WIND™

下一代工业控制系统虚拟化需求

风河Titanium Control能够为关键基础设施提供工业级性能、安全和高可用性

WHEN IT MATTERS, IT RUNS ON WIND RIVER

摘要

当前采用的工业控制系统大多已有30年历史，已日渐过时，这也是各产业所面临的主要商业挑战。尽管传统基础设施多年来为控制系统提供了稳定平台，但缺乏灵活性，且需要高昂的人工维护费用，风河 Titanium Control 能够为关键基础设施提供工业级性能、安全和高可用性，因此无法显著提高运营效率。

虚拟化克服了传统控制系统基础设施的局限性，为工业物联网（IIoT）奠定了基础。将传统跨网络部署的专用硬件设备所具有的控制功能虚拟化，并且集成到了商用服务器（COTS）中，不仅利用了最先进的芯片技术，也减少了资本支出和运营成本，并最大限度提高了能源、医疗与制造等各产业的效率。

风河 Titanium Control 是安全的本地化基础设施平台，能够确保各种规模工业控制系统所需的正常运行时间与性能。Titanium Control 在多个方面达到并超过了工业级标准，包括可靠性、管理、性能、可扩展性和低延时、安全性、开放标准等。

本白皮书详述了 Titanium Control 解决方案的技术 细节，本白皮书详述了 Titanium Control 解决方案的技术 细节。

目录

引言

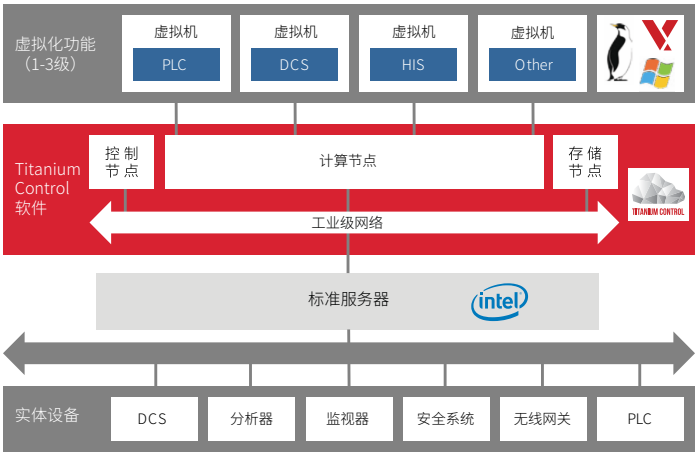
虚拟化是第四次工业革命最重要的科技催化剂之一，也是下一代工业自动化的基础。在IIoT中，虚拟化为公司提供了更高效的工业控制系统基础设施操运营方式，具有多种功能，如提高制造业生产力，保护能源生产中的关键基础设施，为员工确保安全工作环境等。

当前采用的工业控制系统基础设施大多以专有硬件为基础，运营与维护费用日益高昂，生命周期即将结束。同时，由于熟悉设备的资深工程师数量日益减少，造成技术人员不足，维护和更换成本高昂，因此营运支出（OPEX）日益增加。专有硬件不仅限制了运营灵活性，而且增加了工业控制系统的成本和复杂性，而简单的开箱即用级别安全性无法提供端到端威胁防护及防范和检测网络攻击的有效方法。此外，基于硬件的传统解决方法产品生命周期缓慢，不适合快速发展的IT和移动技术，无法和关键基础设施需求保持同步，也无法适应工业自动化核心的相关技术生态系统。

虚拟化使关键基础设施公司能够利用COTS硬件替代传统固定功能硬件，部署安全、鲁棒、灵活的基于软件的解决方案，以削减运营成本。许多曾作为专有设施进行跨工业设施部署的ISA-95一级到三级控制功能都能够实现虚拟化，并且整合到标准企业级服务器中。虚拟化的控制功能包括可编程逻辑控制器（PLC）、分布式控制系统（DCS）、数据采集与监视控制系统（SCADA）软件、人机交互（HMI）和历史数据等。

软件实现成本大大少于劳动密集型的实体设备安装，减少重大资本支出（CAPEX）和OPEX。同时，因为多种虚拟控制功能可以与信息技术（IT）以及操作技术（OT）一同并入工业标准硬件，而不是将各种功能作为专有设施部署，所以虚拟化解决方案减少了对物理服务器的需求。开放、基于软件的解决方案具有灵活性，各公司能够优化控制过程，加速新功能部署。

提高运营效率、节约成本需要正确的工业级虚拟化平台。风河的Titanium Control是为关键服务与应用从新建立的本地化云基础设施平台。风河的网络功能虚拟化（NFV）已经通过电信级基础设施验证，以其行业顶尖的架构为基础，Titanium Control能为任意规模工业控制系统提供所需的正常运行时间、性能和端到端网络安全性。



图表1 Titanium Control支持在标准服务器上运行L1-L3的工业化虚拟控制功能

工业级可靠性

虚拟化工业控制设施需要高度可用的网络。无论是为电网提供每周七天、每天24小时的全天候连续过程操作控制，还是分析生产设施生成的数据，虚拟化控制系统都需要能够确保关键基础设施正常运行时间、避免非计划停机的软件平台。但标准IT级平台并非为关键基础设施所设计，无法实现工业级控制设施所需的可靠性。

Titanium Control 是为实现工业级、99.9999%t可用性专门搭建的平台，能够在两个或更多的物理服务器上运行，每年网络停机时间少于30秒。

> 99.9999%的关键服务可用性

高可用性得益于平台对多种软件和硬件故障的强大容错能力。Titanium Control能够自动检测故障控制器、主机和虚拟机（VW），启动快速恢复，用以尽量减少服务或数据损失。以恢复时间为例，Titanium Control比企业级Linux平台快60倍。

Titanium Control 能够在500毫秒内检测到虚拟机故障，而一个IT级平台需要超过1分钟。Titanium Control能够在1秒内发现故障计算节点，而IT平台需要超过1分钟的时间。同时，平台支持动态虚拟机迁移（包括采用了DPDK特性的虚拟机），所需停机时间少于150毫秒。

故障恢复水平处于行业领先位置
——检测到虚拟机故障所需时间少于150毫秒

在软件升级与补丁方面，Titanium Control 能够确保消除非计划停机时间，并为所需的回滚提供全力支持。Titanium Control 的存储能力设计也确保其存储足以处理虚拟机迁移、虚拟机重启与节点故障等事件。

	企业IT平台能力	工业控制要求	Titanium Control
检测故障虚拟机	> 1分钟	< 1秒	500毫秒
检测故障计算节点	> 1分钟	~ 1秒	1秒
自动检测和恢复控制节点故障	不支持	全面支持	全面支持并对业务无影响
网络连接故障检测	依靠Linux分布	50毫秒	50毫秒
基于DPDK的虚拟机实时迁移	不支持	全面支持	全面支持<150毫秒

图表 2 Titanium Control满足或超出工业控制可靠性要求

实现应用级别高可用性的方式有active/active模式、active/stand-by和N-way active负载均衡模式等，但这些配置都不足以单独为基于软件的控制系统所用。Titanium Control 支持具有高可用性（HA）配置的应用，并利用额外的可靠性功能进行加强。然而，应用级HA并不能满足全系统的工业级弹性需求，如对底层系统资源或服务链不了解，无法保证虚拟化应用的稳定性能，无法从系统级故障中自动恢复，无法支持平台级安全性等。

与应用级HA技术相比，Titanium Control 旨在支持平台级的高可用性，以确保全系统可靠性。

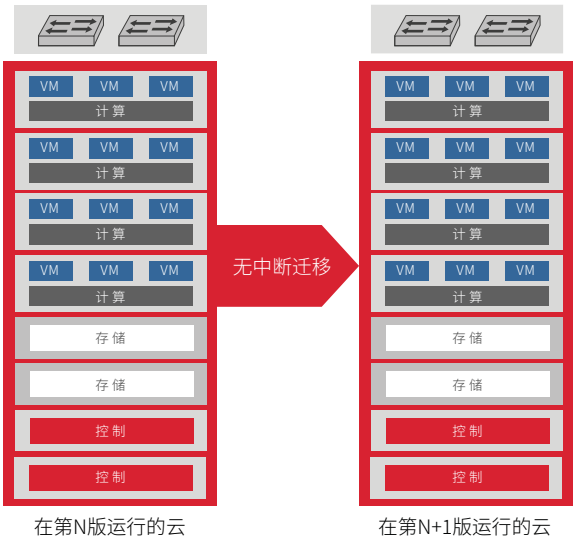
综合管理

Titanium Control 提供综合管理工具和功能，简化虚拟控制系统功能的操作和维护。从最开始，安装和调试程序就得已简化，因此可实现高效、可重复性部署。首先，平台不需要独立的安装程序节点，能够在初始控制器上运行，简化了安装，有助于减少解决方案的整体消耗。用户使用图形用户界面（GUI）以及基于命令行界面（CLI）的方式，利用安装向导快速安装，并自动发现节点和资源，隐藏了配置OpenStack服务的复杂性。安装过程支持从首次到大规模部署的任何场景。

风河 Titanium Control 可管理性的关键特征之一是包含复杂的系统报警、分析、性能管理和故障管理的远程监控，当出现可能影响服务的问题时候能及时提醒用户。平台所监控的参数包括集群连接、关键进程故障和资源利用阈值，能够广泛记录与平台节点和资源相关的重大事件以及主机上的虚拟资源，使管理员得以审查与查询历史报警记录或任何非报警事件。

运行中、无中断维护与安全响应

平台支持热补丁与无中断更新，确保避免因软件维护造成的非计划停机时间。热补丁可通过强大的补丁引擎手动或自动部署，只需一次点击即可迅速在所有系统节点上应用更新。补丁编排工具大大减少了更新时间，直接降低了OPEX。



图表3 无中断软件更新

Titanium Control 管理所有平台软件的无中断更新，包括主机OS变化、新OS包、新版OpenStack以及已升级虚拟化控制层。多节点滚动升级无需额外硬件，仅需两个节点就能完成。若应用程序支持，则可实时迁移主机的应用程序，或进行冷迁移。

平台通过REST API或标准网络协议进行集成

Titanium Control支持REST API和SNMP，方便集成IT级的L4和L5级的管理、编排和监控系统，使管理员能够利用现有网络管理系统。

优化性能、可扩展性和低延时

Titanium Control 能够为虚拟化工控系统功能提供可预测的性能指标，最大化的资源利用率，无缝扩展和低延迟特性。

Titanium Control 支持所有规模部署，无论该工业控制系统包含了

跨地区数据中心的上百台服务器，还是仅要求小型二节点配置以实现高度可用的关键服务和应用，Titanium Control 都能够提供支持。Titanium Control也支持无需高可用性的本地化单节点应用配置。

图表4 完全可扩展系统架构

风河为虚拟可编程逻辑控制器（PLC）等对时序要求严格的工业级应用增强了KVM虚拟架构，实现 Titanium Control 低延时套件，将平均延时减少了74%。低延时套件确保了确定性中断延时，实现了2微秒的平均主机延时和3微秒的平均虚机延时，和企业级虚拟化程序相比有显著改善。在要求较低的使用案例中，平台的标准延时套件支持2微秒的平均主机延时和5微秒的平均虚机延时。

加速虚拟交换机（AVS）是 Titanium Control 的一大功能，它是为实现工业级互联网而建立的用户态虚拟交换机，主要基于 Intel 的DPDK包处理库。平台支持DPDK、SR-IOV、1G、10G和40G以太网，确保超高速分组处理。Titanium Control 的AVS网络吞吐量是开源vSwitch（OVS）系统的40倍。

网络吞吐量是Open vSwitch系统的40倍

AVS的高性能使资源利用更高效。和其他虚拟交换机方案相比，AVS能够利用更少的处理内核达到线速的虚拟交换性能，提高了虚拟机密度。由于运行vSwitch所需的内核减少，VM可以使用更多的内核。最终，更高的虚拟机密度能够减少支持虚拟化工业控制功能所需的物理服务器数量，并尽可能减少CAPEX和OPEX。

平台还提供了加速的东西向虚拟路由，提高了虚机到虚机之间的流量。标准的“vanilla”OpenStack之间通讯提供了基本的虚机路由，但在工业级应用方面的整体性能不佳。Titanium Control DPDK加速虚拟路由器的吞吐量是标准OpenStack内核路由解决方案的250倍，将平均延时减少了9倍。

Titanium Control 虚拟路由器，实现250倍的吞吐量，将延时减少9倍

动态CPU调整进一步优化了资源利用，确保了可预测性能。Titanium Control 能够自动实时增加或减少VM资源，无需重启系统。当虚拟应用程序资源不足，触发了预定义条件，Titanium Control 将分配额外的处理器资源以运行该程序。因此，平台能够根据变化的模式进行动态调整。

Titanium Control 利用因特尔增强型平台感知（EPA）和系统监测优化并实现确定性网络性能。EPA使Titanium Cloud能够根据具体的工作量需求动态验证和限制对虚拟机的资源分配，Titanium Control 从而可以提供可预测网络性能，能够完全符合工业控制系统应用的要求。

信息安全的鲁棒性

各产业几十年来依赖基于硬件的控制系统解决方案，而Titanium Control确保虚拟工业控制系统功能的安全性能够与之媲美。转向虚拟化解决方案并不意味着需要牺牲关键基础设施的安全性。基于软件的解决方案能够为网络和控制系统功能提供端到端安全性。在软件产品生命周期的每个阶段，风河都遵循正规流程，构建安全完整的Titanium Control平台和为虚拟化控制功能所提供的服务。

工业首款支持虚拟可信平台模块（TPM）

风河开发了行业一流的虚拟可信平台模块（vTPM），为虚拟机部署提供最高安全性。vTPM在虚拟系统中复制了基于硬件系统的安全性，将物理硬件的安全性扩展到虚拟机。也就是说，TPM是一项将加密数据与设备集成用于硬件认证来为安全加密处理器加强系统安全性国际标准。虚拟化假定使用工业标准服务器，但并不是所有服务器都包括TPM。风河创建了vTPM特性，他是Titanium Control主机上实体TPM2.0芯片的软件实现。此外，当存在硬件TPM 2.0时，TPM硬件将存储安全传输层协议（TLS）和证书，以保护管理操作。

统一可扩展固件接口(UEFI)安全启动得到了全面支持,保护主机环境,确保虚拟机仅加载可信软件。Titanium Control 引导装载程序、内核以及核心模块均经过签名。系统固件检查系统引导装载程序具有密钥签名,密钥由固件包含的数据库授权。下一阶段的引导装载程序、内核及内核模块也需经过签名验证。安全启动密钥得到妥善保存和管理,一般通过设置菜单进行配置。

此外,Titanium Control包含一整套流程,能够实现连续漏洞检测和修补。保密功能包括安全密钥环数据库,用以验证与主机上虚拟机连接的加密密码和ACL过滤器。为了保护运行时环境、Titanium Control节点上的关键进程、资源和连接性需要持续监控,以确保早期检测与快速恢复。

同时,Titanium Control 支持关键基础设施要求的网络级别认证、授权和计费(AAA),功能包括基于角色的访问控制、强制安全密码、密码有效期、根账户和根命令访问限制,以及非活动用户会话的自动注销。外部操作、管理和维护(OAM)接口通过网络防火墙能够为平台周边提供防护。

此外,风河Titanium Cloud Ecosystem全面提供经验证的第三方安全功能选择,用户能够选择最佳品牌来保护工业控制系统与关键基础设施。

TITANIUM CONTROL 亮点

- 从一个服务器到数百个服务器的动态扩展
- 集成计算、控制和存储功能
- 99.9999%可用性
- 对多种硬件和软件故障的容错性,无单点故障
- 简化安装、调试与维护
- 远程监控、诊断与更新
- 支持对时序要求严格的工业应用
- 支持标准虚机操作系统
- 标准IT类服务器完整功能
- 加速部署专业服务支持

开放标准

Titanium Control以开放标准为基础,允许工业控制系统运营商选择最佳软件解决方案,避免合约受限于特定供应商所提供的装置。开放标准不仅为关键基础设施解决方案提供了有竞争力的选择,而且促进了第三方软件开发商进行创新。

Titanium Control使用的开源云和虚拟化软件包括很多事实标准的开源组件:

Linux、KVM、OpenStack、Ceph和DPDK,但企业级开源软件最初并不是为工业控制系统应用所设计。为满足工业级标准,风河通过增强和扩展优化了超过2000个开源组件。秉承开源宗旨,风河专家不断开拓创新,将修改和补丁回馈到开源社区。

- Linux:Titanium Control通过超700个Linux补丁提供工业自动化所需的可靠性、安全性、可用性和性能。
- 实时KVM:Titanium Control为KVM管理程序添加了内核和用户空间优化,实现持续确定性性能。
- OpenStack:Titanium Control添加了使用基于OpenStack编排所需的可靠性与可用性扩展。
- Ceph:Titanium Control分布式存储解决方案具有高度可扩展性、可用性与性能。

Titanium Control也支持包括Linux、风河开物RTOS®和Windows在内的工业标准虚机操作系统。

Titanium Cloud Ecosystem可提供端到端解决方案,完成工业控制系统实现,包括第三方应用、SDN控制器以及企业级编排和COTS服务器等,自从2014年6月项目启动以来,风河的生态系统已经吸引了超过40家的合作伙伴。为了在 Titanium Control 平台上正常运行,所有合作的硬件与软件解决方案均通过深度技术协作验证,消除了来自不同供应商和开源社区的多种技术组件的集成、测试和文档工作。风河的预验证工作将上市时间提前了18个月,使关键基础设施运营商能够专注于实现业务目标。

风河集团具备多年虚拟化平台设计与维护经验的架构师、软件工程师和验证专家组成的专门团队,致力于帮助传统控制系统基础设施过渡到虚拟化控制功能。风河专家全力支持虚拟化工业控制系统和工业自动化完整解决方案部署,并提供全面的技术支持和必要的专业服务。

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

WIND™