WIND RIVER

Wind River High-Assurance Solutions for Aerospace & Defense

Providing trusted data and sharing secure information have become critical for warfighters in preventing mission compromise, for homeland security personnel in thwarting terrorist attacks, and for first responders in improving readiness for emergencies, while simultaneously reducing device space, weight, power, and operating costs. The answer is multilevel secure (MLS) systems: systems that can run applications at different security or safety levels, from different agencies, or in multination coalitions, on a single processor, with very high assurance that each application is separate and communicates with all others only according to precisely defined security policies.

The problem? With current technologies, multilevel secure systems cannot be practically built on a single processor. While existing multilevel secure systems can process information according to precisely defined security policies enforced with very high assurance, this has traditionally meant building systems with multiple physically separated hardware elements—separate computers, separate areas on a field-programmable gate array (FPGA), separate displays, or separate networks—all requiring expensive equipment and operating procedures.

Wind River, the leader in Device Software Optimization (DSO), has set out to change this by developing the VxWorks MILS platform. Based on open standards, proven operating system technology, and development tools, VxWorks MILS includes comprehensive customer education, support, and services, and, most importantly, a deep partnership with you. We believe this relationship is essential to building and certifying a high-performance MLS system. Together, we'll make your entire system work. Wind River can get you on the road to achieving multilevel systems that are safe, secure, affordable, and certified.

The Need: Secure and Safe Real-Time Operating Systems

What if your developers could architect, design, build, certify, and accredit multilevel secure systems that meet the following requirements?

- Reduce hardware, power, cooling, weight, and space for tightly constrained devices
- Secure communication within an enclave and between systems in different enclaves in the larger Global Information Grid (GIG)
- Resist stressful attacks and degrade securely and gracefully
- Provide simultaneous access by users with different security clearances and need-to-know, while preventing unauthorized access to information (alignment of personnel clearance level and task)

> "Two decades ago, a similar MLS system development would have taken 10 or more years, with monolithic secure operating system evaluation at $50 million to $100 million."
>
> *— Mark Vanfleet, Mathematician, INFOSEC Security Analyst, National Security Agency and a MILS community leader*

> "Development, evaluation, and NSA certification of a highly robust MLS/CDS system—including both application and RTOS—is expected to take three or more years, with RTOS evaluation at a cost of $3 million to $5 million."
>
> *— Dr. Ben Calloni, Lockheed Martin Fellow for Software Security and a MILS community leader*

- Reduce time and cost for development, certification, and accreditation
- Shorten time and reduce cost to reconfigure systems and to add applications
- Lower maintenance cost for spares and training
- Achieve security evaluation, certification, and accreditation within a reasonable and predictable time and cost

What if you could meet these requirements while also meeting guidelines governing the acquisition of information assurance (IA) products for Department of Defense (DoD) programs?

Recognizing that technological advances and threats have drastically changed the way we think about protecting our computing and communications systems, the U.S. Government has issued a policy governing the acquisition of IA products for DoD programs called the National Security Telecommunications and Information Systems Security Policy (NSTISSP No. 11). Since July 2002, all commercial off-the-shelf (COTS) IA products must be evaluated, validated, and certified in accordance with the

Common Criteria for Information Technology Security Evaluation by accredited commercial laboratories. That means these multilevel systems must meet the appropriate evaluation assurance levels (EAL). For critical multilevel systems in the United States, the requirement from the National Security Agency (NSA) is "high robustness," relatively equivalent to Common Criteria EAL6+.

Wind River asserts that MILS (Multiple Independent Levels of Security) is the answer to all these requirements.

The Solution: Multiple Independent Levels of Security

MILS is a software architecture that makes development, certification, accreditation, and deployment of multilevel-capable systems more practical, achievable, and affordable. It can significantly increase protection, reduce development time, and reduce schedule risk in building high-assurance systems that are both safe and secure. Although MILS was created in the 1980s, technology in our industry had not advanced enough to take advantage of it until recently—and until now, a high-performance system implementation did not exist.

A MILS real-time operating system (RTOS) alone does not guarantee that a system is multilevel secure. Further, neither MILS nor Common Criteria certification guarantee that a system is functionally suitable, has adequate performance, or will achieve acceptable lifetime total cost of ownership. Overall system architecture, as well as the properties of middleware, applications, and communications, must all meet functional and performance requirements as well as security requirements. But MILS, using open standards–based COTS products, can be the base for successful high-assurance, high-performance multilevel secure systems. That's where Wind River comes in.

The Wind River MILS solution provides a layered software architecture (RTOS, middleware, applications, and communications) that when combined with an appropriately rigorous certification process enables your developers to create multilevel secure systems.

The VxWorks MILS Platform

Wind River's VxWorks MILS platform combines an OS and tools with middleware, comprehensive customer education, support, and services.

Unlike other commercial MILS implementations, our solution offers performance advantages for drivers, middleware, and applications that ensure that your overall system meets its performance requirements. VxWorks MILS maintains consistent, deterministic, industry-leading system performance, whether your system needs only a few partitions or dozens. We designed VxWorks MILS from the ground up so you can develop and scale systems for your needs, and we did so without compromising performance. This means, as a system developer, you need not worry about RTOS scalability or flexibility when using VxWorks MILS.

The advantages of VxWorks MILS don't stop with these significant performance capabilities. At Wind River, we work hand-in-hand with your organization to help you define and refine the overall system architecture, as well as guide you through the Common Criteria evaluation process. We recognize that to be competitive in the aerospace and defense market, device manufacturers must deliver increasingly complex products on budget and within increasingly stringent schedules. VxWorks MILS helps you meet these business objectives.

Wind River's VxWorks MILS includes the optional Wind River Trusted Stack, a network stack that meets the highest level of Common Criteria certification. In addition, PCS*express*, a partition communication system from Wind River partner Objective Interface Systems, is available as a complement to the Trusted Stack, to enable secure intrasystem and intersystem communications.

To accelerate time-to-market for developers building devices with VxWorks MILS, the platform also includes the Wind River Workbench development suite based on standard Eclipse. Wind River Workbench provides developers with a common interface for all phases of MILS development, debug, and test.

VxWorks MILS Capabilities and Benefits

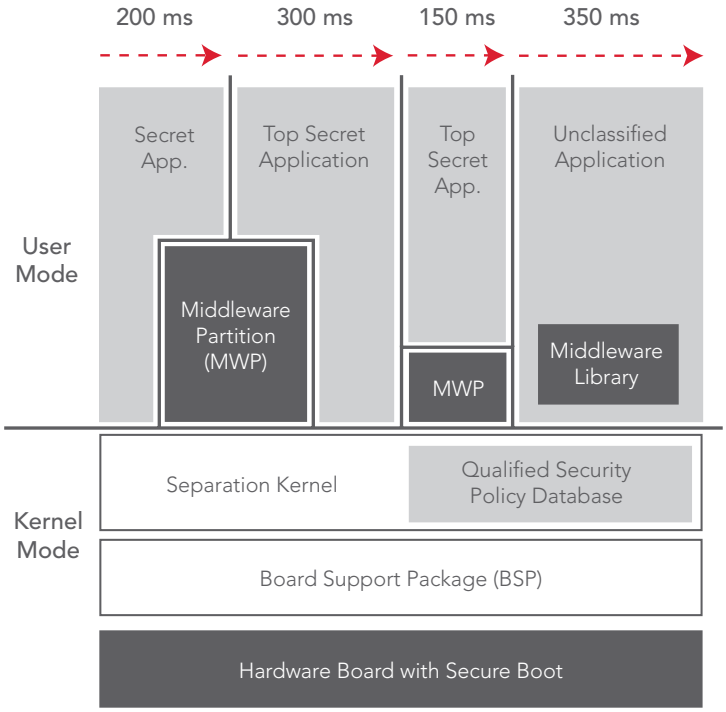
Architecture Development and Deployment

By using VxWorks MILS to implement your complete MLS architecture, you can take advantage of the following:

- **Secure kernel:** Provides robust time and space partitioning conformant to the Separation Kernel Protection Profile (SKPP) under the Common Criteria and is suitable for evaluation to high EAL
- **Security policy database:** Defines resources available to applications and middleware, communications between applications, health monitoring, security audit log, and other features
- **Reference monitor:** Ensures that applications conform to the security policy database
- **Secure audit log:** Provides a log of all attempted violations of security policy and gives reporting access for trusted applications
- **Flexible driver model:** Permits drivers in kernel, middleware, or application layer, or drivers split among two or three layers, to maximize performance within given security requirements
- **High-performance middleware layer:** Supports device drivers, file system, network stack, CORBA, PCS*express*, and other components
- **Secure boot:** Confirms that the booted OS, middleware, and applications are the same as those certified/developed with your company
- **Secure delivery:** Proves that the delivered modules are the same as those certified/developed with your company

Enhanced Flexibility and Portability

Wind River's VxWorks MILS solution provides the following partition operating system APIs: VxWorks, ARINC 653, and POSIX. By offering multiple APIs, we provide you with greater



- **Two Middleware Partitions**
  - Drivers, file system, trusted stack, IPv6, etc.
  - Wind River, customer, or third parties
  - Middleware partitions run in caller's time slot
- **Four Application Partitions**
  - 1 secret
  - 2 top secret
  - 1 unclassified, with its own middleware
- **Time Partitioning**
  - Application partitions run round-robin with exact times, low jitter
  - Very low partition switch time and cache clear if needed

Figure 1: VxWorks MILS system architecture example

flexibility and help reduce the work required to port legacy applications based on VxWorks 5.5, VxWorks 6 kernel mode, ARINC 653, and POSIX applications to VxWorks MILS.

Rapid Configuration with XML

VxWorks MILS includes a powerful, qualified, XML-based rapid configuration tool that enables private and secure insertion and reconfiguration of new applications and security policies. This translates into significant reductions in time and cost during initial development and certification, as well as later in the device life cycle when reconfiguration and/or recertifying applications may be required.

The following are key features of the configuration tool:

- Ability to easily define the static configuration records required for all MILS applications, including the security policy database
- Ability to make changes to independent applications and/or configuration information without rebuilding the entire system, retesting, or recertifying other applications or the underlying OS—unlike "unqualified" systems, where changes may affect other applications and the entire system
- Complete separation of intellectual property and security between the platform provider, application developers, and system integrator, or between application developers at different security classifications
- Full compliance with the DO-297 IMA Development Guidance and Certification Issues Document

The result: the ability to rapidly deploy and redeploy multilevel secure systems (e.g., systems mixing top secret, secret, unclassified, and/or multinational data) without compromising the security or safety of any element.

Powerful Development Environment

Most proprietary development solutions limit flexibility, restrict interoperability of systems, and actually increase the costs of development. Wind River has taken a different approach to helping our MILS clients succeed. Wind River Workbench, based on the Eclipse platform, is a suite of development tools that accelerates time-to-market for developers building devices with VxWorks MILS. Through tight integration with Wind River's RTOSes, Workbench offers the only end-to-end, open standards–based collection of tools for device software design, development, debugging, test, and management.

Unique to this platform are three high-performance tools to aid in the deployment of certified applications in partitioned OS environments. These tools enable your developers to do the following:

- Measure CPU use by individual applications or all applications
- Report memory usage of various areas of the OS, including heaps, stacks, ports, and health monitoring data
- Monitor traffic across sampling and queuing ports in individual partitions

The tools and their reporting interfaces are tested and qualified along with the OS, providing unparalleled ability to test and collect evidence for certification in your exact deployment environment.

Wind River Trusted Stack

Due to increasing connectivity, criticality, and threats in DoD programs, the NSA has acknowledged the need for a standards-based, RFC-compliant IPv4/IPv6 protocol networking stack evaluated to high EAL for proven assurance and robustness. To

address these requirements, Wind River can provide a trusted stack for Common Criteria certification at high EAL levels, including EAL7. Leveraging Wind River's extensive experience with network stack technology, this new stack uses existing APIs to enable rapid transition to a secure network environment.

Features of the Wind River Trusted Stack include the following:

- UDP, IPv4/IPv6, TCP
- Can be shared by multiple applications, or can have multiple instantiations
- Security policies that can be different for kernel vs. stack vs. applications, or for different stack instances
- Configurable security policies and "wiring diagram"
- DO-178B Level A evaluation
- Future high EAL evaluation
- Small memory footprint
- High performance
- Compliance with all current RFCs (standards)
- Hardware-independence

(Availability details on request)

PCSexpress from Objective Interface Systems

PCS*express* is high-performance, real-time communications software from Wind River partner Objective Interface Systems that provides securely separated communications channels between systems. With PCS*express*, developers can easily create high-performance, GIG-connected cross-domain solutions (CDS) that implement cryptography specified in the NSA's Suite B and are suitable for certification under Common Criteria EAL6+, DCID 6/3 PL 5, DO-178B Level A, and FIPS 140-2.

As a complement to a trusted stack, PCS*express* enables secure intersystem communications and strong node/application authentication over a wide variety of communi-cation protocols, including point-to-point (e.g., TCP, UDP, SCTP, RapidIO, Infiniband, VME, PCI) and point-to-multipoint (e.g., IP Multicast, FireWire, USB, Link16). For details, see www.ois.com/pcs.

A Strong Foundation for Aerospace & Defense

Two decades ago, the second customer to purchase Wind River's hard-real-time OS, VxWorks, was the U.S. Department of Defense. Since then, Wind River has been the leading technology choice for aerospace and defense companies around the world. Our VxWorks MILS solution continues that tradition.

Wind River's VxWorks MILS is based on our proven, reliable, high-performance VxWorks 653 RTOS. This OS delivers the stringent foundation aerospace and defense companies need to address the safety and security requirements of mission-critical applications, as well as the portability and reusability requirements of noncritical applications. Wind River device software solutions are flying around the world in military and commercial aircraft and around the solar system in numerous NASA-developed, space-borne vehicles. Specifically, Wind River's VxWorks 653 RTOS is used in the Boeing 787 Dreamliner, the Boeing C-130 AMP, the Boeing 767 tanker, and other aircraft.

The Wind River MILS Approach

Partnering for High-Performance Secure Systems

Building and certifying a real-time multilevel secure system suitable for high-EAL Common Criteria takes several years. But high-EAL certification by itself does not guarantee adequate functionality or performance. VxWorks MILS is the first high-performance, multilevel secure system based on the MILS architecture and a COTS OS.

At Wind River, we believe that cultivating a deep partnership with you—our customer—is crucial to building and certifying a high-EAL, high-performance, multilevel secure system. This partnership is a key component of our MILS solution.

We can help you succeed in the following ways:

- Define and refine overall system architecture to achieve adequate performance with the MILS promise of coresident multiple applications. Examples are application partitioning, driver location, and communication among OS/middleware/application and among applications.
- Modify or augment the separation kernel, board support packages (BSPs), or the middleware layer for specific performance and security needs based on your system.
- Select or develop required Protection Profiles (PP) and security requirements (see Appendix A for definition of terms).
- Collaborate as needed for PPs beyond the SKPP.
- Complete the Security Target, including required customer components.
- Define the explicit hardware/software Target of Evaluation.
- Create secure boot hardware and associated software.
- Create a secure delivery process.
- Create and evaluate BSPs.

Wind River works closely with you, the Common Criteria Testing Laboratory (CCTL), and the National Information Assurance Partnership (NIAP) to support final evaluation of the entire multilevel secure system. This includes the OS, BSPs, middleware, and applications, all as necessitated by the system's security requirements.

Making High-Performance MILS Systems a Reality

Proven open standards. Controlled security, safety, cost, and schedule risk. Wind River's VxWorks MILS is making it all possible. In fact, we think MILS is poised to transform the architecture of other systems as well. From critical public safety, energy generation, and energy distribution to asset extraction and distribution, communications, transportation, health care, financial, and other applications—these will all require high-assurance performance on more cost-effective platforms with a smaller footprint. Wind River will be ready to help build them.

VxWorks MILS is backed by a world-class partner ecosystem, comprehensive professional services, and exceptional customer support. Wind River Professional Services has earned a Capability Maturity Model Integration (CMMI) SW/SE Level 3 rating for all process areas—a testament to the high levels of quality and value in the areas of planning, engineering, and delivery of services.

To learn more about Wind River offerings and product availability, contact us today at 800-545-9463 or inquiries@windriver.com.

Appendix A: Common Criteria

Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, is an international standard that enables the following:

- IT users can specify security requirements for products.
- Vendors can make security claims for products.
- Accredited commercial laboratories can evaluate products to determine whether they meet claims.
- Certification authorities in each country can examine, approve, and certify the evaluation.

The Common Criteria was developed by the governments of Canada, France, Germany, the Netherlands, the United Kingdom, and the United States.

The National Information Assurance Partnership (NIAP), a U.S. government initiative of NSA and the National Institutes of Standards and Technology (NIST) administer the Common Criteria in the United States. NIAP maintains a website for the Common Criteria Evaluation and Validation Scheme at http://www.niap-ccevs.org/cc-scheme/.

Evaluation Under Common Criteria

Common Criteria uses an EAL to define each increasingly rigorous package of assurance requirements. Each numbered package, from EAL1 (lowest assurance) through EAL7 (highest assurance), represents a point on the Common Criteria predefined assurance scale. An EAL can be considered a level of confidence in the security functions of an IT product or system. Products evaluated to EAL1 through EAL4 are mutually accepted by each of the 24 participating countries under the Common Criteria Recognition Agreement (CCRA), while critical systems processing national security information evaluated at EAL5 or higher typically require certification by each member nation. In the United States it is the NIAP Evaluation and Validation Program. For cryptographic products, the NIST Federal Information Processing Standards (FIPS) validation program is used.

The successive evaluation levels define increasing rigor for five representations of the particular IT system to be evaluated: the security requirements model, functional specification, high-level design, detailed or low-level design, and implementation. Each representation at the different EAL level is either specified formally using a mathematical notation, semiformally using a structured natural language, or informally. Rules are provided that require "proof" of the equivalence of adjacent representations, with the required "proof" a function of the type of representation (formal, semiformal, informal). For example, at EAL7, both the security model and functional specification must be specified formally and their equivalent proved mathematically.

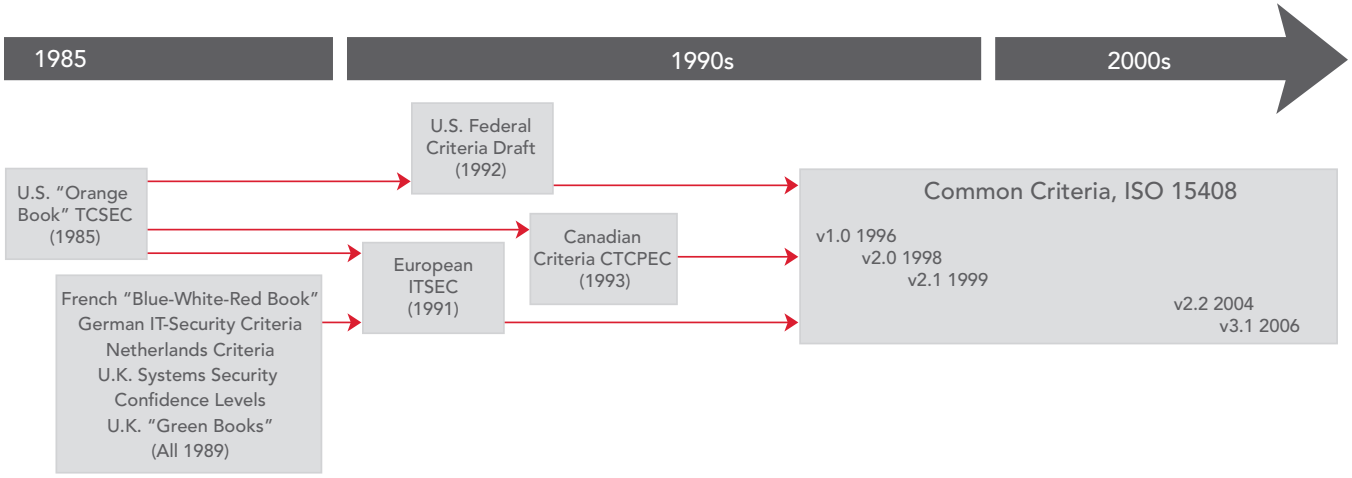


Figure 2: Common Criteria history

EAL	Definition	Requirements	Functional Specification	HLD	Covert Channel Analysis
EAL1	Functionally tested	Informal	Informal	Informal	No
EAL2	Structurally tested	Informal	Informal	Informal	No
EAL3	Methodically tested and checked	Informal	Informal	Informal	No
EAL4	Methodically designed, tested, and reviewed	Informal	Informal	Informal	Obvious vulnerabilities
EAL5	Semiformally designed and tested	Formal	Semiformal	Semiformal	Moderate attack potential
EAL6	Semiformally verified design and tested	Formal	Formal	Semiformal	Systematic
EAL7	Formally verified design and tested	Formal	Formal	Formal	Systematic

Figure 3: Common Criteria evaluation assurance levels

The requirements at the different levels are shown in Figure 3.

Common Criteria Testing Laboratories

In the United States under NIAP, NIST is responsible for accrediting evaluators. Nine evaluators currently are accredited. These are called Common Criteria Testing Laboratories (CCTL). The NSA staffs the "validation body" and is responsible for certifying all evaluations, as well as the in-depth covert channel penetration testing at EAL6 and EAL7.

Importance of Customer and Wind River OS Cooperation

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 both the OS and middleware as well as the customer's application. Wind River assists the customer and CCTL with this process, which may involve three key types of documents:

- **Protection Profile:** An implementation-independent set of security functional and assurance requirements for a category of IT products that meet specific consumer needs. The latest list of approximately 60 types of protection profiles is available at www.commoncriteriaportal.org. Because MILS is evolving, customers may need PPs that do not yet exist. Wind River can take responsibility for these.
- **Security Target:** A set of security functional and assurance requirements and specifications to be used as the basis for evaluation of an identified product or system (the security claims often made by reference to specific PPs).
- **Target of Evaluation:** The IT product or system described in a PP or, more typically at high EAL, a Security Target. The Target of Evaluation is the entity subject to security evaluation.

Common Criteria is the latest development of security policies for information systems. To learn more, visit www.commoncriteriaportal.org.