WIND RIVER VXWORKS MILS PLATFORM

The world’s most critical defense, networking, and industrial infrastructure requires high assurance of security along with protection from intentional threats and inadvertent errors. In addition, there is pressure to increase the capability of these systems while at the same time reducing their costs.

Wind River® VxWorks® MILS Platform provides an operating run-time environment designed for systems having high security, high assurance, and high performance requirements. VxWorks MILS Platform implements an industry-standard system architecture called Multiple Independent Levels of Security (MILS) that enables multiple software components with different security levels, or from different domains, to safely and securely share the same hardware platform. By sharing a single hardware platform (containing either a single processing core or multiple cores) among multiple applications, manufacturers can significantly reduce the costs of the system by reducing size, weight, and power (SWaP) requirements.

VxWorks MILS Platform provides security by strictly enforcing time and space resource allocations, information flow control, and fault isolation so that the system will conform to the security policies as defined by its security architects and system integrators.

Security-critical systems often need to undergo a system-level security evaluation toward gaining an authorization to operate (ATO) or an accreditation. To support such evaluations, VxWorks MILS Platform offers a security evaluation evidence package (currently available only for the single core version of VxWorks MILS Platform) that provides artifacts based on requirements from the “U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness” (SKPP) version 1.03, the Common Criteria (IEC 15408) version 2.3, and RTCA DO-178C (EUROCAE ED-12C) Design Assurance Level (DAL) A. These artifacts can be used to develop security claims of assurance that would be assessed by an evaluator in a system-level security evaluation.

Figure 1: Wind River VxWorks MILS Platform

VxWorks MILS Platform provides security by strictly enforcing time and space resource allocations, information flow control, and fault isolation so that the system will conform to the security policies as defined by its security architects and system integrators.
BENEFITS OF VXWORKS MILS PLATFORM

VxWorks MILS Platform greatly reduces costs by consolidating applications with mixed domains or security levels onto a single hardware platform:

- Reduces operating costs by reducing SWaP requirements through consolidation
- Reduces development and certification costs by isolating highly secure applications from applications with lower security levels, or applications from different domains
- Reduces integration costs by enabling migration of legacy applications to run on the same platform as newly developed applications

VxWorks MILS Platform enables security-critical applications, carrying potentially confidential or mission-critical data, to coexist on the same system with medium- or low-security applications, which may connect to non-secure channels (e.g., the public Internet). This enables cost-effective development of security-critical systems, such as multilevel secure (MLS) systems, which use components at multiple levels of security, and cross-domain solution (CDS) systems, which use components with data from different domains (e.g., different government agencies, or different members of coalitions).

Developer Benefits

Wind River VxWorks MILS Platform offers a range of benefits for security-critical device development teams:

- Allows software components with multiple levels of data security, or from multiple data domains, to run securely on a single core or multi-core processor
- Isolates security-critical code into subcomponents for cost-effective system-level assurance evaluation or certification and accreditation (C&A)
- Enables independent teams to work in parallel on subcomponents using role-based development processes
- Affords cost-effective technology refresh and re-evaluation of subcomponents after deployment, through modular, independent, XML-based configuration data and security policies for each component
- Enables the development of security-critical devices and systems that are ready for system-level high assurance evaluation or C&A

KEY FEATURES

Separation Kernel for High Performance, High Assurance Security

Wind River VxWorks MILS Platform is designed for high assurance of security without compromising on system performance, using a two-level MILS OS architecture (see Figure 1). At the lower level, the VxWorks MILS Platform separation kernel provides secure time and space partitioning, information flow control, and fault isolation. The upper-level partitions are where all user components (e.g., applications, middleware components, and drivers) execute. The VxWorks MILS Platform separation kernel meets the security functional and security assurance requirements in the SKPP, and uses a two-level scheduler yielding near-native partition execution time.
Support for Multiple Industries
VxWorks MILS Platform can be used as the foundation for security-critical devices and systems, where enhanced security characteristics can protect against financial loss, sensitive information loss, or even loss of human life. This applies across multiple industries, such as aerospace and defense, financial, industrial, medical, and automotive.

Multiple Guest OS Environments
VxWorks MILS Platform provides multiple execution environments for applications. Guest operating systems run in partitions, providing asset bridges that enable the reuse of legacy and existing software in VxWorks MILS–based systems.

The High Assurance Environment (HAE) is a small run-time executive, designed to support high-security, single-threaded applications that may undergo high levels of scrutiny in a system-level evaluation or C&A to high assurance levels. The VxWorks Guest OS is available for applications that require multitasking. In addition, because of API compatibility with VxWorks, legacy VxWorks applications are easily ported to VxWorks MILS Platform. Wind River Linux Guest OS enables Linux-based and other open source applications and middleware to run on VxWorks MILS–based systems. The Linux Guest OS provides the same commercial grade, embedded Linux solution as standalone Wind River Linux, with a pre-integrated, fully tested, validated, and supported Linux distribution.

To enhance user-mode application capabilities, VxWorks MILS Platform provides secure inter-partition communications (SIPC), shared memory support, schedule access and modification, security auditing, and safety logging functionalities for components running on HAE, VxWorks Guest OS, and Wind River Linux Guest OS.

Optimized, Integrated Development Suite
VxWorks MILS Platform includes the Eclipse-based Wind River Workbench. This development suite offers one common interface across all development phases of the security-critical system, from development through debug, test, deployment, and maintenance. Workbench includes: a project and build system, an XML-based graphical system configuration tool, the GNU compiler, powerful debugging environments over JTAG and an OS-aware run-time debug agent, and Application Multiplexed I/O (AMIO), which manages individual console windows on the development host for serial communications with each partition on the VxWorks MILS system.

Workbench adheres to RTCA DO-297 (EUROCAE ED-124) “Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations,” enabling streamlined, role-based development, including secure separation of intellectual property. By enabling complete application isolation throughout the product lifecycle, XML-based configuration allows developers to make changes to application or system configuration information without needing to rebuild or retest the entire system. In addition, changes to independent applications can be made without the need to retest or recertify other applications or the underlying operating system. This significantly reduces the time to initial certification as well as the cost of change, maintenance, and recertification throughout the system lifecycle.
PROFESSIONAL SERVICES

High assurance evaluation and C&A can be lengthy, rigorous processes requiring close cooperation between the system manufacturer and the OS vendor. A system-level evaluation or C&A will involve the operating system and middleware as well as the system’s applications. Wind River Professional Services has developed expertise in the design and implementation of safe and secure systems, and can assist Wind River customers with their specific evaluation or C&A requirements of VxWorks MILS-based systems. We also offer a specialized MILS Services Practice, delivering design, integration, and optimization services tailored for security applications, fully equipped to protect ITAR technical data and able to meet government accounting needs.

Figure 2: Wind River VxWorks MILS Platform Ecosystem

PARTNER ECOSYSTEM

Our world-class partner ecosystem, the most comprehensive and best-supported in the embedded software industry, ensures tight integration between Wind River technologies and those of the premier hardware and software companies whose complementary technologies we’ve chosen to augment and enhance our solutions. Partners help extend the capabilities of the Wind River development and run-time platforms by offering out-of-the-box integration and support for key capabilities.