HighIntegritySystems

WITTENSTEIN

What is the SAFE**RTOS**® Design Assurance Pack?

WITTENSTEIN high integrity systems (WHIS) is a specialist safety systems company and the developer of SAFE**RTOS**®, a pre-emptive Real Time Operating System (RTOS) based on the FreeRTOS functional model but specifically redesigned for safety-critical applications.

Independently certified by TÜV SÜD to IEC 61508 SIL 3 and ISO 26262 ASIL D, SAFE**RTOS**® is supplied with a processor and compiler-specific Design Assurance Pack (DAP) or Design History File (DHF).

The DAP/DHF provides the documentation, evidence, and traceability required to support functional safety certification activities, helping organisations to:

- Reduce certification effort
- Improve audit readiness
- Reduce project risk

What's included in the DAP?

A typical DAP contains approximately 70 artefacts organised into the following categories:

Getting Started

Provides installation guidance, API reference information, integration requirements and practical examples.

- SAFE**RTOS**® User Manual
- SAFE**RTOS**® Safety Manual
- FreeRTOS to SAFE**RTOS**® migration guidance
- Demonstration applications and example projects

Configuration and Release Management

Contains an inventory of the materials released, their relating checksums and a record of the changes made to this deliverable over its lifetime.

- Software version description

Planning

Defines the development approach, verification strategy, configuration controls and safety activities used throughout the project.

- Software development plan
- Software configuration management plan
- Software test plan
- Software safety management plan

Requirements

Demonstrates how requirements have been captured, allocated, implemented and verified.

- Customer requirements specification
- MPU customer requirements specification
- FPU customer requirements specification
- Software requirements specification
- MPU software requirements specification
- FPU software requirements specification

Design

Defines the architecture, detailed software design and product-specific implementation of SAFE**RTOS**®.

- Architectural software design description
- Architectural software design description for MPU
- Architectural software design description for FPU
- Detailed software design description
- Product specific software design description

Safety

Identifies hazards, assess risks, document mitigations and evidence supporting compliance with safety standards.

- HAZOPS report
- HAZOPS report for MPU requirements
- Investigations arising from HAZOPS
- API usage safety review
- MPU API usage safety review
- Evidence supporting IEC61508-3 SIL3 claim

Test Procedures

Provides objective evidence of the rigorous verification and validation activities performed throughout development.

- Software code verification test description
- Software integration verification test description

WITTENSTEIN high integrity systems
Americas: +1 408 625 4712
ROTW: +44 1275 395 600

email: sales@high**integrity**systems.com
web: www.high**integrity**systems.com

- Software system verification test description
- Validation test description
- Product variant software integration verification test description
- System verification test description
- Test harness build procedure
- SAFE**RTOS**® test harness

Test Results

Gives an overview of the results from the V&V process, before going into the details of each test case.

- Software test report

Process to generate the DAP

To generate the DAP/DHF, WHIS adheres to an extensive process that includes but is not limited to:

- Create the project structure.
- Identify the high level requirements modules that are applicable to this development.
- Create Development Code Release (DCR) – this contains a prototype of the SAFE**RTOS**® code that allows the host application developer to begin their application.
- Implement the Hazard and Operability Study (HAZOPS) on the new device/silicon, ensuring that any silicon or compiler errata are considered.
- Update port specific design and test documentation in-line with changes introduced by the new device.
- Integrate the WHIS test harness to the new device, pin/device mapping, memory map, debug interface, UART, and IO drivers.
- Create the Software Build Procedure – this contains the instructions for building and running the test harness on the new device.
- Create a Software Version Description (SVD) that lists all the artefacts included in the DAP with the issue number of all documents and the MD5 checksums of all SAFE**RTOS**® source files.
- Run all static, module, integration, verification, system and validation tests.
- Run the extended soak test (minimum 36 hours).
- Create a Safety Manual that includes important information that the host application developer needs to consider when integrating SAFE**RTOS**® into their application.
- Create the Software Test Report that summarises the results of the formal test run.
- Create a Claim – Argument – Evidence (CAE) Report that contains a summary of the evidence to be used to support the arguments and claims required to substantiate the development as being compliant with the relevant safety standard.
- Planning/Design/Code/Verification/Release safety reviews are held to confirm the required artefacts have been created at each stage of the development.
- QA activities - these are to ensure that the correct processes have been followed.
- Independent review - the role of the “Independent Reviewer” is to perform the QA activities.

WHIS believes this level of detail and specific testing (to compiler switch level) is required to make a reliable safety claim.

In addition, SAFE**RTOS**® for DO-178C is developed in accordance with a structured RTCA DO-178C compliant lifecycle, following a controlled V model and is fully traceable from requirements through verification. All design and verification artefacts are independently reviewed and quality assured.

Safety made transparent

The SAFE**RTOS**® DAP/DHF combines certification evidence, complete traceability and practical guidance to provide a clear route to compliance. Rather than relying on the safety claims made about SAFE**RTOS**®, it provides the transparency needed to understand how safety has been achieved and how those claims are supported.

Ready to reduce certification effort?

Discover how the SAFE**RTOS**® DAP/DHF can help your team reduce certification effort, improve audit readiness and accelerate compliance.

Talk to a safety expert:
https://www.highintegritysystems.com/question/

WITTENSTEIN high integrity systems
Americas: +1 408 625 4712
ROTW: +44 1275 395 600

WITTENSTEIN

email: sales@high**integrity**systems.com
web: www.high**integrity**systems.com