



智能边缘

——容器技术的新机遇

WINDRVR





风河开物RTOS®是领先的实时操作系统（RTOS），而容器技术具备安全性、可移植性和敏捷性等优势。如今，两者相互融合，为智能边缘的容器化部署提供了极佳的基石。

应用系统越来越复杂并且为基础设施提供了更全面的支持，但同时也把更多的脆弱点暴露在黑客面前。嵌入式系统中的容器则让智能边缘拥有了应对的手段，以便确保应用系统的安全性。

有了容器所提供的这些能力，航空航天和国防机构、能源供应商、大型制造商和医疗机构都可以借助于低延迟、高带宽和高性能来适应最具挑战性的应用场景。这一趋势的最佳佐证就是：航空电子系统已从最初基于硬件的解决方案演变为灵活、高度可升级、软件定义的基础设施，使得新的技术能够在不需要大量更换硬件的情况下动态地融入新场景。

通过快速更新和补丁，软件容器技术有望成为应对网络安全威胁的有效手段，为商业和航空航天/国防机构带来巨大的效益。然而，只有充分理解软件容器这项技术的安全机制，并且将必要的保护措施作为DevSecOps过程的一部分集成进入解决方案，才能完整全面地发挥其效益。

容器技术日渐成熟

为了进一步加强关键任务应用开发——特别是适应边缘计算应用场景——风河公司最近推出了支持OCI兼容性容器的风河开物RTOS，支持开发人员沿用早已在IT环境中熟练使用的云基础架构、工具和工作流。

在为风河开物RTOS开发容器的过程中，风河开创性地推进了RTOS应用的技术步伐，使其迈入了一个全新时代，实现了嵌入式解决方案的运行环境小型化，而功能又足够强大，可用于各行各业的边缘计算关键应用。

Docker、CoreOS和容器技术的众多领导者制定了基本规则和规范，以便使其符合开放标准。有关此项开放标准的详细信息，以及工具和示例代码，可以通过OpenContainerInitiative和GitHub存储库获得。



自动驾驶汽车正在颠覆市场

Docker、rkt、Railcar、LXC、CRI-O和其他容器运行时软件都依赖于client/host体系结构。在基于风河开物RTOS和容器的DevSecOps典型环境中，应用程序代码都是使用最佳实践安全框架创建的。应用程序作为容器发布到目标端点的host主机上——例如基于风河开物RTOS的设备，以及容器仓库之中。对代码的任何更新或补丁都可以推送到仓库并存储起来。此后，在主机系统需要时即可从仓库中读取，不论是一架飞机、一辆互联汽车还是一个变电站——适用于任何采用容器进行代码分发的车辆、医疗设备、物联网设备或制造基地。

应用软件二进制文件一旦开发完成，就会生成一个标准Docker文件。然后，由开源工具Buildah创建其容器映像，其中包含了应用程序组件文件包。接着将容器推送到容器仓库并复制到目标主机。容器仓库本身——Docker hub、Amazon ECR、Harbor或任何其他兼容OCI的容器仓库——在应用软件完整生命周期内都支持安全容器的访问。面向打包进入该容器的应用软件，任何合法主机都可以自动或手动访问发布到容器仓库的更新信息。

容器的分发过程可以采用不同的方法进行处理。例如，飞机着陆后可以滑行到维修区，连接到机场的服务基础设施，并从系统服务器的容器仓库提取任何最近更新的容器。容器更新将会随后整合进入飞机系统。配备现代无线功能的车辆可以在行驶经过5G基站时从容器中接收软件更新数据，然后在汽车停泊进入车位后自动安装这些更新数据。

由于风河开物RTOS容器实现中采用的技术完全遵循OCI指南，所以开发人员确信，在遵从OCI标准构建起来的基础设施中，他们所构建的容器必将会可靠地运行。另一方面，与基于标准的解决方案不同，软件部署的专有解决方案缺乏灵活性和可预测性，因此在业界通常不那么受欢迎。相比之下，符合OCI的工具——遵循Image Format规范和运行时规范——有效地连通了由容器平台、容器引擎以及基于标准的云提供商环境和内部基础设施所组成的生态系统。



确保容器安全

在任何类型的软件部署中，安全性都是一个至关重要的问题。容器技术如果要在需要提高安全性的环境中取得成功——例如航空航天和国防、汽车应用、能源网络和子系统、机器人技术实施等——就需要采取特别的强化措施。

在应用容器时，云原生开源容器仓库通常会提供一个安全层。例如，Harbor采用策略和基于角色的访问控制来保护容器组件。扫描每个容器映像以确保其不存在已知漏洞，然后在分发之前签名为可信。对于敏感的任务关键型部署，Harbor在跨云计算平台移动容器时提供了一定程度的保证。

遵循DevSecOps软件开发最佳实践是保护容器安全性的最有效方法之一。美国国防部发布了《容器加固指南》（2020年10月），其中概述了对防范安全漏洞非常重要的DevSecOps流程。

风河开物RTOS容器引擎沿用了风河开物RTOS中可用的安全功能，包括验证数字签名。系统架构师可以开发与容器部署操作环境相一致的安全层级。从初始引导操作到断电顺序，有一系列的保护措施。CIA三原则——保密性、完整性和可用性(Confidentiality, Integrity, and Availability)也是风河开物RTOS容器安全性的基础。

各种技术的融合催生了智能边缘



如今，越来越多的应用系统要求低延迟、高带宽性能，面向智能边缘计算的解决方案需求日益增长。为了提供足够高的性能，智能边缘需要依赖的主要新兴技术包括5G网络、人工智能和机器学习、物联网和移动技术，其中也包括越来越多的容器技术。

在众多应用场景中，容器可以帮助解决的边缘挑战包括：

- **制造业运营与工业机器人：**基于人工智能的自动化得到了紧凑、低功耗安装的支持，这类安装要求嵌入式实时操作系统提供关键任务的可靠性。
- **创新医疗保健服务：**远程病患护理、健康监测系统、咨询和其他医疗保健实践，这些应用都可以从容器技术的安全性和灵活性中获益。
- **自动驾驶车辆和智能城市运营：**在许多嵌入式应用场景中，重量轻、低功耗是一个至关重要的因素，这些场景涉及AI控制的车辆、车对车通信、交通流量监控、高级驾驶员辅助系统（ADAS）以及全市范围的预警和警报系统。
- **零售客户个性化与沟通：**自动化信息亭、个性化标牌显示、富媒体产品演示和在线订购系统可以利用智能边缘部署容器技术，提高其功能和灵活性。

未来风河开物RTOS和容器的边缘应用

风河开物RTOS对容器的支持极大地扩展了智能边缘嵌入式应用和场景的发展空间。这一进展使得提供轻量级、低功耗、低延迟的解决方案成为可能，这些解决方案能够满足广泛的行业领域和苛刻的要求。

展望未来，5G网络将变得更加普遍，它提供了一种现成的方法，可以从边缘分发数据和容器，并使用3 GHz蜂窝塔和28 GHz小型蜂窝，而且可以通过光纤网络连接本地和中央数据中心，这将使风河开物RTOS解决方案的潜力进一步得到发挥。这些概念将会产生巨大的影响，特别是在航空航天领域——卫星、无人驾驶飞机、通信和任务飞行控制系统可以安全、可靠地访问智能边缘，使其能力显著增强。

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：010-8477 7100
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
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

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



官方微博



官方微信



WINDRIVER