WIND™

通过软件三步实现医疗设备安全

Jens Wiegand
风河工业和医疗解决方案部总经理

概要

医疗设备的开发人员如何在给产品增添新功能的同时又让它们能够符合相关的安全标准呢？他们该如何在不违反认证标准或不卷入产品责任诉讼的前提下充分利用像多核处理器和嵌入式虚拟技术这样新的软件技术呢？他们该如何应对日趋复杂的开发和测试流程及兼容问题时，又控制好成本和产品上市时间呢？

对的软件平台，加上对的开发工具，再配上正确的使用方法，就能够在既定的时间和预算上，为通过最严苛的安全认证标准做好万全的准备。这篇文章阐述了设备厂商该如何通过三个步骤做好这样的准备。

监管问题

人类的生命安全需要仰仗医疗设备的安全性，这就是为什么在医疗设备的开发中安全性始终是首要考虑的因素，也是为什么开发人员（和监管人员）会在安全问题上慎之又慎。但由于越来越多与安全相关的功能都通过软件实现，而软件技术和开发过程正日趋复杂，因此安全认证也变得难度更大、耗时更长、花费更高。

今天的嵌入式软件技术能够在符合安全认证标准的前提下，降低不断上升的开发成本和复杂性。

软件已经成为医疗设备厂商们一较高下的重要武器。嵌入式软件已经成为包括CT扫描仪、X光机、透析机、医学成像系统、血液分析仪、重症监护呼吸机、共聚焦显微镜系统和清洗装置等在内的众多医疗设备的必需品。

软件的重要性和其对设备安全性的影响同样也是设备监管的必备考量因素。尚未采用稳健的软件开发流程的厂商，在面对未来即将出台的一系列新法规时将感受到更大的压力，而那些已经在努力符合现有的包括医疗产品设计标准IEC 62304、功能安全标准IEC 61508、电磁兼容性标准IEC 60601-1-9和医疗设备风险管理标准ISO 14971等在内的各类认证标准的设备厂商也会发现他们即将面临全新的挑战。

美国食品与药品管理局（FDA）推行的上市前和上市后两种审核标准造成了很大的困扰。FDA的上市前审核标准要求必须有有效的科学证据表明该设备的安全性和效力，通过审核的设备就可以投放市场，但假如该设备在使用过程中发生问题，就必须从市场上撤回并需要再次经过审核，而那时的审核标准已不是它当时上市前使用的那个标准了。也就是说，通过认证能让你的设备上市却不一定能保证它永远不出问题不被下架，因此对设备厂商来说他们需要承担产品责任上的巨大风险。

相对的是，那些在医疗设备软件的生命周期里不断推陈出新的标准和规范（例如IEC62304），却未必能与时俱进。因此许多医疗设备厂商觉得他们应该仅设法做到符合严苛的认证标准，并降低可能的风险。

设计难题

医疗系统和软件的开发流程的日趋复杂化让问题变得更加扑朔迷离：

·据统计，智能设备中的软件数量正以每两年翻一番的速度在增长。

·在嵌入式领域，有许多产品在一台设备上使用32位和64位多处理器架构并同时运行多个操作系统。

·迭代或“敏捷”开发取代了一整个周期的传统开发模式，它将整个开发工作分割成一系列短小的小项目，并根据不断调整的开发需求进行不间断的测试。

认证标准

- IEC 61508：电气、电子和可编程电子安全相关系统的国际标准，旨在确保系统的设计、配置、操作和维护都符合安全完整性等级（SIL）
- ISO 14971：帮助厂商识别医疗设备风险的标准
- IEC 60601-1-9：医疗电气设备的环境意识设计的国际新标准
- IEC 62304：医疗设备软件的生命周期要求的标准

由于越来越多的功能要依靠软件来实现，开发人员致力于在不违反安全认证标准的前提下将过去零散的旧式工具和开发流程与新的工具和技术。例如，在许多设计中，软件的一些部分必须保持原样以具备符合安全认证标准的功能，而其他一些部分则可以在保证让硬件符合安全标准的前提下增加些新特性、功能和创新。

技术融合是降低成本和简化流程的传统途径，但对医疗设备厂商而言情况会更复杂一些：

·需要通过IEC 61508标准的产品如要进行技术整合，就需要再次认证，那么重新认证和重新上市都需要花额外的时间和金钱。

·对有线（以太网）和无线（蓝牙，无线局域网）网络连接日益增高的要求对通信栈的互用性提出了更大的挑战。

·多供应商都有一个庞大的（需要维护的）旧版应用程序库，他们需要找到一个新方法既能创新又不会浪费之前的投入。

接下来我们来看看如何应对这些重重挑战。医疗设备厂商可以通过以下三步借助新嵌入式软件方案的力量来降低成本、简化流程、符合相关安全标准并获得新的竞争优势。

第一步：多核与嵌入式虚拟化技术的整合

多核处理器和嵌入式虚拟化技术作为嵌入市场的两大发展，为那些希望从技术整合中获益的人提供了一个能够符合安全标准的切实解决方案。

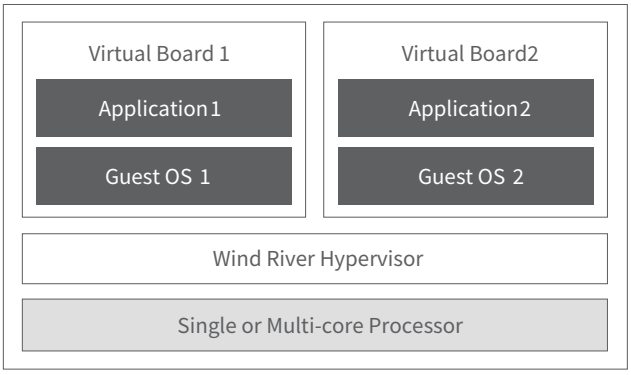
最新的多核处理器与原有的单核处理器相比，在整体性能和能耗比上都有了显著提升，且因为多核可随时满足未来更高的需求，从而提高了程序的可扩展性和软件投资的价值。多核已经是大势所趋，且多核优化操作系统、中间件和各类工具都已经应运而生。借助最新的多核架构和虚拟化概念，医疗设备厂商能够在一个通过安全认证的聚合平台上运行多个操作系统，从而拥有一个低成本、多功能的稳定平台。

而虚拟化这个概念则能让厂商在同一台设备上运行数个互为独立的操作环境—例如，完全可以在同一台设备上同时运行一个像风河开物RTOS这样的实时操作系统和一个类似Linux这样的通用操作系统。这样的独立或者说分割—使得资源的分配更加灵活。例如，既可以将处理能力只分配给一个虚拟主板也可以将其平均分配到多个虚拟主板；通过这种分割，每一块主板都拥有独立的内存空间，且不会影响到其他的虚拟主板。虚拟化技术还能将安全性相关的功能（如soft PLC）与其他功能分隔开。

多核处理器和嵌入式虚拟化技术帮助医疗设备厂商在更少的系统上整合更多的功能、削减成本、简化流程从而腾出更多的精力来努力达到各种严格的安全和监管认证的标准。

第二步：将开放平台标准化

随着人们对嵌入式软件的区分的关注度越来越高，将硬件平台标准化的能力成为考量医疗设备厂商的关键因素。



虚拟系统

例如，实时内核在可编程控制器中的使用现在已经很常见了，而技术融合与整合正顺着价值链不断向上发展，设备厂商要依靠软件来为他们创造一个安全、互联的环境，他们已经准备好将功能进行整合，但还需要很多软件层面的支持。

与此同时，安全问题也在顺着价值链向上攀升，更多的人开始寻求与嵌入式软件开发工具、操作系统和中间件供应商的战略合作。随着系统框架变得越来越开放和标准化，厂商们可以很顺利地将一系列子系统集成在一起。

这些趋势或许还能帮助厂商们解决产品生命周期的问题。通常情况下医疗设备的研发周期在两到三年左右，而上市周期最长达到八年—另外还需要十年以上的技术支持。而这样有时长达二十多年的产品生命周期在经历频繁的升级后可能会延续更长的时间，也就必然需要供应商更强有力的支持。

设备软件供应商能够帮助他们的客户解决此类问题，比如在降低使用成本的基础上保护市场份额和知识产权并缩短产品上市时间。举个例子，模块化的软件方案能解决上市时间的问题但可能会导致对UDP堆栈这样的模块的重复认证带来的高昂费用。而通过模块化认证，标准软件组件可作为认证包中的一部分成为一个受信任的组件，用户可以用这个认证包来应对IEC 61508标准认证，不仅能更快地通过认证，并且能在设计阶段提供更大的灵活性，也为业务带来更大的可预见性。

随着众多设备厂商都开始考虑使用Linux，技术支持开始变得愈发重要。Linux的复杂性和目前面临的难题都被大大低估了，太多厂商没有使用带技术支持的正版商用Linux系统，而仅用免费的Linux系统来胡乱凑数。系统使用的培训、系统的稳定性、开放标准、赔偿保障、文件归档和可扩展性—这些只是专业正版Linux系统的一部分优势，也是您在决定是否购买正版Linux系统时需要考虑的因素。

借由模块化的认证，标准化软件的组件即可成为认证的一部分，客户就能够依此作为通过IEC 61508标准认证的依据。

开放技术与嵌入式虚拟化技术和多核理念一起创造了各种强大的新功能。例如，使用Linux的一大优势就是能够将一个硬件平台中的某个程序中的安全相关与非安全相关的部分分隔开。作为一个开放式操作系统，Linux为潜在的新特性和新的中间件提供了发展空间，这在保证安全的前提下就提高了复杂性。虚拟化技术使Linux和实时操作系统在软件层面实现整合，让安全相关和非安全相关的程序能够在同一个硬件平台上同时运行。多核处理器技术与虚拟化技术使同一个硬件平台上的多个操作系统可以各自在互相独立的、受保护的区域内同时运行。

第三步：创建一个能支持未来变化的基础

软件过程总是被看成一个问题而非一个解决方案，主要原因是每个软件的开发都需要用专门的工具和技术，过程极其复杂。

标准化的开放平台会会提高软件开发过程的适应性，并使之能应对未来的发展变化，但我们仍需要一个能支持各种要求与快速变化的安全认证标准的框架。

确切地说，就是要找一个集操作系统、安全解决方案和各类中间件于一体的东西作为一个稳健的商用现货（COTS）基础。

一个灵活轻便的软件平台有助于在不浪费已投入成本的情况下充分利用新技术。例如，它能让您用虚拟化技术在软件层面整合Linux和实时操作系统，让安全相关和非安全相关的应用程序在同一个硬件平台上运行；它能让您把嵌入式虚拟化技术和多核技术结合起来，使多个操作系统能在同一个硬件平台上（在独立分割的受保护的区域内）同时运行；它还能让安全关键任务在VxWorks这样的实时操作系统中的认证应用程序中运行，同时让通信协议在VxWorks或Linux下运行，实现对该设备的监控功能。

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：0755-2533431
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