

WIND RIVER

Wind River VxWorks MILS Platform 2.0

Companies responsible for creating potent defense, networking, industrial, and other infrastructure systems worldwide are demanding ever increasing functionality and secure and safe operation with very high assurance of protection from intentional or inadvertent threats or errors. At the same time, these systems must often operate with stringent requirements for reducing space, weight, and power (SWaP).

To meet these challenging demands, a new system architecture has emerged called multiple independent levels of security, or MILS. A MILS operating system partitions a single processor among multiple software components, with time and space resource allocation, information flow, and fault isolation all strictly enforced to conform to security policies defined by developers and system integrators.

Use of the MILS architecture enables reduction of SWaP through hardware consolidation. MILS enables security-critical applications, carrying confidential and critical data, to coexist on the same system with medium- or low-security applications that connect to non-secure channels or that have not passed the rigor of high security assurance validation. MILS is an architecture that enables both 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 members of coalitions).

Wind River VxWorks MILS Platform was created for security-certified partitioned systems. Wind River VxWorks MILS Platform 2.0 is a solution for software development of MLS and CDS devices with high security, high robustness, and high performance requirements. VxWorks MILS Platform is designed to be the foundation for your MLS and CDS systems.

VxWorks MILS Platform provides the ability to do the following:

- Run software components with multiple levels of data security on a single processor.
- Run software components with multiple data domains securely on a single processor.
- Run multiple levels of secure networks on a single processor.
- Isolate security-critical code into subcomponents for cost-effective assurance evaluation.
- Enable independent teams to work in parallel on subcomponents.
- Enable cost-effective technology refresh on subcomponents after deployment.
- Enable cost-effective reevaluation to required assurance levels after technology refresh.

Development Suite

XML Configuration	Agent-Based Debugging
GNU Compiler	Wind River ICE 2*
Wind River Workbench	Wind River Workbench, On-Chip Debugging Edition*

Software Partners

Common Criteria Certification Services	Ada for VxWorks
Formal Methods Analysis	Java Virtual Machine
MIL-STD-1553	OpenGL Graphics
Simulation	DDS

Operating System

VxWorks MILS

Hardware Partners

COTS Boards

Services

Education and Installation		Platform Customization	
System Design	Hardware/Software Integration	Design Services	

*Optional Components

Figure 1: Wind River VxWorks MILS Platform

Common Criteria Evaluation

Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard that enables accredited laboratories to evaluate device software to determine whether it meets the security requirements of a product. The National Information Assurance Partnership (NIAP) is a U.S. government initiative to administer the Common Criteria in the United States, under the Common Criteria Evaluation and Validation Scheme (CCEVS).

Features and Benefits

Wind River VxWorks MILS Platform 2.0 offers a range of benefits for defense device development teams, including the following:

- **Powerful two-level scheduling architecture:** VxWorks MILS implements a two-level scheduler that yields better system performance, reducing cost of goods, because a system based on VxWorks MILS Platform requires less processing power.
- **High assurance application support:** User components including applications, middleware, and drivers that require high assurance can use secure interpartition communication across multiple partitions, controlled by a strict policy configured by the system integrator.
- **Medium and low assurance application support:** User components that require medium or low assurance can utilize VxWorks Guest OS support, enabling reuse of existing VxWorks-based intellectual property.
- **Wind River Workbench development suite:** VxWorks MILS Platform includes the Workbench development environment, based on the widely adopted Eclipse framework. Workbench provides deep capabilities that support the entire software design and development life cycle, from hardware bring-up via JTAG or other connection, to platform and application development through agent-based debugging in a partition, to test and deployment, and enables standardization on one common development suite across the enterprise.
- **Tools for configuration and build partitioning:** VxWorks MILS Platform includes tools based on RTCA DO-297/ EUROCAE ED-124 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations, which support configuration and build partitioning of user code for complete application isolation throughout the product life cycle. This enables the reduction of initial development, integration, and certification time and costs as well as the costs for change and maintenance later in the development process.
- **Modular XML configuration data and security policies:** Independent XML-based configuration data and security policies for each user component help speed certification and recertification, reducing cost of obsolescence avoidance.
- **Common Criteria EAL6+ certification:** Wind River VxWorks MILS Platform is in evaluation to be certified to the Common Criteria (ISO/IEC 15408) Evaluation Assurance Level 6+/NSA high robustness.

Wind River VxWorks MILS Platform 2.0 is officially listed by NIAP as being in evaluation for conformance to EAL6+/NSA High Robustness under the CCEVS, in accordance to the U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness version 1.03. By using the VxWorks MILS Platform, users can focus their efforts on development and certification of their user components.

Separation Kernel for High Robustness

VxWorks MILS uses the two-level MILS OS architecture with partitioned environments. The VxWorks MILS separation kernel forms the lower-level operating system. The upper-level user partitions are where all user components (e.g., applications, middleware components, and drivers) execute. VxWorks MILS separation kernel is designed to meet the security specifications for a separation kernel compliant to the U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness version 1.03, or SKPP.

VxWorks MILS Platform 2.0 provides two user-mode execution environments for applications on virtual boards. The high assurance environment (HAE) is a small executive for high-security single-threaded applications that need certification to level EAL6+ under the Common Criteria. The VxWorks Guest OS is a more powerful environment for multitasking applications that shares many APIs with VxWorks 5 and the kernel of VxWorks 6. Developers can port drivers, applications, and middleware from VxWorks 5 and 6 to create medium and lower assurance components for VxWorks MILS Platform. Other important features of the VxWorks MILS Platform run-time include secure interpartition communications (SIPC), shared memory support, and security and safety auditing.

Optimized, Integrated Development Suite

VxWorks MILS Platform includes Eclipse-based Wind River Workbench. This development suite offers one common interface across all development phases of the security device through development, debug, and test. Workbench includes a project and build system, powerful debugging environments over JTAG connections and an OS-aware run-time debug agent, XML-based system configuration, the GNU compiler, and application multiplexed I/O (AMIO), which enables the individual console windows for each virtual board.

Workbench adheres to the DO-297 IMA Development Guidance and Certification Issues document, enabling roles-based security separation of intellectual property data. As part of this separation, XML-based configuration allows developers to make changes to application and/or system configuration information without rebuilding and retesting the entire system. In addition, changes to independent

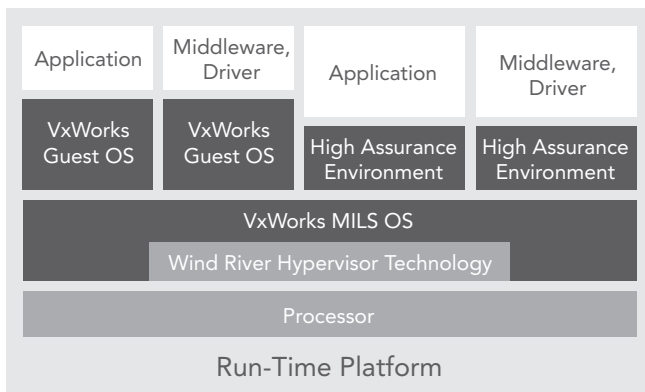


Figure 2: Wind River VxWorks MILS Platform run-time

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 device life cycle.

Proven, Reliable Partner

Common Criteria high-EAL/high-robustness evaluation is an exacting process requiring very close cooperation between the customer and OS vendor and requires several years for multilevel secure systems built on MILS. These activities must be carried out for the OS and middleware as well as the customer's application. Wind River's Professional Services organization has years of expertise in design and implementation of safe and secure systems. Wind River is committed to assisting its customers with their specific evaluation requirements.

Partner Ecosystem

Wind River's world-class partner ecosystem, the most comprehensive and best-supported partner ecosystem in the device software optimization (DSO) industry, ensures tight integration between Wind River technologies and those of the premier hardware and software companies we've chosen to build out our solutions. Partners help to extend the capabilities of Wind River's development and run-time platforms by offering out-of-the-box integration and support for key technologies.

Customer Support and Professional Services

VxWorks MILS Platform includes full access to Wind River's worldwide customer support organization, with 24/7 product support and training available through multiple channels. We also offer a specialized MILS Services Practice, delivering design, integration, and optimization services tailored for security applications, fully equipped to protect International Traffic in Arms (ITAR) technical data and able to meet government accounting needs.