

白皮书

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

多核心和虛擬化在工業控制與安全性相關領域的應用

多核心和虛擬化為提升設備性能、降低設備成本鋪平了道路，因為由此可以實現硬體集中化，並且使整個產品生命週期內的應用升級更加經濟高效。

顛覆性的技術和趨勢正在影響著嵌入式市場，同時也為工業控制領域的設備製造商帶來了巨大的機遇，在產品和商業模式兩個方面都獲得全面的提升。如果能夠借助力於以下技術和行業趨勢，就意味著獲得了巨大的競爭優勢。

- 多核心處理器
- 虛擬化技術
- 安全相關設備不斷增加的複雜度

多核心處理器的成熟，不僅導致了近年來嵌入式市場的一次顛覆性變革，也帶來了最大的商業機遇。最新的Intel®多核心處理器在實現系統整體性能提升的同時，也提高了單個處理器內核心每瓦特功耗所提供的性能。基於多核心處理器的系統還能改善應用的可擴展性並保護軟體投資，因為它允許用更多內核心的處理器來替換原來的處理器，以便滿足未來的需求。走向多核心，這個趨勢已經形成，一個顯著的實證就是，Intel®雙核心和四核心處理器的出貨量已經迅速地超過了單處理器。

第二項技術是虛擬化，它實現了在同一物理硬體平臺上同時運行多個虛擬機的能力，因為它可以對底層處理內核心、記憶體和外設周邊進行抽象模擬。採用虛擬化技術可以在同一設備內同時運行多個作業系統環境，例如一個即時作業系統，例如Wind River VxWorks，再加上一個通用作業系統，例如Wind River Linux，如圖1所示。借助於多核心處理器和虛擬化所獲得的高性能，可以對原先分別運行不同應用的多個獨立設備做集中化，整合為一個設備。設備集中化將會有效地減少硬體數量，提升能源利用效率，從而降低設備的整體物料清單和運行費用。

虛擬化是由Hypervisor來實現的，它具有系統監管（supervisory）功能，能夠保護操作環境，避免作業系統之間相互影響，並且提供了系統隔離措施，以便提升系統的可靠性和安全性。採用此項技術可以讓每個應用的獨立演進，降低了設備生命週期的成本投入。

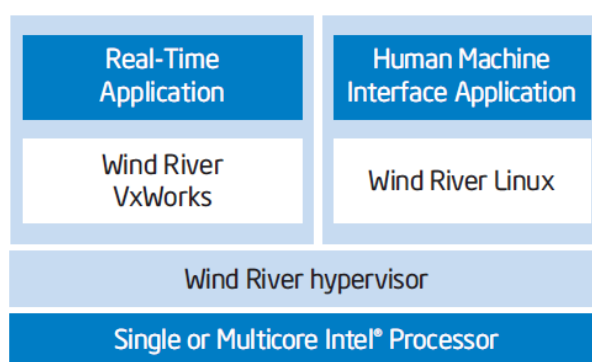


圖1：採用虛擬化技術的系統

隨著對新功能和法規遵從性方面的要求不斷增加，**安全性相關架構**變得越來越複雜。推動複雜度增長的動力之一是工業設備與網路和系統的介面越來越多，例如Internet、top-floor和shop-floor等。因此，設備必須能夠支援不同關鍵級別的各种類型應用軟體（例如安全性群組件、協定棧等）。伴隨著系統複雜度的增加，法規機構也在採取更嚴格的認證方法和流程來確保系統的安全性。多核心和虛擬化相結合，能夠說明工業控制、流程自動化、能源和交通等行業的製造商保護他們的投資開發。這些技術能夠使系統更安全地同時運行更多的程式，因此，可以在確保性能、安全性、可擴展性、認證性和可用性等要素的同時，逐漸完成對現有多核心平臺的升級。Intel多核心處理器的性能已經得到增強，在對軟體做最少變更的前提下，將控制、資料搜集、虛擬化和網路安全性等功能集中化到單一參考板之上。此外，虛擬化層可以減少對硬體的直接依賴，從而保護軟體投資。這使研發人員能夠更輕鬆地遷移和升級到新的設備架構，同時更高效地管理好向商用現貨型（COTS）技術的過渡。本文將進一步詳述Intel和Wind River 多核心及虛擬化技術如何改變工業控制和安全性相關領域應用研發人員的工作方式，徹底避免軟體的相互影響和來自外部的破壞。同樣越來越重要的是法規方面的影響，包括安全相關的應用標準（如IEC 61508、CENELEC 50128、ISO 26262和IEC60880/62138等），以及能源、交通、自動化和工業控制領域的更多細分行業標準。

全面支持工業解決方案處理器

VxWorks、Wind River Linux和Wind River Hypervisor可以在大跨度的Intel系列處理器上運行，並且由一套開放標準工具集提供支援，為多核和多作業系統開發過程帶來更高的效率。

這些功能可以跨越覆蓋工業控制設備的不同類型，呈現在如圖2所示的“自動化金字塔”中的不同層面。企業層（EP）支援運行混合應用軟體的伺服器和工作站，包括協同生產管理（CPM）、財務管理和資產管理等資料庫。Intel Xeon系列處理器為應用提供所需的處理能力，保持業務更順暢、更高效地運行。通過高達8核心甚至更多內核心的配置以及利用大型快取記憶體器來減少上下切換以加速並行處理，這些處理器可以同時運行大量企業級應用。

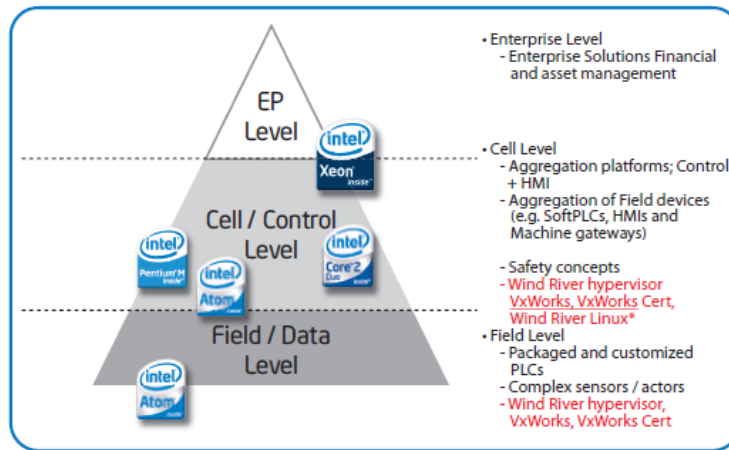


圖2：自動化行業應用金字塔

單元/控制層（Cell/Control Level）中的設備實現了不同關鍵級別的即時控制和人機界面（HMI）功能。這個層面的設備非常適宜採用Wind River hypervisor和Intel多核心處理器，因為它們可提供的計算性能和軟體隔離以及安全性相關應用所必需的可靠性。Intel® Core™2 Duo處理器擁有兩個內核心，可以在其中一個內核心上執行時間關鍵性應用功能，而另外一個內核心上運行其他功能，例如HMI和操作面板。這種多核心處理器具有前所未有的單位功耗性能，更適合於在空間受限系統中應用。

最下面的現場/資料層（Field/Data Level）用於控制平面的底層，將感測器和制動器等連接至控制器，最終傳送到製造設備。通常，這個層面要求採用低功耗的設備，因此面向嵌入式計算設計的Intel® Atom™處理器Z5xx系列（圖3）是很好的選擇。該處理器的功耗設計低至2瓦特，充分體現了Intel架構針對小晶片尺寸、低功耗嵌入式控制設備的優勢。

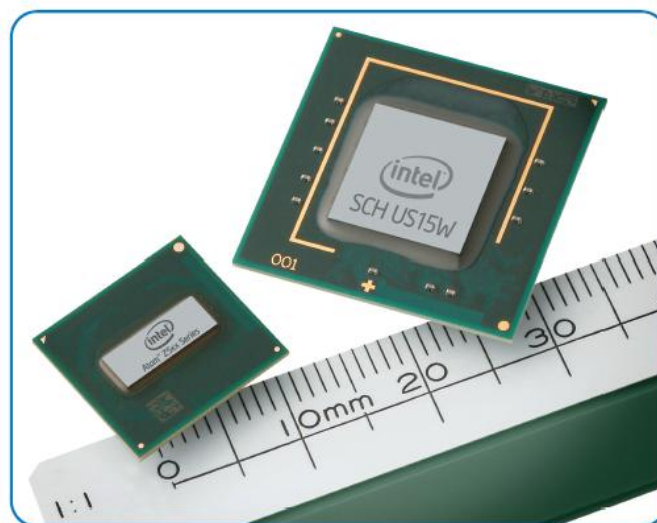


圖3：Intel® Atom™處理器和Intel® System Controller Hub US15W

從最高的企業層到最低的平面底層，採用具備長生命週期支援的嵌入式Intel處理器，研發人員就能構建各種性能級別和同樣代碼基礎的各類平臺。除了這些優勢外，設備製造商會發現，面向通用處理器（如Intel架構處理器）的軟體代碼比面向應用專用硬體的代碼更加易於維護。這是因為Intel處理器能夠被範圍廣泛的系統架構支援，擁有大量成熟的開發工具。例如，作為Intel嵌入式與通信聯盟（Intel Embedded and Communications Alliance）的成員，Wind River 長期與Intel緊密合作，確保能夠在最新處理器產品上市的第一時間就在其解決方案中得以應用。

以Wind River Hypervisor實現虛擬化

如圖4所示，Wind River Hypervisor能夠將物理硬體上的資源分區為虛擬板。每個虛擬硬體板上能運行一個作業系統（即Guest OS）或者一個最小執行程式（executive）。通過提供的配置工具，可以將物理硬體板上的處理內核心、記憶體和設備進行分區。採用合適的調度演算法，處理內核心能夠被專門分配給某一虛擬板，或者由多個虛擬板共用。記憶體進行分區後，每個虛擬板都有其自有的專用記憶體空間，不會對其他虛擬板造成影響。通過分配共用記憶體緩衝器，還能夠實現虛擬板間的高速通訊。經過分區，包括Serial Port或Ethernet模組在內的設備也可以專用於某一虛擬板或者由多個虛擬板共用。

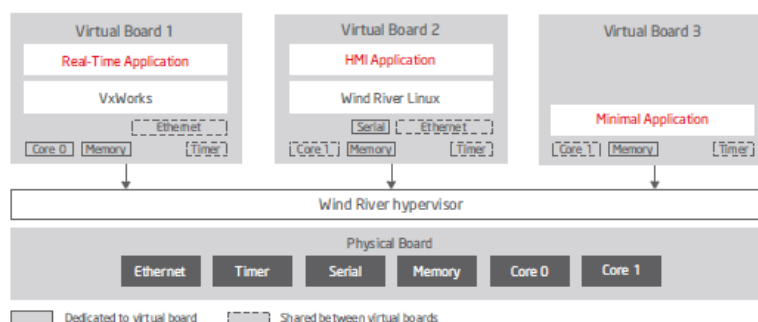


圖4：將系統磁碟分割為虛擬板

虛擬板機制實現了將各類現有私有作業系統向Hypervisor的導入和虛擬化，從而能夠與商用作業系統同時運行。這就提供了技術上可循序漸進的過渡方式，也使得向Intel高級多核心架構等新硬體架構的遷移變得更加容易。因此，我們可以重複使用已開發過的應用程序，並通過採用更佳的通用作業系統（如Wind River Linux），在無需改變程式的情況下創建更多全新的功能特性。

在很多工業領域的應用中，需要採用兩個或更多個的獨立計算平臺來完成整個系統構建。採用獨立硬體的原因是因為各種應用具有不同的屬性特徵。例如，當操作人員需要高級人機界面進行操控交互時，往往需要具有嚴格即時特性要求的控制應用程式。在其他情況下，可能由於性能的局限而必須採用獨立硬體。虛擬板機制所帶來的強大隔離和保護能力，再加上多核處理器技術，形成了強有力的組合，將實現工業系統的全面集中化。

通過虛擬板之間的隔離和保護，避免了某一虛擬板出現故障時對其他虛擬板造成影響。比如，當一個低關鍵級別人機界面應用出現問題時，其他運行高關鍵級別任務系統的虛擬板不會受到任何影響。此外，在某一虛擬板中出現重大故障，需要將該虛擬板重新開機時，Wind

River Hypervisor中的系統監管功能可以針對單個虛擬板進行錯誤探測，還可以單獨重啟發生錯誤的虛擬板，期間仍確保不會影響其他虛擬板的正常運行。這一重要功能將極大地提升工業應用的可靠性。

Wind River Hypervisor只是Wind River 多核心軟體解決方案的組成部分之一。完整的Wind River 多核心軟體解決方案包含了眾多能夠協助工業設備製造商成功部署和應用多核處理器的先進技術，其組成部分包括：

- 對多核心軟體配置和虛擬化的支援
- 面向DO-178B和IEC61508-Part 3安全級別應用的VxWorks平臺
 - 業界領先的即時操作系統VxWorks
 - VxWorks認證（通過嚴格的DO-178B和IEC61508-Part 3安全應用認證的即時操作系統）
 - Wind River Linux
- 用於開發、測試和多核心最佳化及虛擬化的Wind River Workbench

Wind River Hypervisor同時適用於Intel單核心或多核心處理器架構，提供高性能硬體集中化解決方案，同時還保持了硬體的獨立性。

以Intel® Virtualization Technology (Intel® VT) 將虛擬化提升到新水準

通過稱為Intel® Virtualization Technology (Intel® VT) 的虛擬技術，Intel進一步加強了虛擬化的能力。Intel VT能夠在硬體中實現多種虛擬化任務，例如記憶體位址翻譯等，由此減小了Hypervisor軟體佔用的空間，也提升了性能。

Wind River Hypervisor借助於Intel VT提供了強化過的虛擬化性能，同時也提升了可靠性。如果沒有這項新技術，Hypervisor就必須自己負責處理作業系統中的大多數平臺控制任務，這些任務需要大量複雜的計算密集型運算。採用Intel VT後，這些重要而繁雜的操作可以通過硬體來實現，從而極大地降低了Hypervisor軟體的計算處理負擔，進而提升了Hypervisor的性能。此外，對於存儲在無保護記憶體裡的關鍵處理器和作業系統狀態資料，如果沒有硬體的輔助，Hypervisor就成為唯一的保護者。Intel VT加入了強大的強制保護層面，能夠阻止除了Hypervisor以外的其他任何軟體元件訪問關鍵系統資訊。

Intel提供了以下三類虛擬化技術：

- Intel® Virtualization Technology (Intel® VT) for IA-32、Intel® 64和Intel® Architecture (Intel® VT-x)：提供了虛擬機監視器（VMN）高效運行所需的基礎框架。
- Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d)：提供更便捷的虛擬化I/O設備，例如將DMA訪問重映射到分段記憶體區域、過濾和重映射中斷等。
- Intel® Virtualization Technology (Intel® VT) for Connectivity (Intel® VT-c)：與Intel® Ethernet控制器聯合運行，支援將網路流量資料過濾和映射到被特定虛擬機器（VM）“佔有”的指定佇列。

在使用Hypervisor的設備中引入Intel VT，可以提升整個虛擬化系統環境的性能和安全性。

安全認證方面的挑戰

設備製造商所面臨的一大挑戰是在進行安全認證的過程中，必須確保安全相關的軟體滿足特定的需求，並且證實它們實現了與系統其他部分的嚴格隔離與保護。如果系統的硬體和軟體是完全集中化的，就要求那些運行在通用作業系統上的非安全相關軟體也必須通過安全認證。由於通用作業系統（GPOS）的規模和應用程式更為繁多，這項工作往往非常困難和昂貴。此外，為了提升使用者介面和系統連线性，製造商希望能夠經常對非安全相關軟體進行靈活的修改，而不必再忍受產品生命週期內對整個系統無數次重新認證所帶來的成本增加和進度延遲。

應該根據不同的安全關鍵級別，將安全相關元件與系統內其他元件實現時間上和空間上的隔離。目前，隔離的概念通常是指每一項功能使用完全獨立的子系統，但這種做法對於硬體而言效率很低，而且大大增加了成本。此外，各種私有系統和軟體就意味遺留依賴性，當OEM廠商轉向使用新的商用現貨型（COTS）硬體和軟體技術時，這還會給開發人員帶來新的挑戰。但是，如果開發人員在系統設計中能夠考慮好軟體過渡的靈活性，就可以成功部署應用並充分發揮多核心處理器和虛擬化這些新技術的優勢。

降低風險

航空與國防行業已經具備完整定義的ARINC 653安全隔離標準，而其他大多數工業領域的應用都缺乏統一的標準方法來實現安全功能，這就造成對安全標準的解釋處於開放狀態，從而為設備製造商帶來了極大地不可預測性和不確定性。在很多情況下，設備製造商越來越頻繁地需要將各種安全關鍵級別的軟體組合運用，並且要達到更加嚴格的安全標準。在ARINC 653系統環境中，提升軟體隔離性的最有效方法就是將軟體元件作為一個個獨立的模組進行安全認證。

作為市場中通過DO-178B安全認證的ARINC 653系統隔離技術領先提供商，Wind River正在將其技術和經驗融入到工業市場市場，降低並消除風險，幫助工程師開發出具有更高安全性和確定性的軟體應用。利用Wind River Hypervisor的記憶體保護功能，可以確保虛擬板上運行應用的空間隔離，如圖5所示。在該配置下為應用設定了專用、安全的記憶體上下文（context），這是保證獨立軟體模組的安全完整性的關鍵因素。完成空間隔離後，應用將以獨立模組的形式運行，使OEM廠商可以將他們作為更小、更簡單的元件提交認證。此外，在多虛擬板共用一個內核心的情況下，通過將虛擬板指定給獨立的內核心，或利用Hypervisor中合適的調度演算法，還可以實現不同應用間的時間隔離。

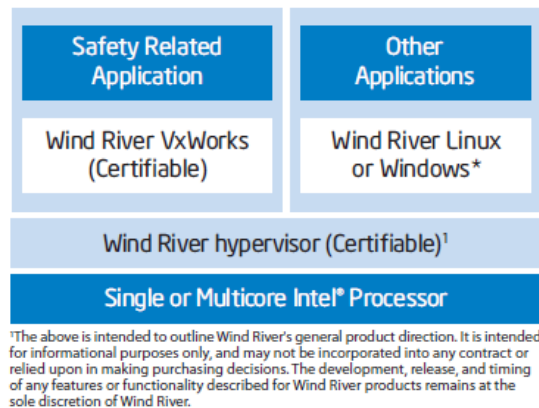


圖5：安全相關應用的虛擬化系統

基於Intel處理器運行的Wind River Hypervisor解決方案能夠提供：

- 實現應用的時間和空間隔離的機制
- 將安全相關功能（如軟體PLC）與其他功能（如圖形化使用者介面）相隔離
- 開放的模組化方法，能夠實現更經濟高效的安全性

滿足未來安全性和性能的需求

多核心和虛擬化技術相結合，為滿足未來工業控制與軌道交通行業對安全性和計算性能的需求鋪平了道路。正因為如此，Intel與Wind River提供的硬體和軟體技術可以讓研發人員採用標準化的方法實現時間和空間的隔離。Intel多核心處理器的卓越處理性能，再加上Intel虛擬化技術，可以確保應用在虛擬化的環境下安全運行。Wind River將提供領先的軟體平臺框架作為有力的支援，包括VxWorks for DO-178B、IEC61508作業系統和Wind River Hypervisor等。

根據IEC61508-Part 3安全標準和從IEC61508規範衍生的其他行業標準，需要對安全關鍵應用做出認證的OEM廠商，只要採用基於Intel處理器架構的Wind River產品，就會受益無窮，因為這樣可以大幅度提升即時虛擬化環境下的安全性和可靠性。

關於Intel嵌入式計算處理器的更多資訊，敬請訪問：www.intel.com/products/embedded

關於Wind River多核心軟體解決方案和Hypervisor產品的更多資訊，敬請訪問：

<http://www.windriver.com/multicore-software>.

