Safety inside! ensured with technology

Ryan D Brooks
(The Boeing Company)

Jyothi G Shivashankar
(Robert Bosch Engineering and Business Solutions)

Eclipsecon 2014 20 Mar 2014 13:30 – 14:05 Room: Grand Peninsula B
Agenda

1. Safety Standards

2. Application Life Cycle Management system
   - Key OSEE Features
   - Traceability reports
   - Variant management
   - Impact Analysis
   - Partner integration

3. The Safety Cycle
   - DO-178B conformance report
   - ISO26262
   - PLM – ALM integration
Safety Standards for Safety Critical systems

Stringent standards require evidence of the quality of:

- Developed Artifacts
- Development Processes
Key OSEE Features for Safety Critical Systems

• System Safety Analysis
• Code Coverage
• End-to-end traceability
• Variant management
• Integrated workflows and processes
• Deliverable document generation
Safety and Assessing Criticality

Hazard Analysis
- Different types of hazards
- Potential failure scenarios

Design Assurance Level
- Determined based on the effects of a failure:
  - Catastrophic
  - Hazardous
  - Major
  - Minor
  - No Effect
- The DAL drives the appropriate level of rigor required

Certification at the most rigorous level is costly
Code Coverage

Test Environment coordinates with mission software to capture raw coverage data

Raw coverage data is imported and merged into OSEE Database

ATS used to disposition coverage methods

ATS provides tracking of code, test, and requirement changes needed to resolve missing coverage

Auto generation of coverage reports for delivery to customer

Currently, OSEE supports statement level coverage which is needed for certifying Level C software
Variants and Exponential Complexity

As the number of variants increases, complexity grows exponentially

Why?
- Managing commonality v.s. specialization
- Team size increases (communication, etc.)
- Task switching with engineers working on multiple variants

OSEE eases the cost of managing this complexity
Integrated processes and workflows in OSEE allow engineers to focus more on engineering and less on process training and manual metrics reporting.

- Work Definitions model the team's workflow and actively guide them through the work to be completed.
- Work Definitions are user-defined and consist of state machines with their own widgets, rules, and routing.
- Each state can be assigned, statused, and transitioned.
Safety Standards for Safety Critical systems

- **IEC 61508 Safety life cycle**
- **RTCA/DO-254**
- **DO-178B**
- **ISO 26262**

Functional Safety standard, titled "Road vehicles – Functional safety". Functional safety features form an integral part of each product development phase, ranging from the specification > design > implementation > integration > verification > validation > production release.
Safety Inside! ensured with technology

ALM – Application Life Cycle Management
An integrated solution that provides seamless workflow from requirements to release

- Requirements Management
- Design
- Model Based Development
- Traceability reports
- Impact Analysis
- Automotive Standards Editors
- Continuous Integration
- Variant Management
- Test Mgmt
- Partner Integration
- Software Sharing Support
- Project Mgmt
- Calibration Workflow
- Calibration Data Manager
- Document Mgmt
- Project Management
- iCTeam
- Impact Analysis
- Automotive Standards Editors
- Build Mgmt

RBEI | 15/01/2014 | © Robert Bosch Engineering and Business Solutions Limited 2013. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
Safety Inside! ensured with technology

Traceability reports – Horizontal & Vertical

Horizontal Traceability report

<table>
<thead>
<tr>
<th>Requirement</th>
<th>WiperControl_3x_branch</th>
<th>WiperControl_100us</th>
<th>WiperControl_3x_workspace</th>
<th>AUTOSAR BSW ICC3</th>
<th>CAN Communication Stack shall be used</th>
<th>AUTOSAR BSW ICC3</th>
<th>Timing_Demo</th>
<th>ECU_Instance</th>
<th>ECU_Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiperControl_3x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiperControl_100us</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Types &amp; Interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiperControl_3x_workspace</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiperControl_100us</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vertical Traceability report

<table>
<thead>
<tr>
<th>Requirement Tag</th>
<th>Simulink Model Tag</th>
<th>Autosar Reference</th>
<th>Code Reference</th>
<th>System Test Specification Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiperControl_100us</td>
<td>Wiper_Control_Design</td>
<td>WiperControl_100us.asmml</td>
<td>WiperControl_100us.c</td>
<td>WiperControl_100us_Test</td>
</tr>
<tr>
<td>Functions</td>
<td>Wiper_Control_Design</td>
<td>WiperControl_100us.asmml</td>
<td>WiperControl_100us.c</td>
<td>WiperControl_100us_Test</td>
</tr>
<tr>
<td>WiperControl_100us Functions</td>
<td>Wiper_Control_Design</td>
<td>WiperControl_100us.asmml</td>
<td>WiperControl_100us.c</td>
<td>WiperControl_100us_Test</td>
</tr>
<tr>
<td>Events</td>
<td>Wiper_Control_Design</td>
<td>WiperControl_3ms.asmml</td>
<td>WiperControl_3ms.c</td>
<td>WiperControl_3ms_Test</td>
</tr>
<tr>
<td>Timing Event</td>
<td>Wiper_Control_Design</td>
<td>WiperControl_3ms.asmml</td>
<td>Timing_Test</td>
<td>Timing_Test</td>
</tr>
<tr>
<td>Types &amp; Interfaces</td>
<td>Wiper_Control_Design</td>
<td>COMSTACK_CFG.asmml</td>
<td>CanCom.c</td>
<td>COMSTACK_CFG_Test</td>
</tr>
<tr>
<td>BSW</td>
<td>Wiper_Control_Design</td>
<td>WiperControl_3ms.asmml</td>
<td>bow.c</td>
<td>BSW_Test</td>
</tr>
<tr>
<td>AUTOSAR BSW ICC3</td>
<td>Wiper_Control_Design</td>
<td>WiperControl_3ms.asmml</td>
<td>CanCom.c</td>
<td>AUTOSAR BSW ICC3_Test</td>
</tr>
<tr>
<td>CAN Communication Stack</td>
<td>Wiper_Control_Design</td>
<td>COMSTACK_CFG.asmml</td>
<td>CanCom.c</td>
<td>CAN_Test</td>
</tr>
<tr>
<td>CAN Communication Stack</td>
<td>Wiper_Control_Design</td>
<td>COMSTACK_CFG.asmml</td>
<td>CanCom.c</td>
<td>Hardware_Test</td>
</tr>
</tbody>
</table>

Count: 4
Safety Inside! ensured with technology

Impact Analysis – Graphical viewer

This graph indicates "dependency conflicts" that arises due to the change.

This color indicate Important information like "team to contact" to solve The issue.

Different project are Indicated as layers in the graph.
Safety Inside! ensured with technology

Impact Analysis – Matrix report
Impact Analysis – Architecture

UI
- DSM Matrix Visualization (SWT)
- Graphs (JUNG)

Source Project

ECLIPSE CDT

Dependency Detail Model

Model
- C / C++ wrapper model

Eclipse Platform
Safety Inside! ensured with technology

Product Line Engineering - Architecture

- **Feature Model**
  - Features, Constraints
- **Variant Model**
  - Feature Selections, Variant Values
- **Evaluation Model**
  - Concrete Feature Model
- **Verification Model**
  - Verified Variants

**Problem Space**
- Product
-REQ
- Feature
- DSG
- SCM
- Build
- Code gen
- Code
- Runtime
- Var/selection/func
- selection
- Runtime selection
- Application data
  selection

**Engineering Solution Space**

**Application Space**

**OSEE Application Framework**

- System Constant Editor
- Feature constraint Editor
- Feature Validator
- Extended Feature Model editor
- Variant Release Manager

**EMF Feature Model**

**PLE Branch Manager**

**Define PL**

**0...x Variants**

**Evaluate, verify**

**Bosch**
Safety Inside! ensured with technology

Integrating the development partners

**Requirements**
- Define
- Review

**Software Sharing**
- Models
- Object code

**Integration & Shared Build**
- Build tools of Suppliers
- Object Code

**Common Workflow and Tool chain** used by both OEM and Suppliers for joint development

**Version Management**
- Object codes
- Datasets

**Acceptance Test**
- Test Cases
- Results

**Calibration Workflow**
- Work Packages
- Datasets versioning
- Tracking
Safety Inside! ensured with technology

- **Requirements**
  - Hardware Req
  - Software Req

- **Design**
  - Hardware design
  - Software design

- **Validation**
  - Hardware simulation
  - Software unit test
  - Safety Req

- **Production**
  - Hardware test plan
  - Software test plan
  - Traceability

- **System Engineering**
  - Hazard Identification
  - Safety Goals
  - Safety Concept

- **ALM-PLM Integration**
  - ALM-PLM Integration

- **ISO 26262**
  - Reports

- **Safety Requirements to HW and SW requirements**
Thank You

Demo
Evaluate This Session

1. Sign-in: [www.eclipsecon.org](http://www.eclipsecon.org)

2. Select session from schedule

3. Evaluate:  +1  0  -1