MathWorks®
Accelerating the pace of engineering and science

DO-178C Workflow with Qualified Code Generation

Qualified Definition Environment
Modelling & Simulation - Verification & Validation

SPECIFICATION
(HLR)

LLR/HLR/Test Cases Traceability

Requirement Traceability
- Authoring
- Import and Synchronize External Requirements (ReqIF)
- Req to Design-Model Traceability Report — MB.A-3 (Obj 4, 6); MB.A-3 (Obj 2)
- Requirement Analysis — MB.A-7 (Obj 3, 4, 6, 7, 11)
- Requirement-Based Testing Track Status — MB.A-8 (Obj 2)

Design
MATLAB and Simulink

Architecture
Decomposition
Allocation
Sequence Diagrams
Algorithms
Control Design
System Analysis
State Machine

Model Conformance Checks

Design Checks
- Design Checks & Metrics — MB.A-3 (Obj 2 to 7); MB.A-4 (Obj 2 to 7, 9, 12)
- Modelling Standards (DO-178C Checks)
- Design constraints (Equivalence classes, Boundary Values, Derived Reqs)

Model Compliance

- Design Error Detection — MB.A-3 (Obj 1, 2, 4 and 7); FM.A-3 (Obj 8 to 11)
- Property Proving — MB.A-4 (Obj 1, 2, 4, 7, 9, 11); FM.A-4 (Obj 14 to 17)
- Automatic Test Case Generation — MB.A-6 (Obj 1 to 4)

Model Coverage Analysis

HLR-Based Test Coverage
- Model Coverage Assessment — MB.A-3 (Obj 1, 4, 5); MB.A-4 (Obj1, 4, 5, 11, 12)
- Simulation Results
- Test Cases
- Model in the Loop (MIL) Functional Testing — MB.A-3 (Obj 1, 2, 4, 7 to 10)
- Pass/Fail Status Determination Report — MB.A-4 (Obj 1, 2, 4, 7 to 9, 11, 14 to 16)

Model Design Analysis

DESIGN
(LLR as a model)

Qualified Implementation Environment
Generation - Verification & Validation

Support Packages

Implementation
- Source Code traceability to LLR
- Automatic Code Generation

SOURCE CODE

Compiler/linker

EXECUTABLE OBJECT CODE

Source Code / LLR Assessment
Code Trace

Code Inspection
- Automatic Code Inspection
- Source Code verification & traceability to LLR — MB.A-5 (Obj 1 to 3, 5, 6)

Source Code Standards Conformance

- Code Conformance (MISRA,…) — MB.A-5 (Obj 4, 6); FM.A-5 (Obj 4, 6)
- Coding Standards

Source Code Robustness

- Absence of Run-Time Errors — MB.A-5 (Obj 2 to 4, 6); FM.A-5 (Obj 2 to 4, 6, 10 to 13); MB.A-6 (Obj 2, 4); FM.A-7 (Obj1, 2 , 5 to 10)

Code & Test Coverage Analysis

Source and Object Code Coverage
- Code Coverage Assessment — MB.A-7 (Obj 1, 4 to 7)
- Test Cases
- Software in the Loop (SIL) Testing — MB.A-3 (Obj 1, 2, 4, 7 to 10)
- Processor in the Loop (PIL) Testing — MB.A-4 (Obj 1, 2, 4, 7 to 9, 11, 14 to 16)
- Pass/Fail Status Test Determination — MB.A-6 (Obj 1 to 4); MB.A-7 (Obj 1)

Source Code Compliance
Executable Object Code Compliance

DO Qualification Kit

Report Templates

Report Generation
Support for Testing, Code Generation and Certification

Specification Artifacts
Documentation SW Data Requirements, Trace Data, Test Cases, Tests Results
Review Reports Specification Model Review Reports

Design Artifacts
Documentation SW Design Description, Trace Data, Test Cases, Tests Results
Review Reports Model Review Reports

Implementation Artifacts
Documentation Generated Source Code, Trace Data
Review Reports Code Review Reports

DASHBOARDS
Model & Code Quality Statistics
Requirement-Based Testing Dashboard

DO-331 - MODEL USAGE EXAMPLE 1

DO-178C supplements
- DO-330 for Tool Qualification
- DO-331 for Model-Based Design (MB.A-y table)
- DO-333 for Formal Methods (FM.A-y table)

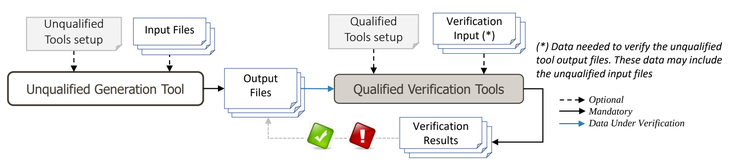
SW Production
Used as Input Reference
<Destination> Under Evaluation

Feature
Qualifiable Feature
Specific Inputs
Deliverable Artifact
Intermediate Artifact

DAL A Certification using a Qualified V&V Approach

Demonstrate the objectives are met using Qualified V&V Tools

DO-178C: Section 12.2
DO-330: Appendix D: FAQ D.7



Tool Qualification Level: *Our tools enable to* ***eliminate or reduce reviews****, same as a qualified code generator would. Enabling to* ***support up to a DAL-A system certification*** *with:*

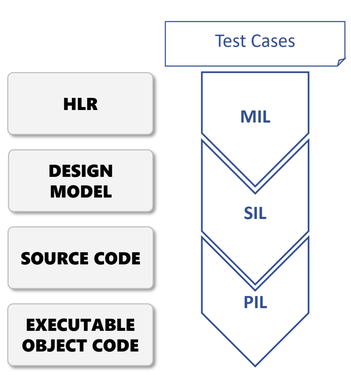
- *A TQL-4 qualification - for Polyspace Code Prover only - when used to justify the elimination or reduction of process(es);*
- *A TQL-5 qualification, otherwise.*

DO Qualification Kit
- Tools Requirements, User Manual and other MathWorks documentation
- Workflow Documentation and Tool Qualification Plans templates
- Verification Inputs Test Cases and Expected Results

Leverage Simulation to Reduce Low Level Testing Effort

Get Credit from the Simulation Test Cases using PIL Execution

DO-178C: Section 6.4
DO-331: Appendix MB.B: FAQ #16
DO-331: Sections MB.6.7 & MB.6.8.2



MB.B.16 **FAQ #16:** **Can simulation support the assessment of test coverage of the low-level requirements contained in a design model?**

Testing Strategy:
- *Define Test Cases in MIL to cover the HLR*
- ***Re-Use*** *the Tests Cases in SIL to validate the Source Code*
- ***Re-Use*** *the Tests Cases in PIL to assess the EOC compliance*
- ***Get Credit*** *from End-to-End Requirement-Based Testing*

Also Available
DO-254 ECSS

MATLAB® & SIMULINK®

Contact us - MathWorks
2021