WIND RIVER

多核——医疗设备应用创新的关键要素

Jens Wiegand
风河公司工业与医疗设备解决方案总经理

提要

近年来，医疗电子设备行业正在发生着根本性的变化。传统的系统设计已经延续了20年，每一项设计都历经了数年的传承和测试。如今，有了全数字化系统，人们希望有更多的创新，产品新功能和新版本的开发越来越快。业界将更多地关注于经济高效性，以便可以在更多的医院和诊所部署更多的新设备。

为了开发下一代安全关键级医疗和工业电子设备，设计人员和系统架构师必须进一步整合硬件、降低成本、加快产品上市速度，同时还不能在平台的稳定性、安全性和可靠性方面打任何一点折扣。

本文就是帮助医疗设备系统设计人员了解应当如何应对所面临的挑战：多核硬件的整合方案、专业设备安全认证的操作系统、Hypervisor软件以及统一并且开放的开发工具套件。

当今安全关键级系统设计的挑战

越来越多医疗设备系统的新功能设计趋向于软件实现，这就使安全性需求成为设计过程中的极大挑战。软件中的部分组件以及对应的硬件已经通过关键安全验证，必须保留不变，同时可以通过增加新的部件来实现功能创新，变的情况下引入了新功能和新产品，但是整个系统必须确保符合各种接口标准和风险评估要求。

解决安全性的问题并且尽可能地利用原有的软件资产，这是非常重要的。但是，这些软件遗产通常都是支离破碎、到处散落的，要把他们整合起来运行并充分发挥新一代电子设备的性能和成本优势，这个过程往往往往要耗费大量的金钱和时间，同时也很难对市场变化做出及时的相应，而且长期维护的成本也会大幅增加。

多核处理器和Hypervisor等针对嵌入式环境做了优化的新兴技术，已经为解决这些问题提供了关键性的动力，因为这些技术既提供了增强安全性的全新机制，也推动了硬件和软件的整合，从而为功能创新打开了方便之门。这些技术不仅对于医疗设备行业非常重要，同时也适用于其他行业领域，包括工业控制和交通设备。

传统上，这些市场一直是由产品的功能性来驱动的，但是到了今天，安全性、稳定性、质量、可维护性和经济高效性，所有这些都上升为最重要的因素。基于IEC 61508基本功能安全标准及其衍生标准的安全性需求适用于各个行业领域，由此也提出了新的挑战，这就是既要满足设备的功能需求，还必须遵循上述安全标准。

面向复杂医疗设备的多核技术

在医疗应用中复杂的诊断设备越来越多，包括X光机、CT扫描机和血液透析机等，其中增加了许多新的功能特性，例如自动报告生成和网络通信等，而且成本也大为降低。

传统方式中，这些设备中的创新和功能升级由逐个分离的硬件系统实现，尤其要遵循各种医疗设备标准，例如针对电磁兼容性的IEC 60601标准（防止设备互相干扰）以及用于风险评估的ISO14971标准。这种架构一直都是采用一个专门的硬件板来实现关键安全功能，通常采用不含任何软件的纯硬件模式，或者只包含严谨编程并经过多年验证的简单软件。另一个硬件板被专门用来实现非关键安全的功能，包括系统管理和网络通

信等。

尽管这种架构在过去这些年完全能够满足需求，但随着新标准、新功能的要求以及为了节省成本和缩小空间所必需的集中化，这种双硬件板的方式已经不再可行。如今，医疗设备软件中增加的功能必须通过检验和认证，确保遵循美国食品与药物管理局（FDA）或欧洲相关管理机构的严格标准，例如用来定义整个软件生命周期过程的IEC 62304标准。

多核设备是满足上述需求的关键性途径。这些设备如今已经进入嵌入式市场，能够满足这些行业市场领域未来5到10年对性能和功能支持的需求。不过，他们仍然延续了PC和企业应用领域的商用化操作系统和企业软件，同时带来了原本就是由PC和企业市场所驱动的成本压缩和集成化。

使用多核处理器内核可以将现有的双硬件板架构集中化为单个硬件板，将其中一个内核用于关键安全软件，另一内核用于其它非关键安全功能。

以Hypervisor实现系统集中化

尽管从理论上可行，但是这种“裸机（bare metal）”方式下的系统设计需要大量的时间和成本，同时还要求经验丰富、人数众多的设计团队。另外，这种方式还需要提供数千行的测试和验证代码以便进行安全认证，而在整个认证过程中开发和运行这些代码将耗费大量的时间。

随着新功能的引入越来越快，安全相关软件的认证逐渐从“使用中才被验证”的模式转变为更规范的面向工具的模式。这也许是当今市场中最大的变化，导致开发人员不确定如何才能适应这些改变，也不确定他们所投资的软件和相关工具在扩展到第三方软件组件时还能通过认证。FDA规定,要达到预上市许可应用的标准和要求，就必须拥有科学有效的依据来支持，说明设备的安全性和有效性不是空中楼阁。要对现货型软件进行验证，其代价是非常高昂的，而且会导致生命周期中的不可预测性。

上述因素推动了Hypervisor这类新的软件解决方案的出现。Hypervisor可以在同一平台不同内核中运行不同的操作系统，使系统设计人员能够利用更广范围的第三方软件，同时保留已有的关键安全软件的应用程序。通常，可以用一个专用处理器运行关键安全软件，而其他处理器运行风河VxWorks等实时操作系统或者Linux之类等通用操作系统。在同一系统平台或者处理器上实现不同关键等级，就需要将现货型软件与VxWorks等专门用于设备安全认证的实时操作系统结合起来。

集中化平台的发展推动了操作系统平台的多样化。VxWorks这种实时操作系统的优势是比Linux这类非实时操作系统具有更高的确定性和更低的复杂度，是实现安全认证的理想选择。Linux则能够在快速实现客户通讯标准或图形用户接口方面具有更大的优势。因此，在同一系统平台中使用两类操作系统可以同时发挥它们各自的优势。通过全新的Hypervisor整合技术，让这种架构方式成为现实。

支持和商用化验证对Linux至关重要

随着越来越多的设备制造商采用Linux操作系统，系统的支持问题开始显现。虽然也有一些相关的技术和较好的开发工具可用于实现集中化，但支离破碎仍然是基于Linux解决方案中存在的最大问题。

制造商们经常试图利用Linux免费版本来东拼西凑，而放弃通过验证并附带技术支持的商用化产品。但是，他们完全低估了Linux的复杂性和业务开发可能面临的挑战。Linux培训、更好的稳定性、符合开放标准、知识产权的保障、完备的文档和可扩展性，这些只是选择专业化管理之下的商业版本所具优势的一部分。因此，在做决策过程中

应该仔细考虑这些因素。

使用Linux的一个重要用途是能够对单一硬件平台内同一应用中的安全关键功能和非安全关键功能进行分区。Linux带来的功能性和新型中间件具有强大的价值潜力，但在安全性需求的环境中却带来了新的复杂度。Hypervisor技术能够实现Linux和实时操作系统在软件层面的集中化，使安全性和非安全性应用可以在同一硬件平台上运行。多核处理器技术和Hypervisor技术的结合使多操作系统在同一硬件平台上并发运行，同时确保隔离和保护。

在同一时间内，安全关键任务可以在通过安全认证的VxWorks实时操作系统中运行，而通信协议则可在VxWorks或Linux甚至其他操作系统中运行，从而在同一设备内实现了Supervisory功能。Hypervisor技术还简化了原有遗留系统的迁移，因为分区架构使同一操作系统的不同版本能够并发运行，因此原有代码无需改变就可以运行，而新代码则可以充分使用新版本操作系统中的全新功能特性。集成服务可以进一步帮助客户消除安全性和集中化项目中的风险，确保产品开发的顺利和可预测性，极大地加快投资回报周期。

安全关键医疗设备系统中的另一重要问题是，使用多操作系统后，在必需使用分离开发工具套件时会造成巨大的困难，从而使开发进程变慢，并且导致更多的程序缺陷和风险。此外，这种情况下还需要完成由FDA设备与放射线健康管理中心所规定的更多软件认证和验证，这就使设备制造商不得不进行这些测试工作，从而耗费更多的投资和时间。

取而代之，可以采用集中化化开发工具套件，例如基于Eclipse开放框架的Wind River Workbench，全面顺应多操作系统架构的发展趋势，使各种面向不同操作系统的应用可以在同一时间、同一环境下完成开发。根据开放的概念，使用统一的测试和静态分析工具，可以为开发团队带来巨大的优势。Eclipse框架的高度开放性，使更多其他工具可以与之集成，从而成为设备开发人员成功的得力助手。

工业应用市场的同类需求

工业应用市场可以细分为6大独立领域——医疗设备应用、交通基础设施、工业控制、测试与测量、能源输送和汽车制造，而且这些领域都面临着非常类似的挑战。它们都要求重要的安全关键系统，并且必须达到严格规定的各种安全标准。

上述领域都有很多相似的需求。例如，在工业自动化领域，出现了大量的分布式控制，复杂度也不断增长，需要能够更快速构建新工厂或工区并保持其灵活性，同时还要确保质量和安全性。同样，在工业控制领域，机器人技术的出现带来了很多变化，需要在机器人和控制单元之间采用近场通信技术来提升系统正常运行时长，确保操作的安全性。另外，设备中需要采用相应的工具来集成通用PC软件，例如文件报表或者Internet访问等，同时还要提升与其他设备连接的安全性。

结论

通过多核硬件、设备安全认证专用操作系统、Hypervisor软件和集中化开放开发工具的组合，能够完全支持并满足医疗设备系统设计人员的需求。这一系列领先技术将帮助设计人员和系统架构师实现硬件集中化、降低开发成本、加快产品上市速度，与此同时提供了能够在软件中加入更多新功能并提高产品安全稳定性的平台，而且会尽可能地重复使用原有遗留代码来构建和维护安全认证的系统环境，这一切都是下一代安全关键医疗设备与工业领域系统开发的关键要素。

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