10 Automotive SPIN Italia Workshop

Le normative e gli standard del settore automotive (ISO 26262,IEC 61508, MISRA, AUTOSAR) come ausilio alla progettazione

Ing. Alberto Sardini albertosardini@it.ibm.com

Milano 25 ottobre 2012

Agenda

- Introduzione
- Normative
- Normative come base per il processo di progettazione : IBM Rational

Agenda

- **Introduzione**
- Normative
- Normative come base per il processo di progettazione : IBM Rational

Systems of Systems

Smart Products

Smarter healthcare

Smarter energy

Products of all types are becoming more instrumented, interconnected and intelligent

Imperatives in developing smarter products and systems

Leapfrog Innovation

Accelerate Delivery

Manage Complexity

Streamline Compliance

Increase Productivity

Ensure Quality

Improve Predictability

Barriers: Silos of people, process, and projects

Geographic Barriers

- Poor communication
- Time differences. Unable to leverage 24x7 activity

Organizational Barriers

- Lack of meaningful collaboration
- Process gaps resulting in rework

Infrastructure Barriers

- Unreliable access to cross-lifecycle information
- Inflexible tooling integration

Agenda

- Introduzione
- **Normative**
- Normative come base per il processo di progettazione : IBM Rational

Industry Compliance, Standards and Frameworks

- Industry Standards
  - Avionics/aerospace
    - DO-178B/C / ED-12B (RTCA/EUROCAE)
  - Medical
    - FDA and IEC 62304
  - Functional safety in process industry
    - IEC 61508
  - Automotive
    - ISO-26262, AUTOSAR, MISRA-C
  - Railway systems
    - EN50128 and EN50129
  - Nuclear
    - IEC 880, IEC 60880, IEC 61513, IEC 62138

- Industry Frameworks
  - DoDAF 2.0 – Department of Defense Architecture Framework
  - MoDAF 1.2 – Ministry of Defense Architecture Framework
  - UPDM 2.0 – Unified Process for DoDAF and MoDAF

Industry Compliance, Standards and Frameworks

- Safety Critical – DO-178B/C
  - DO-178B defines detailed guidelines for development of aviation software that performs intended functions
    - The Federal Aviation Authority (FAA) accepts use of DO-178B as a means of certifying software in avionics
  - DO-178B outlines the *objectives* to be met, the work activities to be performed for each objective, and the *evidence* (output documents) to be supplied for each objective (based on criticality level A-E)
  - DO-178C was made available in January 2012, and includes new objectives (71 rather than 66 for Level A), more rigorous traceability and supplementary documents covering Model based development, tool qualification and formal methods.

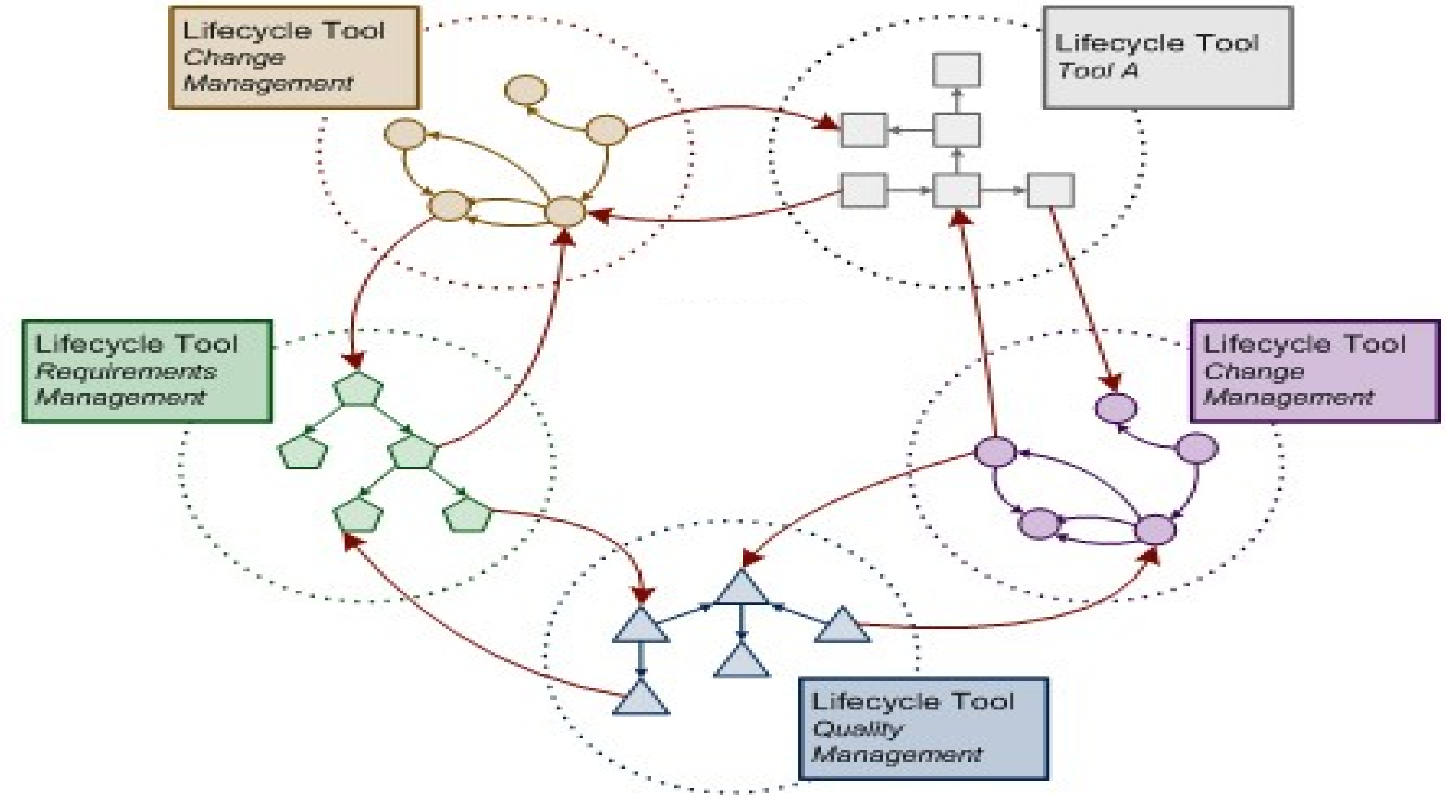
- Functional Safety – ISO-26262
  - A new functional safety standard (released in late 2011) used in Electrical/Electronic Automotive systems. It covers all aspects of the development lifecycle including specification, design, implementation, integration, verification, validation, and production release.

- Architectures – AUTOSAR
  - A open and standardized automotive software Electrical/Electronic architecture, created by OEM and Automotive suppliers. AUTOSAR provides implementation of basic system functions as an industry wide "Standard Core" solution. The standard includes definition of modular software architecture for control units, standardization of interfaces and a runtime environment

Resources from different domain tools need to be linked together

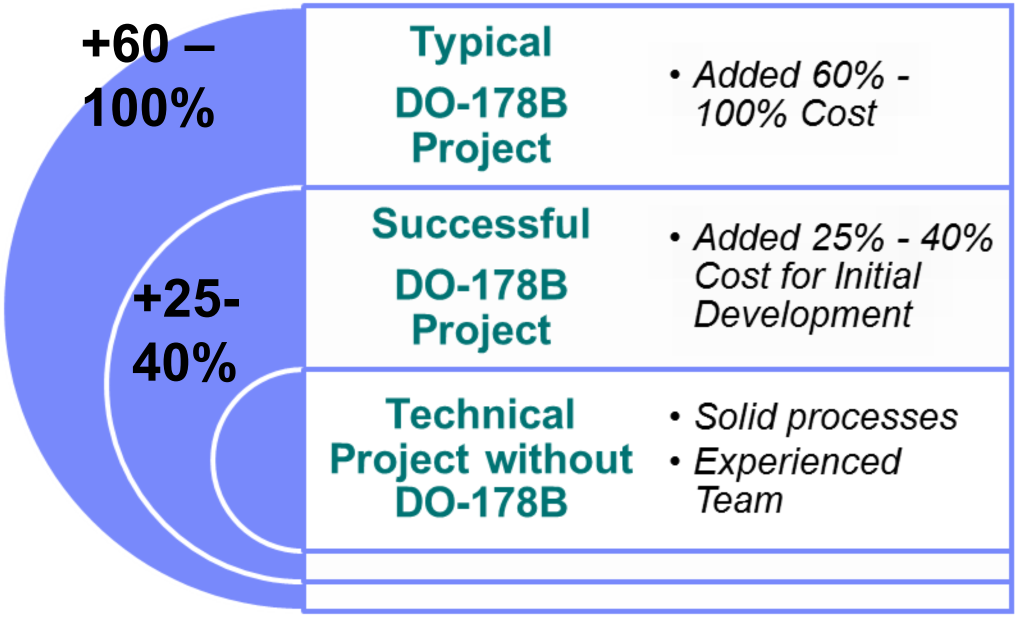
Compliance & Standards standard give advise about:

link, navigation, managing, publishing, etc



Standards often initially increase project costs

Example: DO-178B



+60 – 100%

+25-40%

Typical DO-178B Project

- *Added 60% - 100% Cost*

Successful DO-178B Project

- *Added 25% - 40% Cost for Initial Development*

Technical Project without DO-178B

- *Solid processes*
- *Experienced Team*

Common issues

Inadequate formal plans or not following them

Inadequate level of detail and process for Requirements

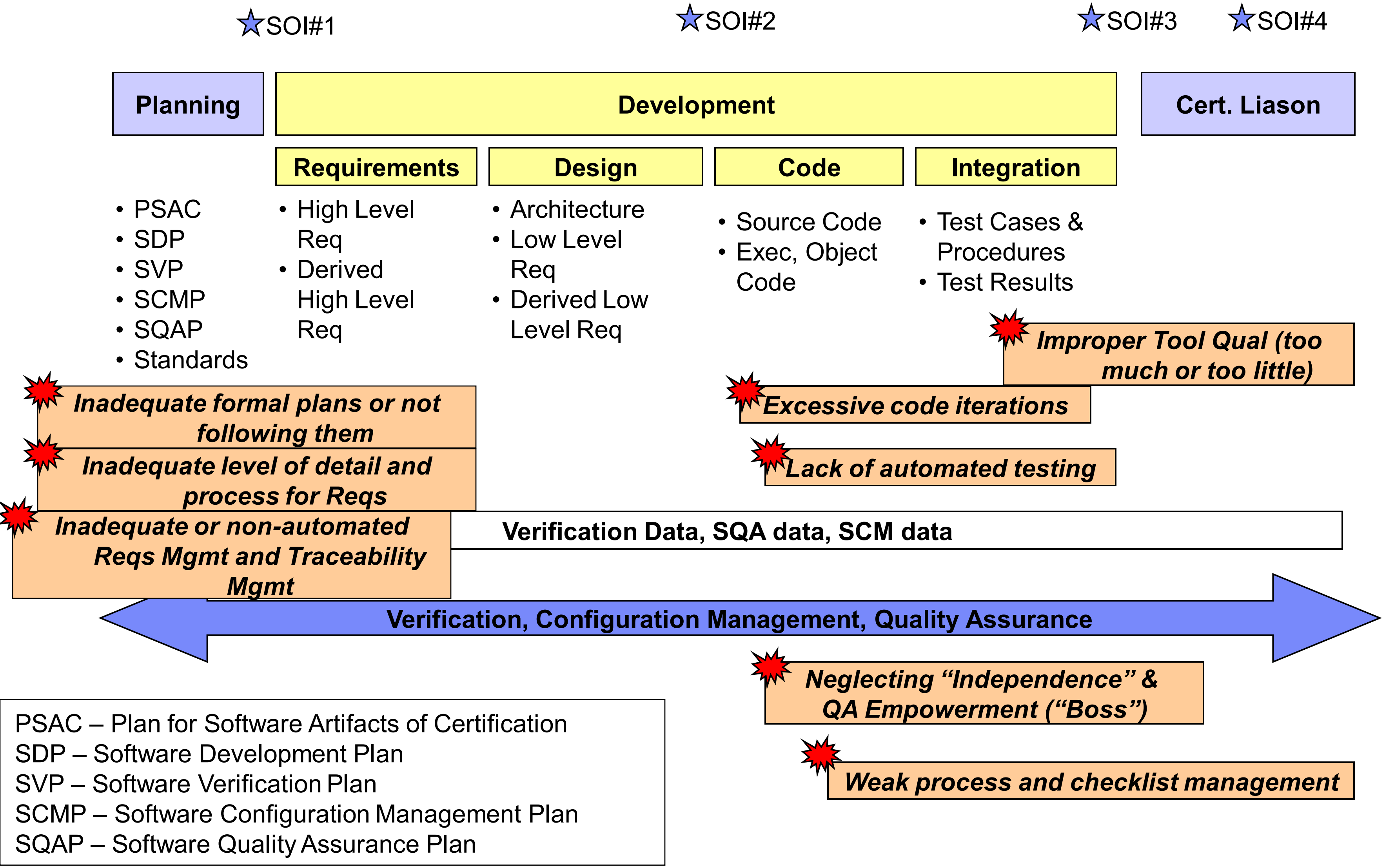
Inadequate or non-automated Requirements Mgmt and Traceability Mgmt

Improper Tool Qualification (too much or too little)

Weak process and checklist management

Source: Avionics Certification – Vance Hilderman and Tony Baghai (avionics publications)

Common Issues arising from adopting Standards. Example: DO-178B



☆SOI#1 ☆SOI#2 ☆SOI#3 ☆SOI#4

Planning

- PSAC
- SDP
- SVP
- SCMP
- SQAP
- Standards

Development

Requirements

- High Level Req
- Derived High Level Req

Design

- Architecture
- Low Level Req
- Derived Low Level Req

Code

- Source Code
- Exec, Object Code

Integration

- Test Cases & Procedures
- Test Results

Cert. Liason

Inadequate formal plans or not following them

Inadequate level of detail and process for Reqs

Inadequate or non-automated Reqs Mgmt and Traceability Mgmt

Improper Tool Qual (too much or too little)

Excessive code iterations

Lack of automated testing

Verification Data, SQA data, SCM data

Verification, Configuration Management, Quality Assurance

Neglecting "Independence" & QA Empowerment ("Boss")

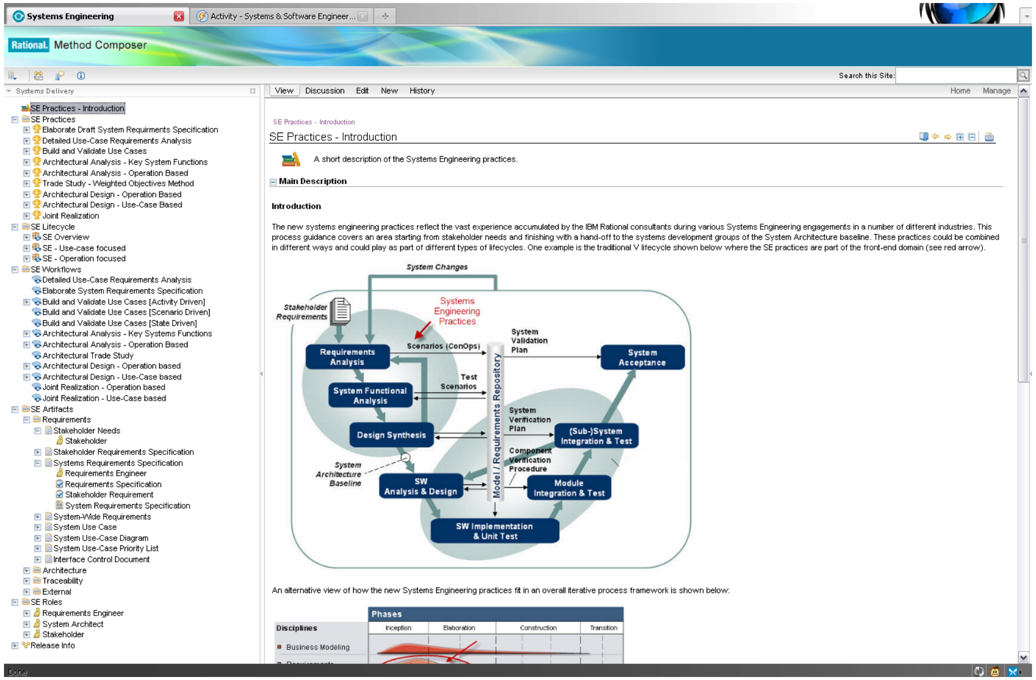
Weak process and checklist management

PSAC – Plan for Software Artifacts of Certification
SDP – Software Development Plan
SVP – Software Verification Plan
SCMP – Software Configuration Management Plan
SQAP – Software Quality Assurance Plan

Process Management and Enactment:
Leverage Compliance & Standards

- **Pre-defined methods and mappings** to industry standards and regulations compliance
- **Unify process management and enactment** with integrated process, methods and tools
  Increase productivity and turn “know-how” into competitive advantage

- **Improve quality and predictability** by leveraging proven practices and patterns of success
- Quickly and easily **compose** right-sized project/team processes and **deploy process, methods and tools to project**
- Surface process guidance in-context directly within practitioner tools to **speed on-boarding, process adoption**



- SE Practices - Introduction
- SE Practices
  - Elaborate Draft System Requirments Specification
  - Detailed Use-Case Requirements Analysis
  - Build and Validate Use Cases
  - Architectural Analysis - Key System Functions
  - Architectural Analysis - Operation Based
  - Trade Study - Weighted Objectives Method
  - Architectural Design - Operation Based
  - Architectural Design - Use-Case Based
  - Joint Realization
- SE Lifecycle
  - SE Overview
  - SE - Use-case focused
  - SE - Operation focused
- SE Workflows
  - Detailed Use-Case Requirements Analysis
  - Elaborate System Requirements Specification
  - Build and Validate Use Cases [Activity Driven]
  - Build and Validate Use Cases [Scenario Driven]
  - Build and Validate Use Cases [State Driven]
  - Architectural Analysis - Key Systems Functions
  - Architectural Analysis - Operation Based
  - Architectural Trade Study
  - Architectural Design - Operation based
  - Architectural Design - Use-Case based
  - Joint Realization - Operation based
  - Joint Realization - Use-Case based
- SE Artifacts
  - Requirements
    - Stakeholder Needs
      - Stakeholder
    - Stakeholder Requirements Specification
    - Systems Requirements Specification
      - Requirements Engineer
      - Requirements Specification
      - Stakeholder Requirement
      - System Requirements Specification
    - System-Wide Requirements
    - System Use Case
    - System Use-Case Diagram
    - System Use-Case Priority List
    - Interface Control Document
  - Architecture
  - Traceability
  - External
- SE Roles
  - Requirements Engineer
  - System Architect
  - Stakeholder
- Release Info

SE Practices - Introduction

SE Practices - Introduction

A short description of the Systems Engineering practices.

Main Description

Introduction

The new systems engineering practices reflect the vast experience accumulated by the IBM Rational consultants during various Systems Engineering engagements in a number of different industries. This process guidance covers an area starting from stakeholder needs and finishing with a hand-off to the systems development groups of the System Architecture baseline. These practices could be combined in different ways and could play as part of different types of lifecycles. One example is the traditional V lifecycle shown below where the SE practices are part of the front-end domain (see red arrow).

System Changes
Stakeholder Requirements
Systems Engineering Practices
Scenarios (ConOps)
System Validation Plan
Requirements Analysis
System Acceptance
Test Scenarios
System Functional Analysis
Model / Requirements Repository
System Verification Plan
Design Synthesis
(Sub-)System Integration & Test
Component Verification Procedure
System Architecture Baseline
SW Analysis & Design
Module Integration & Test
SW Implementation & Unit Test

An alternative view of how the new Systems Engineering practices fit in an overall iterative process framework is shown below:

Agenda

- Introduzione
- Normative
- **Normative come base per il processo di progettazione: IBM Rational**

Turn Compliance & Standards into your competitive advantage

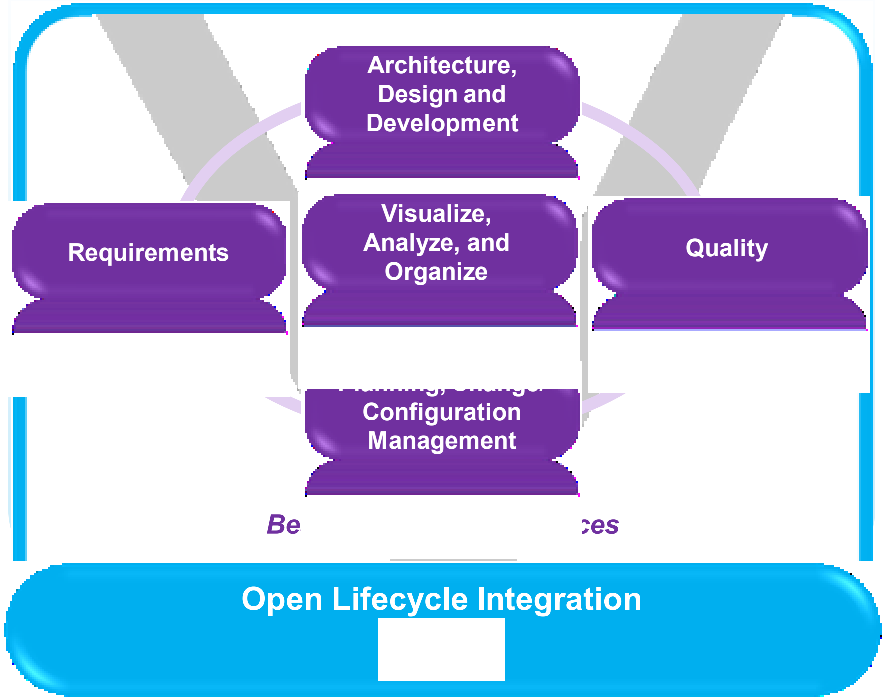
Lead innovation

Manage complexity

IBM Rational Solution for Systems and Software Engineering

Systems Engineering

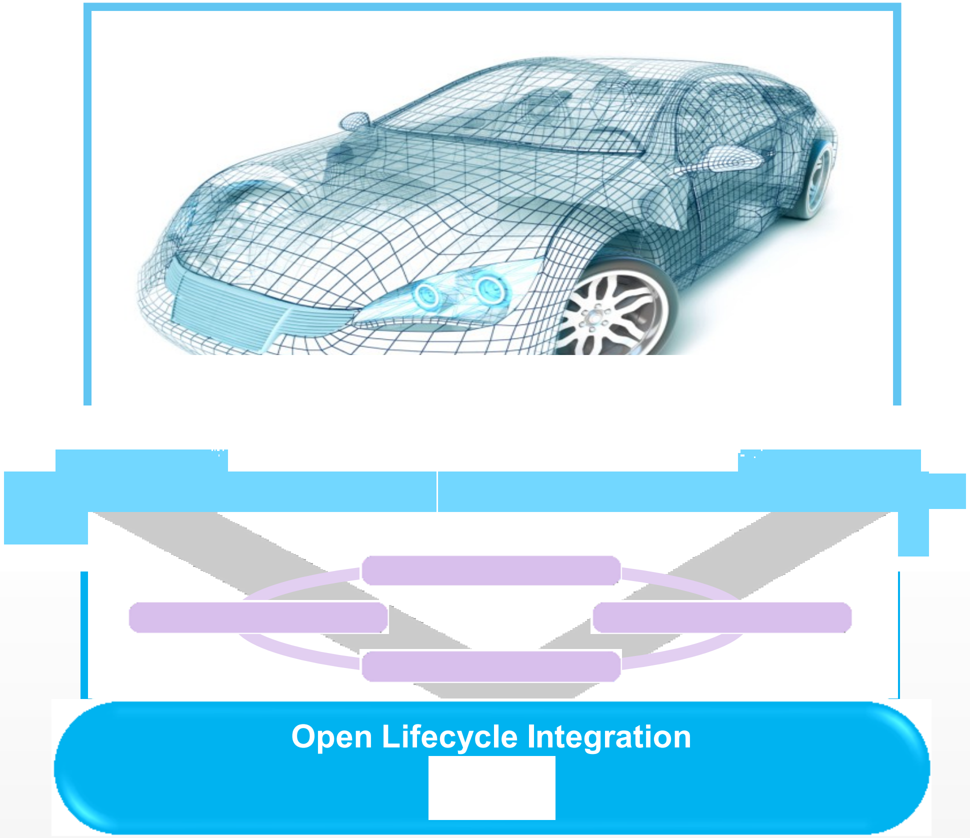
Embedded Software Engineering


Architecture, Design and Development
Requirements
Visualize, Analyze, and Organize
Quality
Configuration Management
Be
ces
Open Lifecycle Integration

Specify, design, implement and validate complex products and the software that powers them with an integrated set of tools, practices, and services.

IBM Rational Automotive industry solutions: functional safety ISO-26262 AUTOSAR

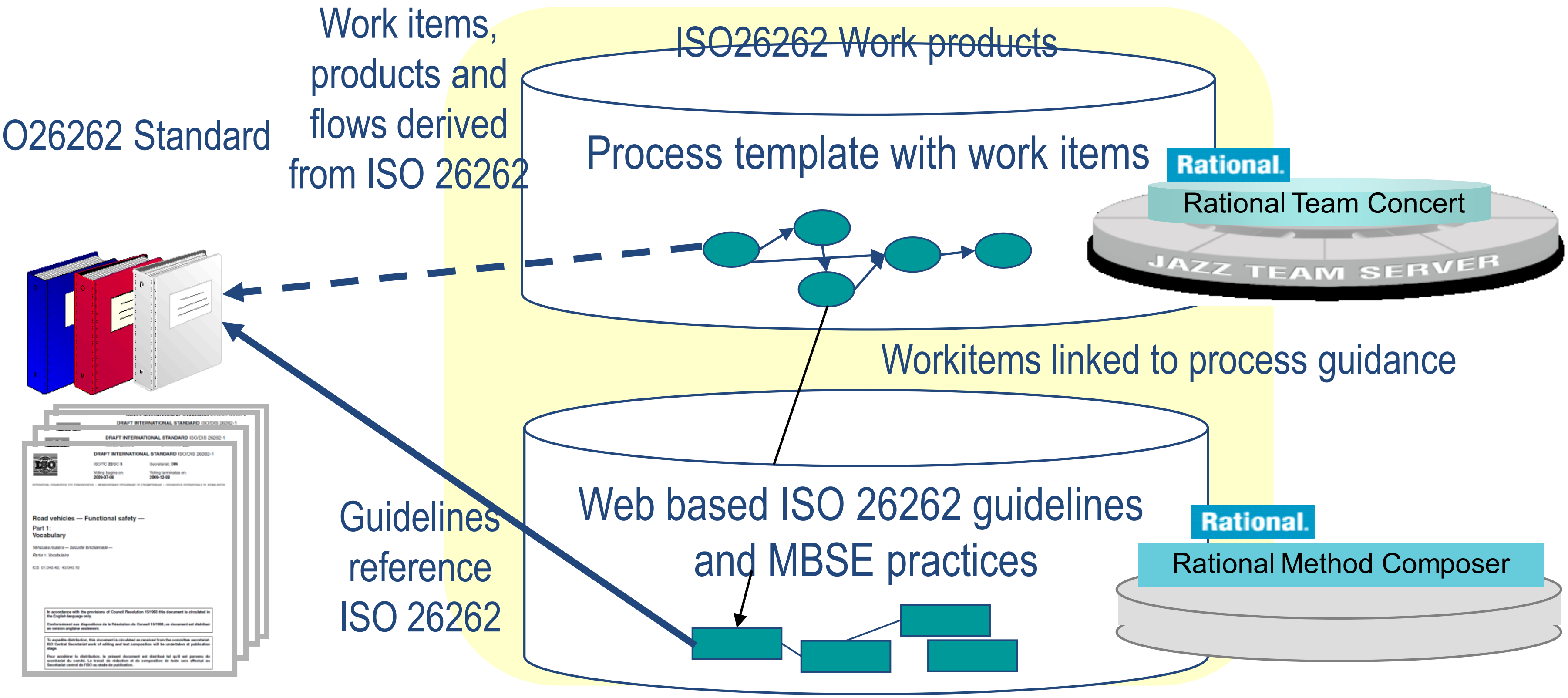
- Updated ISO26262 best practices, aligned with the released version of ISO26262.
- Expanded ISO26262 practice content covering testing/validation and real-time dynamic analysis support with IBM Business Partner INCHRON
- Updated Rational Team Concert 4.0 process and worl item templates for ISO-26262 to allow designers, QA groups to properly manage the project
- Out of the box tool templates for DOORS and Rhapsody to ease customer adoption of solution.
- Out of the box custom ISO-26626 view in RELM
- Process customization guide to help end users adopt our industry practices within their environment.



- Rhapsody Kit for ISO 26262 and IEC 61508 including “TUV fit for purpose certificate” to meet ISO-26262 tool qualification criteria
- Rhapsody AUTOSAR framework

ISO 26262 RTC and RMC

- 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



ISO26262 Standard

Work items, products and flows derived from ISO 26262

ISO26262 Work products

Process template with work items

Rational Team Concert

Workitems linked to process guidance

Web based ISO 26262 guidelines and MBSE practices

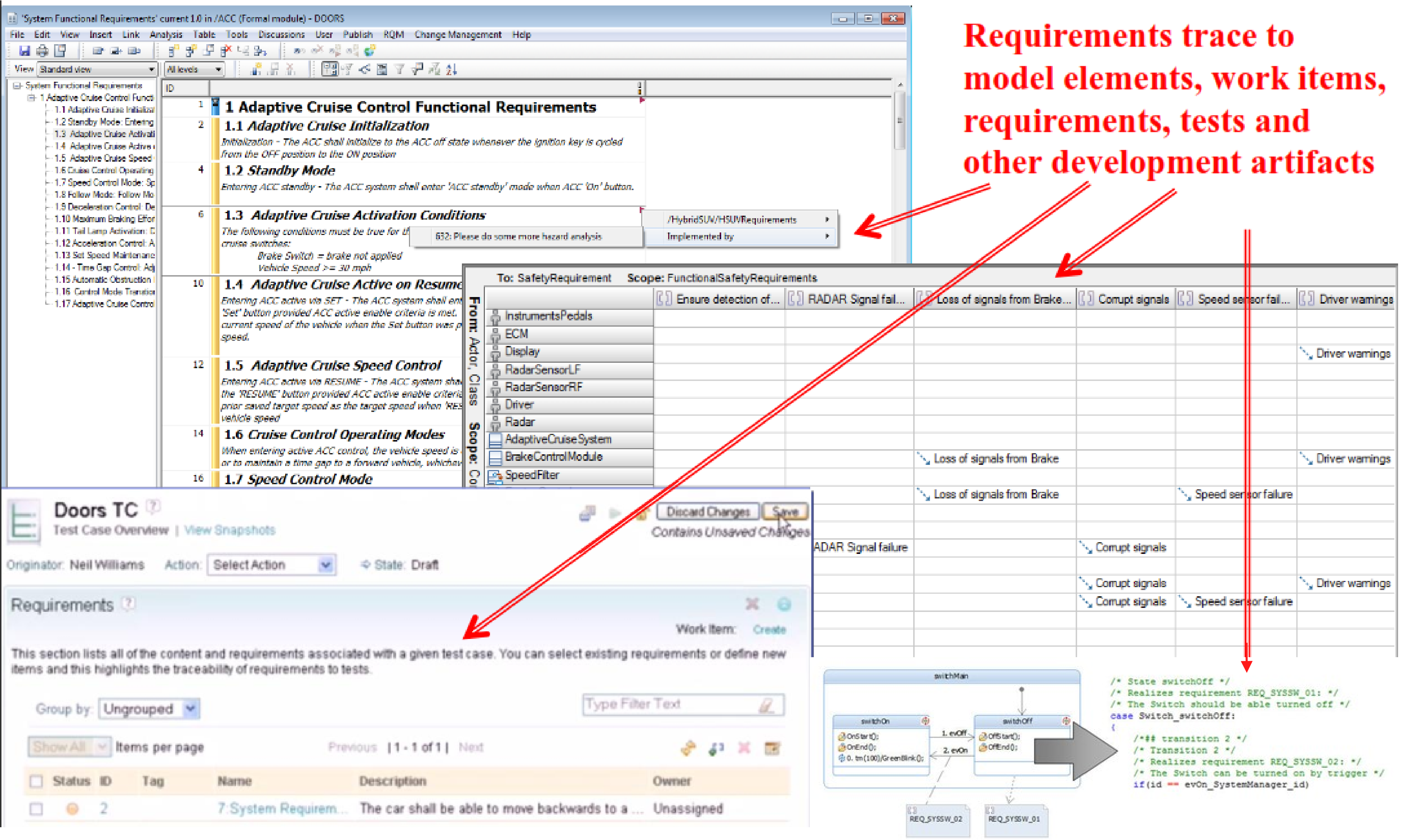
Guidelines reference ISO 26262

Rational Method Composer

Rational.
JAZZ TEAM SERVER
Rational.
DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-1
Road vehicles — Functional safety —
Part 1:
Vocabulary

Meeting objectives outlined in standards: Traceability

Requirements trace to model elements, work items, requirements, tests and other development artifacts



'System Functional Requirements' current 1.0 in /ACC (Formal module) - DOORS
File Edit View Insert Link Analysis Table Tools Discussions User Publish RQM Change Management Help
View Standard view
All levels
System Functional Requirements
1 Adaptive Cruise Control Funct
1.1 Adaptive Cruise Initializat
1.2 Standby Mode: Entering
1.3 Adaptive Cruise Activati
1.4 Adaptive Cruise Active
1.5 Adaptive Cruise Speed
1.6 Cruise Control Operating
1.7 Speed Control Mode: Sp
1.8 Follow Mode: Follow Mo
1.9 Deceleration Control: De
1.10 Maximum Braking Effor
1.11 Tail Lamp Activation: D
1.12 Acceleration Control: A
1.13 Set Speed Maintenanc
1.14 - Time Gap Control: Adj
1.15 Automatic Obstruction
1.16 Control Mode Transitio
1.17 Adaptive Cruise Contro
ID

1 **1 Adaptive Cruise Control Functional Requirements**

2 ***1.1 Adaptive Cruise Initialization***

Initialization - The ACC shall initialize to the ACC off state whenever the ignition key is cycled from the OFF position to the ON position

4 ***1.2 Standby Mode***

Entering ACC standby - The ACC system shall enter 'ACC standby' mode when ACC 'On' button.

6 ***1.3 Adaptive Cruise Activation Conditions***

The following conditions must be true for th
cruise switches:
Brake Switch = brake not applied
Vehicle Speed >= 30 mph

632: Please do some more hazard analysis

/HybridSUV/HSUVRequirements ▸
Implemented by ▸

10 ***1.4 Adaptive Cruise Active on Resume***

Entering ACC active via SET - The ACC system shall ent
'Set' button provided ACC active enable criteria is met.
current speed of the vehicle when the Set button was p
speed.

12 ***1.5 Adaptive Cruise Speed Control***

Entering ACC active via RESUME - The ACC system sha
the 'RESUME' button provided ACC active enable criteria
prior saved target speed as the target speed when 'RES
vehicle speed

14 ***1.6 Cruise Control Operating Modes***

When entering active ACC control, the vehicle speed is
or to maintain a time gap to a forward vehicle, whichev

16 ***1.7 Speed Control Mode***

To: SafetyRequirement **Scope:** FunctionalSafetyRequirements

From: Actor, Class **Scope:** Co

	Ensure detection of...	RADAR Signal fail...	Loss of signals from Brake...	Corrupt signals	Speed sensor fail...	Driver warnings
InstrumentsPedals						
ECM						
Display						Driver warnings
RadarSensorLF						
RadarSensorRF						
Driver						
Radar						
AdaptiveCruiseSystem						
BrakeControlModule			Loss of signals from Brake			Driver warnings
SpeedFilter						
			Loss of signals from Brake		Speed sensor failure	
		ADAR Signal failure		Corrupt signals		
				Corrupt signals		Driver warnings
				Corrupt signals	Speed sensor failure	

Doors TC

Contains Unsaved Changes

Originator: Neil Williams   Action: Select Action   State: Draft

Requirements

This section lists all of the content and requirements associated with a given test case. You can select existing requirements or define new items and this highlights the traceability of requirements to tests.

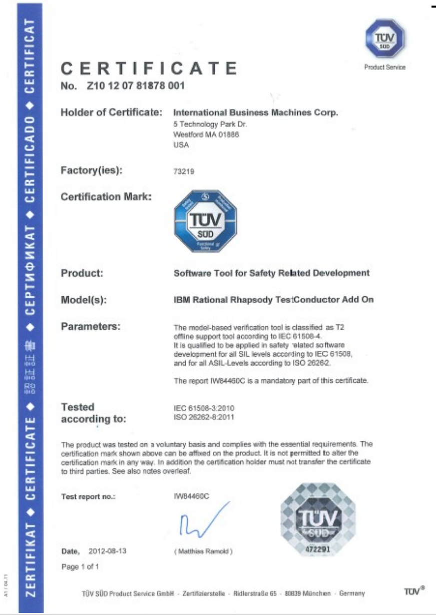
Group by: Ungrouped

☐	Status	ID	Tag	Name	Description	Owner
☐	●	2		7:System Requirem...	The car shall be able to move backwards to a ...	Unassigned

```
/* State switchOff */
/* Realizes requirement REQ_SYSSW_01: */
/* The Switch should be able turned off */
case Switch_switchOff:
{
    /*## transition 2 */
    /* Transition 2 */
    /* Realizes requirement REQ_SYSSW_02: */
    /* The Switch can be turned on by trigger */
    if(id == evOn_SystemManager_id)
```

Rhapsody Kit for ISO 26262 and IEC 61508

- 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
- Certification kits for the SXF (C++) and SMXF (C) frameworks



ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE
No. Z10 12 07 81878 001

Holder of Certificate: International Business Machines Corp.
5 Technology Park Dr.
Westford MA 01886
USA

Factory(ies): 73219

Certification Mark:

Product: Software Tool for Safety Related Development

Model(s): IBM Rational Rhapsody TestConductor Add On

Parameters: The model-based verification tool is classified as T2 offline support tool according to IEC 61508-4. It is qualified to be applied in safety related software development for all SIL levels according to IEC 61508, and for all ASIL-Levels according to ISO 26262.

The report IW84460C is a mandatory part of this certificate.

Tested according to: IEC 61508-3:2010
ISO 26262-8:2011

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.

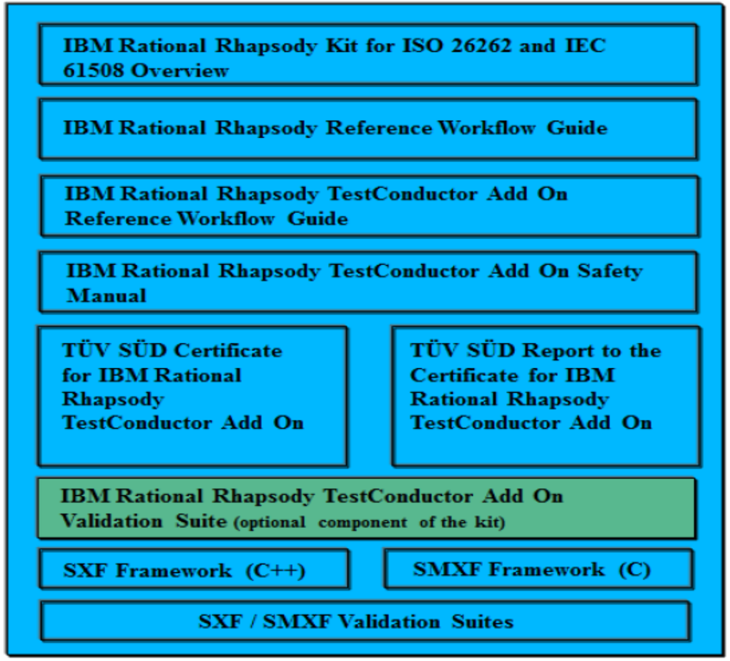
Test report no.: IW84460C

Date, 2012-08-13 (Matthias Ramold)

472291

Page 1 of 1

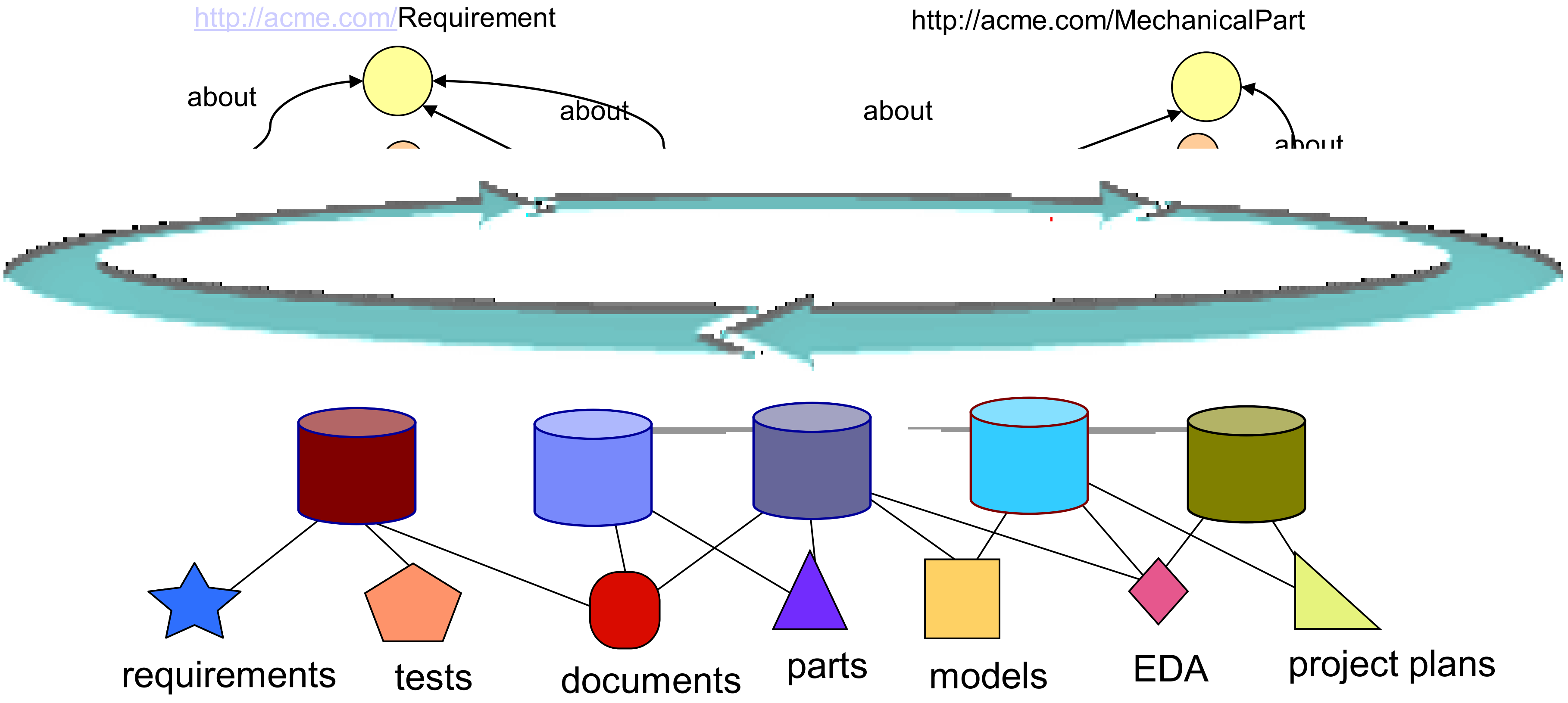
TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80839 München · Germany



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

Leverage the Linked Data concepts of Web Technology

The Web has proven to be the most **scalable**, **open**, and **flexible** integration technology

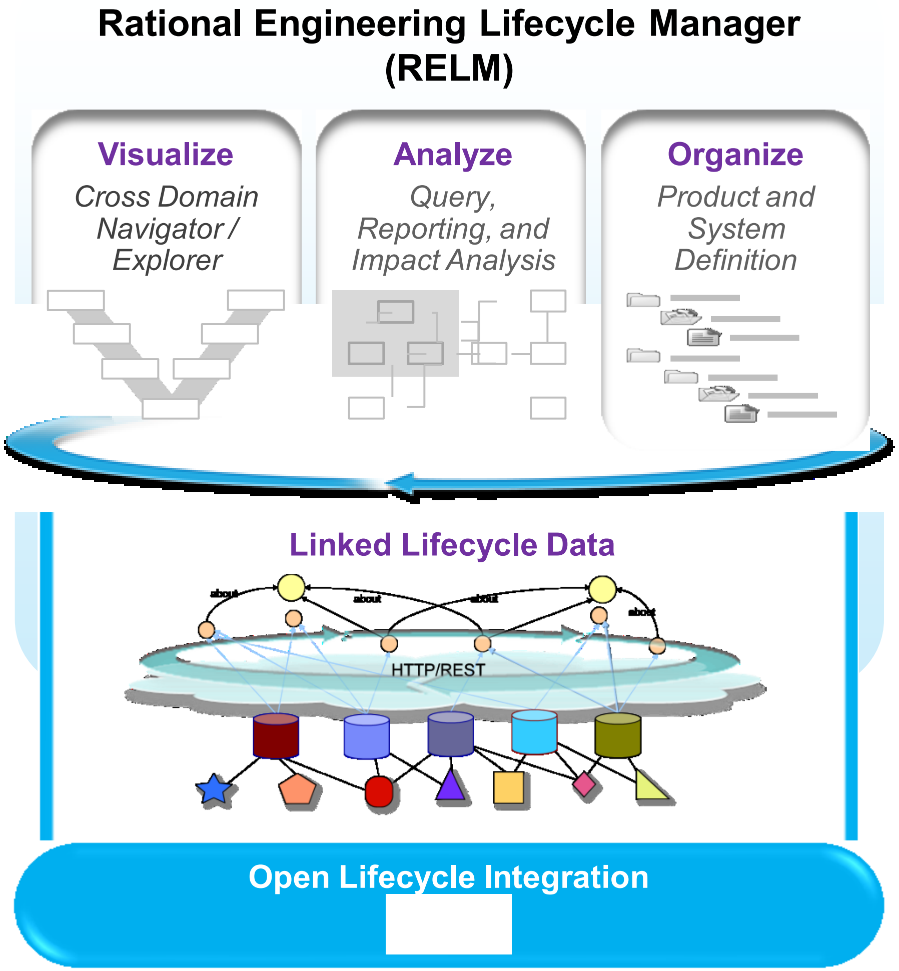


Rational Engineering Lifecycle Manager

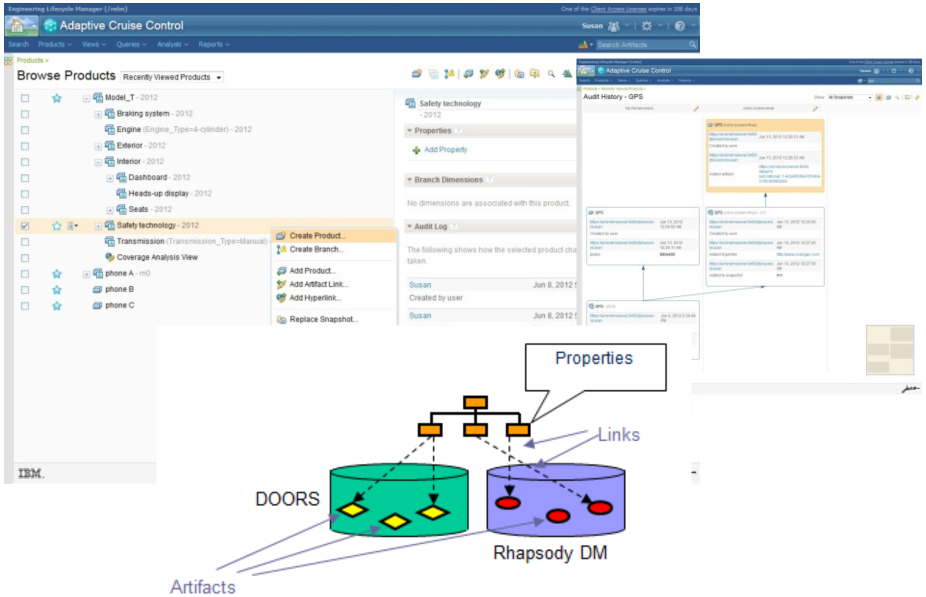
Extending the Rational solution for systems and software engineering

- Uses a Linked Data approach that enables
  - ✓ ***Visibility*** – across many sources of data
  - ✓ ***Organization*** – information in context
  - ✓ **Analysis** - answer questions using that contextualized information

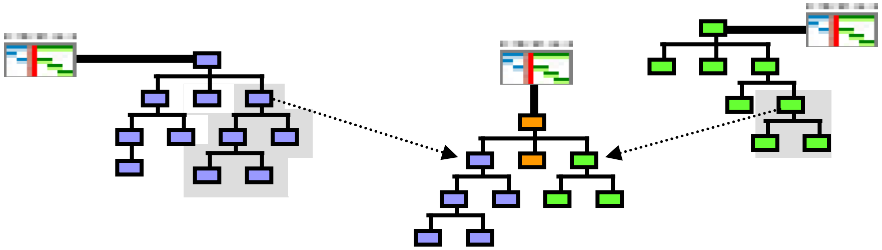
- Allows stakeholders to:
  - manage growing complexity
  - derive knowledge from the available data
  - make timely and correct engineering and business decisions


Rational Engineering Lifecycle Manager (RELM)
Visualize
Cross Domain Navigator / Explorer
Analyze
Query, Reporting, and Impact Analysis
Organize
Product and System Definition
Linked Lifecycle Data
about
about
about
about
HTTP/REST
Open Lifecycle Integration

RELM: Organize and Structure Engineering Data



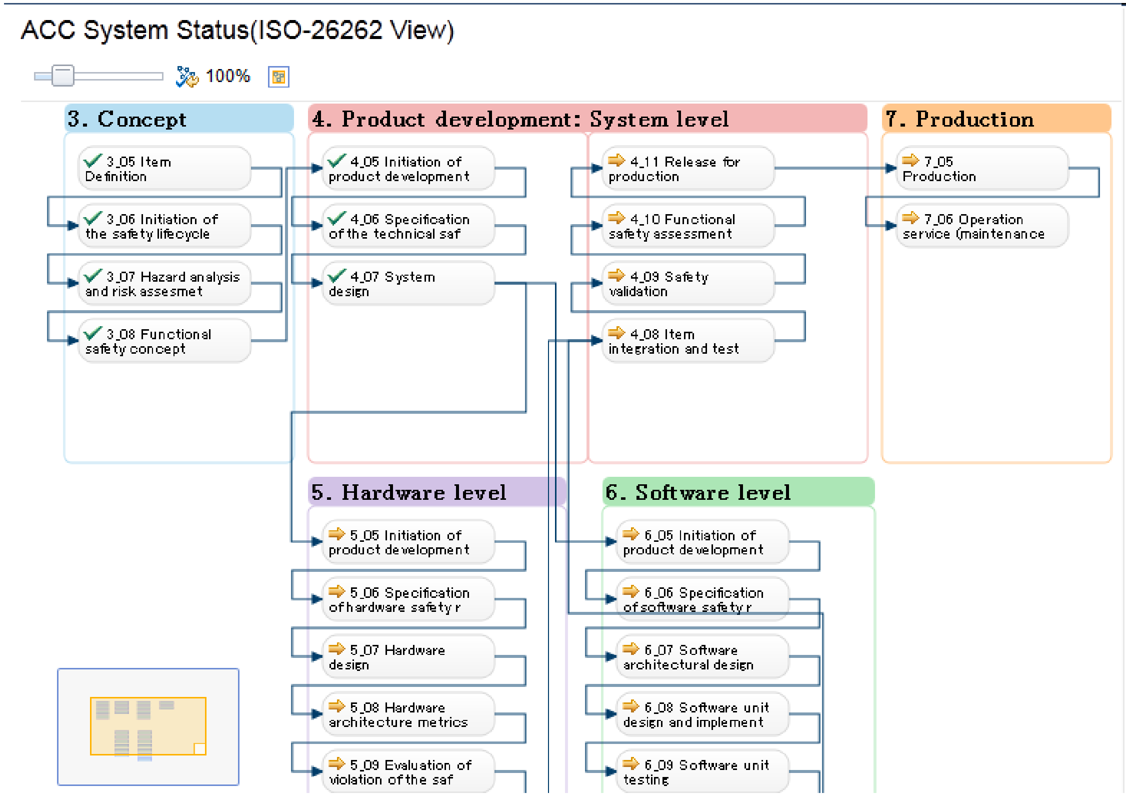
- **Allocate** development lifecycle resources to **definitions of products,** systems, sub-systems, capabilities and components
- Define and compare **versions and variants of products**, systems, sub-systems, capabilities and components
- Specify **re-use of artifacts** across products, systems, sub-systems, capabilities and components
- Provides a context for visualization and analysis (e.g. queries, reports, impact and coverage analysis)



A shared facility to define hierarchies of products, systems, sub-systems, capabilities and components that reflect these dimensions in the underlying engineering artifacts

RELM: Views on ISO 26262 information

- RELM views are a specialized way of viewing information pertaining to the stakeholder
- This RELM example shows the project completion view of an ISO 26262 project, it addresses the concerns of the Project Manager and the Safety Manager.
- RELM supports creating new views or customize predefined views


ACC System Status(ISO-26262 View)
100%
3. Concept
✓ 3_05 Item Definition
✓ 3_06 Initiation of the safety lifecycle
✓ 3_07 Hazard analysis and risk assesmet
✓ 3_08 Functional safety concept
4. Product development: System level
✓ 4_05 Initiation of product development
✓ 4_06 Specification of the technical saf
✓ 4_07 System design
4_11 Release for production
4_10 Functional safety assessment
4_09 Safety validation
4_08 Item integration and test
7. Production
7_05 Production
7_06 Operation service (maintenance
5. Hardware level
5_05 Initiation of product development
5_06 Specification of hardware safety r
5_07 Hardware design
5_08 Hardware architecture metrics
5_09 Evaluation of violation of the saf
6. Software level
6_05 Initiation of product development
6_06 Specification of software safety r
6_07 Software architectural design
6_08 Software unit design and implement
6_09 Software unit testing

ISO-26262 Project completion view in RELM

Example User Story

"So that I can more easily achieve, maintain and monitor compliance to ISO26262, as a Safety Manager I need a view that shows me the different process tasks, their status and related tasks"

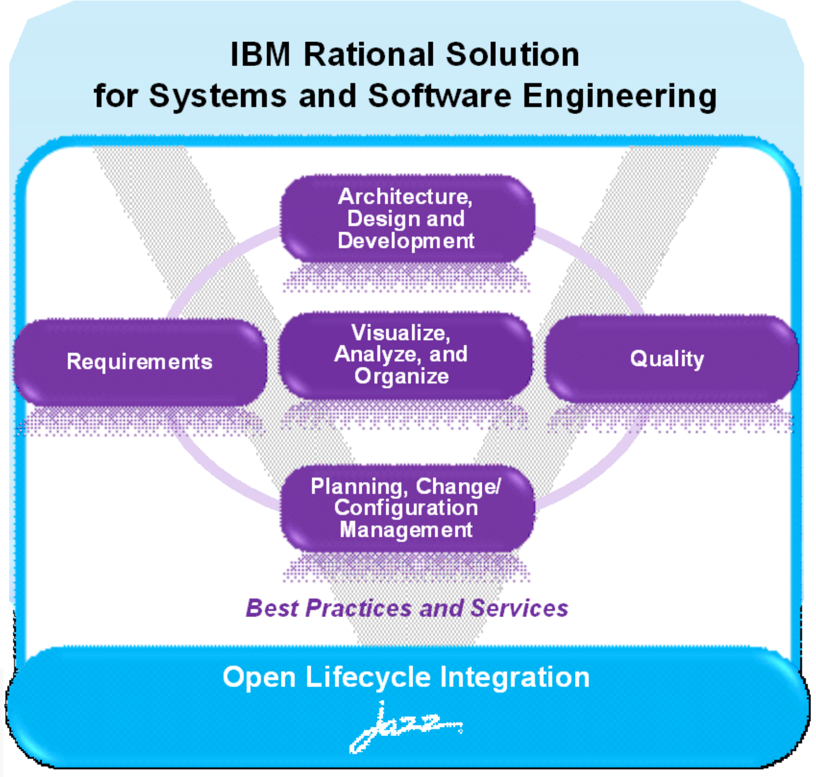
IBM Rational solution for systems and software engineering

Lifecycle

Specify, design, implement and validate complex products and the software that powers them with an integrated systems lifecycle management solution

Achieve greater value from lifecycle traceability with guidance on new ways to view and query linked data.

- **Improve cross lifecycle reporting** with new tool mentors and templates for document generation.
- **Make informed decisions on emerging issues** with new lifecycle metrics.
- **Apply requirements driven quality management** with greater efficiency using new tool mentors.
- **Adopt an easier route towards compliance** with enhanced support for functional safety standards


IBM Rational Solution
for Systems and Software Engineering
Architecture, Design and Development
Requirements
Visualize, Analyze, and Organize
Quality
Planning, Change/ Configuration Management
Best Practices and Services
Open Lifecycle Integration
Jazz

THE FOUNDATION

- IBM Solution for Systems and Software Engineering
  - IBM Rational Method Composer
  - Engineering Lifecycle Manager
  - IBM Rational DOORS
  - IBM Rational Quality Manager
  - IBM Rational Team Concert
  - IBM Rational Rhapsody v8.0 with Design Manager v4.0

“Our ability to maximize the breadth of the IBM software let us provide NASA with demand-based statistics while maintaining control of the costs.”

- Joseph Dress, Requirements Management, Constellation Software Engineering, Corporation

IBM Rational Solution for systems and software engineering

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, Rational, the Rational logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.