MATLAB EXPO 2018

自动化提高设计质量的最佳实践

吴菁

嵌入式系统日益增长的复杂性

紧急制动

车身控制模块

语音识别

电动窗

Vehicle-to-Infrastructure

电动尾门

电动座椅

后备摄像头

长距雷达

全驱

稳定性控制

自适应巡航控制

自动泊车

4 轮转向

电池管理

智能接线盒

电动助力转向

仪表盘

气囊

发动机管理

信息娱乐系统

DC/DC Converter

推进电机控制

导航

传动控制

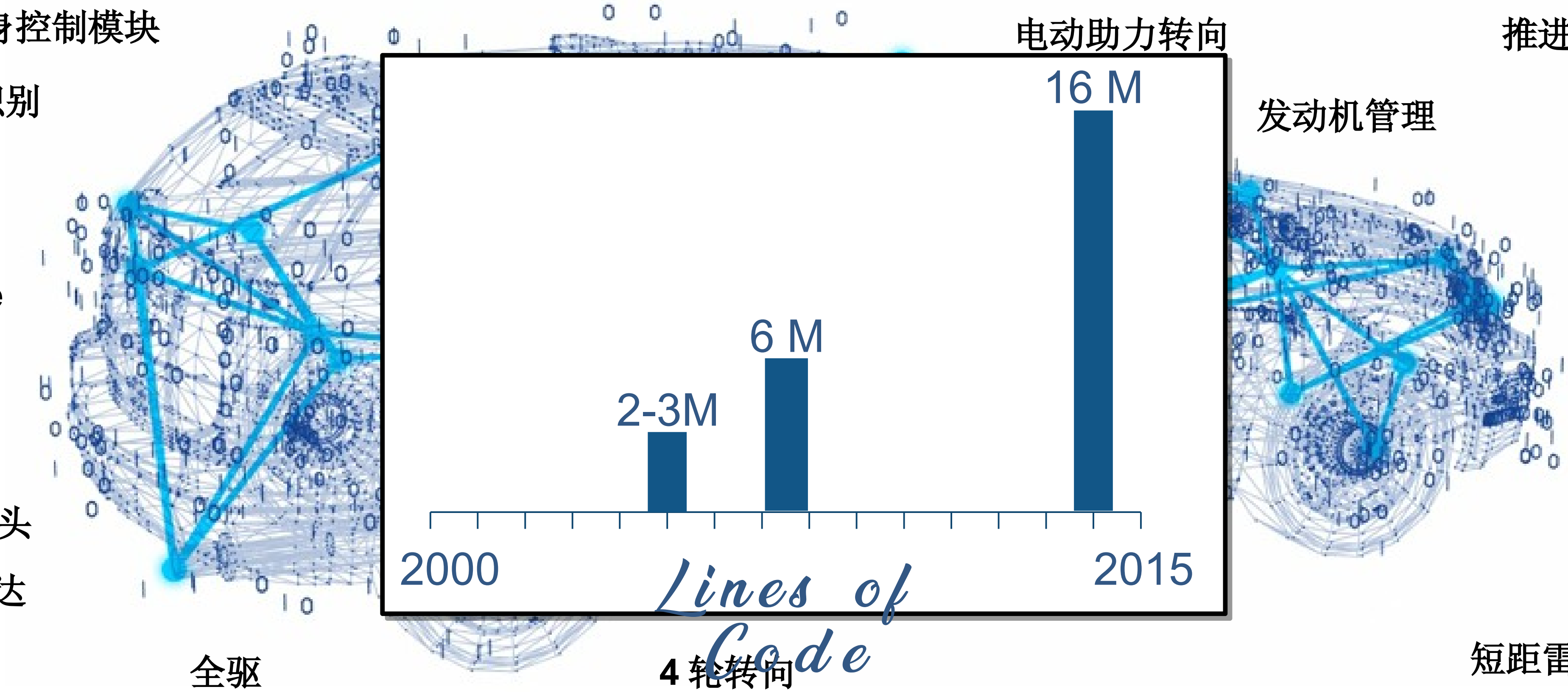
前向摄像头

自适应前向大灯

HVAC 控制

无钥匙进入

短距雷达



Siemens, “Ford Motor Company Case Study,” Siemens PLM Software, 2014
McKendrick, J. “Cars become ‘datacenters on wheels’, carmakers become software companies,” ZDJNet, 2013

为什么高达71%的嵌入式项目以失败告终？

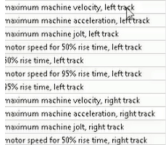
需求管理的匮乏

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

要点

- 在 Simulink 中创建，管理需求
- 早期验证以便快速发现错误
- 自动化手工验证任务
- 遵循安全标准的流程

System Requirements



maximum machine velocity, left track
maximum machine acceleration, left track
maximum machine jolt, left track
motor speed for 50% rise time, left track
50% rise time, left track
motor speed for 95% rise time, left track
95% rise time, left track
maximum machine velocity, right track
maximum machine acceleration, right track
maximum machine jolt, right track
motor speed for 50% rise time, right track

High Level Design

Detailed Design

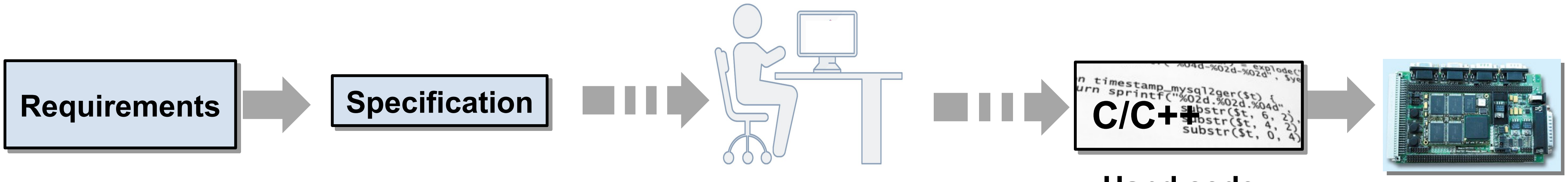
Unit Testing

Integration Testing

Verified & Valida System

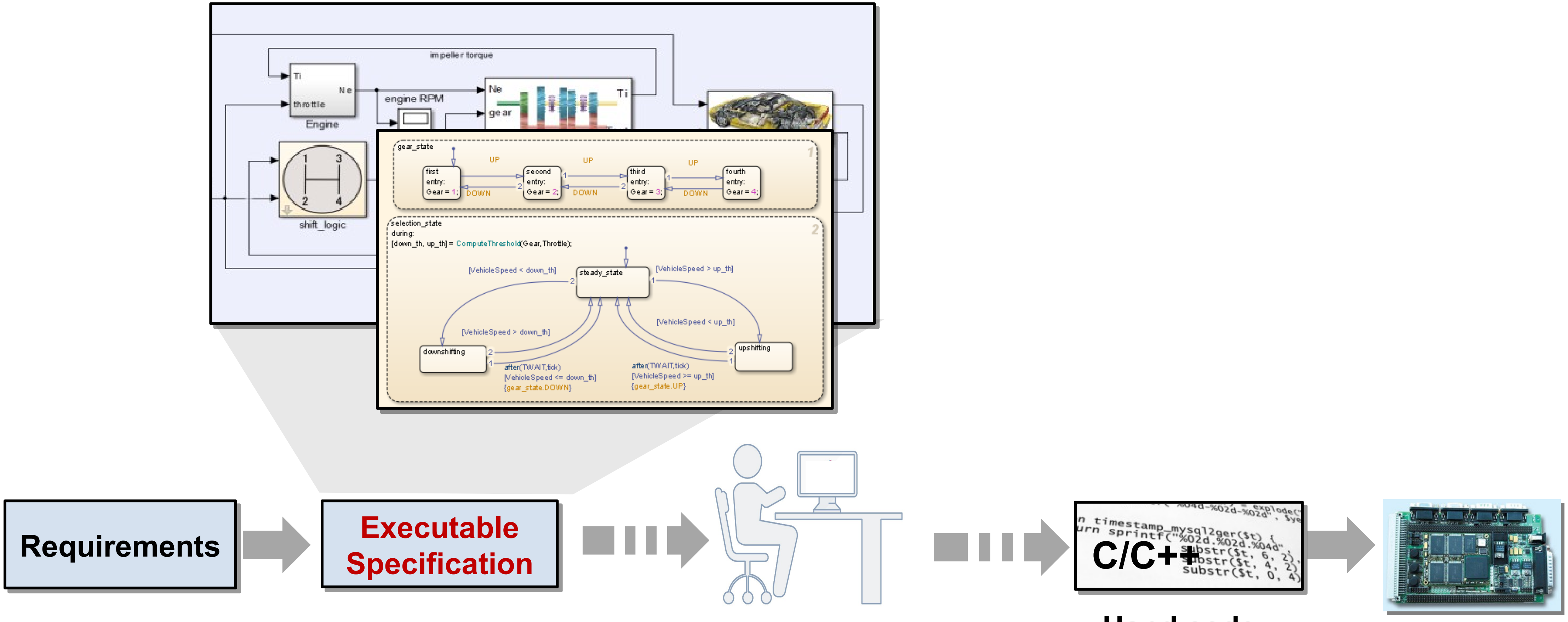
“ 通过早期验证降低成本和项目风险，缩短认证系统的上市时间并提供第一时间即正确的高质量产品代码”
Michael Schwarz, ITK Engineering

传统开发流程的挑战



Hand code

将 Simulink 模型作为规范



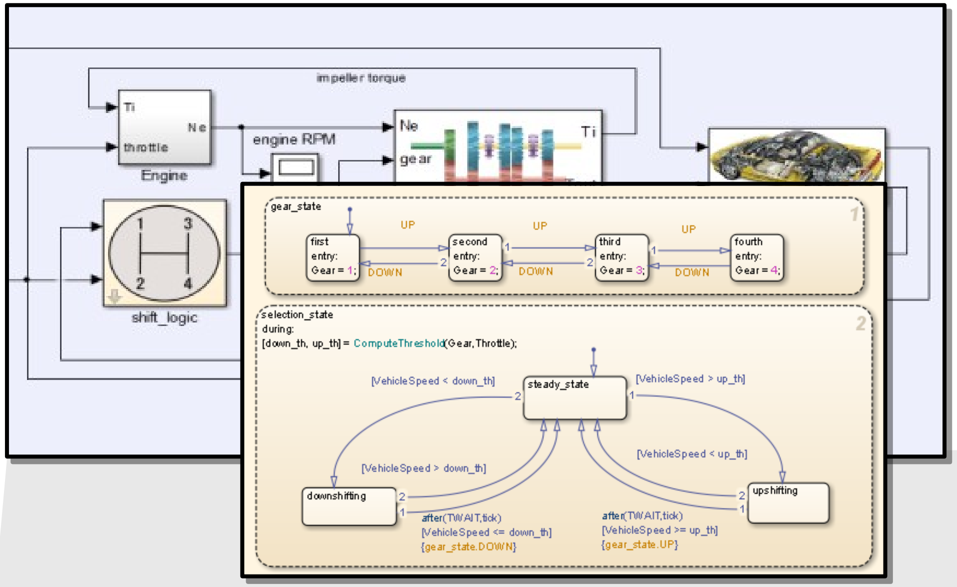
Requirements

Executable Specification

C/C++

Hand code

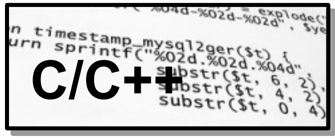
完整的基于模型的设计



Code Generation

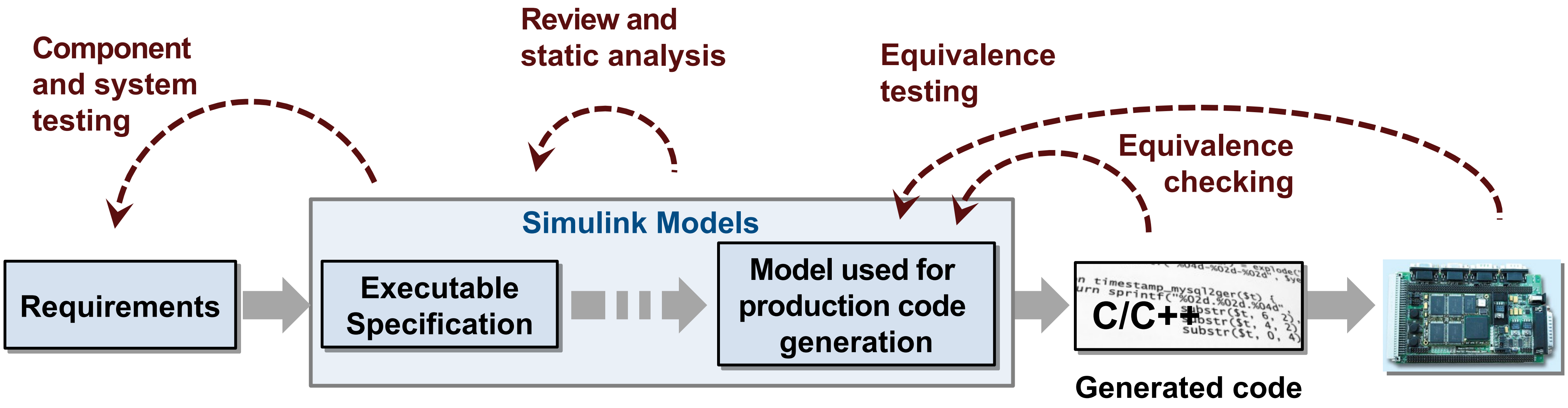
Simulink Models

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



Generated code

基于模型设计的验证流程



Component and system testing

Review and static analysis

Equivalence testing

Equivalence checking

Simulink Models

Requirements

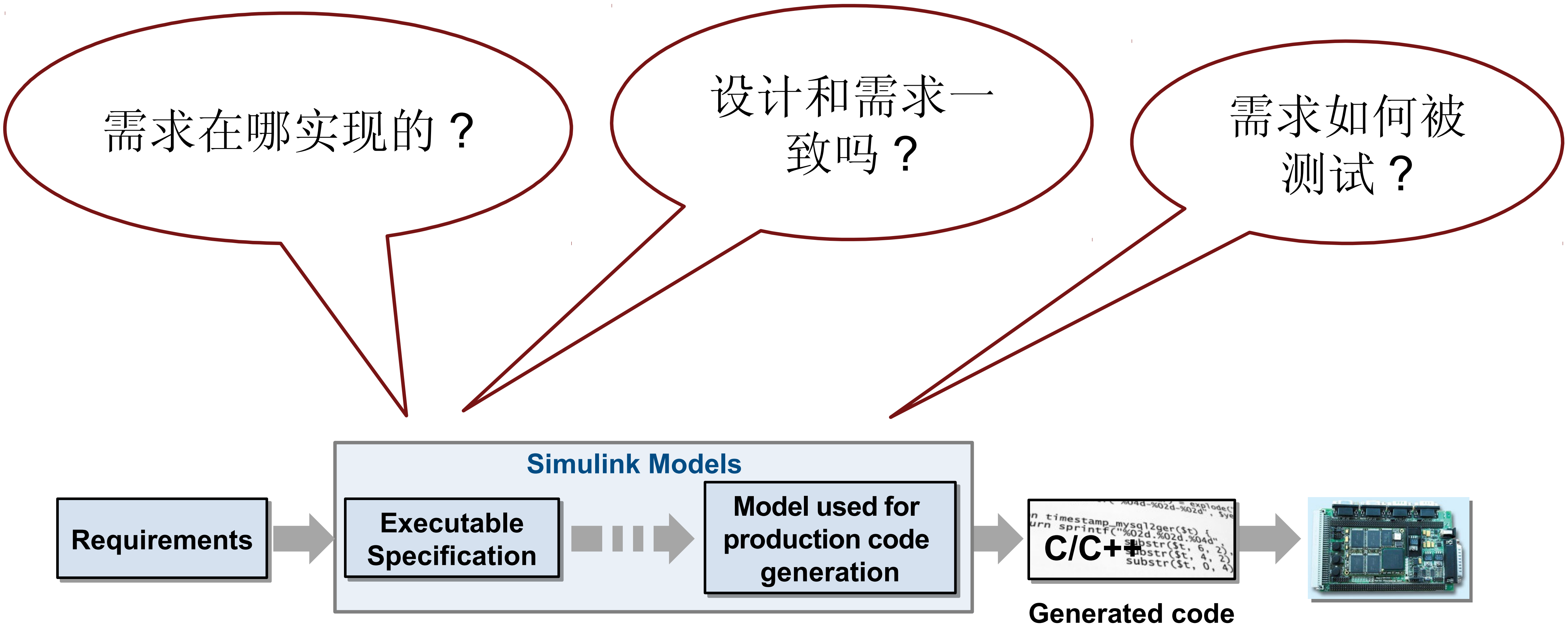
Executable Specification

Model used for production code generation

C/C++

Generated code

来自需求的挑战



需求在哪实现的？

设计和需求一致吗？

需求如何被测试？

Simulink Models

Requirements

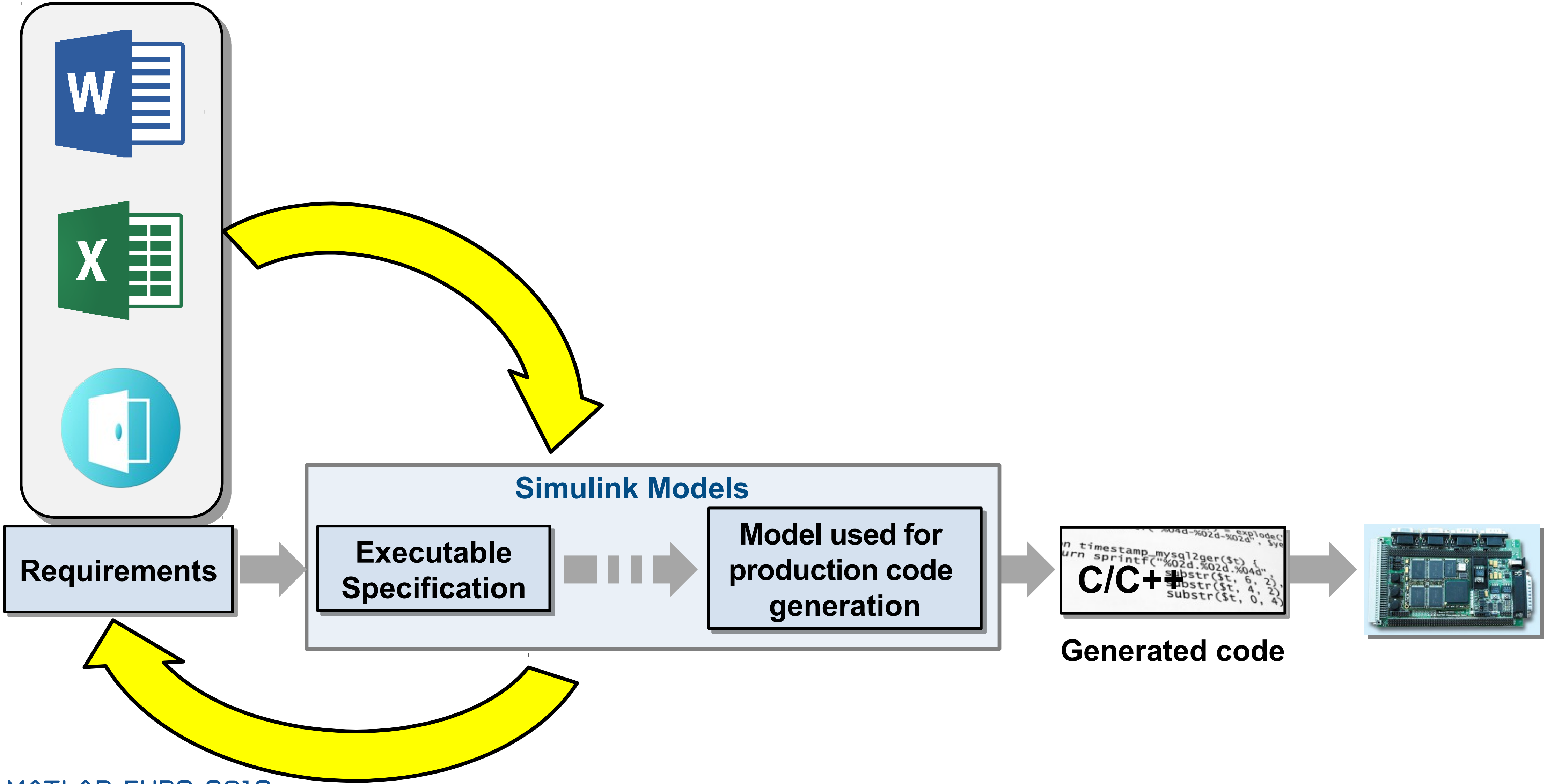
Executable Specification

Model used for production code generation

C/C++

Generated code

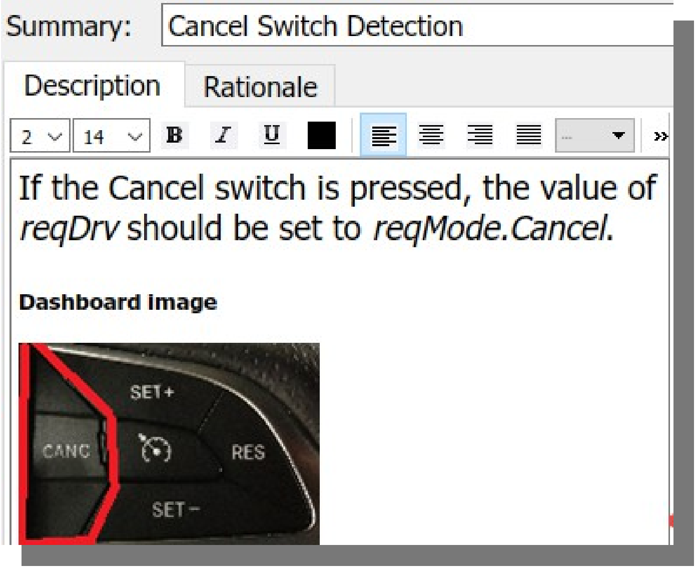
需求和设计之间的缺口


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

Simulink Requirements

R2017b

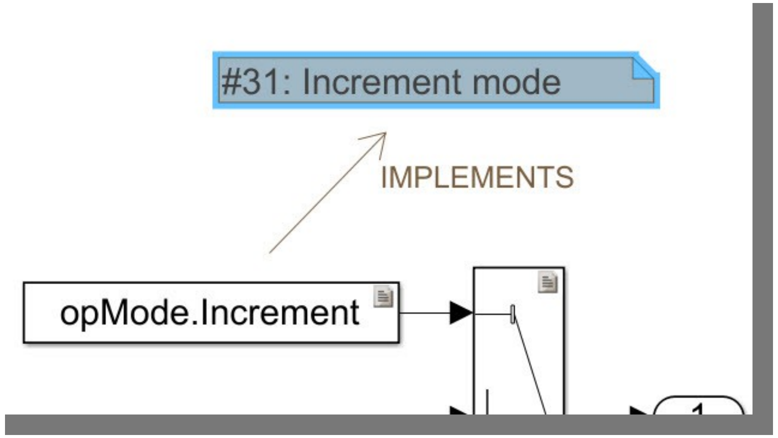
Author



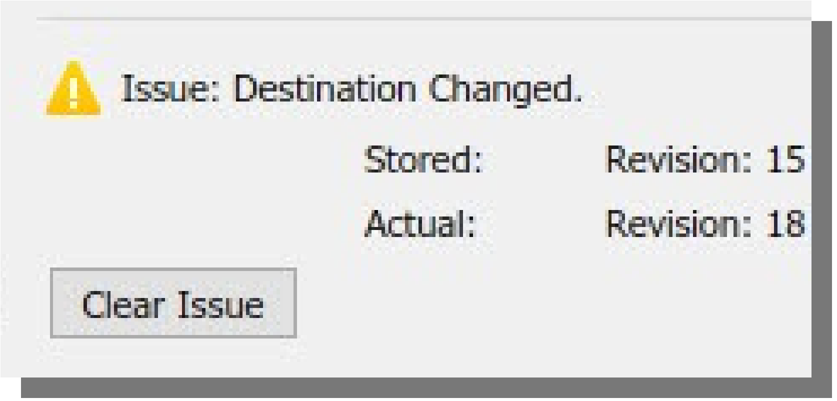
Summary: Cancel Switch Detection

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

Track



Manage

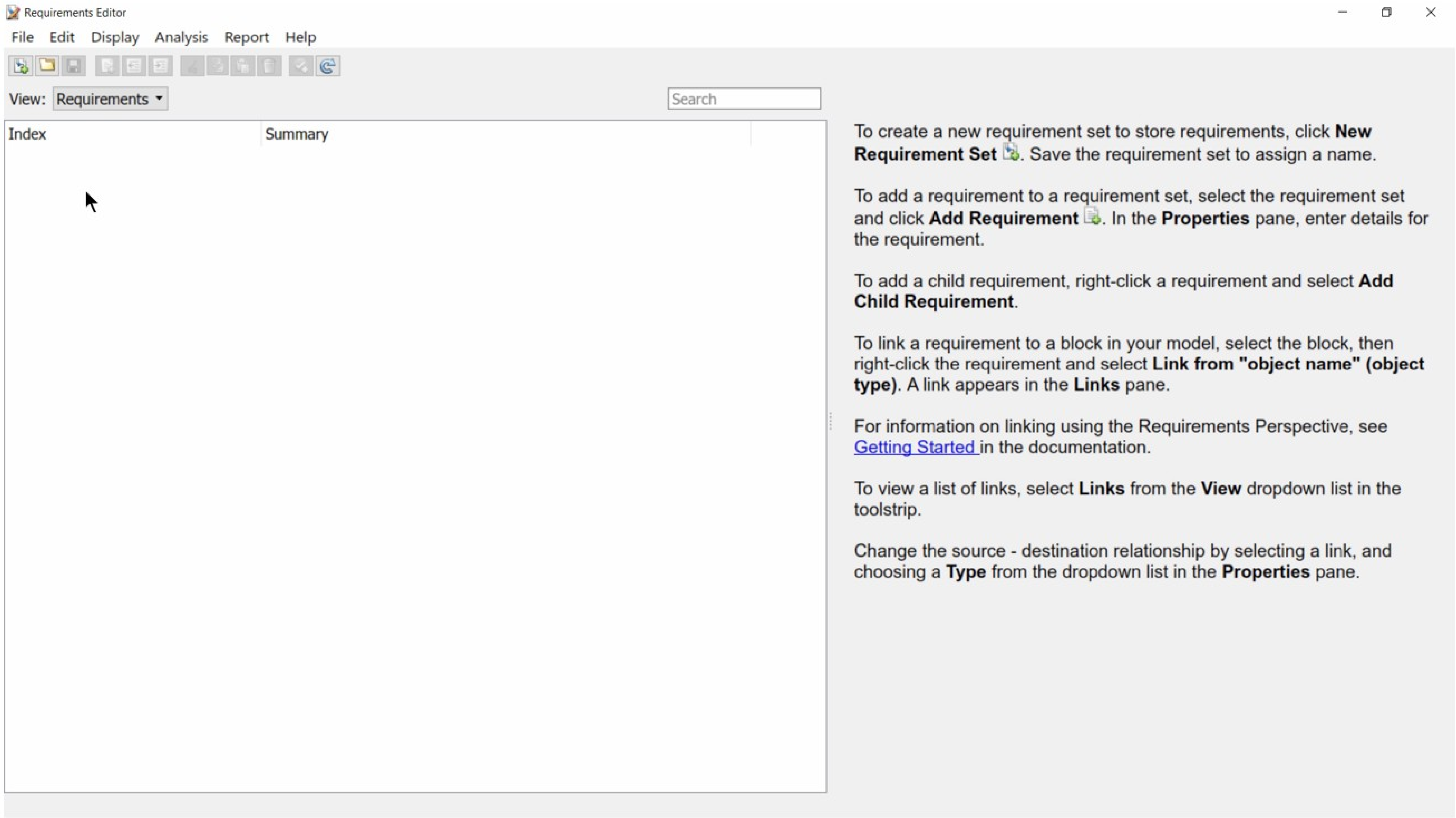


Issue: Destination Changed.

Stored: Revision: 15

Actual: Revision: 18

Requirements Editor



To create a new requirement set to store requirements, click **New Requirement Set**. Save the requirement set to assign a name.

To add a requirement to a requirement set, select the requirement set and click **Add Requirement**. In the **Properties** pane, enter details for the requirement.

To add a child requirement, right-click a requirement and select **Add Child Requirement**.

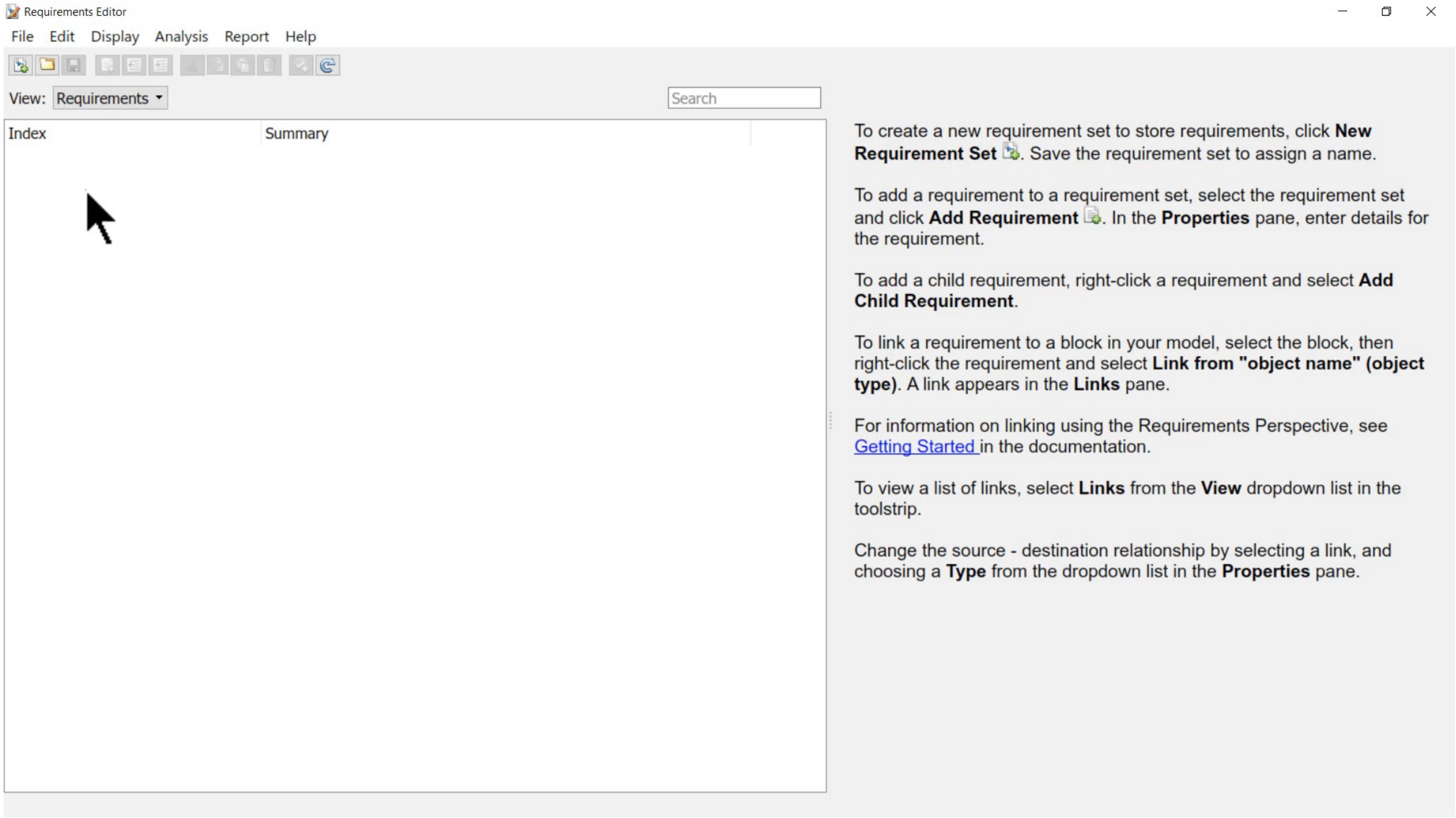
To link a requirement to a block in your model, select the block, then right-click the requirement and select **Link from "object name" (object type)**. A link appears in the **Links** pane.

For information on linking using the Requirements Perspective, see Getting Started in the documentation.

To view a list of links, select **Links** from the **View** dropdown list in the toolstrip.

Change the source - destination relationship by selecting a link, and choosing a **Type** from the dropdown list in the **Properties** pane.

Requirements Editor



To create a new requirement set to store requirements, click **New Requirement Set**. Save the requirement set to assign a name.

To add a requirement to a requirement set, select the requirement set and click **Add Requirement**. In the **Properties** pane, enter details for the requirement.

To add a child requirement, right-click a requirement and select **Add Child Requirement**.

To link a requirement to a block in your model, select the block, then right-click the requirement and select **Link from "object name" (object type)**. A link appears in the **Links** pane.

For information on linking using the Requirements Perspective, see Getting Started in the documentation.

To view a list of links, select **Links** from the **View** dropdown list in the toolstrip.

Change the source - destination relationship by selecting a link, and choosing a **Type** from the dropdown list in the **Properties** pane.

从外部导入需求

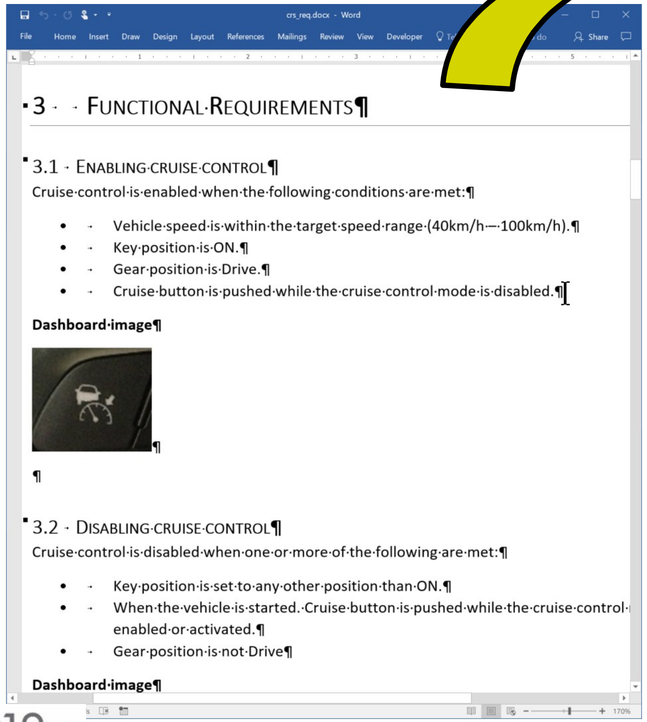
IBM Rational DOORS

R2018a

ReqIF
Requirements Interchange Format

Import

Microsoft Word



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¶

¶

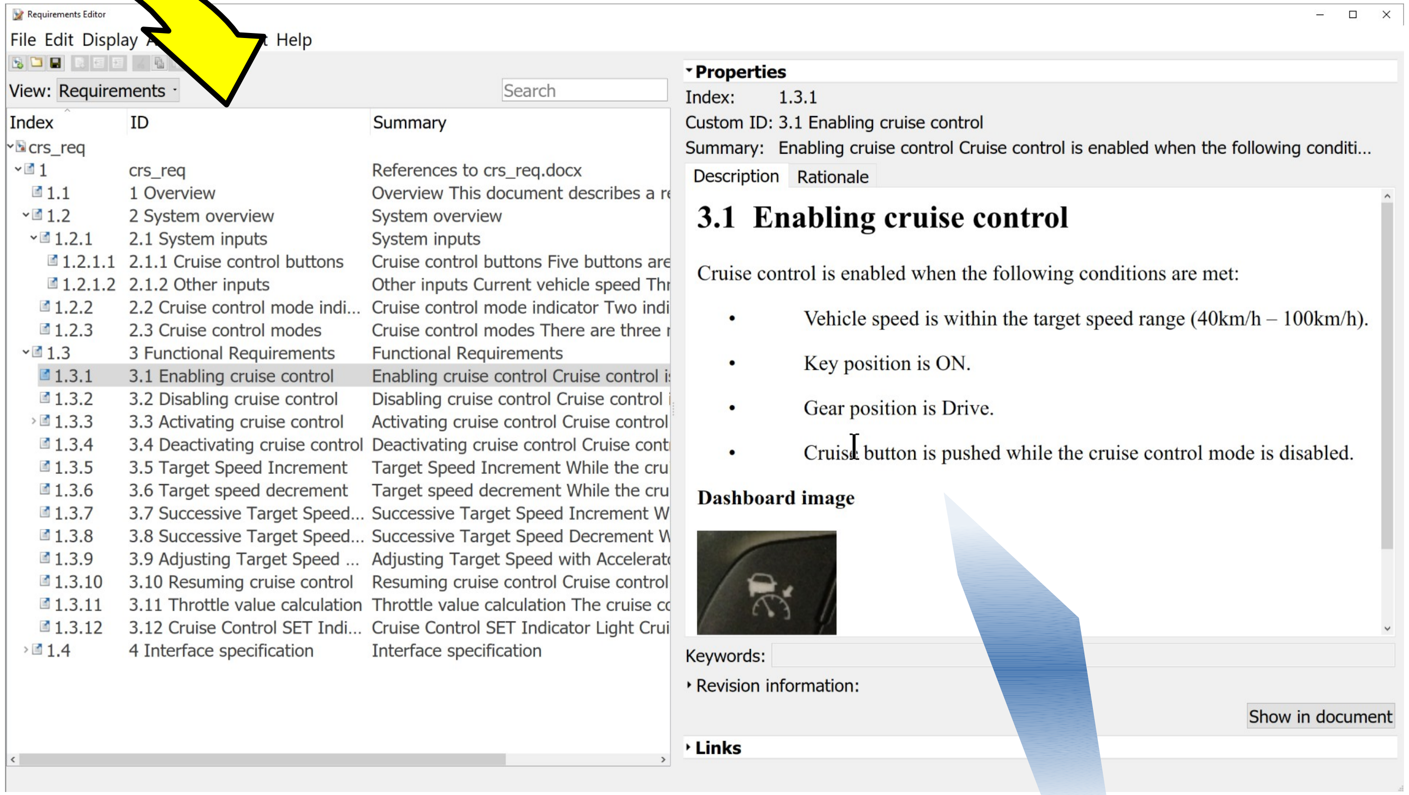
3.2 DISABLING CRUISE CONTROL¶

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¶

Simulink Requirements Editor



View: Requirements

Index	ID	Summary
crs_req		
1	crs_req	References to crs_req.docx
1.1	1 Overview	Overview This document describes a re
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 is
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 cc
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...

Description | Rationale

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:

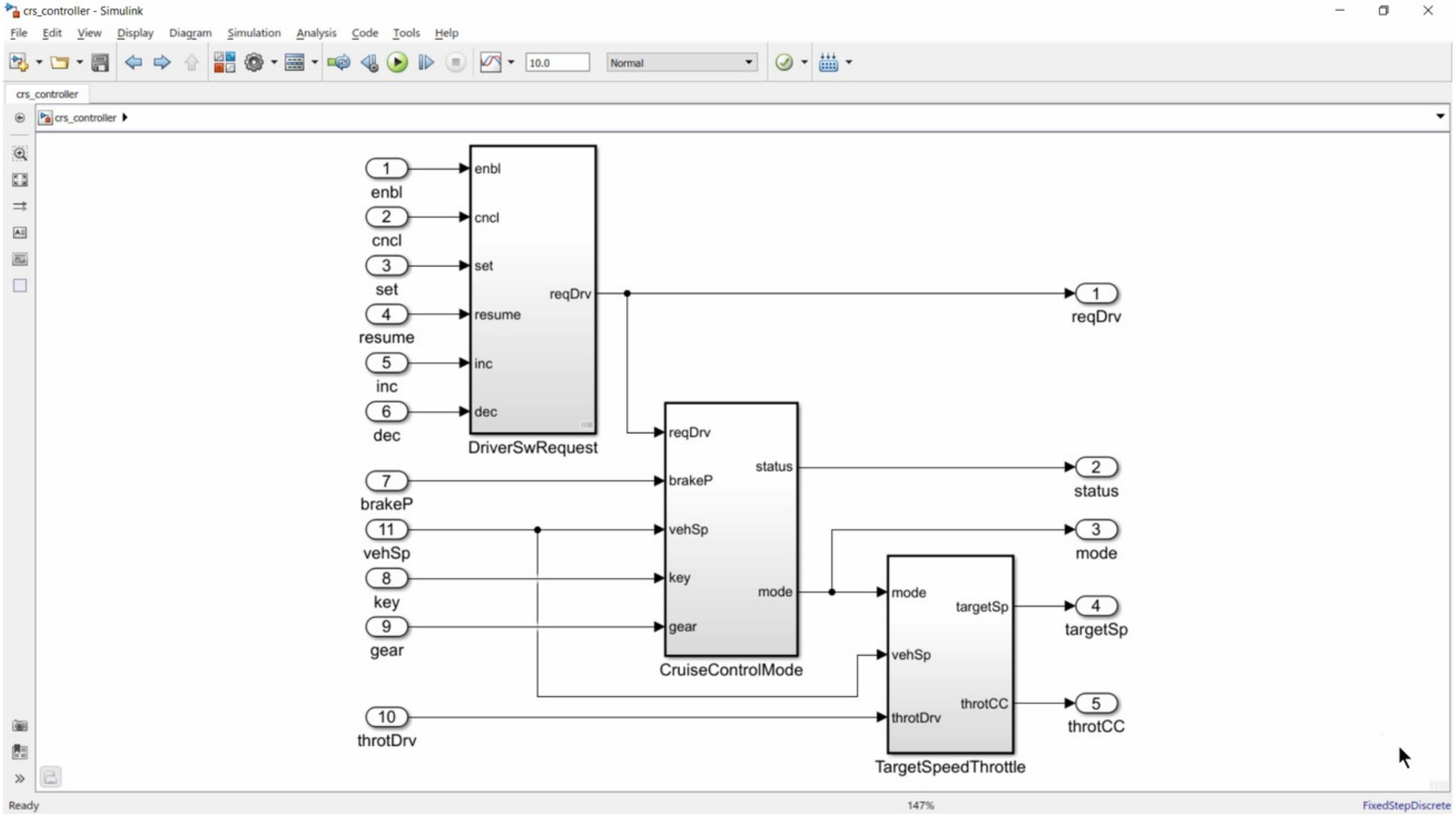
Revision information:

Show in document

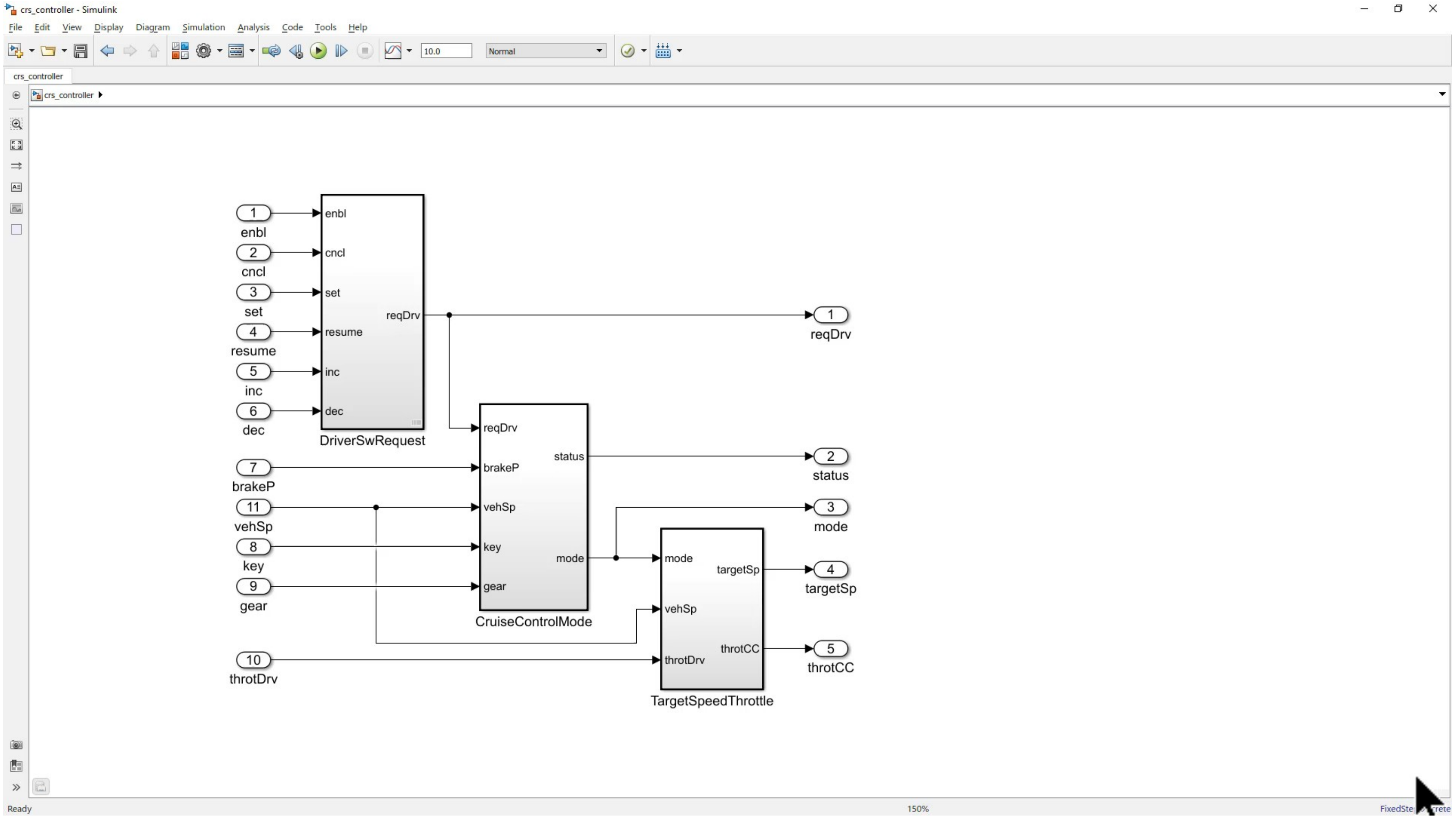
Links

Show in document

Requirements Perspective

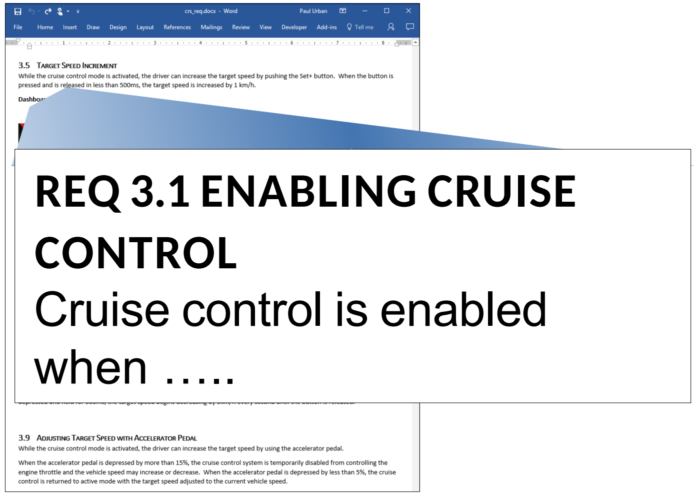


需求透视



crs_controller - Simulink
File Edit View Display Diagram Simulation Analysis Code Tools Help
10.0
Normal
crs_controller
crs_controller
1
enbl
2
cncl
3
set
4
resume
5
inc
6
dec
enbl
cncl
set
resume
inc
dec
reqDrv
DriverSwRequest
1
reqDrv
reqDrv
brakeP
vehSp
key
gear
status
mode
CruiseControlMode
7
brakeP
11
vehSp
8
key
9
gear
2
status
3
mode
mode
vehSp
throtDrv
targetSp
throtCC
TargetSpeedThrottle
4
targetSp
5
throtCC
10
throtDrv
Ready
150%
FixedSte

关联需求，设计和测试



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.

Dashboa

REQ 3.1 ENABLING CRUISE CONTROL

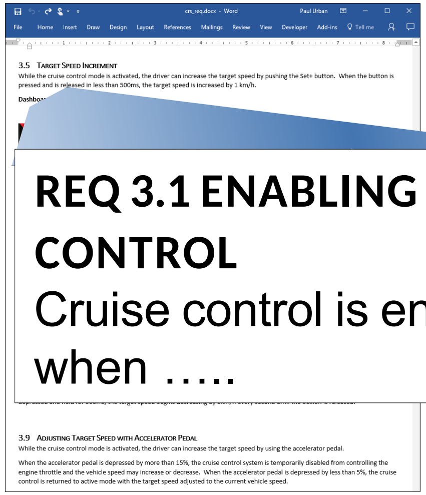
Cruise control is enabled when …..

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.

关联需求，设计和测试



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.

Dashboa

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

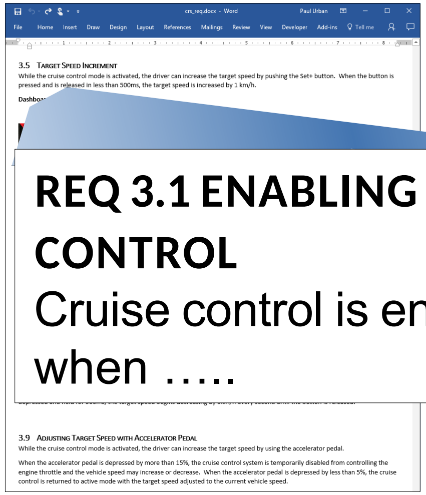
Cruise control is enabled when …..

得到

ENABLE SWITCH DETECTION

If the Enable switch is pressed ……

关联需求，设计和测试



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.

Dashboa

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

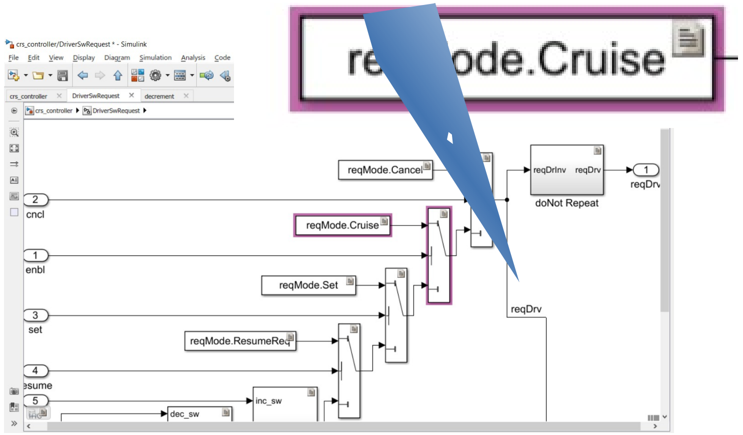
Cruise control is enabled when …..

得到

ENABLE SWITCH DETECTION

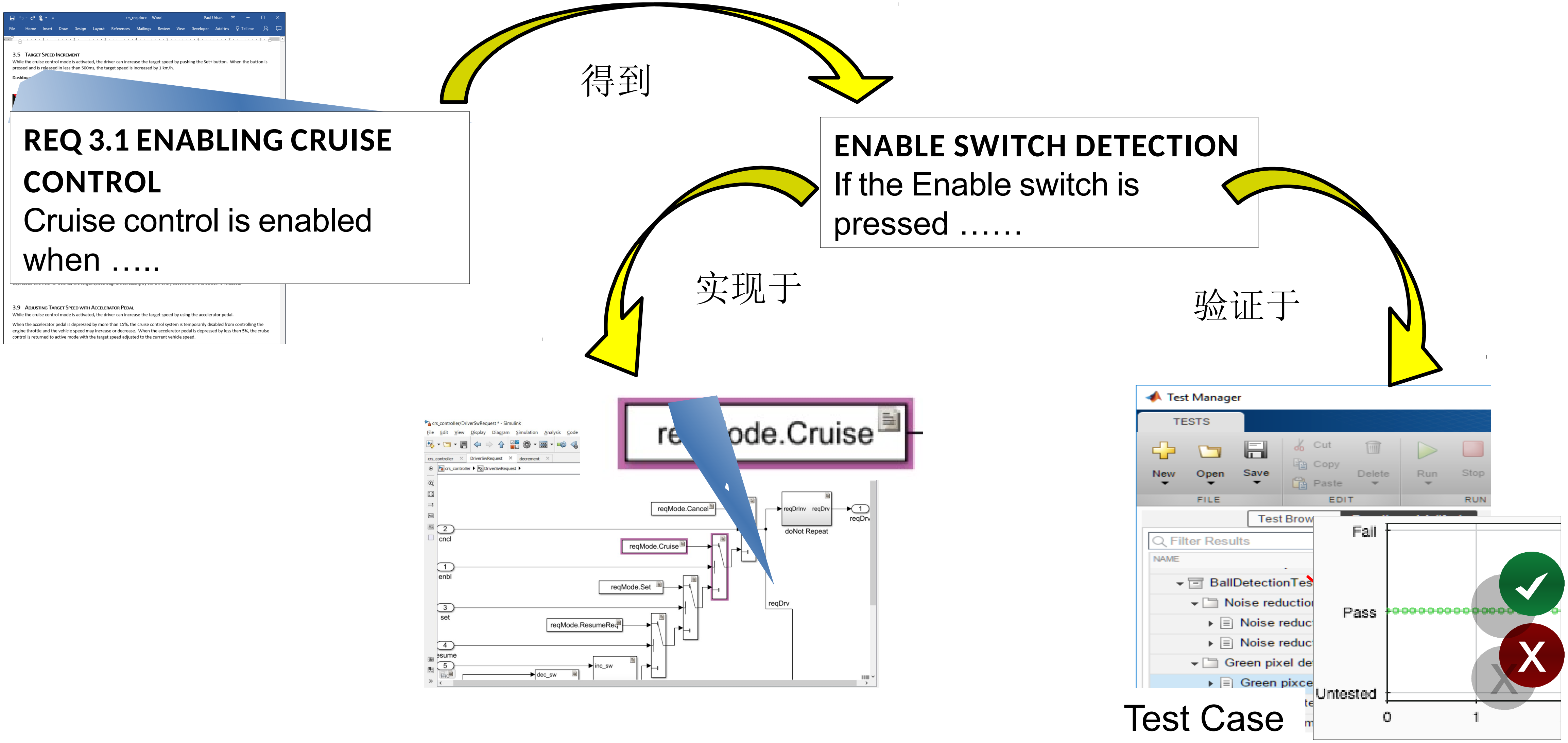
If the Enable switch is pressed ……

实现于



MATLAB EXPO 2018

关联需求，设计和测试



crs_req.docx - Word

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.

Dashboa

REQ 3.1 ENABLING CRUISE CONTROL

Cruise control is enabled when …..

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.

得到

ENABLE SWITCH DETECTION

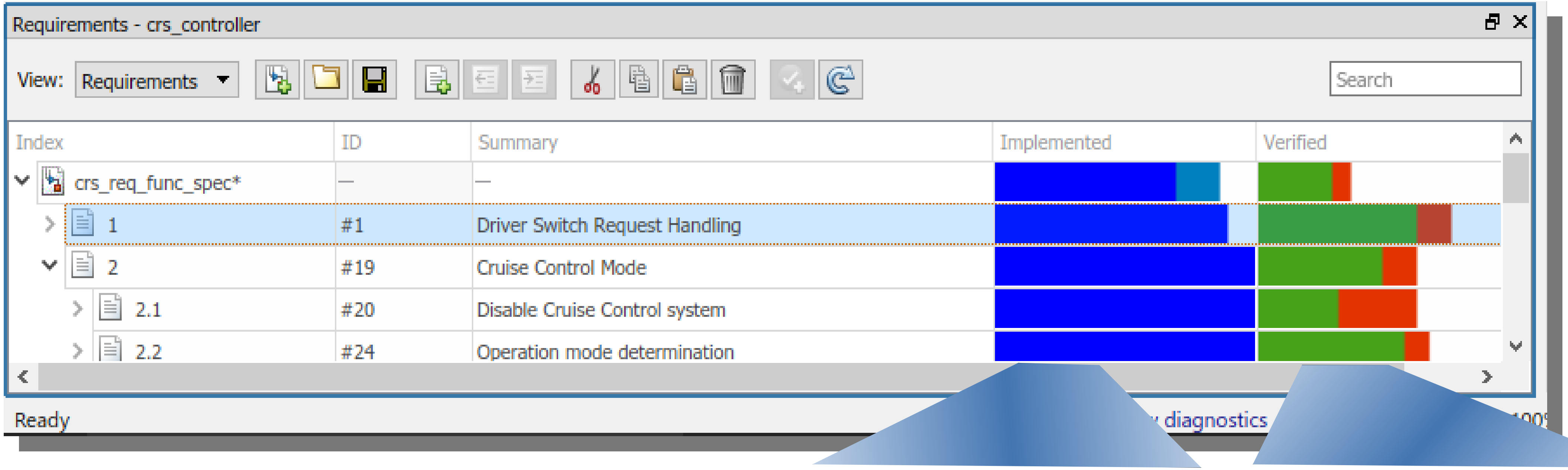
If the Enable switch is pressed ……

实现于

验证于

Test Case

跟踪实现和验证



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

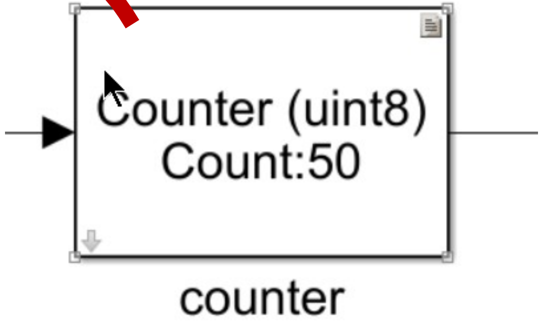
- 🟩 Passed
- 🟥 Failed
- 🟧 No Result
- □ Missing

对变更的响应

Original Requirement

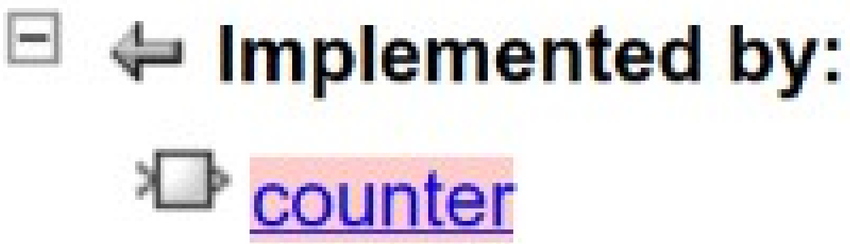
If the switch is pressed and the counter reaches **50** then it shall be recognized as a long press of the switch.

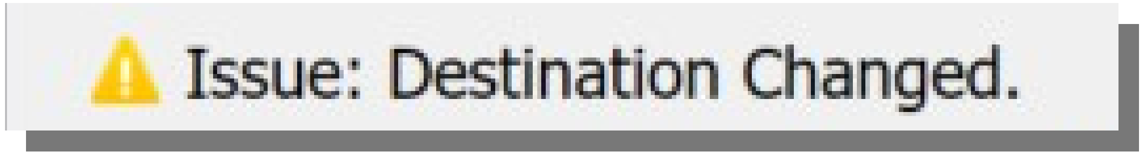
Implements



Updated Requirement

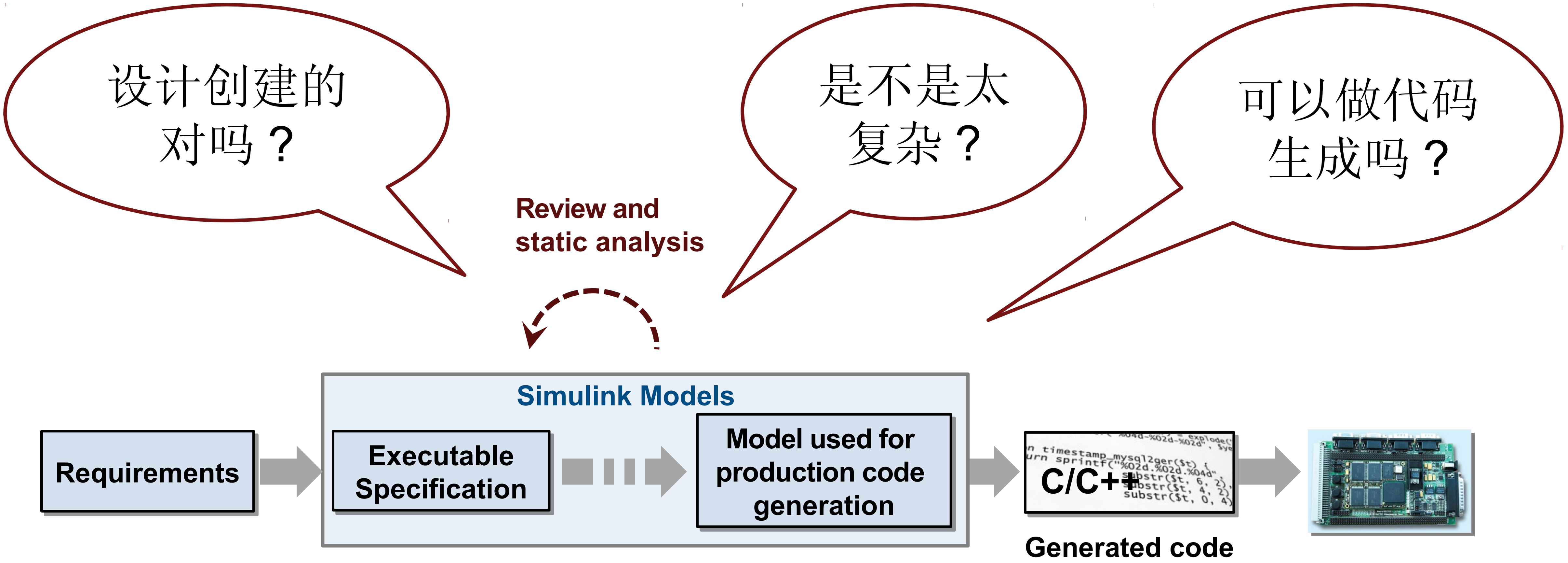
If the switch is pressed and the counter reaches **75** then it shall be recognized as a long press of the switch.





Issue: Destination Changed.

验证设计对指南和标准的遵循



设计创建的对吗？

是不是太复杂？

可以做代码生成吗？

Review and static analysis

Simulink Models

Requirements

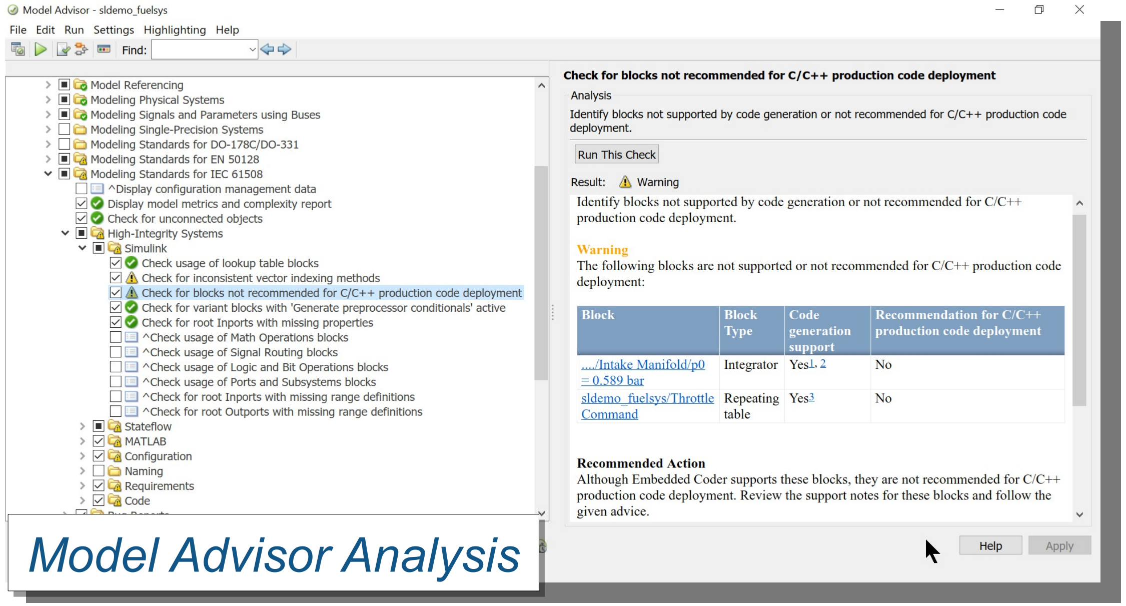
Executable Specification

Model used for production code generation

C/C++

Generated code

使用静态分析进行自动化验证



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.

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

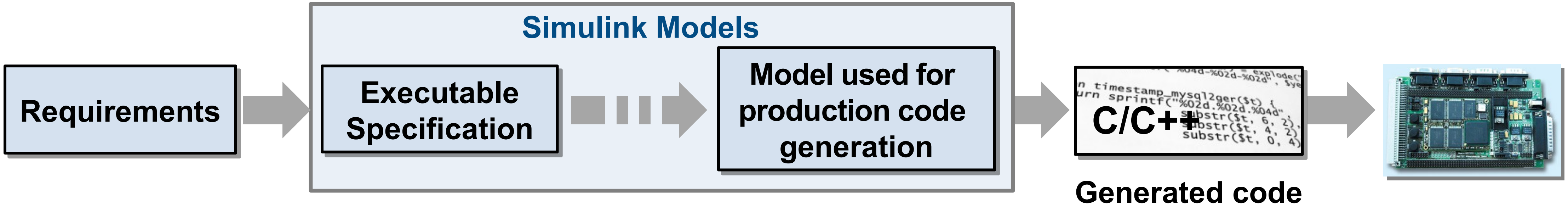
Recommended Action

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.

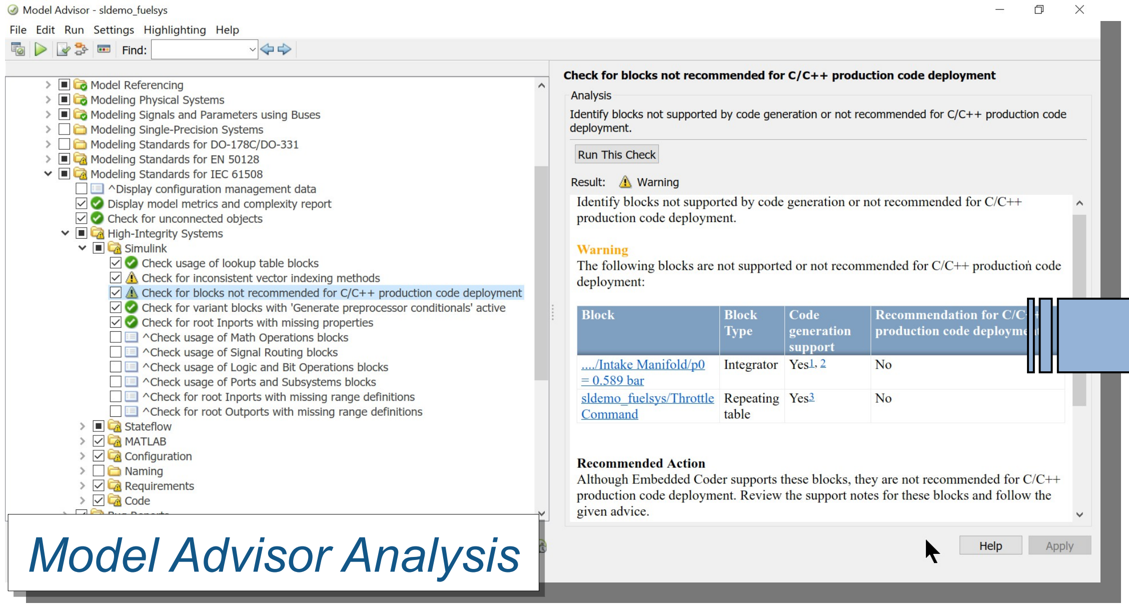
Model Advisor Analysis

检查：

- 可读性和语义
- 性能和效率
- Clones
- 更多……



为走查和文档化工作生成报告



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:

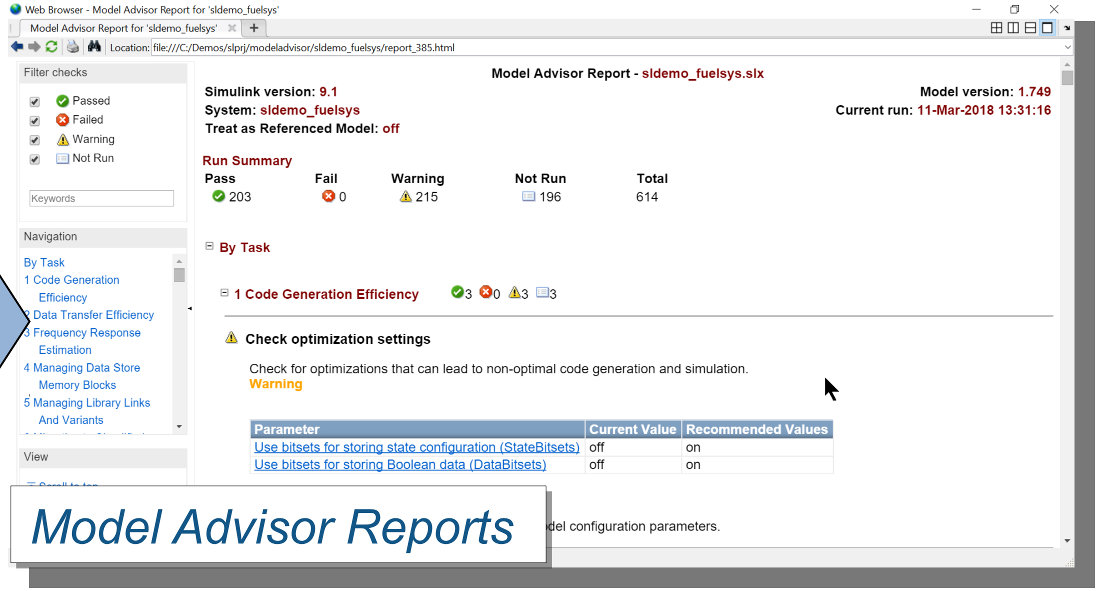
Block	Block Type	Code generation support	Recommendation for C/C++ production code deployment
..../Intake Manifold/p0 = 0.589 bar	Integrator	Yes[1], [2]	No
sldemo_fuelsys/Throttle Command	Repeating table	Yes[3]	No

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.

Help Apply

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**

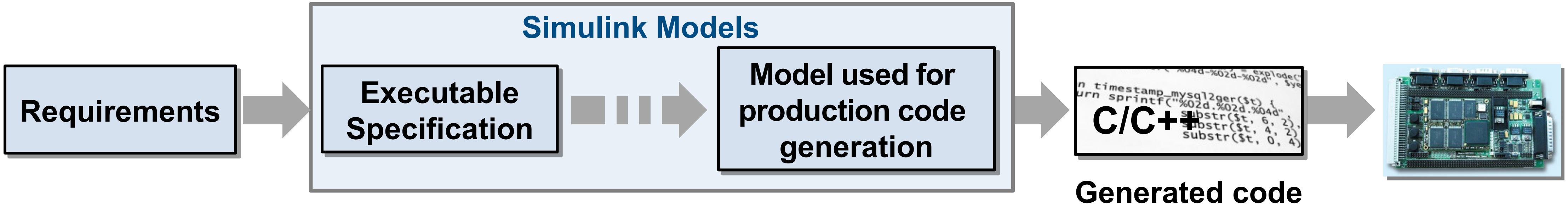
Check for optimizations that can lead to non-optimal code generation and simulation.

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

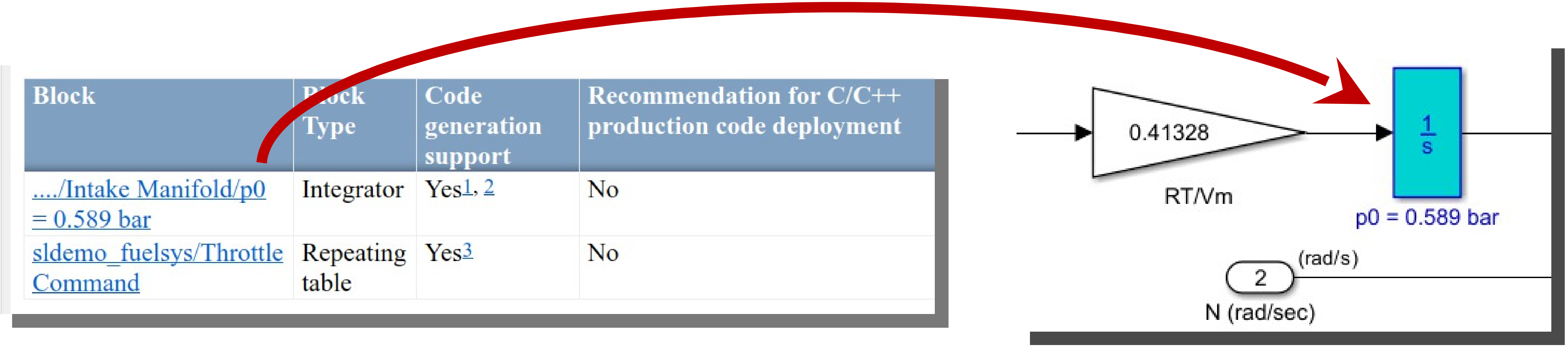
Executable Specification

Model used for production code generation

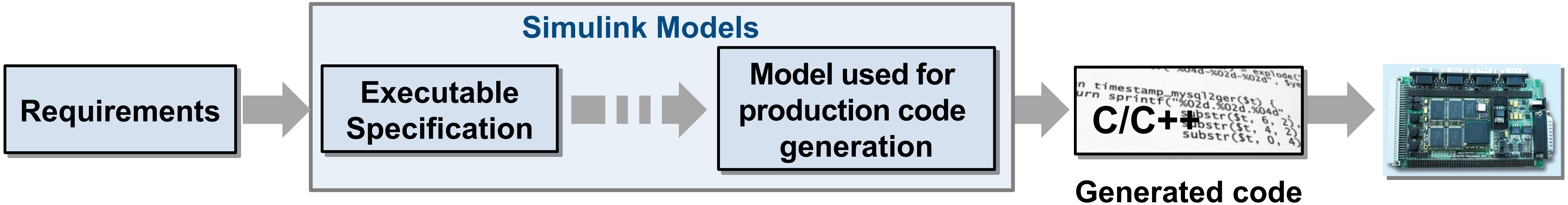
C/C++

Generated code

导航到有问题的模块

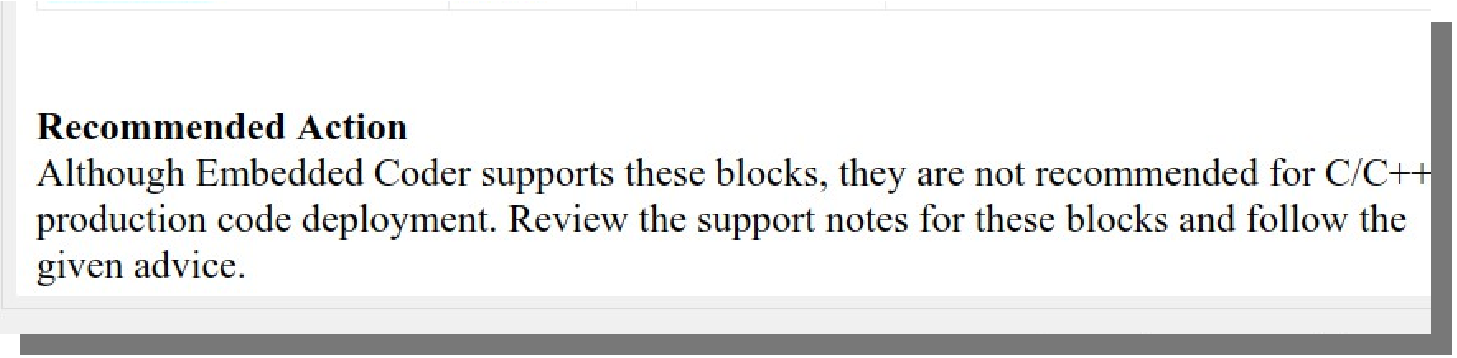


Block	Block Type	Code generation support	Recommendation for C/C++ production code deployment
..../Intake Manifold/p0 = 0.589 bar	Integrator	Yes[1], [2]	No
sldemo_fuelsys/Throttle Command	Repeating table	Yes[3]	No

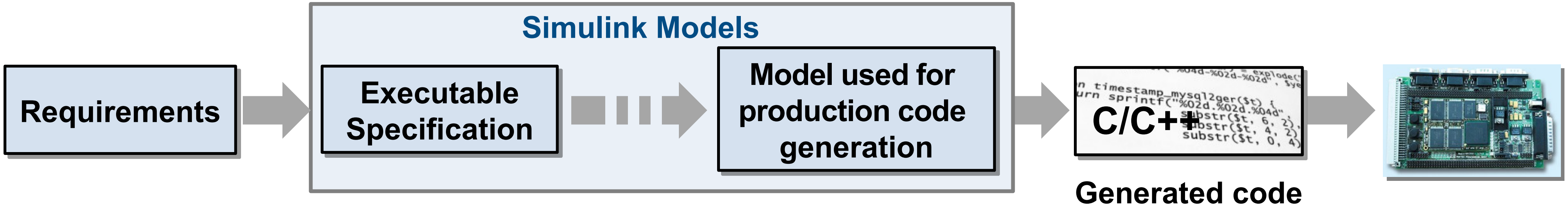


Generated code

用于解决问题或自动纠正的指南

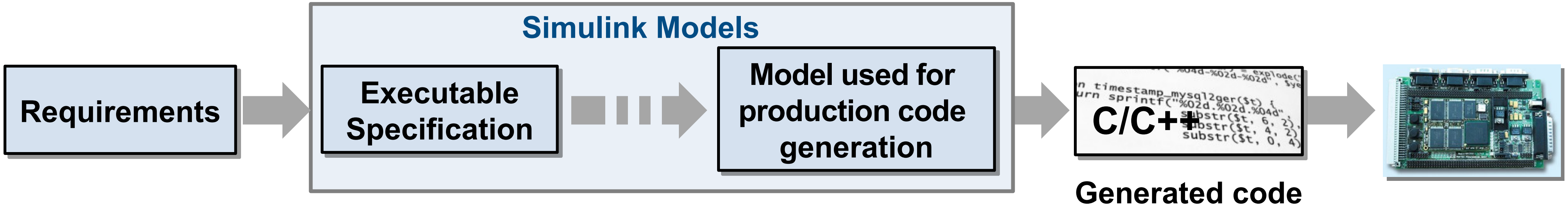


Recommended Action
Although Embedded Coder supports these blocks, they are not recommended for C/C++ production code deployment. Review the support notes for these blocks and follow the given advice.



内建的检查项，用于行业标准和准则的遵循

- 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)



Requirements

Simulink Models

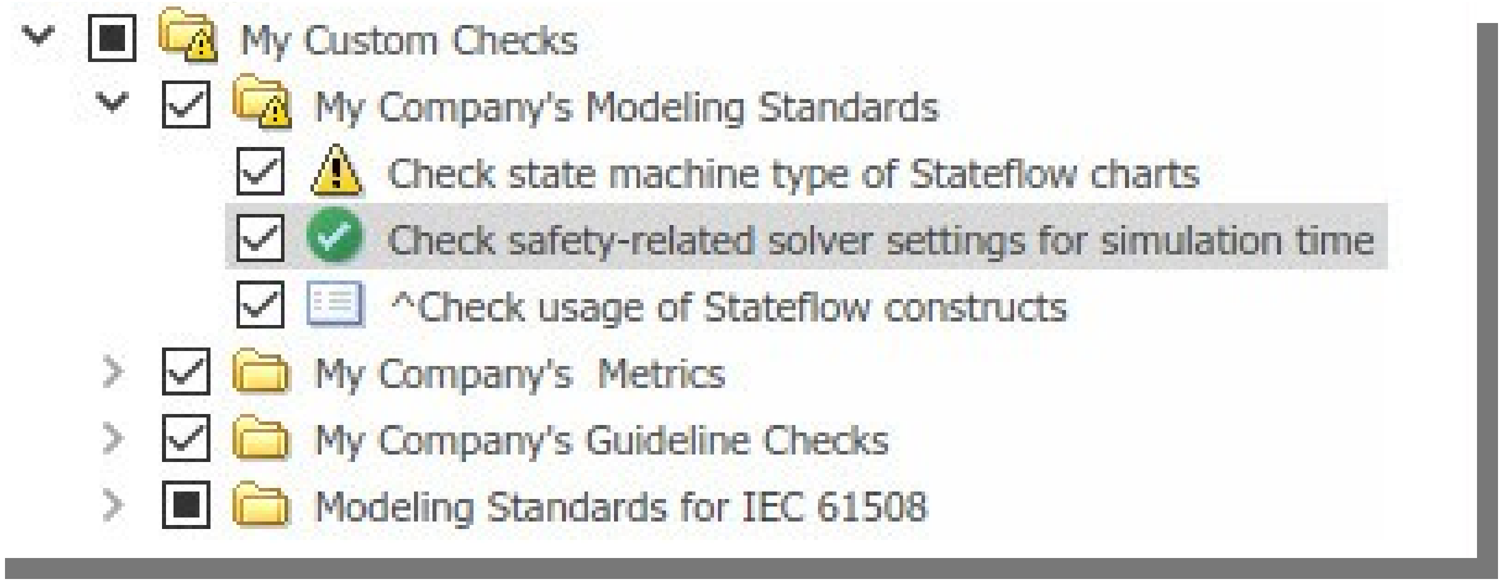
Executable Specification

Model used for production code generation

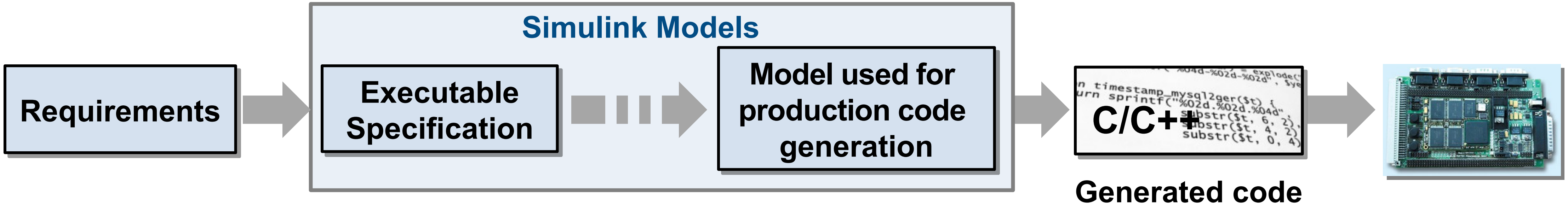
C/C++

Generated code

配置和自定义分析

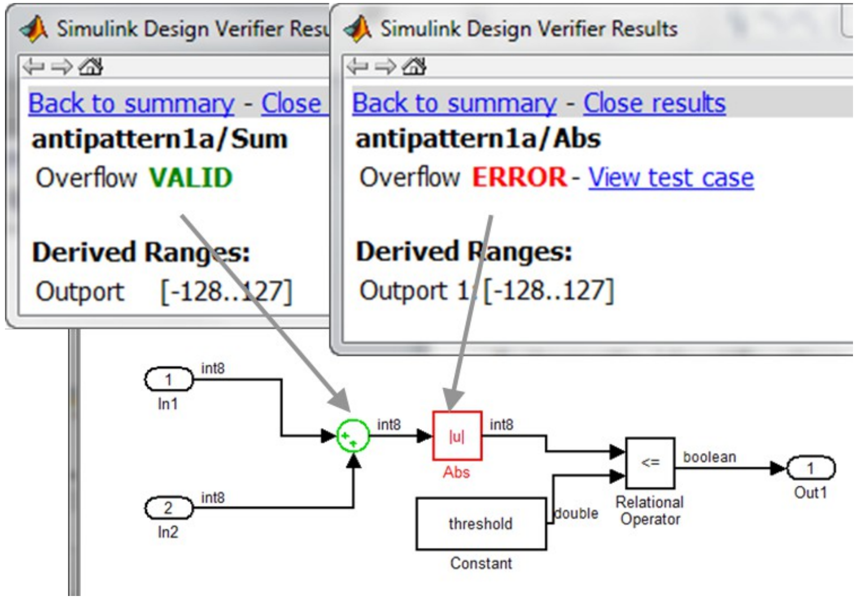


- ■ My Custom Checks
  - ☑ My Company's Modeling Standards
    - ☑ ⚠ Check state machine type of Stateflow charts
    - ☑ ✓ Check safety-related solver settings for simulation time
    - ☑ ^Check usage of Stateflow constructs
  - ☑ My Company's Metrics
  - ☑ My Company's Guideline Checks
  - ■ Modeling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



Generated code

用形式化方法检测设计错误



Simulink Design Verifier Resu

Back to summary - Close

antipattern1a/Sum

Overflow VALID

Derived Ranges:

Outport [-128..127]

Simulink Design Verifier Results

Back to summary - Close results

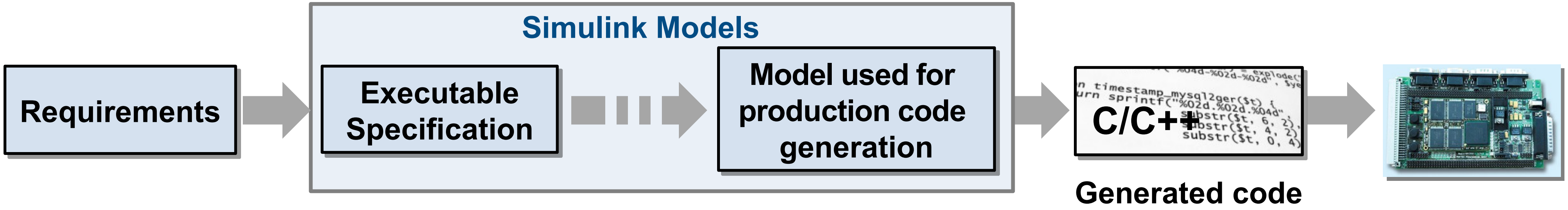
antipattern1a/Abs

Overflow ERROR - View test case

Derived Ranges:

Outport 1 [-128..127]

- 发现运行时设计错误：
  - 整数溢出
  - 死逻辑
  - 被零除
  - 数组越界
  - 范围违规
- 生成反例以重现错误



Simulink Models

Requirements

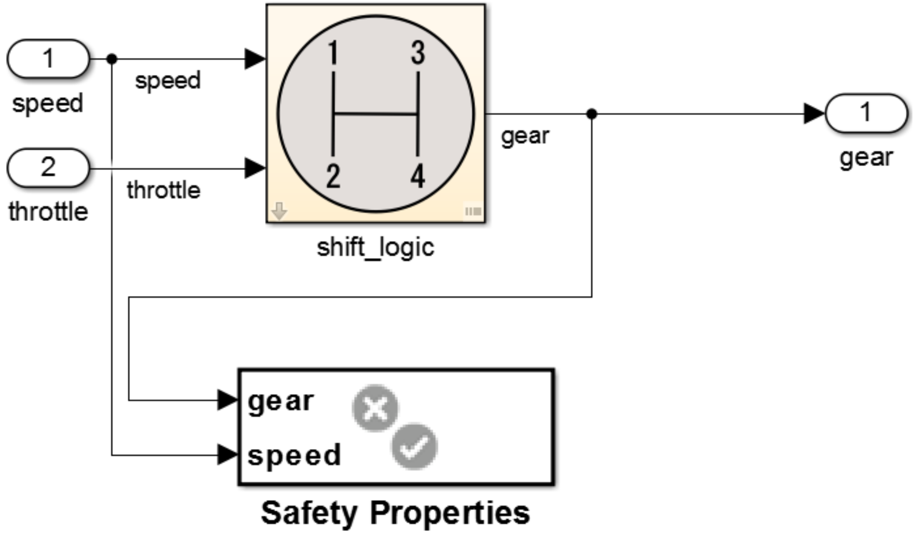
Executable Specification

Model used for production code generation

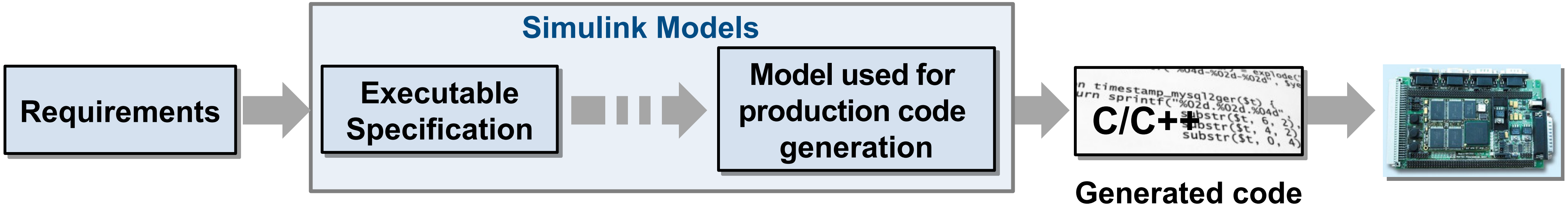
C/C++

Generated code

证明设计符合需求



- 使用形式化需求模型证明设计属性
- 模型功能和安全要求
- 生成用于分析和调试的反例


Requirements

Simulink Models

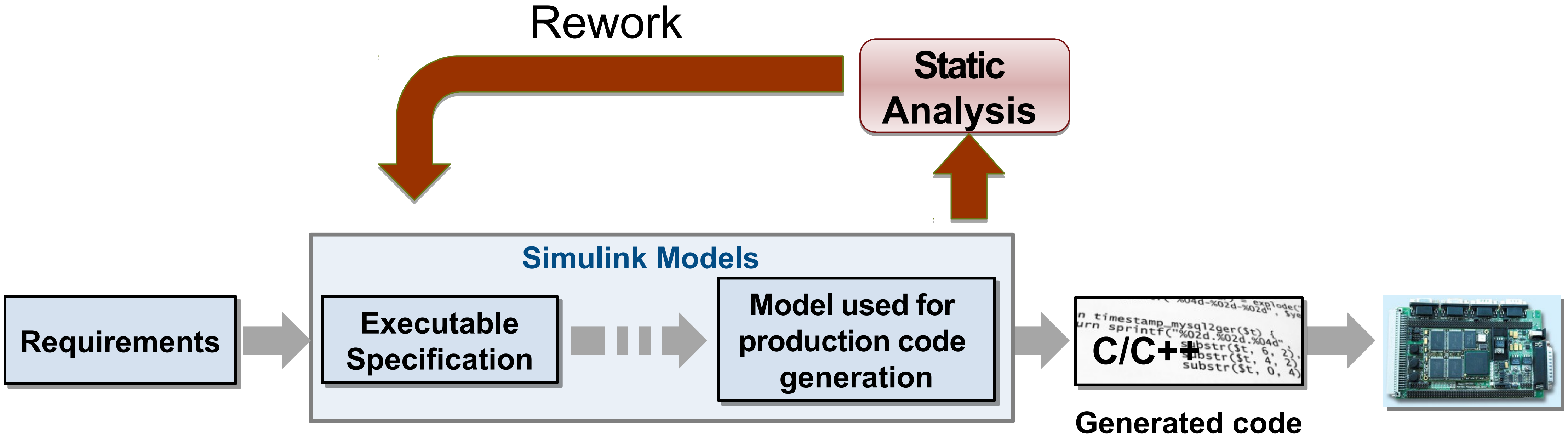
Executable Specification

Model used for production code generation

C/C++

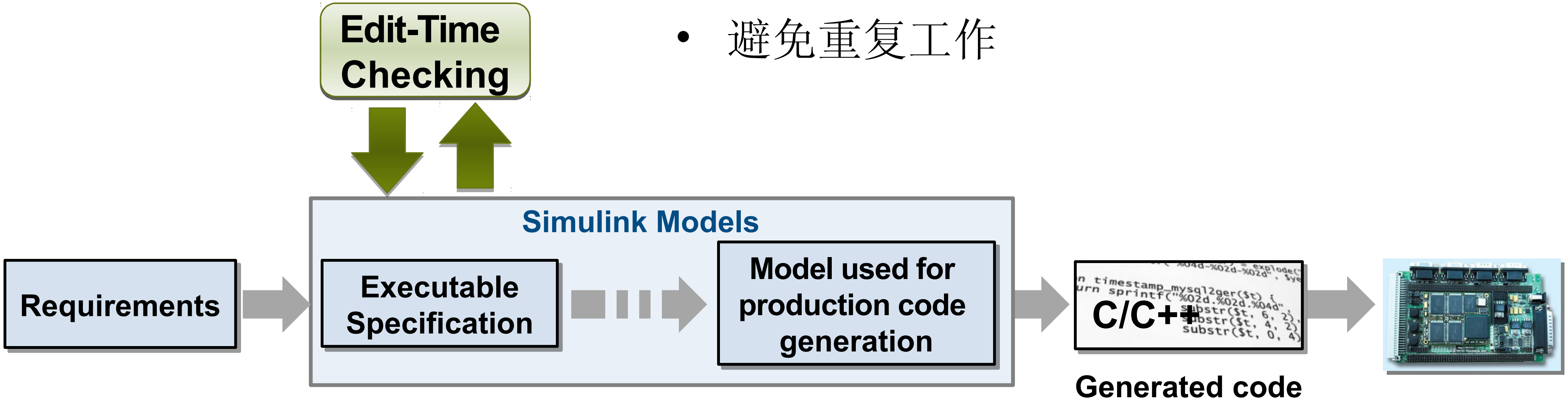
Generated code

对标准和准则的检查经常要延迟执行



使用 Edit-Time 检查，将验证早期化

- 编辑时高亮违规
- 早期修复问题
- 避免重复工作



Edit-Time Checking

Simulink Models

Requirements

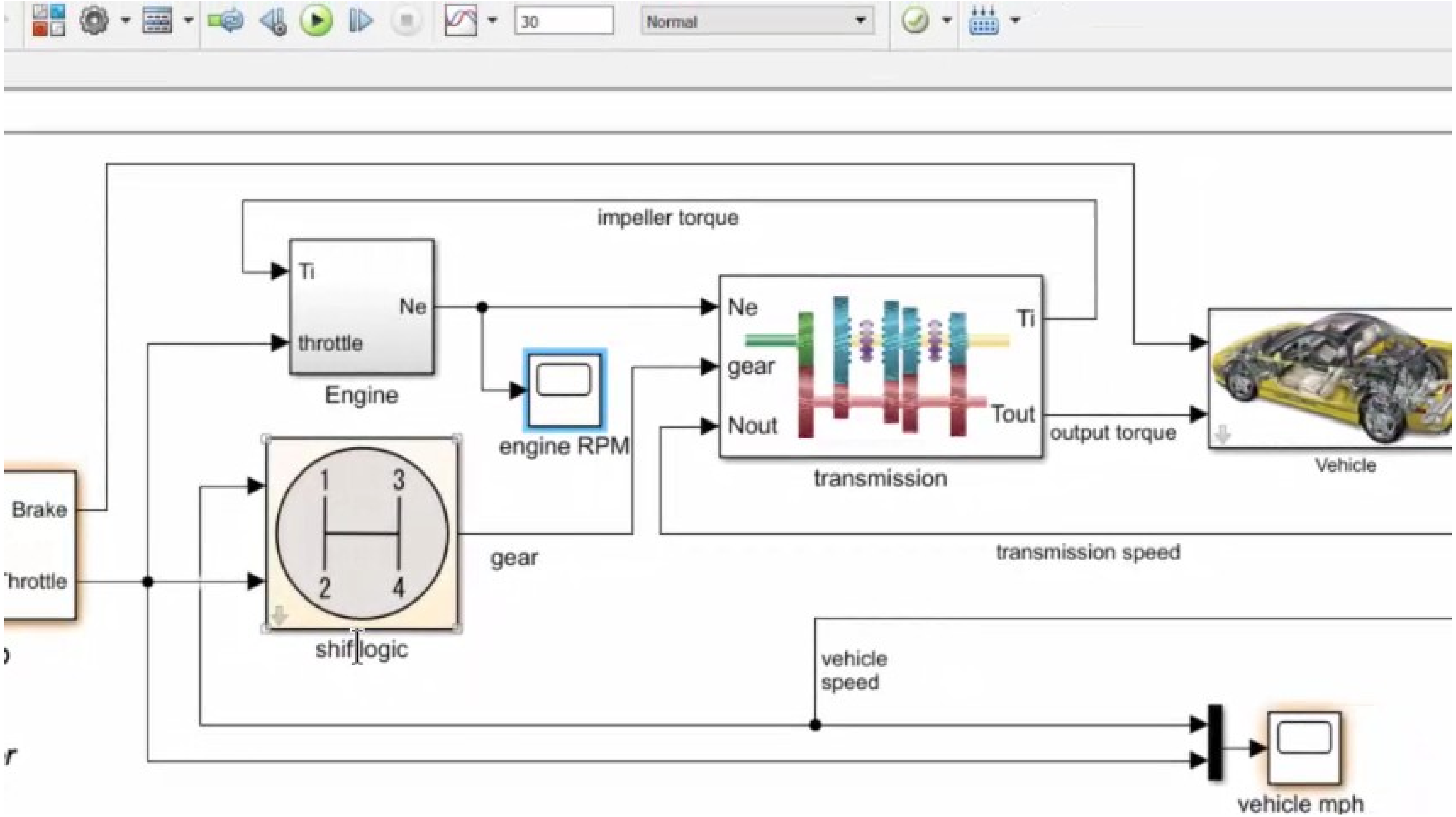
Executable Specification

Model used for production code generation

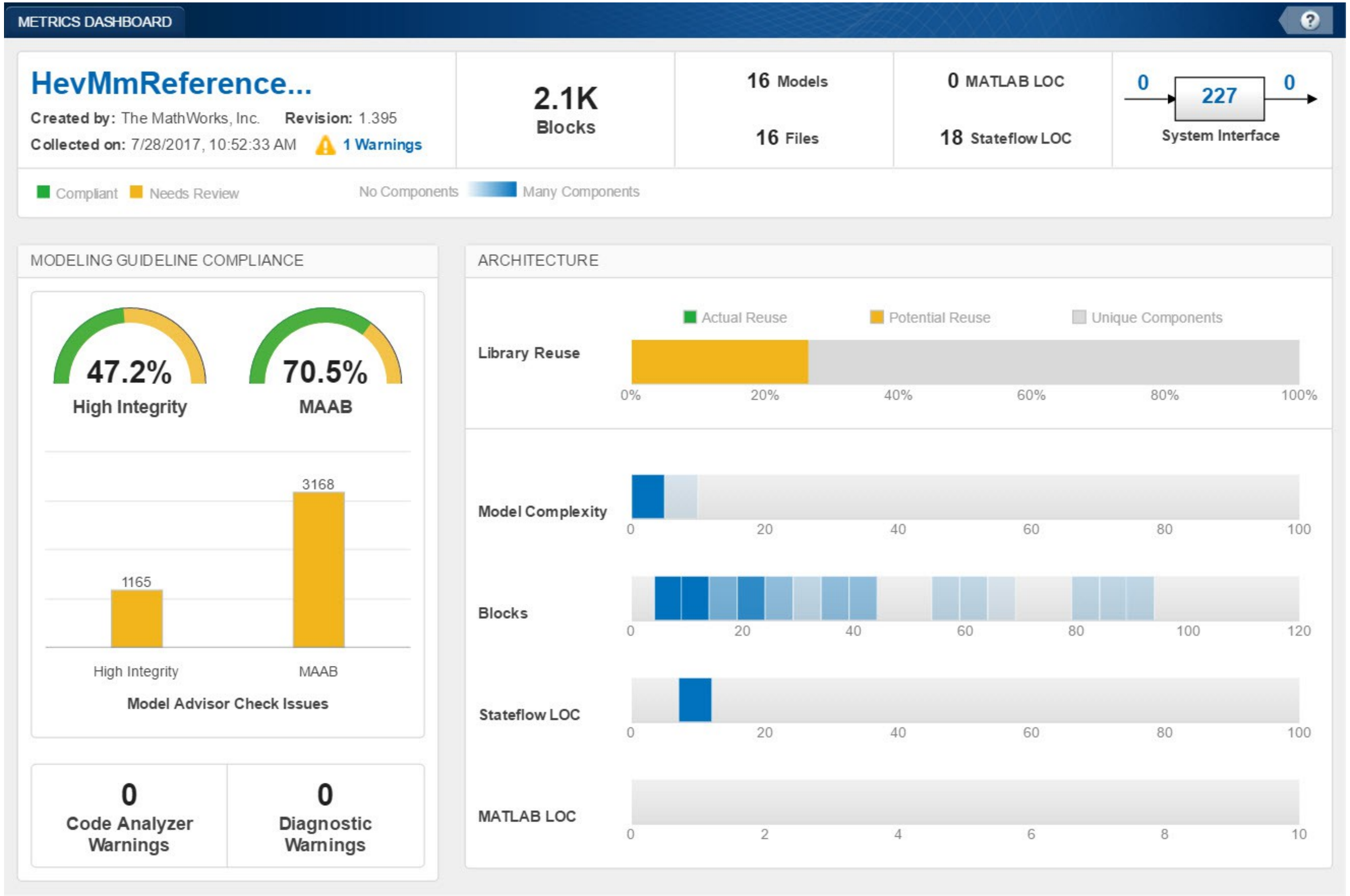
C/C++

Generated code

使用 Edit-Time 检查，查找编辑时的合规性问题



使用 Metrics Dashboard 评估质量



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

Model Advisor Check Issues

0 Code Analyzer Warnings

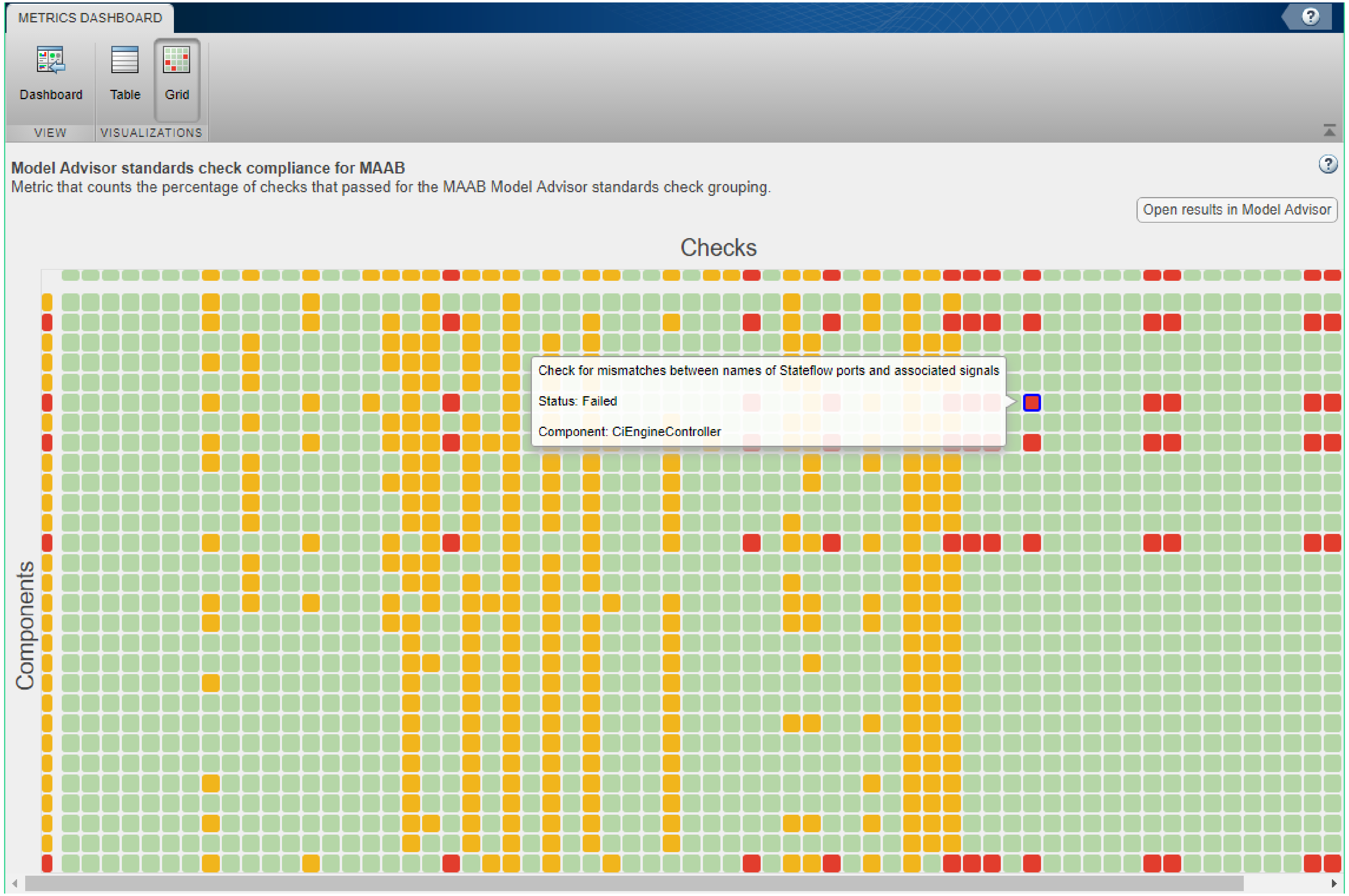
0 Diagnostic Warnings

ARCHITECTURE

- 统一的视图
  - 尺寸
  - 合规
  - 复杂度
- 确定问题区域可能在哪里

网格可视化

R2018a



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

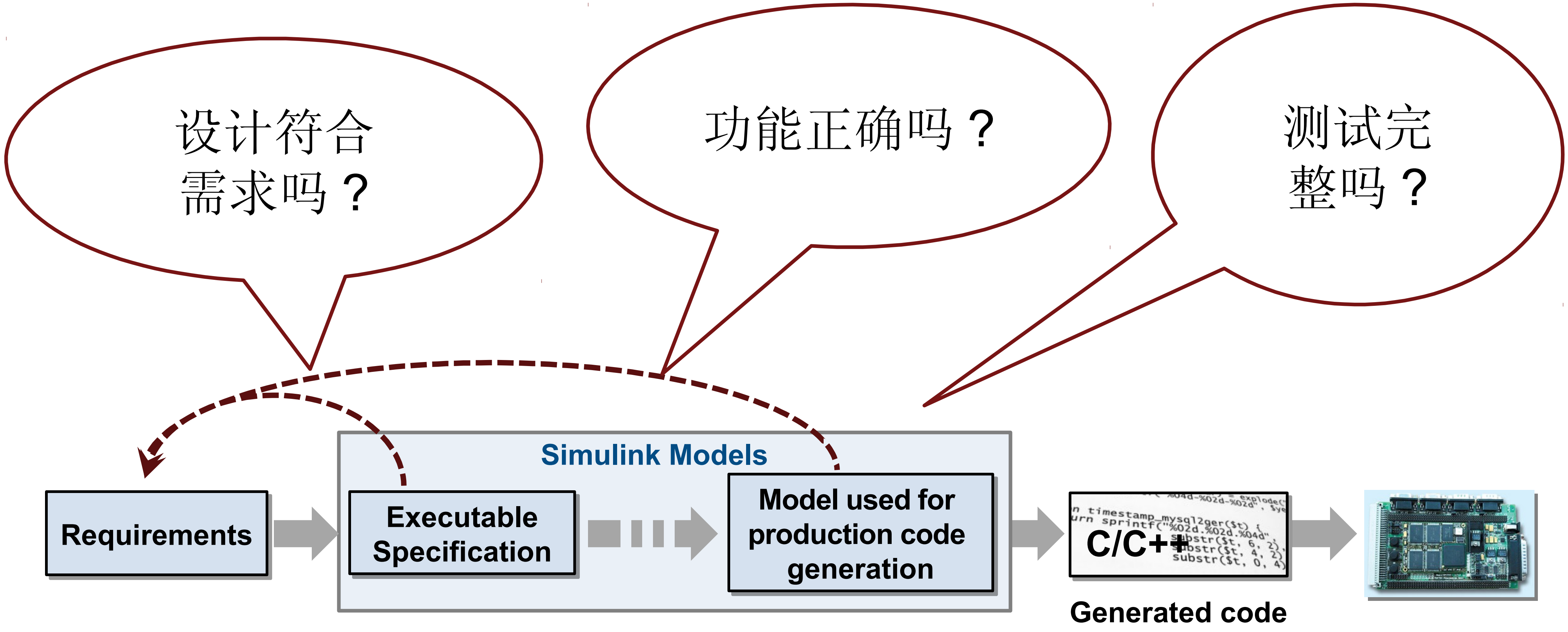
Component: CiEngineController

- 可视化标准检查合规性
  - 发现问题
  - 识别模式
  - 查看热点

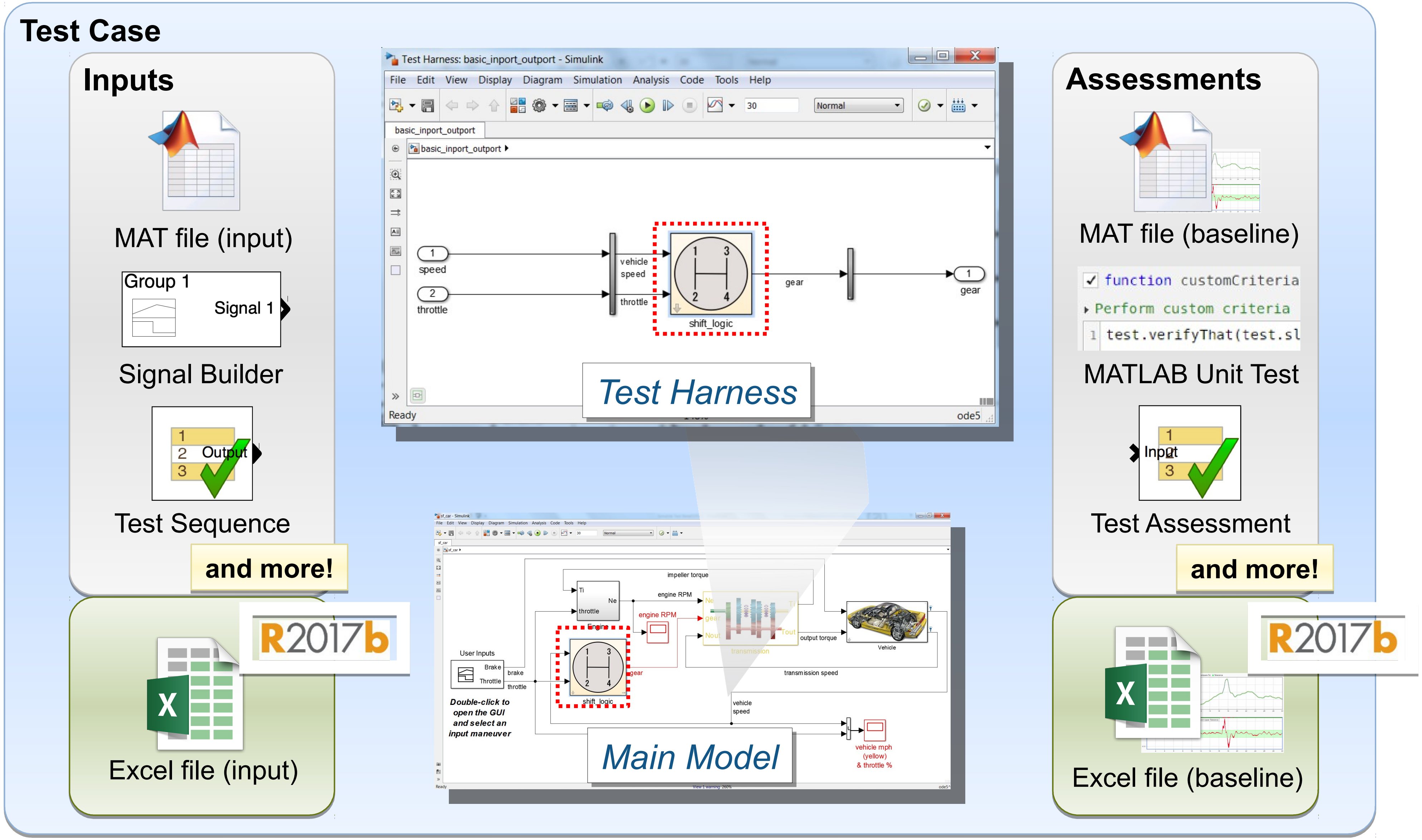
Legend:

🟥	Red:	Fail
🟧	Orange:	Warning
🟩	Green:	Pass
▨	Gray:	Not run

功能性测试


设计符合
需求吗？
功能正确吗？
测试完
整吗？
Simulink Models
Requirements
Executable Specification
Model used for production code generation
C/C++
Generated code

系统的功能性测试



Test Case

Inputs

MAT file (input)

Signal Builder

Test Sequence

and more!

R2017b

Excel file (input)

Assessments

MAT file (baseline)

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

MATLAB Unit Test

Test Assessment

and more!

R2017b

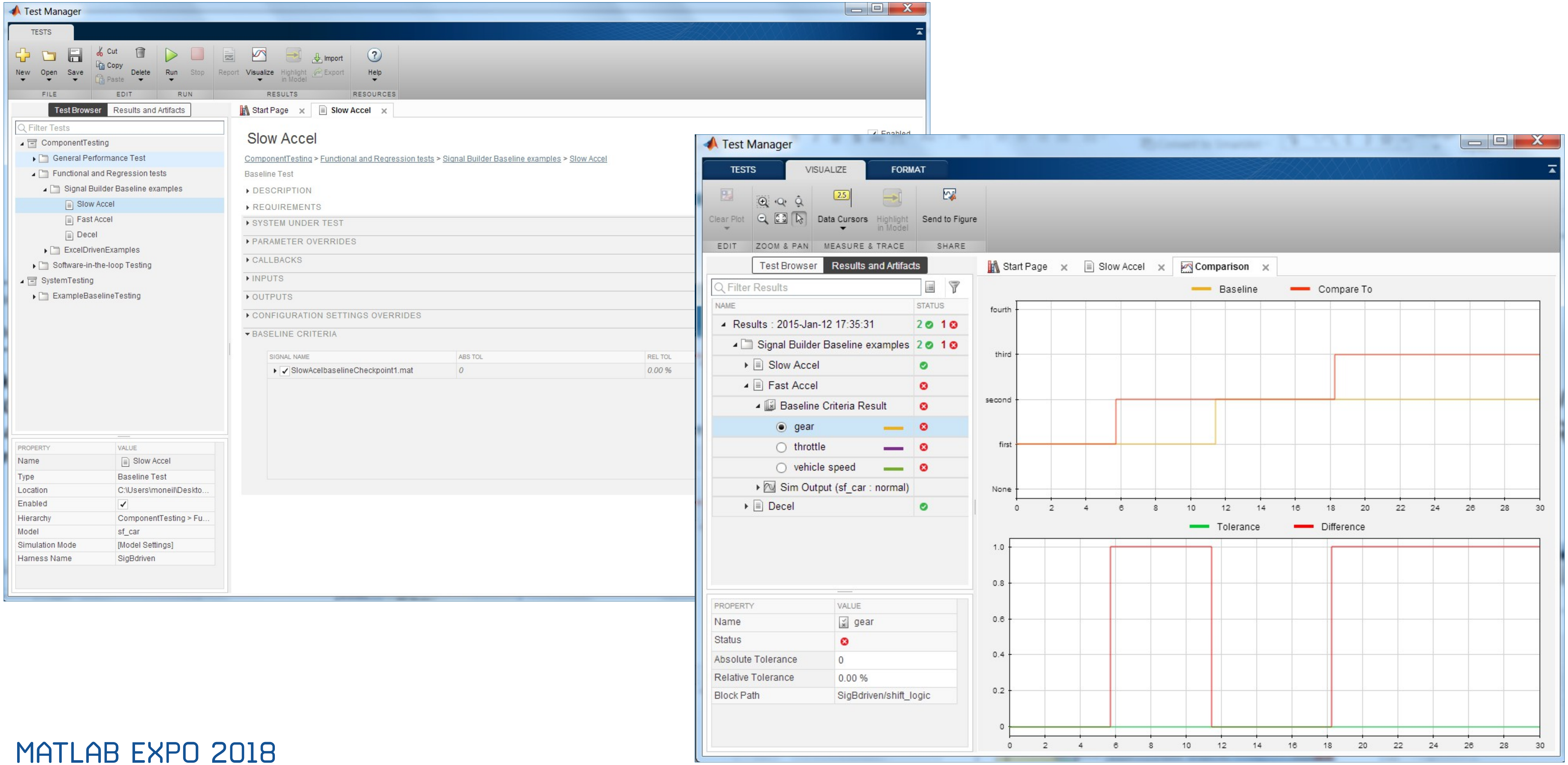
Excel file (baseline)

Test Harness

Main Model

Double-click to open the GUI and select an input maneuver

管理测试和测试结果



- ComponentTesting
  - General Performance Test
  - Functional and Regression tests
    - Signal Builder Baseline examples
      - Slow Accel
      - Fast Accel
      - Decel
    - ExcelDrivenExamples
  - Software-in-the-loop Testing
- SystemTesting
  - ExampleBaselineTesting

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

Slow Accel

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

Baseline Test

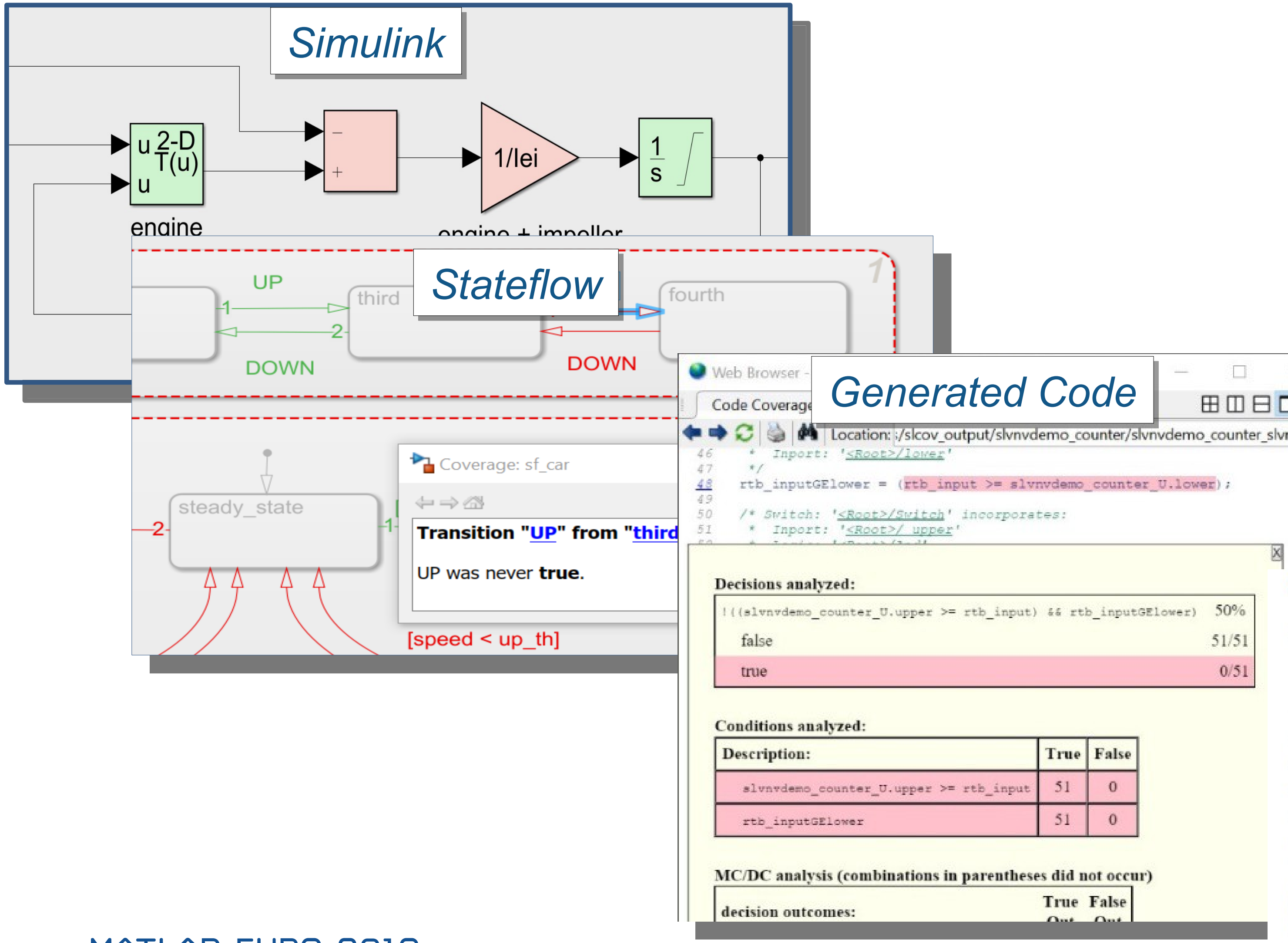
- DESCRIPTION
- REQUIREMENTS
- SYSTEM UNDER TEST
- PARAMETER OVERRIDES
- CALLBACKS
- INPUTS
- OUTPUTS
- CONFIGURATION SETTINGS OVERRIDES
- BASELINE CRITERIA

SIGNAL NAME	ABS TOL	REL TOL
✓ SlowAcelbaselineCheckpoint1.mat	0	0.00 %

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

覆盖率分析用以测量测试



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:

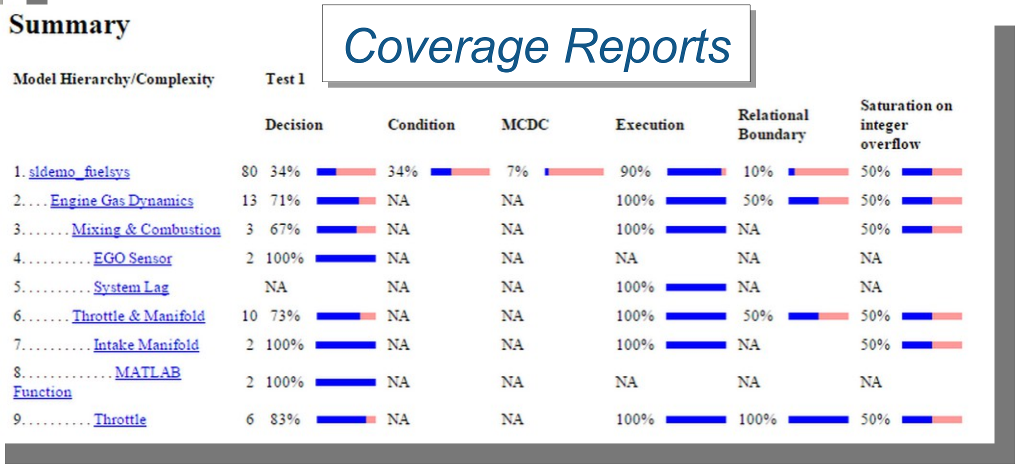
!((slvnvdemo_counter_U.upper >= rtb_input) && rtb_inputGElower)	50%
false	51/51
true	0/51

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

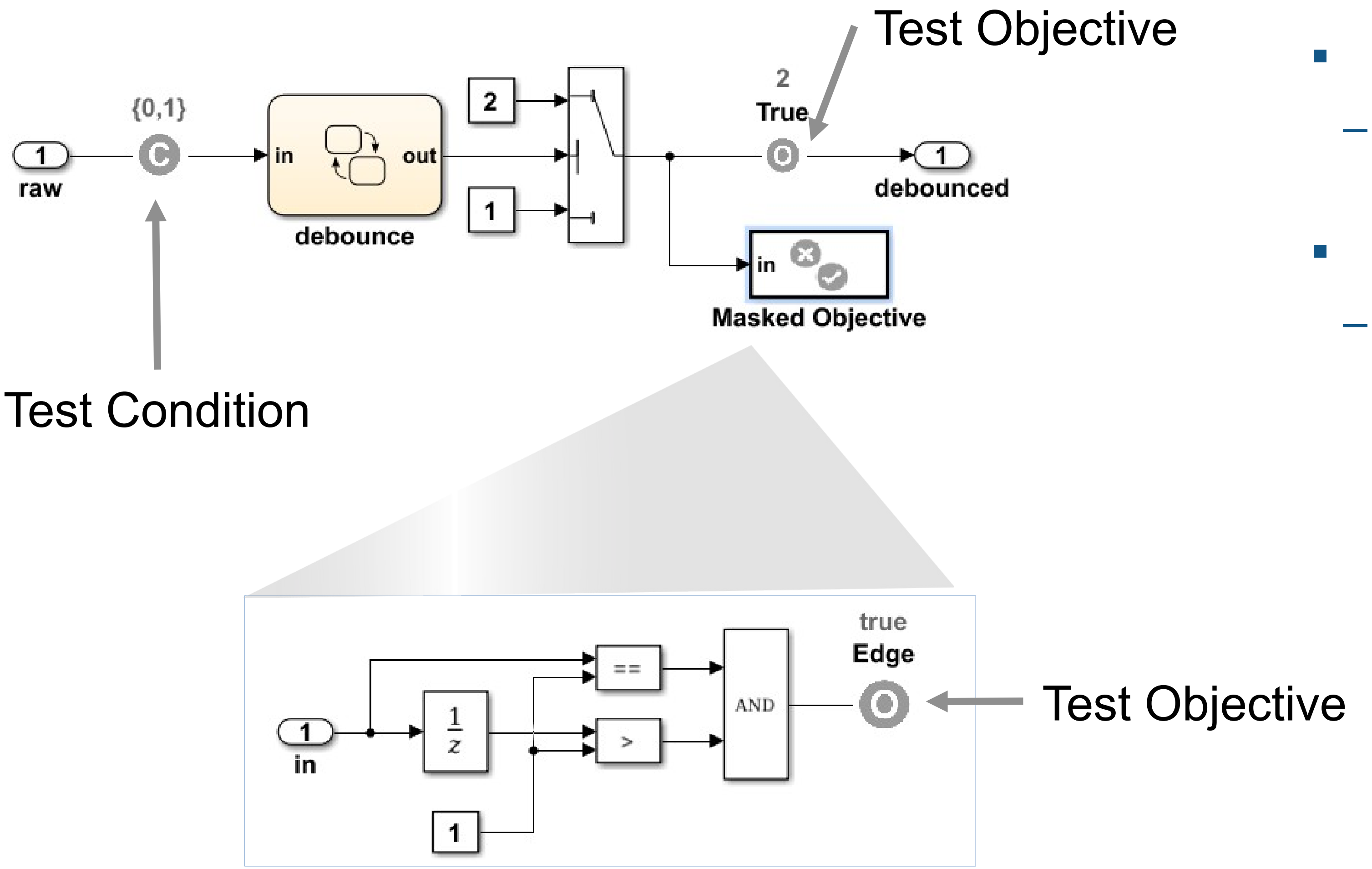


Summary

Model Hierarchy/Complexity		Test 1 Decision	Condition	MCDC	Execution	Relational Boundary	Saturation on integer overflow
1. sldemo_fuelsys	80	34%	34%	7%	90%	10%	50%
2. . . . Engine Gas Dynamics	13	71%	NA	NA	100%	50%	50%
3. . . . . . . Mixing & Combustion	3	67%	NA	NA	100%	NA	50%
4. . . . . EGO Sensor	2	100%	NA	NA	NA	NA	NA
5. . . . . System Lag		NA	NA	NA	100%	NA	NA
6. . . . . . . Throttle & Manifold	10	73%	NA	NA	100%	50%	50%
7. . . . . Intake Manifold	2	100%	NA	NA	100%	NA	50%
8. . . . . MATLAB Function	2	100%	NA	NA	NA	NA	NA
9. . . . . Throttle	6	83%	NA	NA	100%	100%	50%

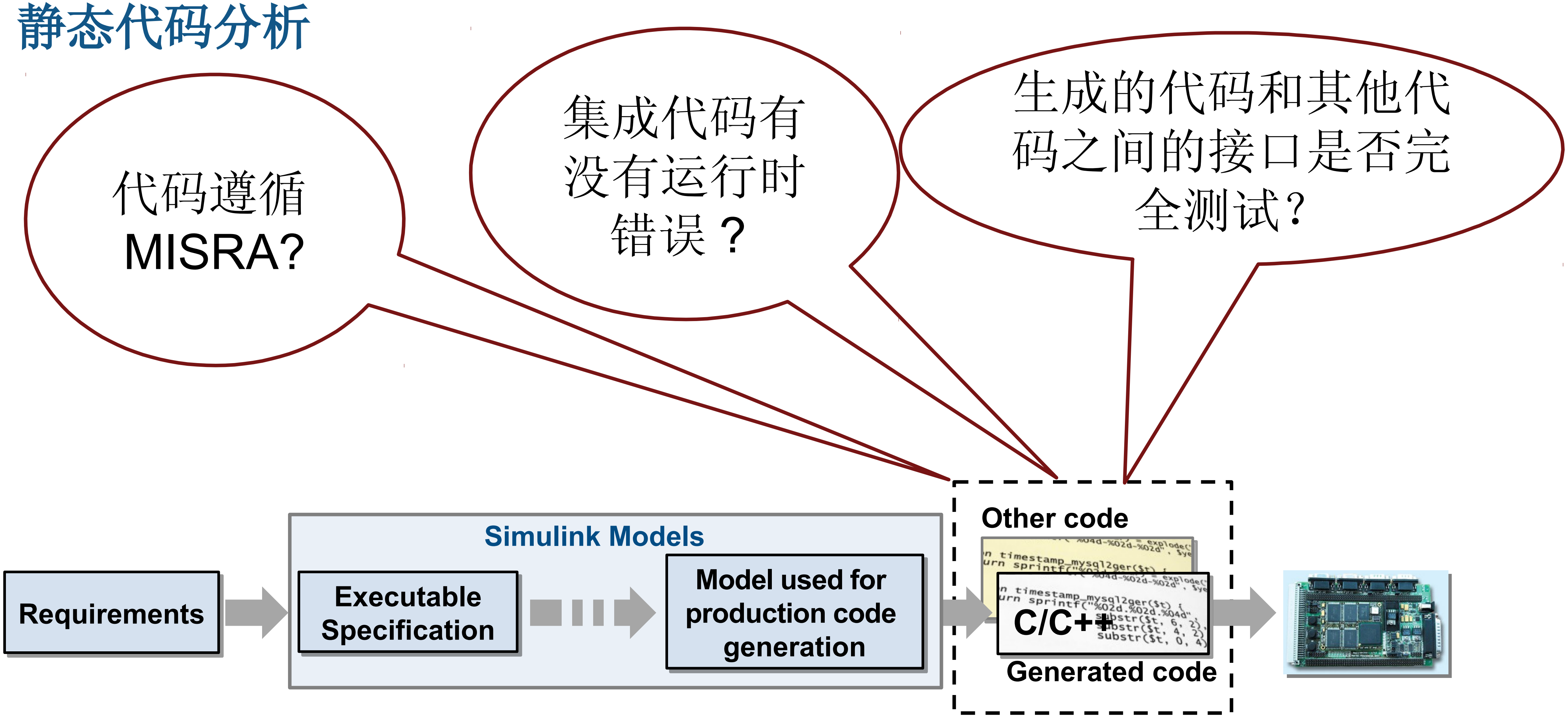
- 确定测试差距
- 丢失需求
- 意想不到的功能
- 设计错误

功能性测试的测试用例生成



- 指定功能测试目标
  - 定义信号在测试用例中必须满足的自定义目标
- 指定功能测试条件
  - 定义信号值约束来限制 test generator

静态代码分析



代码遵循 MISRA?

集成代码有没有运行时错误？

生成的代码和其他代码之间的接口是否完全测试?

Requirements

Simulink Models

Executable Specification

Model used for production code generation

Other code

C/C++

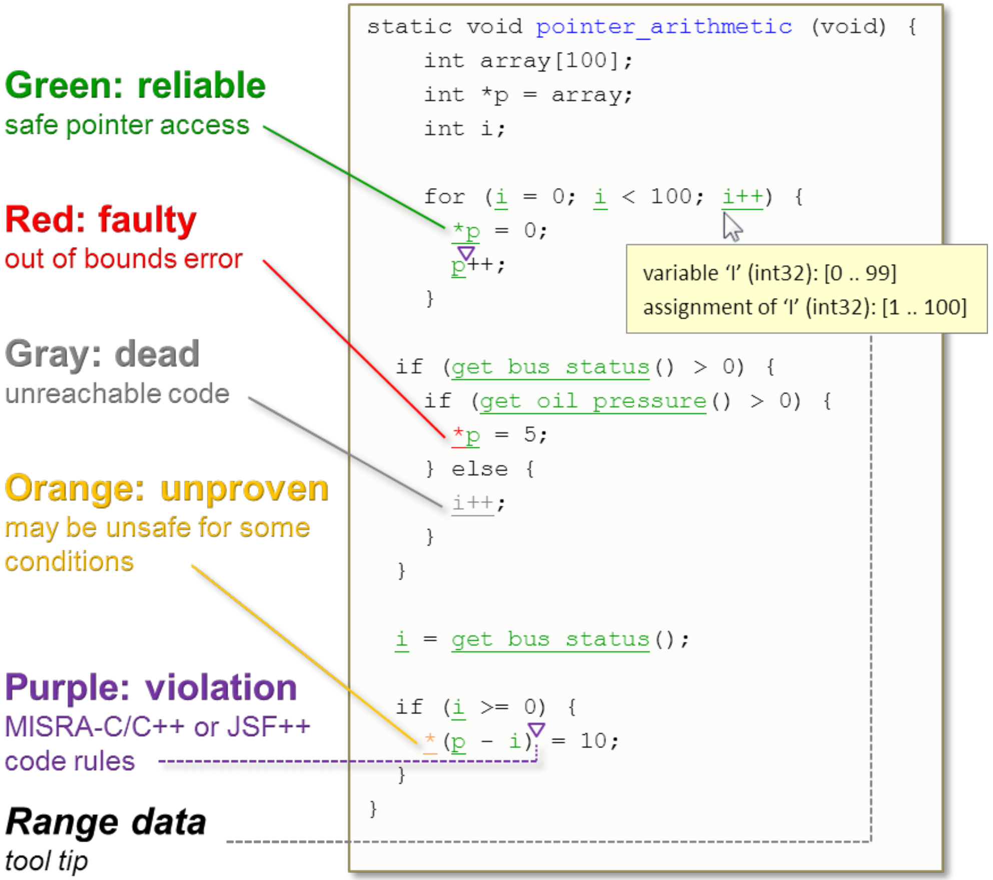
Generated code

The Generated Code is integrated with Other Code (Handwritten)

静态代码分析 Polyspace

- 代码指标和标准
  - 注释密度，圈复杂度 ,...
  - MISRA 及 Cybersecurity标准
  - 支持 DO-178, ISO 26262, ….

- 错误发现和代码验证
  - 检查软件的数据和控制流程
  - 检测错误和安全漏洞
  - 证明没有运行时错误



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

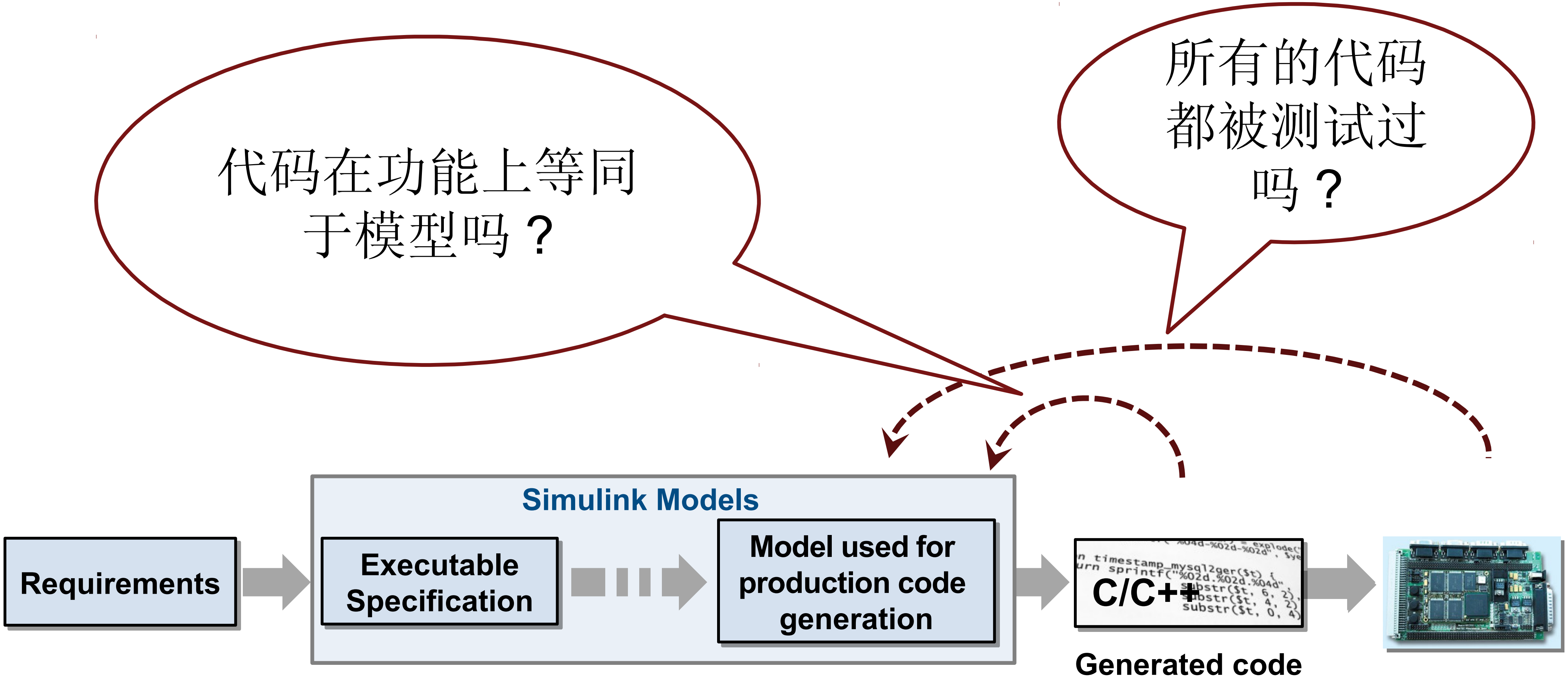
Range data
tool tip

```
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]

Polyspace Code Prover 的结果

等效性测试



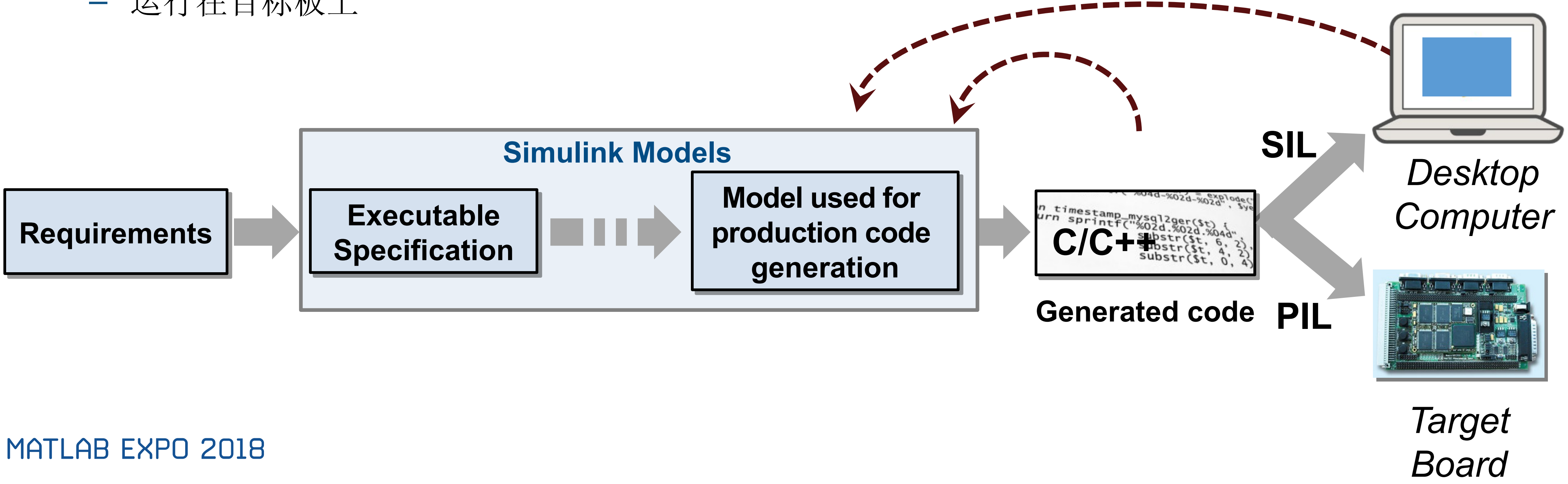
代码在功能上等同于模型吗？

所有的代码都被测试过吗？

等效性测试

- Software in the Loop (SIL)
  - 功能等效性，模型到代码
  - 在台式机 / 笔记本计算机上运行
- Processor in the Loop (PIL)
  - 数值等价，模型到目标码
  - 运行在目标板上

- 重用为模型开发的测试来测试代码
- 收集代码覆盖度指标



使用 IEC 认证套件和 DO 认证套件对工具进行认证

- 对代码生成进行鉴定并验证产品
- 包括文档，测试用例及步骤

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.

Lear 使用基于模型的设计更快地提供高质量的车身控制电子产品

挑战

设计，验证和实现高质量的汽车车身控制电子设备

解决方案

使用基于模型的设计，通过仿真， SIL 和 HIL 测试，实现早期及持续的验证

结果

- 验证需求的时间点提前。 超过 95 %的问题在实现前已经修复，而之前的比例为 30 %
- 开发时间缩短 40 %。 在整个开发周期中生成 700,000 行代码并重用测试用例
- 零保修问题

Lear automotive body electronic control unit.

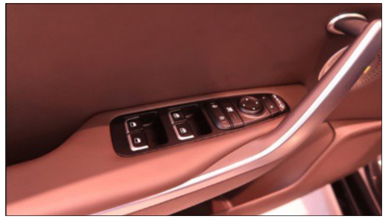
> “我们采用基于模型的设计不仅能够更快地交付质量更好的系统，而且因为我们相信这是一个明智的选择。 最近我们赢得了一个项目，我们的几个竞争对手因时间紧迫而拒绝竞标。 使用基于模型的设计，我们按计划交付了项目，没有任何问题 ."
>
> *- Jason Bauman, Lear Corporation*

Link to user story

参考客户和应用

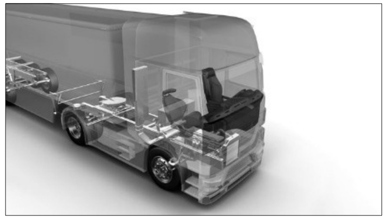
空客直升机通过基于模型的设计加速了 DO-178B 认证软件的开发

软件测试时间缩短了 2/3



LS Automotive 通过基于模型的设计缩短了汽车零部件软件的开发时间

早期检测到规范中的错误



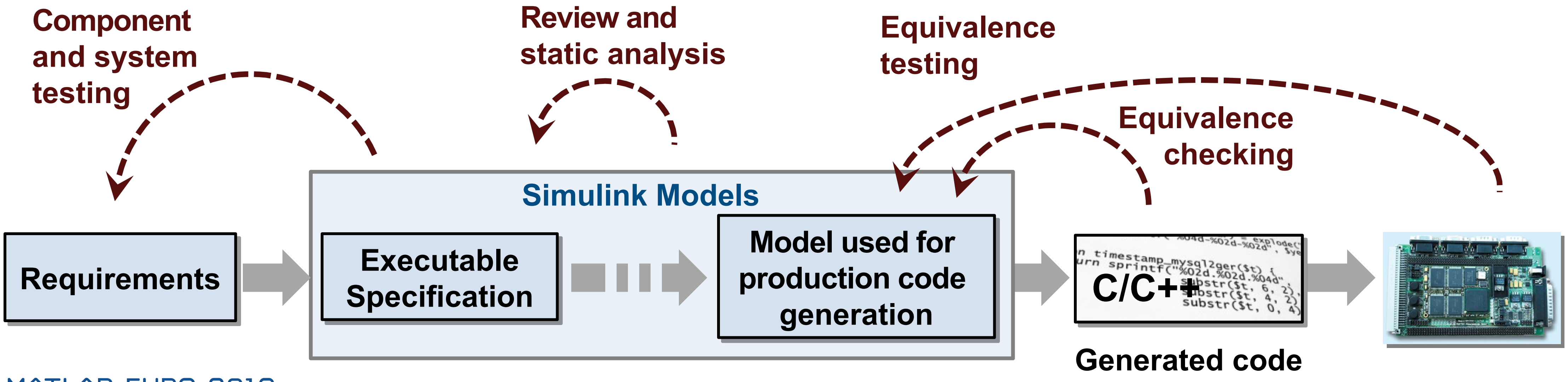
大陆集团为重型卡车开发电子控制空气悬架

验证时间减少高达 50%

More User Stories: www.mathworks.com/company/user_stories.html

总结

- 在 Simulink 中创建，管理需求
- 早期验证以便快速发现错误
- 自动化手工验证任务
- 遵循安全标准的流程



Component and system testing

Review and static analysis

Equivalence testing

Equivalence checking

Simulink Models

Requirements

Executable Specification

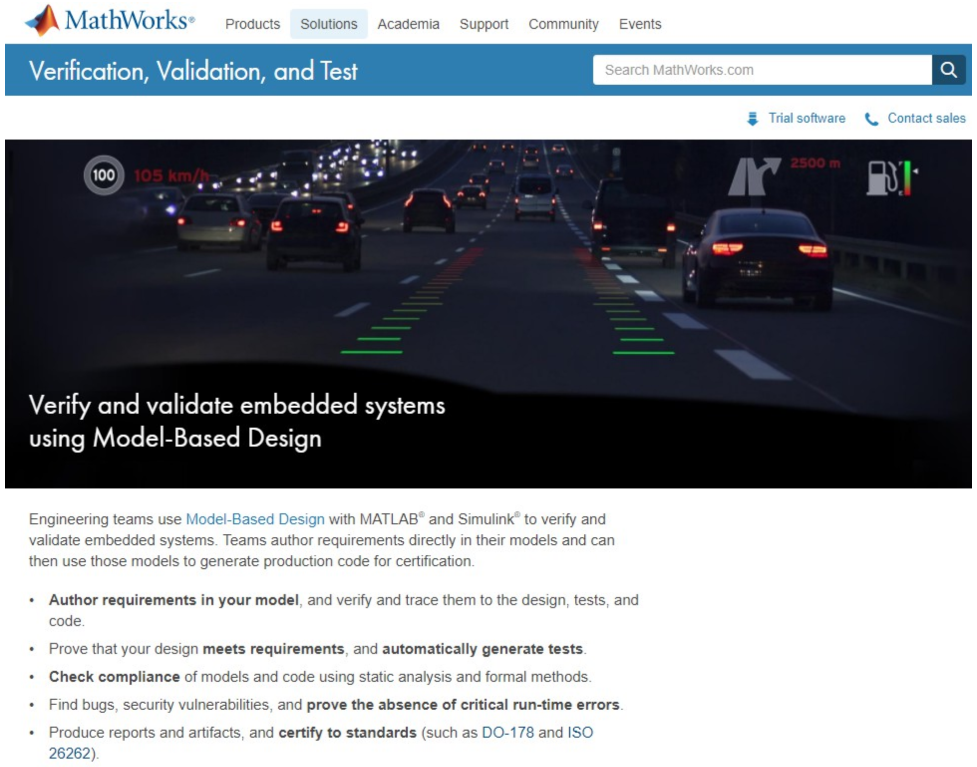
Model used for production code generation

C/C++

Generated code

更多

访问 MathWorks 验证，确认和测试解决方案页面
mathworks.com/solutions/verification-validation.html



Verification, Validation, and Test

Verify and validate embedded systems using Model-Based Design

Engineering teams use Model-Based Design with MATLAB® and Simulink® to verify and validate embedded systems. Teams author requirements directly in their models and can then use those models to generate production code for certification.

- **Author requirements in your model**, and verify and trace them to the design, tests, and code.
- Prove that your design **meets requirements**, and **automatically generate tests**.
- **Check compliance** of models and code using static analysis and formal methods.
- Find bugs, security vulnerabilities, and **prove the absence of critical run-time errors**.
- Produce reports and artifacts, and **certify to standards** (such as DO-178 and ISO 26262).

Thank You!

Backup

Qualify Tools using IEC Certification Kit

for ISO 26262, IEC 61508, and related standards

- Qualify tools, including
  - Embedded Coder
  - Simulink Check
  - Simulink Coverage
  - Simulink Design Verifier
  - Simulink Test
  - Polyspace Bug Finder
  - Polyspace Code Prover
- Support standards, including
  - ISO 26262 (Automotive)
  - IEC 61508 (Industrial)
  - EN 50128 (Rail)
  - IEC 62304 (Medical)

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.

Qualify Tools using DO Qualification Kit

for DO-178, DO-254, and related standards

- Qualify tools, including
  - Simulink Check
  - Simulink Coverage
  - Simulink Code Inspector
  - Simulink Design Verifier
  - Simulink Report Generator
  - Simulink Test
  - Polyspace Bug Finder
  - Polyspace Code Prover
- Support standards, including
  - DO-178 (Flight software)
  - DO-254 (Flight hardware)
  - DO-330 (Tool qualification)

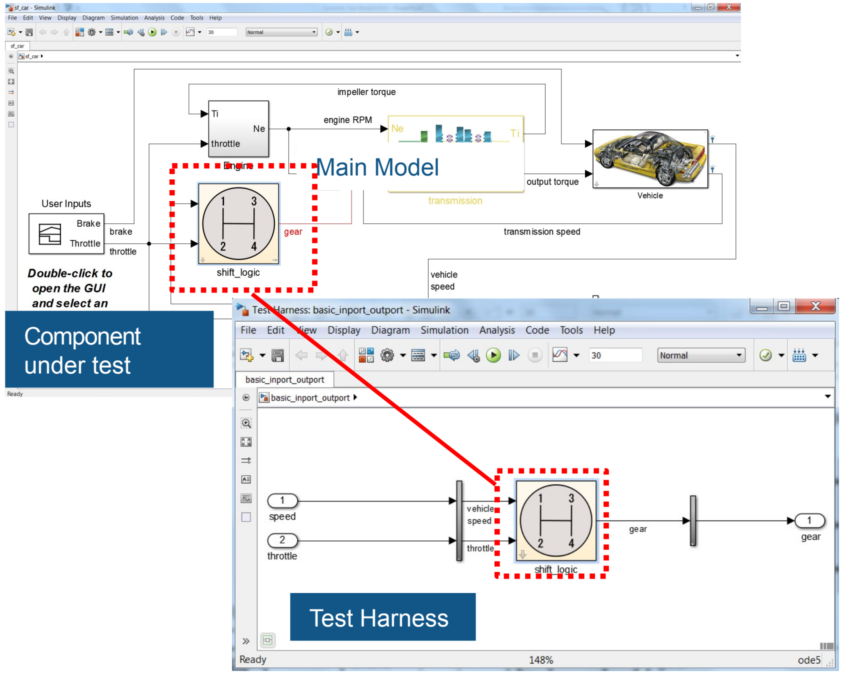
BAE Systems Delivers DO-178B Level A Flight Software on Schedule with Model-Based Design

Primary flight control computers from BAE Systems.

Systematic Functional Testing

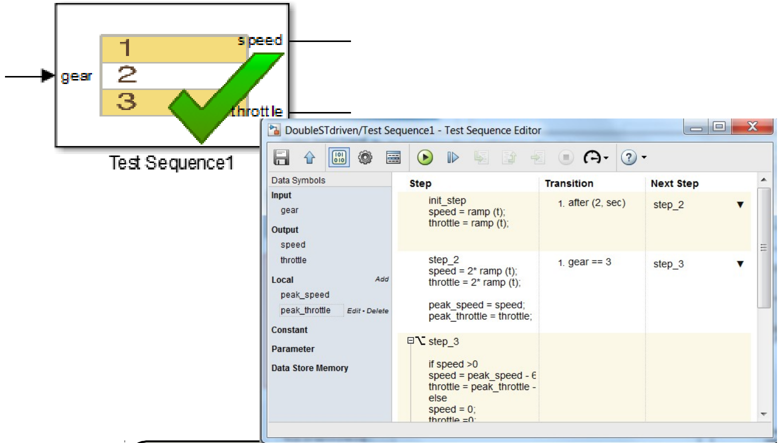
Test Harnesses

- Synchronized, simulation test environment



Test Sequence Block

- Define inputs and assessments based on logical, temporal conditions



Step	Transition	Next Step

init_step
speed = ramp (t);
throttle = ramp (t);
	1. after (2, sec)	step_2

step_2
speed = 2* ramp (t);
throttle = 2* ramp (t);
peak_speed = speed;
peak_throttle = throttle;
	1. gear == 3	step_3

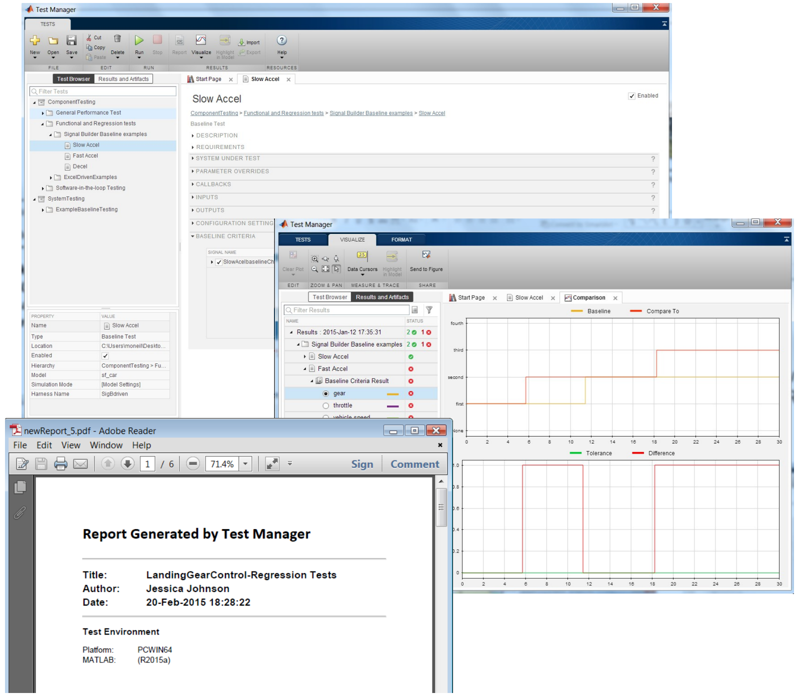
step_3
if speed >0
speed = peak_speed - 6
throttle = peak_throttle -
else
speed = 0;
throttle =0;		

Excel input template and baseline data

R2018a

Test Manager

- Author, execute, manage test cases
- Review, export, report



Property	Value
Enabled	✓
Hierarchy	ComponentTesting > Fu...
Model	sf_car
Simulation Mode	[Model Settings]
Harness Name	SigBdriven

Report Generated by Test Manager

Title: LandingGearControl-Regression Tests
Author: Jessica Johnson
Date: 20-Feb-2015 18:28:22

Test Environment

Platform: PCWIN64
MATLAB: (R2015a)

MATLAB EXPO 2018

Model and Code Coverage identifies gaps in testing

Model Coverage

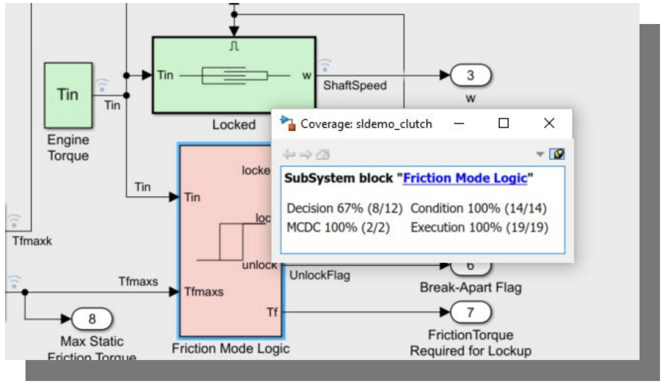
- Measure test completeness
- Identify missing tests or unintended functionality

Generated Code Coverage

- Find untested generated code
- Map results from code to model object

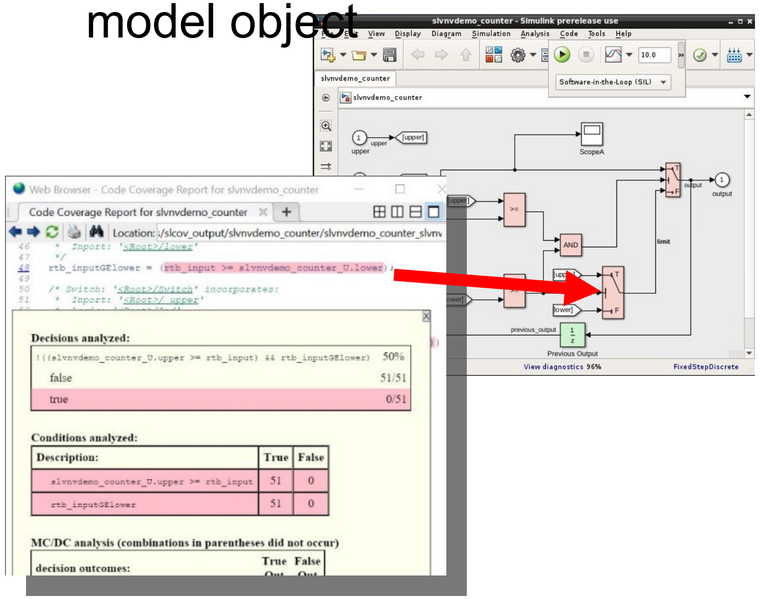
Highlighting and Reporting

- View coverage results on diagrams
- Manage accumulated coverage results



SubSystem block "Friction Mode Logic"

Decision 67% (8/12) Condition 100% (14/14)
MCDC 100% (2/2) Execution 100% (19/19)


slvnvdemo_counter - Simulink prerelease use
View
Display
Diagram
Simulation
Analysis
Code
Tools
Help
slvnvdemo_counter
Software-in-the-Loop (SIL)
upper
[upper]
ScopeA
output
AND
limit
previous_output
Previous Output
View diagnostics 96%
FixedStepDiscrete
Web Browser - Code Coverage Report for slvnvdemo_counter
Code Coverage Report for slvnvdemo_counter
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:

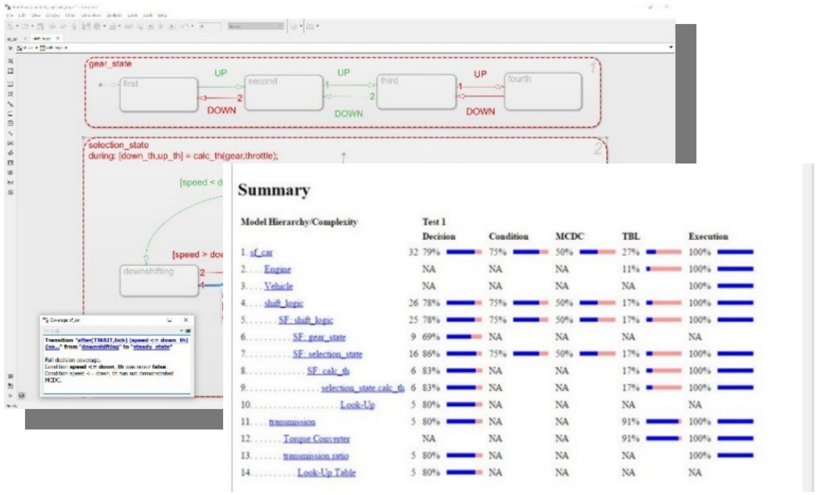
!((slvnvdemo_counter_U.upper >= rtb_input) && rtb_inputGElower)	50%
false	51/51
true	0/51

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

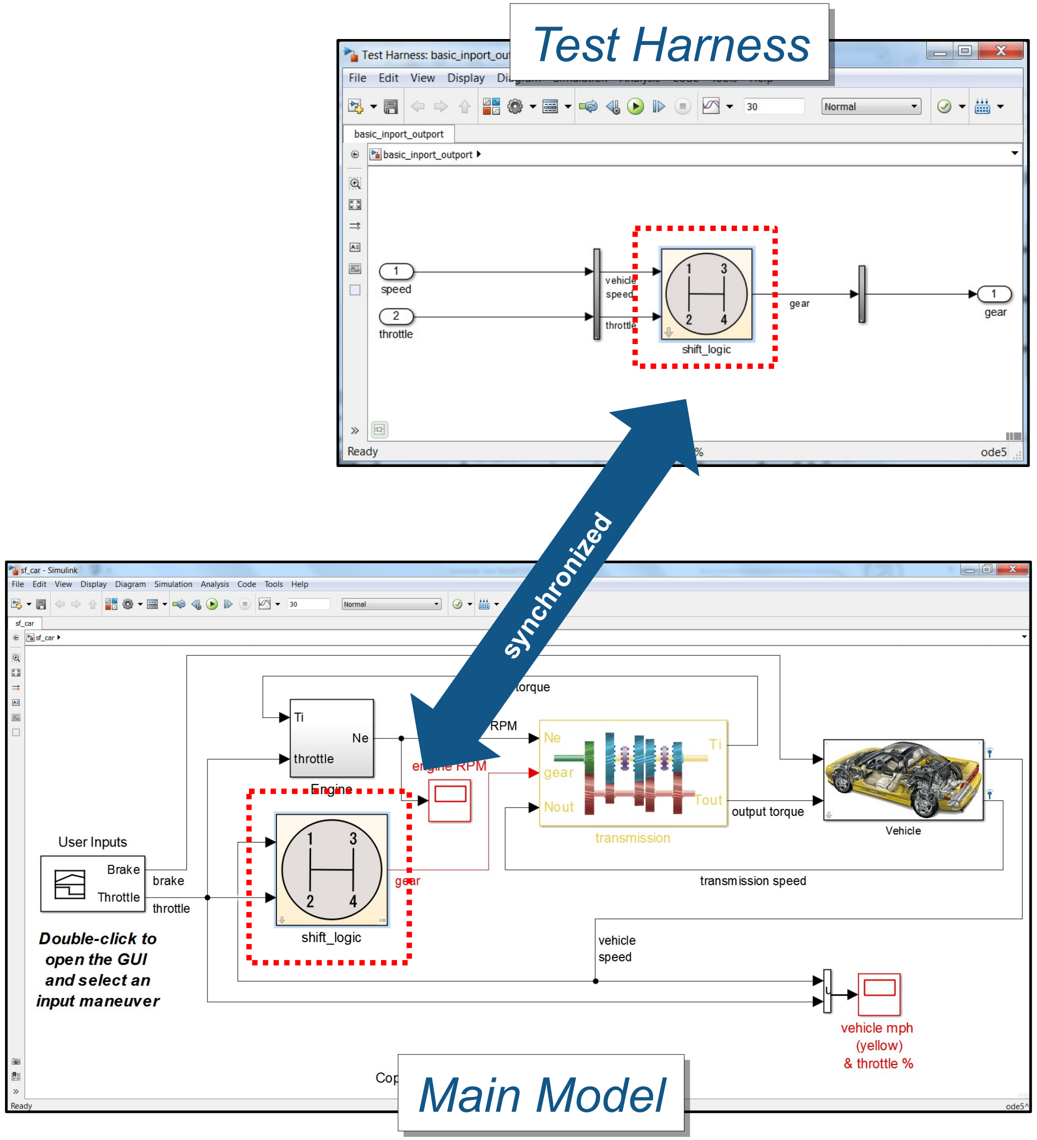


Summary

Model Hierarchy/Complexity		Test 1 Decision	Condition	MCDC	TBL	Execution
1. sf_car	32	79%	75%	50%	27%	100%
2. . . . Engine		NA	NA	NA	11%	100%
3. . . . Vehicle		NA	NA	NA	NA	100%
4. . . . shift_logic	26	78%	75%	50%	17%	100%
5. . . . . . . SF: shift_logic	25	78%	75%	50%	17%	100%
6. . . . . SF: gear_state	9	69%	NA	NA	NA	NA
7. . . . . SF: selection_state	16	86%	75%	50%	17%	100%
8. . . . . SF: calc_th	6	83%	NA	NA	17%	100%
9. . . . . selection_state.calc_th	6	83%	NA	NA	17%	100%
10. . . . . Look-Up	5	80%	NA	NA	NA	NA
11. . . . transmission	5	80%	NA	NA	91%	100%
12. . . . . . . Torque Converter		NA	NA	NA	91%	100%
13. . . . . . . transmission ratio	5	80%	NA	NA	NA	100%
14. . . . . Look-Up Table	5	80%	NA	NA	NA	NA

Test Harness

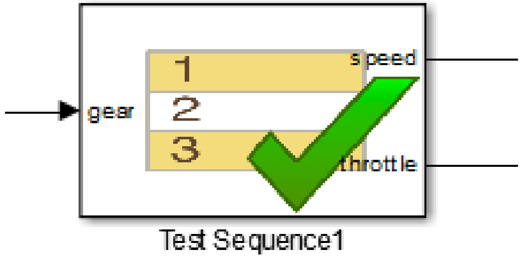
- ✓ Harnesses contained in the model file or external
- ✓ Build harness at unit (subsystem) or system level
- ✓ Synchronized test environment (harness ←→ model)
- ✓ Enables unit testing without requiring new model
- ✓ Configure harness input and output blocks
- ✓ Supports SIL, PIL, HIL

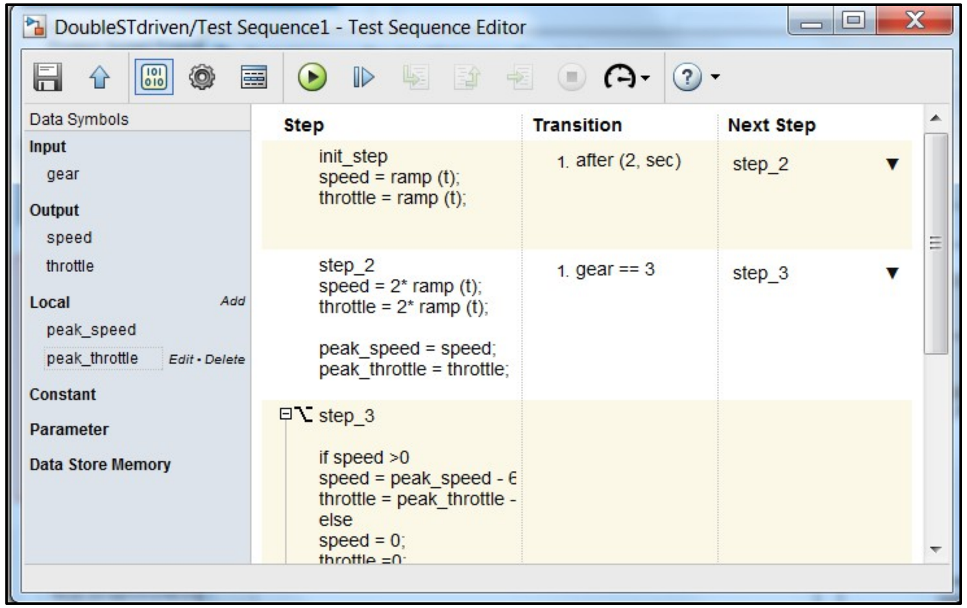


Double-click to open the GUI and select an input maneuver

Test Sequence/Assessment Block

- ✓ Reactive and/or time based test cases
- ✓ Easier translation of test procedures
- ✓ Built on top of Stateflow with extensions for testing (SF license not required)
- ✓ Subset of MATLAB language
- ✓ Steps are temporal or logic-based
- ✓ Create complex test inputs and assessments
- ✓ Supports debugging (breakpoints)




DoubleSTdriven/Test Sequence1 - Test Sequence Editor

Data Symbols

Input
gear

Output
speed
throttle

Local *Add*
peak_speed
peak_throttle *Edit • Delete*

Constant

Parameter

Data Store Memory

Step	Transition	Next Step

init_step
speed = ramp (t);
throttle = ramp (t);
	1. after (2, sec)	step_2 ▼

step_2
speed = 2* ramp (t);
throttle = 2* ramp (t);
 	
peak_speed = speed;
peak_throttle = throttle;
	1. gear == 3	step_3 ▼

⊟ step_3
 	
if speed >0
speed = peak_speed - 6
throttle = peak_throttle -
else
speed = 0;
throttle =0;		