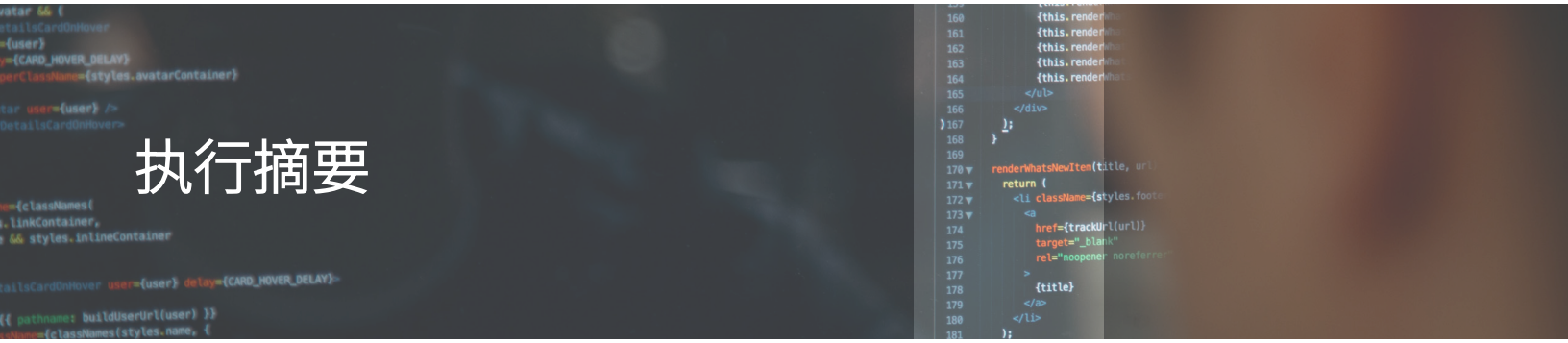
基于容器技术的嵌入式解决方案实践

为嵌入式软件开发和分发带来可移植性、安全性和可管理性

WNDRVR



执行摘要

嵌入式软件开发实践正在发生重大变革，以应对持续的软件生命周期维护和关键安全问题的复杂性。这些挑战引起了众多行业领导者的关注，他们努力推动并确保简化的开发和部署方法的实现与安全性。

互补技术推动了这些变革。这些技术的发展源于边缘计算、自主车辆、用于远程诊断和治疗的医疗设备、机器人技术、航空航天进步以及随着移动宽带和毫米波微蜂窝安装的普及而不断增长的5G技术需求。

采用云原生工具进行开发使团队能够在全球范围内协作。容器通过共享一个具有可重复使用配置的通用环境来实现这一点，用于开发和部署代码。使用容器的一个优势是，它们既适用于现有的嵌入式应用程序，也适用于新设计。无论是开发嵌入式程序还是面向企业的程序，应用程序开发者都可以使用他们熟悉的工具部署用Rust和Python编写的软件。这可以看作是一种“编写一次，随处部署”的方法。

实时操作系统（RTOS），尤其是风河开物RTOS，是嵌入式系统的基础。在风河开物RTOS中引入对容器的支持，以系统地交付和更新软件，这是具有变革性的。对容器的支持可以以实时、确定性的方式动态响应环境中的事件，这是创建软件定义世界的重要且创新的元素。这对于自动化生产线、自动驾驶车辆操作、航空航天应用以及医疗设备来说尤为重要，因为这些领域的数字化转型正在加速推进。

由于嵌入式行业对容器技术优势的认知不足，其采用在一定程度上滞后。此外，将现有解决方案围绕虚拟化（虚拟机）实现作为标准进行整合也阻碍了采用。另一个障碍是对共享内核相关的安全问题的担忧，这可能导致连接到同一主机的应用程序之间的普遍漏洞。最后，由于缺乏熟练的技术人员和开发人员，以及用于实现嵌入式用例的容器解决方案的工具和专业知识，其采用受到阻碍。

正如本文所讨论的，这些问题已经通过多种方式得到了解决，而容器在支持创新嵌入式应用程序方面的多重优势为支持其创建和分发的不断发展的软件架构提供了光明的未来。

揭开容器技术的神秘面纱

容器化技术能够创建一个标准化的软件组件包，包括所有必需的配置文件、库和工具集合，从而使应用程序能够在指定的环境中运行。Linux和风河开物RTOS的容器可以放心地部署在不同的硬件环境和内核版本中。通过共享操作系统内核，容器保持了轻量化和易于管理的特点。这简化了代码的管理和更新，因为在将容器部署到系统中时，无需每次分发操作系统的最新版本。

容器格式与编排

Docker普及了容器的使用，通过工具使任何人都能够轻松构建和分发镜像。2013年发布为开源后，最初的开发者与社区合作，基于其工作成果制定了标准化规范。

标准化推动了容器的采用，扩展了在多个架构之间的互操作性。开放容器倡议（OCI）为容器开发者列出了三项需要遵循的规范：

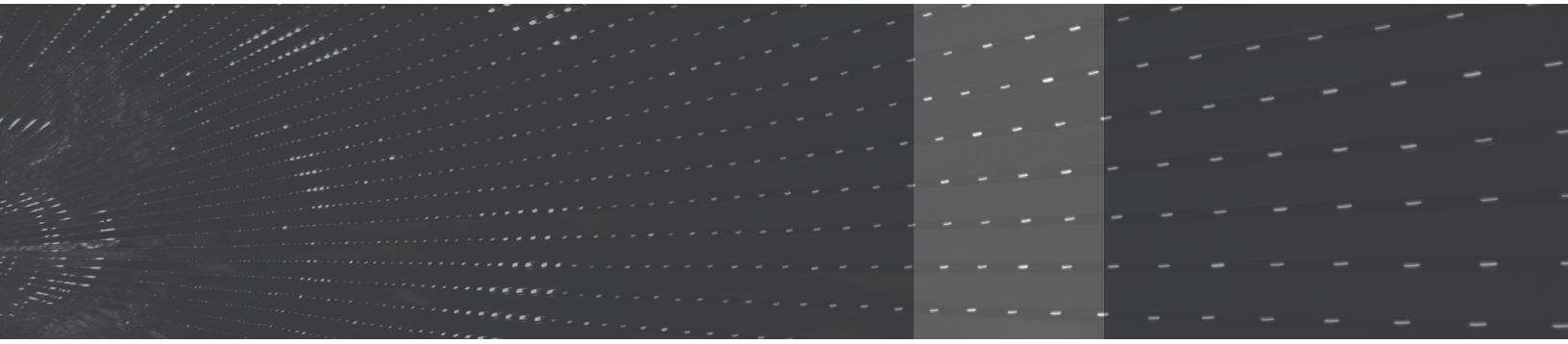
1. 镜像规范：定义了容器镜像，本质上是存储在注册表中的文件系统包，主机可以从中检索这些镜像。
2. 分发规范：提供了一种定位注册表中镜像并下载的方法。
3. 运行时规范：规定了解压镜像内容的规则，即容器运行时将使用的文件系统包。

风河开物RTOS支持这些规范，使得可以使用通用格式和工具来开发和部署容器。风河开物RTOS的容器化工作负载甚至可以由 Kubernetes 控制，以实现跨设备的容器编排。

通过 Wind River Studio，容器的编排可以扩展到管理运行风河开物RTOS的大量设备。例如，可以在 Kubernetes 中配置风河开物RTOS应用程序的软件升级并自动应用。

> “容器技术为您打开了世界，同时强化了安全性并实现了组件的复用。容器还促进了 DevSecOps 的采用，使你的软件更加模块化和灵活。”

—Nicolas Chaillan, *Ask Sage 创始人；前美国空军与太空部队首席软件官*



容器内有什么?

通常，容器与云中部署微服务相关联。然而，容器也可用于部署传统服务和应用程序。风河更进一步，为风河开物RTOS中的嵌入式软件容器化提供支持。

容器从定义上将一组模块化、互联应用的关键元素整合为一个统一的解决方案。其理念是通过许多较小、独立的模块构建大型软件应用程序，如图1（第5页）所示。这种方法利用了经过验证的开源工具、框架和软件，从而加快软件开发速度并降低成本。此外，它还打破了构建单体、不灵活软件应用程序的传统做法，这种做法往往难以创建和更新。相反，这种模块化方法具有可移植性、轻量级操作和敏捷性的优势。这些特性对于支持现代架构至关重要，包括汽车设计中使用的云原生架构和面向服务的架构。风河在风河开物RTOS和Wind River Linux中均支持容器，以构建基于云原生原则的下一代架构，覆盖多个行业。

容器在不同行业中的应用领域

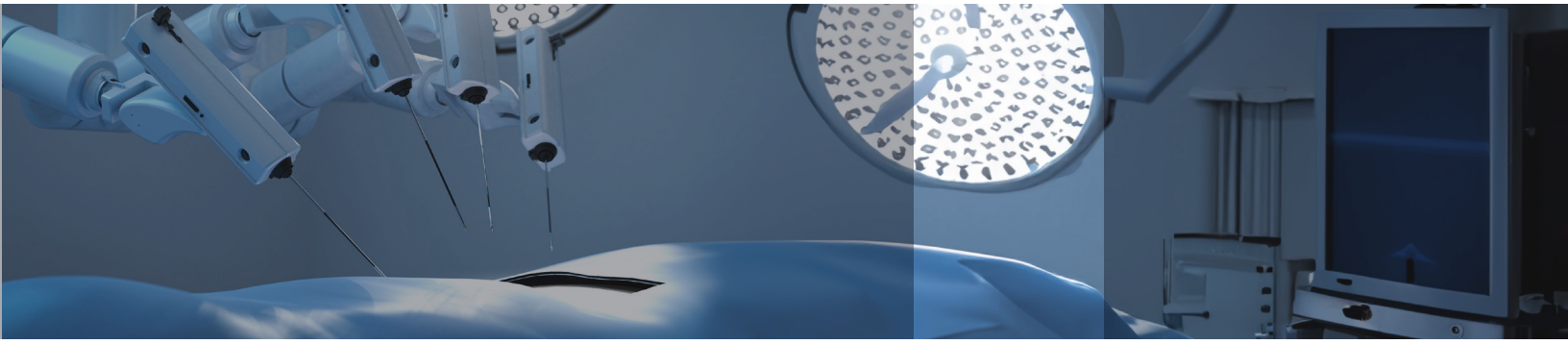
容器非常适合应用于嵌入式软件起重要作用的许多垂直市场，包括：

- **航空电子：** 对于希望优化空间、重量和功耗（SWaP）的商用和军用航空电子公司来说，容器化具有变革性意义。能够将应用程序运行在独立的容器中，而无需依赖底层堆栈，这不仅提高了可移植性，还允许将打包为容器的旧版软件在新系统中重复利用。主要用例包括飞行数据分析、飞行管理系统、3D驾驶舱显示、用户界面、机上娱乐系统和飞机系统监控。

- **汽车：** 容器技术在汽车领域的应用是最具前景的发展之一，特别是在支持自动驾驶和软件定义车辆方面。这种新方法虚拟化了车辆设备，并将多种功能整合到单一硬件系统上。由于模块化和兼容性，容器的概念被用于以更快且更安全的方式进行空中功能更新和升级。容器化的工作负载还可以支持其他用例，例如车载信息娱乐系统、联网汽车服务、实时诊断警报、预测性维护、车队管理、分析和车载远程通信数据。

> “容器化为行业带来了三大急需的优势。首先，它让您能够管理如今单体的软件。其次，它降低了开发成本。第三，容器通过软件相关收入解锁了新的盈利模式。”

—Glen De Vos,
Aptiv公司转型与特别项目高级副总裁



- **工业：**随着工业4.0变革席卷市场，工业领域正在经历转型。通过在单一或分布式系统上运行安全、隔离的容器，可以将工业应用整合到更少的系统中，从而提高可扩展性，简化部署并增强系统更新能力。这还确保了具备预测性维护、AI驱动的机器人和协作机器人、生产线自动化、供应链运营和物流、增强现实、虚拟现实以及控制系统等更新和升级的前瞻性架构。

- **电信：**容器使顶级服务提供商能够部署并安全地更新5G和即将到来的6G网络。一家全球领先的电信设备制造商正在使用容器实施5G网络切片计划，以支持具有不同性能需求的应用，例如增强现实和虚拟现实。配备毫米波功能的5G基站通过容器在智慧城市环境中分发软件，并确保安装了最新的软件补丁。网络工具，例如防火墙和负载均衡器，也可以通过容器实现。

- **医疗：**在高度监管的环境中，设备的高可用性关乎生死，通过在底层安全认证操作系统上运行容器化的工作负载，可以实现应用程序和数据的关键环境隔离。通过容器增强的用例包括远程患者护理、健康监测、成像系统、输液泵以及手术和机器人系统。这些应用可以利用容器来提供安全补丁和关键软件更新。目前正在开发完全自动化的手术机器人，可以在没有人工干预的情况下完成整个手术。

随着容器技术的成熟，其潜在的应用场景几乎是无限的。

应用隔离提升安全性和可靠性

容器通过隔离应用程序及其运行时操作来提高安全性，避免冲突，并实现管理控制。常见的隔离技术包括使用命名空间来控制对系统资源和功能的访问，并限制分配的数量。容器有时使用覆盖文件系统共享公共文件，但会将任何本地更改保留为私有。

风河开物RTOS对其实时进程（RTPs）如何访问内核对象、查看文件和目录以及与内核资源交互具有细粒度的控制。通过限制对系统调用的访问，可以将应用程序彼此隔离，并为其提供一个私有的沙盒环境。文件系统命名空间提供了文件系统的独特视图，允许容器化应用程序独立管理其库和配置。其覆盖文件系统通过重用具有通用基础映像的容器，在不互相干扰的情况下实现了更小的占用空间。风河开物RTOS丰富的网络功能——源自其在电信领域的历史——也使其能够控制提供给应用程序的网络接口及其可通信的端点。

容器提供了额外的安全加固，尤其是在与其他安全措施相结合时。这在容器安全至关重要的嵌入式环境中非常有价值。例如，安全启动技术通过验证从硬件信任根到引导加载程序和内核，再到签名容器和应用程序本身的全部软件组件，建立了一条信任链。将容器安全与安全启动结合起来，为设备上运行的软件提供了端到端的信任链。

混合关键性组件的集成

在某些情况下，容器部署使用高级编程语言或无法认证的开源软件开发的软件。这导致容器具有不同的关键性级别。成功集成这些组件，明确已达成的认证或获得的合规性，可以帮助避免重新进行某些认证流程。通过根据关键性级别隔离组件，可以充分利用敏捷开发实践和DevSecOps工作流程，同时保留简化开发的优势，并维护专用组件的现有认证。

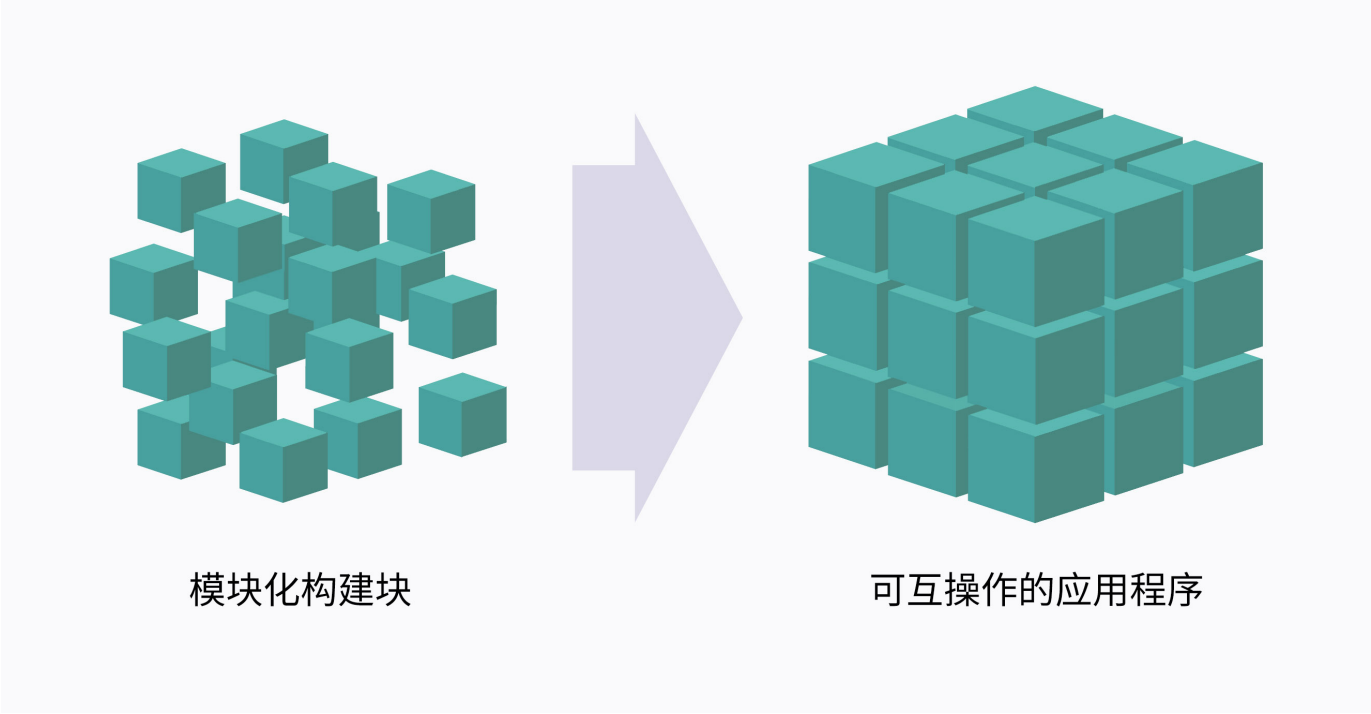


图1. 模块化构建块使快速交付高级功能变得更加容易

嵌入式应用程序部署

在满足车辆、医疗或边缘计算使用场景严格要求的嵌入式应用程序部署中，面临的挑战非常适合通过容器技术来解决。风河的首席技术专家Rob Woolley在他的论文《通过容器更快地部署嵌入式应用程序》中总结了这些优势。他指出：“嵌入式开发人员可以从容器提供的与基础设施无关、可扩展的执行环境中受益。想象一下这样一个设计流程——从开发到测试，再到部署、生产和管理——开发人员可以在团队中共享资源、管道和结果。公司不再受到开发板数量的限制，而是可以利用云的弹性，根据需求设置多个系统实例。”

嵌入式用例通常需要低延迟、响应迅速、确定性行为的特性。风河开物RTOS专为这些类型的部署进行了优化，并支持符合OCI标准的容器，以实现小体积嵌入式解决方案。它在需要严格安全合规和专业认证的产品中有着悠久的使用历史。风河开物RTOS适用于医疗、航空航天、运输以及工业4.0机器人和自动化等行业的高要求用例。

容器的特性非常适合持续集成和部署（CI/CD），能够快速从新的源代码更改中生成新的软件更新。其模块化特性意味着它们可以在自动化编排的DevSecOps工作流中发挥作用（如图2所示）。为风河开物RTOS构建的容器在重视安全性和频繁紧急软件补丁以解决网络安全问题的环境中具有高度的可移植性。

- 符合OCI标准
  - 镜像格式
  - 运行时规范
- 运行时
  - 镜像解析/验证
  - 容器的实例化
  - 应用程序的执行
- 管理器
  - 从注册表中拉取容器的逻辑
  - 用于开发/测试的命令行工具

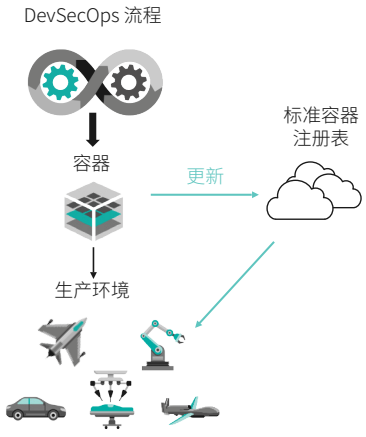


图 2. 创建和分发风河开物RTOS容器

开发CAPS框架

为了简化软件开发并防范潜在的安全漏洞和恶意软件，柯林斯航空公司开发了容器化应用平台系统（CAPS）。一篇最近的白皮书这样描述这一方法：

“基于易于使用的主流技术堆栈，CAPS确保在嵌入式航空电子环境中可靠运行一系列容器化的微服务。这种环境在每次飞行后断电，并且系统从未连接到IT网络进行维护。”

使用风河仿真技术进行容器开发和测试

风河的高级仿真软件为开发人员和系统架构师提供了一种有效的方法，可以在容器部署到实际设备之前测试容器，从而识别并解决软件缺陷。随着DevSecOps模型的广泛采用，容器可以在开发的最早阶段进行设计，以尽量减少嵌入式解决方案的问题并探测潜在问题。

仿真软件能够有效检测安全漏洞，确保这些漏洞不会被忽视，并在容器大规模分发之前将其消除。这项仿真技术使得在虚拟硬件上进行有效测试成为可能，这在探索可能的攻击路径时尤为重要，尤其是在实际系统上难以或无法检查的情况下。

为支持容器的系统创建数字孪生体对于长期运行和升级变得越来越重要。Ask Sage创始人、美国空军和太空军前首席软件官Nicolas Chaillan评论道：“数字孪生在建模和仿真中至关重要。它能够有效地让团队提前知道系统的确切行为表现，而无需实际制造硬件。许多人关注软件敏捷性却忽略了这一点。硬件领域并非总是处于瀑布式开发中。我认为现在很容易通过机架或某种类型的可替换硬件、计算或存储功能来更换硬件，无论是在飞机、舰船还是其他平台上。”

> “数字孪生在建模和仿真中至关重要。它能够有效地让团队在制造硬件之前准确了解系统的行为表现。”
>
> —Nicolas Chaillan

容器技术的前景

重新设计现有嵌入式系统以拥抱软件定义架构绝非易事。然而，整个行业正在逐渐采用容器技术，作为现代开发实践的逻辑演变方向。Aptiv 转型和特殊项目高级副总裁 Glen De Vos 在谈及向软件定义模型设计发展的方向时说道：“我们完成了所有这些概念验证和与汽车 OEM 的研究，以证明‘这就是它可行的原因。’我们现在处于下一个阶段，也就是软件的等效阶段：我们将向您展示基于容器化和 DevOps 环境的智能软件架构，这就是现在的流程。我们认为数据非常具有说服力。事实上，这项技术已经从不可持续变为有利可图。”

嵌入式解决方案的容器技术仍处于早期采用阶段。然而，它是整个行业如何通过模块化组件设计软件的转型的一部分，并通过采用 DevSecOps 实践来增强敏捷性、安全性和持续维护。向云交付软件补丁和升级的转变可以从长远来看为公司节省大量成本，并高效地创造新的机会，以可靠地满足客户需求和行业要求。

随着人们对嵌入式容器技术优势的认知不断增加，以及软件开发人员的容器化技能与这一增长同步发展，该技术承诺了一个光明的未来。

人工智能与容器技术的强强联合

容器技术结合人工智能（AI）和机器学习能够实现强大的功能。示例如下：

- **预测性维护：**嵌入式解决方案中的机器学习模型可以评估部件故障的可能性，触发及时的维护程序并防止意外停机。这在以安全性和可靠性为首要任务的航空航天行业尤为重要。
- **识别和应对安全威胁：**通过使用人工智能监控嵌入式应用程序的行为并阻止入侵，可以降低安全漏洞（包括恶意软件和未经授权的系统访问）带来的风险。
- **平衡资源使用：**人工智能可以在嵌入式容器应用程序中智能分配资源，优化处理器、内存和存储资源的平衡，并提供动态可扩展性以满足应用程序需求。

> “谈到未来的容器化，一个重要点是它将简化人工智能和机器学习的采用，而这取决于容器化以及容器的可扩展性。”
>
> —Nicolas Chaillana

结论

随着嵌入式行业应对软件生命周期维护和关键安全问题的挑战与复杂性，在风河开物RTOS中对容器的支持提供了一个可以定期、可靠并大规模部署更新的解决方案。

风河开物RTOS中容器技术的采用通过利用现有的行业标准和工具为当前和下一代设计开启了创新之门。容器的使用提供了可跨项目复用的模块化软件，从而节省成本并缩短上市时间。

容器技术具有灵活性，能够应对技术变革的加速步伐，适应多种用例，并创造商业机会。访问www.windriver.com.cn/containers，了解风河如何帮助您采用容器技术。

其他资源

什么是嵌入式容器？探索容器技术如何弥合企业系统与嵌入式系统之间的差距。

2023年容器技术炒作周期：从Gartner的洞察中了解容器技术如何助力数字化商业战略。

容器技术为边缘计算注入活力：了解制造商、医疗组织、能源供应商、航空航天公司等如何利用风河开物RTOS中包含的容器支持。

关于风河

风河是为关键任务智能系统提供软件的全球领导者。40年来，该公司一直是创新和开拓的先驱，为数十亿需要最高安全性、安全保障和可靠性的设备和系统提供支持。风河的软件和专业技术正在加速汽车、航空航天、工业、医疗和电信等行业的数字化转型。公司提供一套全面的产品组合，并由世界一流的专业服务和支持以及广泛的合作伙伴生态系统提供支持。欲了解更多信息，请访问风河官网www.windriver.com.cn 。

风河就在您身边

风河开物科技（上海）有限公司	地址：上海市黄浦区中山南一路768号博荟广场C座21楼03单元	电话：021-63585586
风河开物科技（上海）有限公司北京分公司	地址：北京市朝阳区霄云路38号现代汽车大厦19层1902室	电话：010-84777100
风河开物科技（上海）有限公司深圳分公司	地址：深圳市福田区车公庙天安数码时代大厦A座606室	电话：0755-25333408
风河开物科技（上海）有限公司成都分公司	地址：成都市高新区天府软件园D区7号楼1401-1404号	

关于风河更多内容请访问：https://www.windriver.com.cn Email: inquiries-ap-china@windriver.com

官方微信