推动关键基础设施向软件定义平台迁移

PaulParkinson

航空航天领域现场工程总监，EMEA

WNDRVR

执行摘要

关键基础设施中使用的嵌入式系统目前正在经历一场巨大的变革。历史上，这些系统具有不同程度的网络连接性，执行固定的功能，并且可能在现场手动升级，作为长服役周期的一部分。如今，无处不在的网络连接加速了智能边缘嵌入式系统的创新。这推动了对增强应用功能的需求，这些功能不仅执行传统的自动化和控制功能，还增加了更高的智能性。

多个行业对设备支持更高智能的需求日益增长，以实现从自动化系统向自主系统的过渡。这推动了对基于开放标准的软件定义架构的技术需求，以便将多个应用（包括具有不同安全等级和使用多种操作系统的应用）整合到通用计算平台上。这种方法支持应用迁移、可移植性和互操作性，避免了被锁定在专有架构中。

风河开物Hypervisor 通过提供支持基于开放标准的软件定义架构的灵活虚拟化平台，满足了这些共性需求。它基于经过验证的软件技术，能够满足航空航天、汽车、工业和医疗市场的安全认证要求。

目录

执行摘要 2
嵌入式系统从自动化向自主性的演变 3
推动嵌入式虚拟化平台融合的共同市场需求 3
关键基础设施嵌入式虚拟化的演变 4
支持数字化转型的开发工具 6
结论 7

嵌入式系统从自动化向自主性的演变

在过去十年中，嵌入式系统在性能、连接性和能力方面经历了持续的演变。历史上，在能力连续体的一端，一些嵌入式设备执行固定功能，并具有较长的服役寿命。它们可能很少进行系统升级以增加新功能或部署安全更新以应对最新的安全漏洞。没有网络连接的系统需依赖现场手动升级，这种操作不仅耗时且容易出错，其成本还会随设备规模扩大或物理接入难度增加而显著上升。

根据摩尔定律，处理器性能多年来显著提高，网络连接成本持续下降，导致边缘设备连接性大幅增加。这加速了创新，使得新的应用功能能够通过网络基础设施上的安全通信会话更快地部署到边缘设备。这一基础现在正在推动下一代智能设备的开发和部署，以及从自动化向自主化的过渡。

航空航天领域

在航空航天领域，航空电子设计出现了非常显著的趋势，从使用固定功能外场可更换单元（LRU）的分立式航电架构转向采用通用计算平台的集成模块化航电（IMA）架构，这些平台承载着不同安全等级的多个应用。这一转变在商业航空航天领域受到共同需求的推动，即显著降低航空电子系统的整体尺寸、重量和功耗（SWaP）要求，特别是随着支持新航空电子功能的分立式LRU数量的增加。IMA的采用显著减轻了重量，使飞机能够以更少的燃料负载或更多的乘客或有效载荷飞行。基于标准的IMA软件架构的使用也促进了互操作性和集成，对商业项目产生了显著的积极影响，降低了设计锁定的风险，推动了创新，并降低了全生命周期成本。

汽车领域

汽车领域面临着自身的一系列挑战，由于市场竞争激烈且创新速度加快。这受到市场对智能座舱系统（IVI）、OTA软件迭代、高级驾驶辅助系统（ADAS）以及最近的自动驾驶目标的需求推动。这导致过去十年中汽车中使用的处理器数量大幅增加。自动驾驶系统的部署将需要进一步显著增加车载计算能力，包括通用GPU（GPGPU），以支持人工智能（AI）和机器学习（ML）应用。这些汽车系统以及相关的电缆增加了车辆的重量，对车辆性能、燃油经济性、二氧化碳排放和成本产生了负面影响（正如航空航天市场一样）。因此，主要汽车制造商现在使用通用嵌入式计算平台来整合应用并减少SWaP。

工业领域

在工业领域，企业正在拥抱数字化转型，利用工业物联网（IIoT）和工业4.0来应对业务挑战并保持竞争力。智能工厂、能源系统和其他关键基础设施正在采用实时监控能力和分析来测量运营效率，并能够使用分析和预测性维护来最大限度地减少因系统故障导致的停机时间。这种数字化转型是由于在实时控制系统中增加了网络支持的监控能力。企业现在希望通过在通用计算平台上进行工作负载整合和远程升级能力来实现进一步的效率提升。

医疗领域

医疗领域目前正在经历一场医疗保健革命，新技术正在推动先进的成像系统、手术机器人和其他关键医疗设备的发展。患者安全至关重要，因此这些系统必须安全、可靠地运行。当前的网络安全法规意味着医疗设备制造商必须能够轻松地通过空中更新其系统；手动更新由于设备数量庞大且安装基础分布广泛，将不具备成本效益。

推动嵌入式虚拟化平台融合的共同市场需求

尽管每个垂直市场都面临独特的挑战和需求，但在抽象层面上，嵌入式软件平台现在需要类似甚至共同的基本能力。特别是，所有垂直市场都需要一个安全、可靠且具备以下高级需求的平台：

- **混合承载：**整合平台的共同需求是承载关键的实时控制应用和通用应用。它必须隔离安全组件并减少它们对平台其他部分的依赖，以确保整体平台的安全认证成本保持在可承受范围内。
- **开放标准：**各行业越来越需要采用开放标准，以实现应用迁移和可移植性，促进竞争，并防止设计锁定。商业航空航天领域已采用ARINC 653标准用于开放航空电子架构，并使用了商业开放标准（ARINC 653，POSIX®）。汽车领域正在采用自适应AUTOSAR（汽车开放系统架构），以促进商用货架（COTS）硬件和软件的更广泛采用，并提供灵活且可扩展的框架。在工业领域，开放过程自动化论坛（OPAF）致力于开发基于开放标准的安全、可互操作的过程控制架构。
- **重用和可扩展性：**知识产权和先前开发（甚至已通过认证的）的应用应可在新的嵌入式计算平台上重用。这包括依托虚拟化技术利用多核处理器架构提供的性能和可扩展性，屏蔽底层硬件架构的复杂性，实现开发者于硬件细节的解耦。它还要求在平台上部署新应用以提供额外功能。

- **安全性：**在整个设备的操作和生命周期中，确保安全性的需求日益增长。这包括设计、生产、调试、部署和运维，直到生命周期结束时的退役。在部署期间，设备需要在不同阶段安全运行：它需要执行安全初始化以验证部署软件的完整性，确保其未被损坏或篡改；它需要在操作期间提供安全通信，并具备抵御网络攻击的能力；它需要安全地存储处理中的敏感数据和静态数据，包括在断电时。

- **支持现代开发方法：**每个垂直行业的制造商都面临着在更短的时间内交付高质量软件的压力。许多公司现在使用敏捷开发流程来加速变更，同时通过自动化采用持续集成和持续交付方法，显著缩短集成和交付时间，作为DevOps文化的一部分，以提高响应能力。

关键基础设施嵌入式虚拟化的演变

在过去十年中，处理器技术的进步对实际应用架构产生了重大影响；特别是，处理器硬件虚拟化支持的技术演进和产业化成熟使得企业和云计算平台能够高效且大规模地承载虚拟化应用。硬件虚拟化支持也已成功部署在嵌入式系统中，特别是在使用风河开物RTOS 653多核版本的安全关键航电系统中，多个虚拟化应用可以在通用航空电子计算平台上承载。硬件虚拟化、多核处理器架构和基于开放标准的软件定义架构在多个领域的融合，为关键基础设施提供了一个通用的嵌入式虚拟化平台（参见图1）。

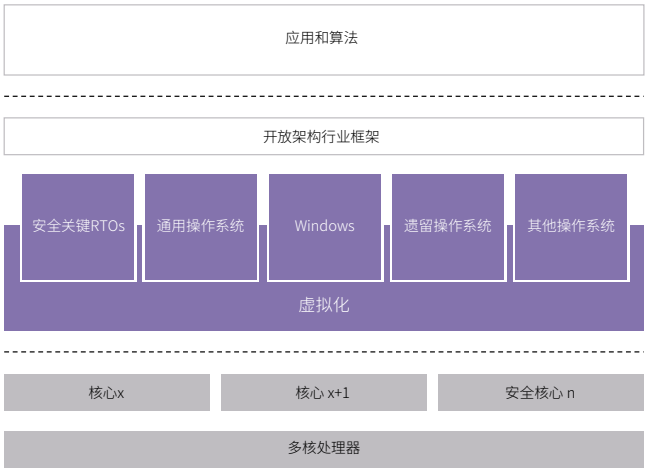

图1. 通用计算平台的软件定义架构

风河通过数十年的经验和在功能安全、信息安全和嵌入式虚拟机管理程序软件技术方面的持续行业领导地位，开发了风河开物Hypervisor，满足了这一市场需求。

虚拟机管理程序和虚拟机

风河开物Hypervisor使用类型I虚拟机管理程序（也称为裸机虚拟机管理程序），如图2所示，它直接在处理器上运行；通过直接中断提供接近本地的实时性能；并提供适合功能安全认证的可扩展性、确定性和小尺寸。这种方法与类型II虚拟机管理程序形成对比，后者专注于从底层物理环境中抽象出来，并提供不适合硬实时应用的尽力而为性能。此外，其尺寸过大，无法进行功能安全认证。类型I虚拟机管理程序方法在多核处理器架构上提供了高效的可扩展性，因为它可以扩展到比传统单片和微内核架构更多的核心。

虚拟机管理程序使用处理器的专用虚拟机管理程序特权级别和完整的硬件虚拟化支持，使32位和64位Guest OS及相关应用能够在虚拟化环境（通常称为虚拟机）中以单独的特权级别运行。这包括风河开物RTOS、风河Linux、Microsoft® Windows®（64位）、Android、裸机以及包括其他Linux发行版在内的第三方操作系统。

虚拟机管理程序还使用处理器的内存管理单元（MMU）来强制执行各个虚拟机的隔离。这防止了Guest OS及其相关应用对另一个虚拟机或特权系统资源进行任何未经授权的编程I/O访问；任何尝试的未经授权访问都会报告给虚拟机管理程序。

许多现代处理器还提供直接内存访问（DMA）引擎，以在源和目标内存位置之间高效传输数据块，例如在系统内存和外部I/O设备（如网络接口）之间。虚拟机管理程序还使用另一个处理器硬件资源，即IOMMU，以确保Guest OS和应用仅在授权的源和目标地址之间执行DMA传输。这意味着风河开物Hypervisor能够承载包含使用未知来源的第三方设备驱动程序的Guest OS的虚拟机，因为IOMMU将检测并防止未经授权的DMA访问。这种隔离能力在功能安全和信息安全方面提供了好处，并支持将多个应用整合到通用嵌入式处理平台上。

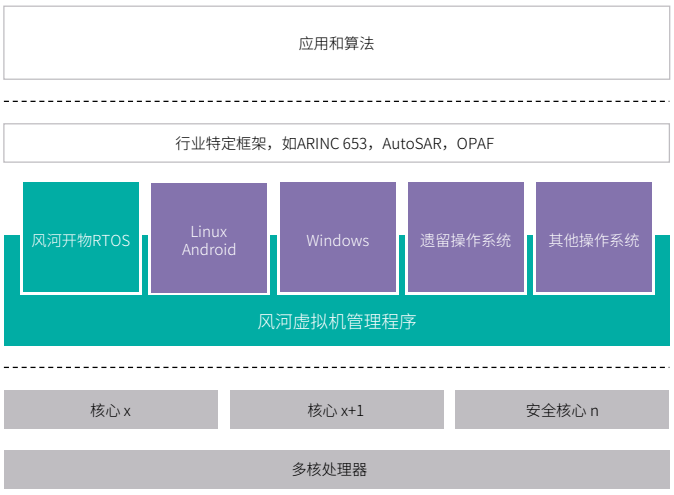

图2. 风河开物Hypervisor架构

这些硬件虚拟化和隔离能力使风河开物Hypervisor能够承载实时和功能安全的风河开物RTOS应用，以及嵌入式Linux应用和通用操作系统，如Microsoft Windows和其他第三方及遗留操作系统。这使得先前开发的软件能够重新托管，保留现有知识产权的投资，并作为现有部署系统和下一代系统之间的资产桥梁，从而降低在役系统升级时的技术风险。

分区间通信

整合平台还需要支持各个虚拟机之间的通信，风河开物Hypervisor提供了多种不同的分区间通信方法：

- 共享内存和虚拟网络接口控制器（VNIC）支持风河开物 RTOS、Linux和Windows以及其他第三方Guest OS之间的通信。
- 安全IPC是一种受控的共享内存实现，支持多个Guest OS（包括风河开物RTOS和风河Linux）之间的通信，可能运行在不同安全级别。

构建时配置

风河开物Hypervisor建立在风河功能安全和信息安全平台的能力之上，这些平台在多个行业的不同认证标准下拥有世界级的认证记录。风河开物Hypervisor还通过支持更广泛的 Guest OS 环境，进一步发展了经过验证的代码库，以支持更广泛的使用案例。

构建时配置旨在系统配置和构建阶段 为 Guest OS 环境分配系统资源，并使这些资源在运行时以可预测和确定性的方式使用，这对于功能安全系统至关重要。前面描述的分区意味着此配置可以支持在不同分区中运行的多个安全关键应用，或包含不同完整性级别应用的混合承载系统。风河在风河开物RTOS 653中开创的独立构建链接和加载（IBLL）方法使应用能够独立配置、构建、链接和加载。这使得单个应用能够通过平台生命周期独立更新，而不会影响其他组件，从而实现增量认证，并显著降低平台的全生命周期成本。

调度

风河开物Hypervisor还支持灵活的调度，以支持广泛的应用使用案例。时间分区调度器使用多个固定持续时间的时间槽的系统调度，定义各个Guest OS及其相关应用的执行时间。时间分区调度器可用于确保通用应用不会超出其分配的时间段，并影响在同一平台上承载的功能安全应用的执行（如图3所示）。

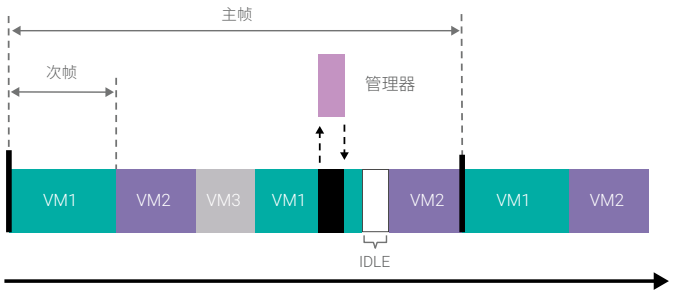

图3：帧调度

风河开物Hypervisor还允许同步各个核心的调度，使不同分区能够在不同核心上同时运行，并提供时间分区，以便包含虚拟机（VM）的分区不能从另一个虚拟机窃取执行时间（见图4）。

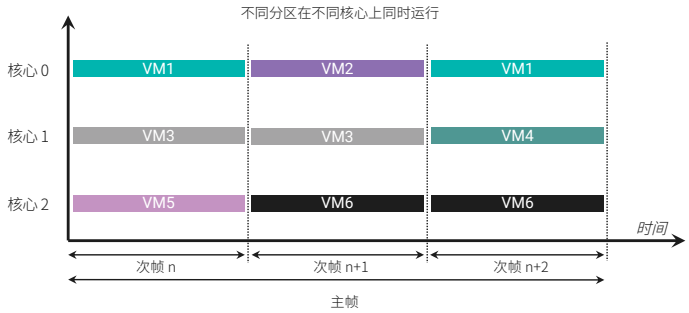

图4. 多核帧调度器

时间分区调度器还允许在系统配置和构建时定义多个调度，并通过可信的Guest OS使用专用的虚拟机管理程序调用（称为hypercall）实现从一个调度到另一个调度的转换。这种对多个调度的支持使得可以使用不同的操作模式，例如初始化模式、操作模式、维护和/或诊断模式。

时间分区调度模型广泛用于要求功能安全的航电系统（风河开物Hypervisor多核实现符合ARINC 653规范1），但这种方法同样适用于需要在同一计算平台上承载通用和功能安全应用的其他市场领域。

健康监控框架

包含多个异构虚拟机的系统需要能够监控、检测和从硬件故障、各个虚拟机内的Guest OS故障以及应用故障中恢复。这要求健康监控框架能够隔离故障并防止故障传播。尽管这些要求在概念上可能看起来简单，但它们实际上很复杂，需要一个复杂的系统级实现来提供平台的持续可用性。风河在开发用于功能安全关键IMA应用的ARINC 653健康监控（HM）框架方面拥有丰富的经验，并将这一专业知识应用于风河开物Hypervisor的健康监控框架开发。

HM框架处理的事件可以是需要关注的故障警报，也可以是提供可以处理或记录的通知消息。HM框架采用分层、表驱动的实现方式，使HM事件能够在应用级别、虚拟机级别或嵌入式平台级别处理（在航空航天领域，这些级别称为进程级别、分区级别和模块级别）。HM框架还允许HM事件在发生级别处理或传递到下一级别；例如，单个虚拟机内的故障、错误处理可以从虚拟机的Guest　OS路由到虚拟机管理程序。这种方法使系统集成商能够在系统配置时确定在发生特定错误时应采取的措施。HM框架还支持在虚拟机和嵌入式平台级别进行冷启动和热启动。这使得单个虚拟机能够在不干扰其他虚拟机的情况下重新启动。

支持数字化转型的开发工具

嵌入式虚拟化平台承诺了许多好处。为了实现这些承诺，需要复杂的开发工具集支持，以管理复杂的系统配置和异构运行环境下应用的构建和部署。

风河在开发集成开发环境、动态可视化工具和仿真平台方面拥有丰富的经验，适用于通用应用和功能安全应用。这一专业知识促成了最新的风河Workbench（见图5）开发环境，为风河开物Hypervisor提供了图形支持，用于系统定义和配置，包括将虚拟机分配到处理器核心以及定义调度。风河Workbench在后台持续验证系统配置，为开发人员提供反馈。它还自动化了许多构建和配置步骤，减轻了系统集成商和应用开发人员的负担（见图5）。

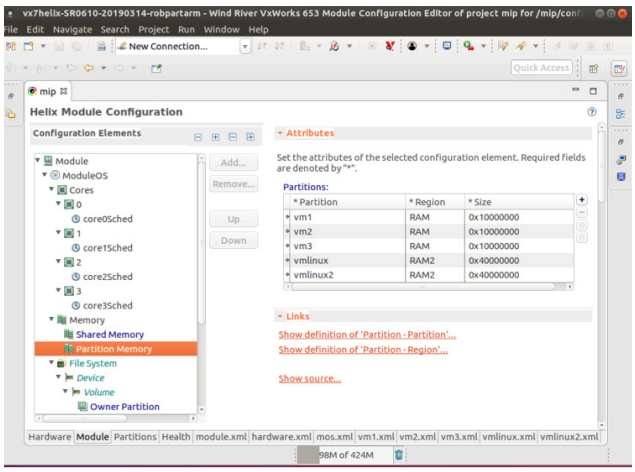

图5. 使用风河Workbench进行系统配置和应用开发

风河系统查看器还提供了系统的图形表示，使开发人员能够查看和理解系统事件之间的交互，例如中断、GuestOS原语、风河开物RTOS应用任务、POSIX线程或ARINC 653进程（见图6）。

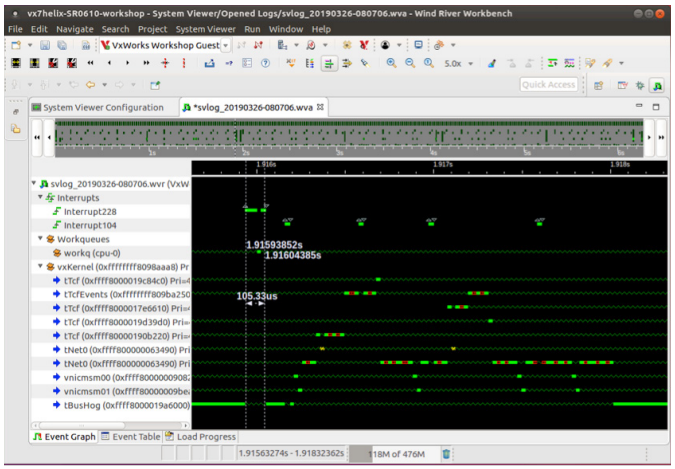

图6. 使用风河系统查看器进行动态可视化

风河开物Hypervisor还使用现代的Clang/LLVM编译器工具链。这提供了多个好处，包括支持最新的C和C++语言标准以及性能优势，如快速编译时间、低内存使用率和通过增加代码优化实现的更快执行速度。

应用可以在嵌入式目标平台上使用风河开物Hypervisor开发，也可以使用Wind River Simics®。Simics打破了硬件可用性的依赖，使虚拟原型设计能够在开发周期的早期进行，减少后期阶段的昂贵返工。风河Studio是首个用于开发任务关键智能边缘系统的云原生平台，其众多功能之一是能够在云中运行Simics容器。Simics还支持大规模并行运行许多测试用例，支持使用持续集成/持续交付（CI/CD）开发风河开物Hypervisor应用。

结论

传统嵌入式系统在功能、可维护性和技术老化方面面临重大挑战。未来系统在软件定义架构和开放标准支持方面有严格的要求。关键基础设施系统越来越需要满足各自垂直市场中的严格安全认证要求。

风河开物Hypervisor通过提供一个嵌入式虚拟化平台来应对这些挑战，该平台可以作为资产桥梁，使传统应用和先前开发的软件能够在现代、可扩展的平台上整合。它支持基于开放标准使用多种操作系统环境开发新应用。它还通过静态和动态配置选项提供灵活性，使广泛的使用案例能够在混合关键性环境中承载和部署，并使用现代开发方法和流程。

如需了解更多关于风河开物Hypervisor的信息，请访问www.windriver.com.cn/products/helix。

1 *风河开物Hypervisor认证版本中的帧调度器符合ARINC　653规范第1部分补充4：所需服务（大多数调度器服务）和ARINC　653规范第2部分补充3：扩展服务（多模块调度服务）。*

风河就在您身边

风河开物科技（上海）有限公司	地址：上海市黄浦区中山南一路768号博荟广场C座21楼03单元	电话：021-63585586
风河开物科技（上海）有限公司北京分公司	地址：北京市朝阳区霄云路38号现代汽车大厦19层1902室	电话：010-84777100
风河开物科技（上海）有限公司深圳分公司	地址：深圳市福田区车公庙天安数码时代大厦A座606室	电话：0755-25333408
风河开物科技（上海）有限公司成都分公司	地址：成都市高新区天府软件园D区7号楼1401-1404号	

关于风河更多内容请访问：https://www.windriver.com.cn　Email: inquiries-ap-china@windriver.com

官方微信