



IBM Software Group

IBM Rational Tool Qualification Kits

Karla Ducharme

*Market Manager for Automotive and Aerospace and Defense
IBM Rational Software
kducharm@us.ibm.com*

Rational software



AGENDA

- IBM Rational Tool Qualification Overview
- IBM Rational DOORS Kit for ISO 26262 and IEC 61508
- IBM Rational Rhapsody Kit for ISO 26262 and IEC 61508
- Tool Qualification Kit for Test RealTime
- ISO 26262 Process Templates



AGENDA

- IBM Rational Tool Qualification Overview
- IBM Rational DOORS Kit for ISO 26262 and IEC 61508
- IBM Rational Rhapsody Kit for ISO 26262 and IEC 61508
- Tool Qualification Kit for Test RealTime
- ISO 26262 Process Templates



IBM Rational Approach to Tool Qualification

Lessen the costs to produce certifiable or compliant products by providing:

- Artifacts that can be used for multiple industries (Auto, A&D, Medical, Nuclear, etc).
- Services to help customers customize or create additional tool qualification assets
- Templates and other artifacts to jumpstart project deployment and tool qualification efforts
- Lifecycle and Design Automation that matters



IBM Rational Approach to Tool Qualification

Providing pieces to simply the compliance/qualification puzzle

Support Processes



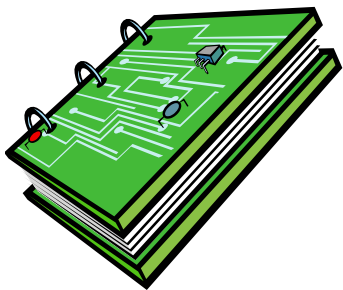
Validation Test Suites



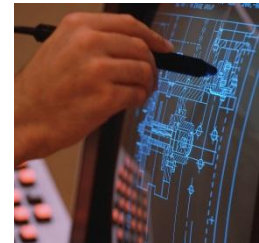
Independent Process Audits



Guidance on how to safely use the tool(s)



Process templates with workflows, roles, required artifacts, process and tool guidance



Tool Architecture Templates



AGENDA

- IBM Rational Tool Qualification Overview
- IBM Rational DOORS Kit for ISO 26262 and IEC 61508
- IBM Rational Rhapsody Kit for ISO 26262 and IEC 61508
- Tool Qualification Kit for Test RealTime
- ISO 26262 Process Templates



The IBM Rational DOORS Kit for ISO 26262 and IEC 61508

- Released as part of DOORS 9.5 on November 28, 2012
- Applicable to DOORS 9.4, 9.4.0.1, and DOORS 9.5 (Not DOORS NG at this time)
- Available for download as part of the DOORS 9.5 via Passport Advantage

Artifact	Description
TÜV SÜD certificate for DOORS for ISO 26262 and IEC 61508	PDF image of the issued certificate
TÜV SÜD report to the certificate	Report for the TÜV SÜD Certificate for Rational DOORS for ISO 26262 and IEC 61508
Rational DOORS Safety Manual	Describes best practices in using DOORS for safety related projects. These recommendations are an integral part of the certificate.
DOORS ISO 26262 Template	DOORS project archive that contains includes basic modules and attributes for capturing requirements and safety information
Intended Use Validation Suite	DOORS project with a set of requirements traced to features, test cases and tests that can be performed in customer environments to document and verify specific uses of DOORS .



Generic TUV Certificate

Users are responsible for verifying that their tool usage complies with the scope of the certificate and executing the tool qualification processes per the standard they are required to comply with

ZERTIFIKAT ◆ CERTIFICATE ◆ CERTIFICADO ◆ CERTIFICAT



Product Service

CERTIFICATE

No. Z10 12 11 82971 001

Holder of Certificate: **IBM Corporation**
 Buchan House
 21 St Andrew Square
 Edinburgh
 EH2 1AY
 UNITED KINGDOM

Factory(ies): 82971

Certification Mark:



Product: **Software Tool for Safety Related Development**

Model(s): **IBM Rational DOORS**

Parameters:
 IBM Rational DOORS is fit for purpose for developing safety related software according to IEC 61508 and/or ISO 26262.
 The report no. IE77001aC is a mandatory part of this certificate.

Tested according to:
 ISO 26262:2011
 IEC 61508-3:2010
 IEC 61508-4:2010

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: IE77001aC


 (Andreas Barwald)

Date: 2012-11-20

Page 1 of 1



TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany





How customers can rely on these artifacts for tool qualification

Tool Qualification Method	Applicability of the TÜV SÜD Certificate and related assets
1a: Increased confidence from use in accordance with 11.4.7	TÜV SÜD has evaluated the customer information and bug tracking of IBM Rational which contributes to an increased confidence because it helps with systematically collecting data and acquiring errors over a large number of customers and projects. The applicable requirements of the qualification method “Increased confidence from use” (ISO 26262, part 8, 11.4.7), were assessed successfully. Tool users can use this result as additional in-formation to substantiate their own argument “Increased confidence from use”.
1b: Evaluation of the tool development process in accordance with 11.4.8	The TÜV SÜD has evaluated the DOORS development process according to an appropriate standard based on the relevant portions of the ISO 26262:2011 standard. The qualification method “Evaluation of the tool development process” (ISO 26262, part 8, 11.4.8), was performed successfully. It can be applied without any restrictions. In addition, IBM Rational holds an ISO 9001 certificate for the DOORS development process as well.
1c: Validation of the software tool in accordance with 11.4.9	<p>The TÜV SÜD has analyzed the validation suite that is used by IBM Rationale for DOORS relative to the usage of features described in the DOORS Safety Manual. It is the responsibility of the customer to check if the described conditions of use and the used features match with the descriptions in the safety manual. Any features not described in the safety manual are not covered by the certificate and need extra measures by the customer (e.g. executing their own validation for those features).</p> <p>In addition, IBM Rational is able to provide a DOORS Intended Use Validation test suite as a basis for customers that desire to run DOORS Validation Tests using DOORS differently than described in the safety manual and to ensure that all features work like intended in their environment. This test suite is not covered by the certificate itself but may be used to enforce the argument for 1c.</p>
1d: Development in accordance with a safety standard	This argument is not applicable, since DOORS was not developed as a safety critical development item according to a safety standard.



DOORS Safety Manual

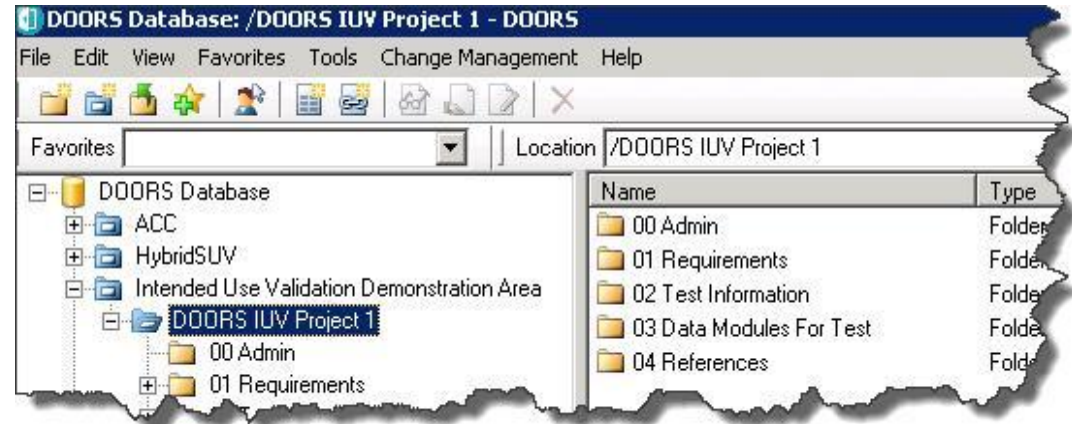
- Provides guidance on installation, administration and usage
- Defines usage at feature level to easily adapt it to numerous use cases
- Defines potential errors such as data corruption from disk error and provides recommended usage to detect or prevent the error
- Each feature analyzed to provide a generic confidence level for Tool error detection (TD) and subsequent tool confidence level (TCL)

Contents

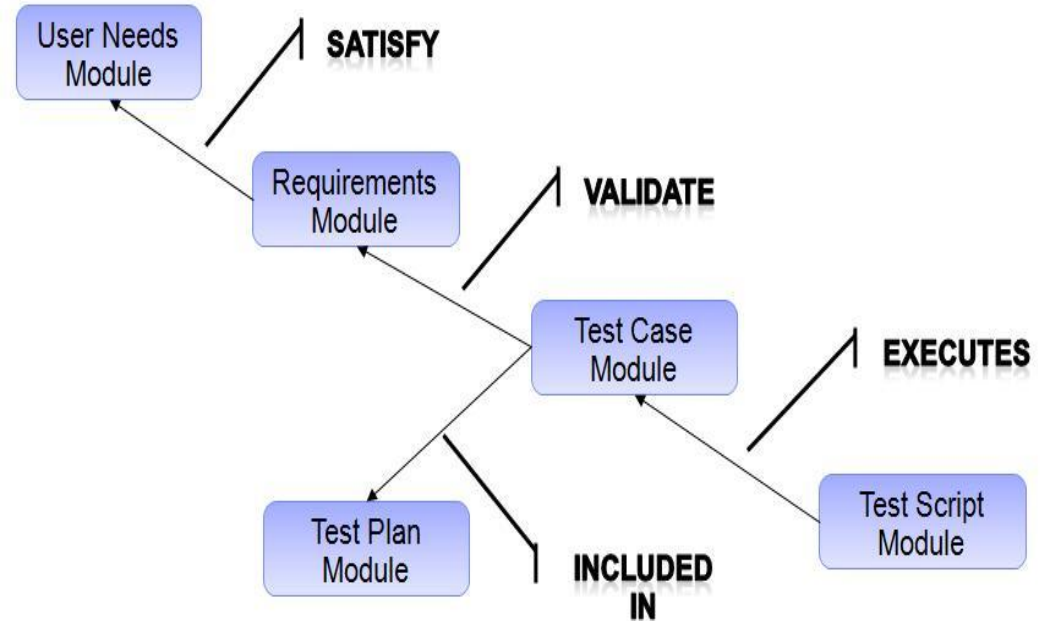
1	Purpose	6
2	Scope of the certification.....	6
2.1	Certified features of DOORS.....	6
2.2	Other features of DOORS.....	8
2.3	Responsibilities of the user	9
3	Overview.....	11
3.1	Purpose of using DOORS.....	11
3.2	Version of DOORS.....	11
3.3	Reference manual.....	13
3.4	Support information.....	14
3.5	Evaluation Method and ISO 26262 Requirements.....	16
4	Practices to use DOORS safely.....	19
4.1	Installation	19
4.2	Data Backup.....	23
4.3	User management	24
4.4	Information architecture.....	27
5	Features of DOORS.....	33
5.1	Features at database level	35
5.2	Features for documents.....	38
5.3	Features for displaying information	43
5.4	Features for links	45
5.5	Features for data exchange.....	49
5.6	Additional features	55
5.7	Features for customizing DOORS.....	58
5.8	Non-critical Features.....	59
6	Detailed descriptions of error checks.....	60



DOORS Intended Use Validation Test Suite



- DOORS project Archive
- Populated with common usage models
- Easy to modify and extend to fit customer specific user scenarios
- Framework for performing validation testing as needed to help qualify DOORS usage
- Supplements TUV SUD certificate and related artifacts
- Leverages manual tests to execute and capture test results
- IBM can provide services to customize and execute in our environment



DOORS Template for ISO 26262

- Capture Severity, Probability and Controllability attributes
- Automatically determines ASIL
 - ▶ Working on matching these attributes to attributes in Rhapsody
- Developing requirements module structure to capture relationships between
 - ▶ Stakeholder (Item Definition) Requirements
 - ▶ Functional Safety Requirements
 - ▶ Technical Safety Requirements
 - ▶ System Safety Requirements
 - ▶ HW and SW safety requirements
- Automatic propagation through Safety Requirement Hierarchy of ASIL
- Delivered as a DOORS project archive

'Adaptive Cruise Control Safety Goals' current 0.0 in /ACC/01 - Stakeholder Requirements (Formal module) - DOORS

ID	The high level safety goals for the ACC system	Severity Class	Probability Class	Controllability Class	Safety Goal A
ACC-SG-2	1 Safety Goals	N/A	N/A	N/A	N/A
ACC-SG-3	1.1 Collision Prevention	N/A	N/A	N/A	N/A
ACC-SG-4	Prevent the vehicle from hitting an obstruction whilst Active Cruise Control mode is active	S2	E2	C3	A
ACC-SG-5	Ensure that when the Active Cruise Control is active it shall identify potential obstructions in its path and make the required warnings and signals to the driver and other relevant systems.	S3	E3	C3	C
ACC-SG-6	1.2 Cruise Control Deactivation	N/A	N/A	N/A	N/A
ACC-SG-8	When the cruise control is active it shall be possible to deactivate it automatically in the case of a potential collision or the vehical speed is less than 25 mph, or by action of the driver using the brake or off switch.	S2	E3	C3	B

'Functional Safety reqs' current 0.0 in /ACC/02 - System Requirements (Formal module) - DOORS

ID	AdaptiveCruiseControlV2.rpy	ASIL Level	Out-links (Adaptive Cruise Control Safety Goals)
FSR14	1.1.6 Driver warnings A mechanism shall be put in place to detect and alarm the driver if a warning signal is sent and not displayed or audibly sounded via the normally specified methods.	B	it shall identify potential obstructions in its path and make required warnings and signals to the driver and other rele systems. Safety Goal ASIL: C Identifier: ACC-SG-8 Safety Goal: When the cruise control is active it shall be to deactivate it automatically in the case of a potential colli the vehical speed is less than 25 mph, or by action of the using the brake or off switch.
FSR15	1.1.7 Driver signals to ACC A mechanism shall be put in place to ensure that any corruption of signals to and from the driver should be recognised.	B	Safety Goal ASIL: B Identifier: ACC-SG-8 Safety Goal: When the cruise control is active it shall be to deactivate it automatically in the case of a potential colli the vehical speed is less than 25 mph, or by action of the using the brake or off switch.
FSR16	1.1.8 Reaction to bad signals If the mechanism to detect and identify corrupt or missing signals does identify the missing signal it shall 1/ In the case of a corrupt signalthe mechanism shall derive the correct signal or safest variation of that signal. 2/ In the case of missing signals the cruise control shall shut down automatically and warn the driver in a suitable manner.	C	Identifier: ACC-SG-5 Safety Goal: Ensure that when the Active Cruise Control it shall identify potential obstructions in its path and make required warnings and signals to the driver and other rele systems. Safety Goal ASIL: C Identifier: ACC-SG-8 Safety Goal: When the cruise control is active it shall be to deactivate it automatically in the case of a potential colli the vehical speed is less than 25 mph, or by action of the using the brake or off switch.
FSR17	1.1.9 If brake sensor pad	B	Identifier: ACC-SG-8 Safety Goal: When the cruise control is active it shall be



AGENDA

- IBM Rational Tool Qualification Overview
- IBM Rational DOORS Kit for ISO 26262 and IEC 61508
- IBM Rational Rhapsody Kit for ISO 26262 and IEC 61508
- Tool Qualification Kit for Test RealTime
- ISO 26262 Process Templates



Rhapsody Kit for ISO 26262 and IEC 61508

Similar Kit for DO-178B/C

- Overview Doc: describes the contents of the Rhapsody kit
- Rhapsody Reference workflow : provides an exemplary workflow for modelling, code generation and verification in safety critical
- Rhapsody TestConductor Add On Workflow: describes testing activities and objectives
- Rhapsody TestConductor Safety Manual: provides additional information for using TestConductor in safety related applications
- TÜV SÜD Certificate for Rhapsody TestConductor Add On
- TÜV SÜD Report on Certificate for ISO 26262 and IEC 61508
- Rhapsody TestConductor Add On Validation Suite: separately available test suite for Rhapsody TestConductor to help in qualification efforts
- Kits for the SXF (C++) and SMXF (C) frameworks



IBM Rational Rhapsody Kit for ISO 26262 and IEC 61508 Overview

IBM Rational Rhapsody Reference Workflow Guide

IBM Rational Rhapsody TestConductor Add On Reference Workflow Guide

IBM Rational 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

IBM Rational Rhapsody TestConductor Add On Validation Suite (optional component of the kit)

SXF Framework (C++)

SMXF Framework (C)

SXF / SMXF Validation Suites

IBM Rational Rhapsody Kit for ISO 26262 and IEC 61508

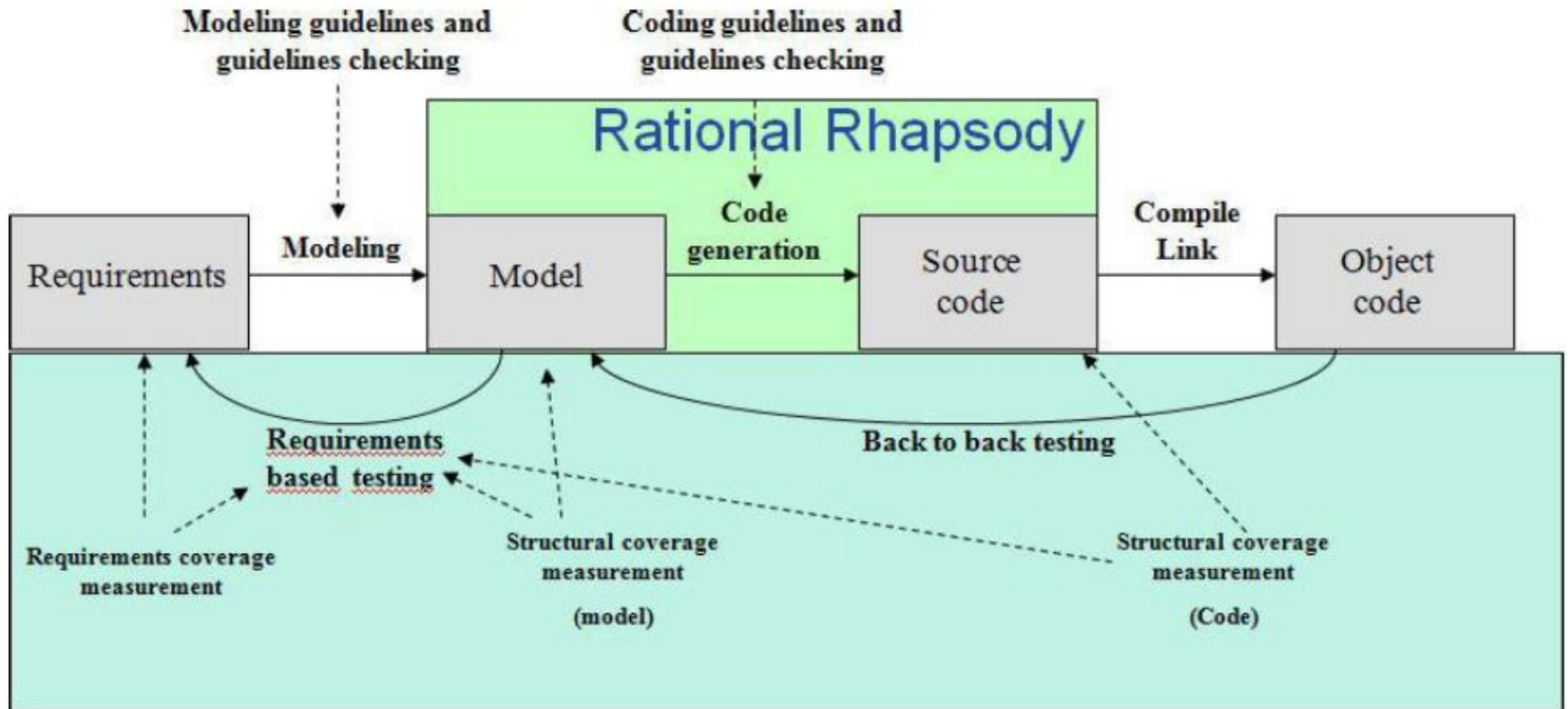


Figure 1: Activities of the IBM Rational Rhapsody Reference Workflow

Describe approach to workflow...using mechanisms such as Back to back testing, Reqs. Based Testing to achieve TD1 for code generation through process and qualified testing capability

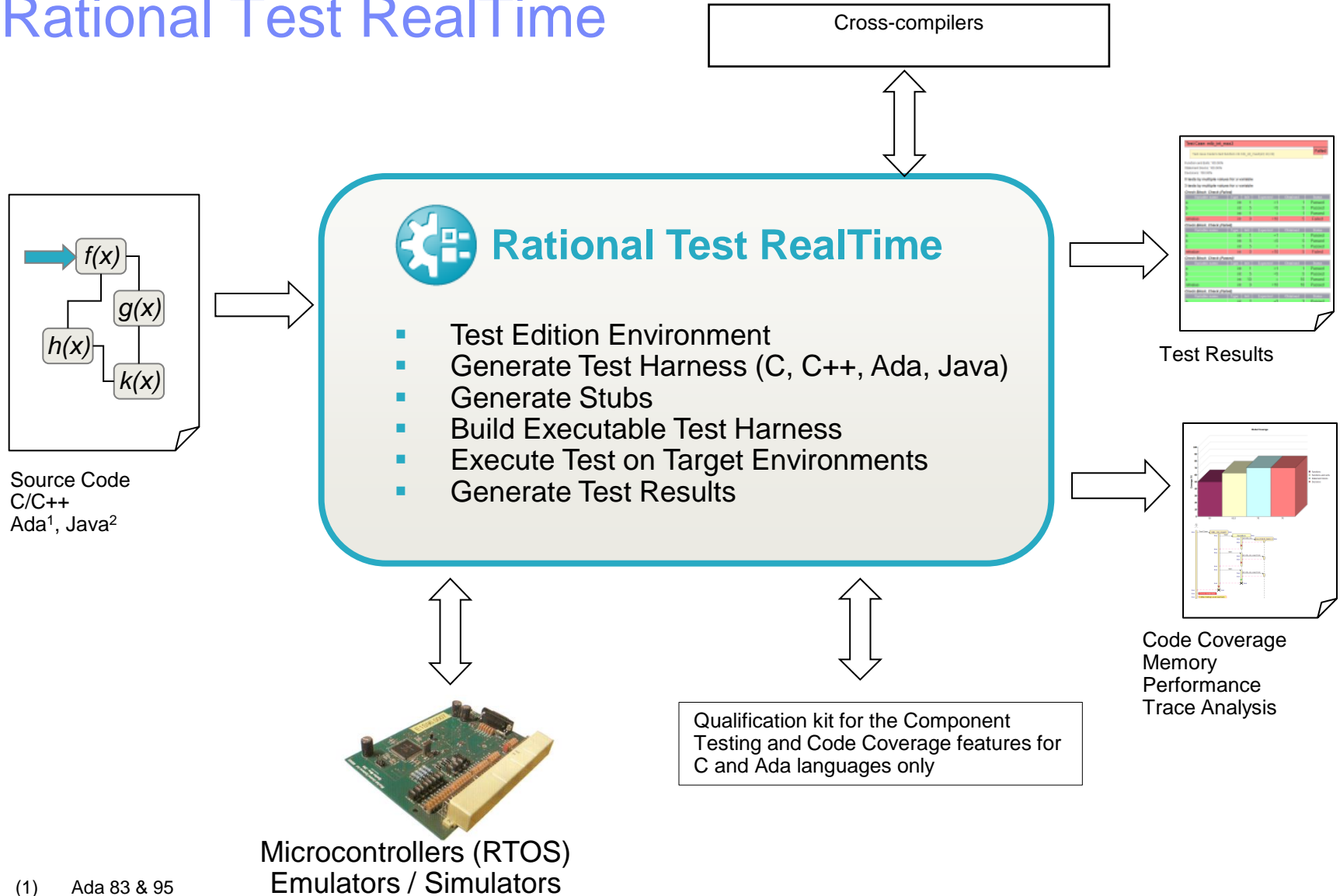


AGENDA

- IBM Rational Tool Qualification Overview
- IBM Rational DOORS Kit for ISO 26262 and IEC 61508
- IBM Rational Rhapsody Kit for ISO 26262 and IEC 61508
- Tool Qualification Kit for Test RealTime
- ISO 26262 Process Templates



Rational Test RealTime



(1) Ada 83 & 95
(2) Java 1.4 J2SE & J2ME

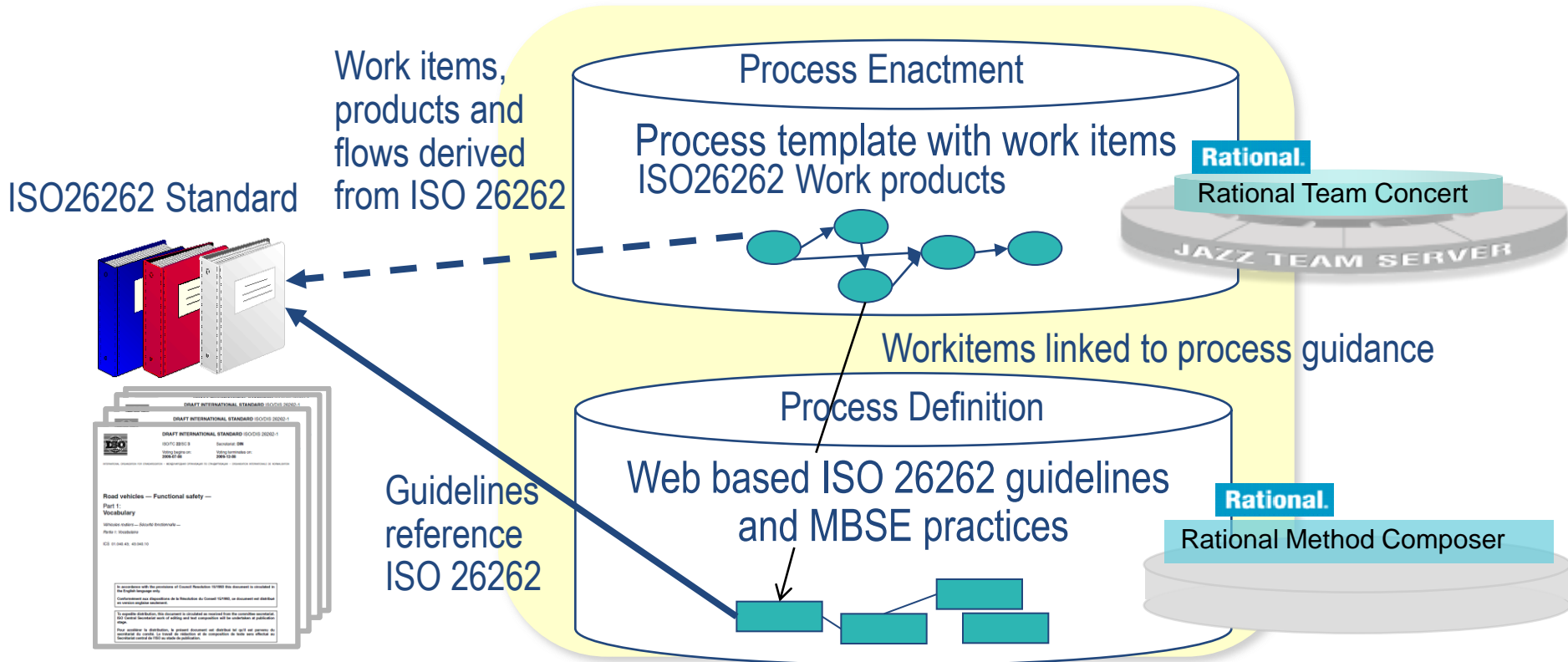
AGENDA

- IBM Rational Tool Qualification Overview
- IBM Rational DOORS Kit for ISO 26262 and IEC 61508
- IBM Rational Rhapsody Kit for ISO 26262 and IEC 61508
- Tool Qualification Kit for Test RealTime
- ISO 26262 Process Templates



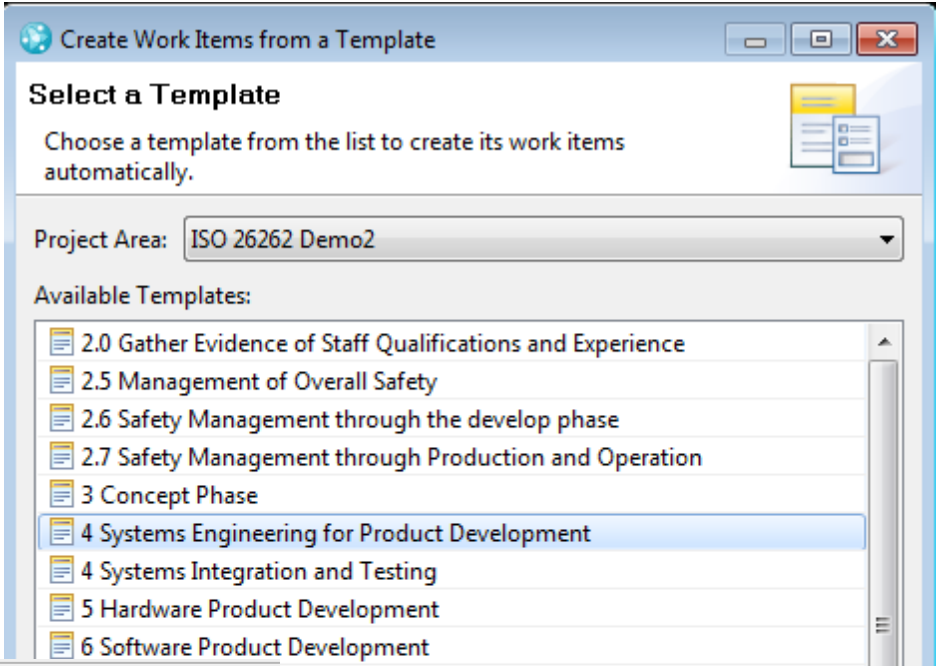
Out-of-the-box ISO 26262 Project Workflows

- Supports all core processes and work products defined in the standard
- Process template implemented in Rational Team Concert
- Guidance and practices implemented in Rational Method Composer



ISO 26262 work item templates

- Work item templates are modularised , it covers
 - Separate safety management section
 - Main concept phases
 - Separation of production and operation activities
 - Aspects of supporting processes



Tag Cloud Problems Pending Changes Team Advisor Work Items

Found 12 work items - 2.6 Safety Management through the develop phase

Id	Status	P	S	Summary	Owned By	Created By
651	New			2.6 Development Safety Management	Unassigned	Graham
652	New			Assign Project Manager	Unassigned	Graham
653	New			Assign Safety Manager	Unassigned	Graham
654	New			Organise Process and Tools Team	Unassigned	Graham
655	New			Develop functional safety assessment plan	Unassigned	Graham
656	New			Determine confirmation measures	Unassigned	Graham
657	New			Develop confirmation plan	Unassigned	Graham
658	New			Organise and ensure sufficient qualified resources are a...	Unassigned	Graham
659	New			Develop safety case	Unassigned	Graham
660	New			Develop safety plan	Unassigned	Graham
661	New			Tool Environment Setup	Unassigned	Graham
662	New			Project independent tailoring of the safety cycle	Unassigned	Graham

of SW tools
of HW components
supplier relationship
ement
nning
Set Up
the functional safety concept, the item is developed fr



Out-of-the-box Process Mappings to DO-178B/C Objectives

▶ DO-178B

 ▼ DO-178C

- Welcome to the Rational Aerospace Solution for DO-178C
- + Getting Started
- + Delivery Processes
- DO-178C Objectives
 - + DO-178C Software Planning Process
 - + DO-178C Software Development Process
 - + DO-178C Verification of Output of SW Requirements
 - + DO-178C Verification of Outputs of SW Design
 - + DO-178C Verification of Outputs of Coding and Integration
 - + DO-178C Testing of Outputs of Integration
 - + DO-178C Verification of Verification Results
 - + DO-178C SW Configuration Management Process
 - + DO-178C SW Quality Assurance Process
 - + DO-178C Certification Liaison Process
- DO-331 MDD
 - DO-331 Software Development Process
 - Objective A.2.8 MB
 - Objective A.2.9 MB
 - Objective A.2.10 MB
 - + DO-331 Verification of Output of SW Requirements
 - + DO-331 Verification of Outputs of SW Design
 - + DO-331 Verification of Verification Results
- + DO-332 OOT
- + DO-178C SW Certification Levels
- + Guidance

DO-331 MDD > DO-331 Software Development Process > Objective A.2.8 MB

Objective A.2.8 MB



Specification Model elements that do not contribute to implementation or realization

Main Description

Required for levels A, B, C, D.

Related elements:

- Identify Elements and Refine Collaborations
- Design and Optimize - Architectural Level
- Design and Optimize - Collaboration Level
- Identify Objects and Classes
- Optimize Subsystems and Component Architecture
- Optimize Collaboration
- Optimize Class

More information:

- Practice: High-Fidelity Modeling
- Practice: Real-Time Architectural Design
- Practice: Real-Time Collaborative Design
- Practice: Real-Time Detailed Design
- Practice: Continuous Integration

Part of this text is copyrighted by RTCA, Inc. and used with permission.
 © Copyright IBM Corp. 1987, 2010. All Rights Reserved



Out-of-the-box Process Mappings to DO-178C Objectives

DO-178B Objectives > DO-178B Software Planning Process > Objective A.1.5

Objective A.1.5



Software development standards are defined.

Main Description

The required outputs are:

- Software Requirements Standards
- Software Design Standards
- Software Code Standards

Required for levels A, B, C.

Related elements:

- Plan Requirements Management Strategy
- Requirements Management Process Description

- Checklists:
 - Platform Independent Model
 - PIM Review
 - Platform Specific Model

- Guidelines:
 - Coding Standard
 - Design Constraints
 - Naming Conventions
 - Source Code

- SW Requirements Standard, SW Design Standard, SW Coding Standard

More information:

- Practice: Requirements Management
- Practice: High-Fidelity Modeling
- Practice: Real-Time Architectural Design
- Practice: Real-Time Collaborative Design
- Practice: Real-Time Detailed Design

DO-178B Objectives > DO-178B Verification of Outputs of Coding and Integration > Objective A.5.5

Objective A.5.5



Source code is traceable to low-level requirements.

Main Description

Traceability of a few source code statements per low-level requirements is required.

This is required for levels A, B, C.

Related elements:

- Translate and Validate - Architecture Level
- Translate and Validate - Collaboration Level
- Translate and Validate - Detailed Level
- Test Iteration [Template]
- Test Findings
- Test Evaluation Summary
- Traceability Record
- Requirements Traceability

More information:

- Practice: Model-Based Testing
- Practice: Independent Testing
- Practice: Requirements Management
- Practice: Elaborate Draft System Requirements Specification





www.ibm/software/rational

