文章编号:1671-4598(2019)11-0206-04 DOI:10.16526/j.cnki.11—4762/tp.2019.11.045 中图分类号:V243, V247.1 文献标识码:A

多核虚拟化分区技术在航空电子系统中的应用

潘 皓
(中国西南电子技术研究所，成都 610036)

摘要：针对当前航空电子系统多核处理平台资源利用率低，用户数量可扩展性不足等问题，提出并实现了一种适用于机载应用的多核分区处理方案，将多核处理器与虚拟化分区技术相结合，解决了用户数量受限于处理器内核数目问题，达到资源利用率最大化目的；实验结果表明，该方法可在同一模块上部署64个以上功能应用，支持多用户协同开发；与传统非对称多处理架构相比，硬件体积减少80%以上，重量减轻75%以上，功耗下降65%以上；提高了系统集成度，实现功能应用的时间、空间和资源访问隔离，提升了系统安全性和可靠性。

关键词：综合模块化航空电子；对称多处理；非对称多处理；并行处理；虚拟化；分区调度

Multi—core Virtualization and Partitioning for Avionics System

Pan Hao
(Southwest China Institute of Electronic Technology, Chengdu 610036, China)

Abstract: The resource utilization of multi—core processing platform for the current avionics system is low. Moreover, the number of system users is limited to cores. Multicore partition method for airborne applications is proposed and implemented, adopting the combination of virtualization and partitioning technology. The limitation of user numbers is resolved, to maximize resource utilization. Experimental results show that the method can be deployed more than 64 functional modules, moreover, multi—user cooperative development is supported; Compared to traditional asymmetric multiprocessing architecture, the reduction of hardware volume is more than 80%, the weight of more than 75%, and the power dissipation is more than 65%. The degree of system integration is improved, and the functionality of the application of time, space and resource access segregation, so as to achieve the goal of improving system security and reliability.

Keywords: integrated modular avionics (IMA); symmetric multiprocessing (SMP); asymmetric multiprocessing (AMP); parallel processing; virtualization; partition scheduling

0 引言

航空电子系统的发展经历了分立式、联合式、综合化和高度综合化阶段。以F—35为代表的第四代航空电子系统，采用综合模块化航空电子（Integrated Modular Avionics，IMA）系统架构，并将综合化的范围从综合数据处理扩展到射频前端，实现了从天线孔径、射频前端信号处理和信息处理层面的传感器高度综合[1-2]。未来，随着数字化不断向射频前端移动，将在更大范围实现资源综合。下一代航空电子系统需要高性能、标准化、通用化的模块，使各种功能线程尽可能复用硬件，在同一套硬件资源上实现多传感器信息融合[3]。

IMA架构降低了系统体积、功耗和重量，有效实现了硬件资源共享，减少了系统模块数量，从而降低了成本、提升了模块的标准化和通用化程度。传统IMA架构采用单核处理器，通过航空电子应用软件接口（APEX，Application Executive)[4]，实现操作系统和应用程序隔离；此外，通过时间、空间分区确保了不同功能应用安全隔离。针对通用处理资源，目前仍采用多个处理器物理整合的方式进行资源综合，以提升并行处理能力[5]。一方面，受制于尺寸、功耗、重量的限制，处理器数量难以继续增加；另一方面，多核处理器系统往往只实现了单核处理，并没有将其优势充分发挥出来。

主流多核处理架构主要包括对称多处理（SMP，Symmetric Multiprocessing）和非对称多处理（AMP，Asymmetric Multiprocessing)。传统的SMP通过共享同一操作系统和硬件资源实现并行处理，如图1所示。此架构组成简单，操作易于实现，但由于未实现对底层硬件资源访问隔离，各个内核耦合度高，一旦某个进程故障会导致与其它进程关联故障，出现处理器工作异常；传统AMP架构如图2所示，通常有多个操作系统在不同内核上执行。AMP架构下各内核相对独立，但由于多个内核需共享存储器和I/O等资源，要重点解决内核间通信和互斥问题，复杂性较高；此外，所有操作系统的协同工作，对驻留在不同操作系统的应用协同开发难度较大[6]。

机载多核处理平台需重点解决软件的确定性、安全隔离、故障定位隔离等问题[7]。2016，FAA发布指导意见书CAST—32A，提出了针对多核处理器的航空电子设备的安全性指导规范[8]，CAST—32A从硬件、操作系统、平台软件、应用软件和系统集成等方面提出了开发过程中需遵循的准则，从而奠定了满足DO—178C安全标准的多核航空

收稿日期:2019-05-06； 修回日期:2019-05-28。

作者简介:潘 皓(1983-)，男，云南富源人，工程师，硕士研究生，主要从事航空电子技术方向的研究。

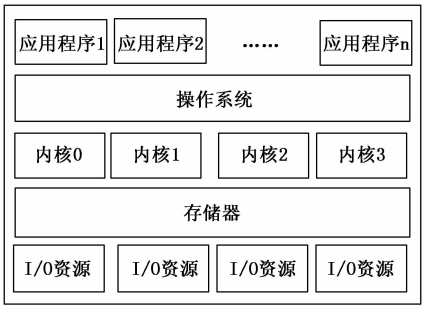

图 1　传统 SMP 架构示意图

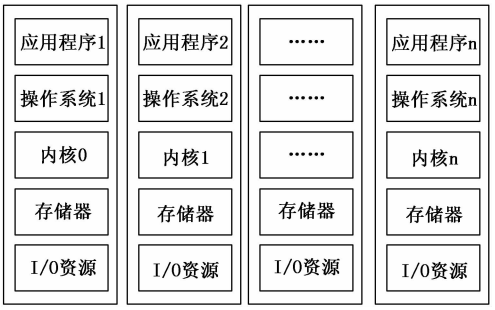

图 2　传统 AMP 架构示意图

电子系统的基础[9-10]。

本文研究了现有多核处理技术应用的不足，提出了一种适用于机载应用的多核虚拟化（virtualization）分区应用方法，将传统的多核硬件平台与虚拟化分区技术相结合，既在特定核上保留了传统基于时间分区的应用调度，又在其他内核上扩展了分区应用，实现多个分区严格隔离和并行处理，可满足多用户协同开发的需求。该方法增强了系统集成度，降低了系统功耗，提高了航空电子系统的可靠性和安全性。

1　多核分区处理系统设计

1.1　需求分析

航空电子产品的研制需满足对可靠性、安全性、测试性、维修性、保障性、环境适应性的要求[11]，此外，还需考虑适航认证要求。多核处理平台的设计应考虑一下要素：

（1）功能性能要求。系统开发者需分析产品需求，评估处理器指令执行速率、运算能力、工作频率，满足系统数据处理能力需求；此外，需综合考虑硬件平台对外通信接口的类型、工作模式及速率等指标，满足接口控制能力需求；最后，还需从平台驻留软件功能的角度，综合考虑处理器内核/线程数量，处理器资源使用率应留有余量，以便于功能扩展，处理器资源使用率一般不超过 70%；

（2）虚拟化支持。虚拟化技术是多核分区处理系统中的核心技术，虚拟化技术可实现对处理器内核、内存、I/O 设备等资源进行分组，得到不同资源分区，每一个资源分区相当于一个虚拟机（VM，Virtual Machine）。各虚拟机由位于硬件与操作系统之间抽象的软件层统一管理，称为虚拟机管理器（Hypervisor）。每一个虚拟机都支持一个客户端操作系统（Guest OS），各分区能够共享某些硬件资源，并提供完善的保护和隔离，保证多核处理环境下的实时性和安全性；

（3）开发工具支持。在系统集成时，存在多用户软件驻留在同一硬件平台上，共享硬件资源。因此，用户程序需实现独立开发和测试，最终由集成商负责整合和测试验证。系统出现故障时，应提供有效的故障维护和检测工具，便于问题定位和故障隔离。当前，多核硬件相对成熟，但基于多核的开发工具和系统软件比较欠缺；

（4）产品全生命周期供货能力。航空产品具有工作环境恶劣，服役时间长（通常为几十年）等特点，系统设计时应考虑供应商对产品全生命周期的保障能力，确保持续供货和产品维护。

1.2　虚拟化分区处理架构

在多核硬件处理平台上，采用虚拟化分区处理技术，实现机载平台上若干个相互独立的不同用户功能模块，为每个功能模块单独分配一个独立的分区，功能模块的应用程序在这个单独的虚拟分区中运行。基于虚拟分区的多核并行处理架构如图 3 所示。

多核虚拟分区处理架构包含 4 个层次，自底向上分别为硬件平台层、核心操作系统层、分区操作系统层和应用软件层，4 个层次相互独立。各层次功能说明如下：

（1）硬件平台层。包括物理实体的多核处理器、存储器以及外部接口资源，这些硬件资源构成一个典型的嵌入式系统。多核处理器包含其内部的若干个内核和实现指令执行的运算资源；存储资源为处理器内核的运算提供指令

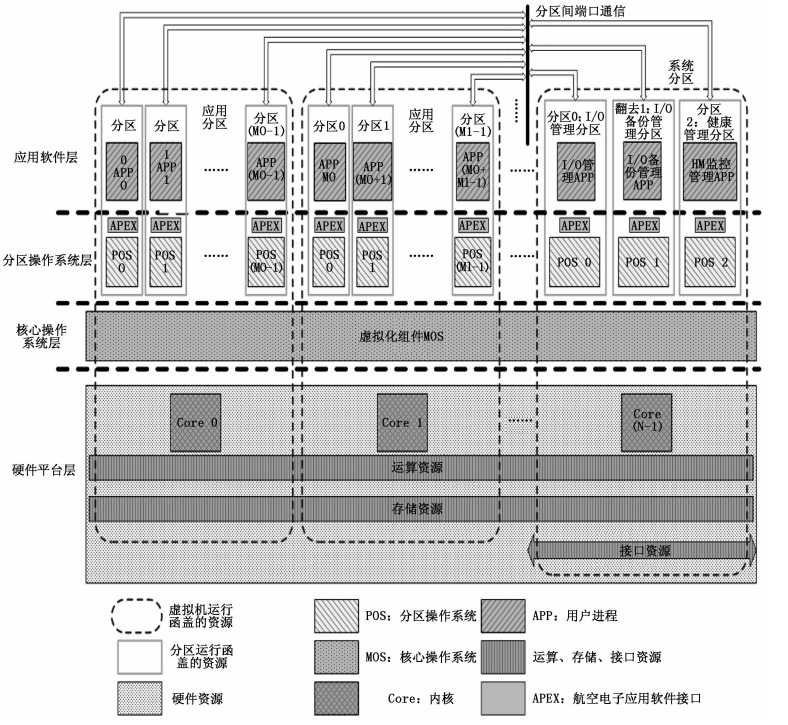

图 3　虚拟化分区处理架构示意图

和数据的存储空间，外部 I/O 资源为多核处理器提供与外部设备进行数据交互的通道。

（2）核心操作系统层。核心操作系统包含运行在多核处理器上的核心操作系统（MOS，module OS）和上层分区操作系统（POS，partitioned OS），MOS 中运行系统监管软件，加载所有虚拟机客户端，同时为虚拟机分配处理器、存储器、I/O 等资源。虚拟机具有系统监管功能，提供分区运行的环境，管理同一个内核上的分区调度，负责分区间通信，通过核心操作系统的管理对底层运算资源、存储资源和接口资源等硬件进行操作和控制。

（3）分区操作系统层。分区操作系统包含运行在虚拟机上的上层 POS 和提供给对应用软件层的若干个应用程序的 API（Application Programming Interface）。分区操作系统管理各自对应的内部资源和分区内多任务调度，并向应用程序提供服务。

（4）应用软件层。应用软件层可分为系统分区（System Partition）和应用分区（Application Partition）。应用软件层包含所有用户功能模块的若干个分区应用程序和接口管理程序、接口备份管理程序和健康管理程序，每个分区应用程序通过端口（Port）与接口管理程序、接口备份管理程序和健康管理应用程序进行通信。

2 分区处理机制

多核处理器硬件平台通过核心操作系统连接分区操作系统和运行在相互独立的若干个分区之上的用户应用程序；在多用户共享同一硬件平台的基础上，核心操作系统运行虚拟机，并在虚拟机上运行分别对应用户分区和 3 个系统分区操作系统 POS，应用分区通过分区间端口通信的方式与 I/O 管理分区交互，用户使用共享接口完成对各分区的独立访问。

2.1 分区规划

（1）功能应用分区。功能应用分区可同时实现机载平台上若干个相互独立的不同用户功能模块，为每个功能模块单独分配一个独立的分区，功能模块的应用程序在这个单独的虚拟分区中运行。从功能实现的角度，综合考虑功能的性能要求、占用的硬件资源等因素，把系统功能划分成若干个子功能，要求各子功能相对独立，把一个或多个子功能划分为一个分区，最终确定分区数量以及各个分区的功能。

多核虚拟分区处理系统中彼此独立的分区数量为 M 个，且多核处理器的第 k 个内核上运行 M_k 个分区，每一个分区中运行一个应用程序，并且满足：

$$M=\sum_{k=1}^{N}M_k \tag{1}$$

其中，N 为每个处理内核可部署的分区数量，其值取决于应用程序的复杂度和实际硬件资源；第 k 个内核上的每个分区上分别运行分区操作系统为 POS0，POS1，……，POS（M_k-1）。

（2）系统分区。各个虚拟分区中的功能应用程序完全独立运行，由与分区操作系统相连的虚拟机进行管理，除了实现用户功能的分区以外，在其中一个内核的虚拟机上单独设置 2 个 I/O 管理分区和 1 个健康管理（HM，Health Monitor）分区，以此来提高多核嵌入式系统的可靠性和安全性。

I/O 管理分区分为接口管理分区、接口备份管理分区，其运行的分区操作系统和接口管理程序、接口备份管理程序专门用于对 I/O 资源进行控制管理。当其中 1 个 I/O 管理分区的管理进程出现异常时，另外 1 个 I/O 管理分区的管理进程仍然可以完成执行接口资源管理的任务。

HM 分区负责监控硬件、应用程序和操作系统的故障和失效，并且隔离故障防止失效蔓延。健康管理程序在进程、分区、模块 3 个层级提供警报检测、警报记录、警报响应的服务，进行健康监控。根据错误级别决定警报响应的操作：模块级别的响应包括复位和关机；分区级别的响应包括重新启动分区；进程级别的响应包括重新加载执行进程。

2.2 分区调度

分区在多核上的部署可分为分区间并行和分区内并行[12-14]。分区间并行是一个分区在一个或多个核上激活，每个分区都在对应核上运行。同一时刻所有分区同时运行在各自对应和核上，这种方式下多个分区间是严格意义上的并行；分区内并行即多个分区部署在同一个处理器内核，分区内任务在时间上并发运行。这种方式下，分区的调度由 MOS 按照预先规划好的调度表来进行周期性调度，当前分区被调度时，其对应的 POS 被激活，达到各分区时间隔离的目的。

2.3 多分区调试

在系统集成联试时，通常采用以太网口进行调试，需要同时访问同一个物理硬件网口，这种方式可通过 I/O 分区代理访问实现。如图 4 所示，若干个用户的终端计算机和一台公用多口交换机组成。每台计算机至少包含一个通用异步串口 UART，连接至多核处理器硬件平台。每台计算机至少包含一个以太网口，通过网线连接交换机来与共用网口连接。用户操作系统分区需要使用共用接口与由若干个用户的终端计算机和一台公用多口交换机组成的外部设备交互时，用户分区操作系统首先将数据发送至 I/O 管理分区操作系统，再由 I/O 管理分区调用设备驱动将数据转发至外部交换设备，由交换设备分发至各用户的终端中；同理，当外部终端访问用户分区时，外部终端会统一访问 I/O 管理分区，再由 I/O 管理分区根据数据传输协议对数据解析，转发至目的用户分区。

多用户协同开发时，可通过 UART 串口向其用户分区操作系统输入调试命令。用户分区操作系统可通过串口超级终端的通用异步收发器 UART 向用户发送命令反馈信息。在接受用户输入的程序加载命令后，用户分区操作系统会向 I/O 管理分区发起发送请求。I/O 管理分区操作系统通过 FTP 加载的方式，通过网口获得用户终端的程序，然后加载至用户分区的内存中，完成程序加载。之后用户即可进行在线调试。

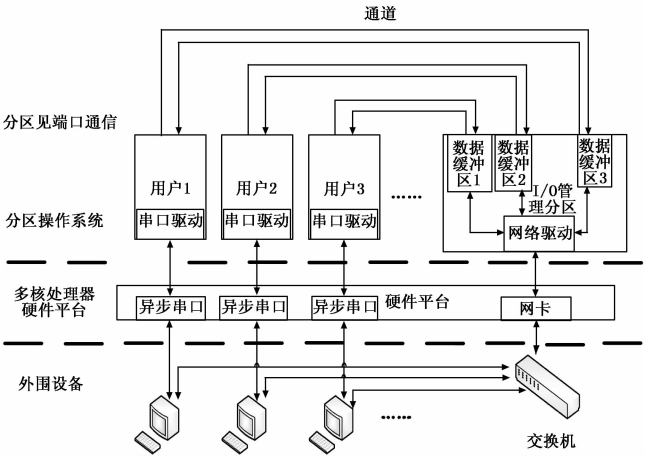

图 4　采用 I/O 分区实现多用户协同开发示意图

3　测试验证分析

根据本文提出的方法，构建了基于 NXP 公司的 T2080 芯片多核硬件处理平台。处理器为 4 核 8 线程，单核最高工作频率为 1.8GHz，系统时钟采用 66MHz，外围 I/O 接口主要包括 Local Bus、SRIO、I^2C、网口及串口，满足综合化航空电子系统对缩合硬件处理平台的要求。

该平台运行 VxWorks 653 3.1，在其上建立 64 个分区进行调度。其中每个物理核（Core）上分配 16 个分区，Core0 上部署了编号 1～16 的 POS，Core1 上部署了编号 17～32 POS，Core2 上部署了编号为 33～48 的 POS，Core 3 上布置了编号 49～64 的 POS。每个 POS 分配了 16M 的内存空间。

64 个分区应用将各自的打印信息通过串口循环输出。其中，前 32 个分区通过 SecureCRT 工具将打印信息通过超级终端显示；后 32 个分区通过 AMIO Console 工具，分成 32 个用户窗口，将信息回显至各自的串口窗口中。分区运行结果如图 5 所示。

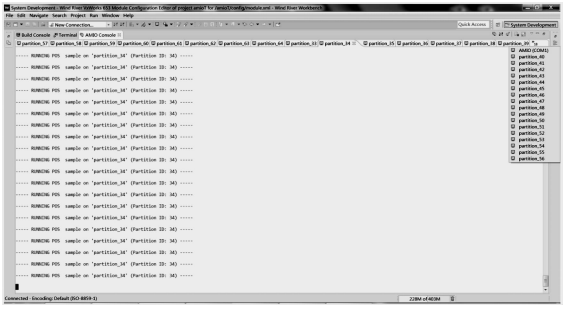

图 5　分区运行结果

相比传统单核的 IMA 平台，该平台将传统 4 个模块的功能合并为一个模块，进一步提升了综合化程度；与传统 AMP 架构相比，生产交付总成本可降低 50%以上，样机体积减少 80%以上，重量减轻 75%以上，功耗下降约 65%以上，用户数量由 4 个扩展至 64 个以上，具有轻小型化、低功耗的特点。64 个分区独立运行，并通过共享串口和以太网口，对同一核上的不同分区或不同核上的分区调试，实现了多用户协同开发。

4　结语

本文提出并实现了一种适用于机载应用的多核分区方案，采用基于多核并行处理和虚拟化技术相结合的系统管理技术，解决了处理器内核数目对用户个数限制的问题，达到了处理资源利用率最大化的目的。该方法可实现功能应用的时间、空间和资源访问隔离，避免多业务间相互影响引起失效蔓延，从而达到提升系统安全性及可靠性的目的。同时，在基于 T2080 多核硬件处理平台下实现了虚拟化分区技术，该平台可替代多个常规的单核处理的模块，减低了生产交付成本，提升了系统的轻小型化水平。采用多核虚拟化分区技术可提升航电系统的集成度，克服现有技术不便于多核调试问题，提高系统联试效率。

参考文献：

[1] 杨军祥，杨　涛，李成文，等. 综合模块化航空电子核心系统技术研究 [J]. 航空计算技术，2017，47 (3)：105－111.

[2] 潘云嵩. DIMA 航电系统资源优化配置研究与实现 [D]. 南京：南京航空航天大学，2017.

[3] 张占芳，王经典，王嘉良. 机载核心处理系统通用化平台研究 [J]. 航空电子技术，2017，48 (4)：7－10.

[4] ARINC Specification 653：Avionics Application Software Standard Interface，Part 1－Required Services [S]. USA：AEEC，2005.

[5] 秦　跌，史晓楠，巨新刚. 多核处理器核间的通信研究与实现 [J]. 现代电子技术，2016，39 (16)：83－87.

[6] 王继刚，刘韫晖. 基于 BMP 架构的多核差异化运行技术研究 [J]. 计算机工程与应用，2019 (7)：66－70. http://kns.cnki.net/kcms/detail/11.2127.TP.20181218.1035.006.html.

[7] 陈　刚，关　楠，吕鸣松，等. 实时多核嵌入式系统研究综述 [J]. 软件学报，2018，29 (7)：2152－2176.

[8] Certification Authorities Software Team (CAST) Position Paper CAST－32A，Multi－core Processors [S]，USA：Federal Aviation Administration，2016.

[9] RTCA/DO－178C，Software Considerations in Airborne Systems and Equipment Certification [S]，USA：RTCA，Inc，2012.

[10] David Radack，Harold G. Tiedeman，Paul Parkinson，Civil Certification of Multi－core Processing Systems in Commercial Avionics [R]. USA：Rockwell Collins，2018.

[11] Lofwenmark A，Nadjmtehrani S. Fault and timing analysis in critical multi－core systems：A survey with an avionics perspective [J]. Journal of Systems Architecture，2018，87 (6)：1－11.

[12] Chronaki K，Rico A，Casas M，et al. Task Scheduling Techniques for Asymmetric Multi－Core Systems [J]. IEEE Transactions on Parallel and Distributed Systems，2017，28 (7)：2074－2087.

[13] 杨骏峰，李　峭. 综合模块化航空电子多约束分区调度方法 [J]. 电子测量技术，2017，40 (6)：152－155.

[14] 陈　平，魏　峰，李蜀瑜. ARINC653 调度算法研究 [J]. 现代电子技术，2015，38 (12)：29－32.