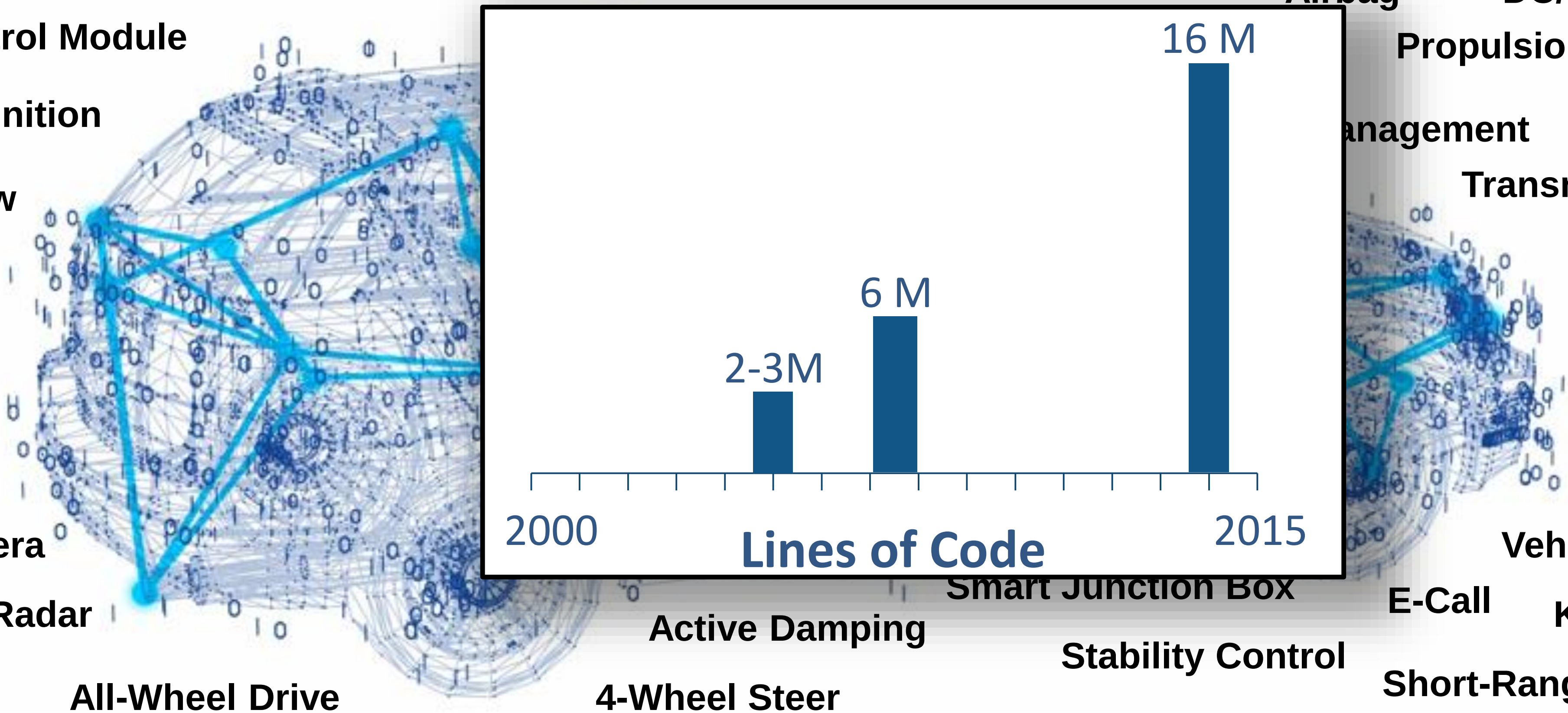
MATLAB EXPO 2018

Automating Best Practices to Improve Design Quality

Magnus Jung, MathWorks

Growing Complexity of Embedded Systems



Battery Management

Stability Control

Automatic Parking

Infotainment

Instrument Panel

Emergency Braking

Adaptive Cruise Control

Smart Junction Box

Airbag

DC/DC Converter

Body Control Module

Propulsion Motor Control

Voice Recognition

Navigation

anagement

Power Window

Transmission Control

Vehicle-to-Infrastructure

Forward Camera

Adaptive Front Lighting

Power Liftgate

HVAC Control

Power Seat

Back-up Camera

Vehicle-to-Vehicle

Smart Junction Box

E-Call

Long-Range Radar

Active Damping

Keyless Entry

Stability Control

Short-Range Radar

All-Wheel Drive

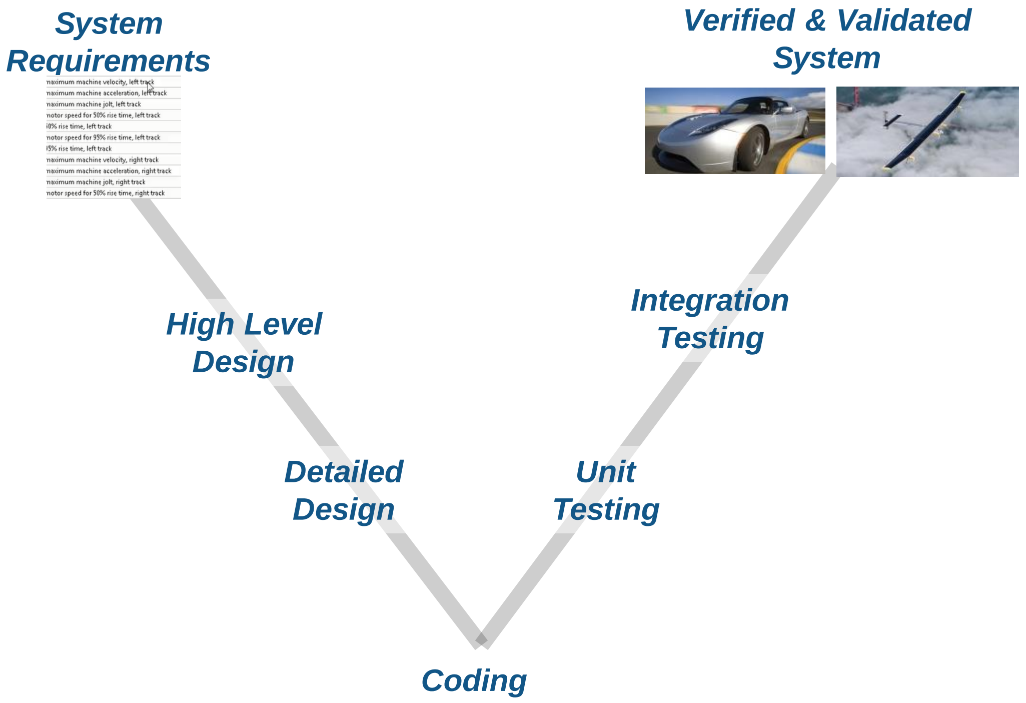
4-Wheel Steer

Siemens, "Ford Motor Company Case Study," Siemens PLM Software, 2014
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



System Requirements

naximum machine velocity, left track
naximum machine acceleration, left track
naximum machine jolt, left track
notor speed for 50% rise time, left track
i0% rise time, left track
notor speed for 95% rise time, left track
i5% rise time, left track
naximum machine velocity, right track
naximum machine acceleration, right track
naximum machine jolt, right track
notor speed for 50% rise time, right track

High Level Design

Detailed Design

Coding

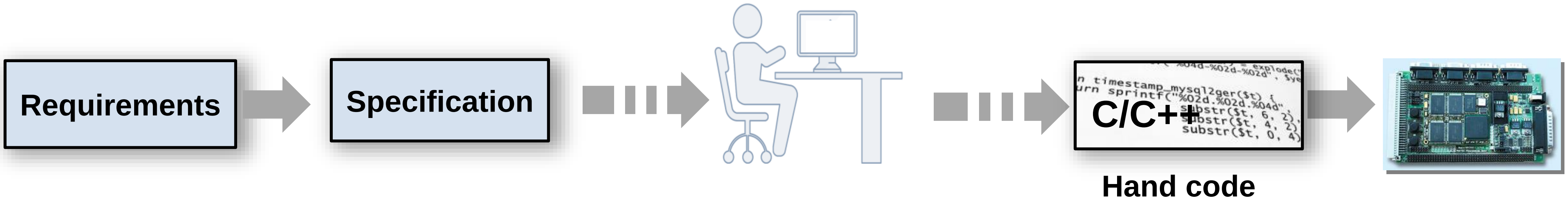
Unit Testing

Integration Testing

Verified & Validated System

"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



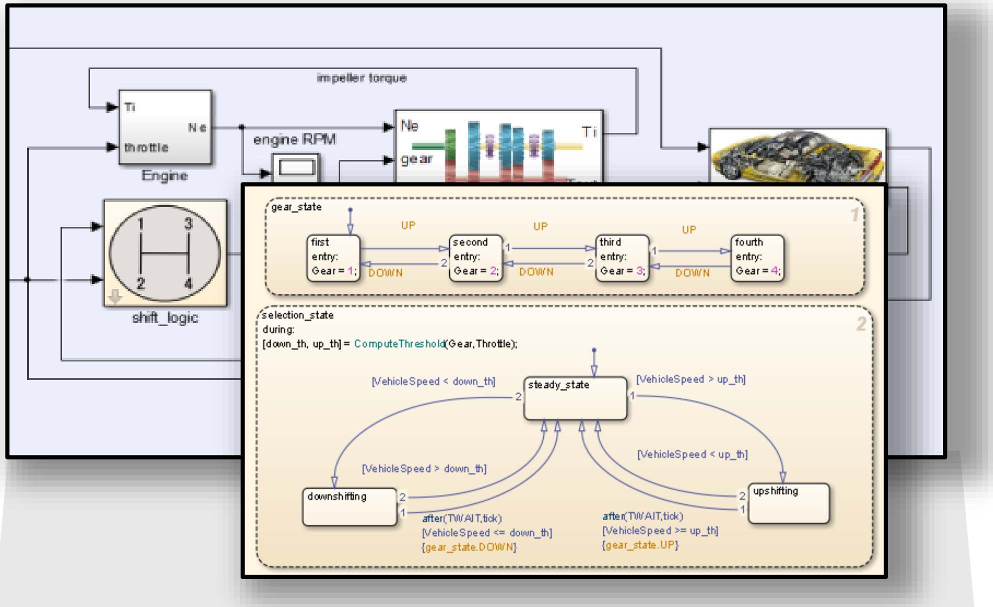
Requirements

Specification

C/C++

Hand code

Development Process with Model Based Design



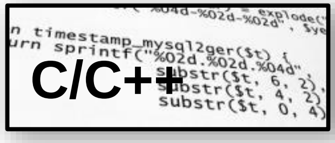
Simulink Models

Requirements

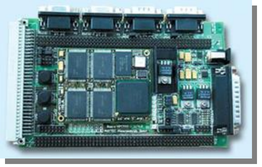
Executable Specification

Model used for production code generation

Code Generation



Generated code

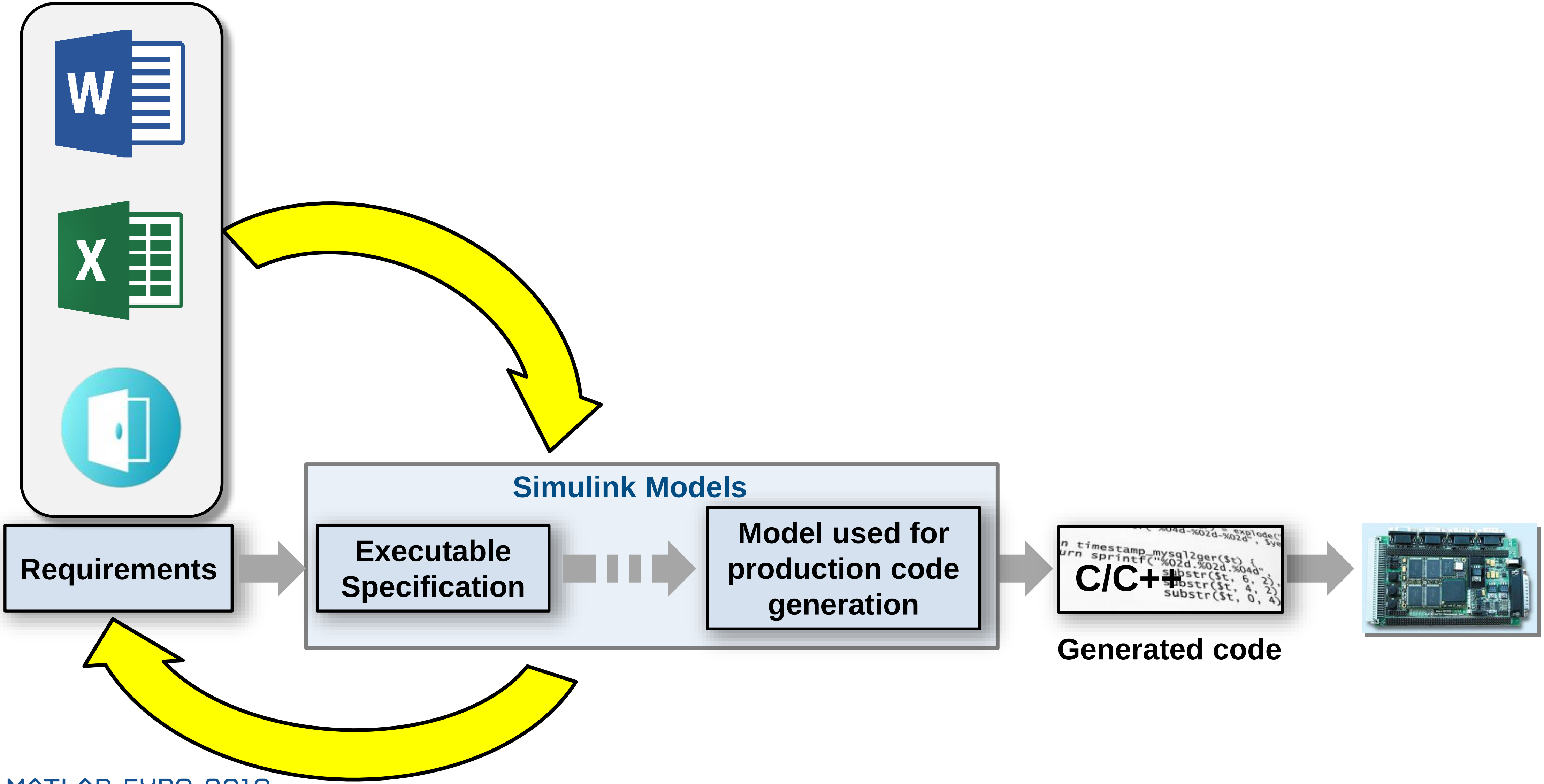


Why do 71% of Embedded Projects Fail?

Poor Requirements Management

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

Gap Between Requirements and Design



Requirements

Simulink Models

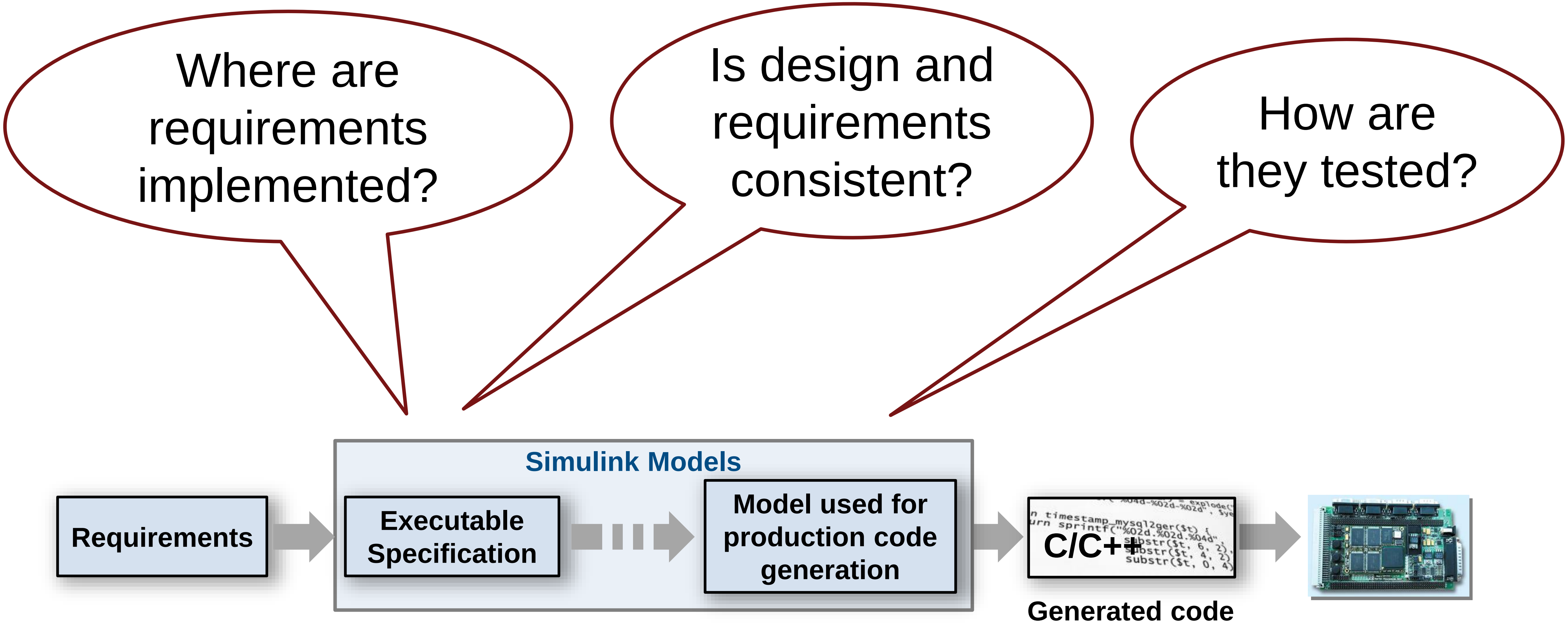
Executable Specification

Model used for production code generation

C/C++

Generated code

Challenges with Requirements



Where are requirements implemented?

Is design and requirements consistent?

How are they tested?

Simulink Models

Requirements

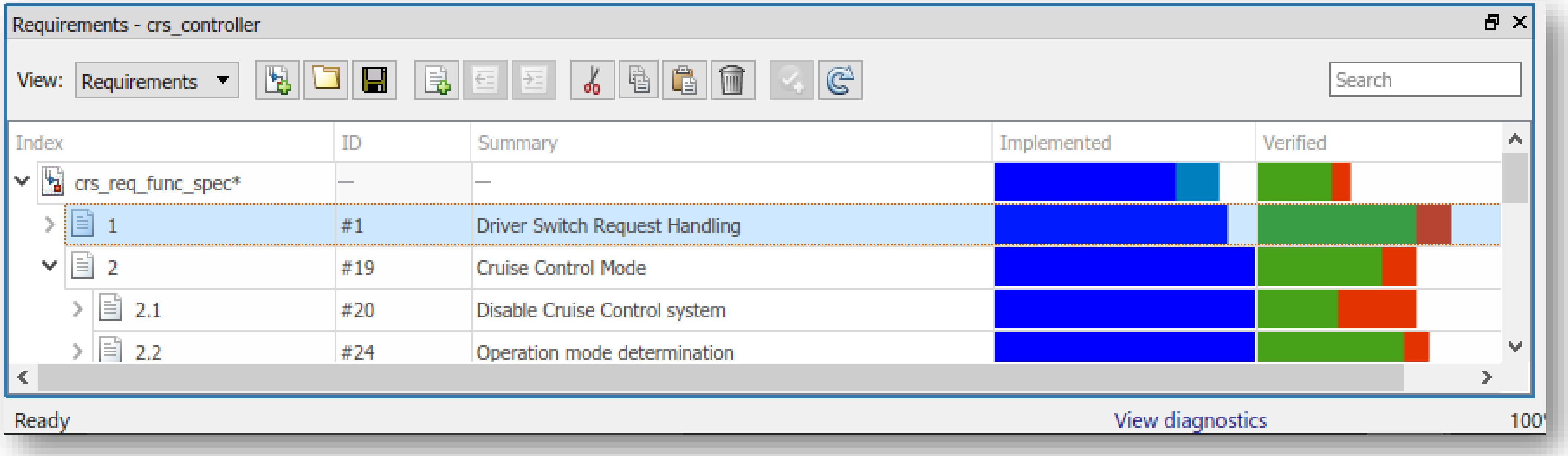
Executable Specification

Model used for production code generation

C/C++

Generated code

Track Implementation and Verification



Requirements - crs_controller

View: Requirements

Search

Index	ID	Summary	Implemented	Verified
crs_req_func_spec*	—	—		
1	#1	Driver Switch Request Handling		
2	#19	Cruise Control Mode		
2.1	#20	Disable Cruise Control system		
2.2	#24	Operation mode determination		

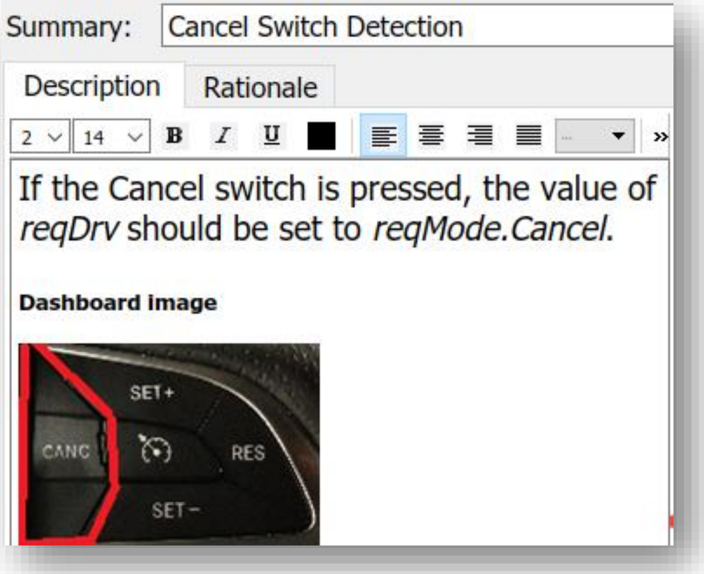
Ready

View diagnostics

100

Working with Requirements

View

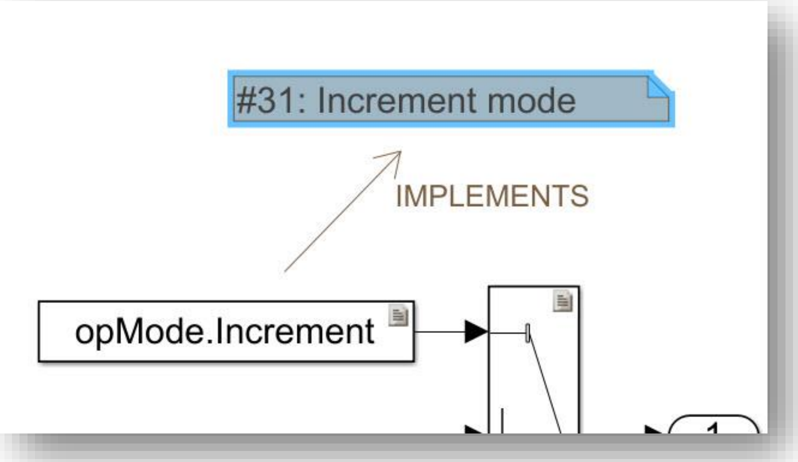


Summary: Cancel Switch Detection

Description | Rationale

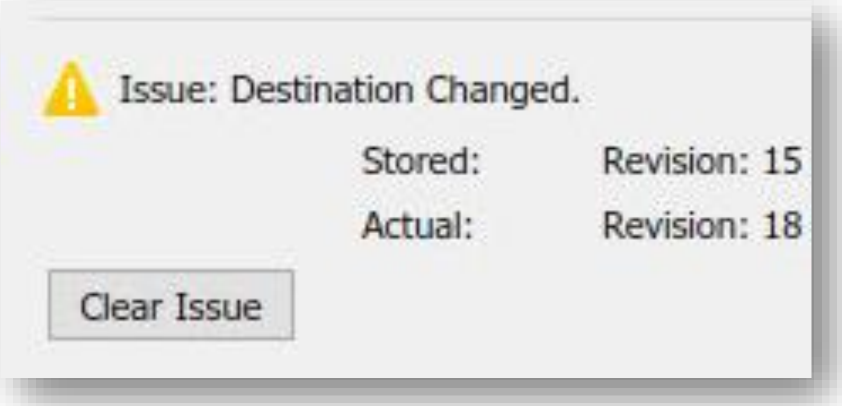
If the Cancel switch is pressed, the value of *reqDrv* should be set to *reqMode.Cancel*.

Dashboard image



Track

Manage



Issue: Destination Changed.

Stored: Revision: 15

Actual: Revision: 18

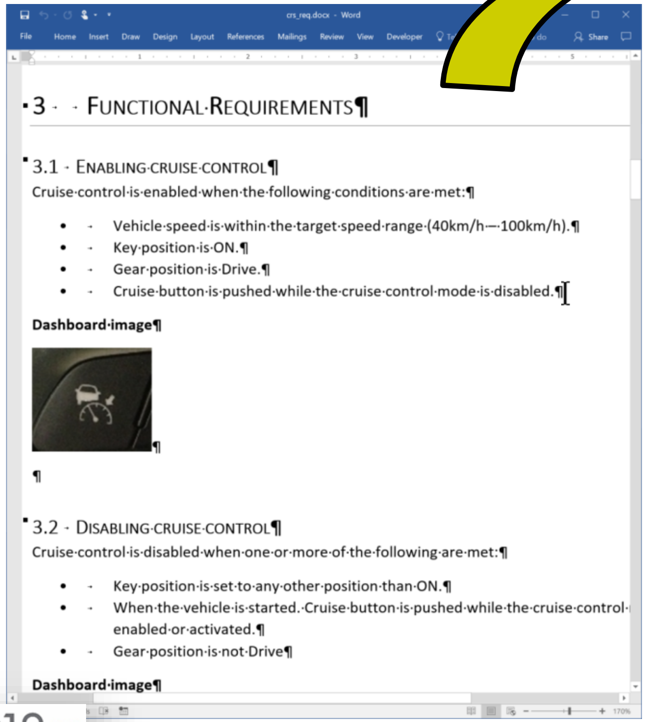
Import Requirements from External Sources

IBM Rational DOORS

R2018a

ReqIF Requirements Interchange Format

Microsoft Word


crs_req.docx - Word
File Home Insert Draw Design Layout References Mailings Review View Developer Share

3 FUNCTIONAL REQUIREMENTS

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

3.2 DISABLING CRUISE CONTROL

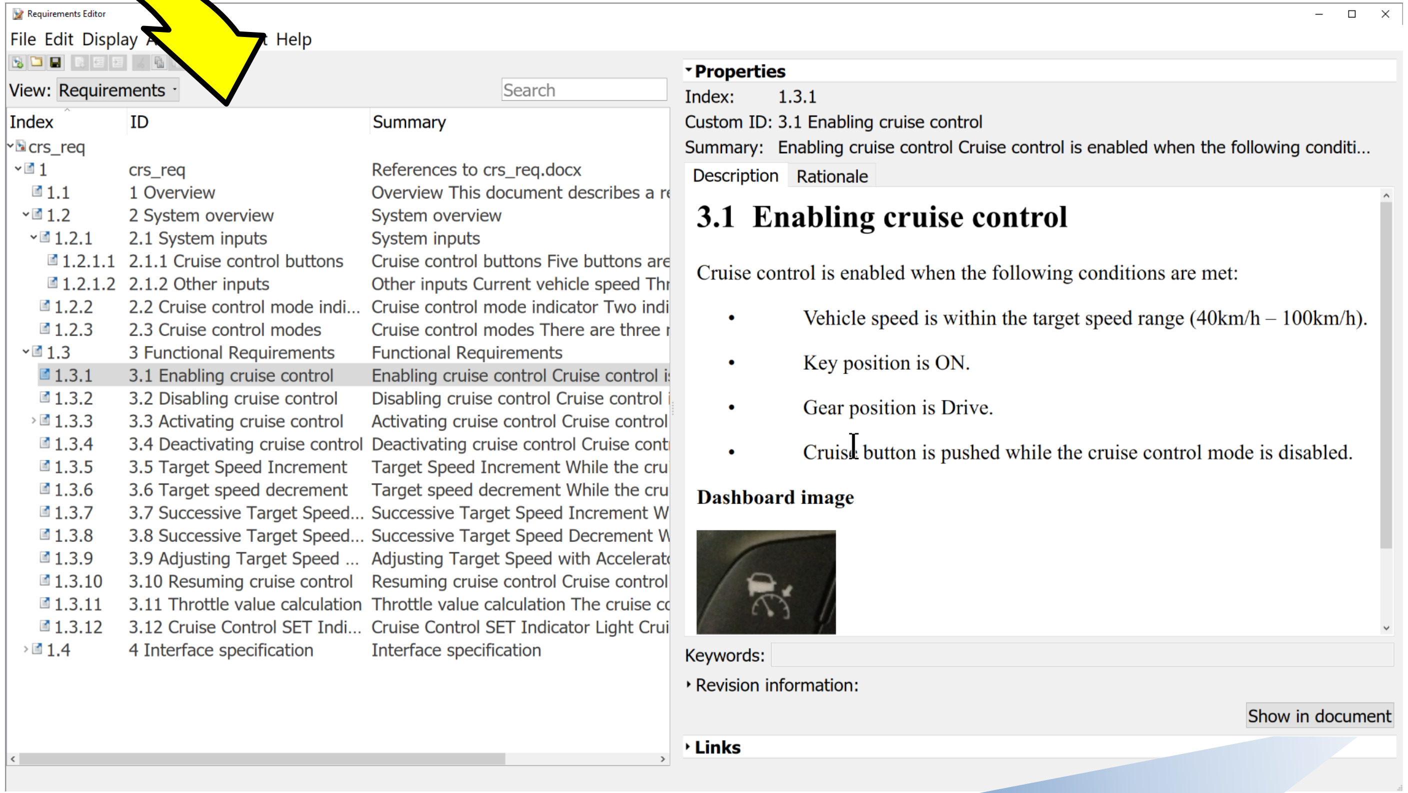
Cruise control is disabled when one or more of the following are met:

- Key position is set to any other position than ON.
- When the vehicle is started. Cruise button is pushed while the cruise control enabled or activated.
- Gear position is not Drive

Dashboard image

Import

Simulink Requirements Editor



Index	ID	Summary
crs_req		
1	crs_req	References to crs_req.docx
1.1	1 Overview	Overview This document describes a r
1.2	2 System overview	System overview
1.2.1	2.1 System inputs	System inputs
1.2.1.1	2.1.1 Cruise control buttons	Cruise control buttons Five buttons are
1.2.1.2	2.1.2 Other inputs	Other inputs Current vehicle speed Thr
1.2.2	2.2 Cruise control mode indi...	Cruise control mode indicator Two indi
1.2.3	2.3 Cruise control modes	Cruise control modes There are three r
1.3	3 Functional Requirements	Functional Requirements
1.3.1	3.1 Enabling cruise control	Enabling cruise control Cruise control i
1.3.2	3.2 Disabling cruise control	Disabling cruise control Cruise control i
1.3.3	3.3 Activating cruise control	Activating cruise control Cruise control
1.3.4	3.4 Deactivating cruise control	Deactivating cruise control Cruise cont
1.3.5	3.5 Target Speed Increment	Target Speed Increment While the cru
1.3.6	3.6 Target speed decrement	Target speed decrement While the cru
1.3.7	3.7 Successive Target Speed...	Successive Target Speed Increment W
1.3.8	3.8 Successive Target Speed...	Successive Target Speed Decrement W
1.3.9	3.9 Adjusting Target Speed ...	Adjusting Target Speed with Accelerat
1.3.10	3.10 Resuming cruise control	Resuming cruise control Cruise control
1.3.11	3.11 Throttle value calculation	Throttle value calculation The cruise co
1.3.12	3.12 Cruise Control SET Indi...	Cruise Control SET Indicator Light Crui
1.4	4 Interface specification	Interface specification

Properties

Index: 1.3.1

Custom ID: 3.1 Enabling cruise control

Summary: Enabling cruise control Cruise control is enabled when the following conditi...

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

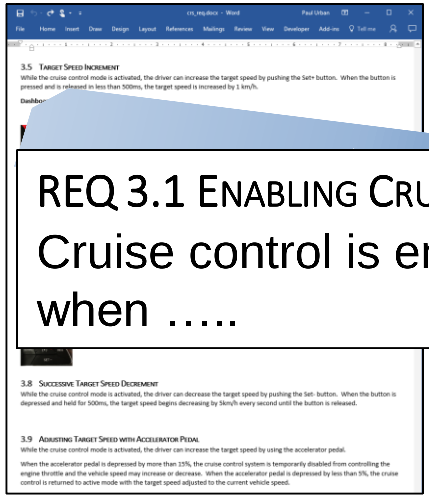
Keywords:

Revision information:

Links

Show in document

Link Requirements, Designs and Tests



3.5 Target Speed Increment

While the cruise control mode is activated, the driver can increase the target speed by pushing the Set+ button. When the button is pressed and is released in less than 500ms, the target speed is increased by 1 km/h.

Dashbo

3.8 Successive Target Speed Decrement

While the cruise control mode is activated, the driver can decrease the target speed by pushing the Set- button. When the button is depressed and held for 500ms, the target speed begins decreasing by 5km/h every second until the button is released.

3.9 Adjusting Target Speed with Accelerator Pedal

While the cruise control mode is activated, the driver can increase the target speed by using the accelerator pedal.

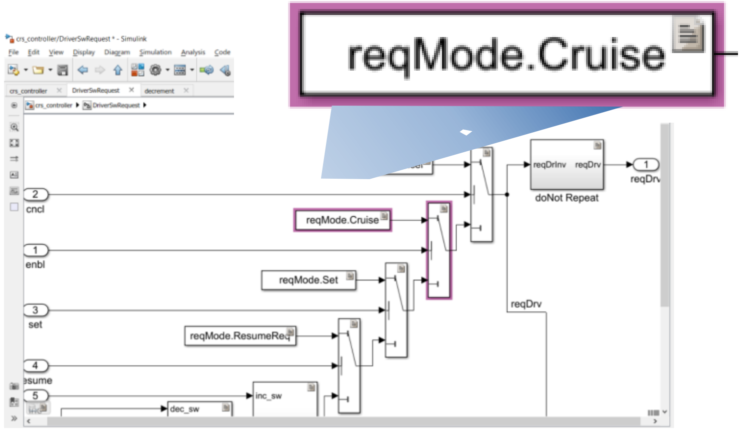
When the accelerator pedal is depressed by more than 15%, the cruise control system is temporarily disabled from controlling the engine throttle and the vehicle speed may increase or decrease. When the accelerator pedal is depressed by less than 5%, the cruise control is returned to active mode with the target speed adjusted to the current vehicle speed.

REQ 3.1 ENABLING CRUISE CONTROL
Cruise control is enabled when …..

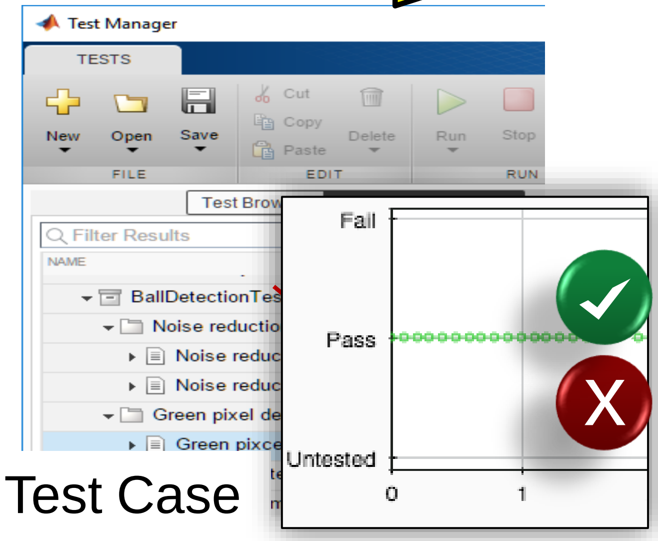
Derives

ENABLE SWITCH DETECTION
If the Enable switch is pressed ……

Implemented By



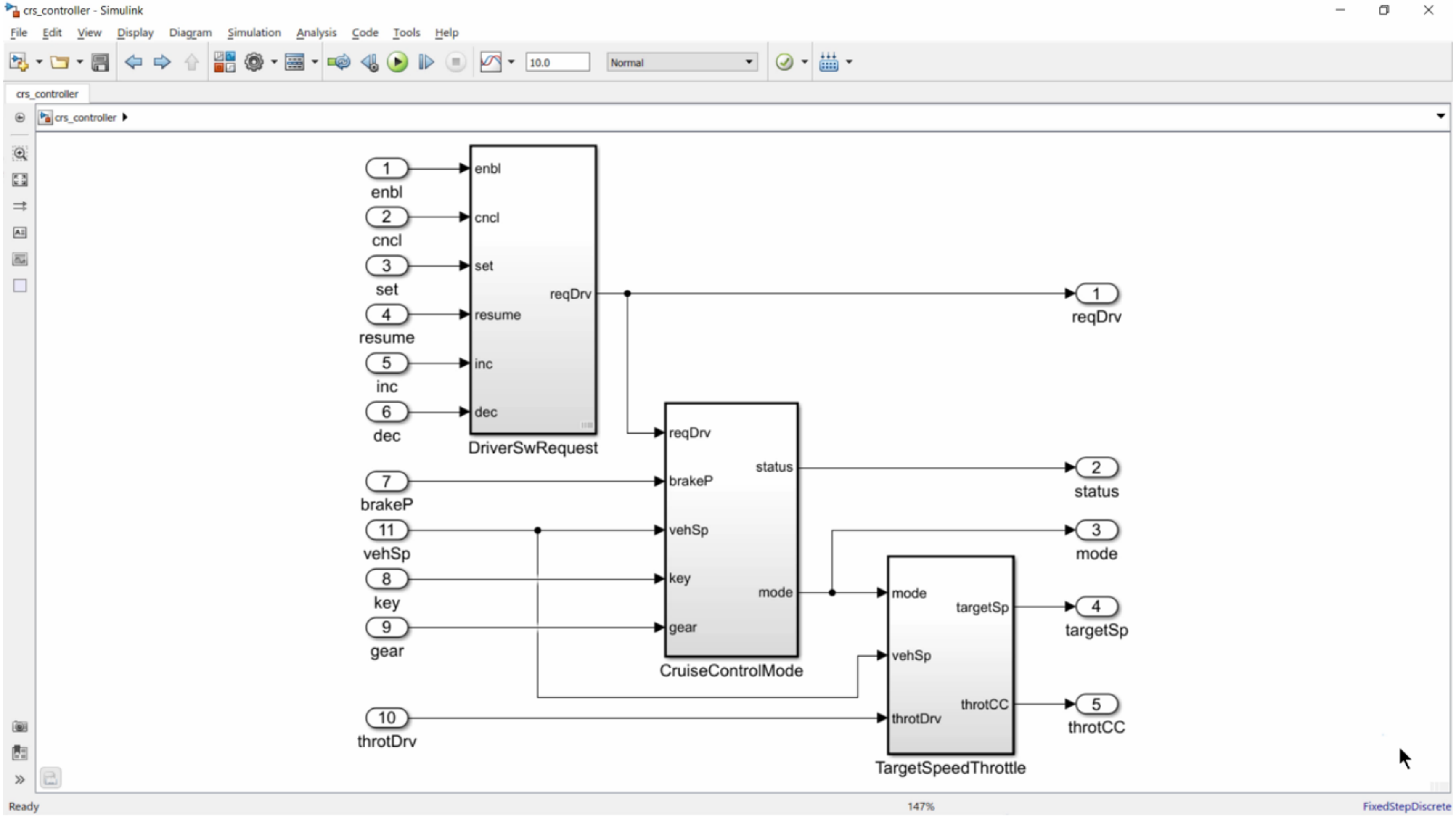
Verified By



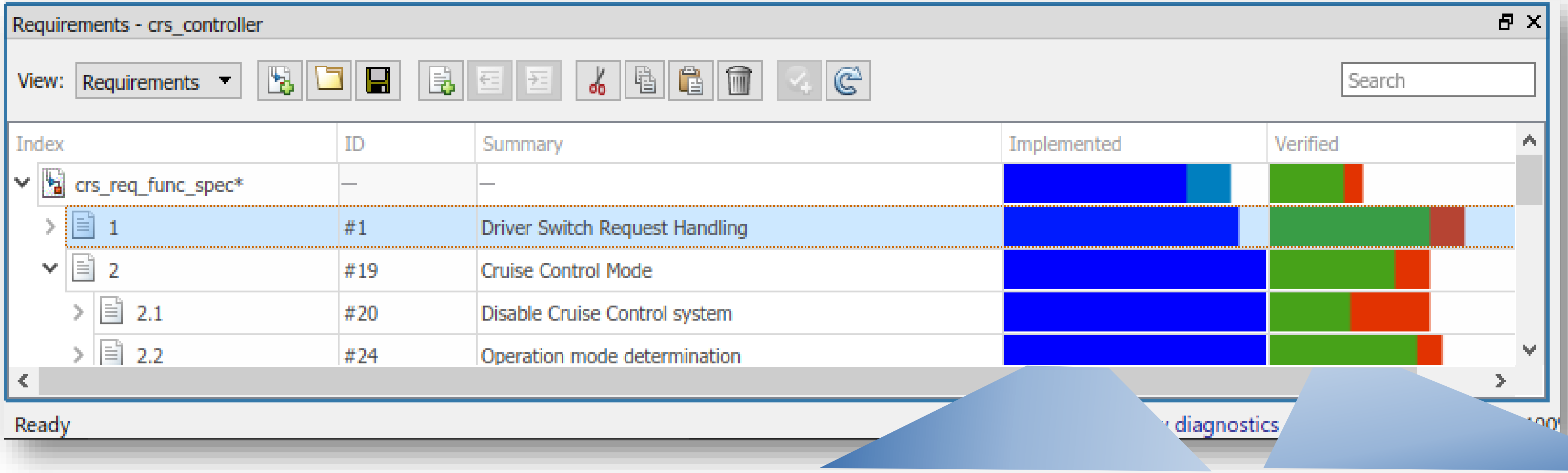
Test Case

MATLAB EXPO 2018

Requirements Perspective



Track Implementation and Verification



Requirements - crs_controller

View: Requirements

Search

Index	ID	Summary	Implemented	Verified
crs_req_func_spec*	—	—		
1	#1	Driver Switch Request Handling		
2	#19	Cruise Control Mode		
2.1	#20	Disable Cruise Control system		
2.2	#24	Operation mode determination		

Ready

diagnostics

Implementation Status

🟦	Implemented
▨	Justified
□	Missing

Verification Status

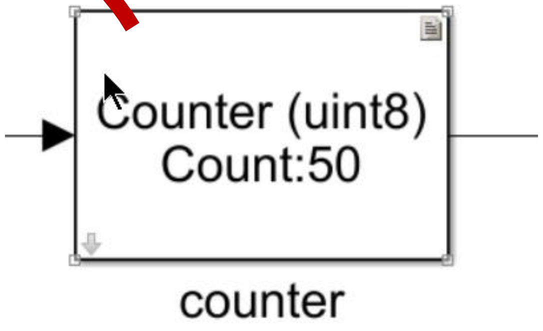
🟩	Passed
🟥	Failed
🟧	No Result
□	Missing

Respond to Change

Original Requirement

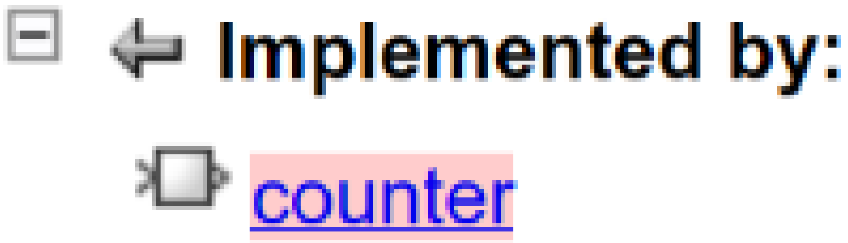
If the switch is pressed and the counter reaches **50** then it shall be recognized as a long press of the switch.

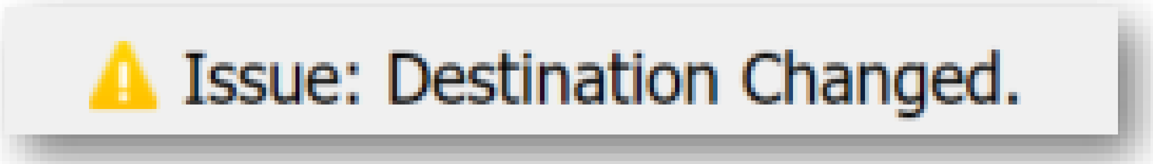
Implements



Updated Requirement

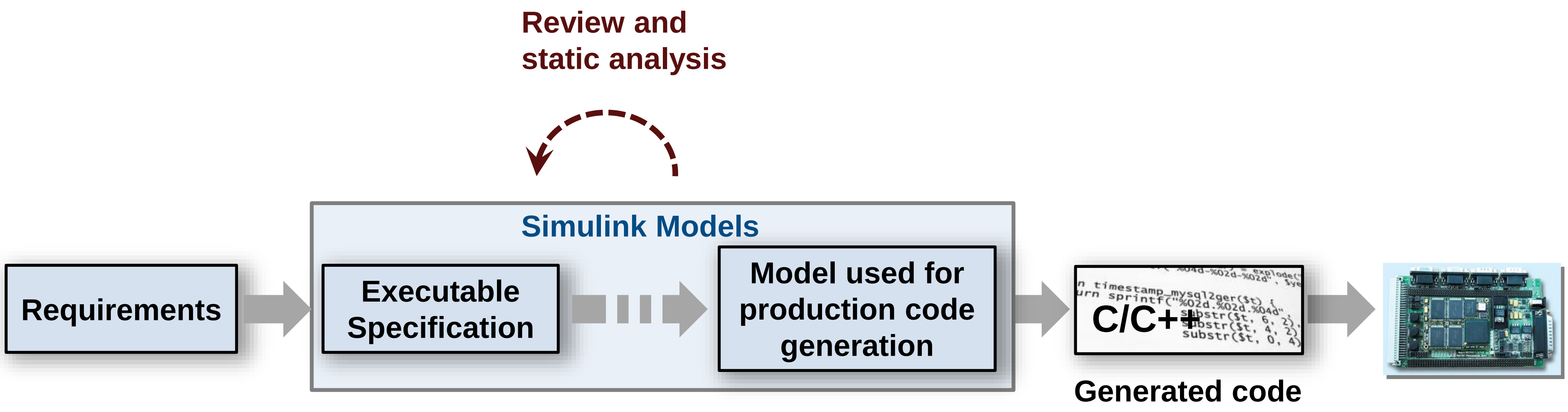
If the switch is pressed and the counter reaches **75** then it shall be recognized as a long press of the switch.





Issue: Destination Changed.

Design Review for Complex Designs



Review and static analysis

Simulink Models

Requirements

Executable Specification

Model used for production code generation

C/C++

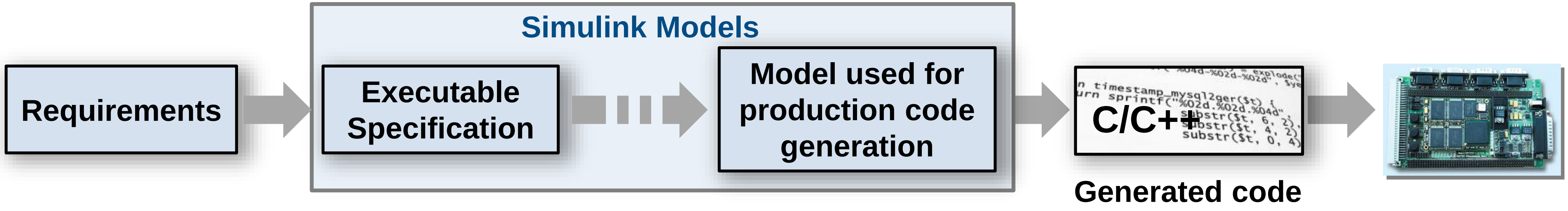
Generated code

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

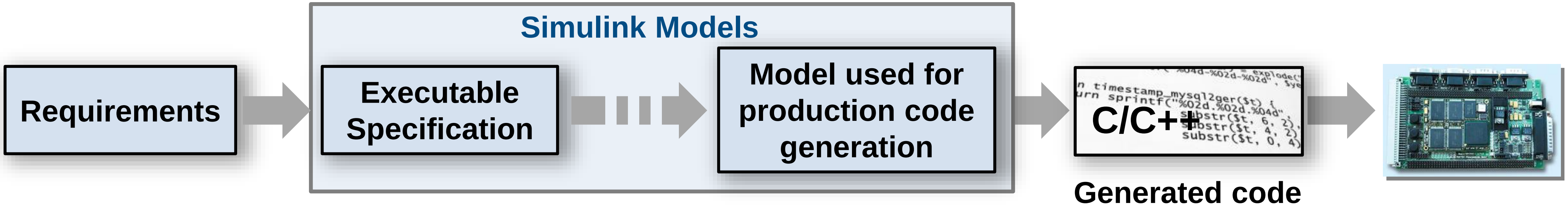
C/C++

Generated code

Verify Design to Guidelines and Standards

Typically:

- Too Late
- Impossible to review consistently
- Heavy manual work



Simulink Models

Requirements

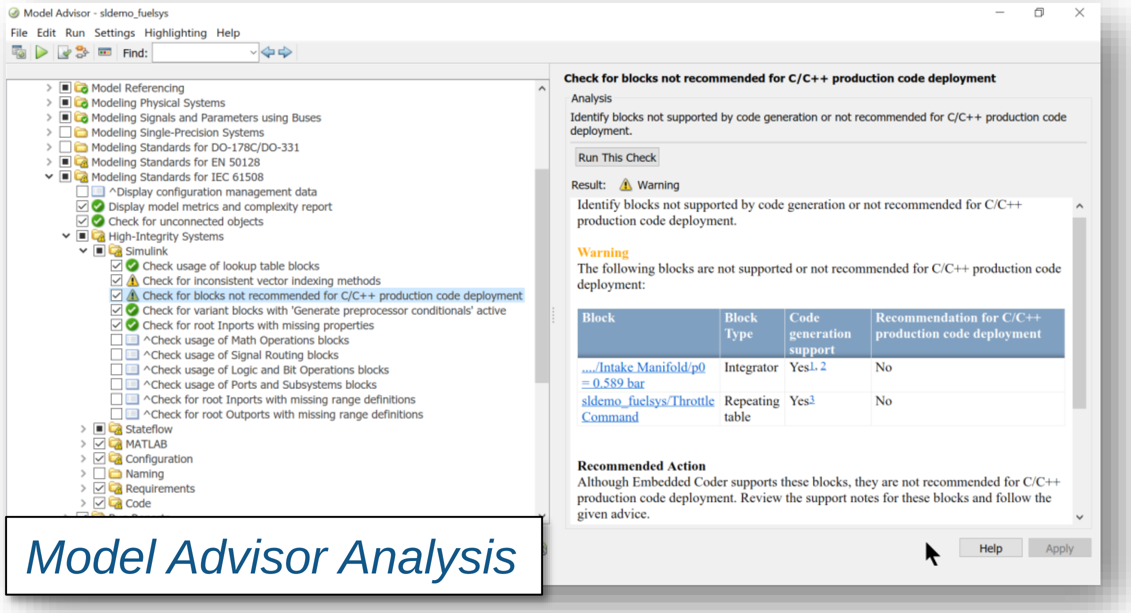
Executable Specification

Model used for production code generation

C/C++

Generated code

Automate verification with static analysis



Model Advisor - sldemo_fuelsys

- ■ Model Referencing
- ■ Modeling Physical Systems
- ■ Modeling Signals and Parameters using Buses
- □ Modeling Single-Precision Systems
- □ Modeling Standards for DO-178C/DO-331
- ■ Modeling Standards for EN 50128
- ■ Modeling Standards for IEC 61508
  - □ ^Display configuration management data
  - ☑ ✓ Display model metrics and complexity report
  - ☑ ✓ Check for unconnected objects
  - ■ High-Integrity Systems
    - ■ Simulink
      - ☑ ✓ Check usage of lookup table blocks
      - ☑ ⚠ Check for inconsistent vector indexing methods
      - ☑ ⚠ Check for blocks not recommended for C/C++ production code deployment
      - ☑ ✓ Check for variant blocks with 'Generate preprocessor conditionals' active
      - ☑ ✓ Check for root Inports with missing properties
      - □ ^Check usage of Math Operations blocks
      - □ ^Check usage of Signal Routing blocks
      - □ ^Check usage of Logic and Bit Operations blocks
      - □ ^Check usage of Ports and Subsystems blocks
      - □ ^Check for root Inports with missing range definitions
      - □ ^Check for root Outports with missing range definitions
    - ■ Stateflow
    - ☑ MATLAB
    - ☑ Configuration
    - □ Naming
    - ☑ Requirements
    - ☑ Code

Check for blocks not recommended for C/C++ production code deployment

Analysis

Identify blocks not supported by code generation or not recommended for C/C++ production code deployment.

Run This Check

Result: ⚠ Warning

Identify blocks not supported by code generation or not recommended for C/C++ production code deployment.

Warning

The following blocks are not supported or not recommended for C/C++ production code deployment:

Block	Block Type	Code generation support	Recommendation for C/C++ production code deployment
..../Intake Manifold/p0 = 0.589 bar	Integrator	Yes1, 2	No
sldemo_fuelsys/Throttle Command	Repeating table	Yes3	No

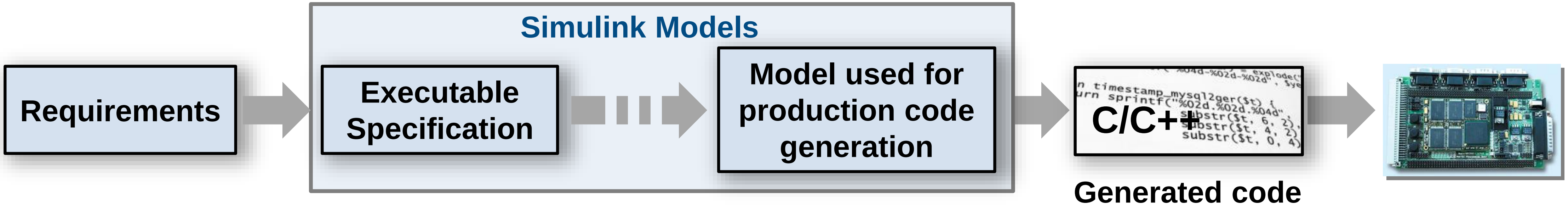
Recommended Action

Although Embedded Coder supports these blocks, they are not recommended for C/C++ production code deployment. Review the support notes for these blocks and follow the given advice.

Model Advisor Analysis

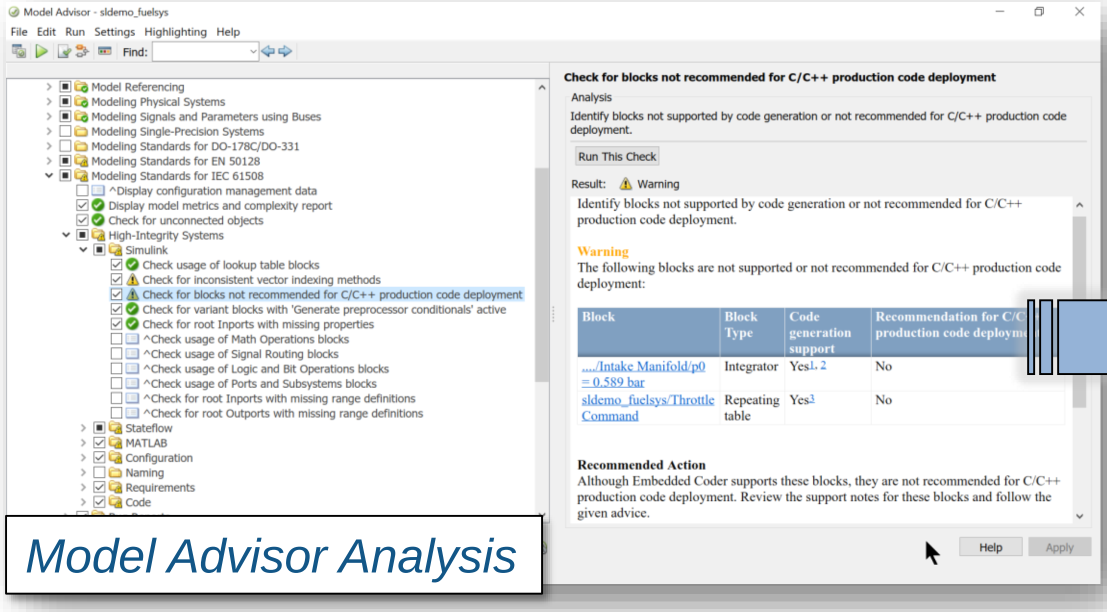
Check for:

- Readability and Semantics
- Performance and Efficiency
- Clones
- …



Generated code

Generate reports for reviews and documentation



Model Advisor - sldemo_fuelsys
File Edit Run Settings Highlighting Help
Find:

- ■ Model Referencing
- ■ Modeling Physical Systems
- ■ Modeling Signals and Parameters using Buses
- □ Modeling Single-Precision Systems
- □ Modeling Standards for DO-178C/DO-331
- ■ Modeling Standards for EN 50128
- ■ Modeling Standards for IEC 61508
  - □ ^Display configuration management data
  - ☑ ✓ Display model metrics and complexity report
  - ☑ ✓ Check for unconnected objects
  - ■ High-Integrity Systems
    - ■ Simulink
      - ☑ ✓ Check usage of lookup table blocks
      - ☑ ⚠ Check for inconsistent vector indexing methods
      - ☑ ⚠ Check for blocks not recommended for C/C++ production code deployment
      - ☑ ✓ Check for variant blocks with 'Generate preprocessor conditionals' active
      - ☑ ✓ Check for root Inports with missing properties
      - □ ^Check usage of Math Operations blocks
      - □ ^Check usage of Signal Routing blocks
      - □ ^Check usage of Logic and Bit Operations blocks
      - □ ^Check usage of Ports and Subsystems blocks
      - □ ^Check for root Inports with missing range definitions
      - □ ^Check for root Outports with missing range definitions
    - ■ Stateflow
    - ☑ MATLAB
    - ☑ Configuration
    - □ Naming
    - ☑ Requirements
    - ☑ Code

Check for blocks not recommended for C/C++ production code deployment

Analysis

Identify blocks not supported by code generation or not recommended for C/C++ production code deployment.

Run This Check

Result: ⚠ Warning

Identify blocks not supported by code generation or not recommended for C/C++ production code deployment.

Warning

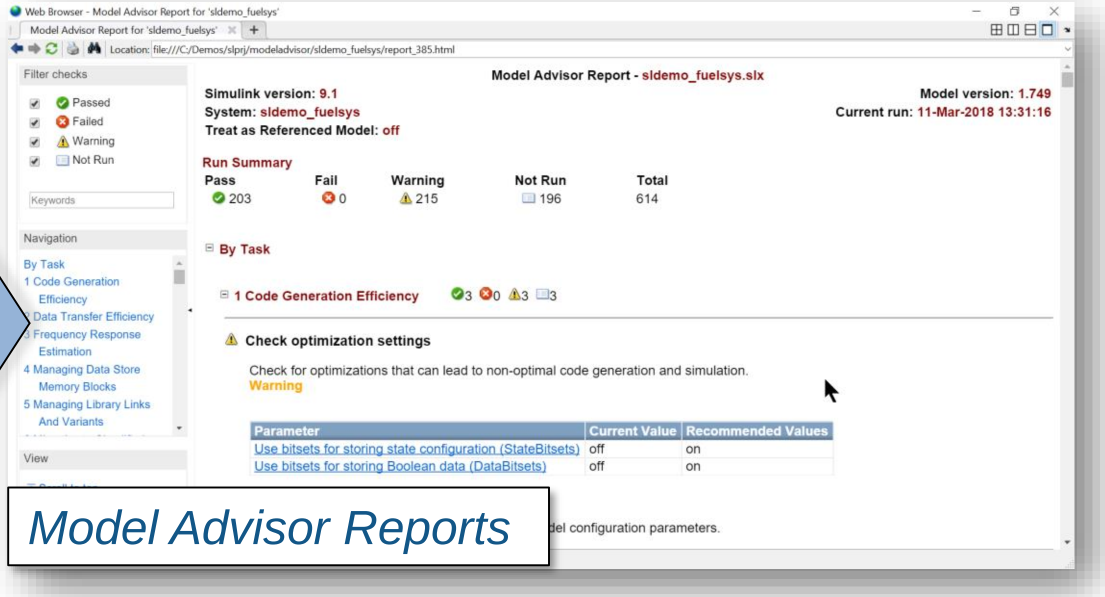
The following blocks are not supported or not recommended for C/C++ production code deployment:

Block	Block Type	Code generation support	Recommendation for C/C++ production code deployment
..../Intake Manifold/p0 = 0.589 bar	Integrator	Yes1, 2	No
sldemo_fuelsys/Throttle Command	Repeating table	Yes3	No

Recommended Action

Although Embedded Coder supports these blocks, they are not recommended for C/C++ production code deployment. Review the support notes for these blocks and follow the given advice.

Model Advisor Analysis



Web Browser - Model Advisor Report for 'sldemo_fuelsys'
Model Advisor Report for 'sldemo_fuelsys'
Location: file:///C:/Demos/slprj/modeladvisor/sldemo_fuelsys/report_385.html
Filter checks
Passed
Failed
Warning
Not Run
Keywords
Navigation
By Task
1 Code Generation Efficiency
2 Data Transfer Efficiency
3 Frequency Response Estimation
4 Managing Data Store Memory Blocks
5 Managing Library Links And Variants
View

Model Advisor Report - sldemo_fuelsys.slx

Simulink version: 9.1
System: sldemo_fuelsys
Treat as Referenced Model: off

Model version: 1.749
Current run: 11-Mar-2018 13:31:16

Run Summary

Pass	Fail	Warning	Not Run	Total
✓ 203	✗ 0	⚠ 215	196	614

By Task

1 Code Generation Efficiency ✓3 ✗0 ⚠3 3

⚠ **Check optimization settings**

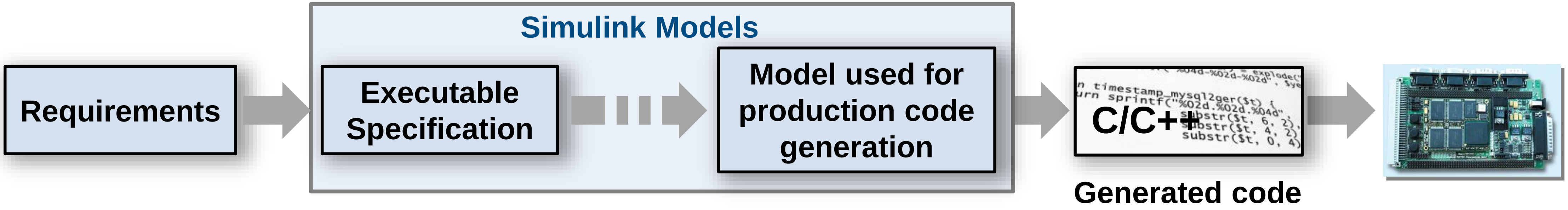
Check for optimizations that can lead to non-optimal code generation and simulation.

Warning

Parameter	Current Value	Recommended Values
Use bitsets for storing state configuration (StateBitsets)	off	on
Use bitsets for storing Boolean data (DataBitsets)	off	on

del configuration parameters.

Model Advisor Reports



Simulink Models

Requirements

Executable Specification

Model used for production code generation

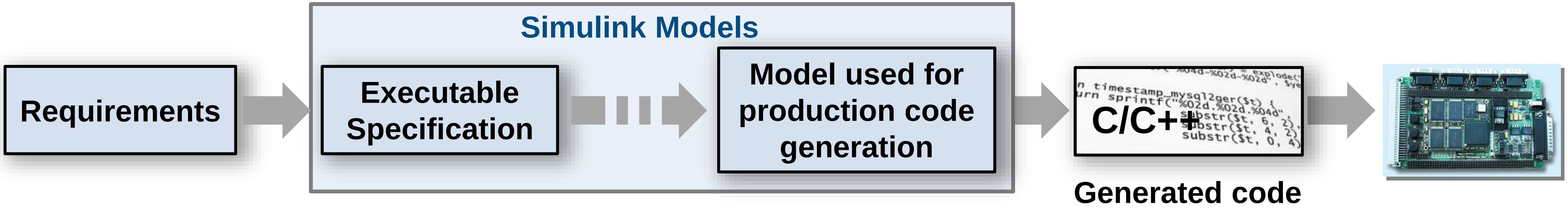
C/C++

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)



Simulink Models

Requirements

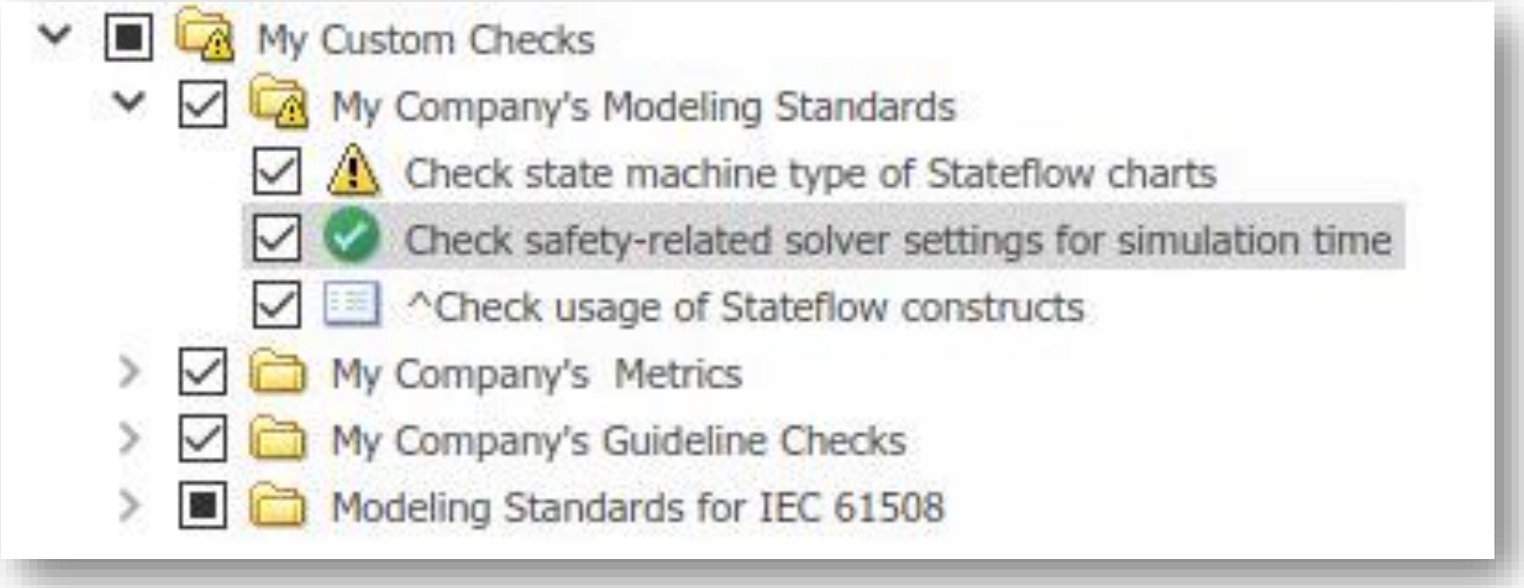
Executable Specification

Model used for production code generation

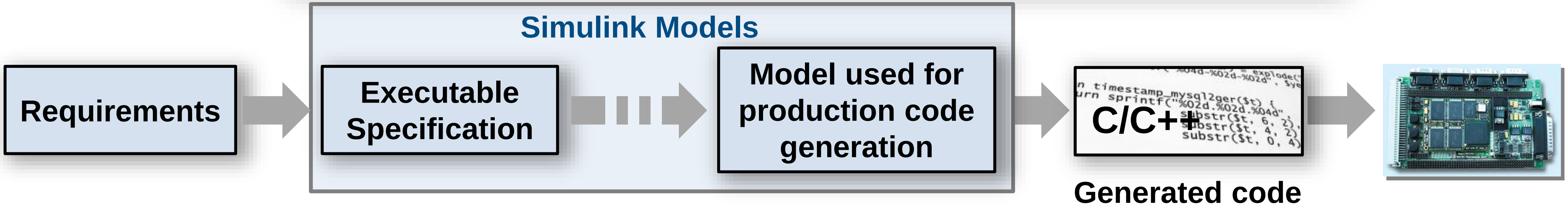
C/C++

Generated code

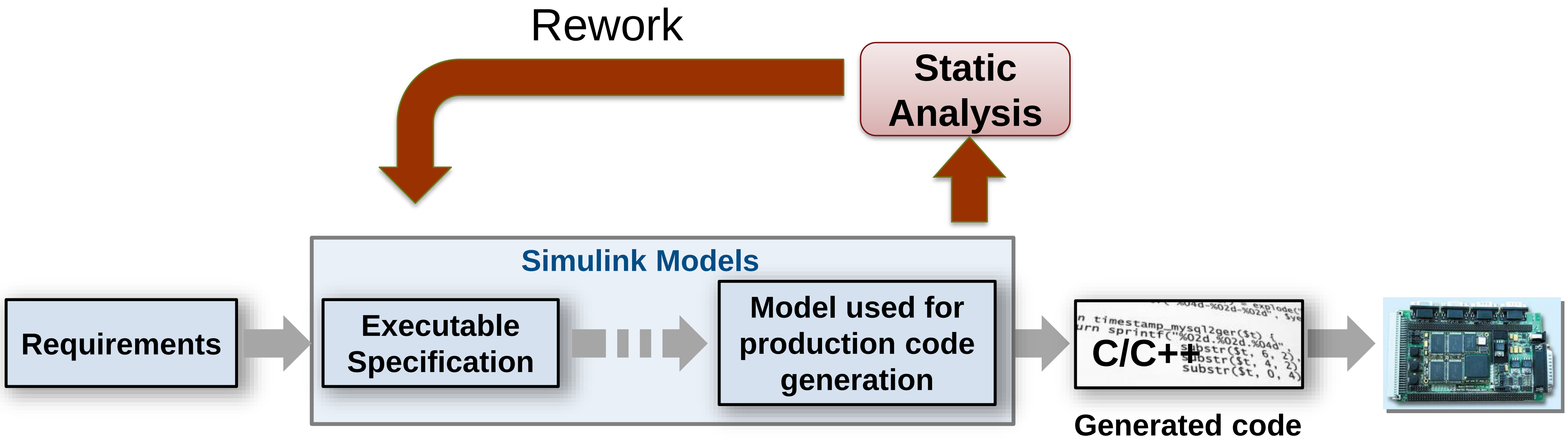
Custom checks for Your Best Practices and Guidlines



- ■ My Custom Checks
  - ☑ My Company's Modeling Standards
    - ☑ ⚠ Check state machine type of Stateflow charts
    - ☑ ✓ Check safety-related solver settings for simulation time
    - ☑ ^Check usage of Stateflow constructs
  - ☑ My Company's Metrics
  - ☑ My Company's Guideline Checks
  - ■ Modeling Standards for IEC 61508



Checks for standards and guidelines are often performed late



Rework

Static Analysis

Simulink Models

Requirements

Executable Specification

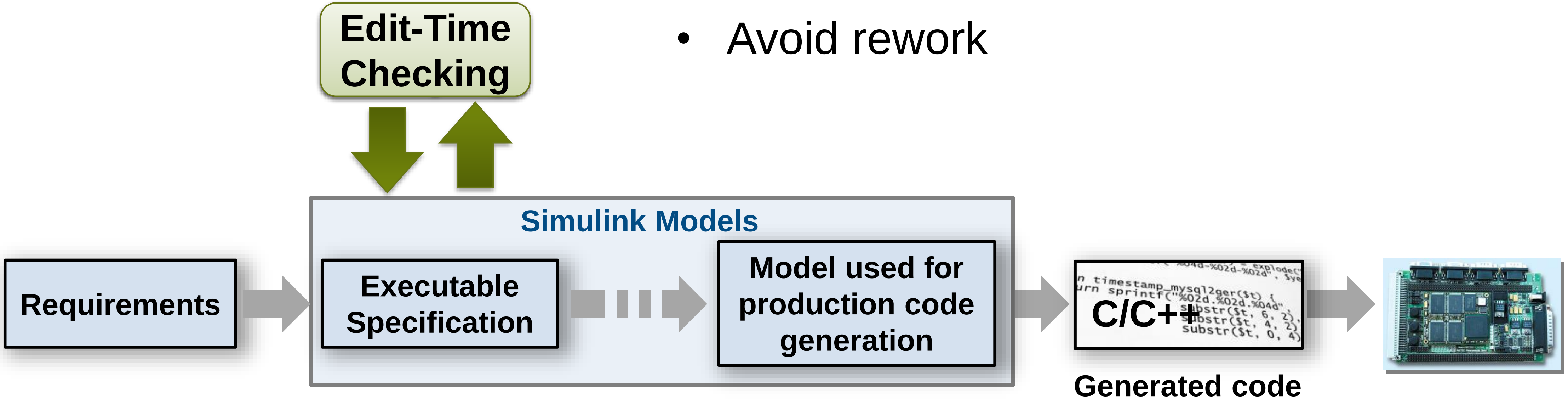
Model used for production code generation

C/C++

Generated code

Shift Verification Earlier With Edit-Time Checking

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



Edit-Time Checking

Simulink Models

Requirements

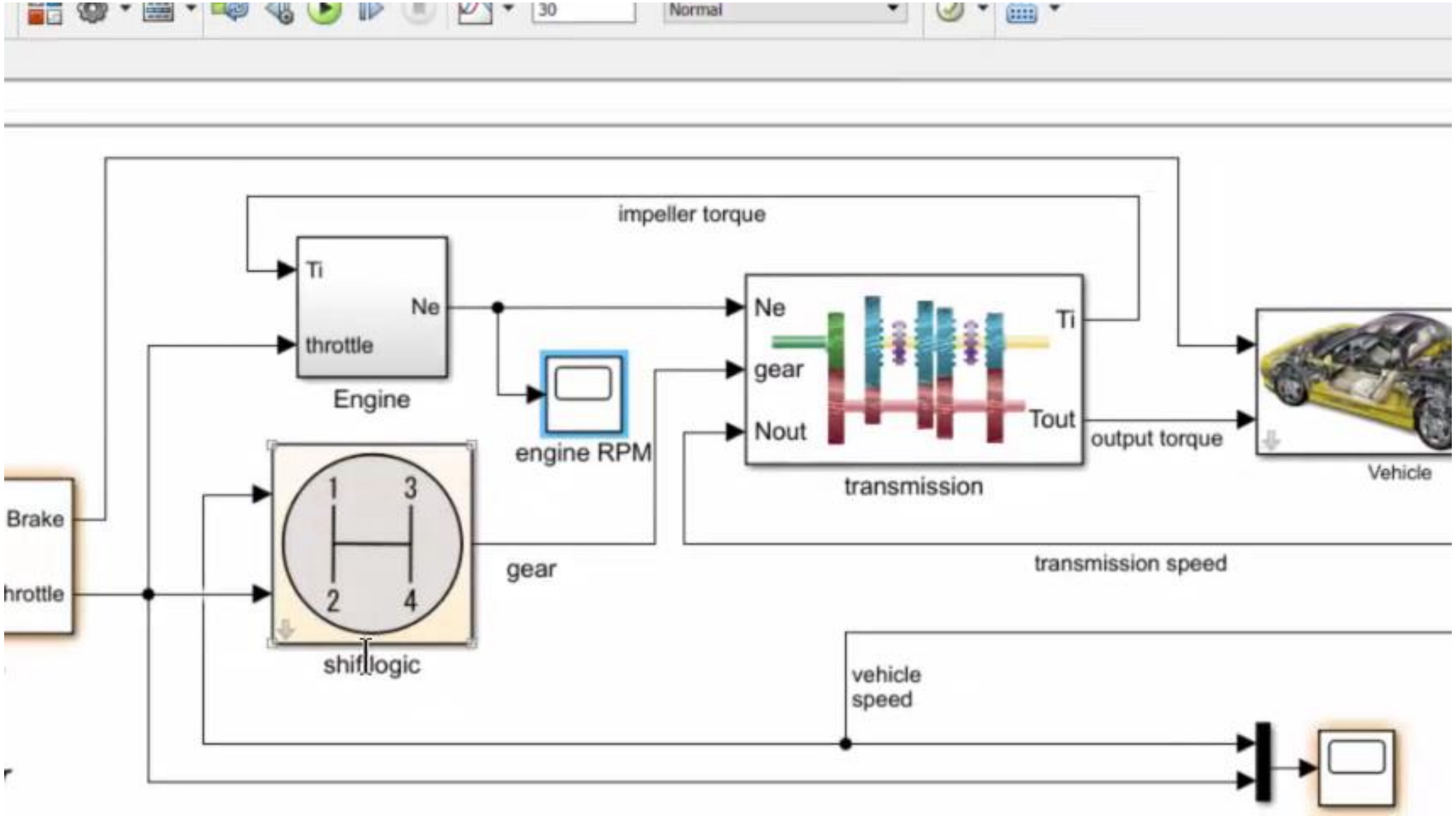
Executable Specification

Model used for production code generation

C/C++

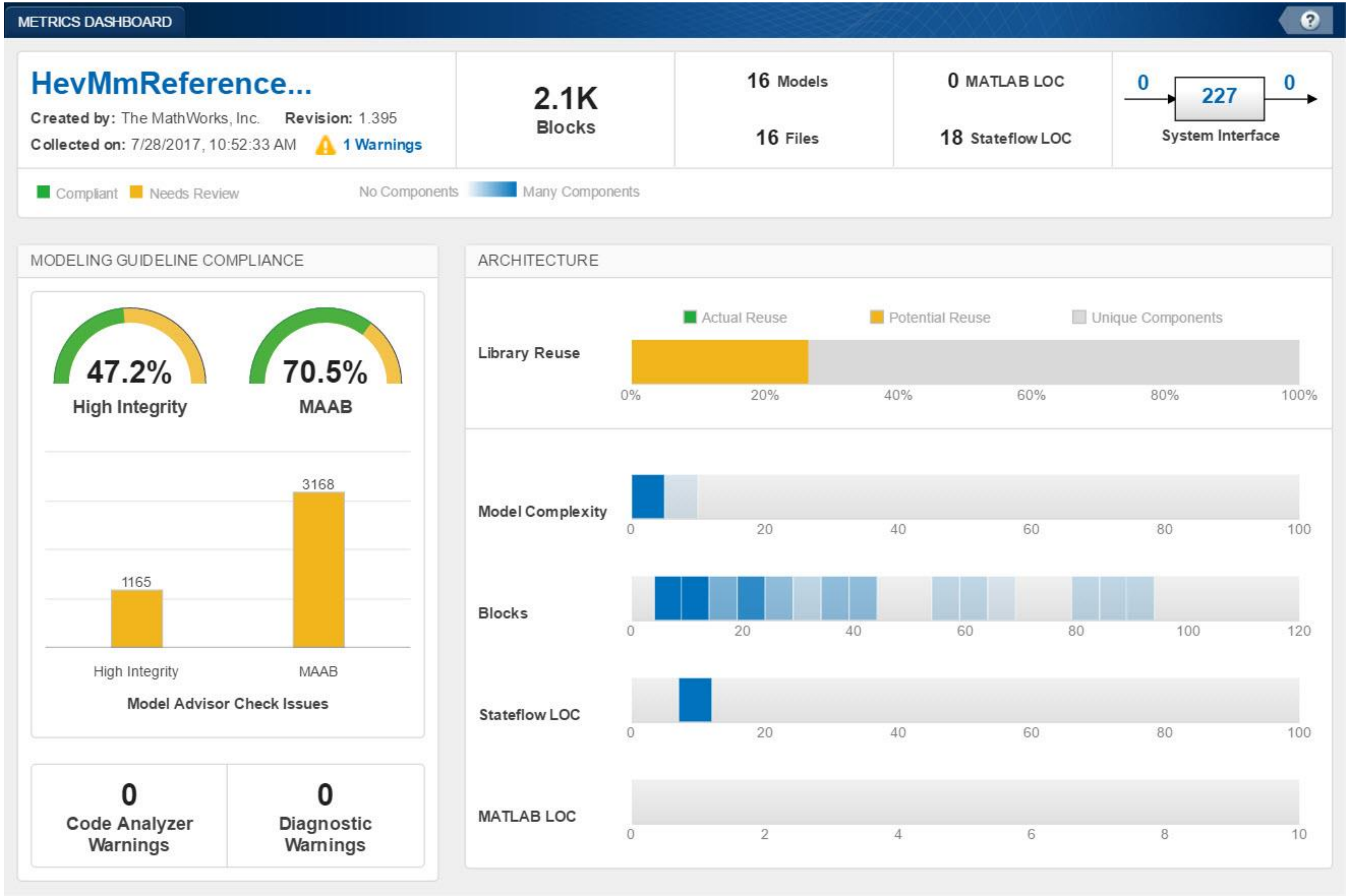
Generated code

Find Compliance Issues as you Edit with Edit-Time Checking



MATLAB EXPO 2018

Assess Quality with Metrics Dashboard



METRICS DASHBOARD

HevMmReference...

Created by: The MathWorks, Inc. **Revision:** 1.395

Collected on: 7/28/2017, 10:52:33 AM ⚠ 1 Warnings

2.1K Blocks

16 Models

16 Files

0 MATLAB LOC

18 Stateflow LOC

0 227 0 System Interface

🟩 Compliant 🟨 Needs Review

No Components – Many Components

MODELING GUIDELINE COMPLIANCE

47.2% High Integrity

70.5% MAAB

0 Code Analyzer Warnings

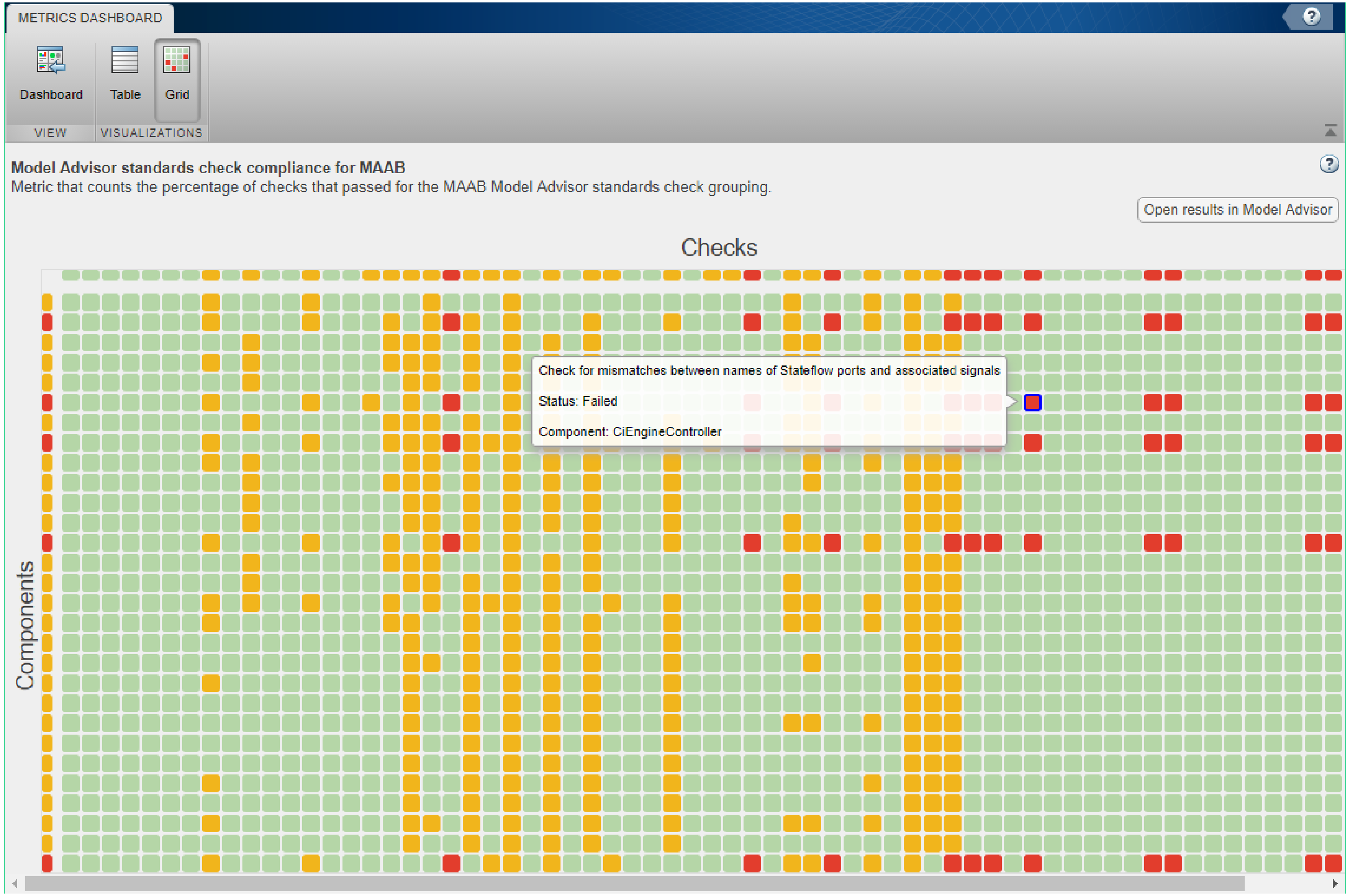
0 Diagnostic Warnings

ARCHITECTURE

- Consolidated view of metrics
  - Size
  - Compliance
  - Complexity

- Identify where problem areas may be

Grid Visualization for Metrics



Model Advisor standards check compliance for MAAB
Metric that counts the percentage of checks that passed for the MAAB Model Advisor standards check grouping.

Check for mismatches between names of Stateflow ports and associated signals

Status: Failed

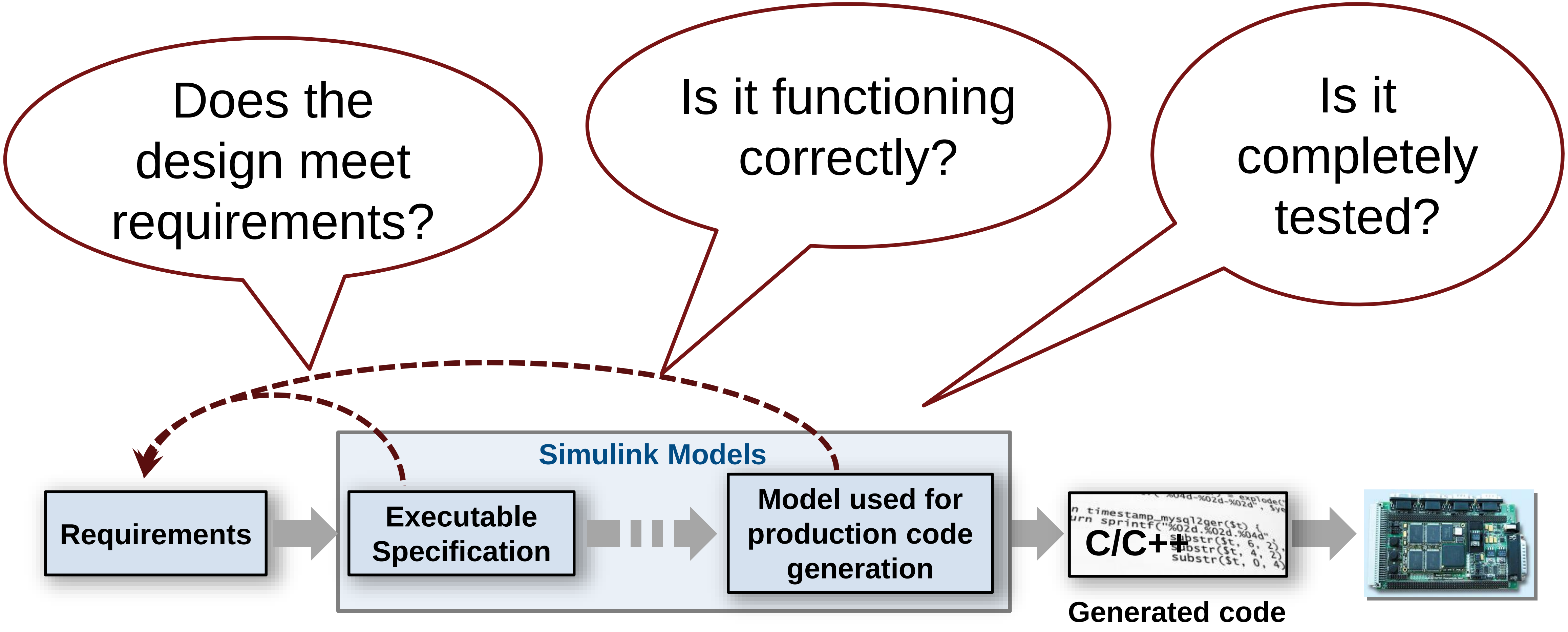
Component: CiEngineController

- 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

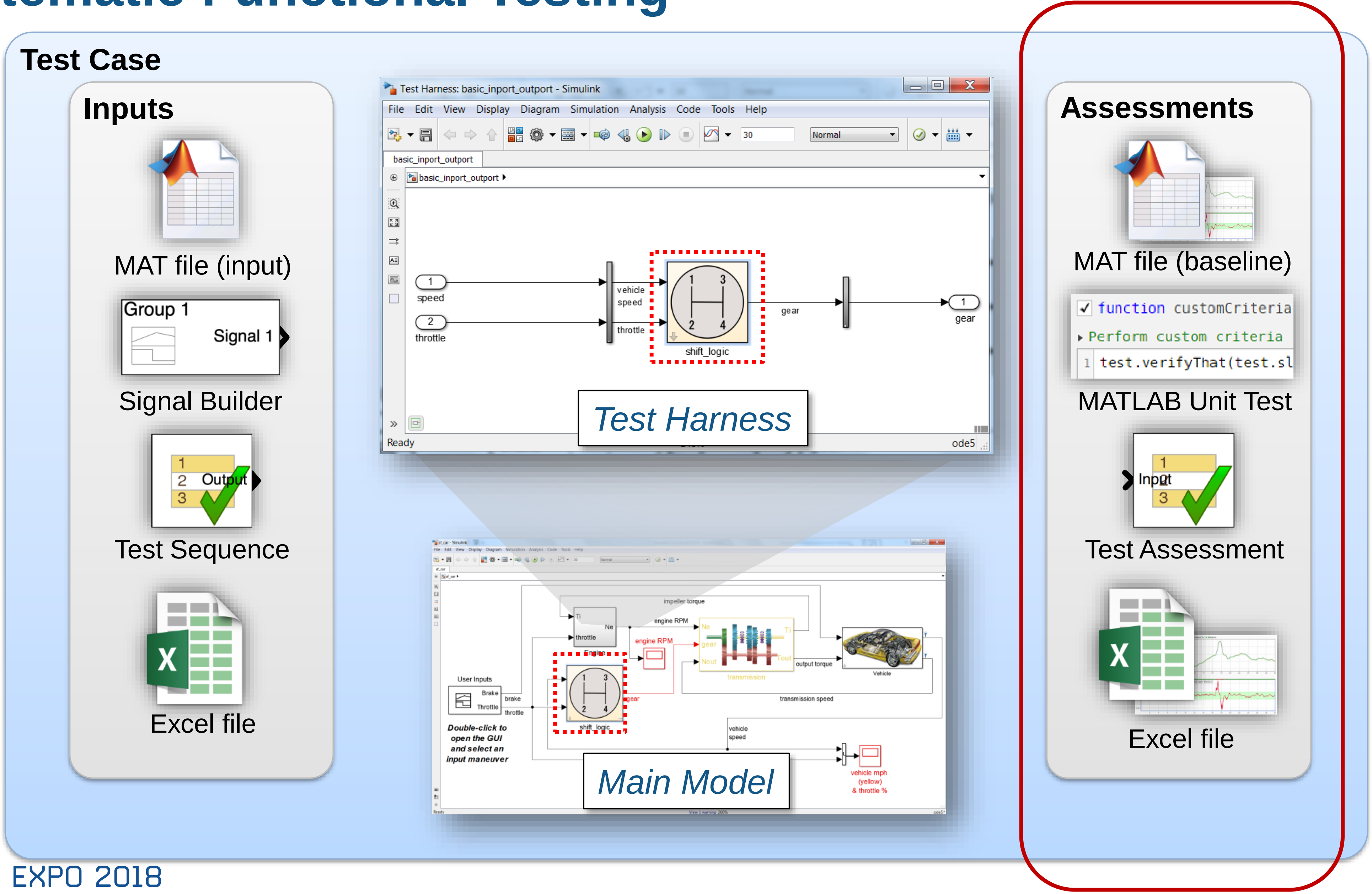
Executable Specification

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

Test Harness

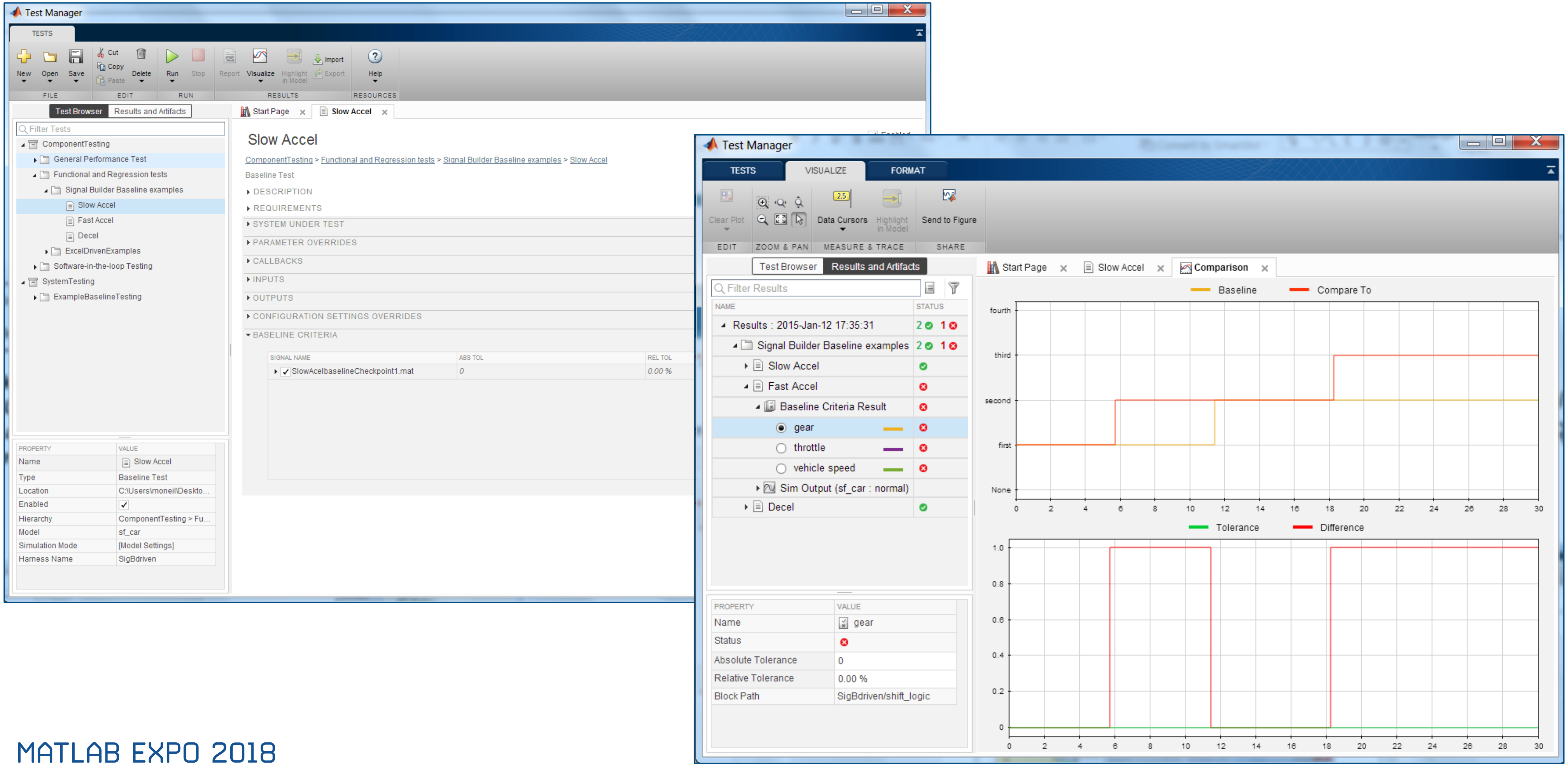
Main Model

Assessments

- MAT file (baseline)
- MATLAB Unit Test
- Test Assessment
- Excel file

```
function customCriteria
Perform custom criteria
test.verifyThat(test.sl
```

Manage Testing and Test Results



Slow Accel

ComponentTesting > Functional and Regression tests > Signal Builder Baseline examples > Slow Accel

Baseline Test

SIGNAL NAME	ABS TOL	REL TOL
☑ SlowAccelbaselineCheckpoint1.mat	0	0.00 %

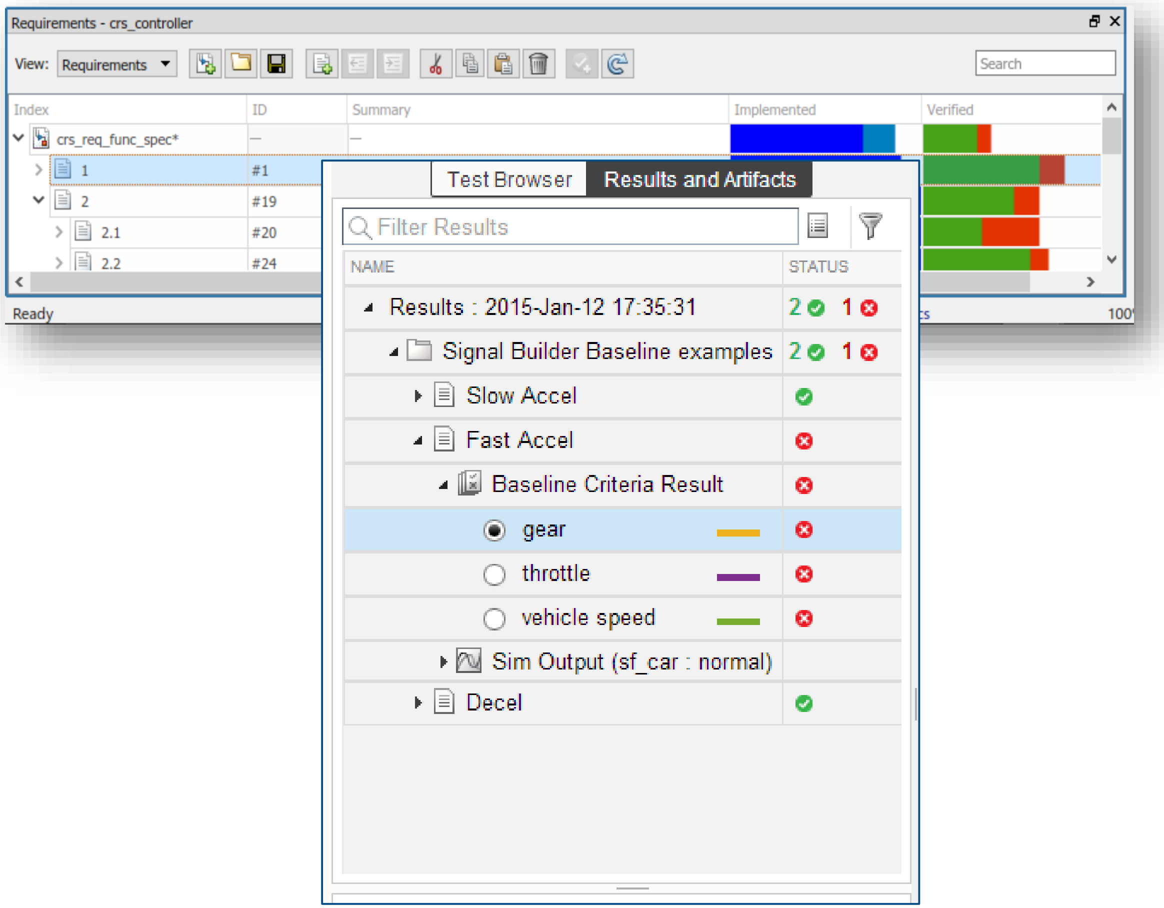
PROPERTY	VALUE
Name	Slow Accel
Type	Baseline Test
Location	C:\Users\moneil\Deskto...
Enabled	✓
Hierarchy	ComponentTesting > Fu...
Model	sf_car
Simulation Mode	[Model Settings]
Harness Name	SigBdriven

NAME	STATUS
Results : 2015-Jan-12 17:35:31	2 ✓ 1 ✗
Signal Builder Baseline examples	2 ✓ 1 ✗
Slow Accel	✓
Fast Accel	✗
Baseline Criteria Result	✗
● gear	✗
○ throttle	✗
○ vehicle speed	✗
Sim Output (sf_car : normal)	
Decel	✓

PROPERTY	VALUE
Name	gear
Status	✗
Absolute Tolerance	0
Relative Tolerance	0.00 %
Block Path	SigBdriven/shift_logic

MATLAB EXPO 2018

Assess Test Completness



Requirements - crs_controller

View: Requirements

Index	ID	Summary	Implemented	Verified
crs_req_func_spec*	—	—	🟦	🟩🟥
1	#1			🟩🟥
2	#19			🟩🟥
2.1	#20			🟩🟥
2.2	#24			🟩🟥

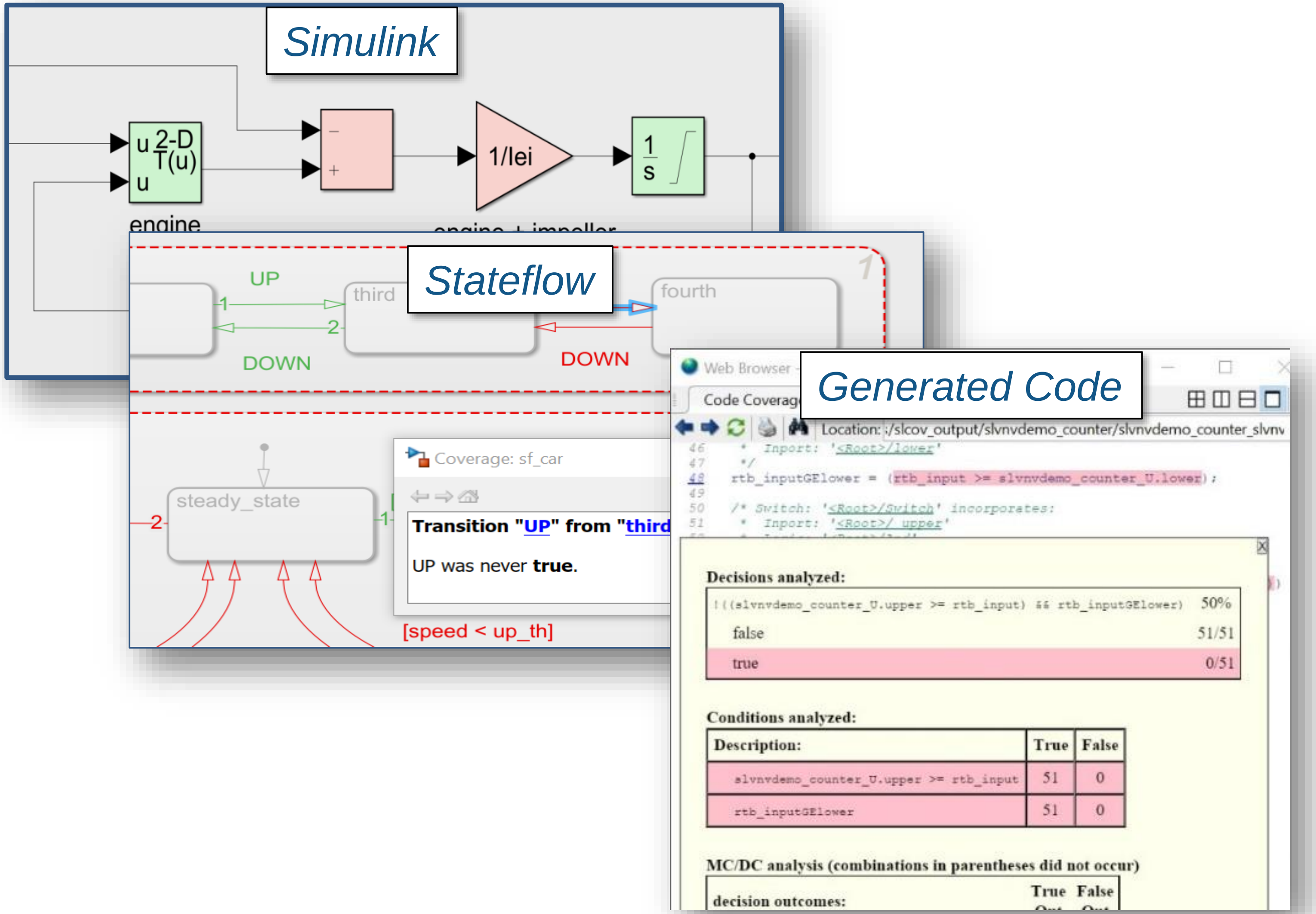
Ready

NAME	STATUS
Results : 2015-Jan-12 17:35:31	2 ✓ 1 ✗
Signal Builder Baseline examples	2 ✓ 1 ✗
Slow Accel	✓
Fast Accel	✗
Baseline Criteria Result	✗
● gear	✗
○ throttle	✗
○ vehicle speed	✗
Sim Output (sf_car : normal)	
Decel	✓

Measure Structural Coverage

- Condition
- Decision
- MCDC
- …

Assess Test Completness – Coverage Analysis



Coverage: sf_car

Transition "UP" from "third

UP was never **true**.

Location: :/slcov_output/slvnvdemo_counter/slvnvdemo_counter_slvnv

```
 *  Inport: '<Root>/lower'
 */
rtb_inputGElower = (rtb_input >= slvnvdemo_counter_U.lower);

/* Switch: '<Root>/Switch' incorporates:
 *  Inport: '<Root>/ upper'
```

Decisions analyzed:

!((slvnvdemo_counter_U.upper >= rtb_input) && rtb_inputGElower)	50%
false	51/51
true	0/51

Conditions analyzed:

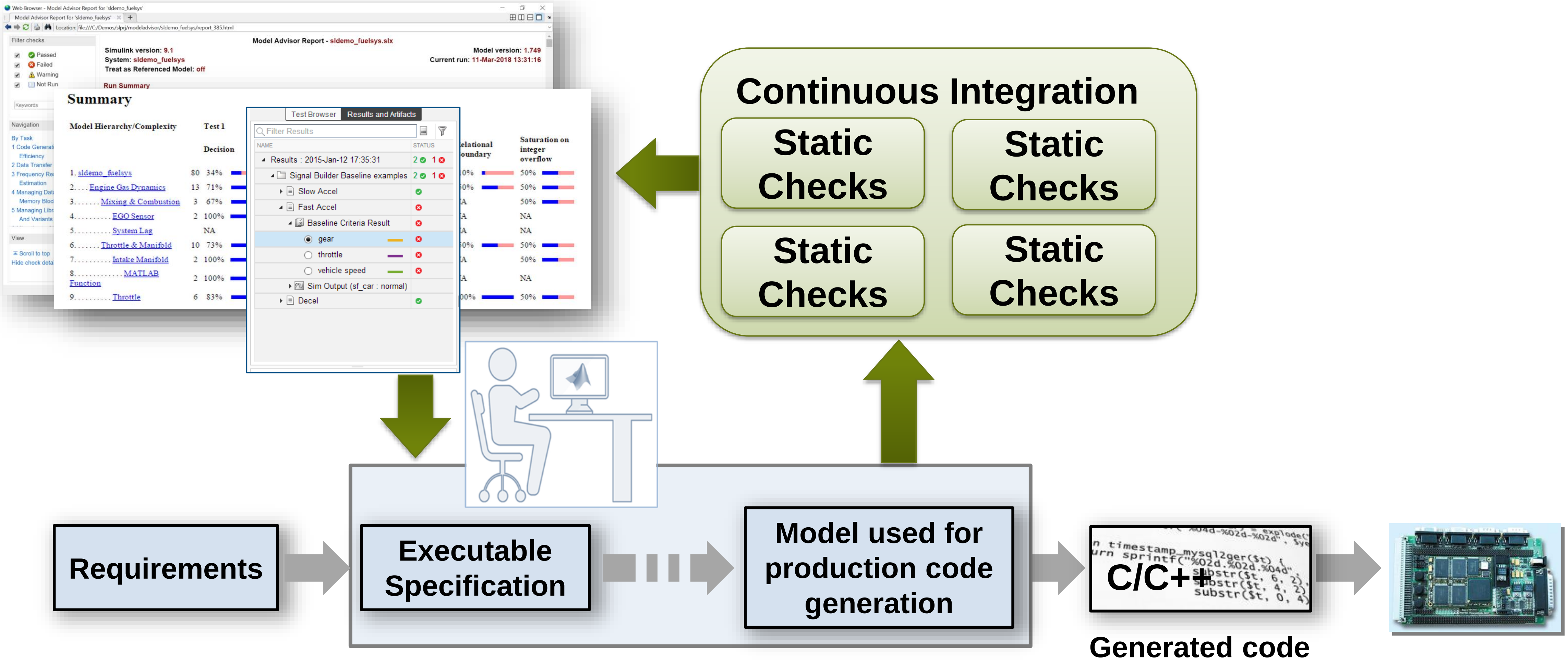
Description:	True	False
slvnvdemo_counter_U.upper >= rtb_input	51	0
rtb_inputGElower	51	0

MC/DC analysis (combinations in parentheses did not occur)

decision outcomes:	True Out	False Out

- Identify testing gaps
- Missing requirements
- Unintended Functionality

Continuous Automated Feedback



Web Browser - Model Advisor Report for 'sldemo_fuelsys'

Model Advisor Report for 'sldemo_fuelsys'

Location: file:///C:/Demos/slprj/modeladvisor/sldemo_fuelsys/report_385.html

Filter checks
☑ Passed
☑ Failed
☑ Warning
☑ Not Run

Keywords

Navigation
By Task
1 Code Generati
Efficiency
2 Data Transfer
3 Frequency Res
Estimation
4 Managing Data
Memory Block
5 Managing Libr
And Variants

View
Scroll to top
Hide check detai

Model Advisor Report - sldemo_fuelsys.slx

Simulink version: 9.1
System: sldemo_fuelsys
Treat as Referenced Model: off

Model version: 1.749
Current run: 11-Mar-2018 13:31:16

Run Summary

Summary

Model Hierarchy/Complexity		Test 1 Decision	elational oundary	Saturation on integer overflow
1. sldemo_fuelsys	80	34%	0%	50%
2. . . . Engine Gas Dynamics	13	71%	0%	50%
3. . . . . . . Mixing & Combustion	3	67%	A	50%
4. . . . . EGO Sensor	2	100%	A	NA
5. . . . . System Lag		NA	A	NA
6. . . . . . . Throttle & Manifold	10	73%	0%	50%
7. . . . . Intake Manifold	2	100%	A	50%
8. . . . . MATLAB Function	2	100%	A	NA
9. . . . . Throttle	6	83%	00%	50%

Test Browser | Results and Artifacts

Filter Results

NAME	STATUS
Results : 2015-Jan-12 17:35:31	2 ✓ 1 ✗
Signal Builder Baseline examples	2 ✓ 1 ✗
Slow Accel	✓
Fast Accel	✗
Baseline Criteria Result	✗
● gear	✗
○ throttle	✗
○ vehicle speed	✗
Sim Output (sf_car : normal)	
Decel	✓

Continuous Integration

Static Checks

Static Checks

Static Checks

Static Checks

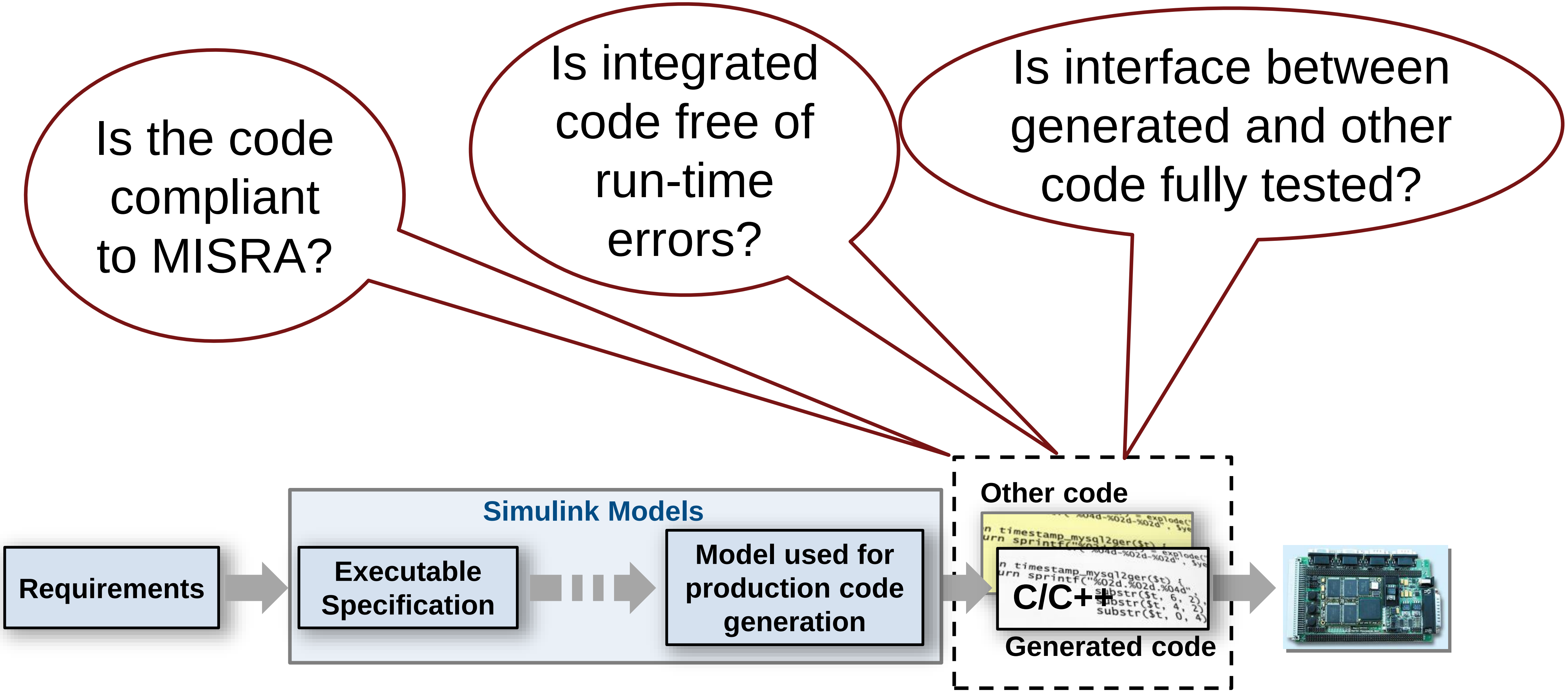
Requirements

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?

Requirements

Simulink Models

Executable Specification

Model used for production code generation

Other code

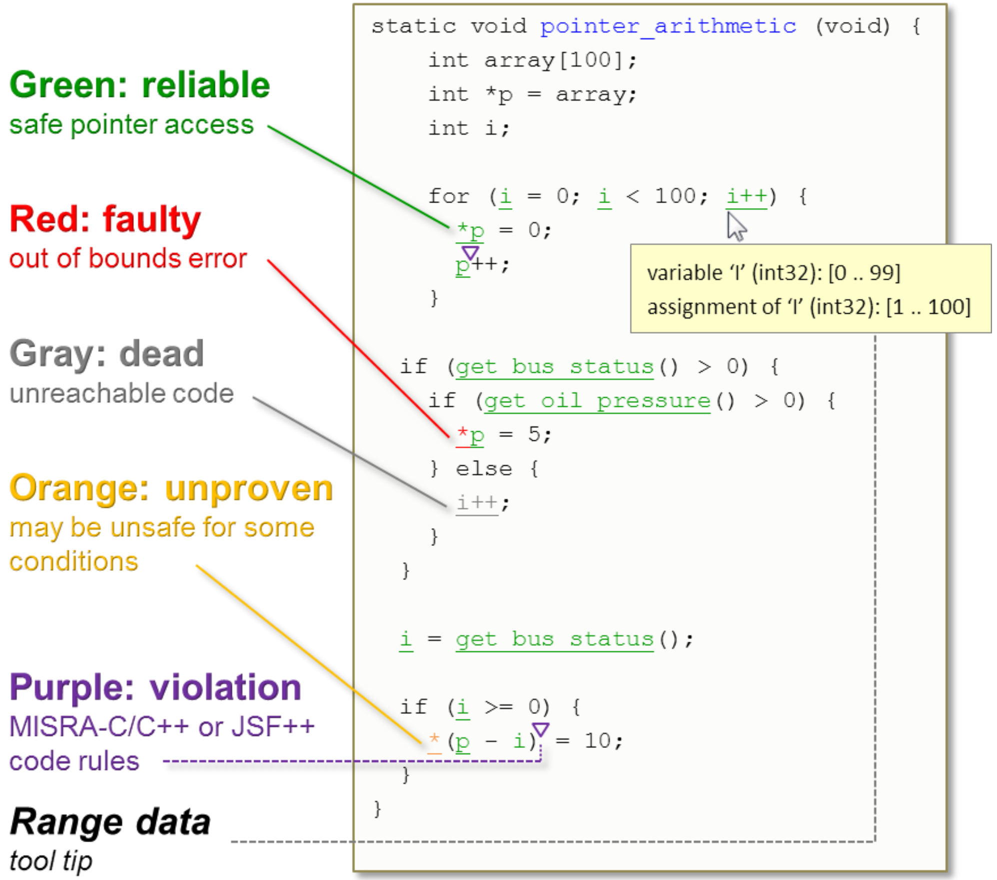
C/C++

Generated code

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



Green: reliable
safe pointer access

Red: faulty
out of bounds error

Gray: dead
unreachable code

Orange: unproven
may be unsafe for some conditions

Purple: violation
MISRA-C/C++ or JSF++ code rules

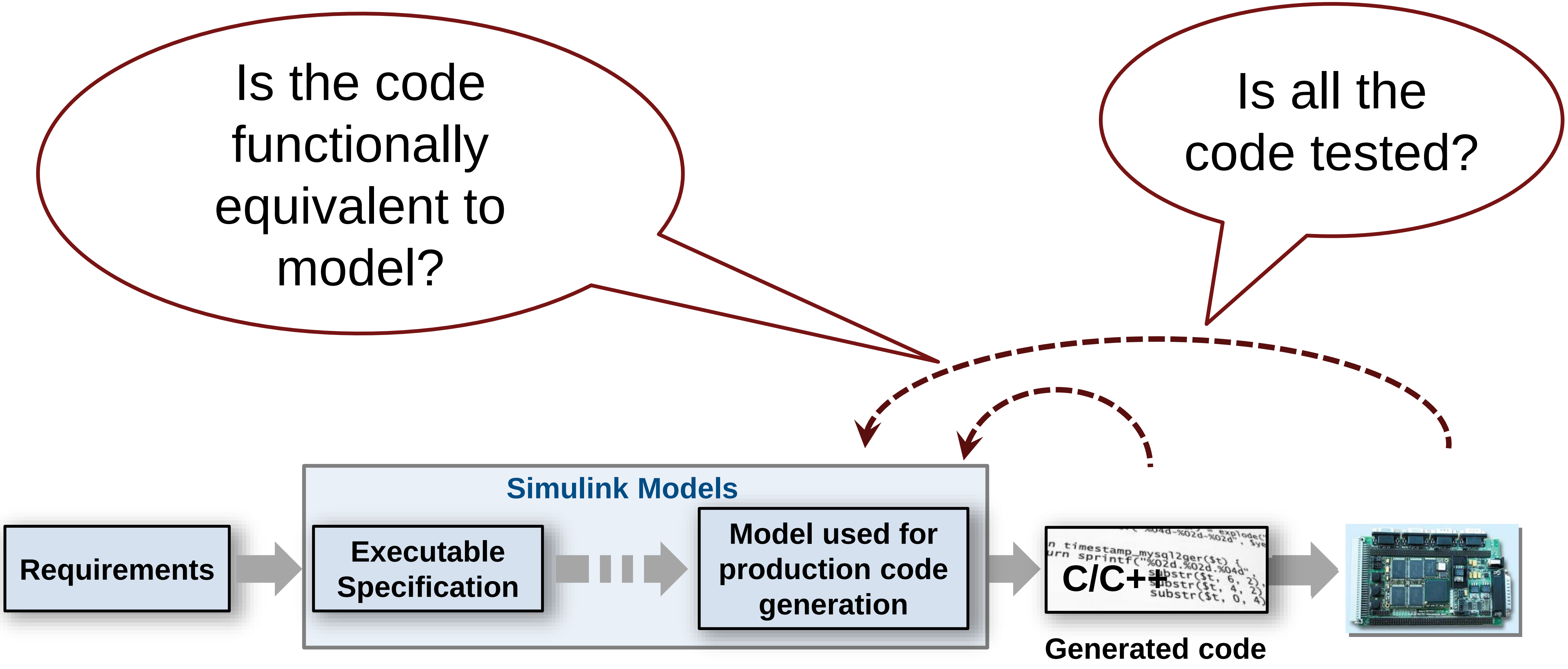
Range data
tool tip

```
static void pointer_arithmetic (void) {
    int array[100];
    int *p = array;
    int i;

    for (i = 0; i < 100; i++) {
      *p = 0;
      p++;
    }

  if (get_bus_status() > 0) {
    if (get_oil_pressure() > 0) {
      *p = 5;
    } else {
      i++;
    }
  }

  i = get_bus_status();

  if (i >= 0) {
    *(p - i) = 10;
  }
}
```

variable ‘I’ (int32): [0 .. 99]
assignment of ‘I’ (int32): [1 .. 100]

Results from Polyspace Code Prover

Equivalence Testing



Is the code functionally equivalent to model?

Is all the code tested?

Requirements

Simulink Models

Executable Specification

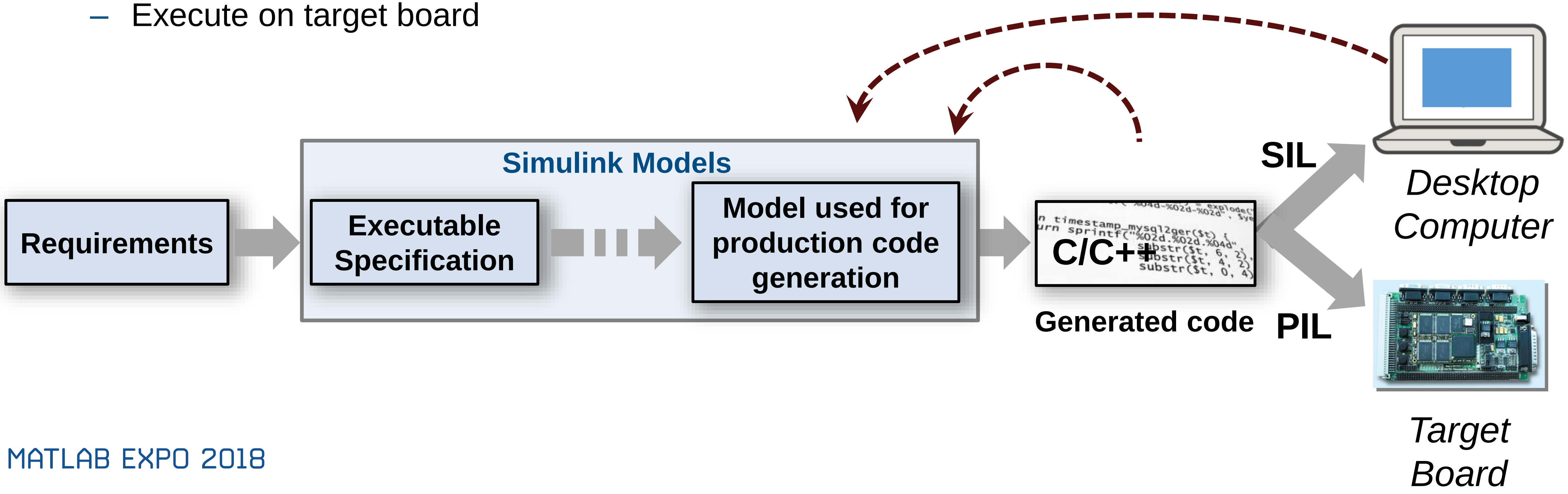
Model used for production code generation

C/C++

Generated code

Equivalence Testing

- Software in the Loop (SIL)
  - Show functional equivalence, model to code
  - Execute on desktop / laptop computer
- Re-use tests developed for model to test code
- Collect code coverage
- Processor in the Loop (PIL)
  - Numerical equivalence, model to target code
  - Execute on target board



Simulink Models

Requirements

Executable Specification

Model used for production code generation

C/C++

Generated code

SIL

PIL

Desktop Computer

Target Board

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

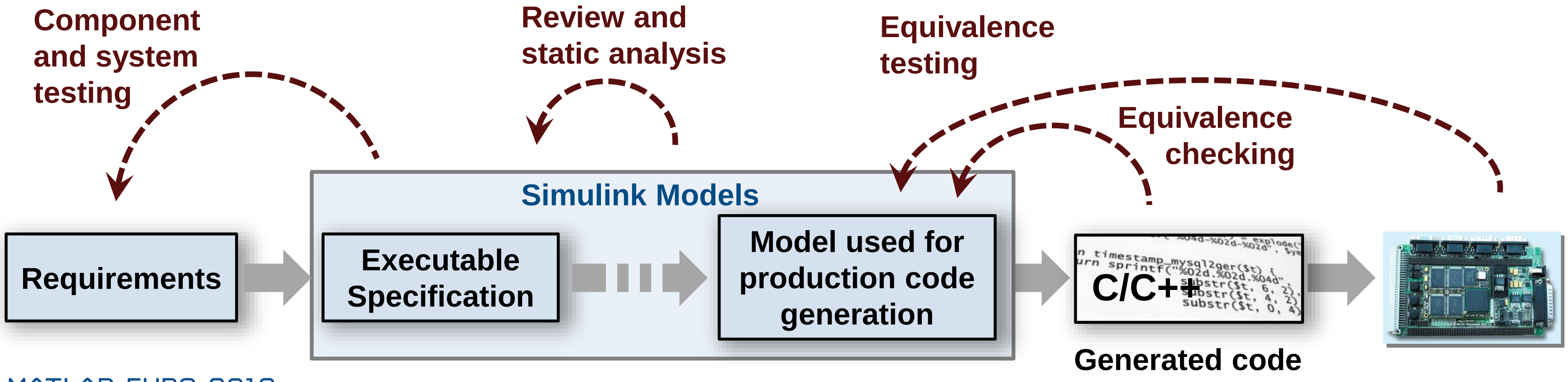
Kostal's electronic steering column lock module.

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

Primary flight control computers from BAE Systems.

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

Thank You!