WIND RIVER

在医疗设备开发设计时，软件设备的安全一直是人们关注的焦点，现在，一种新的研发方法已经初露端倪，将会大大加快医疗设备革新的步伐。

Jens Wiegand

伴随着科技的发展，医疗电子学正在悄悄地发生着根本性的转变。传统的医疗设备技术已经沿用了 20 年，背后酝藏着许多珍贵的科技遗产和大量辛勤测试，而如今社会为了使更多的医院和诊所能够广泛地应用到最新的医疗设备，于是对医疗设备的性价比及数字化应用都提出了更高的要求。

而这种研发思路的改变，意味着现在越来越多的革新将朝着软件革新的方向发展，这给素来以安全性为第一要素的医疗设备设计带来了巨大挑战。医疗设备的软件设计中，任何一个小小的错误都会造成极严重的后果，所以设计师们在软件革新时为确保运行安全必须保留软件中的一些元素，而其他部分则可以加入新的功能和创新。同样，硬件设备也需要伴随着软件的更新而进一步升级，这样才能更好的配合各种软件在抗干扰性和危险评估上的不同标准。

设备系统的安全问题一直是整个软件研发过程中的关键，有着许多前人为我们遗留下的宝贵经验，但该领域的革新成本很高，很难利用电子系统的一些重要变革成果直接为生产服务。鉴于市场的反应性较慢，且长期维护的费用偏高，导致了软件安全技术一直处于孤立、零碎的不良发展状态。

多核处理器和新管理程序技术的出现为市场注入了新的活力，也为硬件和软件设备升级更新奠定了坚实科技基础，有助于推进医疗设备的革新，加强了安全保障。这不仅对医疗设备领域具有重要意义，对工业控制、自动化等其他行业也有着重大影响。

工业行业在过去只在乎设备的功能性，但现在设备安全、质量、可维护性和性价比也越来越得到人们的重视。伴随着适用于所有工业部门的 IEC61508 安全标准及其附属条款的出台，越来越严格的安全标准给各领域的企业带来了新的挑战——如何让设备在即不违反安全标准的条件下仍然保持优秀的功能性。

如今医疗领域对一些复杂的诊断设备，如 X 射线、CT 扫描仪和透析仪等使用已经逐渐变得普遍。使用者往往希望这些设备能够具备自动报告生成和联网等功能，从而一定程度上降低医院行政成本。

为了满足 IEC60601 和 ISO14971 等标准对设备的电磁适应性或风险管理的要求，以往这种设备技术上的革新，必须要将内部程序在系统中的不同控制平台上进行，即在一个控制平台上只执行关键程序，而往往这个控制平台根本不安装操作软件或只配备简单的、已被认证安全的老软件，从而确保关键程序的运行安全；而其他对安全性影响不重点的功能，如：档案管理和联网等则由另外一个控制台所控制。

以前这套双控制台的体系能够很好地完成任务，但随着现在不断有新的行业标准增加，新型医疗设备也更加强调成本和占用空间，使得以前那套双控制台的方法已经不再具有可行性。现在，任何软件在改进新功能的时候都要考虑到其相应的安全问题，比如软件设备必须符合 U.S 食品药品管理局制定的与安全有关的重要标准，以及欧洲 IEC6230 标准对软件使用周期进行的各种限制。

多核化技术是解决以上问题的关键。这种技术现已逐渐在市场上被应用，多核化技术可以有效地满足工业市场在未来 5 至 10 年内的需求。当然，这种装置的成功是离不开近些年商业运营系统和应用软件借助个人电脑和企业市场所完成的革新，它为降低成本和系统整合做出了贡献，也有效地推进了多核化自身的发展。

使用多核处理器可以将目前存在的双控制平台结构转变成简单的单控制台结构。所谓多核就是用一个核来处理与安全相关的软件，其它的则用来操控另外的非关键功能。

尽管理论上来讲这套系统的功能很容易理解，但这种‘硬盘安装式’的整合方法在实际操作中有着相当高的技术难度。成熟的多核化技术，需要相当长的时间和很高的成本，以及拥有丰富经验的开发团队，而且多核化技术还需要通过上万次的测试才能完成安全检测，通过认证获得验证码。

随着越来越多的新功能引入，这套软件的安全认证正在从‘边用边测试’的模型转变成更加规范的‘工具向’形式。这种设计思路的转变也深深地影响了软件销售市场，很多开发商们不清楚怎样去应对这种变化，以及他们在软件和相关工具方面的投资是否可以在这股改革潮流后依然能够得到保障。食品药品管理局制定标准和要求中明确指出：工业用软件上市前必须提供相应有效的科学证明来接受检查，在确保装置的安全和性能后方可流入市场。但相关的成品设备软件取证成本可能会较高，而且频繁的安全标准检查也将造成软件使用寿命的不可预测性。

于是新的软件管理程序解决方法应运而生，该技术允许不同的操作系统能够在同一平台上多核运转，大大拓宽了使用者在第三方软件上的选择面。通常，需要高度安全保障的软件采用的是专用处理机，而其他程序使用的是如 Wind River VxWorks 操作系统或者是 Linux 操作系统。即使在同一系统平台上使用相同处理器，根据安全系数不同，也需要将现有软件与便于用来认证装置的实时多任务操作系统 (如认证的 VxWorks) 所相结合。

不同客户对操作平台性能有着不同的要求，要想达到最好的效果就需要根据侧重点的不同使用不同的操作系统平台。例如实时操作系统 VxWorks，与传统的非实时操作系统如 Linux 相比，在确定性和降低复杂性方面显得更有优势；而相反 Linux 则在大量快速通讯的场合以及图形用户界面两方面上独具优势。两套软件分别是各自领域的佼佼者，那么想要获得最佳的管理效果的唯一办法就是在同一台设备里同时使用这两套操作系统。而实际操作起来，远没有说着这么简单，这种跨系统操作需要极高整合技术，而新的管理程序则将这一切变成可能。

现在有许多设备制造商仍是 Linux 的忠实客户。但是有些问题却被人们忽视了，那就是虽然有一些很好的开发工具在不断地改善着 Linux 平台， 但在目前市场上以 Linux 为基础的技术平台中仍然存在大量的不足。

在软件销售市场上，Linux 的复杂性和商业风险完全被低估了，制造商们通常会随意选择免费的经销商为其提供服务，而不是认真制定可对他们生产及推广真正有帮助的软件经销商。而客户选择一个专业的经销商不仅有利于指导自身更好地掌握 Linux 软件、得到稳定的经销渠道，还能够及时改进以适应市场需求。有利于赔偿金索取、文件搜集，从而使决策层可以对软件性能更准确做出某项决定。

Linux 系统软件的一个重要组成功能就是可以在一个硬件平台上分别同时操作安全性紧急和非紧急的软件。Linux 系统给予了软件中间商相当多的自由空间，所以相应的风险也有所增大。而管理程序技术保障了 Linux 和实时操作系统软件层的更好运转，使安全和不安全的指令都能在同一个硬件平台上运行。总而言之，多核处理技术结合管理程序，使多个操作系统同时在同一平台上的不同区域内兼容运行。

管理程序软件可以使各个操作系统在同一台设备上共同工作，我们便可以利用 VxWorks 的高安全性，在 VxWorks 这样的实时操作系统执行安全任务，然后再通过 Linux 或其他操作系统来执行其他通信任务。管理程序技术还可以很方便地将其中一个系统里的软件转移至另一系统，因为这种控制平台架构允许相同的操作系统的不同版本同时运行，在使源代码运行不变的前提下，新代码也可以在新的环境平稳地运行。另外，良好的集成化售后服务也可以保证用户不被系统安全更新问题和市场前景等问题所困扰，这对保障项目的安全和维护用户的权益都起到了相当大的作用。

但是在一个系统中使用多种操作系统必然会产生一些技术上的难题， 有时候必须使用独立的工具链来解决。这就可能会造成研

发进度的减缓以及加大产生 BUG 的风险，而在特别强调安全性的医疗设备软件里，这种风险绝对是要避免。为有效防止问题的产生，制造商们必须参加由 FDA (放射卫生设备中心) 提供的各种繁多的软件安全验证和测试。只有通过了这些既昂贵又耗时的测试，制造商才可将产品正式投入市场。

相反，一种基于 Eclipse 开放架构的新型整合工具链 Wind River Workbench 应运而生，这种技术能够允许在同一开发环境下对使用不同操作系统的应用程序同时进行开发或操作。这种开放的架构概念使得在多核系统中运行整体测试或静态分析工具成为了可能，同时为软件开发团队带来了巨大的便利。另外 Eclipse 架构的这种独特的开放性，使得其他工具框架与它结合起来相当方便，而这种“兼容”的理念潮流也正在成为仪器开发商们研究的新重点。

总而言之，整个工业市场可以被看作由 6 个有着非常类似要求的独立产业组成的：医学应用、交通基础设施、工业控制、测试、测量、配电和汽车制造。它们有着非常相似的特征，从对关键系统安全性的依赖到一系列必须遵从的执行标准来说，所有这些领域都有类似的需求。例如在加工自动化领域，首要难题是如何更好地进行流水线控制系统以及如何面对整个工程不断增加的复杂性， 还有如何在保证质量和安全的前提下更快地建造和维护新的工厂。而在工业控制领域，机器人技术的出现大大增加了行业内部的差异性，但同时通过机器人控制端与其所属的受控单元方便的联系，更加保证了整个操作的安全性。同样地，制造业里的流水线机床也和其他设备一样，急需兼容常见 PC 软件，并在新添加文件报告和互联网接入系统后，同时加强与其他设备的通信安全。

综上所述，开发商所需的理想医疗系统就应该由以下几方面结合组成，即多核硬件设备、专门为快速通过设备安全认证而设计的操作系统、管理程序软件和开放式架构的工具链。这个组合能够帮助设计师和软件工程师们最大限度地利用系统进行资源整合、在降低软件开发成本和硬件产品上市成本的同时，为广大用户提供一个安全、稳定的平台来进行软件创新、系统环境保障。另外更妙的是，通过多核化这种开放式的系统架构，使得工程师在新系统上重新使用上一代有用的代码也成为了可能，毕竟，这些前人工作的成果对研发新一代安全级别的医疗和工业体系仍然具有至关重要的参考价值。

➢ 关于风河系统公司

风河系统公司 (Wind River) 是全球领先的设备软件优化 (DSO) 提供商，也是业界唯一提供面向行业市场的设备软件平台的厂商。DSO (Device Software Optimization，设备软件优化) 是一套帮助电子制造厂商快速开发设备软件并提升可靠性的工具和方法，并且可以让这些软件的开发成本大幅度降低。同时，软件可靠性的提升将会大幅度降低产品的维护成本。

风河所提供的设备软件平台包括集成化的实时操作系统、开发工具和技术。风河的产品和专业服务已经在许多重要的市场领域得到认可，主要包括空间及国防、汽车电子、消费电子、工业设备和网络基础设施等领域。世界各地的电子设备制造商普遍把风河公司的设备软件产品作为行业标准。包括 NASA 的“勇气号”火星探测器和波音飞机等在内的航空航天设备也普遍采用风河的设备软件。提高产品可靠性，加快产品上市速度是风河公司一贯坚持的企业理念。

风河公司成立于 1981 年，总部位于美国加利福尼亚州 Alameda 市，在全球各地设有办事机构。
关于风河的更多内容，请访问：http://www.windriver.com

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

同步关注风河新浪官方微博，关注 **@风河系统公司**

WIND RIVER

风河（Wind River）公司是Intel(NASDAQ: INTC)的全资子公司，也是全球领先的嵌入式和移动软件提供商。从1981开始至今，风河公司一直是嵌入式设备中计算技术的先锋。在当今世界中，已经有超过10亿台产品应用了风河公司的技术成果。公司网站 **www.windriver.com** 和 **http://www.windriver.com.cn/**