



Qualification Support Kit (QSK)

Datasheet

COPYRIGHT NOTICE:

© QA Systems GmbH

The product name Astrée is a registered trademark of © AbsInt Angewandte Informatik GmbH&S.

All rights reserved. This document, or parts of it, or modified versions of it, may not be copied, reproduced, or transmitted in any form, or by any means, or stored in a retrieval system, or used for any purpose, without the prior written permission of © AbsInt Angewandte Informatik GmbH&S.

ASTRÉE is developed and distributed under license from the CNRS/ENS.

The information contained in this document is subject to change without notice.

Overview

The Astrée Qualification Support Kit (QSK) has been designed to facilitate the tool qualification of Astrée. It aims 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.

The Astrée QSK contains:

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

The QSK enables the tool qualification of Astrée according to following international software safety standards and others:

- > DO-178C / DO-330
- > ISO-26262
- > IEC-61508
- > IEC 62304
- > EN-50128 & EN-50657
- > IEC 60880

Details

Tool Functional Requirements

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

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

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

Test Cases and Test Case Procedures

The Astrée QSK automatically executes a full tool qualification verification test suite on the installed tool configuration and generates the necessary reports for tool qualification.

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 each test case works and what its 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 are respectively 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 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)
- > optionally evaluation test runs

A tool test run is a Astrée analysis project including source code/executable to be analyzed, analyzer options, etc. Depending on the concrete test run, an extra evaluation of the analysis results is necessary to check against an expected result as documented in the TOVVCP. The test run refers to such a 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 in the QSK which detail the established tool development processes with respect to above criteria. Document structures have been designed according to the demands of the DO-178C / DO-330 standards, but the requirements to the development processes among different software safety standards are common so that the documents can be used to meet the tool qualification requirements in other standards, as well.

The tool lifecycle data documents contained in the Astrée QSK are:

- > Software Development Plan
- > Software Configuration Management Plan
- > Software Quality Assurance Plan
- > Software Quality Assurance Records
- > Software Verification Plan
- > Software Verification Results
- > Compliance Certificate.

Astrée QSK Availability

The Astrée Qualification Support Kit (QSK) is available for each version of Astrée.

The QSK includes commercially sensitive tool information, so is only supplied under a Non-Disclosure Agreement from QA Systems.

The Astrée QSK is available for a fee in addition to the tool license(s).

More Information

For further information about Astrée or the Astrée QSK please contact us at:

<https://www.qa-systems.com/tools/astree/>

Sales@qa-systems.com

Support@qa-systems.com