



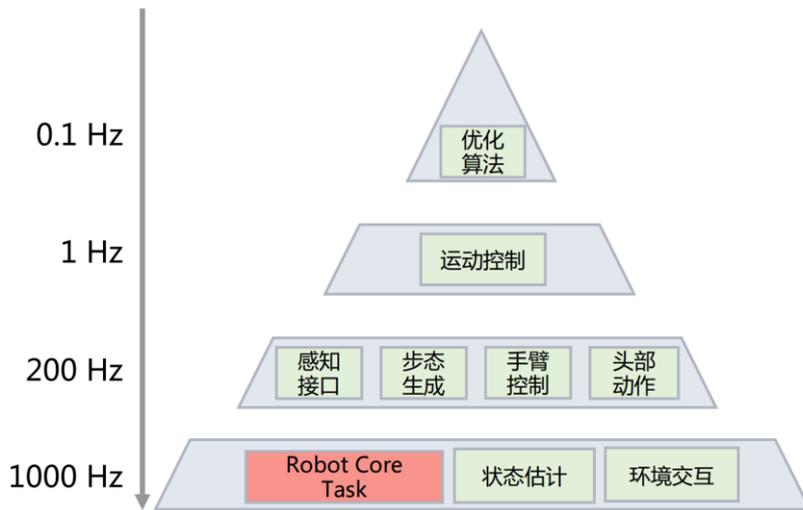
机器人上的虚拟化混合部署探索和实践

睿赛德科技 - 2024.08

机器人系统上的实时控制

需求特点

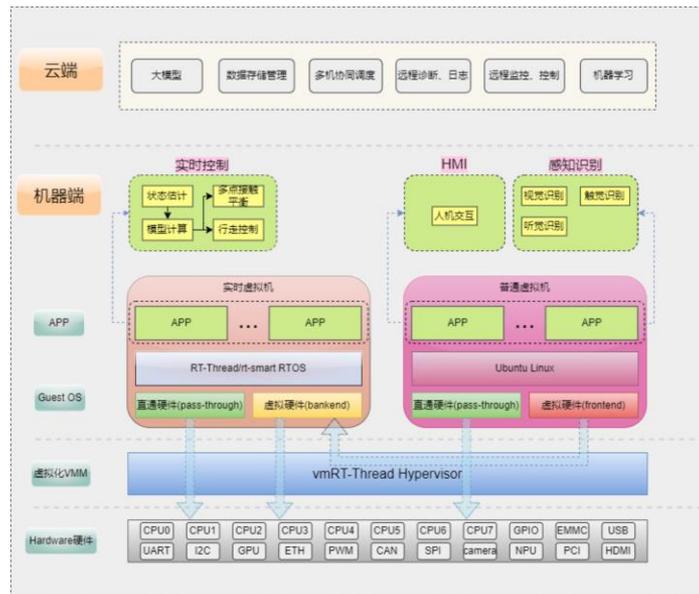
大量的AI感知计算、环境交互与精确的运动控制相结合



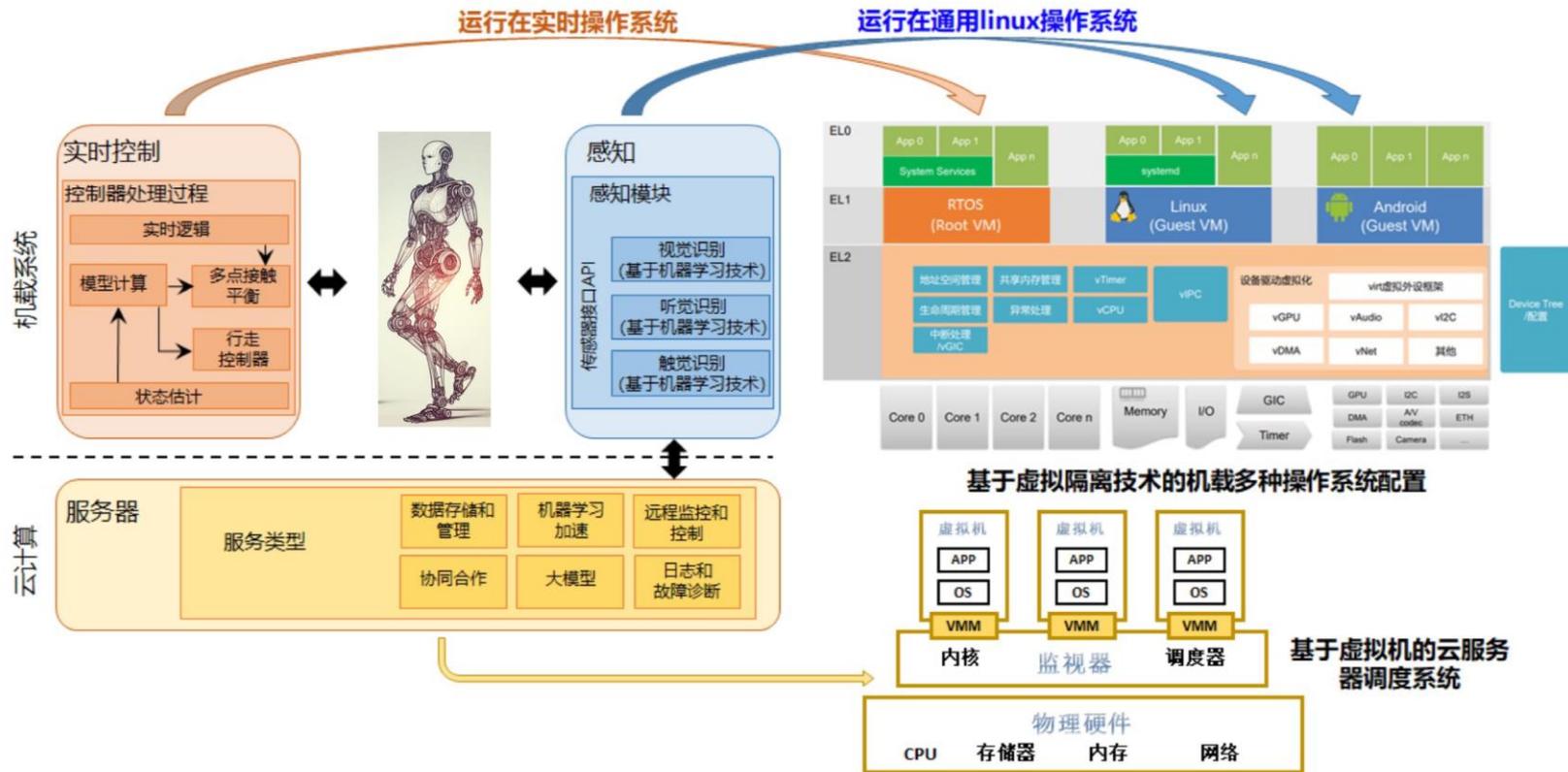
实时性要求：任务在1ms周期时钟下<10us的抖动

虚拟化混合部署方式

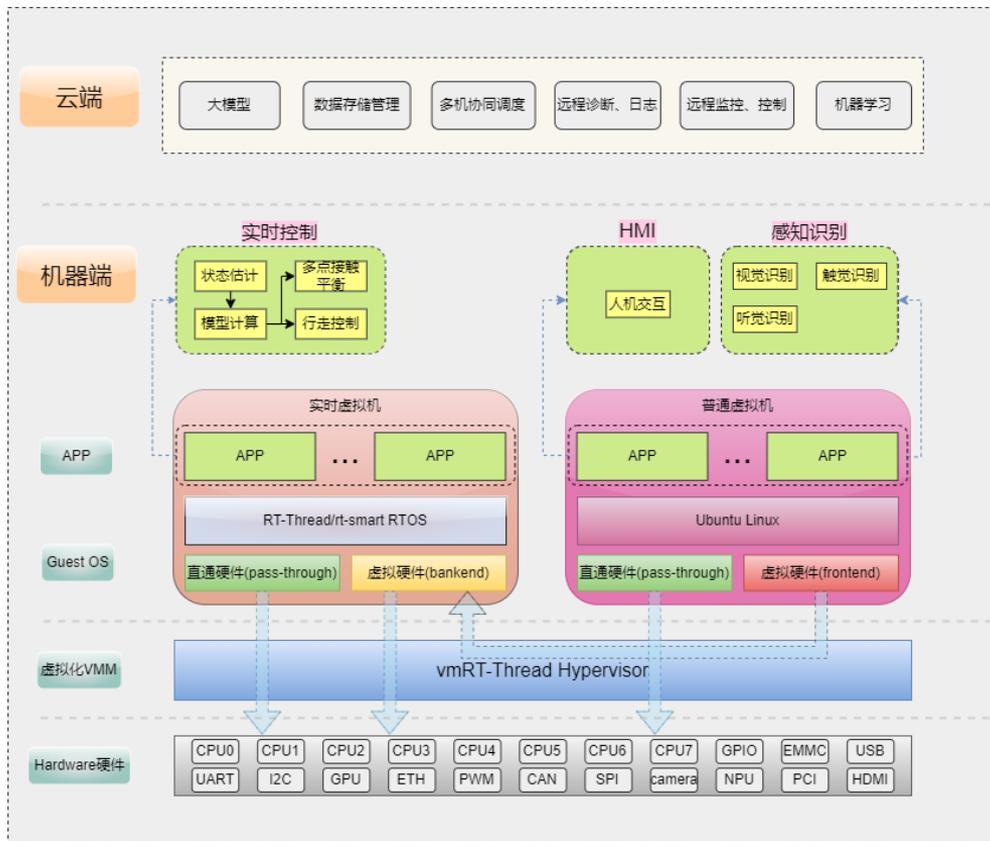
单SOC芯片虚拟化混合部署方案，RT-Thread的实时性与Linux的AI便利兼得



机器人系统上的实时控制与通用系统



机器人系统上的虚拟化混合部署

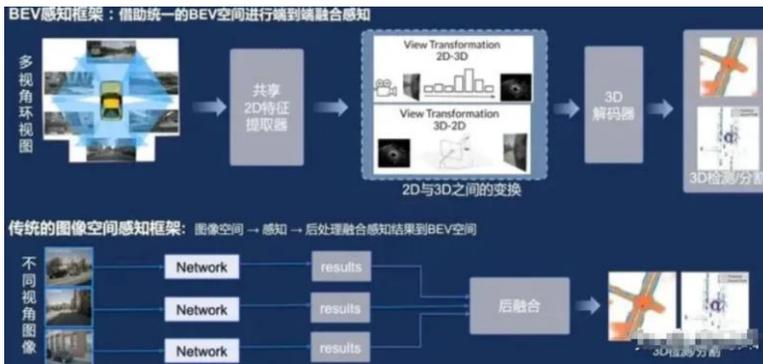
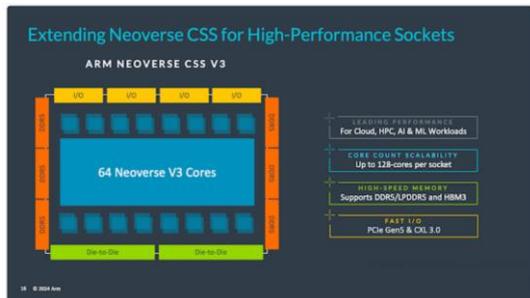


vmRT-Thread是一份Type-1的虚拟机管理器，在之上支持多操作系统运行，并对计算资源进行划分和隔离：

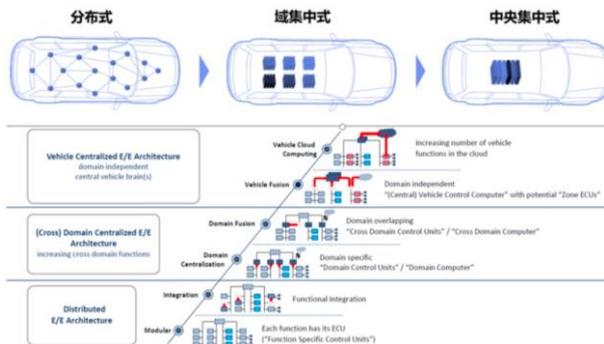
- 对资源进行隔离，保护相互之间的运行时环境互不影响；
- 不同环境下运行不同的操作系统，更好的进行功能切分；
 - 实时性；
 - 功能安全特性；
- 基于Device Tree的方式方便进行资源划分；
- 针对ARM AArch64处理器，在底层EL2接管系统运行，在EL1/0上同时运行多个操作系统；

行业趋势-软硬件

芯片的集成度越来越高、数量和种类越来越多



应用越来越复杂



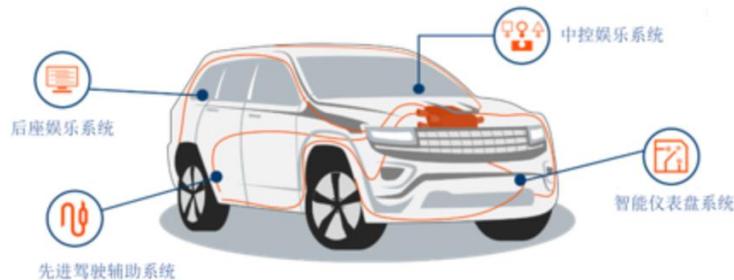
软件规模和集成度提高带来的功能安全和信息安全挑战

特性/解决方案	实时操作系统	Linux操作系统	硬件混合部署	软件混合部署	虚拟化混合部署
实时性	硬实时	软实时	硬实时	硬实时	硬实时
软硬件生态	支持较少	支持丰富	支持丰富	支持丰富	支持丰富
资源隔离	单一地址空间	多进程隔离	硬件隔离	OS间无隔离	硬件隔离
资源分配	N/A	N/A	后期无法修改	后期修改麻烦	只需简单修改
资源共享	N/A	N/A	无法共享	无法共享	灵活共享

随着芯片的算力提升和集成度提高，以及各个行业应用越来越复杂，基于虚拟化技术的集成开发平台，由于其在解决实时安全问题的同时，又能提供丰富软硬件支持，还具备更好的隔离性、灵活性和资源利用率，将会得到越来越广泛的应用。

嵌入式领域的虚拟机管理器情况：

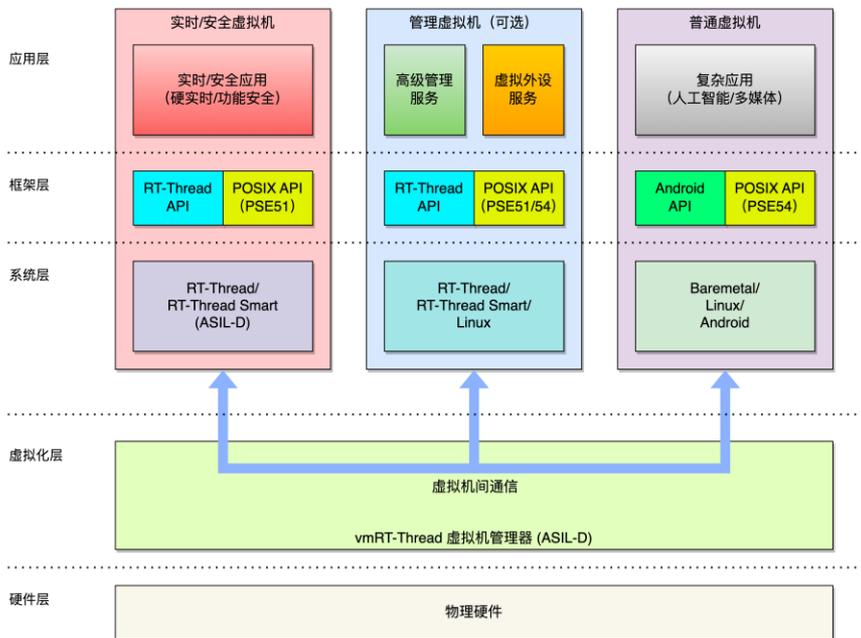
- QNX Hypervisor
- Xen
- Jailhouse
- ACRN (x86, Intel)
- Qemu/KVM (Type-2类型开源虚拟机管理器)



一款符合如下特点的嵌入式虚拟机管理器：

- 适合嵌入式软硬件要求，资源占用小；
- 满足功能安全和信息安全要求；
- 且易于开发、维护和使用；
- 有本地技术支持。

不同安全等级、实时性要求及用户体验与运算能力的集成平台



- 管理服务：包括虚拟机监控和日志等服务；
- 虚拟硬件服务：提供设备虚拟化服务；
- 虚拟硬件驱动：提供虚拟硬件前端驱动；
- 安全应用：对安全要求较高的应用；
- 普通应用：对功能要求较多的应用。

vmRT-Thread 特性



Embedded OS in China
国产嵌入式操作系统产业论坛

超轻量

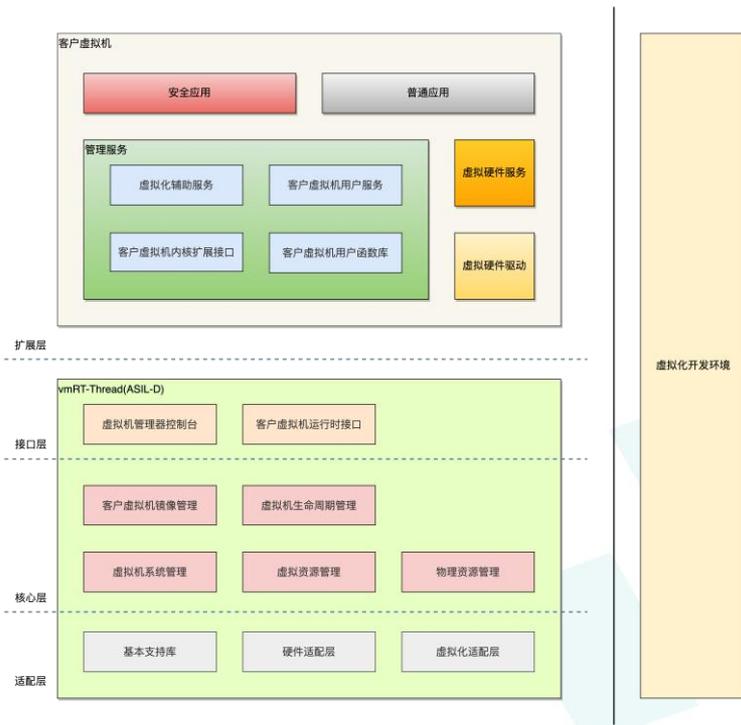
- 核心功能代码约1万行，可容易做到高安全性
- 核心镜像存储空间占用不到1M
- 核心功能运行内存小于64M
- 启动时间短（可低至100ms）

高性能

- CPU虚拟化零损耗
- 支持硬件虚拟化

硬实时

- 中断转发注入延迟：低于10微秒
- 中断直接注入延迟：低于1微秒



vmRT-Thread 理念 - 开箱即用

易于适配

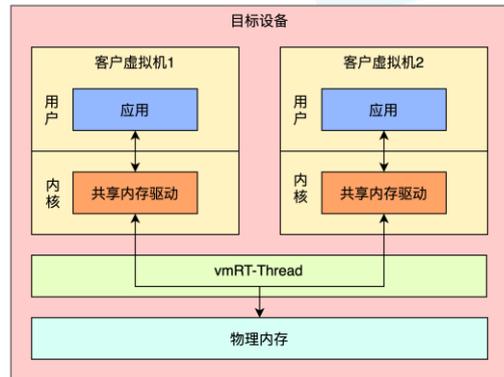
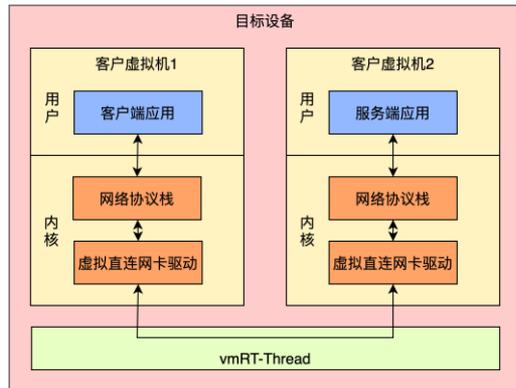
- 按照ARMv8架构标准开发，硬件支持广泛；
- 支持booti、bootimage和bootdistro等引导方式；
- 支持PSCI、SCMI等电源管理规范；
- 支持VirtIO外设半虚拟化规范；
- 支持lvshmem虚拟机间通信规范。

易于使用

- 配置工具
- 构建工具
- 部署工具
- 控制台

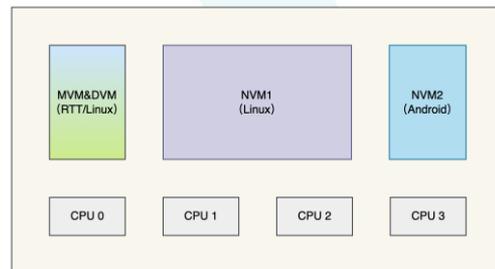
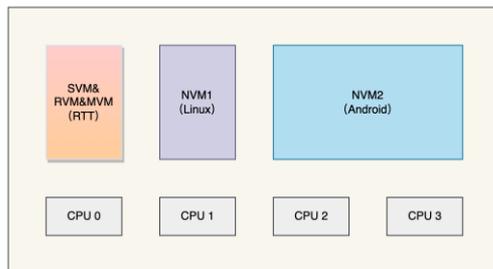
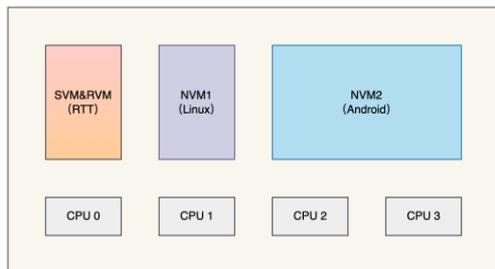
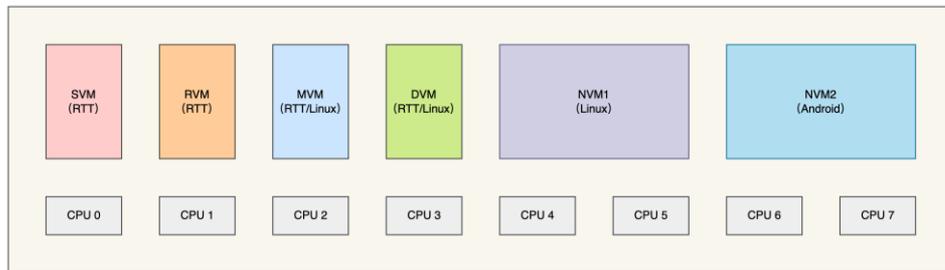
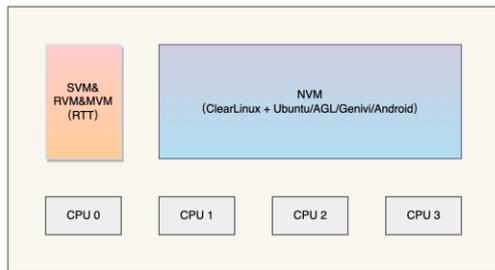
易于开发

- 学习成本低：不管是什么操作系统，无改变需原有开发方式，极少额外学习成本；
- 系统迁移成本低：操作系统几乎不需修改；
- 应用迁移成本低：不同虚拟机中的应用间通信跟多进程一样简单，应用迁移几乎不需要修改；
- 业务支持范围广：可根据业务场景选择合适通信模型Bypass虚拟机管理器，克服Type1隔离造成的性能损失。



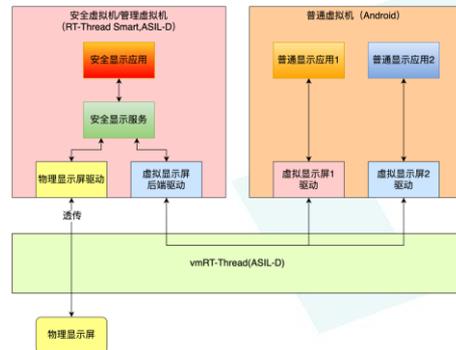
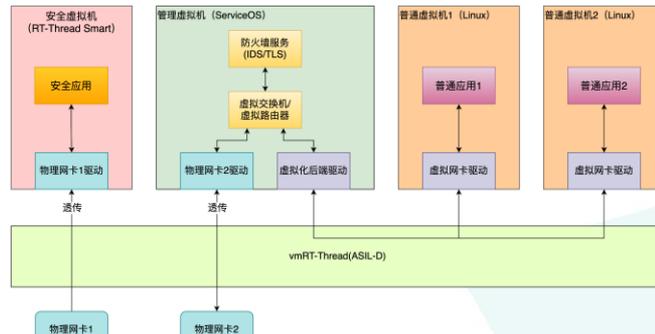
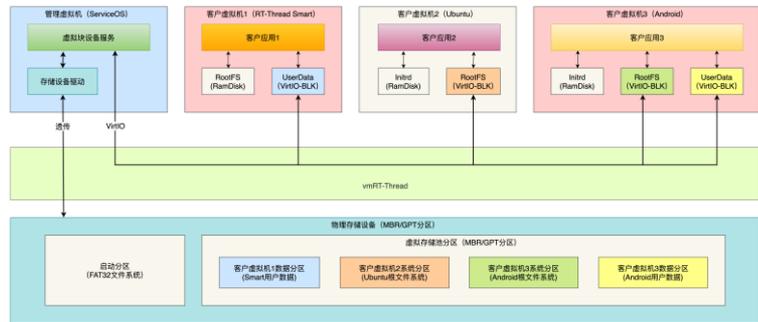
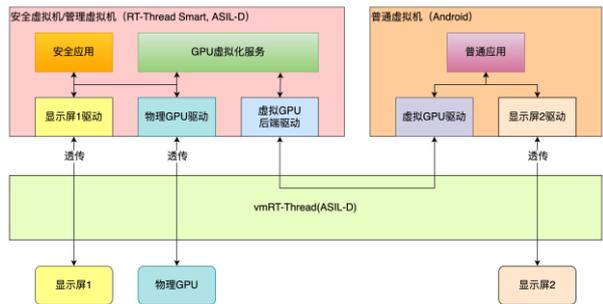
vmRT-Thread 理念 - 部署灵活

可根据业务实际情况进行灵活部署，使用多种多样的虚拟机和操作系统（对RTOS和类Linux系统无特殊限制）组合：



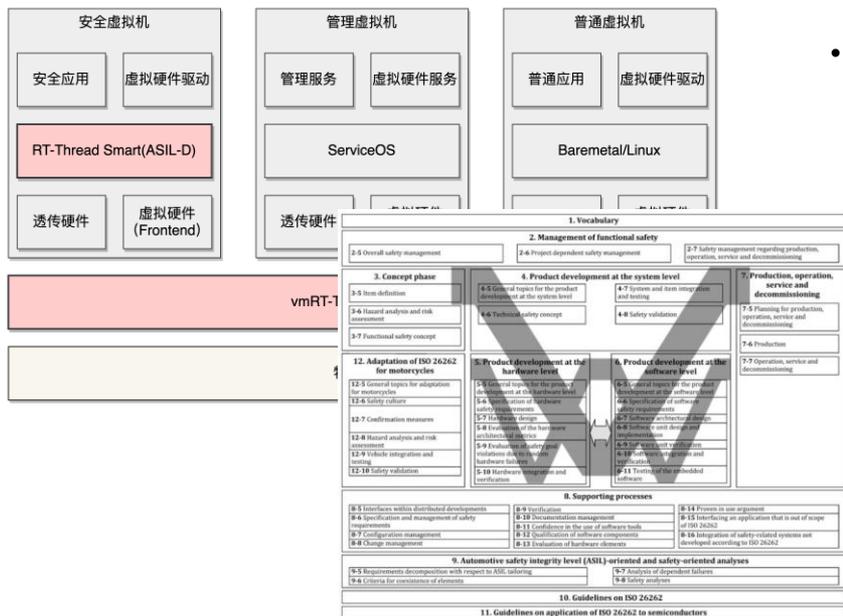
vmRT-Thread 上的外设共享

支持常见的外设共享，包括但不限于：存储、网络、显示和串口等。

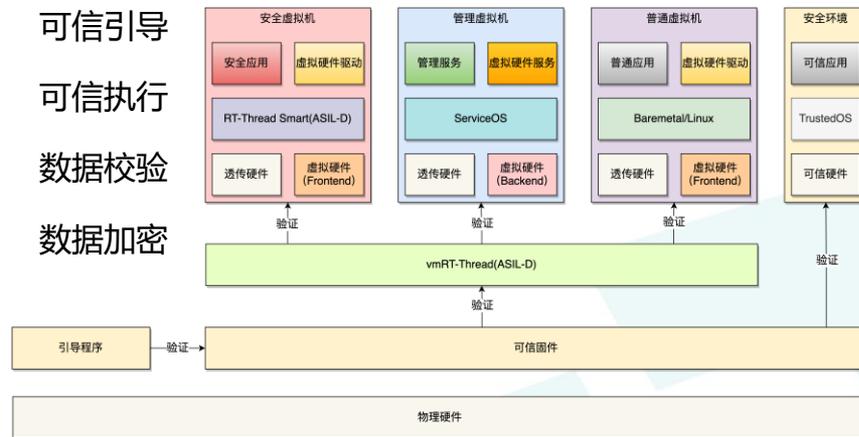


vmRT-Thread 功能安全&信息安全

- 针对高安全性业务场景设计。
- 按功能安全流程开发。

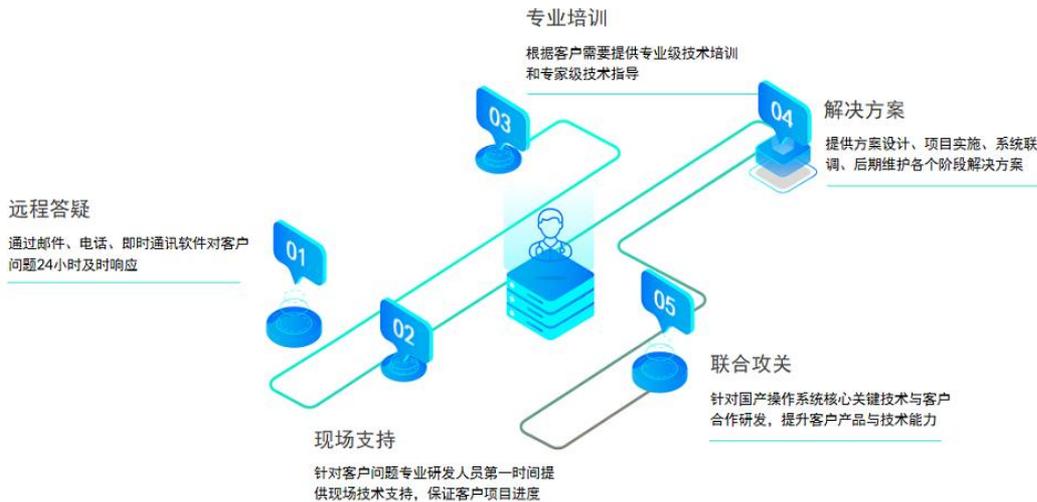


- 可信引导
- 可信执行
- 数据校验
- 数据加密



vmRT-Thread - 技术支持

- 自主知识产权（9项发明专利申请中）；
- 国产芯片支持；
- 可提供远程和驻场服务；
- 重要问题一小时响应；
- 超过十年的嵌入式技术服务经验。



软硬件支持情况



Embedded OS in China
国产嵌入式操作系统产业论坛

软件:

操作系统	状态
RT-Thread/Smart	已支持
Linux + BusyBox	已支持
Linux + BuildRoot	已支持
Linux + Yocto	已支持
Ubuntu	已支持

硬件:

开发板	芯片	状态
Qemu-Virt	Cortex-A72*4	已支持
HD3568	RK3568J	已支持
RockPI 5B	RK3588	已支持
OK3588	RK3588	已支持
RaspPI 4B	BCM2711	已支持

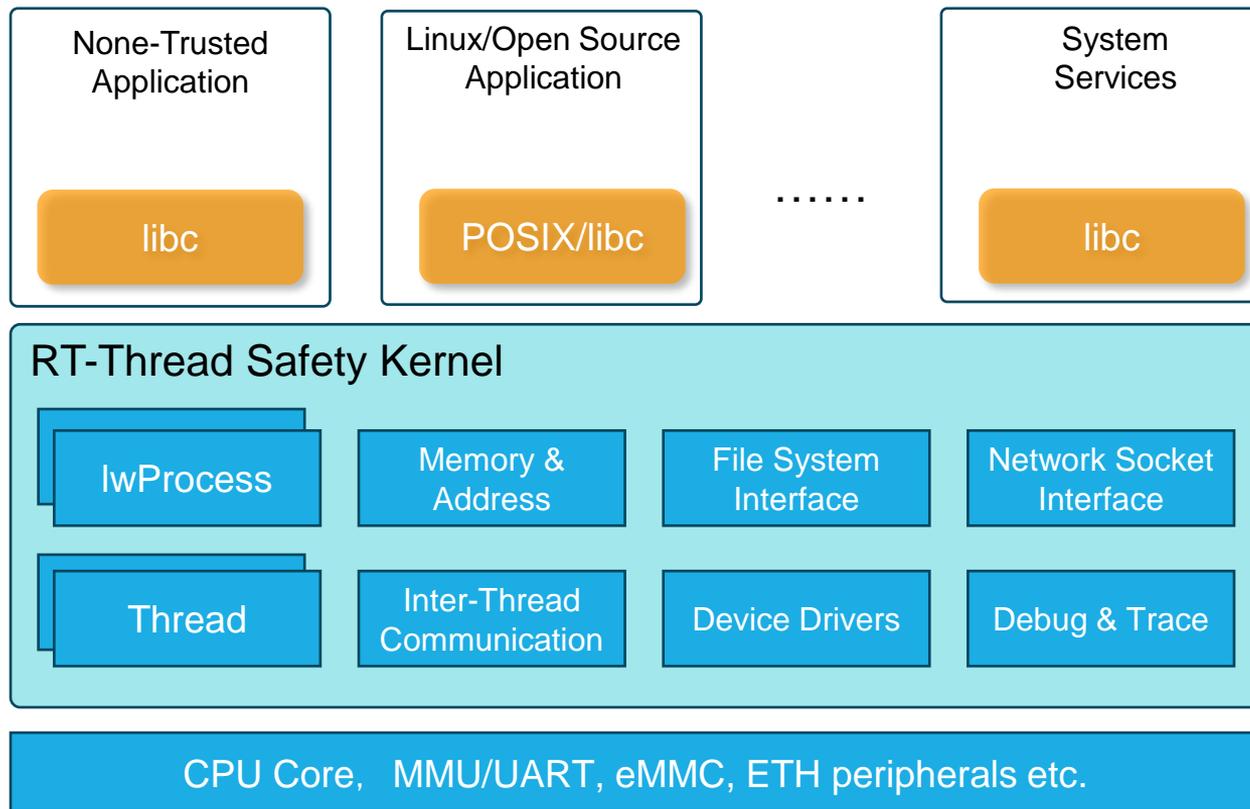
对比情况



特性/虚拟机	vmRT-Thread	QNX	Xen	Jailhouse	ACRN
ARMv8	支持	支持	支持	支持	不支持
CPU共享	分区	支持	支持	分区	支持
内存共享	分区	支持	支持	分区	支持
外设独占	支持	支持	支持	支持	支持
外设共享	支持	支持	支持	不支持	支持
实时性	高	中	低	低	中
国产芯片	多	少	自研	自研	自研
使用成本	低	高	免费	免费	免费
功能安全	支持	支持	不支持	不支持	不支持
本地支持	支持	不支持	不支持	不支持	不支持
特性定制	支持	不支持	不支持	不支持	不支持

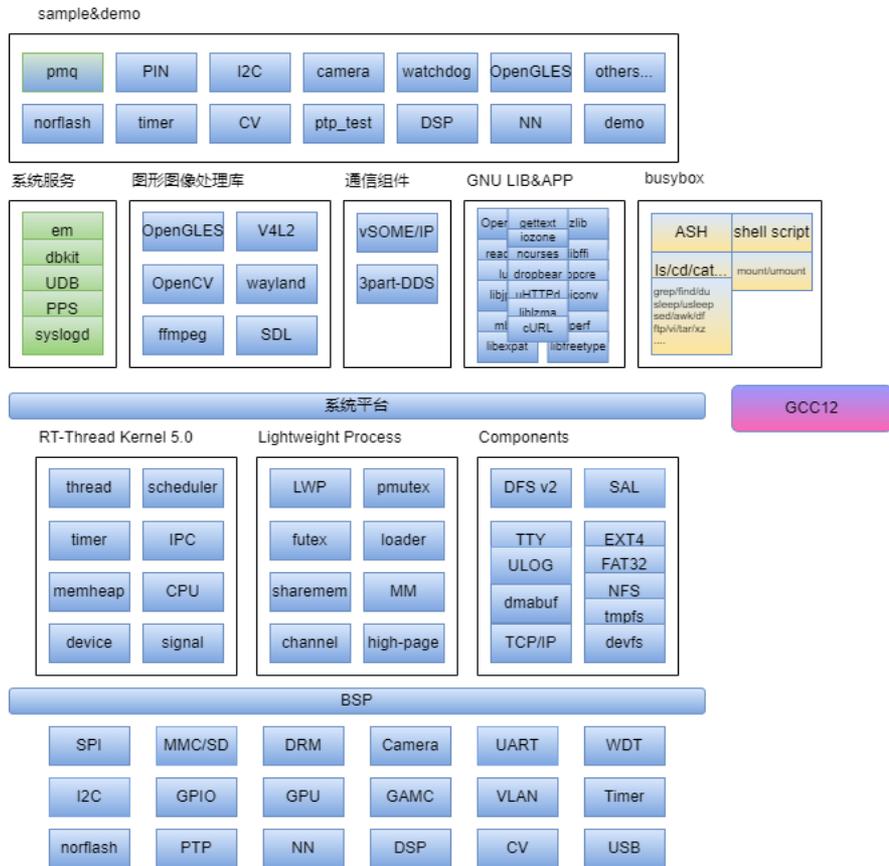
vmRT-Thread上的实时操作系统： RT-Thread Smart

RT-Thread Smart系统架构



- **混合内核实时操作系统**
 - 整体系统分成**内核态**和**用户态**
 - 内核延续RT-Thread内核
 - **非可信应用**放置于系统**用户态**
 - 通用POSIX应用；
 - Linux类开源应用；
 - 产品级功能安全认证；
 - 部分系统服务和内核拆离，可以对系统服务进行独立升级；

RT-Thread Smart系统架构



01. 内核轻量化

- 低至500kB内核尺寸
- 只包含基本功能，同时也可定制（调整系统服务位置）

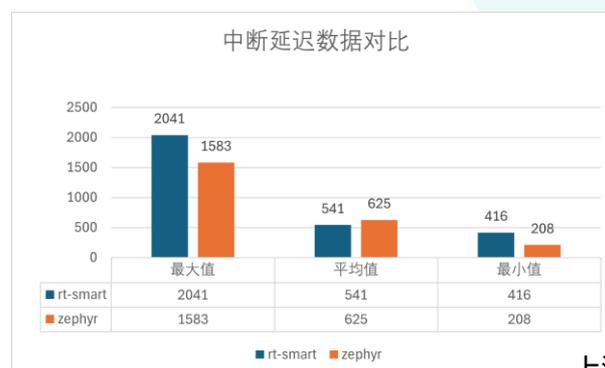
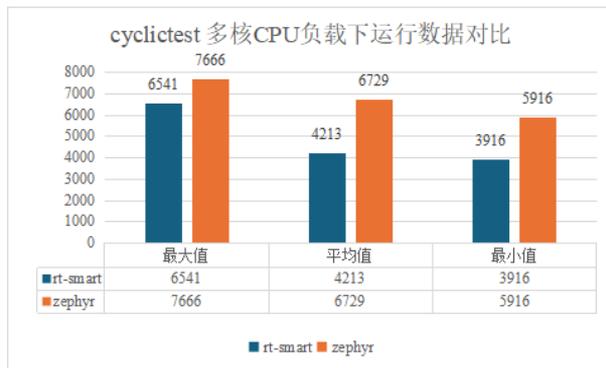
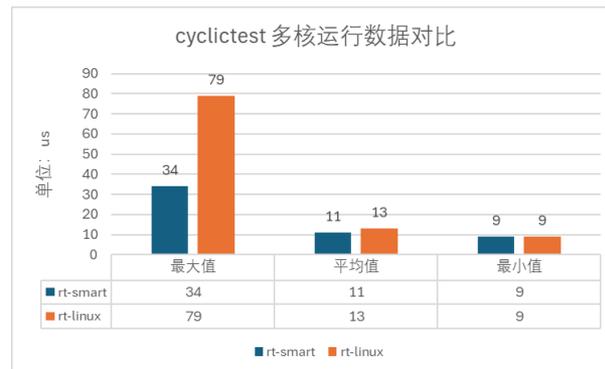
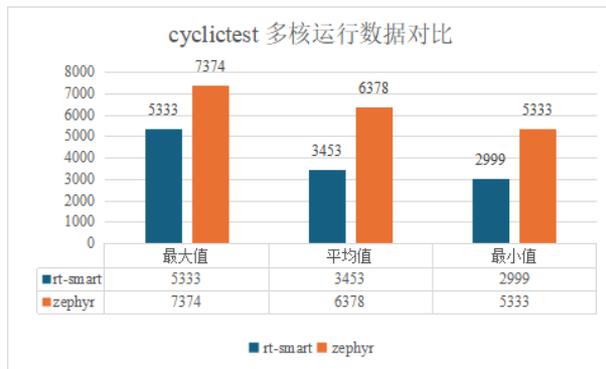
02. 用户态系统服务

- 可拆卸，可重启
- 每个应用进程具备独立的地址空间，相互隔离，安全性好

03. 相同的API风格

- 应用与内核都可延续RT-Thread API;
- 用户态扩展性强

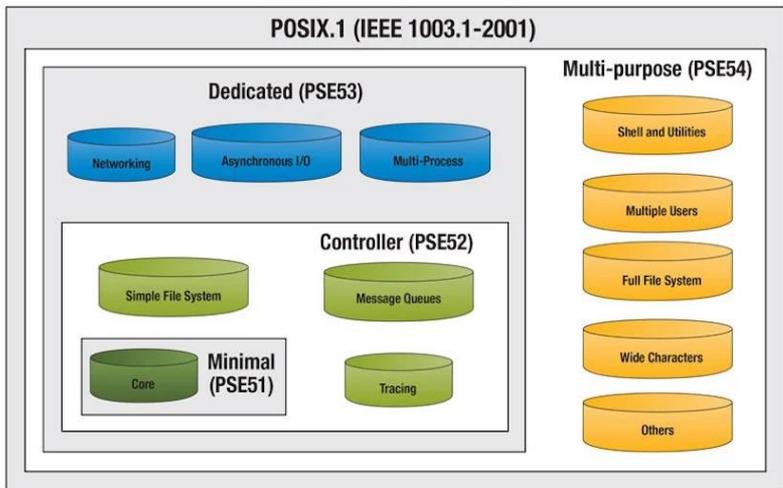
- AArch64 4核硬件环境下，使用相同GCC工具链的实时性测试情况



完整兼容POSIX标准 API、C++11/14

在用户态完整兼容 PSE53 API标准:

- 支持多进程, 包括经典的fork, vfork, pipe系统调用;
- 完整的网络支持, 具备标准的Socket Abstraction Layer (SAL), 并支持UNIX套接字, netlink等;
- 支持POSIX signal, threads等;



01. 完整支持stdc++库

- C++11/14中的标准库, 算法等
- std::vector, std::map, 容器等

02. 并发编程及智能指针

- std::thead、std::future
- std::mutex、std::condition_variable、std::atomic等
- shared_ptr、unique_ptr等

03. 系列语法糖

- auto自动类型;
- lambda表达式及函数等

支持 VS Code 模式进行开发:

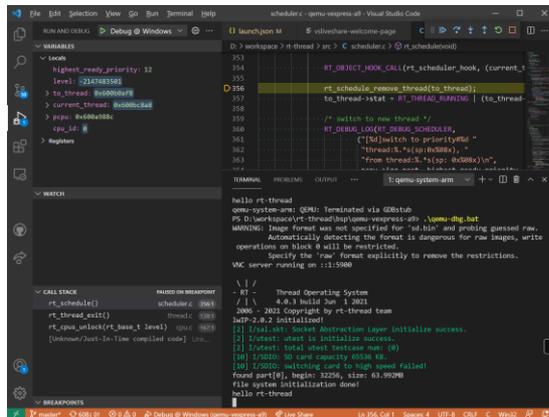
- 创建应用程序
- 连接到远程SSH Server进行开发
- 支持直接调试

Windows & Linux平台下开发

- 推荐Linux平台, 可以更方便进行移植、调试GNU Applications

支持 gdb 调试用户态应用程序:

- 不需要硬件仿真器
- 通过串口连接调试
- 通过网口连接调试
- 支持条件断点, 支持attach到应用程序调试



UART/Networking



SGS **SGS TÜV SAAR**

CERTIFICATE NO. **19100000000000000000** **PAGE 1/1**

LICENCE HOLDER **MANUFACTURING PLANT**

Shanghai Real Thread Electronic Technology Co., Ltd.
5F Bldg.10 NO.88 Daerwen Rd
Pudong New District,
Shanghai,
P.R. China

Shanghai Real Thread Electronic Technology Co., Ltd.
5F Bldg.10 NO.88 Daerwen Rd
Pudong New District,
Shanghai,
P.R. China

PROJECT NO./ID **LICENSED TEST MARK** **CERT. REPORT NO.**

SGS TÜV SAAR **FUNKTIONALE SICHERHEIT GEFÜHRT** **FUNCTIONAL SAFETY APPROVED**

Tested according to **IEC 61508-3:2010**
EN 50128:2011
ISO 26262-2:2018
ISO 26262-4:2018
ISO 26262-8:2018
ISO 26262-9:2018

Certified product(s) **RT-Thread Smart for Safety**

Model(s) **Version 1.0**

Technical Data and Parameter **Usable as part of safety related software acc. to:**

- IEC 61508 up to SIL 3
- EN 50128 up to Software SIL 4
- ISO 26262 up to ASIL D

Specific Requirements **The certificate is based on voluntarily tests. Any changes to the design, components or processing may require repetition of some parts of the qualification in order to retain the certification. The certification report is an integral part of this certificate.**

Certification Body for Functional Safety
SGS-TÜV Saar GmbH
Zertifizierungsstelle für Funktionale Sicherheit

Munich, 21.02.2022
G. Neumann
Gudrun Neumann

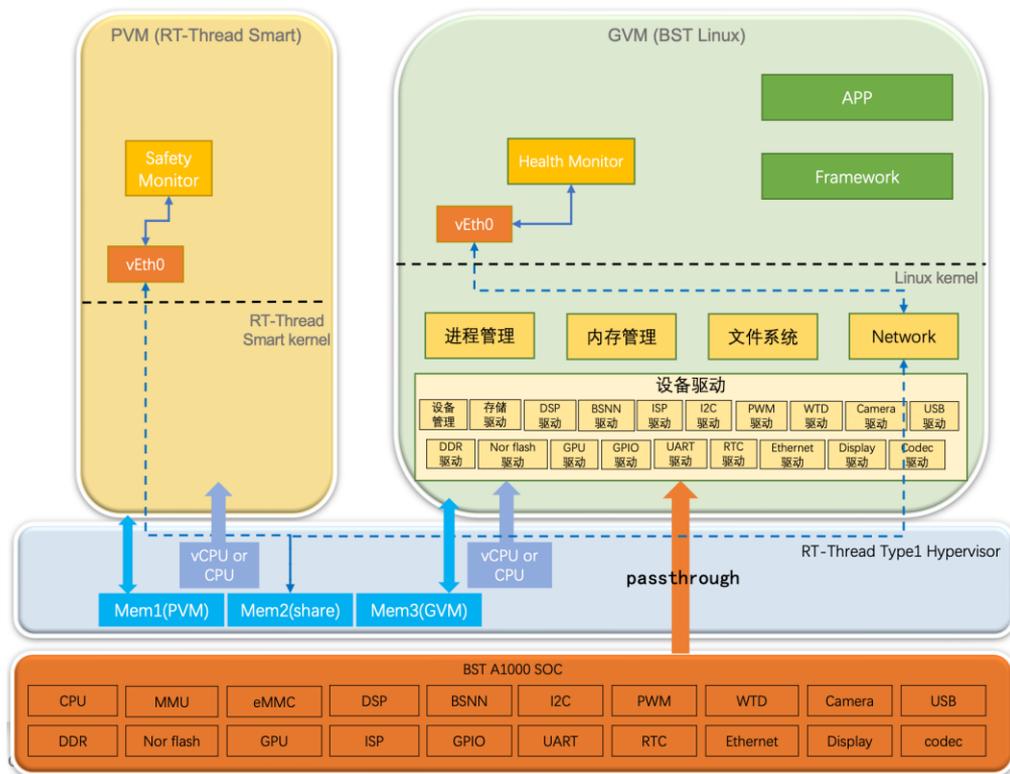
The test mark registration is an integral part of this certificate.
Die Prüf- und Zertifizierungsangabe ist integraler Bestandteil des Zertifikates.
SGS-TÜV Saar GmbH, Postfach 10 15 53, D-66111 Saarbrücken, Germany
Website: www.sgs-tuv-saar.com E-mail: fd@sgs.com

CERTIFICATE

RT-Thread Smart for Safety 具备产品级的功能安全认证:

- IEC61508 SIL3 标准认证
- EN50128 标准认证
- ISO 26262 ASIL-D 标准认证

车载案例：某Tier1环视项目

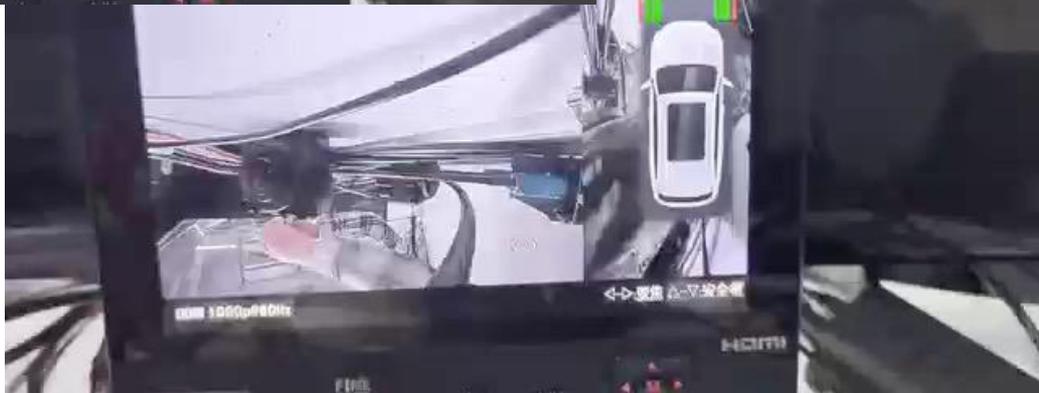


360环视：

- 芯片：BST-A1000，8核A55
- CPU损耗：<3%
- 内存占用：<128MB
- 存储占用：<64MB
- 启动时间：<300ms
- 资源划分：独占方式



上可以正常透传





谢谢!

