分派器

异构共识机制

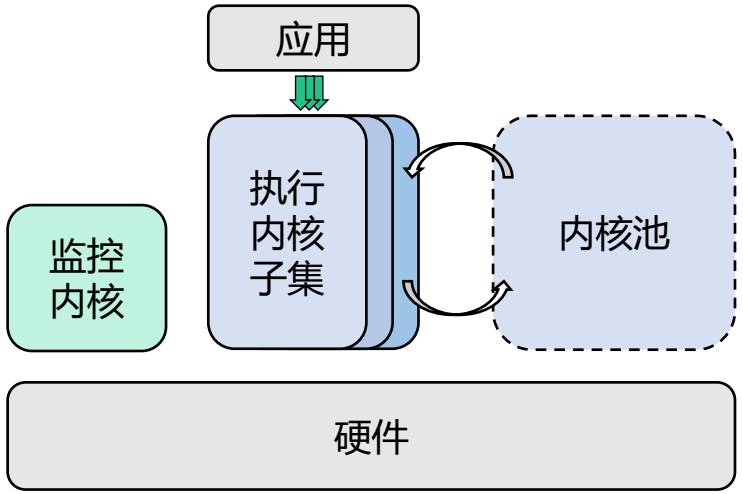


收集差异化运行时信息，经由异构内核表决得到共识

内生安全的多内核操作系统设计

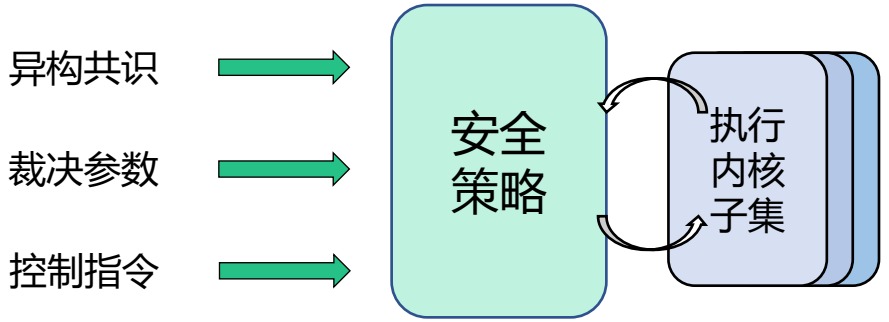
- 动态内核特性

内核子集动态变化



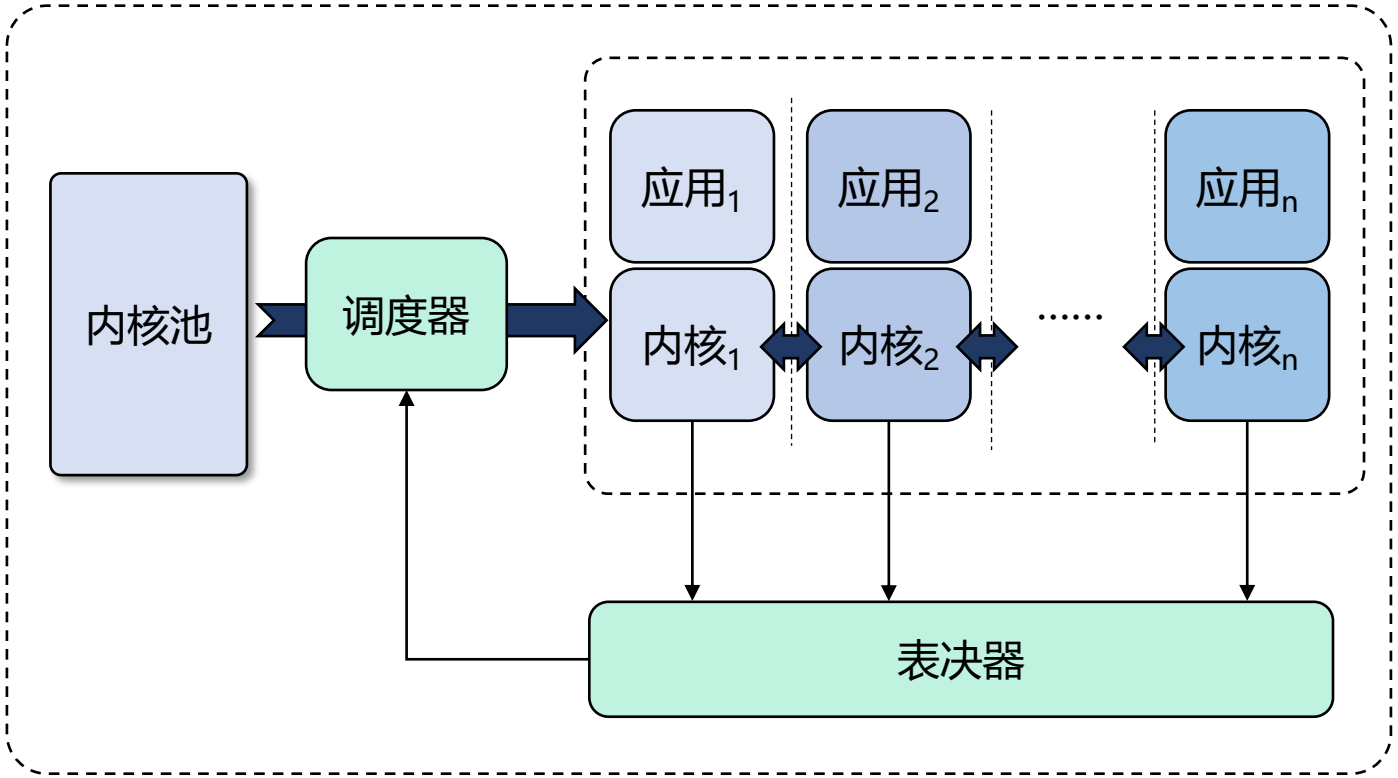
支持时态变化的执行内核集合，包括应用透明的内核间迁移和内核集合的动态加载调度机制

动态迭代策略



基于异构共识机制的安全性裁决和内核集合迭代策略

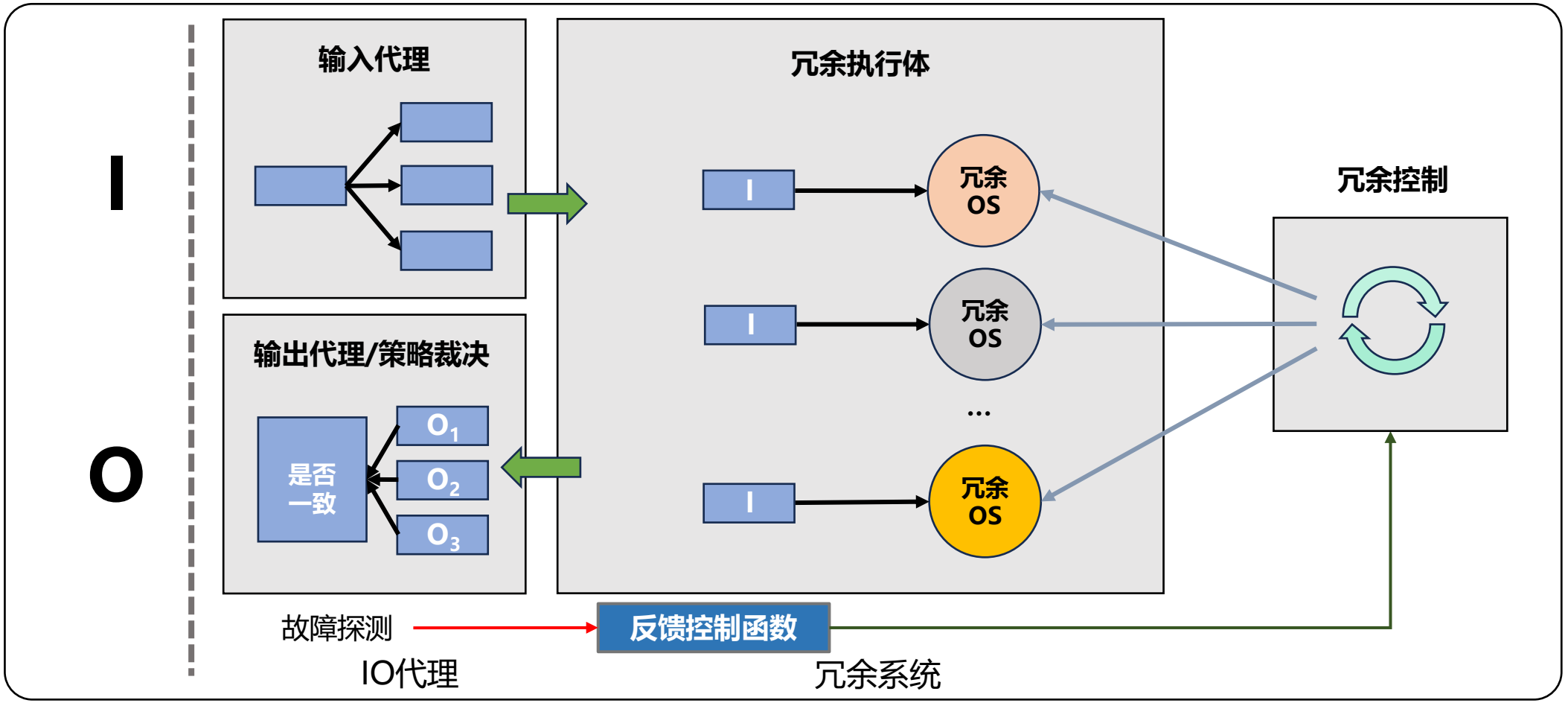
多内核操作系统内生安全原理



- **内核池**
  - 以内核为处理场景元素，池化为异构执行环境集合
- **调度器**
  - 根据安全策略和迭代反馈，选择执行的异构内核子集
- **表决器**
  - 异构内核在执行中藉由表决达成共识，决定下一轮迭代的执行方式

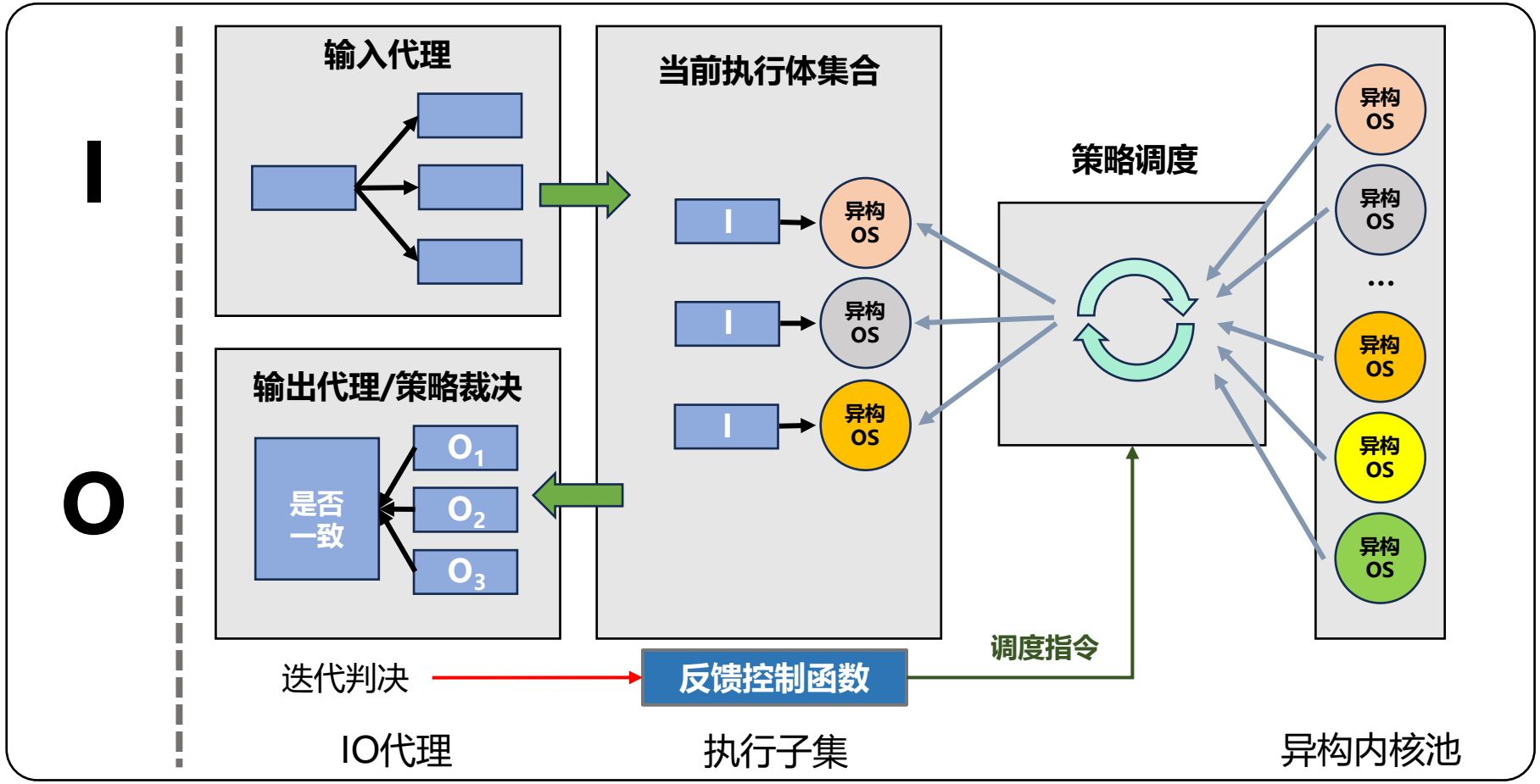
多内核操作系统内生安全原理

- 功能安全原理和机制



多内核操作系统内生安全原理

- 网络安全原理和机制



目录

- 背景和现状
- 问题和挑战
- 系统设计
- **应用案例**

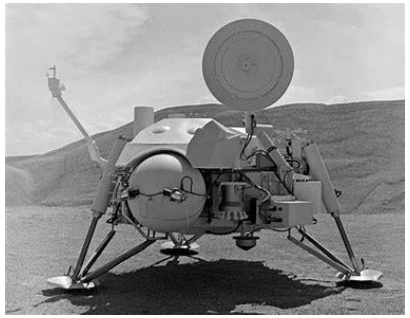
应用场景：星载系统

星载系统面临更严苛的**功能安全需求**

成本高昂	卫星功能故障可能导致作业停顿或系统失联，损失巨额成本	高可靠性
维护复杂	部署在太空，仅支持远程维护，无法实地维护	高可维护

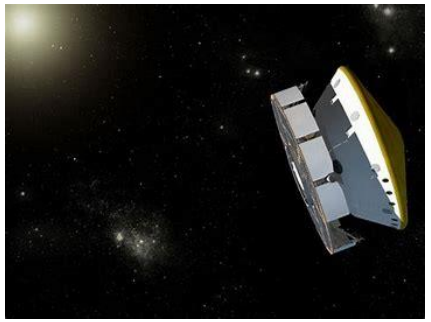
应用场景：星载系统

以**系统更新**为例

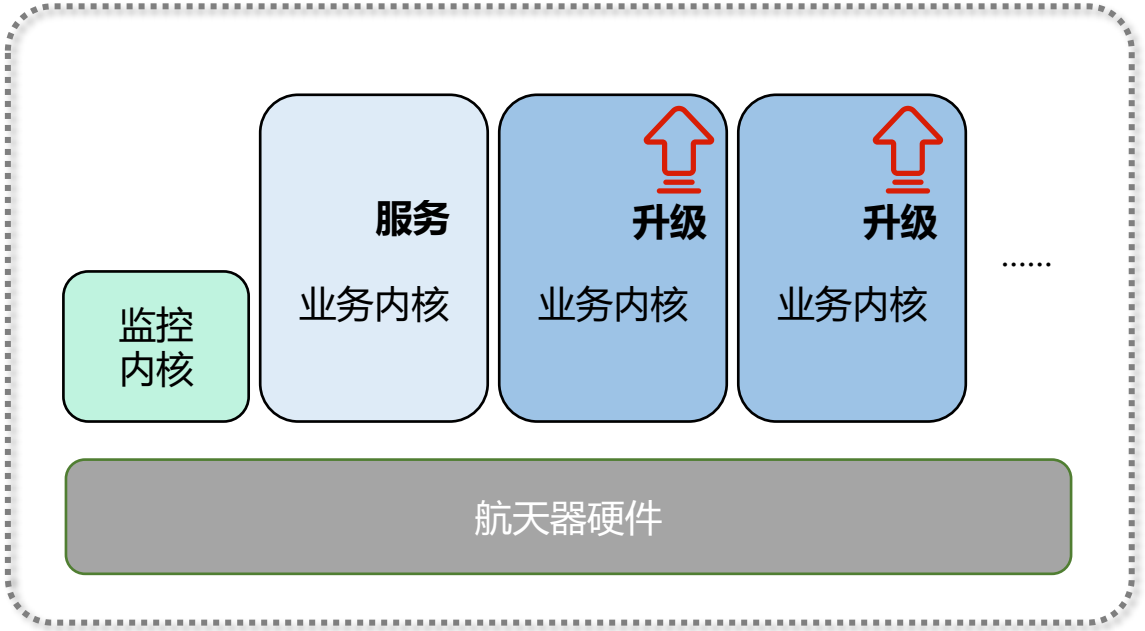


2007年，NASA的火星奥德赛号升级了飞行软件，导致飞行计算机重启，使奥德赛号进入保护模式，推迟了着陆时间。

1999年，NASA的海盗号火星探测器进行了系统升级，导致了一个文件系统错误，使海盗号进入了安全模式，暂停科学任务长达3个月。



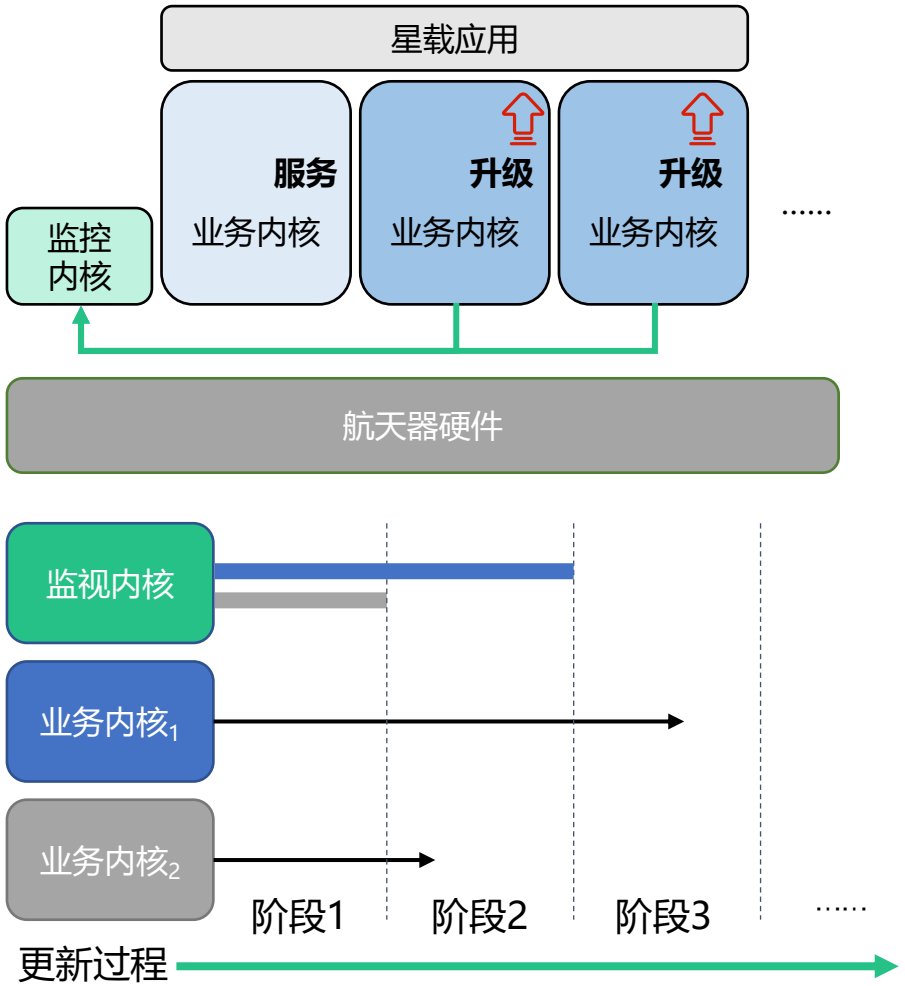
多内核架构提供面向星载系统升级的通用**功能安全**解决方案



- 冗余内核架构以保证更新时的系统可用性
- 监视内核检测更新故障，失败时自动恢复

应用场景：星载系统

系统更新故障检测

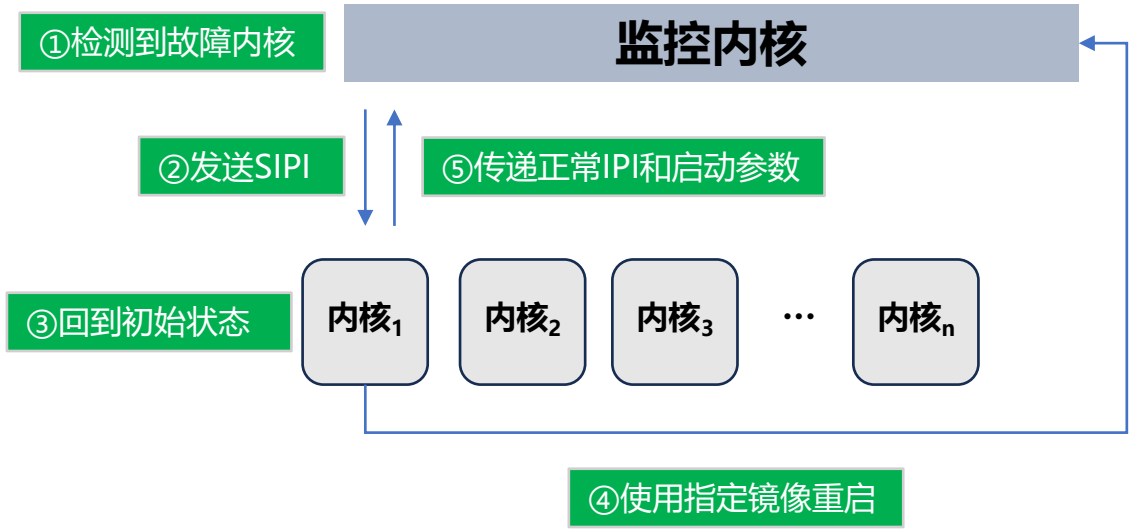


心跳超时机制：检测系统更新部分是否正常

- 冗余架构
  - 监控内核：小的高安全内核，负责资源分配和故障处理
  - 业务内核：大的富功能内核，负责业务计算和设备 I/O
- 阶段心跳
  - 更新内核定期向监控内核报告自身状态
  - 监控内核轮询心跳序列以掌握更新进度
- 超时机制
  - 监控内核为更新副本独立计时，以分布式的思想探测潜在的更新故障和延迟

应用场景：星载系统

系统更新故障恢复



部分重启机制：快速恢复系统的故障部分

- 故障隔离
  - 将更新故障影响限制在局部，不会影响整体系统功能安全
- 轻量恢复
  - 动态修改配置更新启动镜像和参数，快速灵活修复更新故障

展望

内生安全赋能操作系统将能够有望构建安全的操作系统底座，解决操作系统级别功能安全和网络安全保障的难题，实现中需克服如下困难：

- **软件生态和兼容性：异构执行与兼容性的冲突**
- **设备资源的管理：需要有更好的方式以支持更多设备**
- **更多异构架构的支持：当前支持X86/AARCH64架构，未来支持RISC-V等**

FUDAN UNIVERSITY

谢 谢 聆 听 ！