Factsheet

Qualification Support Kit

Release 24.04, b15284646

April 19, 2024

The Qualification Support Kits have been designed to facilitate the tool qualification of aiT, Astrée, StackAnalyzer, and TimeWeaver for certification activities of safety-critical systems. The QSKs aim at demonstrating the correct functioning of the tool in the operational context of the tool user with respect to the relevant tool-influencing parameters like options, code constructs, provided external information for the analyzers, etc.

All QSKs consist of the following parts:

- specification of the tool functional requirements,
- test cases and test case procedures,
- requirements trace data (traceability matrix),
- test suite and execution framework and
- tool lifecycle data.

The QSKs enable the qualification of aiT, Astrée, StackAnalyzer and TimeWeaver in accordance to domain-relevant safety standards like

- DO-178C / DO-330,
- ISO-26262,
- IEC-61508,
- EN-50128 / EN-50657,
- Regulations for medical devices (EN-60601-1, . . .)

and more.

Details

Tool Functional Requirements

This part defines the tool functions and technical features which are stated as requirements to the tool behavior under normal operating conditions. Each such requirement is assigned a unique identifier to enable traceability to the actual validating test cases.

Additionally, the tool operational context and conditions in which the tool computes valid results, i.e., restrictions (like not supported hardware options or specific code constructs), are listed.

In terms of DO-178C / DO-330, the tool functional requirements are called *Tool Operational Requirements (TOR)*.

Test Cases and Test Case Procedures

The test cases demonstrate the correct functioning of all specified functional requirements. Test case definitions include the overall test setup as well as a detailed structural and functional description of each test case, i.e., how the particular test case works and what the particular expected result is. Analogously to the functional requirements, each test case has a unique identifier for cross referencing purposes.

In terms of DO-178C / DO-330, the test cases and their procedure descriptions is called *Tool Operational Verification and Validation Cases and Procedures (TOVVCP)*.

Trace data (Traceability Matrix)

Using the unique identifiers of functional requirements and test cases, a mapping between them can be achieved. This is realized over a so-called traceability matrix, which lists all test cases categorized by the specific covered requirement(s).

Test Suite and Execution Framework

The test suite contains the implementation of the test cases specified in the TOVVCP that are designed to show that the requirements described in the TOR are satisfied. A test case consists of:

- tool test run(s) and
- optionally evaluation test runs.

A tool test run is basically an analysis project of the particular tool including source code/executable to be analyzed, analyzer options, etc. Depending on the concrete tool test run, an extra evaluation of the analysis results is necessary to check against an expected result as documented in the TOVVCP. The above mentioned evaluation test run refers to such an comparison. A dedicated and documented graphical user interface provides convenient access to analyzer results and support for fully automatic execution and evaluation of all test cases including log reporting facilities. The actual result of a tool qualification run, i.e., the execution of all test cases alongside result evaluation, can be stored together with other certification documents. This output of test case execution constitutes the tool verification results. If all test cases pass, compliance to the TOR has been demonstrated.

Tool Lifecycle Data

In addition to demonstrating that the tool operates correctly in the operational context of the tool user, safety standards often also require evidence that the tool development process fulfills certain demands, e.g., with respect to quality assurance, traceability, requirements engineering and verification activities. These issues are covered by documents which detail the established tool development processes at AbsInt with respect to above described criteria. Document structures have been designed according to the demands of the DO-178C standard, but the requirements to the development processes among different safety standards are common so that the documents can be used for a certification according to other standards as well.

The available documents are:

- the Software Development Plan,
- the Software Configuration Management Plan,
- the Software Quality Assurance Plan,
- the Software Quality Assurance Records,
- the Software Verification Plan,
- the Software Verification Results, and finally
- the Compliance Certificate.

Availability

The Qualification Support Kits are available for all our products.

More information

- Visit our website: www.absint.com
- Speak with a product specialist:
  call +49 681 383 600

About AbsInt

AbsInt provides advanced development tools for embedded systems, and tools for analysis, optimization and verification of safety-critical software. Our customers are located in more than 40 countries worldwide. We have distribution agreements with major software distributors in Asia, North America, Middle East, and throughout Europe.

Our headquarters

Science Park 1
66123 Saarbrücken, Germany
Phone: +49 681 383 600
Fax: +49 681 383 60 20
Email: info@absint.com
Web: www.absint.com