

## 邁向多核心 - 醫療設備應用創新的關鍵要素

Jens Wiegand

Wind River 公司工業與醫療設備行業市場總經理

### 提要

近年來，醫療電子設備行業正在發生著根本性的變化。傳統的系統設計已經延續了20年，每一項設計都歷經了數年的傳承和測試。如今，有了全數位化系統，人們希望有更多的創新，產品新功能和新版本的開發越來越快。業界將更多地關注於經濟高效性，以便可以在更多的醫院和診所部署更多的新設備。

為了開發下一代安全關鍵級醫療和工業電子設備，設計人員和系統架構師必須進一步整合硬體、降低成本、加快產品上市速度，同時還不能在平臺的穩定性、安全性和可靠性方面打任何一點折扣。

本文就是說明醫療設備系統設計人員瞭解應當如何應對所面臨的挑戰：多核心硬體的整合方案、已具備安全認證的作業系統、Hypervisor軟體以及開發工具套件。

### 當今安全關鍵級系統設計的挑戰

越來越多醫療設備系統的新功能設計趨向於軟體實現，這就使安全性需求成為設計過程中的極大挑戰。軟體中的部分元件以及對應的硬體已通過關鍵安全驗證，必須保留不予更動，但同時需要增加新的部件來實現產品創新與升級換代，新產品系統仍必須確保符合各種界面標準和風險評估要求。

如何可解決安全性的問題並且盡可能的利用已開發過軟體應用是非常重要的。但是，這些已開發過的軟體如遺產一般，可能已經變的散落不完整。如要把它們整合起來運行並充分發揮新一代電子設備的性能和成本優勢，整個過程往往要耗費大量的金錢和時間，同時也很難對市場變化做出及時的相

應，而且長期維護的成本也會大幅增加。

多核心處理器和Hypervisor等針對嵌入式環境做了最佳化的新興技術，為解決這些問題提供了關鍵性的動力，因為這些技術既提供了增強安全性的全新機制，也推動了硬體和軟體的整合，從而為功能創新打開了方便之門。這些技術不僅對於醫療設備行業非常重要，同時也適用於其他行業領域，包括工業控制和交通設備。

傳統上，這些市場一直是由產品的功能性來驅動的，但是到了今天，安全性、穩定性、品質、可維護性和經濟高效性，所有這些都上升為最重要的因素。基於IEC 61508基本功能安全標準及其衍生標準的安全性需求適用於各個行業領域，由此也提出了新的挑戰，這就是既要滿足設備的功能需求，還必須遵循上述安全標準。

### 面向複雜醫療設備的多核心技術

在醫療應用中複雜的診斷設備越來越多，包括X光機、CT掃描機和血液透析機等，其中增加了許多新的功能特性，例如自動報告生成和網路通信等，而且成本也大為降低。

傳統方式中，這些設備中的創新和功能升級是由各個分離的硬體系統來實現，並各自遵循相關的醫療設備標準，例如針對電磁相容性的IEC 60601標準（防止設備互相干擾）以及用於風險評估的ISO14971標準。這種架構一直都是採用一個專門的硬體板來實現關鍵安全功能，通常採用不含任何軟體的純硬體模式，或者只包含嚴謹程式設計並經過多年驗證的簡單軟體。另一個硬體板被專門用來實現非關鍵安全的功能，包括系統管理和網路通信等。

儘管這種架構在過去這些年完全能夠滿足需求，但隨著新標準、新功能的要求以及為了節省成本和縮小空間所必需的集中化，這種雙硬體板的方式已經不再可行。如今，醫療設備軟體中增加的功能必須通過綜合認證，確保遵循美國食品與藥物管理局(FDA)或歐洲相關管理機構的嚴格標準，例如用來定義整個軟體生命週期過程的IEC 62304標準。

多核心設備是滿足上述需求的關鍵性途徑。這些設備如今已經進入嵌入式市場，能夠滿足這些行業市場領域未來5到10年對性能和功能支援的需求。不過，他們仍然延續了PC和企業應用領域的商用作業系統和企業軟體，同時帶來了原本就是由PC和企業市場所驅動的成本壓縮和集成化。

使用多核心處理器可以將現有的雙硬體板架構集中化為單個硬體板，將其中一個核心用於關鍵安全軟體，另一核心用於其它非關鍵安全功能。

## 以Hypervisor實現系統集中化

儘管從理論上可行，但是這種“裸機(bare metal)”方式的系統設計需要大量的時間和成本，同時還要求經驗豐富、人數眾多的研發團隊。另外，這種方式還需要提供數千行的測試和驗證源代碼以便進行安全認證，而在整個認證過程中開發和運行這些源代碼將耗費大量的時間。

隨著新功能的引入越來越快，安全相關軟體的認證逐漸從“使用中才被驗證”的模式轉變為更規範的面向工具的模式。這也許是當今市場中最大的變化，導致開發人員不確定如何才能適應這些改變，也不確定他們所投資的軟體和相關工具在擴展到協力廠商軟體元件時還能通過認證。FDA規定，要達到預上市許可應用的標準和要求，就必須擁有科學有效的依據來支援，說明設備的安全性和有效性不是空中樓閣。要對軟體進行驗證，其代價是非常高昂的，而且可能會導致

產品生命週期中的不可預測性。

上述因素推動了Hypervisor這類新的軟體解決方案的出現。Hypervisor可以在同一平臺不同內核心中運行不同的作業系統，使系統設計人員能夠利用更廣範圍的協力廠商軟體，同時保留已有的關鍵安全軟體的應用程式。通常，可以用一個專用處理器運行關鍵安全軟體，而其他處理器運行Wind River VxWorks等即時作業系統或者Linux之類等通用作業系統，如此結合就能在同一系統平臺或者處理器上實現不同關鍵等級。

集中化平臺的發展推動了作業系統平臺的多樣化。VxWorks這種即時作業系統的優勢是比Linux這類非即時作業系統具有更高的安全性和較低的複雜度，是實現安全認證的理想選擇。Linux則能夠在實現客戶通訊標準或圖形使用者界面等具有更好的優勢。因此，在同一系統平臺中使用兩類作業系統可以同時發揮它們各自的優勢。通過全新的Hypervisor整合技術，這種架構方式就能成為現實。

## 支持和商用化驗證對Linux至關重要

隨著越來越多的設備製造商採用Linux作業系統，系統的支援問題也開始逐一浮現。雖然有一些相關的技術和開發工具可用于實現集中化，但支離破碎仍然是基於Linux解決方案中存在的最大問題。

製造商們經常試圖利用Linux免費版本來開發，而放棄已通過驗證並附帶技術支援的商用化產品。但是，他們低估了Linux的複雜性和業務開發可能面臨的挑戰。選擇商業版本的優點不勝枚舉：Linux的培訓、穩定性、符合開放標準、智慧財產權的保障、完備的文檔和可擴展性，這些僅僅是選擇商業版本所具優勢的一部分。因此，在做決策過程中應該仔細考慮這些因素。

使用Linux的一個重要用途是能夠對單一硬體平臺內同一應用中的安全關鍵功能和非

安全關鍵功能進行分區。Linux帶來的功能性和新型中介軟體具有強大的價值潛力，但在安全性需求的環境中卻帶來了新的複雜度。Hypervisor技術能夠實現Linux和即時作業系統在軟體層面的集中化，使安全性和非安全性應用可以在同一硬體平臺上運行。多核心處理器技術和Hypervisor技術的結合使多作業系統在同一硬體平臺上併發運行，同時確保隔離和保護。

在同一時間內，安全關鍵任務可以在通過安全認證的VxWorks即時作業系統中運行，而通信協定則可在VxWorks或Linux甚至其他作業系統中運行，從而在同一設備內實現了Supervisor功能。Hypervisor技術也簡化了原有舊系統的遷移，因為分區架構使同一作業系統的不同版本能夠併發運行，因此原有代碼無需改變就可以運行，而新代碼則可以充分使用新版本作業系統中的全新功能特性。集成服務可以進一步說明客戶消除安全性和集中化專案中的風險，確保產品開發的順利和可預測性，極大地加快投資回報週期。

安全關鍵醫療設備系統中的另一重要問題是，使用多作業系統後，在必需使用分離開發工具套件時會造成巨大的困難，從而使開發進程變慢，並且導致更多的程式缺陷和風險。此外，這種情況下還需要完成由FDA設備與放射線健康管理中心所規定的更多軟體認證和驗證，這就使設備製造商不得不進行這些測試工作，從而耗費更多的投資和時間。

取而代之，可以採用集中化開發工具套件，例如基於Eclipse開放框架的Wind River Workbench，順應多作業系統架構的發展趨勢，使各種面向不同作業系統的應用可以在同一時間、同一環境下完成開發。根據開放的概念，使用統一的測試和靜態分析工具，可以為研發團隊帶來巨大的優勢。Eclipse框架的高度開放性，使更多其他工具可以與之集成，從而成為設備開發人員成功的得力助手。

## 工業應用市場的同類需求

工業應用市場可以細分為6大獨立領域——醫療設備應用、交通基礎設施、工業控制、測試與測量、能源輸送和汽車製造，而且這些領域都面臨著非常類似的挑戰。它們都要求重要的安全關鍵系統，並且必須達到嚴格規定的各種安全標準。

上述領域都有很多相似的需求。例如，在工業自動化領域，出現了大量的分散式控制，複雜度也不斷增長，需要能夠更快速構建新工廠或工區並保持其靈活性，同時還要確保品質和安全性。同樣，在工業控制領域，機器人技術的出現帶來了很多變化，機器人和控制單元之間需要採用通信技術來提升系統運行時程，確保操作的安全性。另外，設備中需要採用相應的工具來集成通用PC軟體，例如報表製作或是訪問Internet等，同時還要提升與其他設備連接的安全性。

## 結論

通過多核心硬體、設備安全認證專用作業系統、Hypervisor軟體和開發工具的組合，能夠完全支援並滿足醫療設備系統設計人員的需求。這一系列領先技術將說明設計人員和系統架構師實現硬體集中化、降低開發成本、加快產品上市速度，與此同時提供了能夠在軟體中加入更多新功能並提高產品安全穩定性的平臺，而且會盡可能地重複使用原有舊代碼來構建和維護安全認證的系統環境，這一切都是下一代安全關鍵醫療設備與工業領域系統開發的關鍵要素。

## Wind River 就在您身邊

北京代表處	北京市朝陽區望京中環南路9號望京大廈B座18層	郵編: 100102	電話: 010-84777100	傳真: 010-64398189
上海代表處	上海市西藏路585號新金橋廣場3-H, I, J室	郵編: 200003	電話: 021-63585586/87/89/90	傳真: 021-63585591
深圳代表處	深圳市福田區車公廟天安數碼時代大廈A座606室	郵編: 518040	電話: 0755-25333408/3418/4508/4518	傳真: 0755-25334318
西安代表處	西安市高新區科技二路68號西安軟體園秦風閣H103	郵編: 710075	電話: 029-87607208	傳真: 029-87607209
成都代表處	成都市武侯區武青南路10號5棟2單元303室	郵編: 610045	電話: 028-87491282	傳真: 028-87491282

關於風河更多內容請訪問: <http://www.windriver.com> Email: [inquiries-ap-china@windriver.com](mailto:inquiries-ap-china@windriver.com)

**WIND RIVER**

© 2007 Wind River Systems, Inc. The Wind River logo is a trademark, and Wind River is a registered trademark of Wind River Systems, Inc. Other marks are the property of their respective owners.