Software Safety Qualification Services
A Service of the Wind River Industrial Services Practice

For more than 20 years, Wind River has been helping customers achieve the most demanding certifications. The Wind River Industrial Services Practice provides Software Safety Qualification Services to help our customers address their most demanding software systems certification needs.

Certification with Pre-existing Software

Companies responsible for creating mission-critical industrial systems are becoming increasingly subject to regulatory standards such as IEC 61508, IEC 62304, IEC 60880, FDA, and EN50128.

One of the greatest challenges for system developers in meeting these standards is the incorporation of pre-existing software assets not specifically developed for the current project.

Sources of pre-existing software might be a commercially available product, open source project code, or code developed from a previous in-house development effort. Generally these are operating systems, drivers, board support packages (BSPs), libraries, middleware, and applications. Typically pre-existing software was not developed in accordance with the requirements of a specific safety standard.

Regulatory standards specify a set of requirements that need to be met when pre-existing software is used to implement all or even part of a safety function. Effective incorporation of pre-existing software can have a dramatic impact on the project’s time-to-market, development costs, and overall system performance. Effective utilization of pre-existing software also allows the system manufacturer to concentrate its development efforts on creation of applications needed to run high-value, differentiating, device-specific functions.

To address these requirements design teams are faced with some key challenges:

- How to integrate pre-existing software in a safety-related system while preserving system safety
- How to integrate pre-existing software in a safety-related system while preserving functionality and usability of the software
- How existing verification and validation documents can be integrated into the new system’s documentation set
- Effort and costs that will be incurred by qualifying pre-existing software
- Estimated schedule for qualifying pre-existing software
- Acceptance of the qualification approach by the certification authority
- Maintenance of pre-existing software over the whole life cycle of the safety-related device
- Removal of non-required functions
- Impacts of changing the operating system in a certified system

Software Safety Qualification and Certification Terminology

- Safety: Freedom from unacceptable risk
- Equipment under control: Equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other activities
- Safety function: Function to be implemented by a safety-related system that is intended to achieve or maintain a safe state for the equipment under control
- Safety Integrity Level (SIL): Discrete level (one out of possible four) that specifies the probability of a safety function to fail on demand/per hour
- Verification: Confirmation by testing and provision of objective evidence that the pre-existing software satisfies the software requirements specifications
- Validation: Confirmation by testing and provision of objective evidence that the pre-existing software satisfies the software requirements specifications for a specific intended use
- Qualification: Objective evidence at least equivalent to the development processes eliminated or reduced that pre-existing software can be used in a safety-related system
- Safety-related system: Designated system that implements the required function necessary to achieve or maintain a safe state for the equipment under control
- Certification artifacts: Document set that builds a structured argument that provides a compelling, comprehensible, and valid case that a system is safe for a given application in a given operating environment
In addition to certified operating systems, platforms, middleware, libraries, and development tools, Wind River has a long history of providing consulting services for our customers to help achieve the most demanding certification requirements. The Wind River Industrial Services Practice provides Software Safety Qualification Services to help our customers address their software systems certification needs. Software Safety Qualification Services are intended to help customers plan and execute the integration of pre-existing software into a system development effort that needs to meet defined regulatory standards. Wind River applies a well-proven collaborative approach to helping your team qualify pre-existing software for usage in safety-related systems.

The approach addresses the three tenants of qualification:
1. Operational experience
2. Validation
3. Process compliance

Wind River helps our customers achieve the three tenants by delivering work packages in five required areas. Customers may need help in one or all five of the following requirements:

1. Specification of functionality of pre-existing software:
   - Specify a subset of the functionality.
   - Remove functions that are not required.
   - Specify the configuration.

   The value in effectively performing these tasks is that restricted and specified functionality significantly reduces qualification effort and simplifies safety justification.

2. Documentary evidence of operational experience:
   - Describe the maintenance process.
   - Provide analysis of operational experience.
   - Develop the maintenance process description documentation.

   A well-specified maintenance process can provide adequate documentary evidence that pre-existing software did not cause any hazards and thus contribute to a proven-in-use claim that supports the qualification.

3. Process description:
   - Describe the development process.
   - Develop the required process description.

   The value in describing and developing a process description is to have a straightforward comparison between the actual process and the process requirements in related safety standards. This enables a precise determination of the level of compliance.

4. Validation testing:
   - Document the software requirements specification for the pre-existing software in its new safety-related application.
   - Test against software requirements within the customer target environment.
   - Document the test approach and test results.
   - Perform analysis of test results.
   - Develop the software requirements specification.
   - Develop the software test plan.
   - Support software test execution.
   - Develop the software test report.

   The value of doing validation testing correctly is that 100% of the required functionality works as intended on the target architecture, providing a high level of confidence in the quality of pre-existing software.

5. Safety manual:
   - Describe usage of the pre-existing software.
   - Specify workarounds and countermeasures respectively for bugs/issues identified by analysis of test results and operational experience.
- Document SIL of the pre-existing software that was qualified.
- Document outstanding anomalies.
- Document requirements not met.
- Describe installation procedures.
- Document configuration to which the pre-existing software was qualified.
- Develop the safety manual.

The safety manual ensures integration of pre-existing software in a safety-related system while preserving system safety.

Wind River's staff of software safety experts along with our long working relationships with regulatory and standards bodies ensures that we take the most direct approach in helping your staff prepare for safety qualification.

**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, track record of timely delivery, and in-depth understanding of market and technology dynamics have made Wind River Professional Services a valuable implementation partner to our customers. The Wind River Industrial Services Practice provides consultation services that help our customers with the specific needs of adopting new technologies when safety and regulation compliance is critical.