WIND RIVER

# WIND RIVER VXWORKS MILS PLATFORM 3.0.0.1

## TABLE OF CONTENTS


Run-Time Components . . . 3
- Separation Kernel . . . 4
- Partition Management . . . 5
- Virtualization and Guest Operating Systems . . . 6
- High Assurance Environment . . . 6
- VxWorks Guest OS . . . 6
- Wind River Linux Guest OS . . . 6
- General Network Stack . . . 7
- High Assurance Network Stack . . . 7
- Inter-partition Communications . . . 7
- Security Auditing Logging and Safety Critical Logging . . . 8
- Hardware Support . . . 8
- Middleware . . . 9

VxWorks MILS Platform Development Environment . . . 9
- Eclipse . . . 10
- Project System . . . 10
- Build System . . . 10
- Debugging Environment . . . 11
- Host Shell . . . 11
- System Configuration . . . 11
- XML Compiler and Configuration Tools . . . 12
- Wind River GNU Compiler . . . 12
- Application Multiplexed I/O . . . 12

VxWorks MILS Security Evaluation Evidence Package . . . 13

Technical Specifications . . . 15
- Wind River VxWorks MILS Platform . . . 15
- Wind River Workbench 3.3.4 . . . 15
- Architectures, Hosts, and Board Support Packages . . . 15

Optional Wind River Components . . . 15

Partner Ecosystem . . . 16
- Hardware Partners . . . 16
- Software Partners . . . 16

Wind River Professional Services . . . 17

Wind River Education Services . . . 17

Wind River Customer Support . . . 17

Wind River® VxWorks® MILS Platform provides an operating run-time environment designed for systems having high security, high assurance, and high performance requirements. The 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 among multiple applications, manufacturers can significantly reduce the costs of the system by reducing size, weight, and power (SWaP) requirements. See Figure 1 for a high-level overview of the major components in VxWorks MILS Platform.

VxWorks MILS Platform can be used to partition a single processor among multiple software components, with time and space resource allocation, information flow control, and fault isolation all strictly enforced to conform to security policies defined by security architects and system integrators. As a result, 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 the 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). VxWorks MILS Platform is designed to be the foundation for your security-critical systems, MLS systems, and CDS systems.

Such systems often need to undergo a system-level security evaluation toward an eventual Authorization to Operate (ATO) or accreditation. To support such evaluations, VxWorks MILS Platform provides a security evaluation evidence package 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 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.

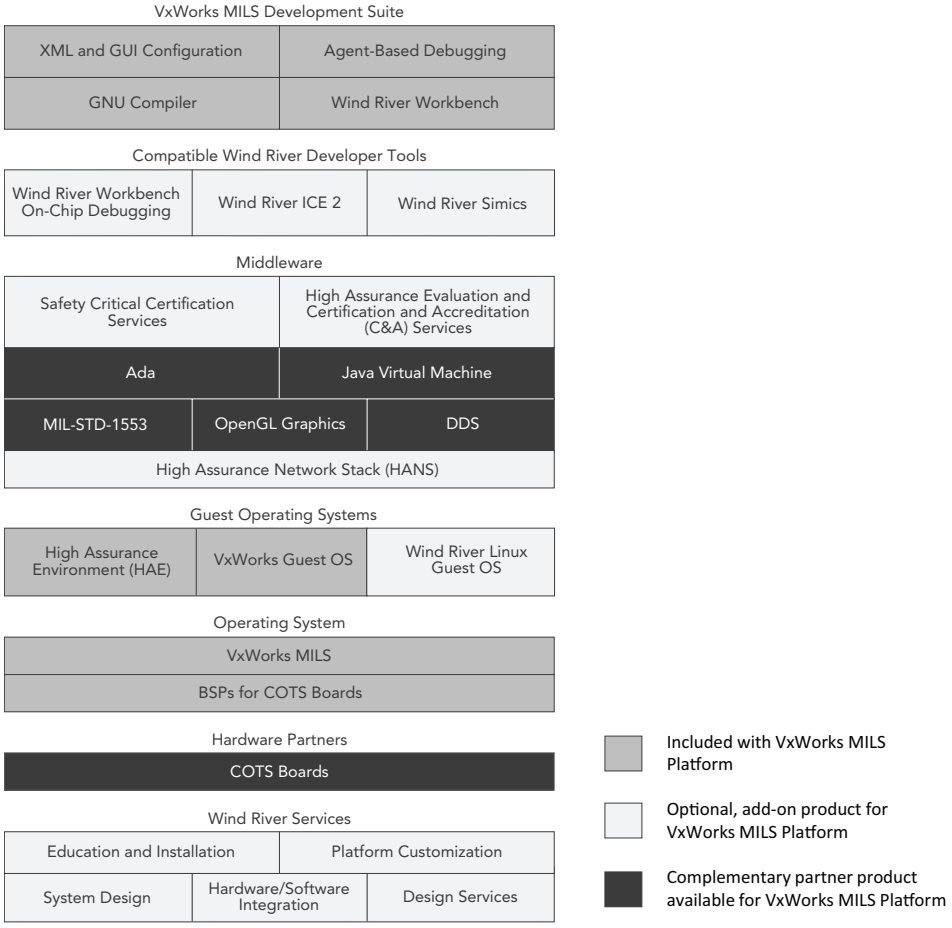


*Figure 1: Wind River VxWorks MILS Platform diagram*

## RUN-TIME COMPONENTS

Wind River VxWorks MILS Platform uses the MILS architecture to provide secure resource allocation and enable application isolation. These capabilities enable VxWorks MILS Platform to create secure, partitioned run-time environments with which to build MLS, CDS, and other security-critical systems. Figure 2 shows the major run-time components of the platform.

The key component of the MILS architecture, and of VxWorks MILS Platform, is the separation kernel that creates and manages the time and space partitions. Applications, middleware, and other code run in the user-mode application partitions on guest operating systems.

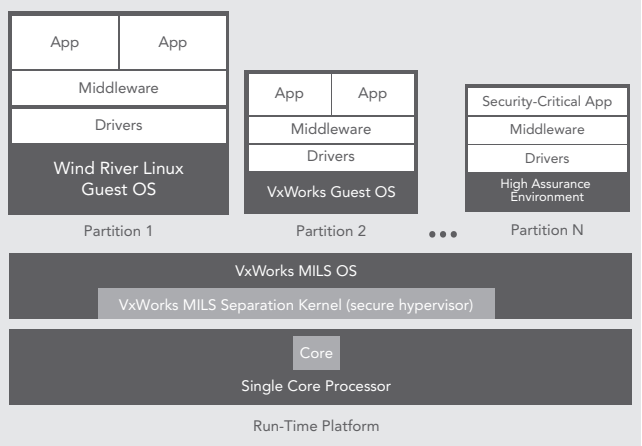


*Figure 2: Wind River VxWorks MILS Platform run-time components*

### Separation Kernel

The VxWorks MILS Platform separation kernel meets the security functional and security assurance requirements for a separation kernel compliant to the SKPP. Although the SKPP was sunset in 2011 as a basis for component-level evaluation, NSA continues to recommend the use of separation kernels for security-critical systems ("SKPP Sunset Q&A," www.niap-ccevs.org/announcements/SKPP%20Sunset%20Q&A.pdf, July 2011).

To achieve the functional requirements specified by the SKPP, the VxWorks MILS separation kernel performs only the four core capabilities of a separation kernel: space partitioning, time partitioning, information flow control, and fault isolation. No user components should run in the separation kernel, to ensure that the enforcement of security policies—through partitioning, information flow control, and isolation—are non-bypassable, evaluatable, always invoked, and tamper-proof (NEAT).

The separation kernel's goal is to minimize covert channels and ensure that the effects of any faulty or corrupt application are limited to the application's partition. Space partitioning is accomplished by allocating all resources under the control of the separation kernel into memory partitions called virtual boards. Time partitioning is accomplished by executing a time-sliced schedule, which the system architect creates to allot every virtual board the execution time it requires. Information flow is controlled through the use of a secure, inter-partition communication mechanism that only allows information to flow along configured channels. Fault isolation, or damage limitation, is achieved through partitioning and information flow control, as well as by implementing the "principle of least privilege," which limits the capabilities of each partition to just those required to accomplish its functions.

Guest operating systems run on the virtual boards, providing support to the user-mode applications, middleware, and drivers running in the partitions. The actions and data of applications in virtual boards are isolated by the separation kernel so that they cannot be detected by, or communicated to, applications in other virtual boards, except where such information flow has been explicitly configured.

**Partition Management**

Applications for a VxWorks MILS–based system are distributed among virtual boards. Virtual boards serve as containers for user components (e.g., applications, middleware, drivers), and are schedulable entities with allocated memory space and physical hardware. Space partitioning is enforced to ensure that actions and data are isolated. Strict control of data flow between virtual boards is enforced by the VxWorks MILS Platform secure inter-partition communication (SIPC) component according to predefined policies.

The VxWorks MILS separation kernel uses a high-performance, two-level scheduling architecture with very low overhead for context switching between virtual boards (see Figure 3). The separation kernel performs the first level scheduling, executing virtual boards run on a predetermined schedule, each during an allotted fixed time slice or slices in the overall schedule. The guest operating system within the virtual board performs the second level of scheduling, executing tasks, threads, and processes according to its local scheduling policy (e.g., priority-preemptive).

The two-level scheduling architecture enables VxWorks MILS Platform to provide near-native execution performance for each guest operating system, when the guest operating system's virtual board is executing during its allocated time slice or slices in the schedule.

To reduce response latencies between communications among virtual boards, VxWorks MILS Platform allows an application in a virtual board to donate part of its allocated execution time to an application in another virtual board, such as one in which a device driver runs. Execution time donation enables higher performance of a VxWorks MILS Platform system while maintaining robustness.

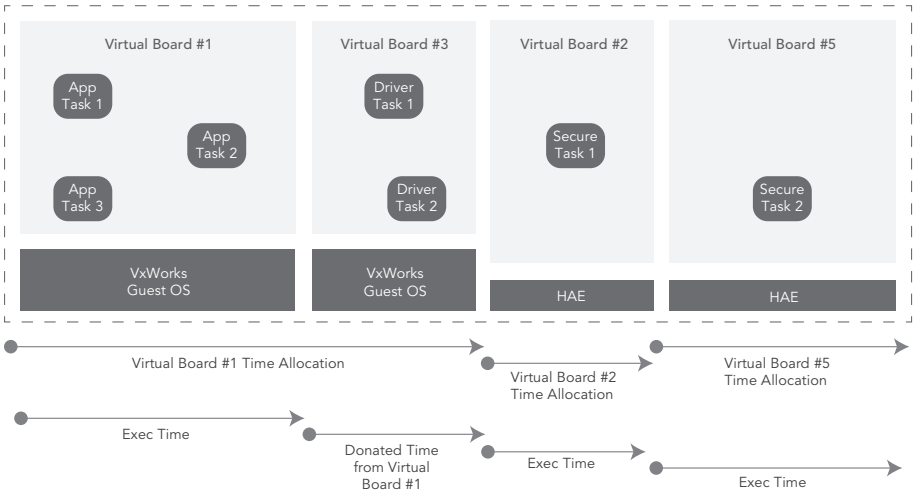


*Figure 3: VxWorks MILS Platform virtual board scheduler with time donation*

### Virtualization and Guest Operating Systems

The VxWorks MILS separation kernel includes hypervisor technology, leveraged from Wind River Hypervisor, that provides virtualization capabilities to enable guest operating systems to run in the VxWorks MILS Platform user-mode partitions, on virtual boards.

To enable a wide variety of user-mode applications, and to provide asset bridges for existing software, VxWorks MILS Platform supports multiple user-mode execution environments for applications on virtual boards:

- The High Assurance Environment (HAE) is a small, run-time executive for security-critical functionality or applications that may require high assurance certification or accreditation.
- VxWorks Guest OS is a powerful, real-time operating system (RTOS) environment for multitasking applications that can be validated at medium or low security assurance levels.
- Wind River Linux Guest OS provides a full Linux kernel and user mode environment for reuse of existing Linux and other open source code on VxWorks MILS–based systems.

### High Assurance Environment

User components that have high assurance evaluation or certification and accreditation (C&A) requirements can run in the HAE, a small, single-threaded, user-mode execution environment for virtual boards that provides an ANSI C programming interface and SIPC.

Following the MILS architecture, security-critical portions of applications should be separated from non-security-critical portions and run on the HAE. Examples of such security-critical components are data guards, data filters, and downgraders. By isolating security-critical components, the amount of code requiring high assurance evaluation can be reduced, while enabling higher scrutiny of such code, leading to systems with higher assurance of overall security.

### VxWorks Guest OS

Applications with less stringent security requirements can run on a VxWorks Guest OS virtual board. VxWorks Guest OS provides the standard VxWorks priority-preemptive multitasking environment within a virtual board, and also provides standard VxWorks RTOS system services, including task synchronization, inter-task communication, and I/O system calls.

VxWorks Guest OS enables portability from existing and legacy VxWorks-based products. Because it directly shares its codebase with the partition OS from VxWorks 653, developers can repurpose ARINC 653 applications for VxWorks MILS Platform. In addition, VxWorks Guest OS shares many APIs with VxWorks 5 and the VxWorks 6 kernel. Developers can port drivers, applications, and middleware from VxWorks 5 and 6 to create medium and low assurance applications and components for VxWorks MILS Platform.

### Wind River Linux Guest OS

VxWorks MILS Platform includes support for Wind River Linux to run as a guest OS on virtual boards. This enables Linux and other open source applications and middleware to run on VxWorks MILS Platform–based systems. Wind River Linux 4.3 Guest OS provides the same commercial-grade, embedded Linux solution as standalone Wind River Linux, with a standard 2.6.34 kernel, GNU GCC 4.4.1, and outstanding performance on industry-standard benchmarks as a guest OS.

Wind River Linux Guest OS contains a pre-integrated, fully tested, validated, and supported Linux distribution with rich tools, and uses the same Wind River Workbench development environment used with VxWorks MILS Platform. Wind River Linux Guest OS also provides core networking, connectivity protocols, and NFS client support.

### General Network Stack

General Network Stack is an IPv4-based network stack that runs on, and is included with, VxWorks Guest OS. It provides UDP, TCP, IGMP, multicast, and other basic networking capabilities similar to most Unix-like operating systems. This network stack is suitable for use with low and medium assurance applications and components.

### High Assurance Network Stack

High Assurance Network Stack (HANS) is an optional, add-on product available for VxWorks MILS Platform 3.0.0.1. HANS uses a two-partition architecture to provide an IPv4-based network stack capable of supporting separated data streams, thus enabling multi-single-level secure (MSLS) networking, or networking for CDS systems.

The High Assurance Network Foundation Layer runs in an HAE virtual board and can discriminate incoming and outgoing packets based on data labeling (e.g., 802.1Q virtual LAN support) to separate data streams and route them to the High Assurance Protocols Stack on the appropriate application virtual boards. This network foundation layer has been designed and developed to be amenable to high assurance evaluation or C&A.

The High Assurance Protocols Stack runs on a VxWorks Guest OS virtual board and supports IPv4-based UDP, TCP, IGMP, and multicast. The High Assurance Network Foundation Layer is capable of supporting multiple data streams destined for multiple High Assurance Protocol Stacks of different applications, each running on a separate VxWorks Guest OS virtual board. The dual-partition architecture of HANS also enables multiple VxWorks Guest OS applications to share a common Ethernet port in a secure manner.

### Inter-partition Communications

The VxWorks MILS Secure Inter-partition Communications (SIPC) component provides a secure communication mechanism between virtual boards. SIPC guarantees data delivery, so data can reach only the intended recipient virtual board. SIPC is suitable for high assurance evaluation or C&A and can be used by user components running in the HAE, on VxWorks Guest OS, or on Wind River Linux Guest OS. Its API is designed around the ARINC 653 APEX queuing and sampling port interfaces, providing a programming environment familiar to ARINC 653 developers, as well as enabling ARINC 653 applications to be ported into VxWorks MILS Platform.

SIPC ensures secure control of information flow between user partitions (see Figure 4). Messages pass from one virtual board to another through unidirectional channels, following security flow policies specified using configuration at system integration time.

Shared memory may also be used as a form of secure inter-partition communication between virtual boards. Shared memory regions have access privileges that are configured in the system security policy and enforced at run time by the separation kernel. Once granted access to a shared memory region, two virtual boards can share data by writing to and reading from that region. For legacy applications and drivers relying on shared memory, this feature allows straightforward porting to the VxWorks MILS Platform environment in the HAE, on VxWorks Guest OS, or on Wind River Linux Guest OS.

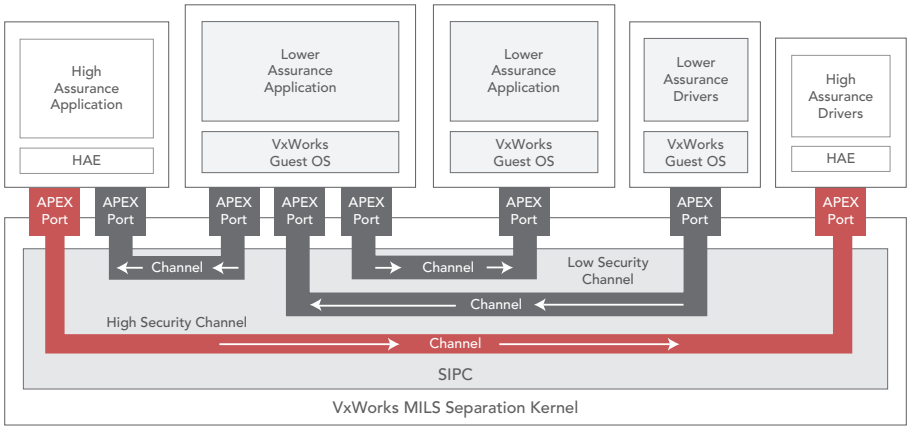


*Figure 4: VxWorks MILS SIPC*

### Security Auditing Logging and Safety Critical Logging

VxWorks MILS Platform manages two kinds of logs: security audit logs and safety critical logs. Each virtual board has both a security audit log and a safety critical log; there is also a security audit log and a safety critical log for the MILS kernel.

Security audit logs record events that could impact the security of the MILS system. Safety critical logs record events that could impact the stability of applications in the MILS system; these can also be generally used by applications to record any type of event. Both types of logs are managed at the MILS system level, and applications can be configured to be enabled to collect (i.e., read) the logs. Access privileges to the security audit and safety critical logs are part of the VxWorks MILS system security policy configuration.

### Hardware Support

Device drivers and the network stacks run on virtual boards. They have allotted space partitioning and share the same data isolation and fault isolation properties as applications. They can run in specific time slices just like applications, or they can be called like middleware and run in the time slice of the calling application though the VxWorks MILS execution time donation.

VxWorks MILS Platform includes support for Ethernet and RS-232 drivers, and provides board support packages (BSPs) for the Curtiss-Wright VPX6-185 (with PowerPC MPC8641D processor) and Wind River SBC8548 (with PowerPC MPC8548 processor). Partner technology is available for MIL-STD-1553 support.

### Middleware

Middleware that is available for VxWorks can be ported to the VxWorks Guest OS. Middleware enables applications to take advantage of advanced technologies in a MILS system. Complementary technologies for VxWorks MILS Platform that are enabled by middleware include the following:

- Ada (through Wind River partner AdaCore)
- Data Distribution Service (DDS) (through Wind River partner RTI)
- Java Virtual Machine (through Wind River partner Atego)
- OpenGL (through Wind River partner Presagis)

## VXWORKS MILS PLATFORM DEVELOPMENT ENVIRONMENT

Wind River VxWorks MILS Platform includes the Wind River Workbench development suite. This Eclipse-based development environment offers one common interface across all development phases from board bring-up through development, debug, and test, for all of the VxWorks MILS Platform run-time environments (see Figure 5). Workbench inherits Eclipse's intuitive development environment for working with complex code. Many Wind River partners extend the development environment to provide more powerful design and analysis tools.

Workbench includes the following components:

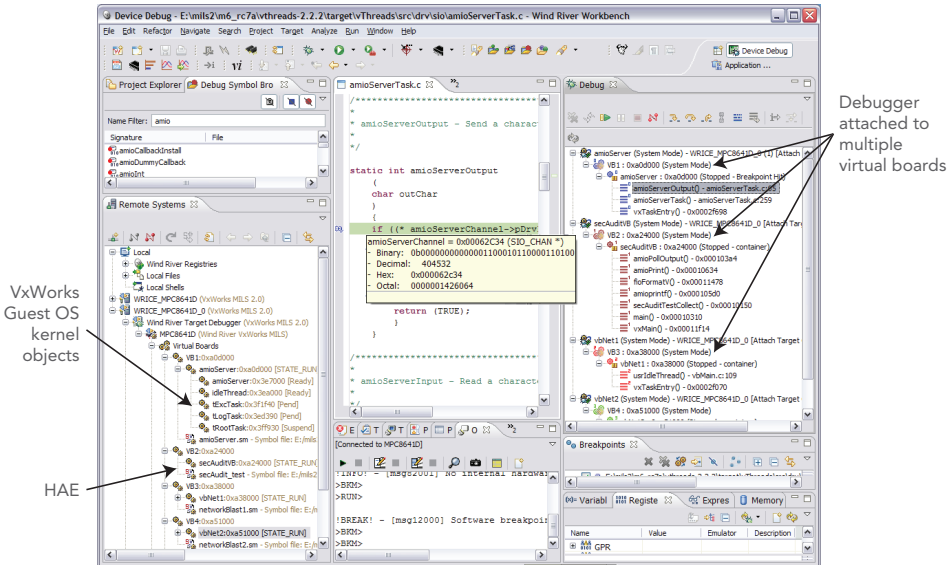


*Figure 5: Wind River Workbench in VxWorks MILS Platform*



WIND RIVER

### Eclipse

Open, extensible, and backed by a strong community of commercial and open source developers, the Eclipse framework supplies the necessary infrastructure to graphically and functionally integrate the components of Workbench, and a wide range of additional integrated functionality. Wind River has extended the Eclipse framework with unique technology to handle the complexity of project management and debugging in partitioned operating systems such as VxWorks MILS.

### Project System

The Workbench project system allows developers to organize and manage the primary components in a VxWorks MILS Platform development project, including source files and target systems.

VxWorks MILS Platform projects of different types can be created for configuring and building VxWorks MILS separation kernel images as well as images for HAE, VxWorks Guest OS, and Wind River Linux Guest OS virtual boards for MILS application development. By design, Workbench enables users to manage multiple projects simultaneously and independently so that information separation between different development groups can be assured.

### Build System

Security-critical systems can be extremely complex, with a large number of components integrated into one system, each with strict policies on the data it can expose or isolate. The challenge in developing this complexity is managing each sub-project so that all teams can work independently, developing independent components in parallel and asynchronously. Throughout the lifecycle of such systems, applications are extended and modified over time. Since system-level evaluation or C&A is costly and time-consuming, the development process must minimize the system-level effects of component integration, thus minimizing any impact on existing evaluation evidence, for cost-effective scalability and extensibility over the system's lifetime.

VxWorks MILS Platform supports this modularized approach for handling parallel development, complex teamwork, and system integration. The Workbench build system specifies the tools, options, and parameters to use when building VxWorks MILS Platform software projects, enabling developers to set build parameters easily from the project level down to the individual file level. The build system, using RTCA DO-297 ("Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations") role-based separation, supports independent build, link, and load (that is, the individual components do not require source or binaries from other parts of the system to build, link, and load). In this way, each team working on a component can manage its own build independently of other teams. Furthermore, the system impact of integrating or changing a particular component can be minimized, facilitating system-level evaluations and re-evaluations.

Finally, the system integrator collects the image files, created independently by each component team, for integration into the complete MILS system. VxWorks MILS Platform provides powerful configuration tools for the system integrator to define strict policies for each application and the inter-application communication mechanism.

### Debugging Environment

The debugging environment in VxWorks MILS Platform extends the powerful debug and analysis capabilities of Eclipse to provide kernel debugging, virtual board debugging, time-slice-specific breakpoint management, symbol browsing, and stack tracing, with device connections and context awareness. The debug environment between Workbench and the MILS system can be in one of the following modes:

- An on-chip debugger using JTAG allows VxWorks MILS separation kernel bring-up debugging, Wind River Linux Guest OS kernel debugging, and debugging in HAE and VxWorks Guest OS environments.
- The VxWorks MILS Platform run-time debug agent allows debugging of software components running in the HAE and VxWorks Guest OS, executing in a virtual board.
- The Wind River Linux user-mode agent allows Workbench debugging of software components running on Wind River Linux Guest OS in user space.

Wind River Workbench On-Chip Debugging is a JTAG-based environment for debugging hardware bring-up, BSP development, and virtual board initialization, as well as application development. Workbench On-Chip Debugging provides source-level debugging in system mode with full system visibility and control, using separate connections to each virtual board.

The VxWorks MILS Platform run-time debug agent provides a debugging environment through an Ethernet connection, useful when JTAG is unavailable. The agent can be used to debug HAE components and VxWorks Guest OS components. It can be configured in and out of the system with no impact to evaluation or certification, and can also be configured to debug only a certain subset of virtual boards, to limit system visibility to only what is important to a particular application supplier.

### Host Shell

The host shell provides a command-line interface with gdb syntax for debugging in HAE and VxWorks Guest OS environments. The host shell uses either the VxWorks MILS debug agent or on-chip debugging to communicate with the MILS system, and provides run control and register and memory access.

The host shell receives commands, executes them locally on the development host, and dispatches requests to the run-time agent on the MILS system for any action involving the symbol table, applications, or data. Since the shell executes on the host system, it can be used with minimal intrusion on the MILS system resources in the lab development environment.

In addition, the host shell can also be used for interactive debugging and monitoring, or for scripting and batch mode operations such as automated testing.

### System Configuration

The build system for VxWorks MILS Platform supports the role-based separation approach to development. Virtual boards are independently built, linked, and loaded, but can still reference the entire system. The image files from virtual boards can be independently loaded and updated on the system.

The VxWorks MILS Platform system configuration specifies the security policies of each MILS object, including scheduling, virtual board resource access, and SIPC. The underlying configuration data is based on XML schemas and tables, similar to ARINC 653 configuration data. For security and certification purposes, translation of system configuration data into binaries must be traced. All tools performing the translation must be proven to be reliable and consistent.

### XML Compiler and Configuration Tools

VxWorks MILS Platform security policies are written in XML. These XML files are compiled into binary objects and linkable images using the Wind River XML configuration generation tools, including XML Configuration Verification (VerCon-X) and Configuration Vector Generation (CVGEN). These configuration images are then loaded on the target to be referenced during system boot.

These XML configuration tools allow developers to make changes to application and system configuration information without rebuilding and retesting the entire system. Changes to software components can be made without the need to retest other components in the system or the underlying VxWorks MILS separation kernel. This can significantly reduce the time for initial evaluation or C&A, as well as reduce the cost of change and maintenance throughout the MILS system lifecycle. In addition, these tools fully comply with the DO-297 document, enabling intellectual property and security separation between the platform provider, application developer, and system integrator.

### Wind River GNU Compiler

Several versions of Wind River GNU Compiler are used for the different run-time environments in VxWorks MILS Platform. Wind River has modified general distribution versions of the compiler specifically for use with the VxWorks product line.

- GNU GCC 4.1.2 is the default compiler for the VxWorks MILS separation kernel, for the HAE, and for user components that run in the HAE.
- GNU GCC 4.3.3 is the default compiler for the VxWorks Guest OS and all user components that run on the VxWorks Guest OS.
- GNU GCC 4.4.1 is the compiler version for Wind River Linux Guest OS as well as all user components and software that run on Wind River Linux Guest OS.

### Application Multiplexed I/O

Console I/O sent from MILS system–based applications to the development host are often used in the course of development and for demonstration purposes. The console output can provide valuable troubleshooting data that can shorten the debugging cycle. For MILS systems with a single serial port and multiple virtual boards, VxWorks MILS Platform includes Application Multiplexed I/O (AMIO), which provides the capability for the serial port to be shared among multiple virtual boards. Once configured with AMIO, a VxWorks Guest OS application can read from and write to the serial port using standard VxWorks I/O APIs as if it had sole use of the serial port.

On the host side, de-multiplexing I/O is performed by the Wind River Monitor host application. Console I/O for each virtual board is displayed in a separate AMIO console window as if multiple independent systems were running, enabling easy viewing of I/O from each virtual board. Thus, serial port sharing is transparent to the developer.

## VXWORKS MILS SECURITY EVALUATION EVIDENCE PACKAGE

Systems built using Wind River VxWorks MILS Platform may undergo an evaluation by a government or other agency to assess the level of assurance that the system security requirements have been met. Such an evaluation may be required, for example, to obtain an ATO for the system, or to pass a C&A process.

A system-level evaluation depends on the target of evaluation (TOE), which comprises the specific hardware, software, and configurations used by the system. System manufacturers will have to meet the requirements of their system's particular evaluation or C&A process, which may include providing documentation as to how the system's underlying separation kernel provides assurance that the system security policies are met.

The VxWorks MILS Security Evaluation Evidence Package provides this type of documentation for VxWorks MILS Platform, which a system manufacturer can use as part of its overall evaluation or C&A documentation package. The VxWorks MILS Security Evaluation Evidence Package is based on the SKPP and the Common Criteria 2.3.

In addition, since VxWorks MILS Platform may be used to provide security for avionics systems, it has been designed to meet the safety critical requirements of RTCA DO-178C (EUROCAE ED-12C) DAL A. The VxWorks MILS Security Evaluation Evidence Package includes safety critical certification evidence in accordance with that standard.

Specifically, the VxWorks MILS Security Evaluation Evidence Package includes the following:

- VxWorks MILS Security Target
- VxWorks MILS source code files and binary files
- Security evaluation evidence:
  - Configuration Management (for Common Criteria assurance class ACM)
    - Configuration list
    - CM plan
    - CM audit records
    - Acceptance plan and procedure evidence
    - Integration procedures and evidence
  - Development (ADV)
    - Architectural design
    - Configuration vector generation and validation documentation
    - Semiformal functional specification
    - Design documents

    - Coding standard
    - Trace tables
  - Guidance Documents (AGD)
    - Administrator guidance
    - User guidance
  - Lifecycle Support (ALC)
    - Development security documentation
    - Evidence of use of security measures
    - TOE developer flaw remediation procedures
    - TOE user flaw remediation procedures
    - Lifecycle definition documentation
    - Development tools and techniques
  - Testing (ATE)
    - Functional test plan
    - Test procedure description
    - Expected test results
    - Actual test results
    - Analysis of test coverage
    - Analysis of depth of testing
  - Vulnerability assessment (AVA)
    - Systematic covert channel analysis results
    - Internal documentation on insecure states
    - Vulnerability analysis documentation results
- VxWorks MILS 3.0.0.1 DO-178C DAL A Certification Evidence
  - Plan for Software Aspects of Certification (PSAC)
  - Software Quality Assurance Plan (SQAP)
  - Software Configuration Management Plan (SCMP)
  - Software Development Plan (SDP)
    - Software requirements standards
    - Software design standards
    - Software coding standards
  - Software Verification Plan (SVP)
  - Software Requirements Specification (SRS)
  - Software Design Document (SDD)
  - Software Lifecycle Environment Configuration Index (SECI)
  - Traceability matrix
  - Software development folder
    - Design reviews
    - Code reviews
    - Test reviews
    - Functional tests
    - Coverage results
  - Software Accomplishment Summary (SAS)
  - Software Vulnerability Analysis (SVA)

The VxWorks MILS Security Evaluation Evidence Package applies to the VxWorks MILS kernel and the HAE. Note that the package is currently only available for the single core version of VxWorks MILS Platform.

## TECHNICAL SPECIFICATIONS

### Wind River VxWorks MILS Platform

- VxWorks MILS 3.0.0.1 separation kernel
- VxWorks MILS High Assurance Environment (HAE) 1.2
- VxWorks MILS VxWorks Guest OS 1.1
- VxWorks MILS 3.0.0.1 General Network Stack, with IPv4, UDP, and TCP
- VxWorks MILS 3.0.0.1 Secure IPC (SIPC)
- VxWorks MILS 3.0.0.1 device drivers: RS-232 and Ethernet

### Wind River Workbench 3.3.4

- Eclipse 3.8.1 framework
- MILS system configuration
- MILS project system
- MILS build system
- Debugger
- Host shell
- VxWorks MILS debug agent
- Wind River GNU Compiler 4.1.2 and 4.3.3
- Index-based global text search-and-replace

### Architectures, Hosts, and Board Support Packages

*Supported Target Architectures*

- PowerPC 86xx (MPC8641D)
- PowerPC 85xx (MPC8548)

*Supported Hosts*

- Microsoft Windows XP Professional (Service Pack 3), x86-32
- Microsoft Windows 7 (Service Pack 1), x86-32 or x86-64

*Supported Board Support Packages*

- BSP for Curtiss-Wright VPX6-185
- BSP for Wind River SBC8548

## OPTIONAL WIND RIVER COMPONENTS

The following products are available as optional, add-on components to Wind River VxWorks MILS Platform 3.0.0.1:

- High Assurance Network Stack (HANS) 1.1 for VxWorks MILS 3.0.0.1
- Wind River Linux 4.3 Guest OS for VxWorks MILS 3.0.0.1

- Wind River Workbench On-Chip Debugging 3.3.4
- Wind River ICE 2
- Wind River Probe

## PARTNER ECOSYSTEM

The Wind River partner ecosystem ensures tight integration between Wind River core technologies and those of the premier hardware and software companies chosen to complement Wind River solutions. The Wind River Customer Support team is trained to troubleshoot partner technologies used with Wind River products.

### Hardware Partners

Wind River hardware partners for Wind River VxWorks MILS Platform include the following:

- Curtiss-Wright Controls Embedded Computing
- Freescale
- GE Intelligent Platforms

For a full list of Wind River hardware partners, refer to www.windriver.com/partners.

### Software Partners

Technology components provided by our software partners include the following:

| Tools | Partner |
|---|---|
| Ada support | AdaCore |
| Java | Atego (Aonix) |
| Graphics | Presagis |

Software development tools provided by our software partners include the following:

| Tools | Partner |
|---|---|
| Ada development tools | AdaCore |
| Java development tools | Atego (Aonix) |
| Qualified graphics design tools | Presagis |

## WIND RIVER PROFESSIONAL SERVICES

Wind River VxWorks MILS Platform is complemented by Wind River Professional Services, a CMMI Level 3–certified organization that provides security-critical device and system manufacturers with expert outsourced engineering services. Experienced aerospace and defense specialists are available to help with implementing parts or all of the system. Services include installation and orientation, design of partitioned RTOSes, assistance with creating security-critical code, BSP and driver migration and creation, software system and middleware integration, legacy application and infrastructure migration, platform extensions, and process compliance.

For more information, visit www.windriver.com/services/aerospace_and_defense.html.

## WIND RIVER EDUCATION SERVICES

With more than 30 years of embedded software experience, Wind River provides education services in every region of the world. For VxWorks MILS Platform, we offer flexible training options to meet your business and learning needs, including public, private, and custom courses. For your specific project challenges, Wind River Mentoring provides coaching by experienced engineers to help you integrate Wind River solutions into your environment. And when you're too busy to attend a whole class, our on-demand learning options provide around-the-clock access to advanced and specialized topics. All of our education services are led by expert engineers who are closely connected to the Wind River technical community for access to specific expertise.

For more information, visit www.windriver.com/education.

## WIND RIVER CUSTOMER SUPPORT

Wind River VxWorks MILS Platform is backed by our award-winning global support organization. With six major support centers, 21 additional support hubs, and more than 150 experts worldwide, you can get the help you need in the language and time zone that work best for you. Our online Wind River Support Network provides multifaceted self-help options, including an active Q&A Forum. Optional premium services are available, including designated support engineers and hosting of customer-specific environments. Wind River Customer Support has achieved Service Capability and Performance certification.

Customers with a current maintenance or subscription agreement are eligible for all updates of VxWorks MILS Platform free of charge. Customers under a current subscription are also eligible for all upgrades of VxWorks MILS Platform free of charge.

For more information, visit www.windriver.com/support.

WIND RIVER

Wind River is a world leader in embedded software for intelligent connected systems. The company has been pioneering computing inside embedded devices since 1981, and its technology is found in more than 1 billion products. To learn more, visit Wind River at www.windriver.com

©2014 Wind River Systems, Inc. The Wind River logo is a trademark of Wind River Systems, Inc., and Wind River and VxWorks are registered trademarks of Wind River Systems, Inc. Rev. 01/2014