WIND RIVER RTCA DO-178 SOFTWARE CERTIFICATION SERVICES

Wind River® Professional Services RTCA DO-178 Practice provides software certification services to help our customers address their demanding software systems certification needs. Wind River provides assistance in the following areas:

- RTCA DO-178 gap analysis, examining existing processes to identify gaps in meeting DO-178 certification requirements
- Development of VxWorks® 653 or VxWorks Cert DO-178-compliant board support packages (BSPs)
- Full DO-178 verification and validation services for a BSP or an existing software base

RTCA DO-178 GAP ANALYSIS

Wind River can perform a complete DO-178B or DO-178C gap analysis of current software development processes, requirements, design data, source code, test methodology, and tools. This gap analysis will also provide an estimate of the time, effort, and special expertise required to take the necessary steps to meet DO-178 certification.

Wind River will send technical experts to your site to collect data for the gap analysis. The gap analysis begins with an interview of the key engineers to get a complete understanding of the current development process, the tools used in development, and the software verification process.

The next step is to perform a planning process audit by reviewing software planning documentation, including the following:

- Overview of current standards of development and testing
- Review and analysis of the software quality assurance plan and software quality organization
- Review and analysis of the software configuration management plan and software configuration management environment
- Review of standards (coding standards, requirements standards, etc.)
- Review of software verification plans and test plans and procedures

After the planning process audit, we will perform a development process audit, including the following:

- Overview of current design data, build process, tools for requirements, and static and dynamic analysis tools
- Review of system requirements, interface control documents (ICDs) (if applicable), and high-level requirements to determine how the latter are documented, reviewed, and traceable to system requirements
- Review of the software architecture to determine how it is defined, reviewed, and analyzed
- Review of low-level requirements to determine how they are documented, reviewed, and traceable to high-level requirements
- Review of source code to determine how it implements low-level requirements, is traceable to the low-level requirements, and has been internally reviewed
- Review of the problem report process and how problems are corrected
- Review of how source code and software documentation is stored, archived, and revised

Next we will perform a verification process audit, including the following:

- Overview of current tools and processes used for verification of requirements, design data, source code, and test plans, procedures, and results
- Review of the configuration control process to assess methodology for the evolution and revision of software, as well as how software changes impact revision to software documentation and retesting
- Evaluation of how test cases and procedures are documented, reviewed, and placed under configuration control
- Determination of the extent to which test cases and procedures have been executed and passed, including an examination of what tools are used in the testing process (test harnesses, coverage tools, etc.)
- Determination of the viability of the compiler and linker to support DO-178 requirements
- Determination of the extent to which test results are documented and complete
- Review of how the software testing environment is documented and controlled
- Traceability analysis from requirements to design to source code implementation to test cases and results; determination, if possible, of the extent of code coverage achieved through requirements-based testing

The next step is an application hardware and software analysis, including the following:

- Overview of software functionality, gathering metrics on the number of requirements, functions, source lines of code (SLOC) counts, language constructs, and architecture
- Identification of any special run-time libraries used in the application (standard C and math libraries) and assessment of the extent to which these libraries have been documented and verified
- Interviews of individuals who build, test, and verify the application regarding low-level testing, integration, and system verification processes
- Evaluation of system-testing and regression-testing methodology

WIND

The Wind River experts will compile all the gathered data into a DO-178 Gap Analysis Report. The report includes a summary matrix that provides an overall assessment of the current state of your software development processes with regard to the level of DO-178 compliance you are seeking.

Direct Consulting to Implement a DO-178-Compliant Process

Using the information gathered in the gap analysis, Wind River experts can assist you with implementing a fully DO-178-compliant software planning, development, and verification process. This process can then be used to develop, produce, and certify software autonomously, without outside assistance.

DEVELOPMENT OF VXWORKS 653 OR VXWORKS CERT DO-178-COMPLIANT BOARD SUPPORT PACKAGES

Wind River Professional Services has deep experience developing DO-178-compliant BSPs on VxWorks 653 and VxWorks Cert for custom hardware platforms. Following our DO-178B/C compliant processes, Wind River can perform the following services:

- Develop and document requirements and design for a custom hardware BSP
- Create a VxWorks 653 or VxWorks Cert BSP
- Write an acceptance test plan to validate the BSP
- Create an acceptance test case for each requirement
- Integrate a BSP with system software components (onsite or offsite)
- Perform testing (onsite or offsite)

FULL DO-178 VERIFICATION AND VALIDATION SERVICES

Wind River Professional Services can provide you with resources and tools to completely reverse engineer your software design and artifacts using the Wind River DO-178B/C compliant processes, defined below:

- **Project management:** Organization of resources and schedules
- **Planning:** Definition of certification strategy and planning documents, including the Plan for Software Aspects of Certification (PSAC), Software Development Plan (SDP), Software Verification Plan (SVP), and appropriate standards
- **Configuration management:** Control and management of the software and software life cycle data, including problem reports and software updates
- **Quality assurance:** Assurance of independence and enforcement of software life cycle processes and activities
- **Requirements:** Definition and review of high-level and low-level software requirements
- **Design:** Definition and review of software design
- **Coding:** Definition and review of software source and object code
- **Integration:** Cohesion of software modules into one or more functional components
- **Verification:** Review of requirements, design, and source and object code, as well as test plans, procedures, results, and coverage analysis

- **Documentation:** Production of all required DO-178B or DO-178C documentation to support Level A or lower certification
- **Certification liaison:** Relationship with the certification authority and, if required, approval of the PSAC, Software Accomplishment Summary (SAS), and Software Configuration Index (SCI)

If your software is previously developed software, Wind River will undertake a reverse engineering process to reconstruct all the required DO-178 documentation and activities. Wind River will follow the guidance of Position Paper CAST-18, "Reverse Engineering in Certification Projects", to ensure this effort is done with as little certification risk as possible. Figure 1 shows this process.
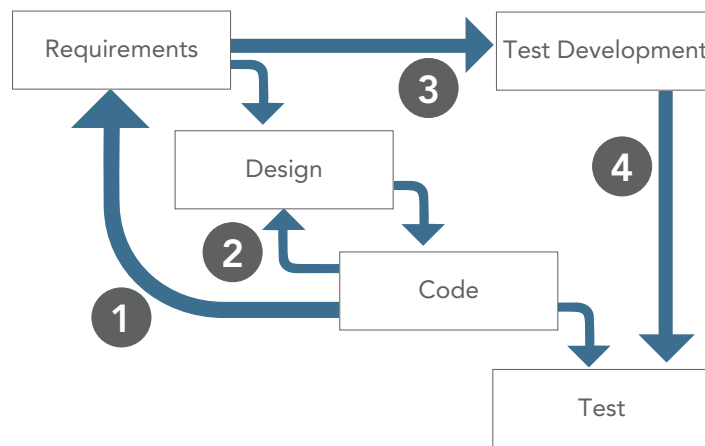

Figure 1: Wind River reverse engineering process

In Step 1, we examine the entire code structure and reverse engineer high-level and low-level requirements. In Step 2, we reverse engineer design data (in the form of pseudo-code or similar documentation). The requirements and design data will then be traced together and linked with the source code itself.

In Step 3, we produce the test cases from the requirements (not from the design or source code). These requirements-based tests are executed in Step 4, and the coverage of the source and object code is then analyzed against the desired level of DO-178 requirements. This process is repeated until complete source and object coverage is achieved.

Wind River will produce the following documentation that can be submitted for certification anywhere in the world:

Documentation Produced by Wind River

PRODUCT NAME	PRODUCT DESCRIPTION
Plan for Software Aspects of Certification	Provides the certification authorities an overview of the means of compliance and insight into the planning aspects for delivery of the product
Software Quality Assurance Plan	Defines the software quality assurance process and activities
Software Configuration Management Plan	Defines the configuration management (CM) system and change control process
Software Development Plan Software Requirements Standard Software Design Standard Software Coding Standard	Define the processes used for requirements analysis, development, and test for the software product; include the standards for requirements, design, and code
Software Verification Plan	Defines the test philosophy, test methods, and approach to be used to verify the software product
Software Test Plan	Documents the project-specific approach to verifying the software product
Software Requirements Specification	Defines the high-level requirements applicable to the software
Tool Requirements Document	Defines the required functional behavior of a verification tool under normal operating conditions
Software Design Document	Describes the design of the software
Software Configuration Index	Identifies the components of the certifiable software, with version information necessary to support regeneration of the product
Software Life Cycle Environment Configuration Index	Identifies the tools used to build and test the software
Tool Qualification Document	Documents the qualification evidence for a verification tool against the requirements established in the PSAC and Tool Requirements Document

WIND

PRODUCT NAME	PRODUCT DESCRIPTION
Software Development Folder	Includes as a minimum: • Reference to the applicable requirements • Reference to the implementation (design and code) • Evidence of reviews for the requirements, design, code, and test procedures and test results • Software test procedures • Software test results • Analysis documents for verification, coverage analysis, and any special case analysis • Change history (CM system) • Applicable problem reports
Traceability Matrix	Provides traceability from the requirements to the built software to test for the delivered software product
Software Accomplishment Summary	Documents the actual versus planned (in the PSAC) activities and results for the project; provides a summary of the means of compliance used for the software; and justifies any deviations from the plans
Sources	Provides the source files for the following: • Software • Test procedures • Build and test scripts
Results	Documents the results of the functional and structural coverage testing, including the actual results and any applicable analyses performed (including coverage analysis)
Libraries	Linkable versions of the "as tested" libraries

WIND

DO-178B SAFETY CERTIFICATION EXAMPLE PROJECTS

The following table lists a few of the DO-178B certification projects to which Wind River has contributed.

Examples of Past Projects

CUSTOMER	PROGRAM	PRODUCT	LEVEL	AGENCY
Boeing/GE	787 Common Core System	VxWorks 653	A	FAA
Boeing/GE	KC-767 AFMC	VxWorks 653	B-D	FAA
Boeing/GE	KC-767 Hose Deploy	VxWorks Cert	B	FAA
Boeing/GE	KC-767 MCDU	VxWorks Cert	B	FAA
BARCO	CDMS-3000 (MOSArt)	VxWorks 653	A	EASA
BARCO	Ilyushin 96	VxWorks 653	C	NIIAO
Cobham FR	A330 905E Wing Pod	VxWorks Cert	A	INTA
EADS Eurocopter	EC 225LP	VxWorks Cert	A	EASA
EADS CASA	A330 MRTT ARBS	VxWorks 653	A	INTA
EADS CASA	A330 MRTT MIC	VxWorks Cert	B	INTA
LogicaCMG	EGNOS	VxWorks Cert	B	ESA
Raytheon	WAAS	VxWorks Cert	B	FAA

WIND RIVER PROFESSIONAL SERVICES

Wind River Professional Services has a strong track record of guiding our customers through the complexities of new technology adoption. Certified to CMMI Level 3 across all of our global development centers, our proven engagement methodology, timely delivery, and in-depth understanding of market and technology dynamics have made Professional Services a valuable implementation partner to our customers. Our RTCA DO-178 Practice provides consultation services that help our customers with the specific needs of adopting new technologies when safety and regulation compliance is critical.

Contact us today for more information on how Wind River Professional Services can assist your company with RTCA DO-178 certification. To find your local Wind River sales contact, visit www.windriver.com/company/contact/index.html, call 800-545-WIND (9463), or email inquiries@windriver.com.