MATLAB EXPO 2018

Automating Best Practices to Improve Design Quality

Magnus Jung, MathWorks
Growing Complexity of Embedded Systems

McKendrick, J. “Cars become ‘datacenters on wheels’, carmakers become software companies,” ZDJNet, 2013
Key Topics

How to:

- Handle project complexity
- Enable early detection of defects
- Automate verification activities
- Ensure conformance to safety standards

“Reduce costs and project risk through early verification, shorten time to market on a certified system, and deliver high-quality production code that was first-time right” Michael Schwarz, ITK Engineering
Development Process

Requirements → Specification → C/C++ → Hand code
Development Process with Model Based Design

Simulink Models

- Requirements
- Executable Specification
- Model used for production code generation

Code Generation

C/C++

Generated code
Why do 71% of Embedded Projects Fail?

Poor Requirements Management

Sources: Christopher Lindquist, Fixing the Requirements Mess, CIO Magazine, Nov 2005
Challenges with Requirements

Where are requirements implemented?

Is design and requirements consistent?

How are they tested?

Simulink Models

Requirements → Executable Specification → Model used for production code generation → C/C++ → Generated code
Track Implementation and Verification

![Image of requirements diagram]

- Index: 1, ID: #1, Summary: Driver Switch Request Handling
- Index: 2, ID: #19, Summary: Cruise Control Mode
- Index: 2.1, ID: #20, Summary: Disable Cruise Control system
- Index: 2.2, ID: #24, Summary: Operation mode determination
Working with Requirements

View

Track

Manage

If the Cancel switch is pressed, the value of reqDrv should be set to reqMode.Cancel.
Import Requirements from External Sources

- Microsoft Word
- IBM Rational DOORS
- ReqIF
- Simulink Requirements Editor

Import

3.1 Enabling cruise control

Cruise control is enabled when the following conditions are met:

- Vehicle speed is within the target speed range (40km/h – 100km/h).
- Key position is ON.
- Gear position is Drive.
- Cruise button is pushed while the cruise control mode is disabled.

Dashboard image

Keywords:
- Revision information:
- Links:

Show in document
REQ 3.1 ENABLING CRUISE CONTROL
Cruise control is enabled when.....

ENABLE SWITCH DETECTION
If the Enable switch is pressed......

Implemented By

Derived From

Verified By

Test Case
Requirements Perspective
Track Implementation and Verification

![Requirements Table]

**Implementation Status**
- Implemented
- Justified
- Missing

**Verification Status**
- Passed
- Failed
- No Result
- Missing
Respond to Change

Original Requirement
If the switch is pressed and the counter reaches 50 then it shall be recognized as a long press of the switch.

Updated Requirement
If the switch is pressed and the counter reaches 75 then it shall be recognized as a long press of the switch.

Issue: Destination Changed.
Design Review for Complex Designs

- Requirements
- Executable Specification
- Model used for production code generation

Simulink Models

Review and static analysis

C/C++

Generated code
Verify Design to Guidelines and Standards

- Designed to best practices?
- Component Size and Complexity?
- Optimized for Code Generation?

Simulink Models:
- Requirements
- Executable Specification
- Model used for production code generation
- C/C++
- Generated code
Verify Design to Guidelines and Standards

Typically:

- Too Late
- Impossible to review consistently
- Heavy manual work
Automate verification with static analysis

Check for:
- Readability and Semantics
- Performance and Efficiency
- Clones
- ...

Model Advisor Analysis

Simulink Models

Requirements → Executable Specification → Model used for production code generation → C/C++ → Generated code

MATLAB EXPO 2018
Generate reports for reviews and documentation

Model Advisor Analysis

Model Advisor Reports

Simulink Models

Requirements

Executable Specification

Model used for production code generation

C/C++

Generated code
Built in checks for industry standards and guidelines

- DO-178/DO-331
- ISO 26262
- IEC 61508
- IEC 62304
- EN 50128

- MISRA C:2012
- CERT C, CWE, ISO/IEC TS 17961
- MAAB (MathWorks Automotive Advisory Board)
- JMAAB (Japan MATLAB Automotive Advisory Board)
Custom checks for Your Best Practices and Guidelines

Simulink Models

Requirements → Executable Specification → Model used for production code generation → C/C++ → Generated code
Checks for standards and guidelines are often performed late

- **Requirements**
- **Executable Specification**
- **Model used for production code generation**

**Simulink Models**

**Static Analysis**

**C/C++**

**Generated code**

**Rework**
Shift Verification Earlier With Edit-Time Checking

- Highlight violations as you edit
- Fix issues earlier
- Avoid rework

Simulink Models

Requirements → Executable Specification → Model used for production code generation → C/C++ → Generated code
Find Compliance Issues as you Edit with Edit-Time Checking
Assess Quality with Metrics Dashboard

- Consolidated view of metrics
  - Size
  - Compliance
  - Complexity

- Identify where problem areas may be
Grid Visualization for Metrics

- Visualize Standards
- Check Compliance
  - Find Issues
  - Identify patterns
  - See hot spots

Legend:
- Red: Fail
- Orange: Warning
- Green: Pass
- Gray: Not run
Systematic Functional Testing

Does the design meet requirements?

Is it functioning correctly?

Is it completely tested?

Simulink Models

Requirements → Executable Specification → Model used for production code generation → C/C++ → Generated code
Systematic Functional Testing

Test Case

Inputs
- MAT file (input)
- Signal Builder
- Test Sequence
- Excel file

Main Model

Test Harness

Assessments
- MAT file (baseline)
- MATLAB Unit Test
- Test Assessment
- Excel file
Manage Testing and Test Results
Assess Test Completeness

Measure Structural Coverage
- Condition
- Decision
- MCDC
- ...
Assess Test Completeness – Coverage Analysis

- Identify testing gaps
- Missing requirements
- Unintended Functionality
Continuous Automated Feedback

Continuous Integration

Static Checks
Static Checks
Static Checks
Static Checks

Requirements
Executable Specification
Model used for production code generation
C/C++
Generated code
Is the code compliant to MISRA?

Is integrated code free of run-time errors?

Is interface between generated and other code fully tested?

The Generated Code is integrated with Other Code (Handwritten)
Static Code Analysis with Polyspace

- Code metrics and standards
  - Comment density, cyclomatic complexity,…
  - MISRA and Cybersecurity standards
  - Support for DO-178, ISO 26262, ….

- Bug finding and code proving
  - Check data and control flow of software
  - Detect bugs and security vulnerabilities
  - Prove absence of runtime errors

Results from Polyspace Code Prover
Equivalence Testing

Is the code functionally equivalent to model?

Is all the code tested?

Simulink Models

Requirements ➔ Executable Specification ➔ Model used for production code generation ➔ C/C++ ➔ Generated code
Equivalence Testing

- **Software in the Loop (SIL)**
  - Show functional equivalence, model to code
  - Execute on desktop / laptop computer

- **Processor in the Loop (PIL)**
  - Numerical equivalence, model to target code
  - Execute on target board

- Re-use tests developed for model to test code
- Collect code coverage
Qualify tools with IEC Certification Kit and DO Qualification Kit

- Qualify code generation and verification products
- Includes documentation, test cases and procedures

KOSTAL Asia R&D Center Receives ISO 26262 ASIL D Certification for Automotive Software Developed with Model-Based Design

BAE Systems Delivers DO-178B Level A Flight Software on Schedule with Model-Based Design
Summary

- Handle project complexity
- Enable early detection of defects
- Automate verification activities
- Ensure conformance to safety standards

Component and system testing

Review and static analysis

Equivalence testing

Equivalence checking

Simulink Models

Requirements

Executable Specification

Model used for production code generation

C/C++

Generated code

MATLAB EXPO 2018
Thank You!