IBM® Engineering Systems Design Rhapsody®

IBM Engineering Systems Design Rhapsody Kit for DO-178B/C Overview

Version 1.14

License Agreement

Trademarks

Table of Contents

1. Purpose

This document provides an overview of the various artifacts in the IBM Engineering Systems Design Rhapsody Kit for DO-178B/C. The IBM Engineering Systems Design Rhapsody Kit for DO-178B/C includes guidance on how to capably develop safety-related software with IBM Engineering Systems Design Rhapsody by meeting the tool qualification objectives described in the safety-related standards DO-178B (1), DO-178C (2), and DO-331 (7). The IBM Engineering Systems Design Rhapsody Kit for DO-178B/C contains the following artifacts:

- IBM Engineering Systems Design Rhapsody Kit for DO-178B/C Overview (this document)
- IBM Engineering Systems Design Rhapsody Reference Workflow Guide
- IBM Engineering Systems Design Rhapsody - TestConductor Add On Reference Workflow Guide
- IBM Engineering Systems Design Rhapsody - TestConductor Add On Safety Manual
- IBM Engineering Systems Design Rhapsody - TestConductor Add On Qualification Kit for DO-178B/C Overview
- IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite
- IBM Engineering Systems Design PSAC for SMXF (Plan for Software Aspects of Certification)
- IBM Engineering Systems Design Rhapsody SXF / SMXF Frameworks (C++ / C)
- IBM Engineering Systems Design Rhapsody SXF / SMXF Validation Suites

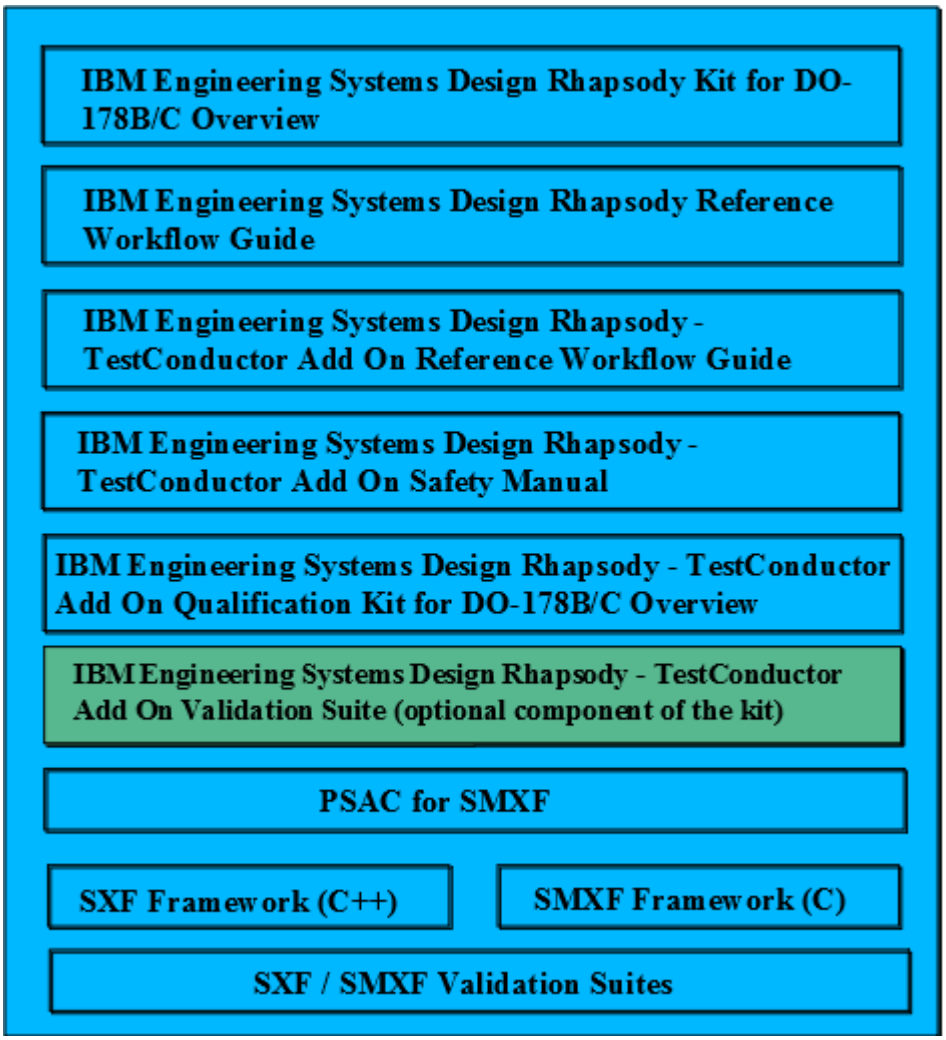

Figure 1: IBM Engineering Systems Design Rhapsody Kit for DO-178B/C

2. Overview about the IBM Engineering Systems Design Rhapsody Kit for DO-178B/C

The current document describes the content of the IBM Engineering Systems Design Rhapsody Kit for DO-178B/C.

2.1 IBM Engineering Systems Design Rhapsody Reference Workflow Guide

The IBM Engineering Systems Design Rhapsody Reference Workflow Guide document (3) focuses on developing safety-related projects with Engineering Systems Design Rhapsody. When developing safety-related software additional quality objectives have to be met in order to produce and deliver “safe” systems. These additional quality objectives essentially depend on

- a specific industrial domain where the product under development shall be deployed,

- an appropriate safety standard that must be applied for a particular domain.

The scope of this document covers software that is developed according to DO-178B (1) or DO-178C (2) or DO-331 (7). DO-178B was released in 1992 and became a commonly used safety standard in the Aerospace industry. DO-178C was published in 2011and will be the commonly used standard in Aerospace in the future. It also provides documents how to leverage from model based methods (DO-331), from object oriented technology, and from formal methods. Such standards describe proven processes and methods for the development of safety-related software, provide guidelines and recommendations for customizing the process and methods to a specific customer process, and also describe what it means to qualify tools in order to use them for the development and testing of safety-related software.

In the IBM Engineering Systems Design Rhapsody Reference Workflow Guide document, focus is placed on UML model-based development and testing of safety-related software with IBM Engineering Systems Design Rhapsody. Also included is the *IBM Engineering Systems Design Rhapsody Reference Workflow* which provides a broader view of the development process spanning requirements, available methods, solutions, and tools.

2.2 IBM Engineering Systems Design Rhapsody - TestConductor Add On Reference Workflow Guide

The IBM Engineering Systems Design Rhapsody - TestConductor Add On Reference Workflow Guide document (4) serves as a reference for testing activities to perform in a model based development process using IBM Engineering Systems Design Rhapsody with the IBM Engineering Systems Design Rhapsody - TestConductor Add On (5). It complements the document IBM Engineering Systems Design Rhapsody Reference Workflow Guide (3) that focuses on the model based development with IBM Engineering Systems Design Rhapsody in safety-related projects. The IBM Engineering Systems Design Rhapsody - TestConductor Add On Reference Workflow Guide document provides further information and describes variations of the IBM Engineering Systems Design Rhapsody Reference Workflow, focusing on testing methods as provided by IBM Engineering Systems Design Rhapsody - TestConductor Add On.

2.3 IBM Engineering Systems Design Rhapsody - TestConductor Add On Safety Manual

The IBM Engineering Systems Design Rhapsody - TestConductor Add On Safety Manual (6) provides guidance on using IBM Engineering Systems Design Rhapsody - TestConductor Add On for testing activities in a model based development process when developing safety-related software. This safety manual complements the previous documents, and provides additional information for installing and using IBM Engineering Systems Design Rhapsody - TestConductor Add On in safety-related projects.

2.4 IBM Engineering Systems Design Rhapsody - TestConductor Add On Qualification Kit for DO-178B/C Overview

The IBM Engineering Systems Design Rhapsody - TestConductor Add On Qualification Kit for DO-178B/C Overview (8) provides guidance to qualify IBM Engineering Systems Design Rhapsody - TestConductor Add On for DO178-B/C projects. Core of the approach is to follow the recommendations of the DO-330 “Software Tool Qualification Considerations”. In order to fulfill the obligations as described in DO-330 a TestConductor validation suite has been developed and been made available to customers. This enables customers to qualify TestConductor for their projects.

2.5 IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite

Note: the TestConductor Validation Suite is an optional component of the kit.

The IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite (9) is one of the fundamental elements used for the qualification and certification of IBM Engineering Systems Design Rhapsody - TestConductor Add On. The Validation Suite has been designed for verifying the correctness for all relevant IBM Engineering Systems Design Rhapsody -TestConductor Add On features for model based testing of IBM Engineering Systems Design Rhapsody models and code. By applying the validation suite a pre-qualification of the tool has been performed. “Pre-qualification” means it is a general tool qualification independent of a specific customer project. If the certification of a customer product requires tool qualification the validation suite can be used to support the tool qualification.

The validation suite consists of

- detailed feature specifications
- detailed test specifications linked to feature specifications
- test implementations for test specifications and test results

The customer/user can use the Validation Suite to reproduce and verify the test results, and to enhance the test scope to user specific environments.

The IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite is not part of the IBM Engineering Systems Design Rhapsody - TestConductor Add On installation. For each Rhapsody major release an appropriate IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite is available. IBM Engineering Systems Design Rhapsody - TestConductor Add On customers can get access to the validation suite through this link:

https://www.ibm.com/services/forms/preLogin.do?source=swg-rhp8tstcdtr

The IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite is delivered as a password protected zip file. A valid IBM Engineering Systems Design Rhapsody - TestConductor Add On license is needed to unzip it. The IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite can be opened with the function

"Rhapsody->Tools->TestConductor->Help->Open Report to the Certificate".

After invoking this function the tool displays a password to the user. This password should be used to unzip the file.

Further distribution of the unprotected IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite is strictly prohibited.

2.6 IBM Engineering Systems Design Rhapsody PSAC for SMXF

The IBM Engineering Systems Design Plan for Software Aspects of Certification for SMXF (PSAC for SMXF) provides information to the user regarding SMXF specification, implementation, testing, etc. This information supports customers during their product certification efforts.

2.7 IBM Engineering Systems Design Rhapsody SXF / SMXF Frameworks (C++ / C)

IBM Engineering Systems Design Rhapsody provides an Object eXecution Framework (OXF) library that is used for standard C and C++ code generation. For safety-related development IBM Engineering Systems Design Rhapsody provides two dedicated libraries called Simplified eXecution Framework (SXF) and Simplified MicroC eXecution Framework (SMXF). The SXF library is the safety-related C++ framework library. It's a comprehensive C++ library that is suitable to be used in safety-related production C++ code environments. The C counterpart of the SXF library is the SMXF library. This is a comprehensive C library that is suitable to be used in safety-related production C code environments.

Both libraries are delivered as part of the standard Rhapsody installation kit for Windows.

2.8 IBM Engineering Systems Design Rhapsody SXF / SMXF Validation Suites

In order to be able using the SXF or SMXF for safety-related developments it is needed to do a systematic qualification of the simplified frameworks. The SXF and SMXF come equipped with validation suites containing:

- Test cases to verify functional correctness of the SXF/SXMF functionality
- Code coverage report after execution of the requirements based test suite
- Requirements coverage report using ReporterPlus. All framework classes and operations are traced to requirements
- MISRA compliance statements

By executing the proper validation suite it can be verified that the chosen framework is fit for its purpose.

Both validation suites are delivered as part of the standard Rhapsody installation kit for Windows.

3. Appendix A: List of References

1. Software Considerations in Airborne Systems and Equipment Certification*, RTCA Inc., RTCA DO-178B.* 1992.
2. Software Considerations in Airborne Systems and Equipment Certification*, RTCA Inc., RTCA DO-178C.* 2011.
3. *IBM Engineering Systems Design Rhapsody Reference Workflow Guide*.
4. *IBM Engineering Systems Design Rhapsody - TestConductor Add On Reference Workflow Guide*.
5. *IBM* Engineering Systems Design Rhapsody - TestConductor Add On. [Online] https://www.ibm.com/us-en/marketplace/systems-design-rhapsody
6. *IBM Engineering Systems Design Rhapsody - TestConductor Add On Safety Manual*.
7. Model-Based Development and Verification – Supplement to DO-178C and DO-278A*, RTCA Inc., RTCA DO-331.* 2011.
8. *IBM Engineering Systems Design Rhapsody - TestConductor Add On Qualification Kit for DO-178B/C Overview.*
9. *IBM Engineering Systems Design Rhapsody - TestConductor Add On Validation Suite*.