Model-Based Design for High Integrity Software and Hardware
Agenda

- Relevant standards

- DO workflow – Common Elements

- DO-178B - Software Considerations and Workflows

- DO-254 – Hardware Considerations and Workflows

- Additional Topics
Standards Background

System Development Processes (ARP 4754)

Software Life Cycle Process (DO-178B)

Hardware Design Life Cycle Process (DO-254)
Benefits of Model-Based Design

- Use models to validate and verify requirements and designs early in the process
- Re-use tests throughout design cycle
- Automatically generate design and verification artifacts
- Streamline process by qualifying verification tools
Agenda

- Relevant standards

- DO workflow – Common Elements

- DO-178B - Software Considerations and Workflows

- DO-254 – Hardware Considerations and Workflows

- Additional Topics
DO Workflow Example

- Requirements
- Model
- Conformance
- Validate
- Trace
- Verify

DO-178B DO-254
DO Workflow Example

Trace
Simulink Verification and Validation: Requirements Management Interface

Validate

Requirements

Simulink & Stateflow

Model

* DO Qualifiable Tool
Requirements linking and traceability

- Bi-directional linking with requirements
  - For Simulink and Stateflow
  - Requirements consistency checks
  - Extensibility API
  - Report generation

- Links to Documents and Requirements Management Packages.

IBM DOORS
ReqTracer
Microsoft Word
Microsoft Excel
PDF
HTML
DO Workflow

- **Trace**
  - Requirements
  - Simulink & Stateflow
  - Model

- **Validate**
  - Conformance Model Advisor

* DO Qualifiable Tool
Simulink Model Advisor

- Model Advisor is used to:
  - Enforce model standards and best practices
  - Detect modeling and code generation issues
  - Pre-defined sets of checks for DO-178B and MAAB Style Guides
  - Automated report generation
DO Workflow Example

- Trace
- Validate
- Requirements
- Model
- Conformance

Verify
SystemTest*
Simulink Design Verifier:
Property Proving
Model Coverage

* DO Qualifiable Tool
SystemTest

- Manage tests and analyze results for system verification and validation

Simulink System Model

Setup Test and Variables

Run Simulations

Analyze Results
Simulink Design Verifier
Property Proving & Test Generation

- **Property Proving**
  - Functional testing
  - Property proving
  - Generates an example of a violation
  - Produces detailed analysis reports

- **Test Generation**
  - Automatically generates test vectors for model coverage
  - Detects unreachable states
  - Saves test vectors and generates report

- Uses formal methods, not simulation
DO Workflow Example

**Trace**
Simulink Verification and Validation: Requirements Management Interface

**Validate**
Simulink & Stateflow

**Conformance**
Model Advisor*

**Verify**
SystemTest*
Simulink Design Verifier: Property Proving Model Coverage

* DO Qualifiable Tool
Agenda

- Relevant standards
- DO workflow – Common Elements
- **DO-178B - Software Considerations and Workflows**
- DO-254 – Hardware Considerations and Workflows
- Additional Topics
DO-178B Workflow Example

- **Requirements**
  - Validate
  - Trace
  - Conformance

- **Model**
  - Conformance
  - Trace
  - Verify

- **Source Code**
  - Trace
  - Conformance
  - Verify

- **Object Code**
  - Verify
DO-178B Workflow Example

**Requirements** → **Model** → **Source Code**

- **Validate**
- **Trace**
  - Model/Code Trace Report
  - Real-Time Workshop® Embedded Coder™
- **Conformance**
- **Verify**
Real-Time Workshop® Embedded Coder

- Automatically generates C code from Simulink® and Stateflow® models
- Code is ANSI/ISO-C compliant
Model-to-Code and Code-to-Model Traceability

Simulink Verification and Validation

Real-Time Workshop
Embedded Coder

Traceability Report

Eliminated / Virtual Blocks

<table>
<thead>
<tr>
<th>Block Name</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Root&gt;/Build ERT</td>
<td>Empty SubSystem</td>
</tr>
<tr>
<td>&lt;Root&gt;/Mux</td>
<td>Mux</td>
</tr>
<tr>
<td>&lt;Root&gt;/Scope</td>
<td>Eliminated unused block</td>
</tr>
<tr>
<td>&lt;Root&gt;/View RTW</td>
<td>Empty SubSystem</td>
</tr>
</tbody>
</table>

Traceable Blocks

<table>
<thead>
<tr>
<th>Block Name</th>
<th>Code Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Root&gt;/INC2</td>
<td>rtwdemo_hyperlinks.c:36</td>
</tr>
<tr>
<td>&lt;Root&gt;/INC3</td>
<td>rtwdemo_hyperlinks.c:37</td>
</tr>
<tr>
<td>&lt;Root&gt;/LIMIT</td>
<td>rtwdemo_hyperlinks.c:44</td>
</tr>
<tr>
<td>&lt;Root&gt;/RESET</td>
<td>rtwdemo_hyperlinks.c:54</td>
</tr>
<tr>
<td>&lt;Root&gt;/RelOpt</td>
<td>rtwdemo_hyperlinks.c:43</td>
</tr>
<tr>
<td>&lt;Root&gt;/Sum</td>
<td>rtwdemo_hyperlinks.c:35</td>
</tr>
<tr>
<td>&lt;Root&gt;/Switch</td>
<td>rtwdemo_hyperlinks.c:55</td>
</tr>
</tbody>
</table>
DO-178B Workflow Example

- **Validate**
  - Requirements

- **Trace**
  - Model
  - Source Code

- **Conformance** PolySpace*

- **Verify**
PolySpace

- Verification of C/C++ and Ada code
- Detects run-time errors
- Streamlines high integrity DO-178B workflows
  - Rule checking features (MISRA-C and JSF++)
  - Source code color scheme
  - DO-178B artifact generation capabilities
  - Qualification kit available
DO-178B Workflow Example

- **Validate**
  - Requirements
  - Model
  - Source Code
  - Object Code

- **Trace**
  - Requirements → Model
  - Model → Source Code
  - Source Code → Object Code

- **Conformance**
  - Requirements → Model
  - Model → Source Code
  - Source Code → Object Code

- **Verify**
  - SystemTest*
  - Embedded IDE Link

- **Verify**
  - Simulink Design Verifier:
    - Test Generation
    - Embedded IDE Link
Processor-in-the-Loop Testing

Embedded IDE Link

- Model in simulation and code on the processor running in parallel

PIL also provides execution profiling, code coverage reports, and interactive debugging.
DO-178B Workflow Summary

- **Trace**
  - Simulink Verification and Validation: Requirements Management Interface
- **Validate**
  - Requirements
  - Simulink & Stateflow
  - Model
  - Source Code
  - Object Code
- **Verify**
  - SystemTest*
  - Embedded IDE Link
  - Property Proving Model Coverage
  - Test Generation
  - Embedded IDE Link

*DO Qualifiable Tool
Agenda

- Relevant standards
- DO workflow – Common Elements
- DO-178B - Software Considerations and Workflows
- DO-254 – Hardware Considerations and Workflows
- Additional Topics
DO-254 Workflow Example

- High Level Requirements
- Conceptual Model
- Detailed Design (RTL)
- Detailed Design (Net-List)
- Hardware

Flow:
1. **Trace** from High Level Requirements to Conceptual Model
2. **Conformance** from Conceptual Model to Detailed Design (RTL)
3. **Validate** from Detailed Design (RTL) to Detailed Design (Net-List)
4. **Verify** from Detailed Design (Net-List) to Hardware
5. **Verify** from Detailed Design (Net-List) to Conceptual Model
6. **Verify** from Detailed Design (Net-List) to High Level Requirements

Notes:
- **DO-178B** and **DO-254** are referenced in the diagram.
DO-254 Workflow Example

High Level Requirements

Conceptual Model

Simulink HDL Coder

Detailed Design (RTL)

Trace Model/Code Trace Report

Validate

Conformance

Verify

DO-178B  DO-254
HDL Code Generation with Simulink HDL Coder

- Simulink HDL Coder
  - Generate behavioral HDL
  - Readable and traceable to requirements
  - Target-Independent
  - Bit Accurate/Cycle True
  - Customizable via options and Control Files

- Full model support
  - Simulink (datapath)
  - Stateflow® (control logic)
  - Embedded MATLAB
Model-to-HDL and HDL-to-Model Traceability

Simulink Verification and Validation

- Use the Traceability Report section of the Simulink HDL Coder HDL generation report to review mapping.
DO-254 Workflow Example

High Level Requirements → Conceptual Model → Detailed Design (RTL) → Detailed Design (Net-List)

- Trace
- Conformance
- Validate
- Verify

* DO Qualifiable Tool
EDA Simulator Link™ block Brings Together Leading Tools for Modeling and HDL Simulation

- EDA Simulator Link™ block is a fast, bidirectional cosimulation interface for system-level functional verification using ModelSim, Incisive or Discovery.

- Benefit: Reuse test environment in the executable specification to verify the implementation.
DO-254 Workflow Example

- **High Level Requirements**
  - Trace
  - Conformance

- **Conceptual Model**
  - Trace

- **Detailed Design (RTL)**
  - Trace

- **Detailed Design (Net-List)**
  - Trace

- **Hardware**

**EDA Partner Tools**

- **CoSim / HIL**
  - Verify SystemTest™*
  - Verify Vendor HIL Solution

- **Verify**
  - SystemTest™*
  - EDA Simulator Link
  - HDL Simulator

* DO Qualifiable Tool
DO-254 Workflow Example (Partners)

**EDA Partner Tools**

**Trace**
- Simulink® Verification and Validation™: Requirements Management Interface
- Model/Code Trace Report

**CoSim / HIL**
- **Verify**
  - SystemTest™*
  - Vendor HIL Solution

**Verify**
- SystemTest™*
- EDA Simulator Link
- HDL Simulator

**Verify**
- SystemTest™*
- EDA Simulator Link
- HDL Simulator

**Verify**
- SystemTest™*
- Vendor HIL Solution

**DO-254 Workflow Example (Partners)**

- **High Level Requirements**
  - Simulink & Stateflow
  - Conceptual Model
  - Conformance Model Advisor

- **Simulink & Code Trace**
  - Trace
  - Model/Code Trace Report

- **Auto Generated HDL**
  - Conformance
  - Detailed Design (Net-List)
  - Hardware

* DO-254 Qualifiable Tool
Agenda

- Relevant standards
- Benefits of Model-Based Design
- DO-178B - Software Considerations and Workflows
- DO-254 – Hardware Considerations and Workflows
- Additional Topics
DO Qualification Kit

- Tool Qualification Plan and Tool Operational Requirements
- Test case models and code, test procedures, and expected results
- Traceability tables mapping test cases to requirements
- Qualification materials for Simulink verification, validation, and test tools
- Qualification materials for PolySpace code verification tools