

航空电子领域虚拟化技术应用研究

吉沛琦, 张明远, 曲国远

(中国航空无线电电子研究所, 上海 200233)

[摘 要] 随着航空电子系统承载的应用日趋复杂, 飞机对机载设备的计算力和功耗比要求不断提升, 这也推动了嵌入式多核处理器的加速应用和普及。多核处理器在航空电子设备中的深入应用, 随之而来的是运行的软件复杂度急剧上升。随着商用领域嵌入式虚拟化的出现, 如何将该技术更有效的应用到航空电子领域, 成为必须要研究的课题。本文结合航空电子本身的特点, 概述航空电子多核处理器平台上嵌入式虚拟化的特征及应用思路, 为航空电子领域虚拟化的技术研究提供参考。

[关键词] 嵌入式虚拟化; 多核处理器; ARINC 653; hypervisor

[中图分类号] TP316

[文献标识码] A

[文章编号] 1006-141X(2022)02-0027-06

Research on Application of Virtualization Based on Avionics

JI Pei-qi, ZHANG Ming-yuan, QU Guo-yuan

(China National Aeronautical Radio Electronics Research Institute, Shanghai 200233, China)

Abstract: Thanks to the high-speed development of aviation electronic technology, the computing requirements of aircraft on the on-board computer continue to increase. This promotes the application and popularization of embedded multi-core processors on aircraft. The in-depth application of multi-core processors has brought about a sharp increase in the complexity of airborne software. With the prevalence of embedded multi-core virtualization in the commercial field, the application of avionics system design faces challenges. How to effectively apply these technologies to the field of avionics has become a topic that must be studied. Combining the characteristics of avionics, the characteristics and application ideas of embedded virtualization on the avionics multi-core processor platform are summarized, and reference is provided for the technical research of virtualization in the avionics.

Key words: embedded virtualization; multi-core processor; ARINC 653, hypervisor

近年来, 随着我国机载航空电子设备的高速发展, 在核心设备中开始大量应用嵌入式多核处理器, 较为典型的如 PowerPC 架构下 T1040 系列、T2080 系列, ARM 架构下的 IMX、LS1026、Xilinx MPSOC、国产飞腾(双核、四核、八核)处理器、海思处理器以及 MIPS 架构的龙芯等等。根据当前

处理器的发展趋势, 诸如 Xilinx ZynqUltraScaleMP-SOC 这种可应用于航空电子领域的嵌入式 SOC 已经越来越多, 甚至内部集成的处理器核心将会以两位数计加速应用, 处理器的集成度和复杂度也在急剧上升。

收稿日期: 2021-07-07

引用格式: 吉沛琦, 张明远, 曲国远. 航空电子领域虚拟化技术应用研究 [J]. 航空电子技术, 2022, 53(2): 27-32.

随之而来的是航空电子软件的设计难度显著提升,当前已工程化应用的航空电子核心硬件设备已经成为高度通用化的资源平台,通过利用多核处理器的高集成度实现承载几十甚至上百个不同功能和安全等级的应用,同时还必须保证这些应用互相隔离不受影响,能安全、可靠和实时地共享外部资源。在航空电子领域越来越强调敏捷开发的形势下,多核处理器的应用不仅对面向应用的航空电子系统设计提出了更高的要求,也对处理器底层软件、操作系统乃至应用软件的设计和实现带来了前所未有的挑战。在 IT 行业、工业领域,在硬件底层通过程度不同的虚拟化设计提供统一的虚拟执行环境,以此来提升整体的扩展性,大幅降低架构设计的复杂度。经过 50 多年的发展,从处理器硬件、操作系统到工具各自都已经形成了一套成熟、完整的技术体系。

本文针对嵌入式虚拟化技术,研究和探讨在航空领域的应用,为高安全高实时性的机载多核处理器平台底层支持软件提供可行、合理的思路和解决方案。

1 嵌入式虚拟化概述

嵌入式虚拟化是指在嵌入式系统中利用处理器提供的硬件辅助加速能力,将硬件资源(处理器、存储、网络等)抽象为特定对象,从而为应用软件和嵌入式操作系统提供虚拟硬件环境的技术。

嵌入式虚拟化功能实现的核心是虚拟机监控程序,也被称作 Hypervisor。虚拟机监控程序会启用处理器自身提供的虚拟化功能单元,通过处理器特权级别的指令和状态对所有的硬件资源进行统一管理;在启动和运行过程中根据特定的策略对创建的所有虚拟机进行调度,同时捕获虚拟机的所有超权限的访问和操作。

Hypervisor 分 I 型和 II 型, I 型是直接运行在硬件之上(也就是裸机)并提供虚拟机环境, II 型是运行在一个传统操作系统中并提供虚拟机环境。在嵌入式设备中为了提高效率和实时性,一般采用 I 型 Hypervisor 实现虚拟化。图 1 展示了嵌入式系统中虚拟化技术常见的架构层次,其中虚拟机内也支持直接运行应用软件来提高效率,这是用于不依赖操作系统的场景。虚拟机中运行的操作系统成为客

户操作系统(Guest OS),在 ARINC 653 规范中可以用作分区操作系统(Partition OS)。

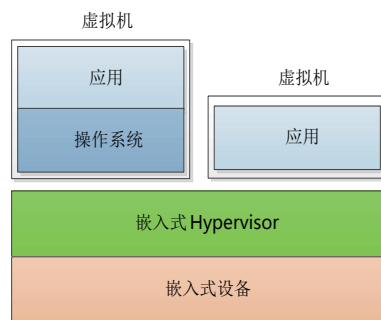


图 1 嵌入式虚拟化架构

上述的嵌入式虚拟化目前无论是在车载系统还是在工业领域均有广泛的应用。图 2 是在汽车生产线的一种应用场景,该嵌入式系统既要完成机器臂的控制和焊接,又要与工程师的平板电脑连接,并显示当前的状态以及操作响应。在这种场景下,嵌入式系统中的多核处理器可以实现至少提供两个虚拟机,其中一个运行实时控制软件,另一个运行安卓系统运行用户界面(UI: User Interface)和交互应用。此外,在车载系统领域不断推出的高集成度系统级芯片(SOC: System on Chip)通过虚拟化技术,可以将 AI、显示、自动驾驶、通信等等进行集成,充分利用了当前不断提升的处理器能力,并降低了系统的规模和生产成本。



图 2 汽车制造领域的嵌入式虚拟化应用场景

2 机载嵌入式虚拟化的特征

在机载航空电子系统中,操作系统等基础软件执行环境应具备高安全、高可靠、高实时性,并且计算、存储资源应占用少。

(1) 效率

嵌入式 Hypervisor 必须处理传统虚拟化环境之外的限制,因此必须规模小且有极高的使用效率;

(2) 安全性

需要更容易验证和证明无漏洞。嵌入式 Hypervisor 程序作为系统中唯一以特权模式运行的部分, 规模和复杂度越小平台就更安全可靠。其充当的是可信计算基 (TCB: Trusted Computing Base^[1]);

(3) 通信

嵌入式 Hypervisor 的目标是运行多个 Guest OS, 因此需要既有效又安全的通信通道, 并允许特权和非特权应用程序共存;

(4) 隔离

隔离 Guest OS 和应用程序的能力关系到嵌入式系统的安全性。需要提供可靠安全的容器, 从而允许专有软件与开源软件在隔离的环境中共存;

(5) 确定性

嵌入式 Hypervisor 必须支持实时功能的调度, 具有实时特征的调度允许关键功能与一些尽力运行的应用程序共存。

3 机载多核虚拟化设计

3.1 嵌入式 Hypervisor 的设计

(1) 实时性安全性设计

以当前机载主流应用的 ARMv8 架构处理器为例, 充分利用其硬件在安全、指令执行方面的功能, 提高虚拟机代码运行的效率和安全性。

在 ARMv8 架构中^[2], 定义了四层安全等级 (异常等级, Exception Level) 的指令结构。这四层级的指令体系包括: 用户层 EL0、内核层 EL1、虚拟机管理层 EL2 以及安全监控层 EL3。具体结构如图 3 所示。

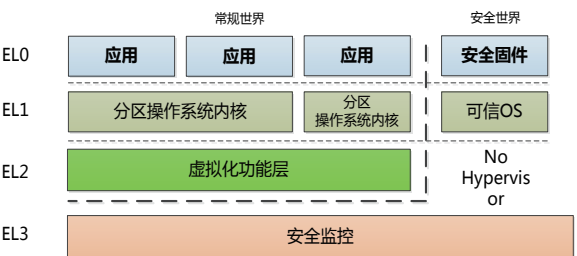


图 3 ARMv8 异常等级架构

处理器在正常运行的情况下处于 EL0 级或者 EL1 状态, 并运行应用软件、分区操作系统内核的指令和功能。当由于应用或者分区操作系统指令运行异常、中断触发以及执行系统调用时, 处理器进

入 EL2 等级状态并开始执行虚拟化功能的软件, 完成异常的处理、中断向分区的传递以及系统调用服务等只能在 EL2 下才可以执行的功能。当本次 EL2 等级的功能执行完成后, 根据当前状态返回到 EL0/EL1 等级状态。

ARMv8 的这种指令架构体系和运行模式, 确保了在提供虚拟化能力的情况下软件指令的运行不受任何影响, 并使得处理器在硬件层面支持了运行在 EL2 层级的虚拟化中间件实现对其上的操作系统内核进行完全的控制和管理, 进而实现符合航空电子设备中 ARINC 653 规范和 GJB 5357A 中对操作系统核心层的功能定义。

基于上述特征, 可以实现程度更深的故障监控 (HM: Health Monitor) 和故障恢复, 如图 4 所示。在 EL2 层级实现了对 EL1 上操作系统的监控和控制。当由于 EL1 层的操作系统内核故障甚至死机时, EL2 层的虚拟化中间软件仍然运行, 并可以执行健康监控和故障恢复等操作。无论是记录故障当前的现场、还是重新装载和运行故障的分区操作系统, 都对整个多核处理器硬件平台的健壮性、健康管理的程度实现了很大程度的提升。

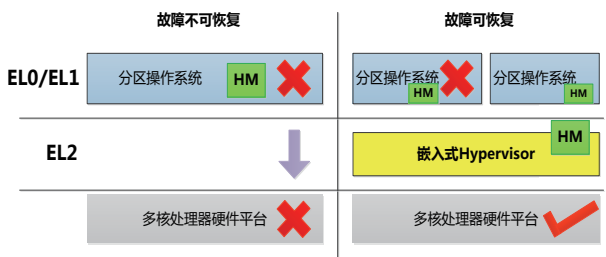


图 4 基于 Hypervisor 的故障监控设计

(2) 空间隔离设计

空间隔离指的是同一个处理器上的每个分区或者 GuestOS 都在限定的环境内运行互相不受影响。这个也是航空设备对操作系统分区的基本要求。

在 ARMv8 架构及其虚拟化场景下, 处理器采用两个阶段地址实现地址翻译。分区操作系统运行在非安全模式的 EL1 和 EL0, 当其中的进程访问分区的虚拟地址 (VA: Virtual Address) 时内存管理单元会将 VA 翻译成中间物理地址 (IPA: Intermediate Physical Address), 这是阶段 1 的地址翻译, 然后内存管理单元再将 IPA 翻译成物理地址 (PA: Physical Address), 这是阶段 2 地址翻译。如图 5 所示。

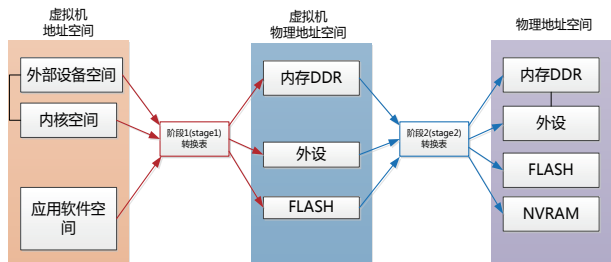


图 5 ARMv8 地址翻译机制

通过 ARMv8 的这种空间访问地址翻译机制，可以控制虚拟机是否可以访问特定的某一块物理内存以及出现在虚拟机内存空间的位置。这种能力对于虚拟机的存储空间隔离至关重要，从而可以分别构建分区层操作系统的虚拟内存空间管理和虚拟化功能层（也就是核心层）的内存空间管理，这种处理器层面的功能确保了既可以满足分区层内存空间管理的通用性和独立性，也可以满足在航空电子系统应用场景下对嵌入式设备在空间隔离方面的要求。

此外，通过地址翻译的机制可以支持分区操作系统对地址空间的无差异化使用。也就是说同一处理器上运行的多个分区操作系统均可以使用相同的地址空间管理自身的 MMU 和访问。结合 32 位指令和 64 位指令的兼容能力，可以做到旧应用的最小化改动和移植，提升了硬件平台的集成能力。

(3) 时钟虚拟化和时间调度设计

在机载设备中，根据 ARINC 653 的规范^[3]和 GJB 5357A^[4]的规定，分区操作系统的调度应可按照分时的方式运行和调度。

在 ARMv8 架构中，每个 ARM 内核都有一组通用时钟，这些通用时钟都由同一个系统计数器提供基准计数。每个处理器物理内核包含了两种时钟供 EL1 级的操作系统使用：物理时钟和虚拟时钟。物理时钟产生绝对时间，虚拟时钟在物理时钟的基础上减去偏移，虚拟化中间件负责调度运行的虚拟内核（vCore）指定对应的偏移寄存器，如图 6 所示。

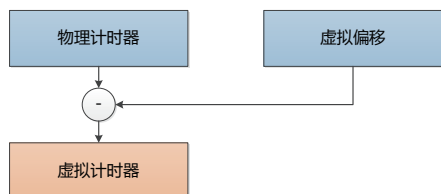


图 6 时钟虚拟化

通过上述机制使得虚拟时间只会覆盖虚拟内核实际运行的时间，从而实现了各个虚拟内核上运

行的分区操作系统基于时间窗口的调度，也就是 ARINC 653 规范和 GJB 5357A 标准中定义的时间调度功能。如图 7 所示，分别对虚拟内核 vCore0 和 vCore1 上运行的分区操作系统进行时间调度。

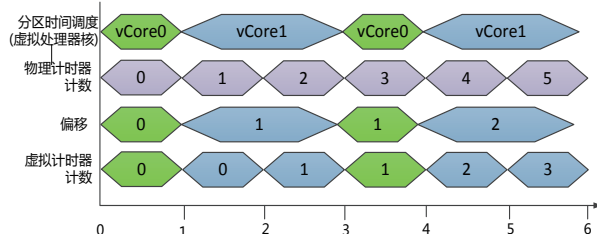


图 7 分区时间调度原理

3.2 分区操作系统虚拟化设计

嵌入式 Hypervisor 只提供了运行虚拟机或者分区操作系统的基础。而在分区操作系统内部，需要提供基于虚拟化能力并经良好设计的接口和服务。

多核处理与操作系统接口主要用于为应用提供屏蔽物理差异和细节、符合标准的数据通信接口和服务接口。主要包括分区操作系统的常规接口、分区操作系统多核接口、分区系统调用接口、操作系统适配软件以及 IO 服务软件及其接口。

3.2.1 分区系统调用接口

(1) 虚拟机管理接口

虚拟化中间件软件可以响应分区层的虚拟机管理系统调用请求，该接口库作为嵌入到分区操作系统的组件，提供了一套以虚拟机为颗粒度的控制管理接口。这些接口可供应用调用，并实现以分区为单位的重构、状态管理等功能。

(2) 调度管理接口

虚拟化中间件软件可以响应分区层的调度管理系统调用请求，该接口库作为嵌入到分区操作系统的组件，提供了对当前处理器所有物理核时间调度配置进行管理的服务。调度管理接口支持获取指定处理器核上正在执行的调度配置，支持切换指定处理器核上的调度配置。

(3) 处理器资源管理接口

虚拟化中间件软件可以响应分区层的资源管理系统调用请求，该接口库作为嵌入到分区操作系统的组件，提供了对当前处理器上所有分区可用可配置的资源进行管理的服务。

3.2.2 IO 服务设计

IO 服务软件运行于分区操作系统中, 为应用提供屏蔽物理设备差异并基于消息的通用通信组件服

务, 该软件将外部 IO 设备驱动进行抽象, 并向上提供符合参考架构标准的 IO 层接口。如图 8 所示。

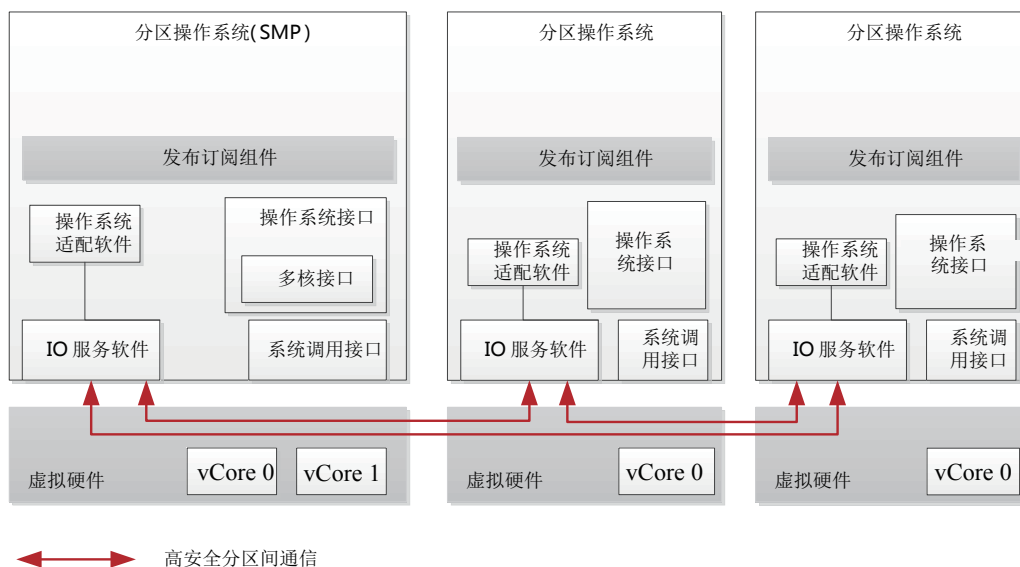


图 8 IO 服务框架

IO 服务软件具有以下功能: (1) 提供基于标准适配层的通信控制器驱动程序的挂接, 由其完成底层数据通信的收发控制; (2) 支持的数据接口和通信总线包括 FC 总线、串行总线、共享内存 (SHM: Share Memory)、I2C、以太网、FC 总线、PCIe 总线和 RapidIO 总线; (3) 支持消息处理流程的查看; (4) 支持基于共享地址空间访问的底层数据通信接口; (5) 符合 FACE IOS 层规范标准^[5]。

3.3 多核共享资源访问时间确定性评估

在航空电子领域, 尤其是涉及民用高安全的应用场景, 国内多核处理器平台的使用仍然保持较为谨慎的态度。根据 2016 年推出的 CAST-32A^[6] 指导文件, 本论文在多核平台的应用方面考虑几下方面:

(1) 确定影响系统架构设计的多核之间可能产生干扰的因素;

(2) 识别多核之间资源共享, 以及验证共享资源对于系统确定性的影响手段;

(3) 确定 OS、应用以及多核处理器, 对于不同应用场景的可能配置组合;

(4) 识别对于确定性有影响的关键配置, 并记录在案, 为将来满足此目标提供输入;

(5) 识别多核确定性影响因素, 并给出一定的应对方案或者测试输入;

(6) 确定不同核、多个分区共同运行时对于系统的配置方案, 为下一步测试提供输入;

(7) 识别共享资源确定是否有数据、控制耦合, 以及出现的场景。

多核处理器可以同时执行多个软件应用程序, 因为它们有两个或多个处理核心, 每个核心可以承载和执行不同的软件应用程序。因此, 多个应用程序可能试图同时访问多核处理器的同一共享资源 (例如内存、Cache 和外部接口), 从而引起对这些资源的竞争。大多数多核处理器都有内部机制, 例如“互连”来处理仲裁对多核处理器资源的竞争, 但是应用程序之间对共享资源的争用通常会导致对资源的访问延迟。这些延迟是应用程序之间时间干扰的一种形式, 这可能导致应用程序执行的时间比单独执行时长得多。因此, 对于开发基于航空电子计算的安全关键型设备来说, 仍然是一个重大挑战。在安全关键型系统中, 多核平台的优势必须大于风险。因此评估验证环境的建立就显得尤为重要。具体的影响有内核对软件安全性的影响和共享内存对软件安全性的影响。

结合前文论述, 本论文设计了一套通用多核测试验证评估方法, 具体测试评估内容如表 1 所示。

表 1 多核测试评估项

测试项	测试内容
不同 Cache 情形下内存访问安全性评估	不同 Cache 组合的内存性能测试
	不同 Cache 组合的内存时延测试
	不同 Cache 模式的内存性能测试
	多核共享内存的基本功能测试
核间通信安全性评估	多核内存读写功能测试
	非 0 核启动功能
	不同核内存读写功能
	测试 IPI 时延
外围接口通信安全性评估	测试复杂条件下 IPI 时延
	测试时钟中断时延
	测试 PCIe 中断时延
	测试 PCIe 传输性能
	测试不同 Cache 模式下 PCIe 传输性能

以共享内存测试为例,如图 9 所示。当共享 L2 Cache 时,测试核 0 内存读写受到其他处理器核的干扰,随着同样运行内存读写程序的干扰核数量的增加,核 0 上的单位内存读写时间以约百分之一到千分之一的量级增长。而对 L2 Cache 按核分区会降低内存读写性能 2%~3%。后者的这种下降是确定不变的,也就是说在任何应用场景保持不变,而前者会由于场景不同,产生不确定数量的性能下降。

由此可以看出,验证测试可以对多核平台的应用、软件架构以及系统架构产生指导核参考。

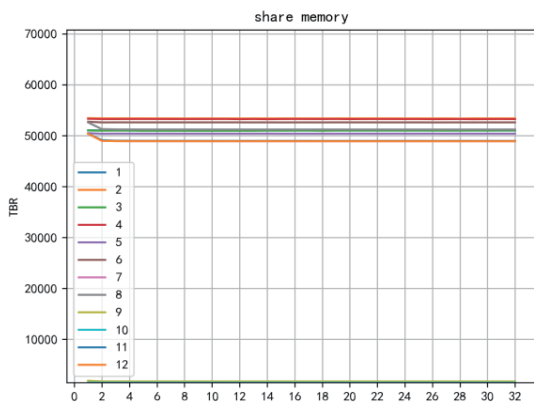


图 9 共享内存

4 结论

本文针对机载嵌入式设备和多核处理器平台,利用当前工业领域的嵌入式虚拟化技术,设计和构建了一套安全、可靠和实时的机载多核虚拟化解方案,能够满足航空电子系统在高集成度和高安全共存的情况下对基础软件的更高要求,为机载通用计算平台提供了操作系统设计参考。

参 考 文 献

- [1] 沈晴霓,杜虹,卿斯汉.虚拟可信平台层次化安全体系结构设计[J].北京工业大学学报,2010,(5):605-610.
- [2] Arm Limited. Architecture reference manual Armv8, for Armv8-a architecture profile[M]. 2019, (7):2268-2276.
- [3] Aeronautical Radio, Inc. Avionics application software standard interface[M]. 2003-10.
- [4] 中央军委装备发展部.航空电子应用软件接口要求, GJB 5357-2005[S]. 中央军委装备发展部, 2005.
- [5] Open Group. Future airborne capability environment (FACE™), Edition 2.1[M]. Open Group, 2014.
- [6] Certification Authorities Software Team. Certification authorities software team position paper CAST-32A: multicore processors[M]. 2016.