白皮书

Wind River® Hypervisor
和操作系统
Intel® 嵌入式计算
专用处理器

多核和虚拟化在工业与安全性相关领域的应用

多核和虚拟化为提升设备性能、降低设备成本铺平了道路，因为由此可以实现硬件集中化，并且使整个产品生命周期内的应用升级更加经济高效。

颠覆性的技术和趋势正在影响着嵌入式市场，同时也为工业领域的设备制造商带来了巨大的机遇，在产品和商业模式两个方面都获得全面的提升。如果能够借力于于以下技术和行业趋势，就意味着获得了巨大的竞争优势。

- **多核处理器**
- **虚拟化技术**
- **安全相关设备不断增加的复杂度**

多核处理器的成熟，不仅导致了近年来嵌入式市场的一次颠覆性变革，也带来了最大的商业机遇。最新的Intel®多核处理器在实现系统整体性能提升的同时，也提高了单个处理器内核每瓦特功耗所提供的性能。基于多核处理器的系统还能改善应用的可扩展性并保护软件投资，因为它允许用更多内核的处理器来替换原来的处理器，以便满足未来的需求。走向多核，这股潮流势不可挡，一个显著的实证就是，Intel®双核和四核处理器的出货了已经迅速地超过了单核处理器。

第二项技术是虚拟化，它实现了在同一物理硬件平台上同时运行多个虚拟机的能力，因为它可以对底层处理内核、内存和外设进行抽象。采用虚拟化技术可以在同一设备内同时运行多个操作系统环境，例如一个实时操作系统，例如风河VxWorks，再加上一个通用操作系统，例如风河Linux，如图1所示。借助于多核处理器和虚拟化所获得的高性能，可以对原先分别运行不同应用的多个独立设备做集中化，整合为一个设备。设备集中化将会有效地减少硬件数量，提升能源利用效率，从而降低设备的整体物料清单和运行费用。

虚拟化是由Hypervisor来实现的，它具有系统监管（supervisory）功能，能够保护操作环境，避免操作系统之间相互影响，并且提供了系统隔离措施，以便提升系统的可靠性和安全性。采用此项技术可以让每个应用的独立演进，降低了设备生命周期的成本投入。

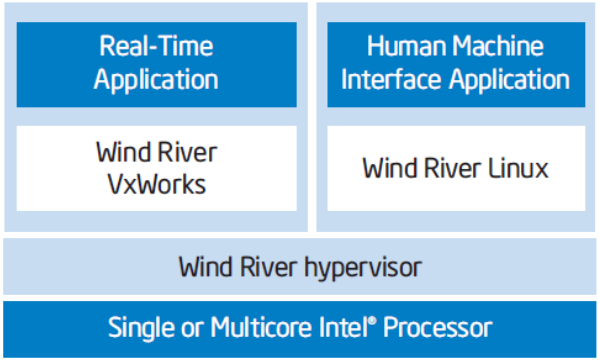

图1：采用虚拟化技术的系统

随着对新功能和法规遵从性方面的要求不断增加，**安全性相关架构**变得越来越复杂。推动复杂度增长的动力之一是工业设备与网络和系统的接口越来越多，例如Internet、top-floor和shop-floor等。因此，设备必须能够支持不同关键级别的各种类型应用软件（例如安全组件、协议栈等）。伴随着系统复杂度的增加，法规机构也在采取更严格的认证方法和流程来确保系统的安全性。多核和虚拟化相结合，能够帮助工业控制、流程自动化、能源和交通等行业的制造商保护他们的开发投资。这些技术能够使系统更安全地同时运行更多的程序，因此，可以在确保性能、安全性、可扩展性、认证性和可用性等要素的同时，逐渐完成对现有多核平台的升级。Intel多核处理器的性能已经得到增强，在对软件做最少变更的前提下，将控制、数据搜集、虚拟化和网络安全性等功能集中化到一个单板之上。此外，虚拟化层可以减少对硬件的直接依赖，从而保护软件投资。这使开发人员能够更轻松地迁移和升级到新的设备架构，同时更高效地管理好向商用现货型（COTS）技术的过渡。本文将进一步详述Intel和风河多核及虚拟化技术如何改变工业和安全性相关领域应用开发人员的工作方式，彻底避免软件的相互影响和来自外部的破坏。同样越来越重要的是法规方面的影响，包括安全相关的应用标准（如IEC 61508、CENELEC 50128、ISO 26262和IEC60880/62138等），以及能源、交通、自动化和工业控制领域的更多细分行业标准。

全面支持工业解决方案处理器

VxWorks、Wind River Linux和Wind River Hypervisor可以在大跨度的Intel系列处理器上运行，并且由一套开放标准工具集提供支持，为多核和多操作系统开发过程带来更高的效率。这些功能可以跨越覆盖工业控制设备的不同类型，呈现在如图2所示的“自动化金字塔”中的不

同层面。企业层（EP）支持运行混合应用软件的服务器和工作站，包括协同生产管理（CPM）、财务管理和资产管理等数据库。Intel Xeon系列处理器为应用提供所需的处理能力，保持业务更顺畅、更高效地运行。通过高达8核甚至更多内核的配置以及利用大型片上高速缓存器来减少上下文切换以加速并行处理，这些处理器可以同时运行大量企业级应用。

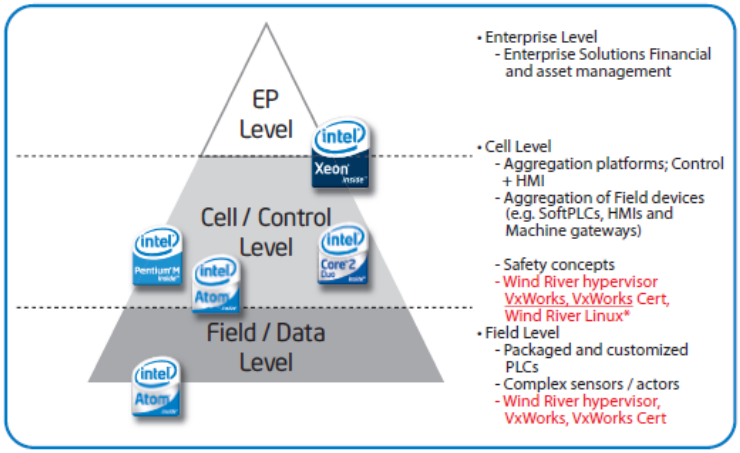

图2：自动化行业应用金字塔

单元/控制层（Cell/Control Level）中的设备实现了不同关键级别的实时控制和人机界面（HMI）功能。这个层面的设备非常适宜采用Wind River hypervisor和Intel多核处理器，因为它们可提供的计算性能和软件隔离以及安全性相关应用所必需的可靠性。Intel® Core™2 Duo处理器拥有两个内核，可以在其中一个内核上运行时间关键性应用功能，而另外一个内核上运行其他功能，例如HMI和操作面板。这种多核处理器具有前所未有的单位功耗性能，更适合于在空间受限系统中应用。

最下面的现场/数据层（Field/Data Level）用于控制工厂的底层车间，将传感器和制动器等连接至控制器，最终传送到制造设备。通常，这个层面要求采用低功耗的设备，因此面向嵌入式计算设计的Intel® Atom™处理器Z5xx系列（图3）是很好的选择。该处理器的功耗设计低至2瓦特，充分体现了Intel架构针对小芯片尺寸、低功耗嵌入式控制设备的优势。

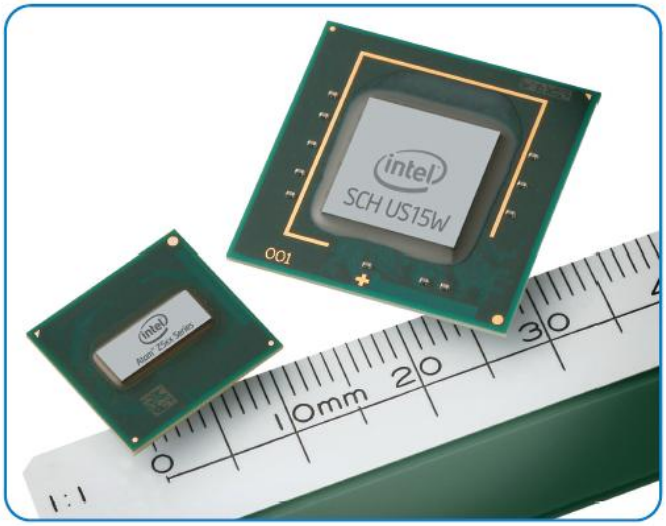

图3：Intel® Atom™处理器和Intel® System Controller Hub US15W

从从最高的企业层到最低的车间现场层，采用具备长生命周期支持的嵌入式Intel处理器，开发人员就能构建各种性能级别和同样代码基础的各类平台。除了这些优势外，设备制造商会发现，面向通用处理器（如Intel架构处理器）的软件代码比面向应用专用硬件的代码更加易于维护。这是因为Intel处理器能够被范围广泛的系统架构支持，拥有大量成熟的开发工具。例如，作为Intel嵌入式与通信联盟（Intel Embedded and Communications Alliance）的成员，风河长期与Intel紧密合作，确保能够在最新处理器产品上市的第一时间就在其解决方案中得以应用。

以Wind River Hypervisor实现虚拟化

如图4所示，Wind River Hypervisor能够将物理硬件上的资源分区为虚拟板。每个虚拟硬件板上能运行一个操作系统（即访客操作系统）或者一个最小执行程序（executive）。通过提供的配置工具，可以将物理硬件板上的处理内核、内存和设备进行分区。采用合适的调度算法，处理内核能够被专门分配给某一虚拟板，或者由多个虚拟板共享。内存进行分区后，每个虚拟板都有其自有的专用内存空间，不会对其他虚拟板造成影响。通过分配共享内存缓冲器，还能够实现虚拟板间的高速通讯。经过分区，包括串行线路或以太网模块在内的设备也可以专用于某一虚拟板或者由多个虚拟板共享。

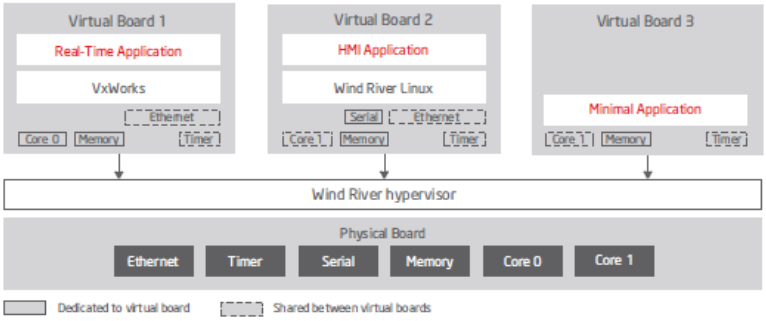

图4：将系统分区为虚拟板

虚拟板机制实现了将各类现有私有操作系统向Hypervisor的导入和虚拟化，从而能够与商用操作系统同时运行。这就提供了向COTS技术循序渐进的过渡方式，也使得向Intel高级多核架构等新硬件架构的迁移变得更加容易。因此，我们可以重复使用现有的那些非常健壮的遗留应用，并通过采用更佳的通用操作系统（如Wind River Linux），在无需改变程序的情况下创建更多全新的功能特性。

在很多工业领域的应用中，需要采用两个或更多个的独立计算平台来完成整个系统构建。采用独立硬件的原因是因为各种应用具有不同的属性特征。例如，当操作人员需要高级人机界面进行操控交互时，往往需要具有严格实时特性要求的控制应用程序。在其他情况下，可能由于性能的局限而必须采用独立硬件。虚拟板机制所带来的强大隔离和保护能力，再加上多核处理器技术，形成了强有力的组合，将实现工业系统的全面集中化。

通过虚拟板之间的隔离和保护，避免了某一虚拟板出现故障时对其他虚拟板造成影响。比如，当一个低关键级别人机界面应用出现问题时，其他运行高关键级别任务系统的虚拟板不会受到任何影响。此外，在某一虚拟板中出现重大故障，需要将该虚拟板重新启动时，Wind River Hypervisor中的系统监管功能可以针对单个虚拟版进行错误探测，还可以单独重启发生错误的虚拟版，期间仍确保不会影响其他虚拟版的正常运行。这一重要功能将极大地提升工业应用的可靠性。

Wind River Hypervisor只是风河多核软件解决方案的组成部分之一。完整的风河多核软件解决方案包含了众多能够帮助工业设备制造商成功部署和应用多核处理器的先进技术，其组成部分包括：

- 对多核软件配置和虚拟化的支持
- 面向DO-178B和IEC61508-Part 3安全级别应用的VxWorks平台
  - 业界领先的实时操作系统VxWorks
  - VxWorks认证（通过严格的DO-178B和IEC61508-Part 3安全应用认证的实时操作系统）
  - Wind River Linux
- 用于开发、调试和多核优化及虚拟化的Wind River Workbench

Wind River Hypervisor同时适用于Intel单核或多核处理器架构，提供高性能硬件集中化解决方案，同时还保持了硬件的独立性。

以Intel® Virtualization Technology（Intel® VT）将虚拟化提升到新水平

通过称为Intel® Virtualization Technology（Intel® VT）的补充硬件辅助技术，Intel进一步加强了虚拟化的能力。Intel VT能够在硬件中实现多种虚拟化任务，例如内存地址翻译等，由此减小了Hypervisor软件占用的空间，也提升了性能。

Wind River Hypervisor借助于Intel VT提供了更加优化的虚拟化性能，同时也提升了可靠性。如果没有这项新技术，Hypervisor就必须自己负责处理操作系统中的大多数平台控制任务，这些任务需要大量复杂的计算密集型运算。采用Intel VT后，这些重要而繁杂的操作可以通过硬件来实现，从而极大地降低了Hypervisor软件的计算处理负担，进而提升了Hypervisor的性能。此外，对于存储在无保护内存里的关键处理器和操作系统状态数据，如果没有硬件的辅助，Hypervisor就成为唯一的保护者。Intel VT加入了强大的强制保护层面，能够阻止除了Hypervisor以外的其他任何软件组件访问关键系统信息。

Intel提供了以下三类虚拟化技术：

- Intel® Virtualization Technology (Intel® VT) for IA-32、Intel® 64和Intel® Architecture (Intel® VT-x)：提供了虚拟机监视器（VMN）高效运行所需的基础框架。
- Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d)：提供更便捷的虚拟化I/O设备，例如将DMA访问重映射到分段内存区域、过滤和重映射中断等。
- Intel® Virtualization Technology (Intel® VT) for Connectivity (Intel® VT-c)：与Intel® Ethernet控制器联合运行，支持将网络流量数据过滤和映射到被特定虚拟机（VM）“占有”的指定队列。

在使用Hypervisor的设备中引入Intel VT，可以提升整个虚拟化系统环境的性能和安全性。

安全认证方面的挑战

设备制造商所面临的一大挑战是在进行安全认证的过程中，必须确保安全相关的软件满足特定的需求，并且证实它们实现了与系统其他部分的严格隔离与保护。如果系统的硬件和软件

是完全集中化的，就要求那些运行在通用操作系统上的非安全相关软件也必须通过安全认证。由于通用操作系统（GPOS）的规模和应用程序更为繁多，这项工作往往非常困难和昂贵。此外，为了提升用户接口和系统连接性，制造商希望能够经常对非安全相关软件进行灵活的修改，而不必再忍受产品生命周期内对整个系统无数次重新认证所带来的成本增加和进度延迟。

应该根据不同的安全关键级别，将安全相关组件与系统内其他组件实现时间上和空间上的隔离。目前，隔离的概念通常是指每一项功能使用完全独立的子系统，但这种做法对于硬件而言效率很低，而且大大增加了成本。此外，各种私有系统和软件就意味遗留依赖性，当OEM厂商转向使用新的商用现货型（COTS）硬件和软件技术时，这还会给开发人员带来新的挑战。但是，如果开发人员在系统设计中能够考虑好软件过渡的灵活性，就可以成功部署应用并充分发挥多核处理器和虚拟化这些新技术的优势。

降低风险

航空与国防行业已经具备完整定义的ARINC 653安全隔离标准，而其他大多数工业领域的应用都缺乏统一的标准方法来实现安全功能，这就造成对安全标准的解释处于开放状态，从而为设备制造商带来了极大地不可预测性和不确定性。在很多情况下，设备制造商越来越频繁地需要将各种安全关键级别的软件组合运用，并且要达到更加严格的安全标准。在ARINC 653系统环境中，提升软件隔离性的最有效方法就是将软件组件作为一个个独立的模块进行安全认证。

作为市场中通过DO-178B安全认证的ARINC 653系统隔离技术领先提供商，风河正在将其技术和经验融入到工业市场市场，降低并消除风险，帮助工程师开发出具有更高安全性和确定性的软件应用。利用Wind River Hypervisor的内存保护功能，可以确保虚拟板上运行应用的空间隔离，如图5所示。在该配置下为应用设定了专用、安全的内存上下文（context），这是保证独立软件模块的安全完整性的关键因素。完成空间隔离后，应用将以独立模块的形式运行，使OEM厂商可以将他们作为更小、更简单的组件提交认证。此外，在多虚拟板共享一个内核的情况下，通过将虚拟板指定给独立的内核，或利用Hypervisor中合适的调度算法，还可以实现不同应用间的时间隔离。

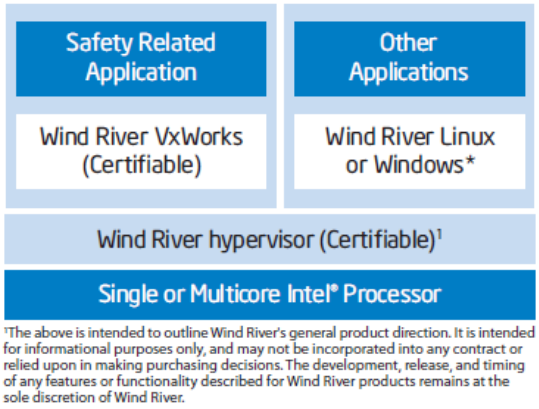

图5：安全相关应用的虚拟化系统

基于Intel处理器运行的风河性能优化Hypervisor解决方案能够提供：

- 实现应用的时间和空间隔离的机制
- 将安全相关功能（如软件PLC）与其他功能（如图形化用户接口）相隔离
- 开放的模块化方法，能够实现更经济高效的安全性

满足未来安全性和性能的需求

多核和虚拟化技术相结合，为满足未来工业与交通行业对安全性和计算性能的需求铺平了道路。正因为如此，Intel与风河提供的硬件和软件技术可以帮助开发人员采用标准化的方法实现时间和空间的隔离。Intel多核处理器的卓越处理性能，再加上Intel虚拟化技术，可以确保应用在虚拟化的环境下安全运行。风河将提供领先的软件平台框架作为有力的支持，包括VxWorks for DO-178B、IEC61508操作系统和Wind River Hypervisor等。

根据IEC61508-Part 3安全标准和从IEC61508规范衍生的其他行业标准，需要对安全关键应用做出认证的OEM厂商，只要采用基于Intel处理器架构的风河产品，就会受益无穷，因为这样可以大幅度提升实时虚拟化环境下的安全性和可靠性。

关于Intel嵌入式计算处理器的更多信息，敬请访问：www.intel.com/products/embedded
关于风河多核软件解决方案和Hypervisor产品的更多信息，敬请访问：
http://www.windriver.com/multicore-software.

Wind River 就在您身边

北京代表处	北京市朝阳区望京中环南路9号望京大厦B座18层	邮编：100102	电话：010-84777100	传真：010-64398189
上海代表处	上海市西藏路585号新金桥广场3-H,I,J室	邮编：200003	电话：021-63585586/87/89/90	传真：021-63585591
深圳代表处	深圳市福田区车公庙天安数码时代大厦A座606室	邮编：518040	电话：0755-25333408/3418/4508/4518	传真：0755-25334318
西安代表处	西安市高新区科技二路68号西安软件园秦风阁H103	邮编：710075	电话：029-87607208	传真：029-87607209
成都代表处	成都市高新区天府软件园二期D7 14层	邮编：610041	电话：028-65318000	传真：028-65319983

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

WIND RIVER