WIND™

Requirements for Virtualization in Next-Generation Industrial Control Systems

Wind River Titanium Control Delivers Industrial Grade Performance, Security, and High Availability for Critical Infrastructure

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Many of the industrial control systems in use today were installed 30 years ago and are now becoming outdated, presenting major business challenges to industries. While the legacy infrastructure has provided a stable platform for control systems for many years, it lacks flexibility, requires costly manual maintenance, and does not allow valuable system data to be easily accessed and analyzed, which would significantly improve operational efficiency.

Virtualization overcomes the limitations of legacy control systems infrastructure and provides the foundation for the Industrial Internet of Things (IIoT). Control functions that were previously deployed across the network as dedicated hardware appliances can be virtualized and consolidated onto commercial off-the-shelf (COTS) servers, which not only leverages the most advanced silicon technology but also reduces capital expenditure, lowers operating costs, and maximizes efficiency for a variety of industrial sectors, including energy, healthcare, and manufacturing.

Wind River® Titanium Control is a secure, on-premise cloud infrastructure platform that ensures the uptime and performance needed for industrial control systems at any scale. Titanium Control meets and exceeds industrial grade requirements for reliability; management; performance, scalability, and low latency; security; and open standards.

This paper presents the technical details of the Titanium Control solution and examines how the virtualization platform meets industrial requirements.

TABLE OF CONTENTS

INTRODUCTION

Virtualization is one of the most important technology catalysts for the Fourth Industrial Revolution and a foundation for next-generation industrial automation. In IIoT, virtualization provides companies a more efficient way to operate industrial control systems infrastructure, which serves a range of functions such as increasing productivity in manufacturing, securing critical infrastructure in energy production, and ensuring safe work environments for employees.

Much of the industrial control systems infrastructure in use today is built on proprietary hardware that is becoming too expensive to operate and maintain and is nearing end-of-life. Operating expenditure (OPEX) is on the rise due to high maintenance and replacement costs as well as low availability of technicians, as the pool of skilled engineers familiar with the equipment has shrunk over time. Proprietary hardware restricts operational flexibility, adding cost and complexity to industrial control systems. Simple box level security does not provide end-to-end threat protection or effective means to prevent and detect cyberattacks. Furthermore, legacy hardware-based solutions have slow product lifecycles that are out of step with fast-moving IT and mobile technologies. They cannot keep pace with the needs of the critical infrastructure, nor with the relevant technology ecosystem at the heart of industrial automation.

Virtualization enables critical infrastructure companies to slash their operational costs by deploying secure, robust, flexible software-based solutions leveraging COTS hardware as alternatives to legacy, fixed function hardware. Many ISA-95 Level 1 through Level 3 control functions that were previously deployed across industrial facilities as dedicated appliances can be virtualized and consolidated onto standard enterprise-class servers. Virtualized control functions include programmable logic controllers (PLCs), distributed control systems (DCSs), supervisory control and data acquisition (SCADA) software, human machine interfaces (HMIs), and historians.

Significant capital expenditure (CAPEX) and OPEX savings are realized from software implementations that are far less expensive than labor-intensive installations of physical equipment. Also, virtualized solutions require fewer physical servers, as multiple virtual control functions can be consolidated onto industry-standard hardware, along with information technology (IT) and operational technology (OT) functions, rather than deploying each function as a dedicated appliance. The flexibility of open, software-based solutions allows companies to optimize control processes and accelerate the deployment of new functions.

Achieving operational efficiency and cost savings requires the right industrial-grade virtualization platform. Wind River built Titanium Control, an on-premise cloud infrastructure platform for critical services and applications, from the ground up. Based on the Wind River industry-leading architecture that is proven in telecommunications infrastructure for Network Functions Virtualization (NFV), Titanium Control delivers the uptime, performance, and end-to-end network security needed for industrial control systems at any scale.

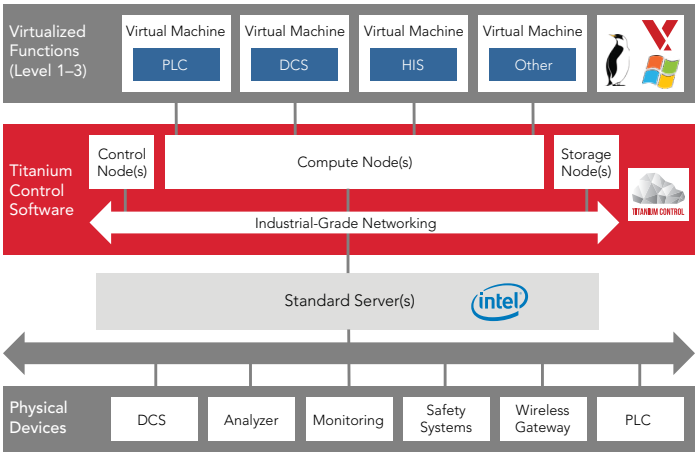

Figure 1. Titanium Control supports Level 1–3 virtualized control functions on standard servers

INDUSTRIAL GRADE RELIABILITY

Virtualized industrial control applications require highly available networks. Whether controlling continuous process operations 24 hours per day, seven days per week for an electricity grid or analyzing data generated from a manufacturing facility, virtualized control functions need a software platform that ensures uptime and avoids unplanned downtime for critical infrastructure. But standard IT-grade platforms cannot deliver the reliability required for industrial control applications because they are not designed for critical infrastructure.

Titanium Control is purpose-built at the platform level to deliver industrial-grade, six-nines (99.9999%) availability when running on as few as two or more physical servers, which equates to less than 30 seconds of network downtime per year.

99.9999% availability for critical services

This high reliability is due to the platform's robust fault tolerance to multiple software and hardware faults. Titanium Control automatically detects failed controllers, hosts, and virtual machines (VMs) and initiates rapid recovery with minimal loss of service or data. For example, Titanium Control recovery time is 60 times faster than an enterprise Linux platform.

Titanium Control can detect a failed VM in 500 milliseconds, whereas an IT-grade platform would take more than one minute to detect VM failures. Titanium Control detects a failed compute node in one second, while an IT platform would take more than one minute. The platform also supports live VM migration (including DPDK-based VMs) with less than 150 milliseconds of outage time.

Industry-leading fault recovery—less than 150 milliseconds of a failed VM

When it comes to software upgrades and patching, Titanium Control ensures that there is no unplanned downtime and offers full support for rollbacks if needed. Titanium Control's storage capability is also designed to ensure that volumes survive events including VM migrations, VM restarts, and node failures.

	Enterprise IT Platform Capability	Industrial Control Requirements	Titanium Control
Detection of failed VM	> 1 minute	< 1 second	500 ms
Detection of failed compute node	> 1 minute	~ 1 second	1 second
Automated controller node failure detection and recovery	No support	Full support	Full support with zero impact
Network link failure detection	Depends on Linux distribution	50 ms	50 ms
Live migration for DPDK-based VMs	No support	Full support	Full support: <150 ms

Figure 2. Titanium Control meets or exceeds industrial control reliability requirements

There are several approaches for implementing high availability at the application level—i.e., active/active, active/standby, and N-way active with load balancing—but these features alone are not sufficient for software-based control systems. Titanium Control supports applications with high-availability (HA) features and augments them with additional reliability features. However, HA at the application level does not meet full system level requirements for industrial grade resiliency. For example, there is no awareness of underlying system resources or service chains, no guarantee of consistent virtualized app performance, no automated recovery from system-level failures, and no support for platform-level security.

In contrast to application-level HA techniques, Titanium Control is inherently designed to support high availability at the platform level to ensure reliability across the entire system.

COMPREHENSIVE MANAGEMENT

Titanium Control provides comprehensive management tools and features that simplify the operation and maintenance of virtualized control system functions. From the outset, installation and commissioning procedures are streamlined so that deployments are efficient and repeatable. To begin with, the platform does not require a separate installer node and runs on the initial controller, which simplifies installation and contributes to reducing the solution's overall footprint. Graphical user interface (GUI) and command-line interface (CLI)–based wizards guide users through inputting the system bootstrap data, and nodes and resources are automatically discovered, which hides the complexity of configuring OpenStack services. The installation process supports any scenario, from first-time to large-scale deployments.

A key feature of Wind River Titanium Control manageability is remote monitoring with sophisticated system alarms, analytics, performance management, and fault management, which instantly alert users to problems that could affect services. The platform monitors parameters including cluster connectivity, critical process failures, and resource utilization thresholds. Significant events related to the platform nodes and resources, as well as hosted virtual resources, are extensively logged, enabling administrators to review and query historical alarms or any non-alarm event.

In-service, hitless maintenance and security response

To ensure that there is no unplanned downtime due to software maintenance, the platform supports in-service patching and hitless upgrades. In-service software patches are deployed manually or automatically via a powerful patch orchestration engine, which

rapidly applies the software update across all nodes in the system with one click. The patch orchestration tool significantly reduces the time to conduct upgrades, which directly results in OPEX savings.

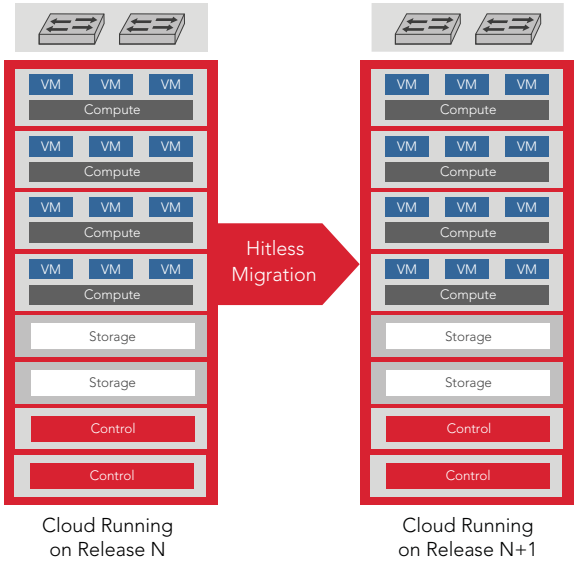

Figure 3. Hitless software update

Titanium Control manages hitless upgrades of all platform software, including host OS changes, new OS packages, a new OpenStack release, and upgraded virtualization control layers. Rolling upgrades across multiple nodes do not require additional hardware and can be achieved with just two nodes. Hosted applications can be migrated live, if the apps support it, or migrated cold.

> Platform integration via REST API or standard network protocols

With support for REST APIs and SNMP, Titanium Control integrates with third-party IT-based Level 4 and Level 5 management, orchestration, and supervisory functions, enabling administrators to leverage existing network management systems.

OPTIMIZED PERFORMANCE, SCALABILITY, AND LOW LATENCY

Titanium Control delivers predictable performance, maximizes resource utilization, scales seamlessly, and reduces latency for virtualized control system functions.

Deployments of all sizes are supported by Titanium Control, whether the industrial control system comprises hundreds of servers in data centers across multiple geographic regions or simply requires a small, two-node configuration for highly available critical services and applications. Titanium Control also supports an on-premise, single node configuration for applications that do not require high availability.

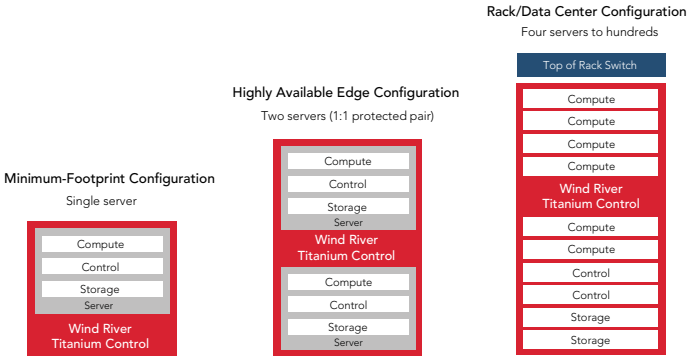

Figure 4. Fully scalable system level architecture

For time-critical industrial applications such as virtual programmable logic controllers (PLCs), Wind River developed enhancements to the KVM hypervisor to create Titanium Control's low latency profile, which reduces average latency by 74%. The low latency profile ensures deterministic interrupt latency, achieving average host latency of two microseconds and average guest latency of three microseconds, which are significant improvements compared to enterprise-grade hypervisors. For less demanding use cases, the platform's standard latency profile supports average host latency of two microseconds and average guest latency of five microseconds.

Titanium Control features an accelerated virtual switch (AVS), a user space vSwitch that was built for industrial grade networking based on the Data Plane Development Kit (DPDK) packet processing resource library. Support for DPDK, single root I/O virtualization (SR-IOV), 1G, 10G, and 40G Ethernet ensures ultra-fast packet processing. Titanium Control's AVS achieves network throughput that is up to 40 times higher than Open vSwitch (OVS)-based systems.

> Up to to 40 times higher throughput than Open vSwitch–based systems

The high performance of AVS results in more efficient resource utilization. The AVS achieves line rate virtual switching performance using fewer processing cores than competing virtual switches, which increases VM density. Since fewer cores are needed to run the vSwitch, more cores are available for VMs. Ultimately, greater VM density minimizes CAPEX and OPEX, as fewer physical servers are needed to support virtualized industrial control functions.

The platform also features accelerated virtual routing for east-west, VM-to-VM traffic. Standard, "vanilla" OpenStack has a basic router for VM-to-VM traffic, but its overall performance is poor for industrial grade applications. Titanium Control's DPDK-accelerated virtual router achieves 250 times higher throughput than the standard OpenStack-based kernel routing solution and a 9 times reduction in average latency.

> Titanium Control's virtual router: 250x higher throughput and 9x latency reduction

Dynamic CPU scaling further optimizes resource utilization and ensures predictable performance. Titanium Control automatically increases or decreases VM resources in real time without requiring a system reboot. When a virtual application experiences a surge that sets off a predefined trigger, Titanium Control allocates additional cores to running the application. In this way, the platform dynamically scales up or down and in or out based on changing capacity patterns.

Titanium Control leverages Intel's Enhanced Platform Awareness (EPA) and system monitoring to achieve optimized, deterministic network performance. EPA enables Titanium Cloud to dynamically validate and restrict resource assignments to VMs based on the specific workload requirements. This capability enables Titanium Control to deliver predictable levels of network performance that are precisely aligned with the requirements of industrial control system applications.

ROBUST SECURITY

Titanium Control ensures that the virtualized industrial control system functions are just as secure as the hardware-based control system solutions that industries have relied on for decades. Migrating to a virtualized solution does not mean having to compromise on security for critical infrastructure. Software-based solutions provide end-to-end security for the network as well as for the control system functions. During every phase of the software product lifecycle, Wind River follows formal procedures to establish the security and integrity of the Titanium Control platform and the services it provides to virtualized control functions.

> Industry's first virtual Trusted Platform Module

Wind River developed the industry-leading virtual Trusted Platform Module (vTPM) to deliver the highest security in VM deployments. The vTPM replicates hardware-based security in virtualized systems, extending the security from physical hardware into VMs. That is, TPM is an international standard for a secure crypto-processor that hardens system security by integrating cryptographic data into devices and using it for hardware authentication. Virtualization assumes the use of industry standard servers, but not all servers include TPM. Wind River created the vTPM, which is a software implementation of TPM 2.0 that is instantiated on the encrypted Titanium Control host. In addition, when hardware TPM 2.0 is present, Transport Layer Security (TLS) and certificates are stored in the TPM hardware to protect management operations.

The host environment is protected with full support for Unified Extensible Firmware Interface (UEFI) secure boot, which ensures that VMs only load trusted software. Titanium Control boot loaders, kernels, and kernel modules are all signed. The system's firmware checks that the system boot loader is signed with a cryptographic key authorized by a database contained in the firmware. Signature verification also occurs in the next-stage boot loaders, kernel, and kernel modules. The secure boot keys are securely stored and managed, typically configured through a setup menu.

In addition, Titanium Control supports a comprehensive set of features that deliver continuous vulnerability monitoring and patching. Confidentiality features include a secure keyring database for storing encrypted passwords and ACL filters for authenticating connectivity to hosted VMs. To protect the runtime environment, critical processes, resources, and connectivity on Titanium Control nodes are constantly monitored, ensuring early detection and rapid recovery.

Titanium Control also supports the network-level authentication, authorization, and accounting (AAA) capabilities that critical infrastructure requires. Features include role-based access control, secure password enforcement, password aging, restricted access to root account and root commands, and auto logout of inactive user sessions. A network firewall on external operations, administration, and management (OAM) interface protects the platform's perimeter.

TITANIUM CONTROL HIGHLIGHTS

- Dynamic scalability from one server to hundreds
- Integrated compute, control, and storage functions
- Six-nines uptime
- Fault tolerant to multiple hardware and software faults with no single point of failure
- Simplified installation, commissioning, and maintenance
- Remote monitoring, diagnostics, and updates
- Support for time-critical industrial applications
- Support for standard guest operating systems
- Full functionality on standard IT class servers
- Professional Services support for accelerated deployment

Furthermore, the Wind River Titanium Cloud Ecosystem offers a comprehensive selection of validated, third-party security functions, allowing users to choose best-of-breed functions to secure industrial control systems and critical infrastructure.

OPEN STANDARDS

Titanium Control is built upon open standards, which allow operators of industrial control systems to select best-of-breed software solutions and avoid being locked into inflexible contracts for vendor-specific appliances. Open standards not only enable competitive choices for critical infrastructure solutions but also foster innovation from third-party software developers.

The open source cloud and virtualization software in Titanium Control includes de facto standards Linux, KVM, OpenStack, Ceph, and DPDK. But enterprise-grade open software was not originally designed for industry control system applications. Through enhancements and extensions, Wind River has optimized more than 2,000 open source components to meet industrial grade requirements. True to the ethos of open source, Wind River experts contribute modifications and patches back into open source communities and contribute to a continuous cycle of innovation.

- **Linux:** Via more than 700 patches to Linux, Titanium Control provides the reliability, security, availability, and performance needed for industrial automation.
- **Real-time KVM:** Titanium Control adds kernel and user space optimizations to the KVM hypervisor to deliver consistent and deterministic performance.
- **OpenStack:** Titanium Control adds the reliability and availability extensions required to use OpenStack-based orchestration.
- **Ceph:** Titanium Control's distributed storage solution is highly scalable, available, and performing.

Titanium Control also supports industry-standard guest operating systems, including Linux, VxWorks®, and Windows.

To complete industrial control system implementations, end-to-end solutions are available from the Titanium Cloud Ecosystem, including third-party applications, SDN controllers, and orchestrators as well as leading enterprise-class and COTS servers. Launched in June 2014, the ecosystem has attracted more than 40 members. Through in-depth technical collaboration, all partner hardware and software solutions are validated to operate correctly with Titanium Control, which removes the need to integrate, test, and document multiple technology components from different vendors and open source communities. Wind River's pre-validation work accelerates time-to-market by up to 18 months and allows critical infrastructure operators to focus on achieving their business objectives.

To help with the transition from legacy control system infrastructure to virtualized control functions, Wind River has dedicated teams of architects, software engineers, and validation specialists with years of experience in designing and maintaining virtualization platforms. Wind River experts provide all the support and professional services needed to deploy complete solutions for virtualized industrial control systems and industrial automation.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.