WIND RIVER

Wind River VxWorks Cert Platform

Wind River VxWorks Cert Platform enables safety critical systems developers access to Wind River's commercial off-the-shelf (COTS) platform for delivering applications that must be certified to the stringent requirements of software safety standards. These include RTCA DO-178B, EUROCAE ED-12B ("Software Considerations in Airborne Systems and Equipment Certification") and IEC 61508 (functional safety of electrical/electronic/ programmable electronic safety-related systems [E/E/PES]). With VxWorks Cert Platform, developers can take full advantage of technological advances in microprocessors that the VxWorks COTS real-time operating system (RTOS) enables, with the assurance that they will have a strong operating system foundation to meet the most demanding safety certification standards.

Safety in the Avionics Market

The avionics market has a history of success using standard commercial microprocessors for a variety of flight-critical applications that can directly affect aircraft safety and reliability. To ensure that airborne systems contain a consistent high quality to meet the

demands of a variety of safety criticality levels, the global aerospace community developed the RTCA DO-178B and EUROCAE ED-12B airborne avionics standards to provide guidance on creating, certifying, and deploying these devices. These specifications are now uniformly enforced by a wide range of commercial aviation control organizations, including the U.S. Federal Aviation Administration (FAA), the European Aviation Safety Agency (EASA), Transport Canada, and others.

The aviation community reviewed input from every aerospace manufacturer in the world to create these standards that specify 66 objectives that describe recommended software life cycle and testing guidelines for the aviation industry. Wind River's DO-178B and ED-12B COTS Certification Evidence DVD contains a complete COTS certification package that meets these stringent objectives and therefore enables our customers faster time-to-market and gives equipment manufacturers a competitive advantage in the ability to leverage additional, ready-made technology from Wind River partners.

Safety in the Medical and Industrial Markets

IEC (International Electrotechnical Commission) 61508 is internationally recognized as the standard for software functional safety in industrial systems. Wind River's IEC 61508 Certification Evidence DVD includes a safety manual and safety certificate indicating that the

VxWorks Cert Platform Components and Hosts

Included Components
- Wind River Workbench 3.2
- VxWorks 6.6 RTOS
- VxWorks Cert 6.6
- GNU Compiler 4.1.2
- Wind River Compiler 5.6.0
- MPC 8349E reference BSP (PowerPC 603 architecture, PowerPC e300 core)
- Curtiss-Wright SVME/DMV-183 BSP with certification evidence (PowerPC 604 architecture, PowerPC e600 core)
- IDP945 reference BSP (Intel Core 2 Duo, 945 Chipset)
- Kontron CP6016 BSP (Intel Core 2 Duo, 5100 Chipset)
- Portwell Nano 8044 BSP (Atom)

Optional Components
- TCP/UDP/IPv4 network stack with multicast for VxWorks Cert
- Wind River Cert Highly Reliable File System for VxWorks Cert
- Workbench plug-in for on-chip debugging

Supported Hosts
- Windows XP Professional, Windows 7
- Solaris 10
- Red Hat Enterprise Linux, Workstation 4 and 5, Desktop 5
- Red Hat Fedora 13
- OpenSUSE Linux 11.2
- Novell SUSE Linux Enterprise Desktop 10 SP2 and 11
- Ubuntu Desktop 10.04

Table of Contents

VxWorks Cert 6.6 RTOS is certified to the stringent standards of IEC 61508 Software Integrity Level (SIL) 3. The medical, railway, nuclear systems, and automotive markets have all produced safety certification standards derived from IEC 61508. The certification of VxWorks Cert 6.6 ensures that our customers meet safety requirements of certification boards while leveraging Wind River's extensive partner solutions. Our customers reduce risk with our safety solution and have the competitive advantage of getting products to market faster.

Integrated Development Environment

VxWorks Cert Platform includes the award-winning Wind River Workbench development suite. Wind River Workbench is an Eclipse-based collection of tools designed to accelerate time-to-market for developers building devices with VxWorks 6 real-time operating systems. From hardware and board initialization to application development, Workbench offers deep capability across the development process in a single integrated environment, with complete platform integration, including powerful tools for debugging, code analysis, and test. Based on the Eclipse framework, Workbench can be extended through in-house, third-party, open source, and commercial plug-ins.

In addition to the Workbench Eclipse-based environment, VxWorks Cert Platform provides a full-featured command-line build system and debugging tools for developers who prefer this type of environment. These command-line tools can be easily integrated into a customized build system. The Workbench development environment helps reduce development costs and manage code complexity, eases tool integration, and enables standardization on a common development foundation across the enterprise.

Development Suite

Wind River Workbench	
Wind River Compiler	Workbench Debugger
GNU Compiler	Host Shell
Wind River Workbench On-Chip Debugging*	VxWorks Simulator

Software Partners

Java	OpenGL Graphics
Certification Services	Simulation Platforms
Design Tools	Ada

Operating System and Middleware

IEC 61508 SIL3 Certification Evidence*	DO-178B Level A Certification Evidence*
Safety-Certified Network Stack (TCP/UDP/IPv4)*	
Cert Highly Reliable File System*	
VxWorks Cert 6.6	

Hardware Partner

COTS Boards

Services

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

*Optional

Figure 1: Wind River VxWorks Cert Platform

Leveraging the Power of VxWorks 6

VxWorks Cert Platform includes a full commercial version of the VxWorks 6 RTOS as an integral part of the development package. This enables the use of a standard VxWorks 6 development environment, including the Wind River run-time analysis tools: Simulator, System Viewer, and Source Analyzer.

The certified VxWorks Cert 6.6 RTOS includes more than 480 kernel mode APIs and 150 user mode APIs selected from VxWorks 6, all of which are fully deterministic and deployable under guidelines outlined in the DO-178B and IEC 61508 safety standards. These include cache, clock, event flag, interrupt, memory management, message queue, ring buffer, semaphore, signal, and task management calls, along with a wide array of C and C++ library functions.

With VxWorks Cert 6.6, developers enjoy the following advantages:

- VxWorks 6 code does not need to be modified. All common system calls used in development environments can be immediately transitioned into a safety-certifiable environment.
- This system call commonality drives a minimal learning curve for developers already familiar with VxWorks 6 because the Workbench development environment and VxWorks 6 calls are the same in both uncertified and certified configurations.
- VxWorks Cert 6.6 is a COTS product, with the full leverage of COTS components: standardized usage, significantly lower costs, open toolchains, and shared certification evidence for rapid acceptance by safety certification boards.

VxWorks Cert 6.6 supports both C and C++ development. Many parts of the standard C libraries are in the kernel mode and user mode APIs, including parts of the error codes, math functions, string functions, utilities, and input/output functions. Developers can make use of object-oriented programming using the VxWorks Cert C++ language subset, which includes basic C++ constructs such as classes, inheritance, namespaces, polymorphism, and virtual functions.

User mode application support introduced in VxWorks Cert 6.6.2 brings VxWorks 6 real-time processes (RTP) to a safety-certifiable environment. The VxWorks Cert 6.6 RTP API subset allows applications to take advantage of memory protection, thus simplifying software integration between parallel development groups.

Contact your local Wind River sales representative for complete details on our VxWorks Cert 6.6 APIs and on the VxWorks Cert 6.6 C++ feature subset.

DO-178B Certification Evidence DVD

VxWorks Cert Platform is backed by the industry's most comprehensive set of certification artifacts, which support all RTCA DO-178B and EUROCAE ED-12B Level A requirements. Wind River's DO-178B and ED-12B COTS Certification Evidence DVD contains all of the required DO-178B Level A documentation, the software vulnerability analysis document, full source code, tests, code and test reviews, all test results, and full object-level code coverage listings. All files are fully hyperlinked to enable rapid traceability analysis of certification data, from the requirements, design, source and binary code, and test cases, using a simple browser. With this certification evidence DVD, the review of piles of printed and individual computer-based certification artifacts at locations distant from your engineering teams or certification authorities is no longer required.

This hyperlinked evidence contains more than 40,000 files including the following:

- Plan for Software Aspects of Certification (PSAC)
- Software Quality Assurance Plan
- 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)
- Version Description Document (VDD)
- Traceability Matrix
- Software Development Folder
  - Design reviews
  - VxWorks 6 source files
  - VxWorks 6 binary files
  - Code reviews
  - Test reviews
  - Functional tests
  - Coverage results (object level)
- Software Accomplishment Summary (SAS)
- Software Vulnerability Analysis (will be required by DO-178C)

This certification evidence can also be used, without modification, in related safety certification efforts, such as RTCA DO-278 ground-based systems certifications, for instance.

IEC 61508 Certification Evidence DVD

VxWorks Cert Platform supports all IEC 61508 SIL 3 requirements. The fully hyperlinked IEC 61508 Certification Evidence DVD enables rapid traceability analysis of certification data, from the requirements, design, source and binary code, and test case phases, using a simple browser. This DVD eliminates the need to review printed and individual computer-based certification artifacts. It includes the VxWorks Cert IEC 61508 Safety Manual and all required IEC 61508 SIL 3 documentation. The certification package also contains the TUV certificate for VxWorks Cert Platform.

This certification evidence can also be used in related IEC 61508 safety certification efforts, such as the CENELEC (European Committee for Electrotechnical Standardization) railway application standards, for example.

The certification package includes the following pieces of evidence:

- IEC 61508 safety certificate for VxWorks Cert 6.6
- Safety Manual for VxWorks Cert 6.6
- Safety Plan for VxWorks Cert 6.6
- Software Quality Assurance Plan (SQAP)
- Software Configuration Management Plan (SCMP)
- Software Development Plan (SDP)
- Software Requirements Standard (SRStd)
- Software Design Standard (SDStd)
- Software Coding Standard (SCStd)
- Software Verification Plan (SVP)
- Functional Safety Management Plan (FSMP)
- Software Test Plan (STP)
- Software Plans Addendum (SPA)
- Software Requirements Specification (SRS)
- Software Vulnerability Analysis (SVA)
- Software Design Document (SDD)
- Software Configuration Index (SCI)

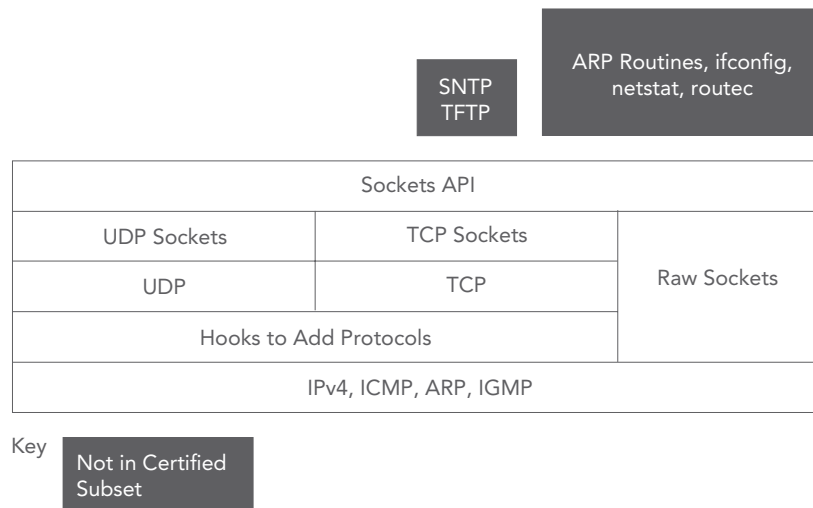| SNTP TFTP	ARP Routines, ifconfig, netstat, routec	
Sockets API		
UDP Sockets	TCP Sockets	Raw Sockets
UDP	TCP	
Hooks to Add Protocols		
IPv4, ICMP, ARP, IGMP		

Key — Not in Certified Subset
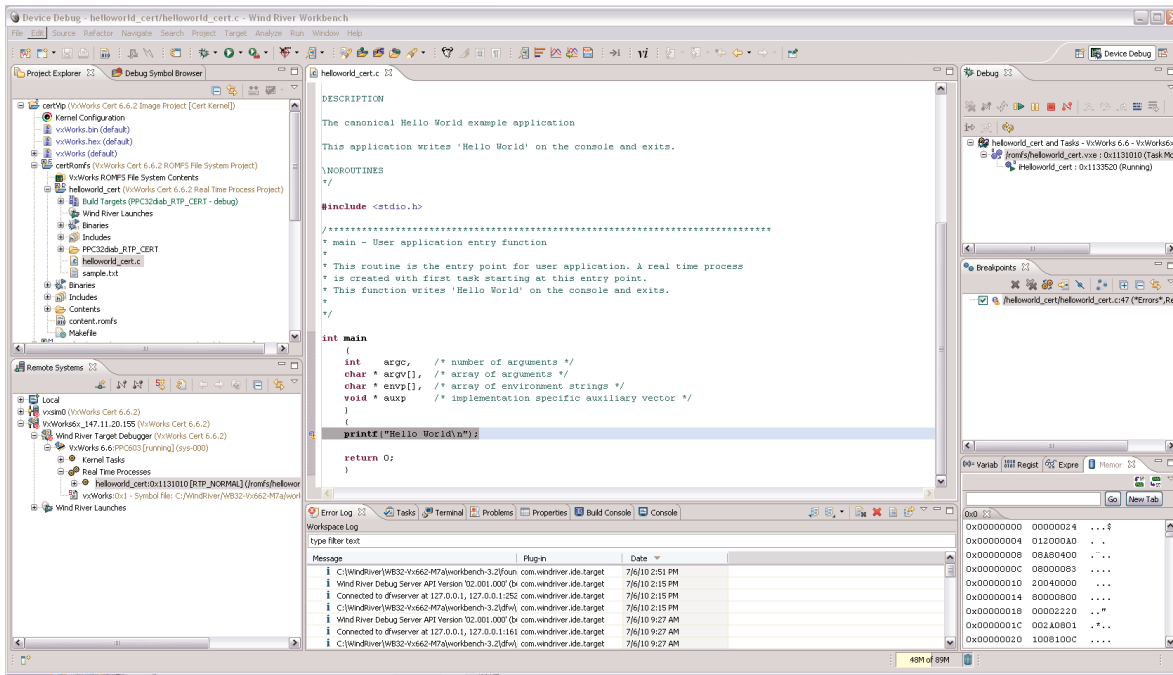
Figure 2: Certified network stack

Figure 3: Wind River Workbench

- Software Life Cycle Environment Configuration Index (SECI)
- Software Development Folder (SDF)
- Requirements Traceability Document (RTD)
- Qualification documents for tools used in certification process (structural coverage analysis, automated link verification tool, traceability tools)
  - Tool Operational Requirements Document (TOR)
  - Tool Qualification Document (TQD)
- Artifact Verification of Traceability
- Link Verification of Traceability

Wind River Cert Network Stack

Wind River Cert Network Stack for VxWorks Cert is an embedded TCP/UDP/IPv4 network stack that can be used in conjunction with VxWorks Cert Platform. This network stack has complete certification evidence, available for DO-178B at the highest level, Level A, and for IEC 61508 SIL3. This network stack uses the same APIs as Wind River's networking stack and supports the BSD sockets API (datagram, stream, and raw sockets), enabling the easy migration of networking software from VxWorks and Linux platforms.

Wind River Cert Highly Reliable File System

Wind River Cert Highly Reliable File

System for VxWorks Cert is a certification subset of the embedded fail-safe file system running in kernel mode. This transactional file system provides a default automatic commit policy option and a high-speed commit policy option for improved performance. Cert Highly Reliable File System is capable of supporting large file sizes over 16GB and hierarchical directory structures, enabling accurate persistent storage for safety-critical data in certified environments.

Wind River Workbench 3.2

Provided as part of the VxWorks Cert Platform, Wind River Workbench supports application development based on the full-featured VxWorks 6 kernel. This allows for optimization and testing, using the full power of Workbench's industry-leading tools and techniques. It provides developers with a very rich programming and debugging environment. Using the full-featured VxWorks 6 kernel for application development allows the use of all of the standard Workbench tools for VxWorks 6 development, including the VxWorks Simulator and the Workbench analysis tools such as System Viewer, Code Coverage Analyzer, Data Monitor, Memory Analyzer, and Performance Profiler. As the project moves into

certification test and deployment, a subset of the standard VxWorks 6 tools are available that allow developers to debug applications built with the certification kernel and perform final testing and integration on the deliverable system hardware.

For VxWorks Cert 6.6 projects that use the certified kernel, Workbench includes the following features.

Eclipse

Because of its openness, capability, and strong community support, Eclipse was chosen as the framework for the Wind River Workbench development suite. The Eclipse 3.5 framework supplies the necessary infrastructure to graphically and functionally integrate the components of Workbench. Open, extensible, and backed by a strong community of commercial and open source developers, the Eclipse framework provides a wide range of additional integrated functionality.

Project System

The Workbench project system allows developers to organize and manage the primary components in a device software development project, including source files and target systems. VxWorks 6 projects of different

types can be created for configuring and building kernel images and board support packages (BSPs) as well as both kernel module and RTP application projects that use VxWorks 6 and either C or C++. By design, Workbench enables users to manage multiple projects simultaneously.

Workbench allows easy transition between non-certified and certified application projects by providing build specifications for either environment. This allows the user to simply rebuild the same project with either the standard or certified version of the VxWorks 6 kernel.

Build System

The Workbench build system specifies the tools, options, and parameters to use when building VxWorks 6 software projects, enabling developers to set build parameters easily from the project level down to the individual file level. The build system allows for setting build properties at the global level or providing fine-grained control at the level of an individual file, and everything in between.

Command-Line Project Build System

In addition to the Workbench build system, a full-featured command-line build system is provided for developers who prefer this type of environment. Using GNU make, Tcl libraries, and VxWorks-specific tools, developers can configure VxWorks 6 source and build VxWorks 6 images as well as develop applications and libraries using command-line build facilities. These command-line tools can be easily integrated into a customized build system.

Wind River Compiler and Wind River GNU Compiler

Wind River Compiler is the default C compiler for building the VxWorks Cert 6.6 kernel, RTPs, libraries, BSPs, and applications in Wind River Workbench. This compiler's optimization capabilities are based on and extend the industry-hardened Diab compiler technology, and it produces robust, tight, fast-executing code.

Wind River GNU Compiler is based on the Free Software Foundation (FSF) distribution of the GNU compiler. Wind River has optimized a standard version of this compiler specifically for use with VxWorks 6.

Both compilers are included and supported as part of Wind River Workbench for VxWorks Cert 6.6 for application development.

Workbench Debugger

Workbench debugger addresses the needs of developers involved with hardware bring-up, firmware/driver/BSP development, and application development. It provides more capability than the GNU debugger (GDB) or other basic source-level debuggers. These capabilities can be extended further with Wind River's on-chip debugging solutions. In combination, these tools provide the necessary functionality for hardware bring-up, device driver/BSP debugging, kernel debugging, and application software debugging.

Workbench debugger provides extensive browsing and inspection capabilities on objects in the target platform. This awareness of VxWorks Cert 6.6 objects allows for an enhanced debugging experience that allows greater insight and productivity when debugging.

VxWorks Simulator 6

VxWorks Simulator 6 is a complete prototyping and simulation tool for VxWorks 6 applications. VxWorks Cert 6.6 static kernel modules (SKM) can run on the VxWorks Simulator using the standard VxWorks kernel. It enables you to develop and test significant portions of your cert kernel modules earlier in the development cycle, before hardware is available. It can also lower your development cost by allowing developers to share fewer hardware targets, enabling host-based development.

Host Shell

The Host Shell provides a command-line debugging interface that allows you to invoke both VxWorks Cert 6.6 and application module subroutines. The Host Shell executes on the development host, not the target; but it enables you to spawn tasks, read from or write to target devices, and exert full control over the target. Because the Host Shell executes on the host system, you can use it with minimal intrusion on target resources.

Wind River Workbench On-Chip Debugging

The Workbench development environment provided with VxWorks Cert Platform can be enabled for on-chip debugging. When using VxWorks Cert 6.6, the target debug agent must be removed before final certification. In this situation, Wind River Workbench On-Chip Debugging is the optimal debugging solution. Wind River's on-chip debugging capability, along with Wind River ICE, Wind River Trace, or Wind River Probe hardware, provides system-level debugging capability when debugging with a target debug agent is not possible. On-chip debugging provides developers with complete system-level control of their environments at all times, enabling more efficient and effective hardware bring-up, firmware development, and device driver and BSP generation.

Partner Ecosystem

Wind River's world-class partner ecosystem ensures tight integration between our core technologies and those of the premier hardware and software companies we've chosen to complement our solutions. Our partners help extend the capabilities of Wind River's development and run-time platforms by offering out-of-the-box integration and support for key technologies. Our customer support team is trained to troubleshoot partner technologies in use with Wind River products, making ours the most comprehensive and best-supported partner ecosystem in the embedded software industry.

Professional Services

Wind River Professional Services enables companies to reduce risk and improve competitiveness. Our team delivers device software expertise within structured engagements that

directly address key development challenges and contribute to the success of our clients. Wind River's successful device software engagements stretch across a spectrum of technologies, from set-top boxes to spacecraft, cell phones, and industrial robots. Our proven engagement methodology, a track record of timely delivery, and in-depth understanding of market and technology dynamics make Wind River a valuable implementation partner to clients worldwide.

Wind River solutions are augmented by market-focused services practices that build on the collective expertise of our engineers to provide timely and cost-effective design, integration, migration, and optimization services. Our services practices are built on four key pillars:

- **Tailored services:** Our services are tailored to the unique requirements of the vertical markets in which we focus.
- **Specialized expertise:** We deliver our services using specialized skills, knowledge, and experience that help us meet the specific needs of a vertical market or technology. This includes in-depth knowledge not only of Wind River products and technology but the technology of our partners in a given vertical industry, open source technologies, the nuances of the industry, and how all these requirements combine to drive the needs of the customer.
- **Portfolio of intellectual property:** We offer a portfolio of solutions, some developed in conjunction with our customers, that can help reduce the cost and time frame of solution delivery.
- **Project management:** We employ a global project management approach based on best practices and refined by more than 20 years of advanced systems development experience.

Installation and Orientation Service

Wind River offers an Installation and Orientation Service to ensure your project starts on time and without hassle by delivering the following:

- **Onsite installation:** Guided install on your hardware and host platform, along with a sample build process, demonstrations, and examples of customizations
- **Hands-on orientation:** Architecture, development file system, adding open source packages, porting drivers, addressing design issues
- **Advice:** Introduction to Wind River support channels and processes, additional services, project review, and consultation

The Wind River Installation and Orientation Service will expedite your path to productivity, allow you to rest assured that we have eliminated a common source of user error, and help you realize all of the platform's potential.

Education Services

New products and new development approaches can create extraordinary value, if individuals and teams learn to use them effectively. Lack of product knowledge can cause longer development schedules, poor quality, and higher costs. To help your team achieve optimal results from your technology investment, Wind River offers flexible education and coaching services to fit your schedule and project requirements.

Public Classes

Public classes provide detailed information on product, technology, and design-related topics. Hands-on exercises allow students to experiment with the products. Attending a public class may be the most cost-effective option for individuals or a small development team.

Private Classes

Private training classes include participants exclusively from your company. If you have a large project team or a number of new users, private classes may provide you the best value:

- You can tailor the agenda. Our instructors consult with you to determine which topics should be included and emphasized. Your participants do not waste precious class time on topics that are unimportant to them.
- Class discussions can cover your specific project needs, technical requirements, and challenges.
- You provide a location convenient for your employees, or choose Live Remote delivery; either way, your employees save travel expenses and time away from the office

Wind River Mentoring

Wind River provides expert assistance, best practices, and coaching to help you integrate Wind River solutions into your environment. Wind River Mentoring combined with formal training classes speed you through the steepest part of the learning curve. Your team can avoid lengthy trial-and-error cycles and quickly become productive with your Wind River solutions.

The following are examples of Wind River Mentoring services:

- **Product installation:** A Wind River expert will install the products you've purchased and handle special requirements, such as multisite installation, installation on shared workstations, license server deployment, and plug-ins.
- **Tools integration:** A subject-matter expert will provide guidance on your specific data, system, and process integration, to optimize workflow and productivity. Depending on the complexity of your environment, the consultant can also help integrate licensing, edit-compile-debug workflow, advanced debugging visualization tools, kernel and application build configurations, and code repository systems.
- **Technology adoption:** A subject-matter expert will analyze and assist in formulating a technology adoption plan that includes such items as the design framework, application integration, and deployment—while taking into consideration best practices and maintenance issues. We can provide workflow reference material for new developers or infrequent users.
- **Technology assistance:** Wind River experts will provide guidance on various technology-related topics such as configuration, device drivers, debugging techniques, and performance optimization specific to your unique needs.

Mentoring is also available remotely. You can arrange for a regular schedule of check-ins with an engineering specialist, ensuring that you remove productivity obstacles early and catch problems before they impact other parts of a project.

Live Remote Delivery

Live Remote delivery is a flexible alternative to classroom training or in-person mentoring.

Live Remote classes provide a remote-access, instructor-led environment that allows you to participate in live training events from the convenience of your home or office, or anywhere you have an Internet connection. You can watch live demonstrations, listen to lectures, practice hands-on lab exercises, ask questions, and receive feedback just as you would in a conventional class.

Most Wind River training courses and Wind River Mentoring are available for Live Remote delivery:

- Save the trouble, expense, and time of traveling to a training site.
- Receive efficient, multisite training; your team members who are spread across geographic regions can collaborate within the same training or mentoring session.

Support Services

Wind River Customer Support, a Service Capability and Performance (SCP)–certified organization, provides support for Wind River VxWorks Cert Platform. Your subscription to VxWorks Cert Platform includes full maintenance and support, delivered through Wind River's global customer support organization and our Online Support (OLS) website. Customers with a current subscription receive both maintenance updates and major upgrades.

Visit our Online Support website at http://www.windriver.com/support for fast access to product manuals, downloadable software, and other problem-solving resources. OLS offers a comprehensive knowledge base with a robust search feature for locating product information and manuals by keyword, author, published date, document type, language, and solution category.

Additional support features, including proactive email alerts covering particular technologies, platforms, or product patches and technical tips for common problems, are available for all customers on subscription.

Support on modified or unsupported configurations is best-effort-based. Wind River Customer Support will try to reproduce the problem on a supported configuration. If the problem can be validated, Wind River will provide a fix that will be tested on a supported configuration. Wind River Professional Services can provide support for boards or host operating system versions that are not supported by the standard product as well as for customized versions of the source code or additional nonstandard packages.

If you cannot find the information you need through Online Support, contact our global support team for access to the industry's most knowledgeable and experienced support staff. For contact details, visit http://www.windriver.com/support/contact.html. For more details on our support processes, including escalations and defect resolution, consult Wind River's Customer Support User's Guide (CSUG), available at www.windriver.com/support/resources/csug.pdf

North America, South America, Asia/Pacific

support@windriver.com
Toll-free tel.: 800-872-4977
(800-USA-4WRS)
Tel.: 510-748-4100
Fax: 510-749-2164
Hours: 6:00 a.m.–5:00 p.m. (Pacific time)

Japan

support-jp@windriver.com
Tel.: +81 3 5778 6001
Fax: +81 3 5778 6003
Hours: 9:00 a.m.–5:30 p.m. (local time)

Europe, Middle East, Africa

support-ec@windriver.com
Toll-free tel.: +800 4977 4977
France tel.: +33 1 64 86 66 10
France fax: +33 1 64 86 66 66
Germany tel.: +49 899 624 45 444
Germany fax: +49 899 624 45 999
Italy tel.: +39 011 2448 411
Italy fax: +39 011 2448 499
Middle East Region tel.: +972 9741 9561
Middle East Region fax: +972 9746 0867
Nordic tel.: +46 8 594 611 20
Nordic fax: +46 8 594 611 49
UK tel.: +44 1793 831 393
UK fax: +44 1793 831 808
Hours: 9:00 a.m.–6:00 p.m. (local time)

WIND RIVER

Wind River is a leader in embedded and mobile software. We enable companies to develop, run, and manage device software faster, better, at lower cost, and more reliably. www.windriver.com