IBM® Rational® Rhapsody®

IBM Rational Rhapsody Kit for ISO 26262, IEC 61508, IEC 62304 and EN 50128 Overview

Version 1.11

License Agreement

The information in this publication is subject to change without notice, and BTC Embedded Systems AG assumes no responsibility for any errors which may appear herein. No warranties, either expressed or implied, are made regarding Rhapsody software including documentation and its fitness for any particular purpose.

Trademarks

IBM® Rational® Rhapsody®, IBM® Rational® Rhapsody® Automatic Test Generation Add On, and IBM® Rational® Rhapsody® TestConductor Add On are registered trademarks of IBM Corporation.

All other product or company names mentioned herein may be trademarks or registered trademarks of their respective owners.

Table of Contents

1. Purpose

This document provides an overview of the various artifacts in the IBM Rational Rhapsody Kit for ISO 26262, IEC 61508, IEC 62304 and EN 50128. The IBM Rational Rhapsody Kit for ISO 26262, IEC 61508, IEC 62304 and EN 50128 includes guidance on how to capably develop safety-related software with IBM Rational Rhapsody by meeting the tool qualification objectives described in the safety-related standards ISO 26262 (1), IEC 61508 Edition 2.0 (2), IEC 62304 (10) and EN 50128 (11). The IBM Rational Rhapsody Kit for ISO 26262, IEC 61508, IEC 62304 and EN 50128 contains the following artifacts:

- Rhapsody Kit for ISO 26262, IEC 61508, IEC 62304 and EN 50128 Overview (this document)
- Rhapsody Reference Workflow Guide
- Rhapsody TestConductor Add On Reference Workflow Guide
- Rhapsody TestConductor Add On Safety Manual
- TÜV SÜD Certificate for IBM Rational Rhapsody TestConductor Add On
- TÜV SÜD Report to the Certificate for IBM Rational Rhapsody TestConductor Add On
- Rhapsody TestConductor Add On Validation Suite (Note: the TestConductor Validation Suite is an optional component of the kit)
- IBM Rational Rhapsody SXF / SMXF Frameworks (C++ / C)
- IBM Rational Rhapsody SXF / SMXF Validation Suites

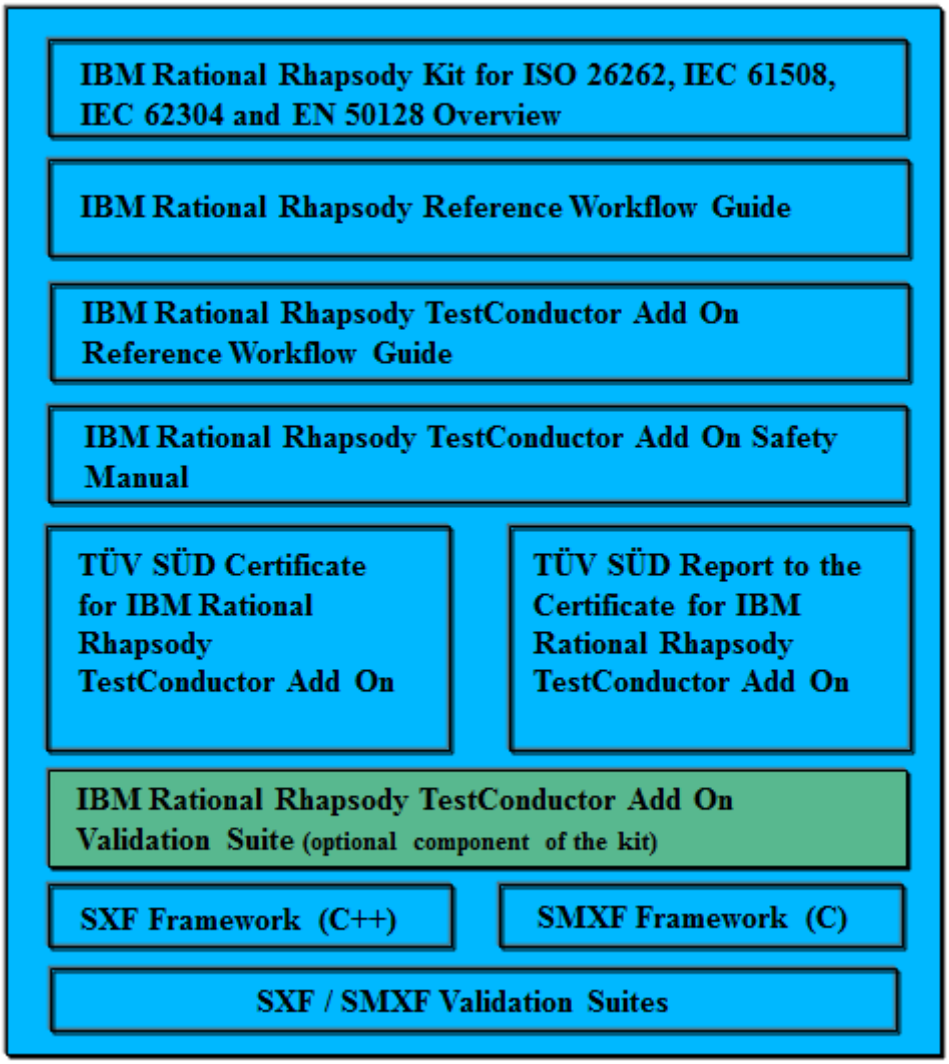

Figure 1: IBM Rational Rhapsody Kit for ISO 26262, IEC 61508, IEC 62304 and EN 50128

2. Overview about the IBM Rational Rhapsody Kit for ISO 26262, IEC 61508, IEC 62304 and EN 50128

The current document describes the content of the IBM Rational Rhapsody Kit for ISO 26262, IEC 61508, IEC 62304 and EN 50128.

2.1 IBM Rational Rhapsody Reference Workflow Guide

The IBM Rational Rhapsody Reference Workflow Guide document (3) focuses on developing safety-related projects with Rational 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 ISO 26262 (1), IEC 61508 (2), IEC 62304 (10) or EN 50128 (11). ISO 26262 was released in 2011 and is becoming a commonly used safety standard in the Automotive industry. IEC 61508 Edition 2.0 was published in 2010 and is a commonly used standard for the development of electrical/electronic/programmable electronic safety-related systems. IEC 62304 was released in 2006 for the medical industry. An updated version of EN 50128 was published in 2012 and is a commonly used standard for the development of Software for Railway Control and Protection Systems. 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 Rational Rhapsody Reference Workflow Guide document, focus is placed on UML model-based development and testing of safety-related software with IBM Rational Rhapsody. Also included is the *IBM Rational Rhapsody Reference Workflow* which provides a broader view of the development process spanning requirements, available methods, solutions, and tools.

2.2 IBM Rational Rhapsody TestConductor Add On Reference Workflow Guide

The IBM Rational 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 Rational Rhapsody with the IBM Rational Rhapsody TestConductor Add On (5). It

complements the document IBM Rational Rhapsody Reference Workflow Guide (3) that focuses on the model based development with IBM Rational Rhapsody in safety-related projects. The IBM Rational Rhapsody TestConductor Add On Reference Workflow Guide document provides further information and describes variations of the IBM Rational Rhapsody Reference Workflow, focusing on testing methods as provided by IBM Rational Rhapsody TestConductor Add On.

2.3 IBM Rational Rhapsody TestConductor Add On Safety Manual

The IBM Rational Rhapsody TestConductor Add On Safety Manual (6) provides guidance on using IBM Rational Rhapsody TestConductor 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 Rational Rhapsody TestConductor in safety-related projects.

2.4 TÜV SÜD Certificate for IBM Rational Rhapsody TestConductor Add On

The official IBM Rational Rhapsody TestConductor Certificate (7) was issued by TÜV SÜD Product Service GmbH, Germany. This certificate states that IBM Rational Rhapsody TestConductor Add On is qualified to be applied in safety-related software development for all SIL levels according to IEC 61508, IEC 62304 and EN 50128, and for all ASIL levels according to ISO 26262.

2.5 TÜV SÜD Report to the Certificate for IBM Rational Rhapsody TestConductor Add On

The Report to the Certificate for IBM Rational Rhapsody TestConductor Add On (8) describes in detail the meaning and the constraints of the IBM Rational Rhapsody TestConductor certificate. It explains the results of the independent testing and certification of IBM Rational Rhapsody TestConductor Add On.

The Report to the Certificate for IBM Rational Rhapsody TestConductor Add On is part of the IBM Rational Rhapsody TestConductor Add On documentation installation. The document is password protected. A valid IBM Rational Rhapsody TestConductor Add On license is needed to open this document. The Report to the Certificate (PDF format) 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 entered into the PDF viewer to eventually open the Report to the Certificate.

Further distribution of the unprotected document is strictly prohibited.

2.6 IBM Rational Rhapsody TestConductor Add On Validation Suite

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

The IBM Rational Rhapsody TestConductor Add On Validation Suite (9) is one of the fundamental elements used for the qualification and certification of IBM Rational Rhapsody TestConductor Add On. The Validation Suite has been designed for verifying the correctness for all relevant IBM Rational Rhapsody TestConductor Add On features for model based testing of IBM Rational 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 Rational Rhapsody TestConductor Add On Validation Suite is not part of the IBM Rational Rhapsody TestConductor Add On installation. For each Rhapsody major release an appropriate IBM Rational Rhapsody TestConductor Add On Validation Suite is available. IBM Rational 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 Rational Rhapsody TestConductor Add On Validation Suite is delivered as a password protected zip file. A valid IBM Rational Rhapsody TestConductor Add On license is needed to unzip it. The IBM Rational 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 Rational Rhapsody TestConductor Add On Validation Suite is strictly prohibited.

2.7 IBM Rational Rhapsody SXF / SMXF Frameworks (C++ / C)

IBM Rational Rhapsody provides an Object eXecution Framework (OXF) library that is used for standard C and C++ code generation. For safety-related development IBM Rational 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 Rational 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 Figures

4. Appendix B: List of References

1. *Road vehicles – Functional Safety, International Organization for Standardization, ISO 26262.* 2011.
2. *Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508, Edition 2.0.* 2010.
3. *IBM Rational Rhapsody Reference Workflow Guide*.
4. *IBM Rational Rhapsody TestConductor Add On Reference Workflow Guide*.
5. *IBM* Rational Rhapsody TestConductor AddOn. [Online] http://www-01.ibm.com/software/awdtools/rhapsody/.
6. *IBM Rational Rhapsody TestConductor Add On Safety Manual*.
7. *TÜV SÜD Certificate for IBM Rational Rhapsody TestConductor Add On, No. Z10-16-02-81878-003.* 2016.
8. *TÜV SÜD Report to the Certificate for IBM Rational Rhapsody TestConductor Add On, No. IW84460C-1.3.1.* 2016.
9. *IBM Rational Rhapsody TestConductor Add On Validation Suite*.
10. *Medical device software – Software life cycle processes, IEC 62304 Edition 1.0*, 2006.
11. *Railway Applications: Software for Railway Control and Protection Systems, EN 50128*, 2011.