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

To meet these challenging demands, a comprehensive, security-based system architecture called Multiple Independent Levels of Security, or MILS, can be used. A MILS separation kernel partitions a single processor or core of a multi-core processor among multiple software components, assuring time and space resource allocation, information flow control, and fault isolation are all strictly enforced to implement security policies that address specific security requirements. The MILS architecture enables security architects to configure the system following the principle of least privilege, which requires that each system component be granted access only to the resources needed to complete its functions. Least privilege enables the development of devices and systems that are more resilient against attacks, and better at mitigating potential damage from defective or malicious software.

Wind River® works with suppliers in the development of secure systems by:

- Assuring protection of high value information, through a secure layered architecture, from attackers possessing a medium to high attack potential
- Addressing complex security and regulatory requirements
- Maximizing the reuse of legacy software in the secure system
- Defining a secure development process to aid in reducing the overall effort to design and certify a platform that meets complex security and regulatory requirements
- Evaluating single-core versus multi-core usage

**WIND RIVER VXWORKS MILS PLATFORM**

Wind River VxWorks® MILS Platform was created to bring federated applications of differing security levels or domains together onto a single hardware platform. VxWorks MILS Platform is a solution for software development of multilevel secure (MLS) and cross-domain solutions (CDS) devices with high security, high assurance, and high performance requirements. VxWorks MILS Platform uses a secure, Type 1 hypervisor-based separation kernel that provides guest operating systems in virtualized user-mode environments.

The VxWorks MILS Platform separation kernel meets the security functional and security assurance requirements for a separation kernel compliant to the “U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness” (SKPP), version 1.03.
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-ccews.org/announcements/SKPP%20Sunset%20Q&A.pdf, July 2011), making VxWorks MILS Platform an ideal platform for a broad range of security critical devices.

To support the full span of evaluation activities, VxWorks MILS Platform provides a complete set of artifacts to support a system-level evaluation process, based on the internationally recognized Common Criteria.

**WIND RIVER MILS PLATFORM SOLUTION ASSESSMENT**

One of the key challenges associated with the implementation of a complete MILS architecture is that MLS systems cannot be practically built on a single processor or core with currently available technologies. While existing MLS systems process information according to precisely defined security policies enforced with very high assurance, this has traditionally meant building systems with multiple, physically separated (i.e., “air gapped”) hardware elements—separate computers, separate displays, and separate networks—all requiring expensive equipment and operating procedures.

To address the limitations of currently available secure hardware technologies, Wind River Professional Services provides turnkey services to design teams to rapidly apply the high assurance qualities of Wind River VxWorks MILS Platform. Among these services is the Wind River VxWorks MILS Platform Solution Assessment. Its goal is to help your team define a low-risk, technical, and programmatic approach to achieving a secure architecture by developing a system solution that meets your overall system requirements, and preparing your program for successful certification and accreditation (C&A).

During the study, Wind River MILS information assurance experts will work collaboratively with your design and program teams to interpret system security requirements, architect an MILS system, and develop recommendations on processor and device configurations. The insights gathered during this study will leverage an understanding of issues relating to the use of VxWorks MILS Platform on the selected candidate architecture for the customer project.

![Figure 1: Wind River VxWorks MILS Platform run-time](image)
MAJOR ACTIVITIES

During the study, Wind River MILS information assurance experts will work with your organization and customer to complete the following tasks:

- Review functional requirements, security requirements, regulatory requirements, features, and specifications for candidate hardware and software architectures.
- Review evaluation requirements (Common Criteria, DO-178C, IASRD, etc.) and define an appropriate process for achieving evaluation.
- Evaluate system architectures and information flows, and provide a system recommendation with all supporting documentation, rationale, and analysis.
- Prepare MILS system-level block diagram(s) with information flows of the overall system required for supporting C&A activities.
- Conduct performance analysis and real-time operating system (RTOS) timing analysis, and identify potential risk areas.
- Define the guest operating system usage and allocation (VxWorks, Wind River Linux, High Assurance Environment).
- Document secure development environment requirements, reference configurations, and third-party components (graphics, networking, etc.).
- Develop a secure system architecture.
- Develop a secure device driver partitioning architecture.
- Develop a secure networking architecture with required protocols.
- Develop a secure graphics architecture.
- Identify secure file system requirements.
- Develop a secure information flow architecture.
- Develop a secure boot and startup architecture.
- Evaluate system reliability and failure modes and effects, and provide redundancy or backup recommendations with supporting documentation, rationale, and analysis, as required.
- Develop a risk matrix and perform a risk assessment. This risk assessment will also address the maturity of the product and approach (i.e., Technical Readiness Level), the degree of “pioneering” involved (new ground for this project approach), and the risks associated with the pioneering aspects to be undertaken.

DELIVERABLES

At the conclusion of the Wind River VxWorks MILS Platform Solution Assessment, Wind River delivers to you the products identified in Table 1, which become your intellectual property. These deliverables will be presented to your team, and your customer, if needed, to support you through the program architecture and planning process.
Wind River Professional Services is a CMMI Level 3–certified organization that provides security-critical device and system manufacturers with expert outsourced engineering services. Experienced information assurance 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 certification services tailored for security and mission-critical applications. Professional Services is fully equipped to protect International Traffic in Arms Regulations (ITAR) technical data and is able to meet the needs of government accounting.

In addition to the Wind River VxWorks MILS Platform Solution Assessment, VxWorks MILS Platform services include the following:

- Wind River VxWorks MILS Platform Design, Integration, Porting, and Migrations Services
- Wind River VxWorks MILS Platform Certification Services

Professional Services welcomes the opportunity to discuss VxWorks MILS Platform services to meet your specific needs. For further information, contact your local Wind River sales representative by visiting www.windriver.com/company/contact, calling 800-545-WIND (9463), or sending an email to inquiries@windriver.com.

**Table 1: Wind River VxWorks MILS Platform Solution Assessment Deliverables**

<table>
<thead>
<tr>
<th>Deliverables</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wind River VxWorks MILS Platform Solution Assessment document: Contains system architectures, information flow, and system recommendations, with supporting documentation, rationale, and analysis</td>
<td>Clearly articulates the preferred architecture, benefits, and supporting evidence so that program-level and business decisions may be made with confidence</td>
</tr>
<tr>
<td>Risk matrix: Contains an assessment of the maturity of the intended technologies and approach</td>
<td>Identifies major risks, and provides mitigation plans so that proactive activities may be undertaken to reduce program costs and schedule impact</td>
</tr>
<tr>
<td>Detailed design-phase planning document: Contains detailed design-phase task definition for security-related needs</td>
<td>Clearly defines the design-phase activities needed to produce an evaluatable program, including suggested prototyping efforts</td>
</tr>
<tr>
<td>Implementation-phase planning document: Contains implementation-phase task definition for security-related needs</td>
<td>Clearly defines the implementation activities needed to ensure that program security requirements are met</td>
</tr>
<tr>
<td>Technical consulting: Consists of Wind River experts collaborating onsite with your project engineers for effective knowledge transfer</td>
<td>Ensures that your team gets the most out of our recommendations and are able to transfer knowledge and skills in-house</td>
</tr>
</tbody>
</table>

**PARTNERING FOR YOUR SUCCESS**

Wind River guides customers through the complexities of the entire MILS system development lifecycle. Our unique combination of platforms and expertly delivered services enables our customers to architect, design, build, certify, and accredit MILS systems that meet the most demanding mission-critical system requirements:

- Reduced system SWaP
- Secure communication within an enclave and between systems
- Provisioning of simultaneous access by users with different security clearances or from different domains, while preventing unauthorized access to information
- Reduced time and cost for development, certification, and accreditation
- Reduced time and cost to reconfigure systems and to add applications
- Security evaluation, certification, and accreditation within a reasonable and predictable time and cost
- Meeting of guidelines governing the acquisition of information assurance products for U.S. Department of Defense programs

The Wind River VxWorks MILS Platform Solution Assessment service is the first step in realizing these system requirements.