

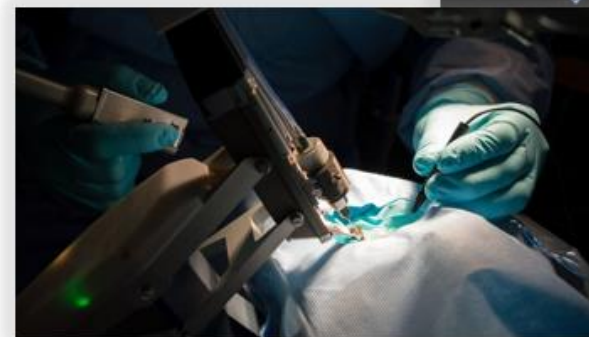
MATLAB EXPO

动态测试和静态分析的自动化加速行业标准认证
胡乐华, MathWorks 中国高级应用工程师



复杂系统认证和交付的巨大挑战

- 需要满足行业或客户的标准
 - DO-178C (航空), ISO 26262 (汽车), IEC 62304 (医疗器械), IEC 61508 (电气/电子), MISRA等.
- 关键安全系统项目的时间和成本是一般的20~30倍之多*
- 开发周期后期发现问题导致成本急剧上升



*Source: [Certification Requirements for Safety-Critical Software](#)

Table 5 — Notations for software unit design

Notations		ASIL			
		A	B	C	D
1a	Natural language ^a	++	++	++	++
1b	Informal notations	++	++	+	+
1c	Semi-formal notations ^b	+	+	++	++
1d	Formal notations	+	+	+	+

^a Natural language can complement the use of notations for example where some topics are more readily expressed in natural language or provide an explanation and rationale for decisions captured in the notations.

EXAMPLE To avoid possible ambiguity of natural language when designing complex elements, a combination of an activity diagram with natural language can be used.

^b Semi-formal notations can include pseudocode or modelling with UML®, SysML®, Simulink® or Stateflow®.

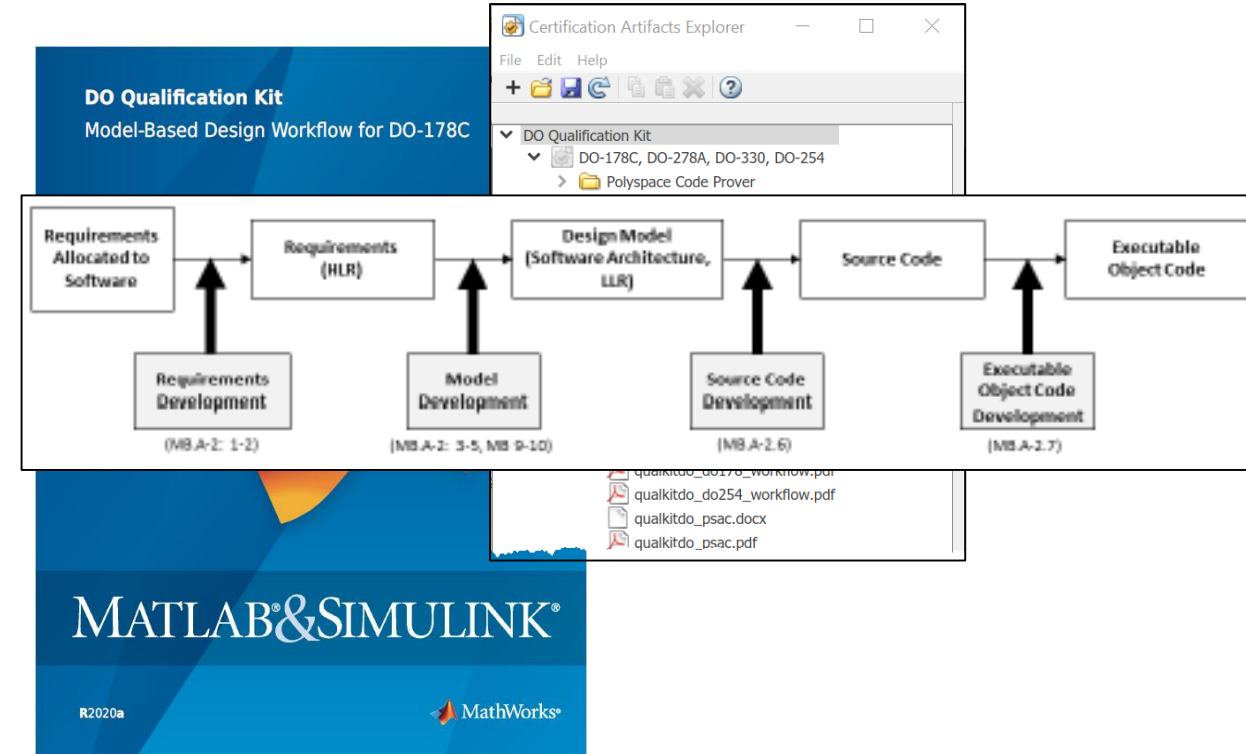
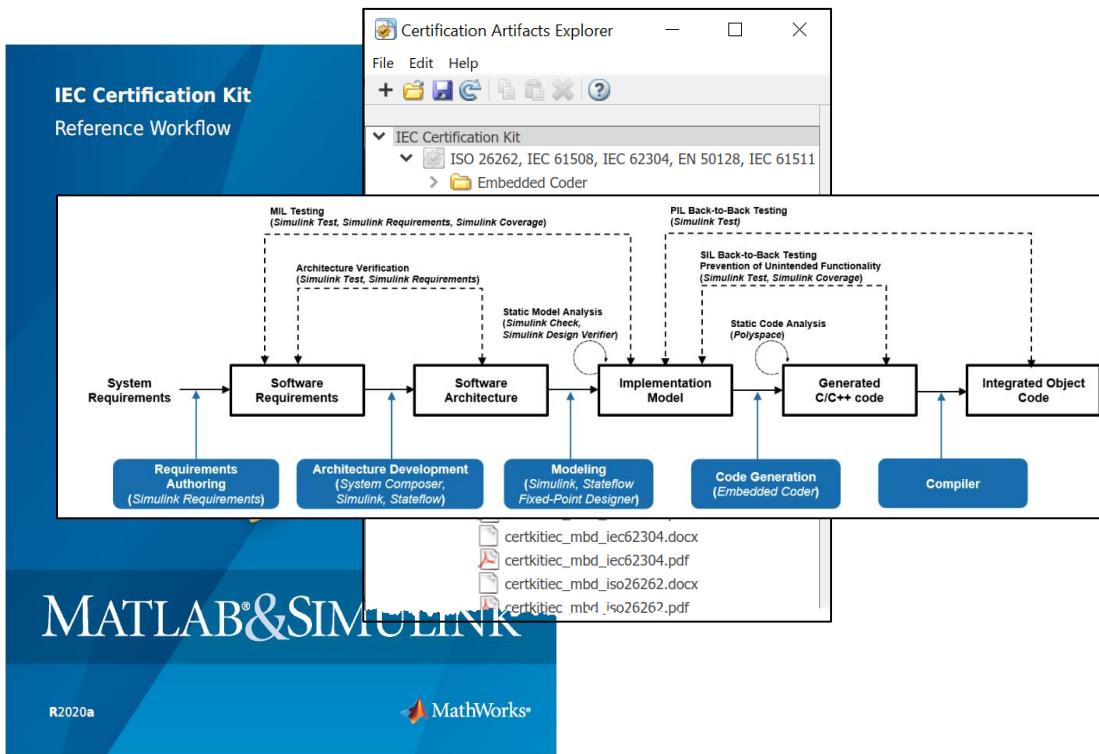
NOTE UML®, SysML®, Simulink® and Stateflow® are examples of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of these products.

NOTE In the case of model-based development with automatic code generation, the methods for representing the software unit design are applied to the model which serves as the basis for the code generation.

表 2 Software Architecture Design 也有同样的表述

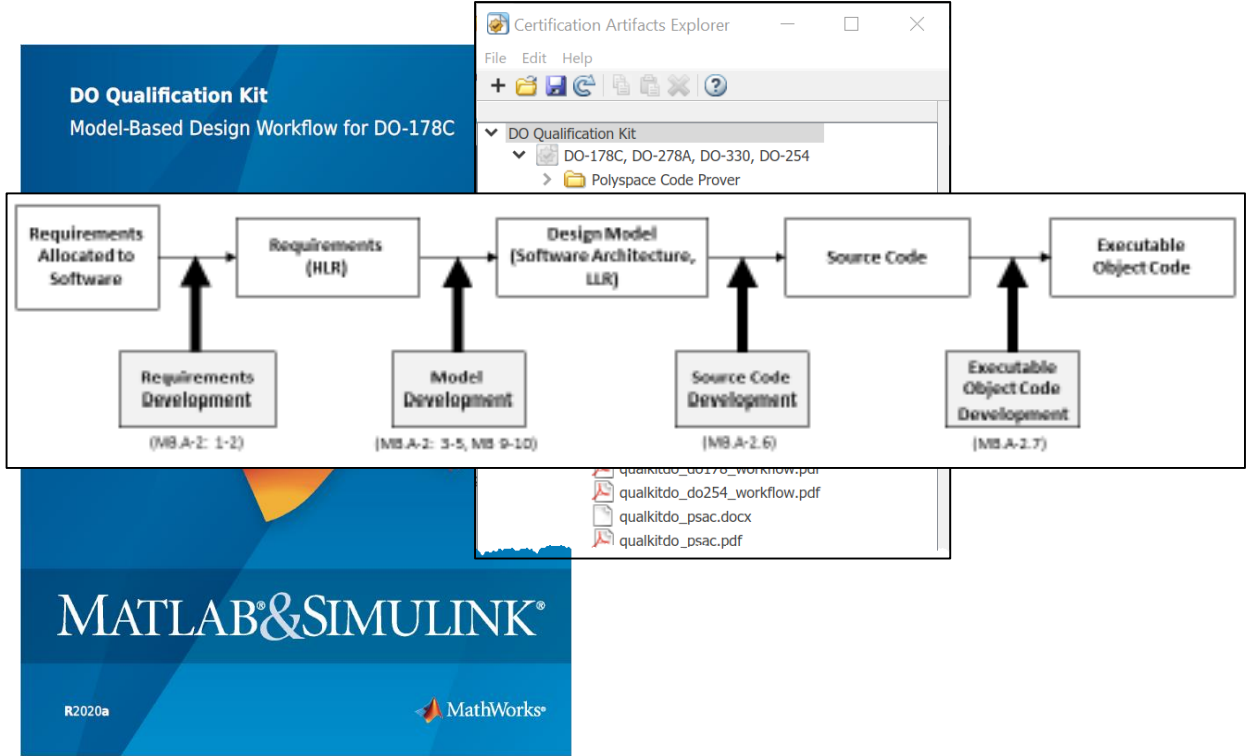
使用 IEC Certification Kit 和 DO Qualification Kit 进行工具认证

- 能够对代码生成和验证产品工具进行认证
- 包含文档、测试用例和认证流程



使用 IEC Certification Kit 和 DO Qualification Kit 进行工具认证

- 能够对代码生成和验证产品工具进行认证
- 包含文档、测试用例和认证流程



使用 IEC Certification Kit 和 DO Qualification Kit 进行工具认证

- 能够对代码生成和验证产品工具进行认证
- 包含文档、测试用例和认证流程

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.

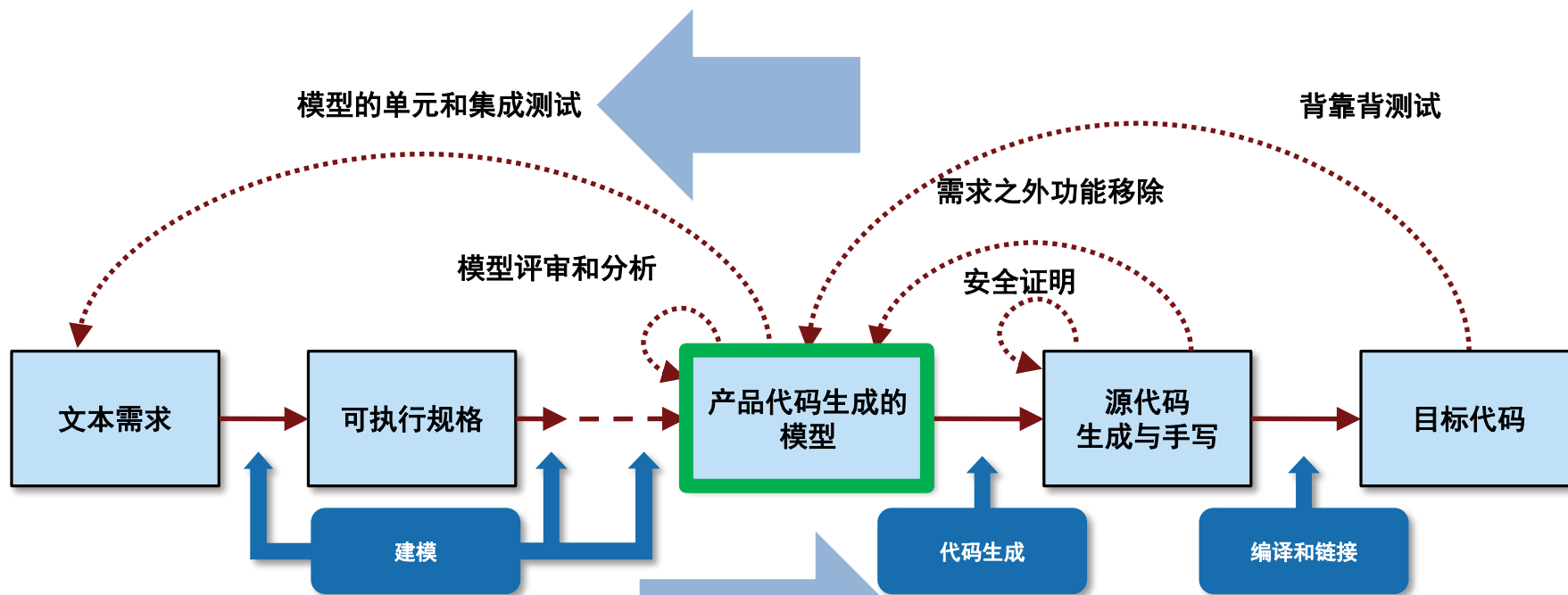
使用参考流程满足认证标准

模型验证

在设计阶段发现设计缺陷

代码验证

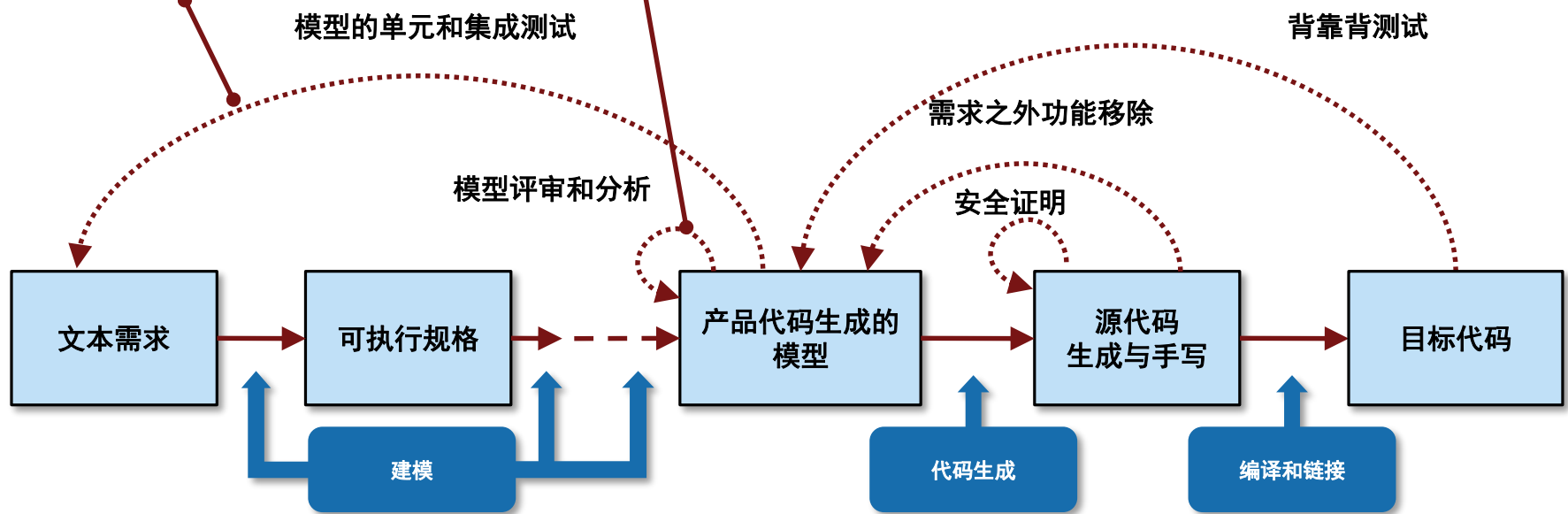
在代码层面提高可靠度



模型验证: 在设计阶段发现设计缺陷

模型验证

- 需求管理
- 基于需求的测试
- 测量模型覆盖率
- 模型覆盖度测试
- 标准服从性检查
- 设计缺陷检查
- 模型行为证明

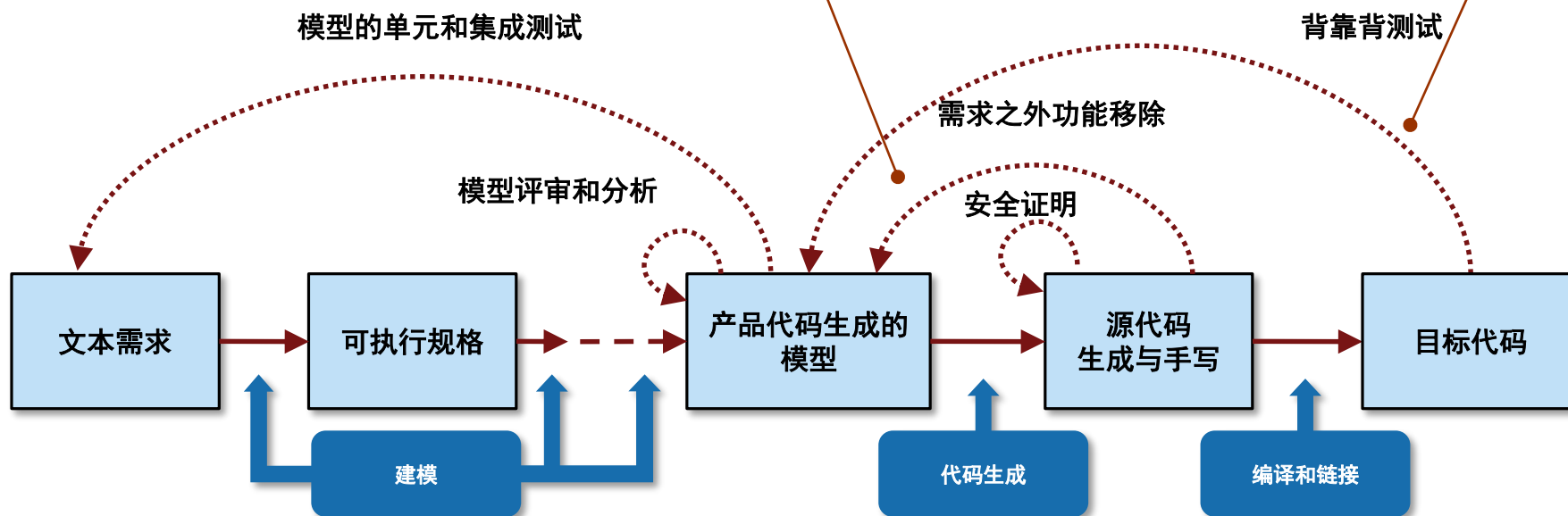


代码验证: 在代码层面提高可靠度

代码验证

- 代码与模型和需求追述
- 代码覆盖度测试
- SIL/PIL 一致性测试

- 生成测试向量, 达到代码100%覆盖
- 代码缺陷检查
- 无运行时错误证明



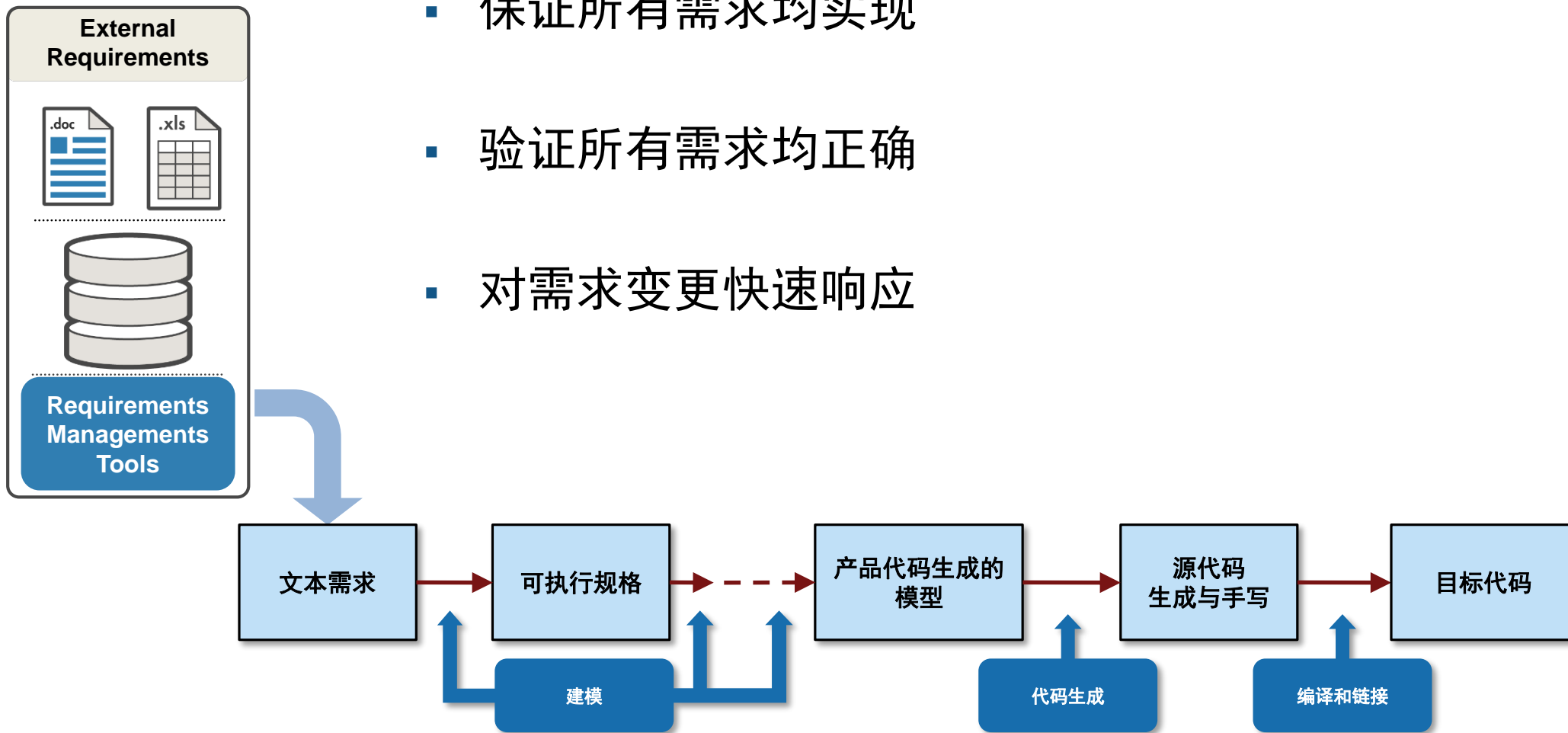
模型验证

- 需求管理
- 基于需求的测试
- 测量模型覆盖率
- 模型覆盖度测试
- 标准服从性检查
- 设计缺陷检查
- 模型行为证明

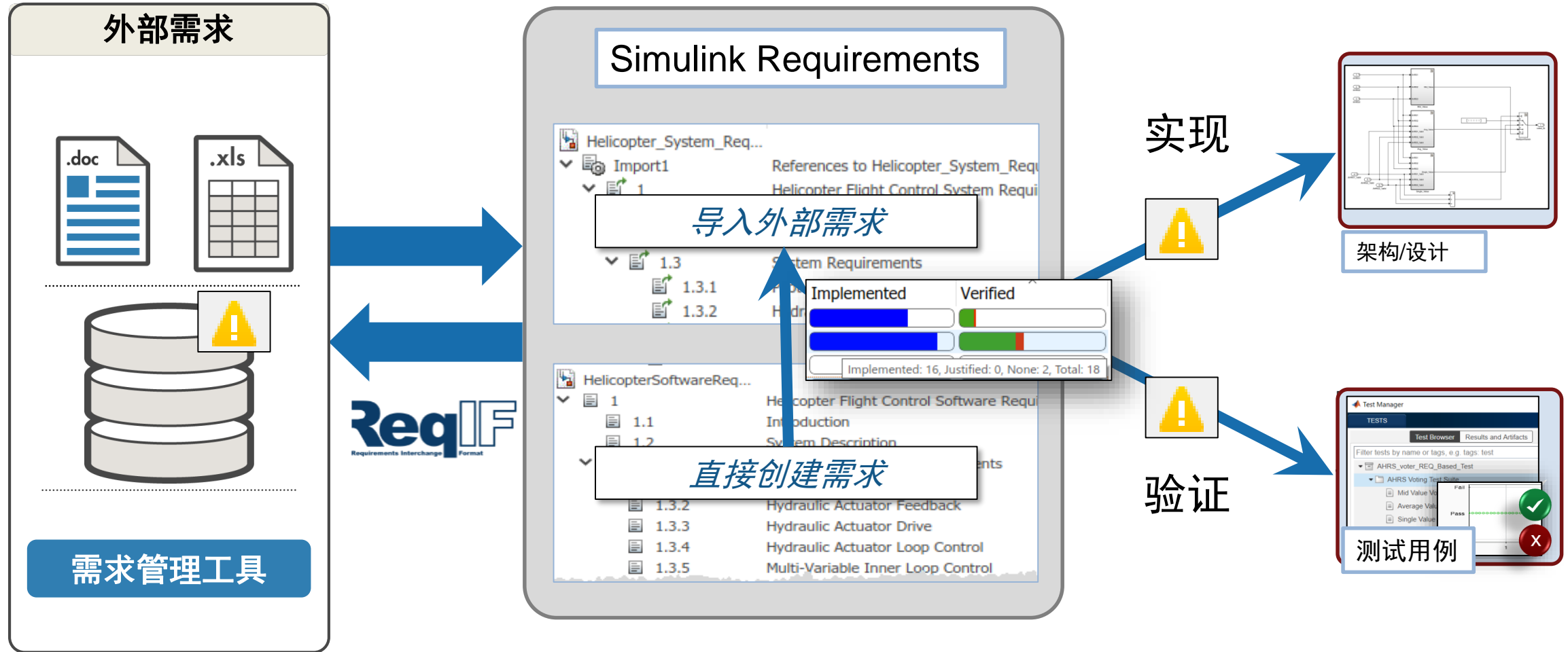
模型的单元和集成测试



需求管理



将需求、架构和设计放在一个框架下工作



演示: 需求视图

The screenshot displays a Simulink model for a cruise control system and its associated requirements table. The model includes inputs for 'enable', 'brake', 'speed', 'set', 'inc', and 'dec'. It features logic blocks for AND, OR, and NOT, along with a PI Controller and a target speed computation block. A requirement 'ENABLE: Engage cruise control' is shown to be implemented by the model.

Requirements - cruiseControlRBTcovExample

Index	Summary	Implemented	Verified
1	Set target speed	100%	100%
2	Brake disengages cruise control	100%	100%
3	Engage cruise control	100%	100%
4	Increment set speed	100%	100%
5	Decrement set speed	100%	100%
6	Throttle to maintain set speed	100%	100%
1	Disable Throttle when Braking	0%	0%

测试和需求的追溯性

The screenshot displays a Simulink model for a cruise control system. The model includes inputs for enable, brake, speed, set, inc, and dec. It features logic blocks for AND, OR, NOT, and a PI Controller. Key components include 'Active Control', 'Determine if the control is active', 'Compute the target speed', and 'PI Controller'. The output is 'throt' (throttle). Below the model is a Requirements table for 'cruiseControlRBTcovExample'.

Index	Summary	Implemented	Verified
1	SET button locks set speed	Blue bar	Yellow bar
2	Applying BRAKE disengages cruise control	Blue bar	Yellow bar
3	ENABLE button engages cruise control	Blue bar	Yellow bar
4	INCREMENT button increases set speed	Blue bar	Green bar
5	DECREMENT button decreases set speed	Blue bar	Green bar
6	THROTTLE applied smoothly if speed differs from target	Blue bar	Red bar

The Test Manager interface shows a list of tests under the 'cruiseControlRBTcovTests' suite. The tests listed are:

- Set Speed Test
- Brake Test
- Enable Test
- Increment Test
- Decrement Test
- Throttle Test

测试验证状态

- 通过 (Pass) - Green square
- 不通过 (Fail) - Red square
- 未执行 (Not Executed) - Yellow square
- 无测试用例 (No Test Case) - White square with black border

使用追溯性矩阵审查和分析追溯关系

Summary	Implemented	Verified
SET button locks set speed		
Applying BRAKE disengages cruise control		
ENABLE button engages cruise control		
INCREMENT button increases set speed		
DECREMENT button decreases set speed		
THROTTLE applied smoothly if speed differs from target		

需求与测试用例没有建立关联

使用追溯性矩阵审查和分析追溯关系

- 需求、模型和测试追溯性审查
- 建立筛选视图
- 高亮缺失的关联
- 创建关联，补充缺失

The screenshot shows the Traceability Matrix tool interface. The main window displays a traceability matrix for 'Simulink Requirements vs Simulink Test'. The matrix is organized into columns for requirements and tests. A red circle highlights a specific cell in the matrix, and a context menu is open over it, showing options for 'Left', 'Top', and 'Link'. The context menu is set to 'None (Create)'. Below the main grid, a summary table is visible, showing the status of various requirements.

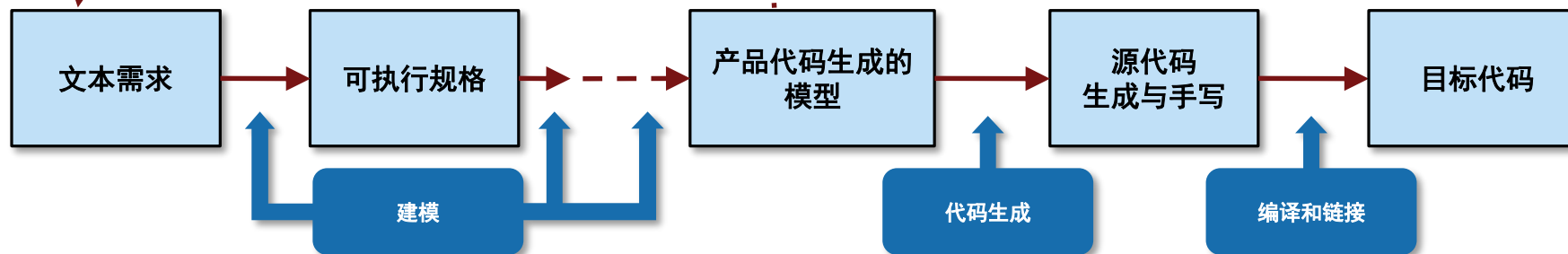
Summary	Implemented	Verified
SET button locks set speed	Blue bar	Green bar with red segment
Applying BRAKE disengages cruise control	Blue bar	Green bar
ENABLE button engages cruise control	Blue bar	Green bar
INCREMENT button increases set speed	Blue bar	Green bar
DECREMENT button decreases set speed	Blue bar	Green bar
THROTTLE applied smoothly if speed differs from target	Blue bar	Red bar

模型的系统功能测试

模型验证

- 需求管理
- **基于需求的测试**
- 测量模型覆盖率
- 模型覆盖度测试
- 标准服从性检查
- 设计缺陷检查
- 模型行为证明

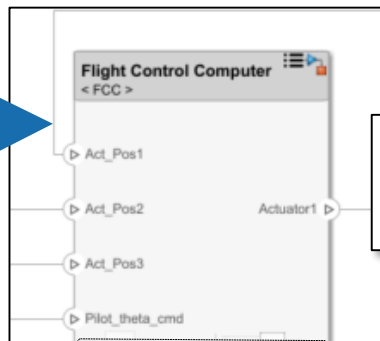
模型的单元和集成测试



使用 Simulink Test 进行基于需求的验证

功能需求
飞行控制系统应...

被实现



System Composer /
Simulink /
Stateflow

被验证

测试用例

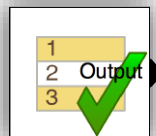
测试输入



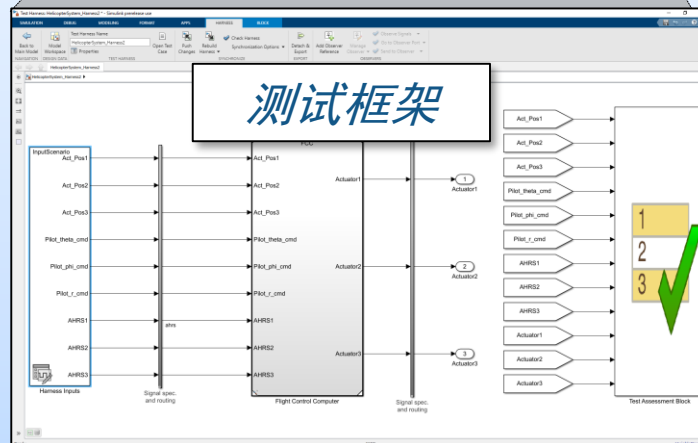
MAT / Excel
file (input)



Signal Editor



Test Sequence



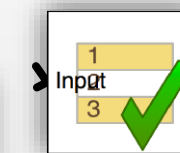
测试框架

Simulink Test

输出评估



MAT / Excel
File (baseline)



Test
Assessments

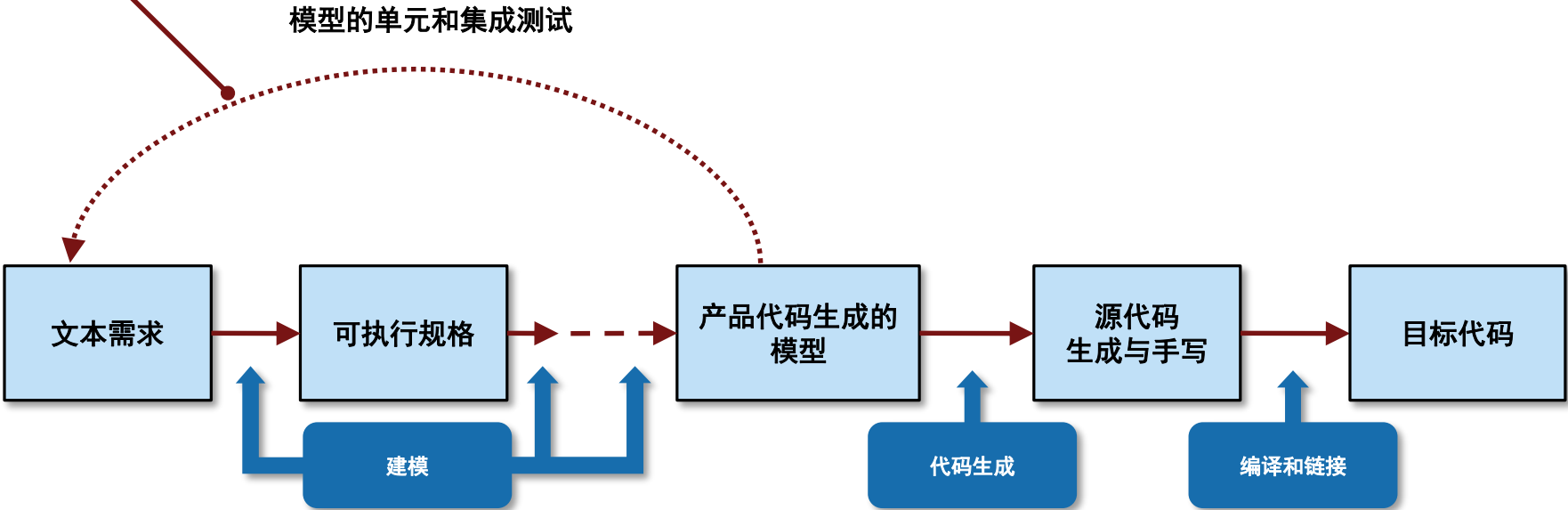
```
function customCriteria  
Perform custom criteria  
1 test.verifyThat(test.sl
```

MATLAB Unit Test

测试完整性度量

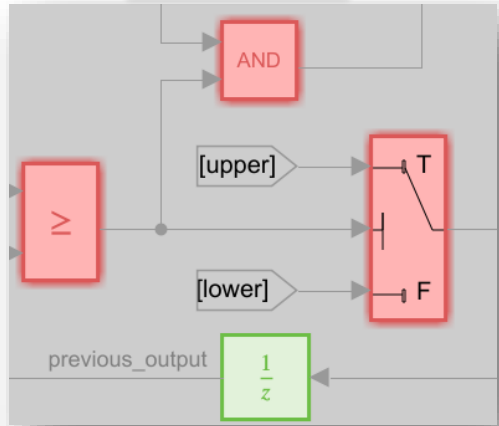
模型验证

- 需求管理
- 基于需求的测试
- 测量模型覆盖率**
- 模型覆盖度测试
- 标准服从性检查
- 设计缺陷检查
- 模型行为证明



覆盖度分析

Simulink



Stateflow



Code

Coverage annotation

Links to model element

```

Code
rtwdemo_sil_topmodel.c
99 /* Output and update for enable system: '<Root>/CounterTypeB' */
100 static void CounterTypeB(void)
101 {
102     /* Outputs for Enabled SubSystem: '<Root>/CounterTypeB' incorporates:
103      * EnablePort: '<S2>/Enable'
104      */
105     if (enable) {
106         /* Decision covered false, but not true
107          * Inport: '<Root>/reset'
108          * Inport: '<Root>/ticks_to_count'
109          * Output: '<Root>/count_b'
110          * Sum: '<S2>/Add'
111          */
112     }
113     if (rtu.reset) {
114         rtv.count_b = 0;
    
```

Tooltip with code coverage results

- 识别测试不足
- 需求不全
- 非需要功能
- 设计错误

Coverage Reports

Summary

Model Hierarchy/Complexity	Test 1	Decision	Condition	MCDC	Execution	Relational Boundary	Saturation on integer overflow
1. sidemo_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	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%

覆盖度结果中测试和需求的追溯关系

NAME

- Results: 2020-Mar-02 22:14:00
- cruseControlRBTcovTests
 - Cruise Control Test Suite
 - Brake Test
 - Decrement Test
 - Enable Test
 - Increment Test
 - Set Speed Test
 - Throttle Test

Coverage Details

2. SubSystem block "Controller"

[Justify or Exclude](#)

Parent: [/cruseControlRBTcovExample](#)

Child Systems: [PI Controller](#)

Metric	Coverage (this object)	Coverage (inc. descendants)
Cyclomatic Complexity	0	7
Condition	NA	100% (12/12) condition outcomes
Decision	NA	100% (12/12) decision outcomes
Execution	NA	100% (17/17) objective outcomes

Logic block "[Logical Operator](#)"

[Justify or Exclude](#)

Requirement Testing Details

Implemented Requirements	Verified by Tests	Associated Runs
Brake disengages cruise control	Brake Test	T2
Engage cruise control	Enable Test	T3

Parent: [cruseControlRBTcovExample/Controller](#)

Metric	Coverage
Cyclomatic Complexity	0
Condition	100% (6/6) condition outcomes
Execution	100% (1/1) objective outcomes

Conditions analyzed

Description	Time	Exec

Requirements - cruseControlRBTcovExample

View: Requirements

Index	ID	Summary	Implemented	Verified
cruseControlRBTcovReqs				
1	SET_SPEED	Set speed	 	
2	BRAKE	Brake disengages cruise control	 	
3	ENABLE	Engage cruise control	 	
4	INCREMENT	Increment set speed	 	
5	DECREMENT	Decrement set speed	 	
6	THROTTLE	Throttle to maintain set speed	 	

模型覆盖度限定在基于需求测试中

NAME	STATUS
Results: 2020-Mar-02 22:14:00	6
cruiseControlRBTCovTests	6
Cruise Control Test Suite	6
Brake Test	
Decrement Test	
Enable Test	
Increment Test	
Set Speed Test	
Throttle Test	

AGGREGATED COVERAGE RESULTS

Create a coverage report from coverage results to justify or exclude missing coverage. The filters and updated coverage values will be displayed with this result.

ANALYZED MODEL	REPORT	COMPLEXI...	DECISION	CONDITION	EXECUTION
cruiseControlRBTCovExample		8	92%	100%	76%

Scope coverage results to linked requirements + Add Tests for Missing Coverage Export

模型覆盖度限定在基于需求测试中

R2020a

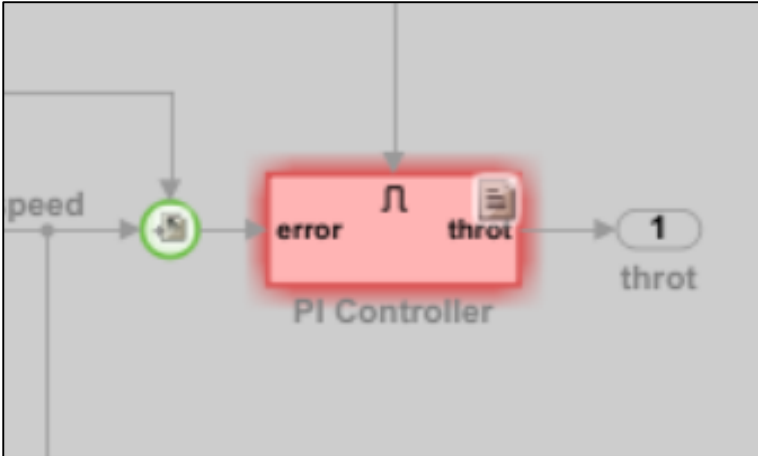
The screenshot displays the MATLAB Simulink environment. The main workspace shows a Simulink model for a cruise control system. A blue callout box with the text "识别未关联需求" (Identify unassociated requirements) points to a red circle in the model. The Requirements table at the bottom shows a requirement with index 6 and ID THROTTLE. The Coverage Details window on the right shows the coverage for a Constant block, with a table indicating 0% coverage for the block executed.

识别未关联需求

Index	ID	Summary	Implemented
6	THROTTLE	Throttle to maintain set speed	<div style="width: 100%; height: 10px; background-color: blue;"></div>

Block executed	Coverage
	0%
	-- 11

覆盖度结果中测试和需求的追溯关系

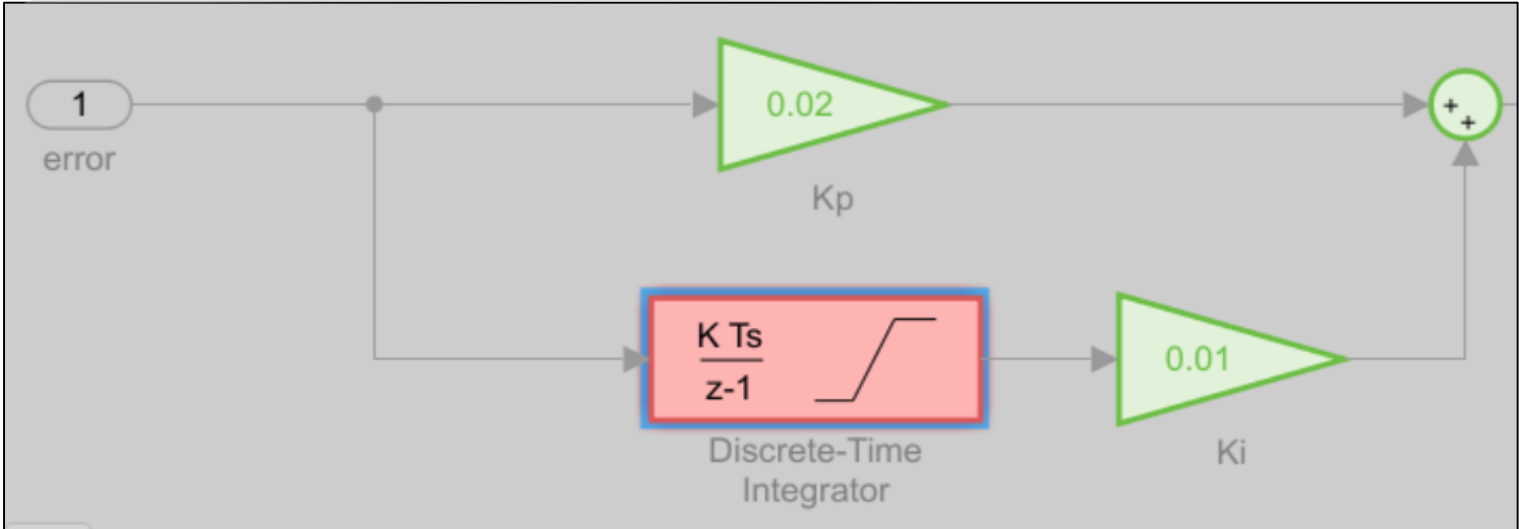


3. SubSystem block "PI Controller"

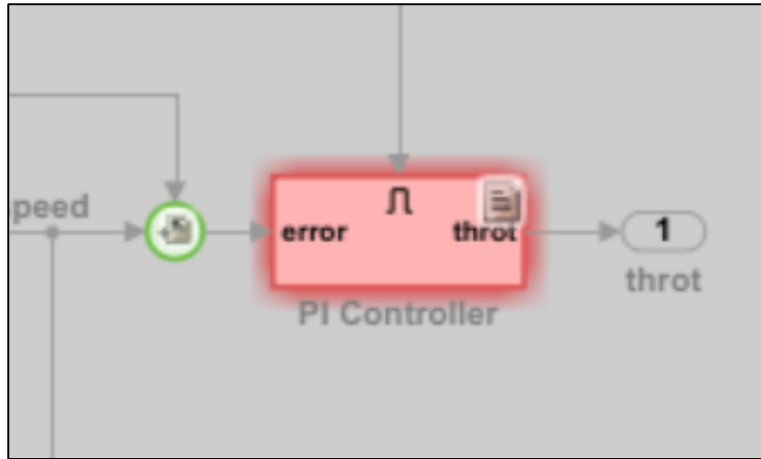
[Justify or Exclude](#)

Requirement Testing Details

Implemented Requirements	Verified by Tests	Associated Runs
Throttle to maintain set speed	Throttle Test	T6



覆盖度结果中测试和需求的追溯关系



3. SubSystem block "[PI Controller](#)"

[Justify or Exclude](#)

Requirement Testing Details

Implemented Requirements	Verified by Tests	Associated Runs
Throttle to maintain set speed	Throttle Test	T6

DiscreteIntegrator block "[Discrete-Time Integrator](#)"

[Justify or Exclude](#)

Parent: [cruiseControlRBTCovExample/Controller/PI Controller](#)

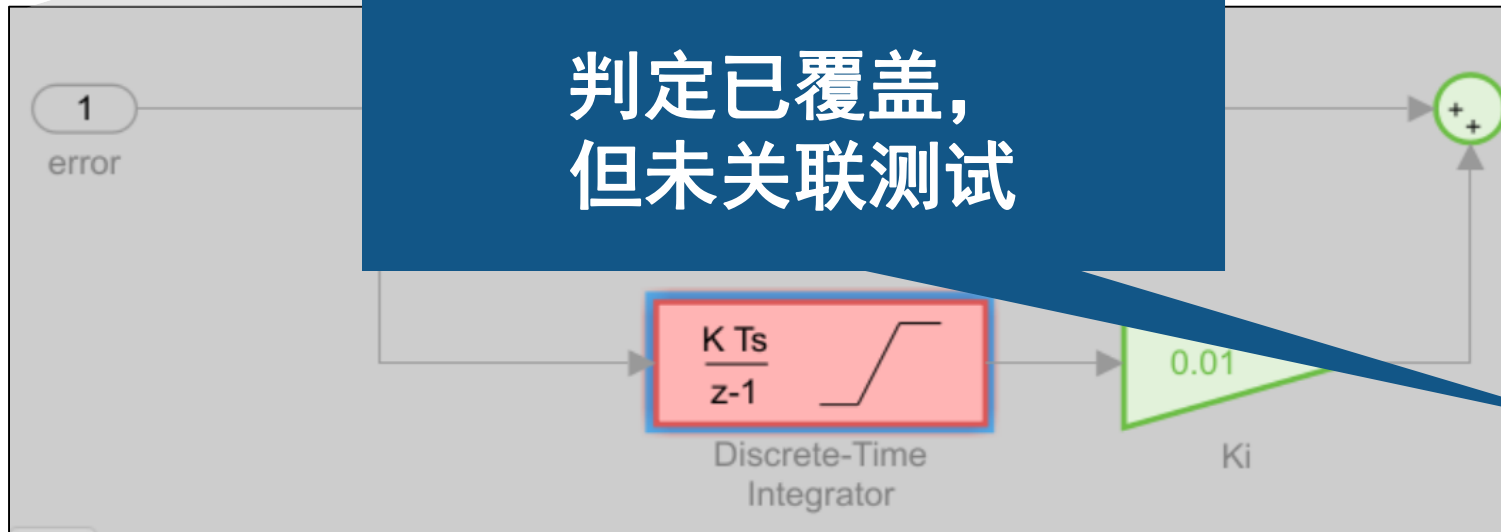
Uncovered Links:

Metric	Coverage
Cyclomatic Complexity	2
Decision	75% (3/4) decision outcomes
Execution	100% (1/1) objective outcomes

Decisions analyzed

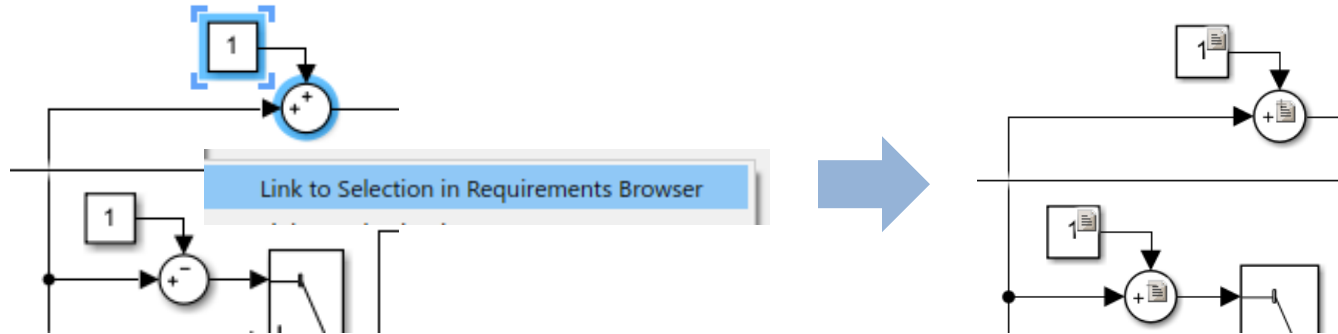
integration result <= lower limit	100%
false	391/801 T6
true	410/801 T6
integration result >= upper limit	50%
false	801/801 T6
true	0/801 T4

判定已覆盖，
但未关联测试



基于需求测试覆盖度不足的处理

- 添加模型和需求的关联



- 更新测试：提高目标速度

▼ INPUTS* ?

Include input data in test result

Stop simulation at last time point

EXTERNAL INPUTS

NAME	FILE	SHEET	STATUS
<input type="checkbox"/> td_throttle.mat	C:\Demos\examples\R2020a\sir		Mapped
<input checked="" type="checkbox"/> td_throttle_updated.mat	C:\Demos\examples\R2020a\sir		Mapped

100%覆盖度时，测试不通过

Results: 2020-Mar-02 23:59:38	5	1
cruiseControlRBTcovTests	5	1
Cruise Control Test Suite	5	1
Brake Test		
Decrement Test		
Enable Test		
Increment Test		
Set Speed Test		
Throttle Test		

AGGREGATED COVERAGE RESULTS

Create a coverage report from coverage results to justify or exclude missing coverage. The filters and updated coverage values will be displayed with this result.

ANALYZED MODEL	REPORT	COMPLEXI	DECISION	CONDITION	EXECUTION
<u>cruiseControlRBTcovExample</u>		8	100%	100%	100%

Scope coverage results to linked requirements

[+ Add Tests for Missing Coverage](#) [Export](#)

添加测试，发现错误

- Results: 2020-Mar-02
 - cruiseControlRB
 - Cruise Control
 - Brake Test
 - Decrement
 - Enable Test
 - Increment T
 - Set Speed 1
 - Throttle Test

✖ Throttle changes within limits

ASSESSMENT

- At any point of time, throttle_deriv must be greater than -1 and less than 1

SYMBOLS

- throttle_deriv

Error 1 of 1

Expected Behavior



Actual Result



Explanation

Assessment 'Throttle changes within limits' failed from 10.5 s to 12 s.

- Expected 'throttle_deriv' to be greater than '-1' and less than '1'.
- At 11.67 s, expected value to be greater than -1 and less than 1, actual value is **2.309499999999999**.

EXPRESSION TREE

- Throttle changes within limits: At any point of time, throttle_deriv must be greater than -1 and less than 1
- throttle_deriv must be greater than -1 and less than 1

PLOTS



the missing coverage. The filters and

DECISION	CONDITION	EXECUTION
100%	100%	100%

Id Tests for Missing Coverage Export

基于需求测试的模型覆盖度

R2020a

The screenshot shows the Test Manager interface. On the left, a tree view shows the test hierarchy: Results: 2019-Oct-02 19:02:58 (2 passed), dTestReqLinkBasic_Tests (2 passed), MyTestSuite (2 passed), Testcase 1 (1 passed), and Testcase 2 (1 passed). The main panel shows 'Results: 2019-Oct-02 19:02:58' with a 'SUMMARY' section and an 'AGGREGATED COVERAGE RESULTS' table. The table has columns for ANALYZED MODEL, REPORT, COMPLEXI..., DECISION, and EXECUTION. The row for 'mTestReqLinkBasic' shows 5 complexity, 33% decision coverage, and 25% execution coverage. A checkbox labeled 'Scope coverage results to linked requirements' is checked and highlighted with a red box. Below the table are buttons for '+ Add Tests for Missing Coverage' and 'Export'.

DO-178C 6.4.4.2 ... coverage information collected during requirements-based testing to confirm that ...

MultiPortSwitch block "MPSwitch1"

Requirement Testing Details

Implemented Requirements	Verified by Tests	Associated Runs
Requirement 1	Testcase 1	T1

Metric Coverage

Cyclomatic Complexity 2

Decision 33% (1/3) decision outcomes

Execution 100% (1/1) objective outcomes

Decisions analyzed

truncated input value	33%
= 1 (output is from input port 1)	51/51 T1
= 2 (output is from input port 2)	0/51 T2
= *,3 (output is from input port 3)	0/51

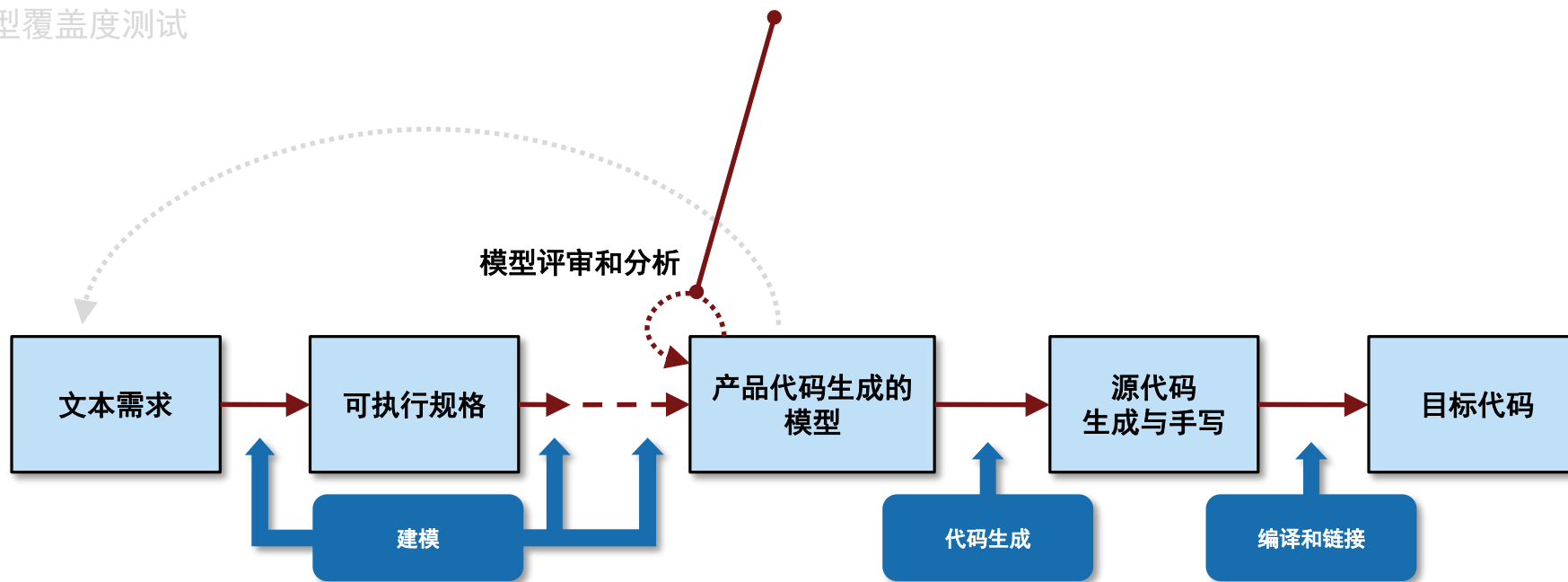
Hit by linked RBT -- Satisfied

Hit, but not by linked RBT -- Unsatisfied

标准服从性检查

模型验证

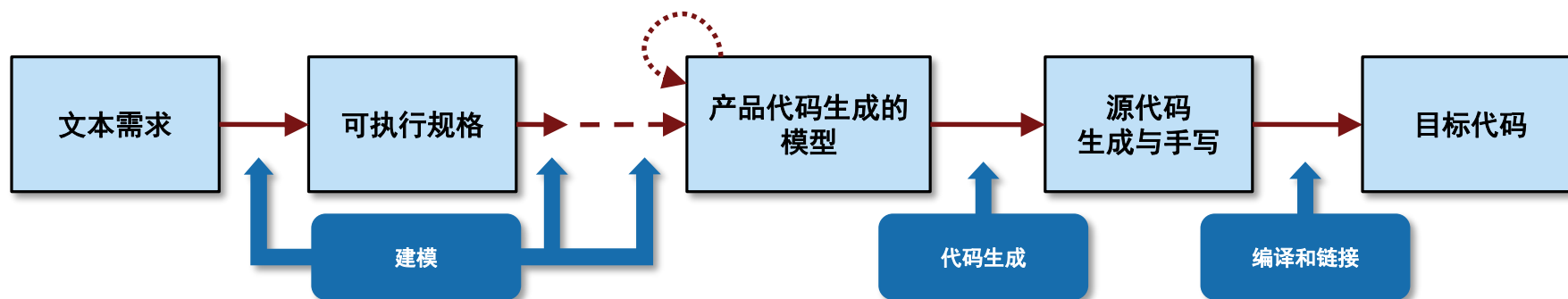
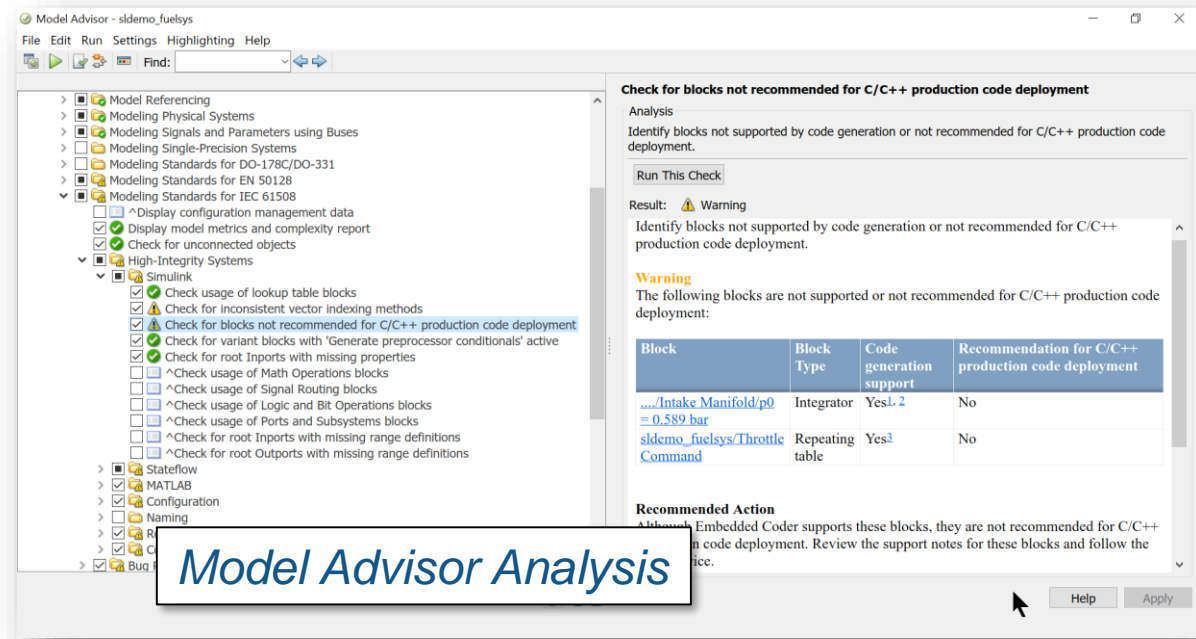
- 需求管理
- 基于需求的测试
- 测量模型覆盖率
- 模型覆盖度测试
- **标准服从性检查**
- 设计缺陷检查
- 模型行为证明



检查设计对设计规范和行业标准的符合性

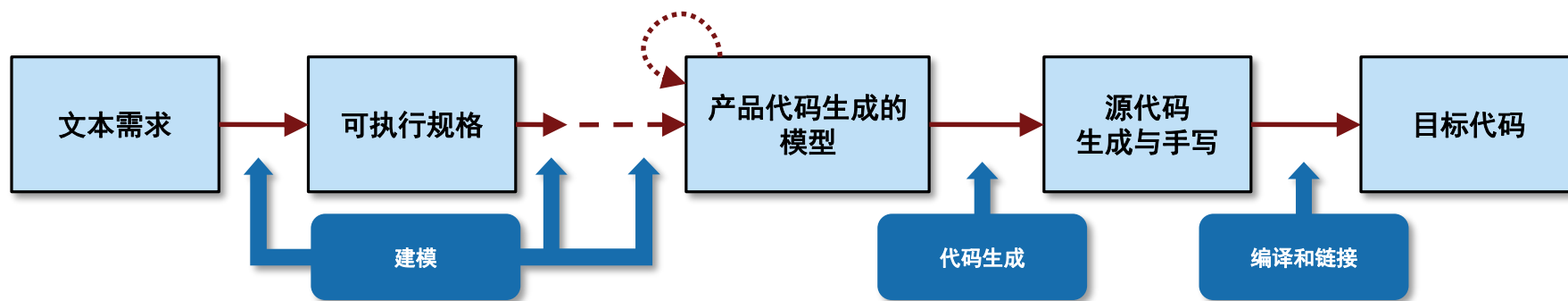
检查:

- 可读性与语义
- 性能和效率
- 复制的模块等



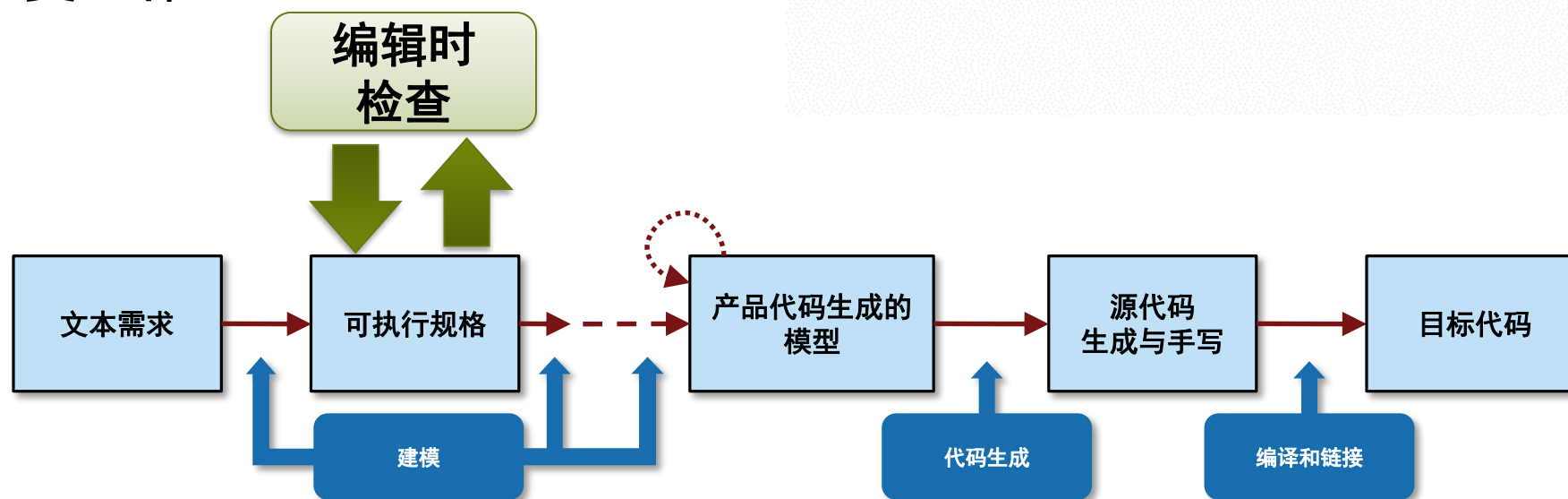
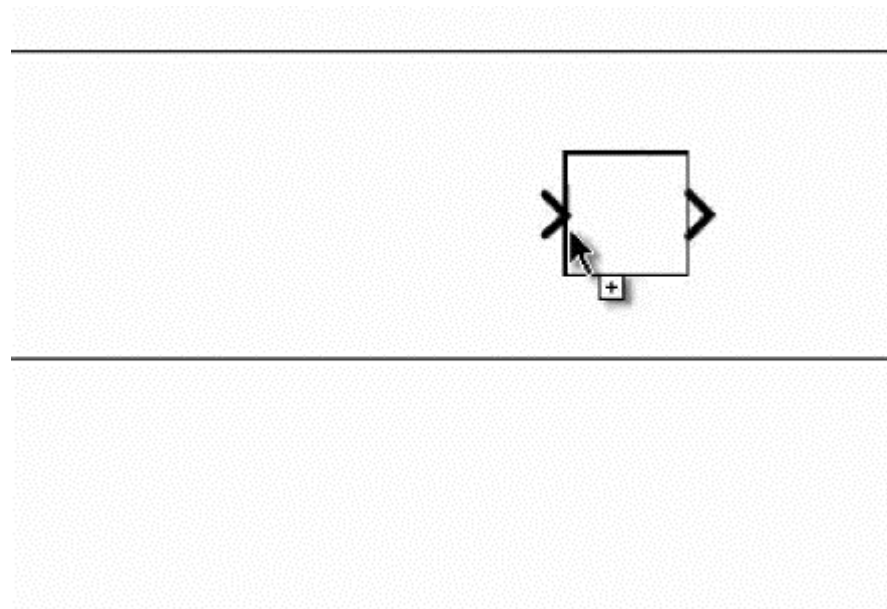
内置工业标准和规范的检查

- DO-178/DO-331
- MISRA C:2012
- ISO 26262
- CERT C, CWE, ISO/IEC TS 17961
- IEC 61508
- MAB (MathWorks Advisory Board)
- IEC 62304
- JMAAB (Japan MATLAB Automotive Advisory Board)
- EN 50128



使用编辑时检查提早进行验证

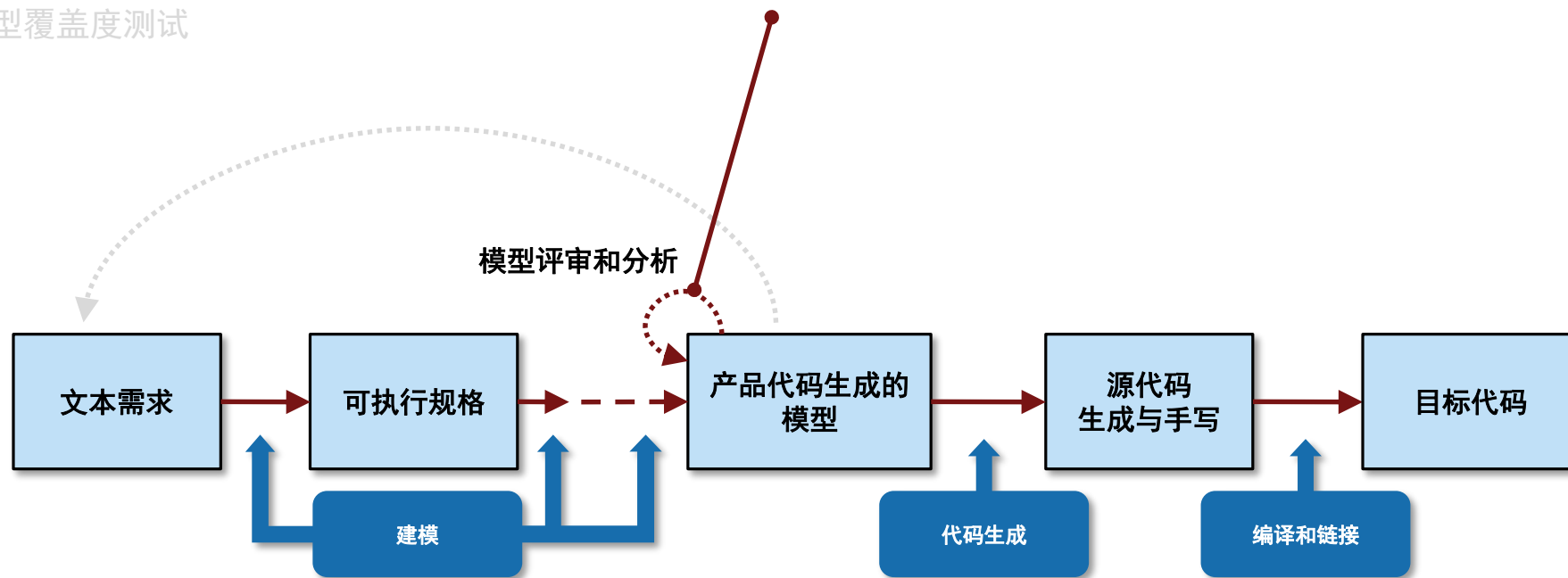
- 编辑时高亮规则违反
- 早期修复问题
- 避免重复工作



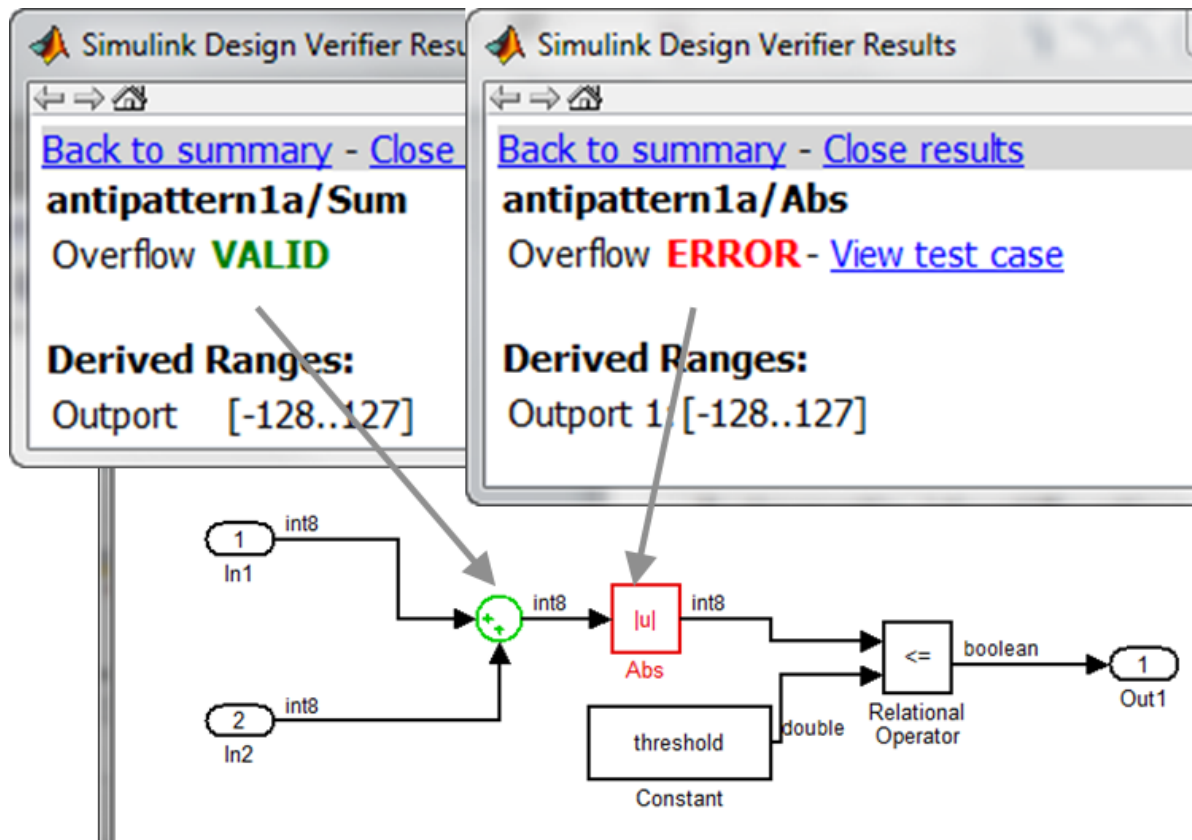
使用形式化方法检查设计错误

模型验证

- 需求管理
- 基于需求的测试
- 测量模型覆盖率
- 模型覆盖度测试
- 标准服从性检查
- **设计缺陷检查**
- 模型行为证明



使用形式化方法检查设计错误



■ 检查设计缺陷

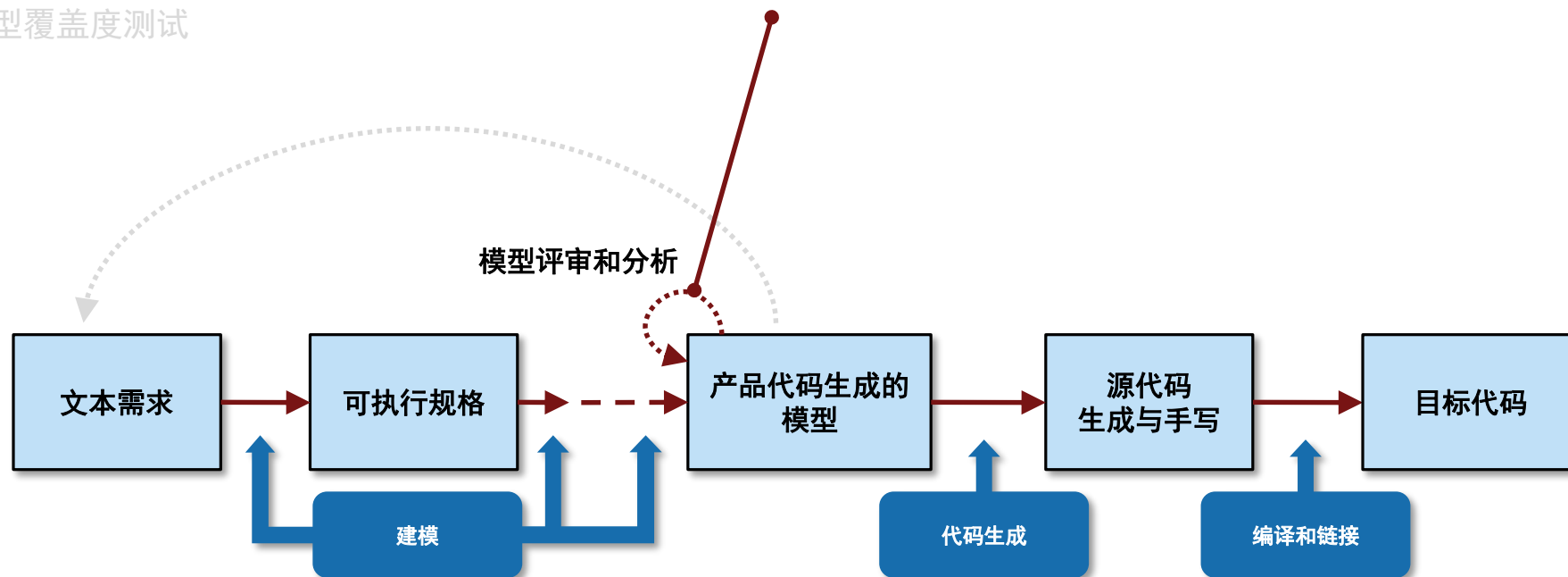
- 整形溢出
- 死逻辑
- 除零
- 数组越界

■ 生成反例复现错误

证明模型行为满足需求

模型验证

- 需求管理
- 基于需求的测试
- 测量模型覆盖率
- 模型覆盖度测试
- 标准服从性检查
- 设计缺陷检查
- **模型行为证明**

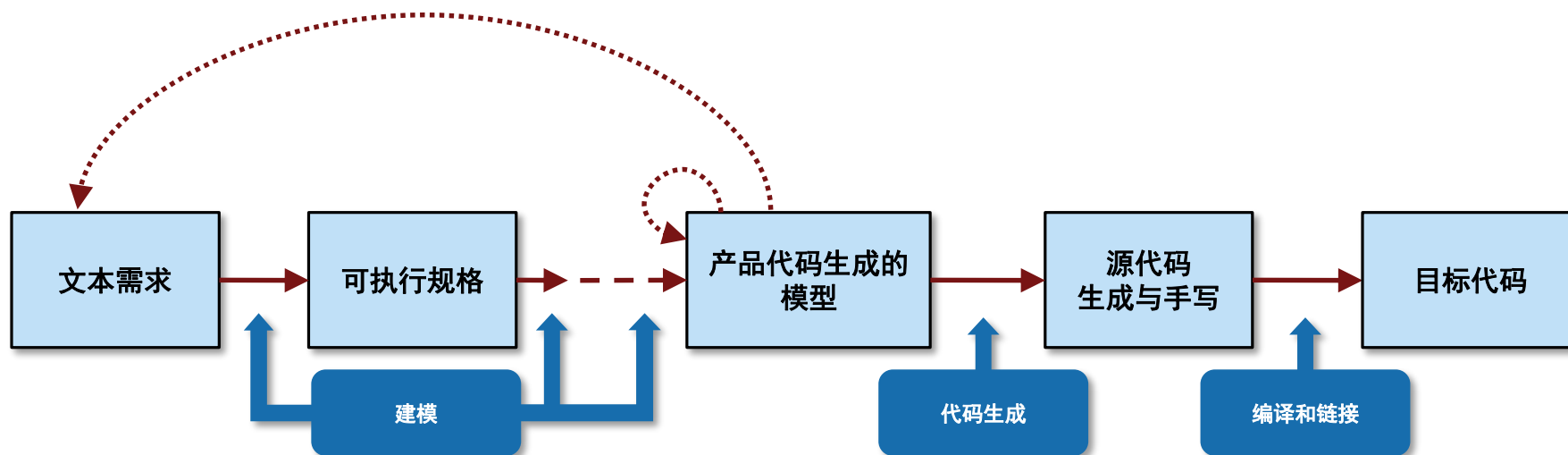


证明模型行为满足需求

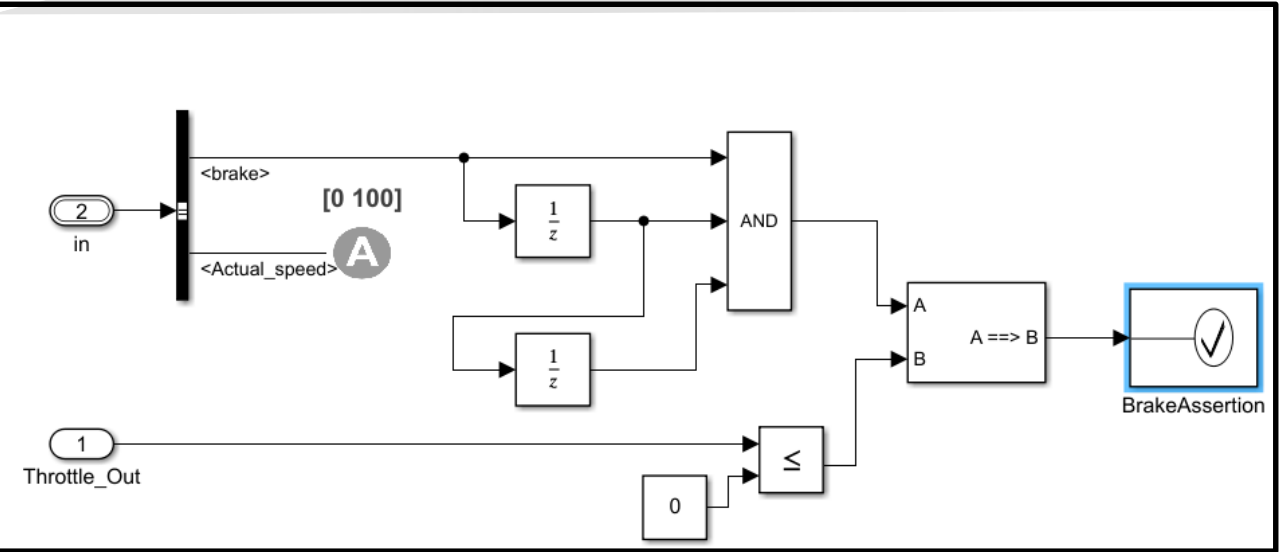
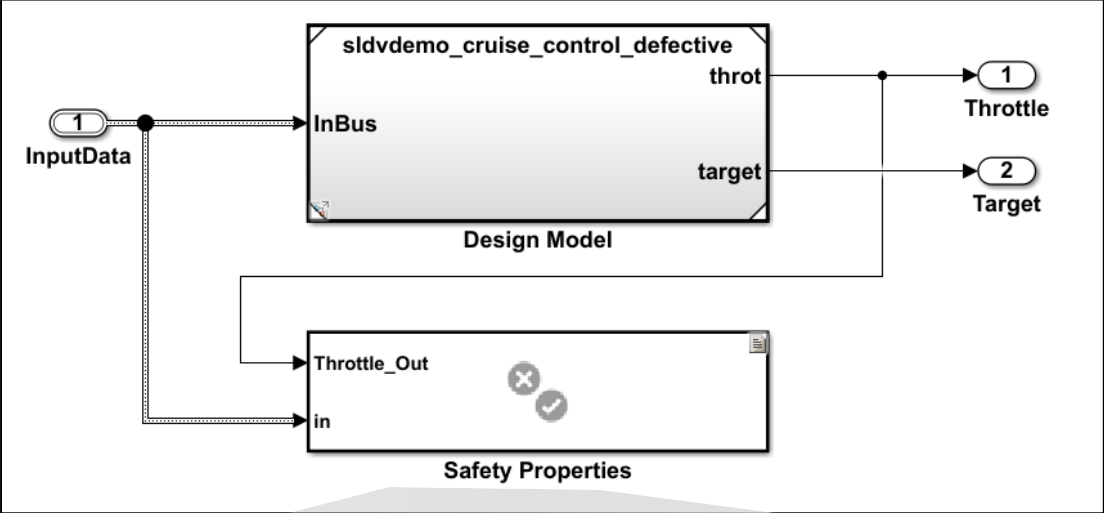
功能安全需求:

当刹车持续作用3个迭代周期，油门应归零。

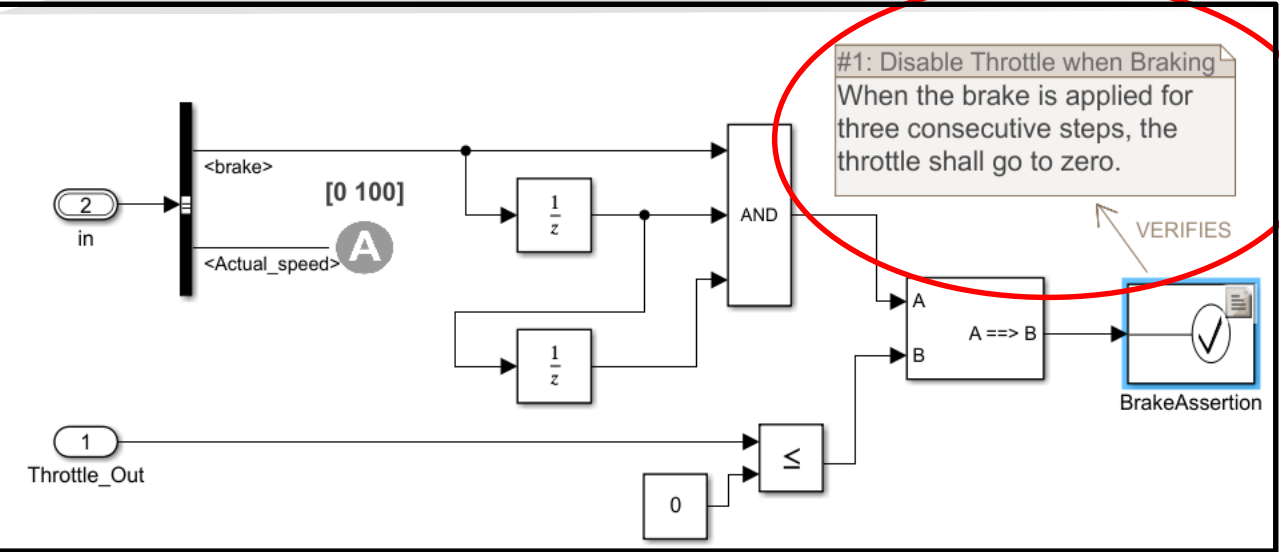
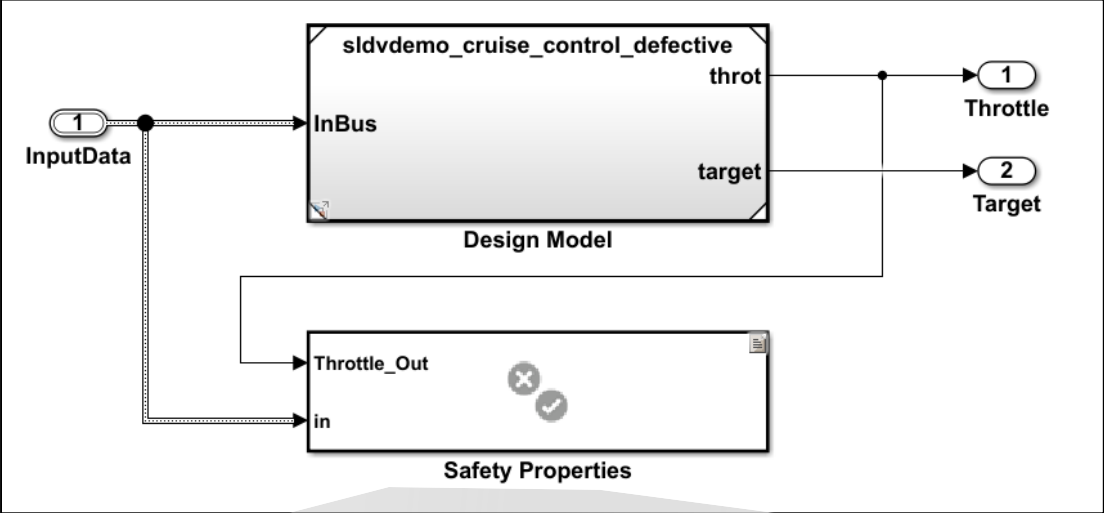
- 需要证明：设计完全满足功能需求



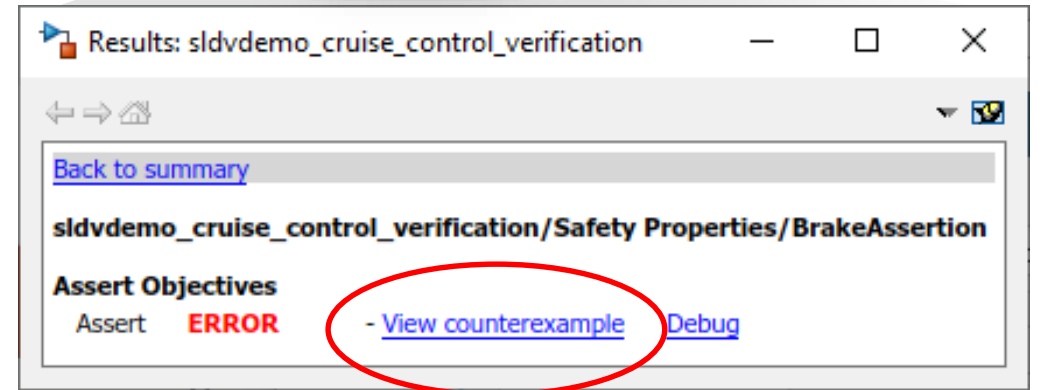
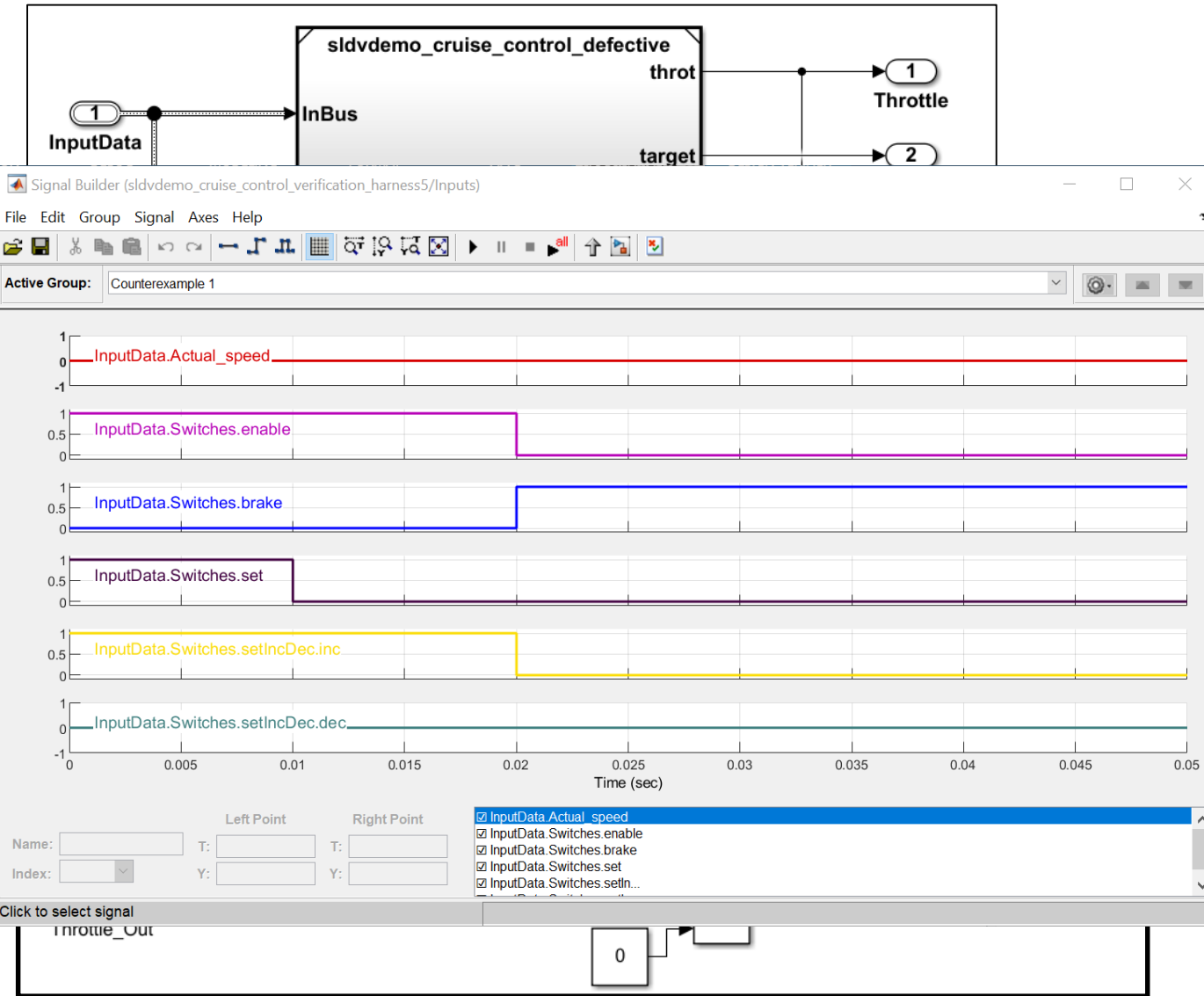
功能需求和安全需求建模



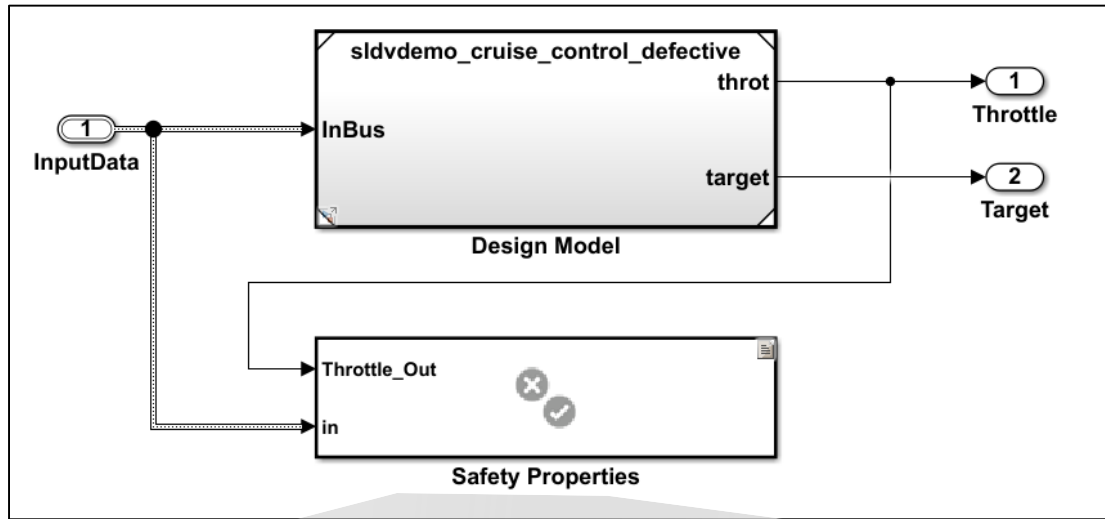
将需求与属性建立关联



证明设计满足需求



Model Slicer 用于属性证明反例的调试



Results: sldvdemo_cruise_control_verification

Model Slicer

► Slice configuration list

Name: :ontrol_verification/Safety Properties/BrakeAssertion : Assert

Description:
This slice configuration is autogenerated for debugging the falsified property 'sldvdemo_cruise_control_verification/Safety Properties/BrakeAssertion : Assert'.

Signal propagation: upstream

Starting Points [clear all]

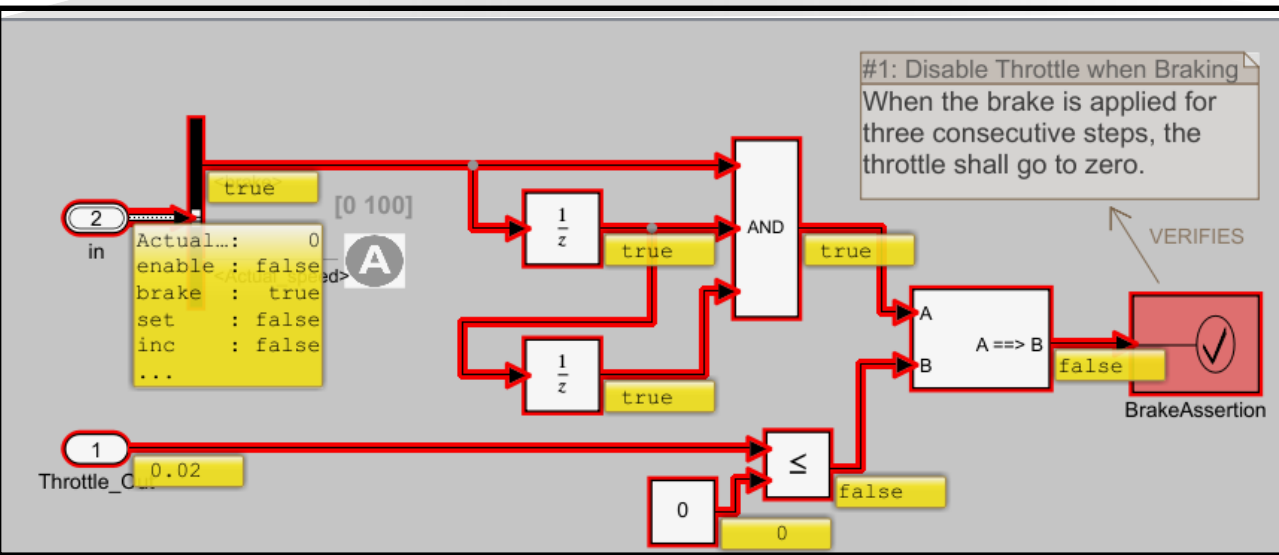
BrakeAssertion

Simulation time window (Enabled)

Safety Properties/BrakeAssertion

Debug

Debug Using Slicer



模型分割中的常见问题处理

分割

找到与非预期行为相关的模型

分析依赖性

理解大型、复杂模型中，数据流和控制流的依赖关系

审查分离的模型

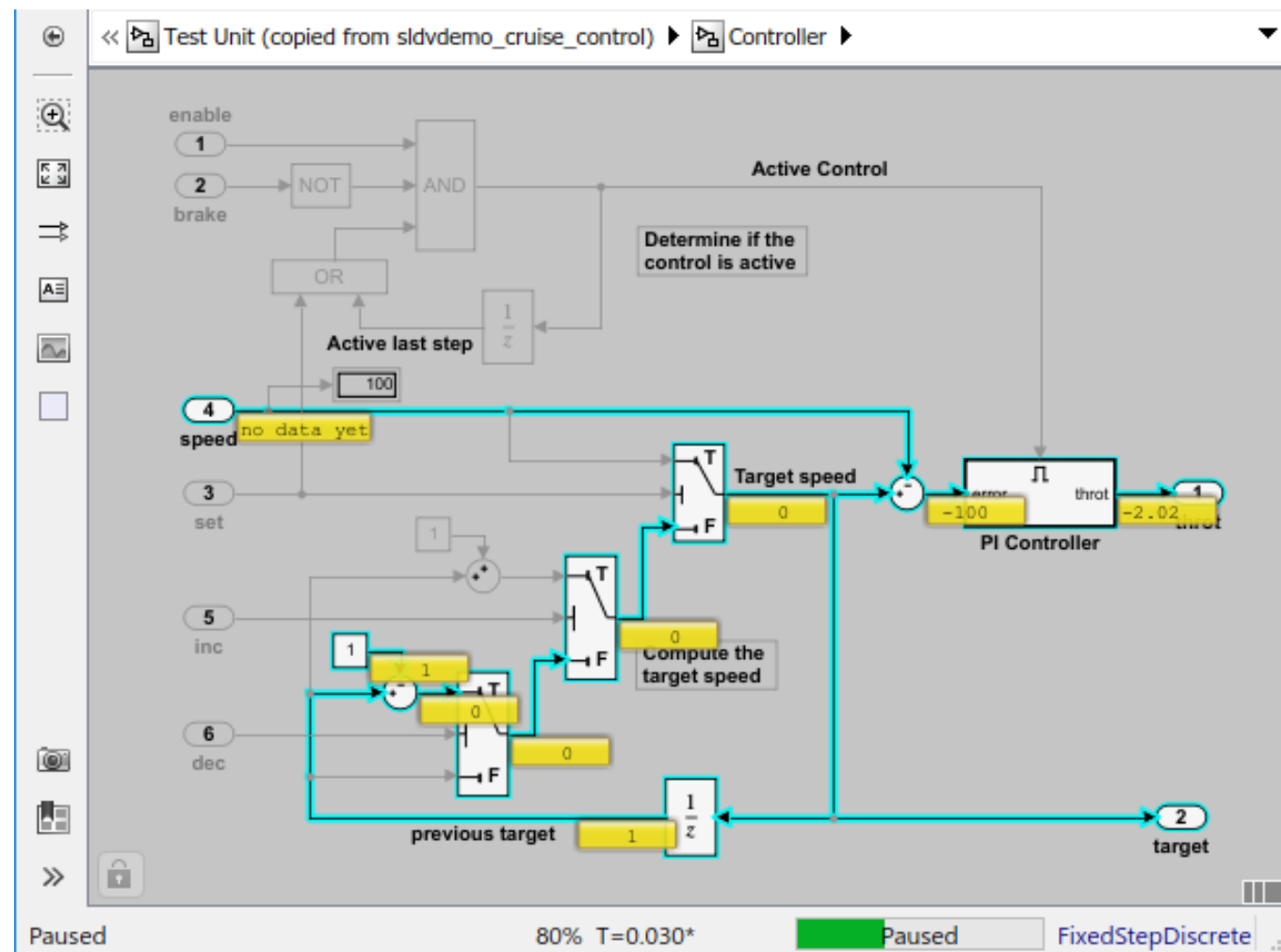
高亮分割的模型时间窗口、不通过状态、stateflow的转换

仿真行为调试

对分离的模型单步调试，理解信号、端口值及其传递关系

修改后的模型

迭代

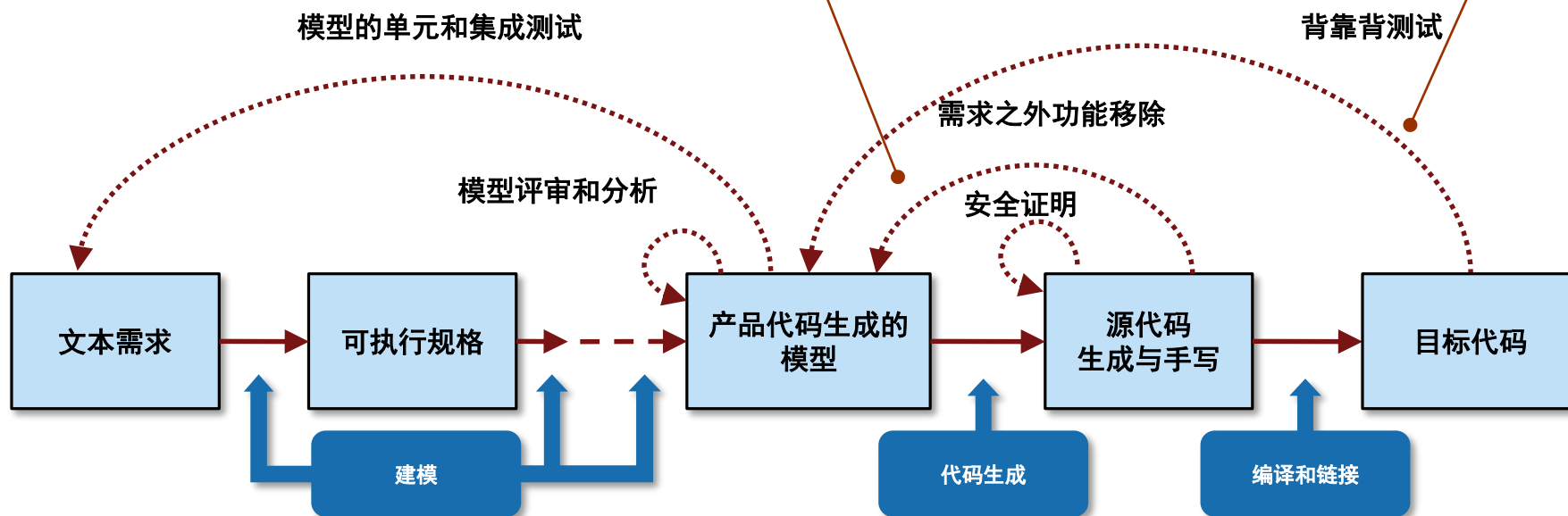


代码验证: 在代码层面提高可靠度

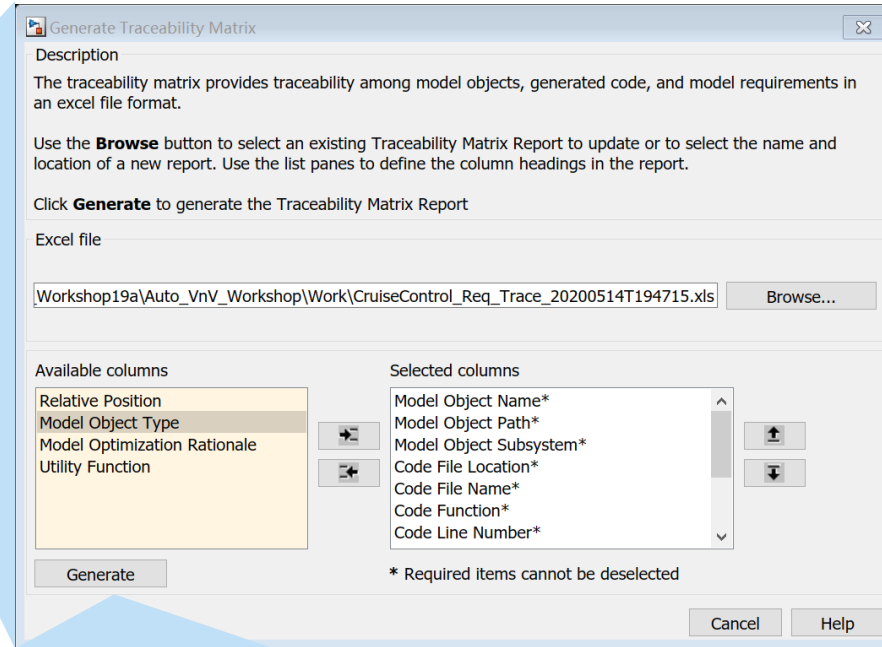
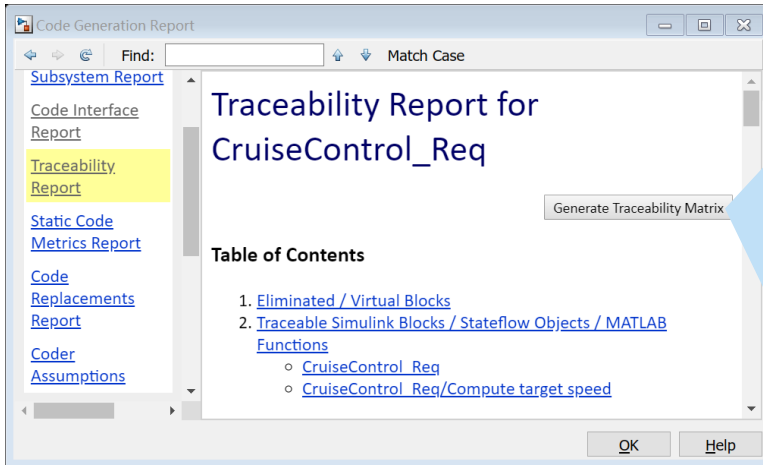
代码验证

- 代码与模型和需求追述
- 代码覆盖度测试
- SIL/PIL 一致性测试

- 生成测试向量, 达到代码100%覆盖
- 代码缺陷检查
- 无运行时错误证明

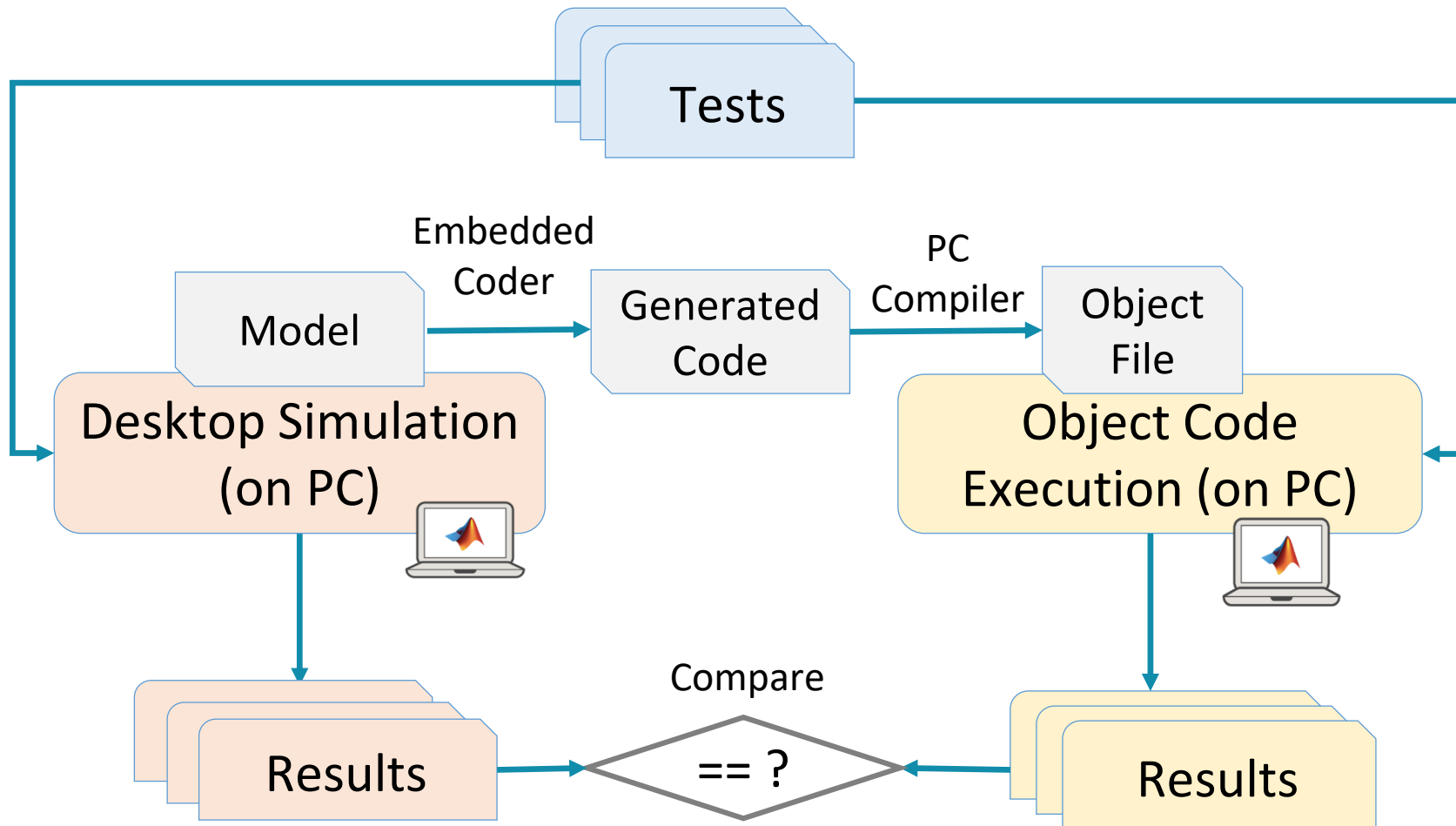


生成追溯性矩阵



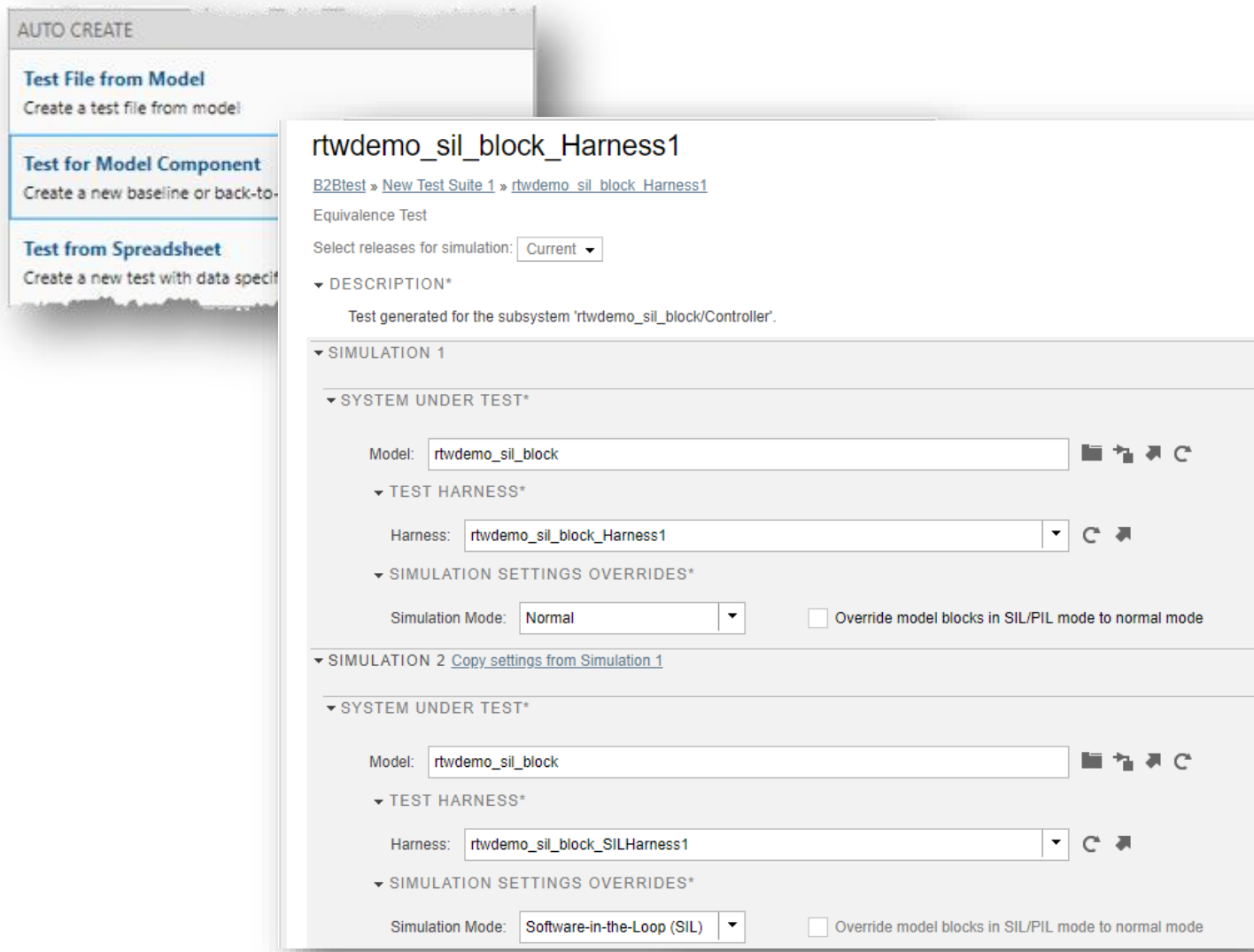
A	B	C	E	F	G	H	K	L
Model Object Name	Model Object Path	Model Object Subsystem	Code File Name	Code Function	e Line Num	Model Object Unique ID	Requirements Source	Requirements Location
CruiseOnOff	CruiseControl_Req	CruiseControl_Req	CruiseControl_Req.c	Global	42	CruiseControl_Req:26	MW_CruiseControl.slreqx	Enable/Disable Switch (MW_CruiseControl#2):2
CruiseOnOff	CruiseControl_Req	CruiseControl_Req	CruiseControl_Req.c	CruiseControl_Req_step	63	CruiseControl_Req:26	MW_CruiseControl.slreqx	Enable/Disable Switch (MW_CruiseControl#2):2
CruiseOnOff	CruiseControl_Req	CruiseControl_Req	CruiseControl_Req.c	CruiseControl_Req_step	76	CruiseControl_Req:26	MW_CruiseControl.slreqx	Enable/Disable Switch (MW_CruiseControl#2):2
CruiseOnOff	CruiseControl_Req	CruiseControl_Req	CruiseControl_Req.c	CruiseControl_Req_step	105	CruiseControl_Req:26	MW_CruiseControl.slreqx	Enable/Disable Switch (MW_CruiseControl#2):2
CruiseOnOff	CruiseControl_Req	CruiseControl_Req	CruiseControl_Req.c	CruiseControl_Req_step	284	CruiseControl_Req:26	MW_CruiseControl.slreqx	Enable/Disable Switch (MW_CruiseControl#2):2
CruiseOnOff	CruiseControl_Req	CruiseControl_Req	CruiseControl_Req.h	Global	69	CruiseControl_Req:26	MW_CruiseControl.slreqx	Enable/Disable Switch (MW_CruiseControl#2):2

背靠背测试代码和模型行为一致性



- 使用 Simulink Test 自动化测试
- 跨软件版本测试

使用 Test Manager 为向导自动生成测试用例

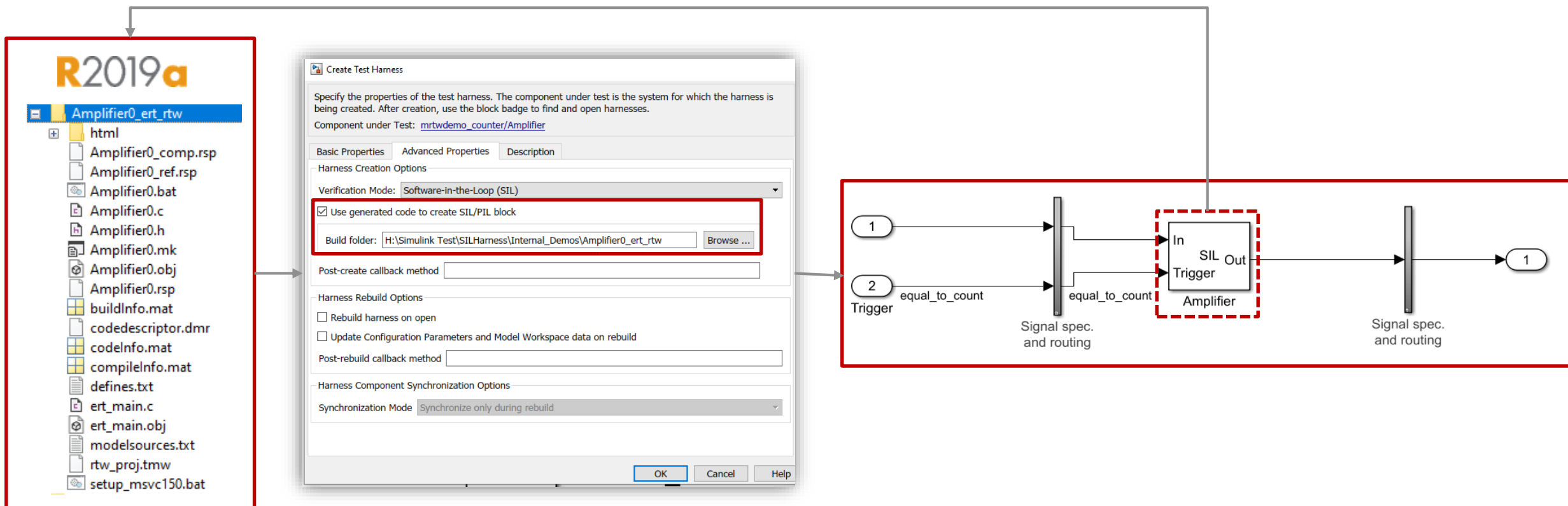


- 向导式步骤定义输入、测试类型和输出格式
- 向导式生成需要的测试框架
- 使用 Simulink Design Verifier 自动生成测试用例

支持跨版本的SIL/PIL 测试框架生成

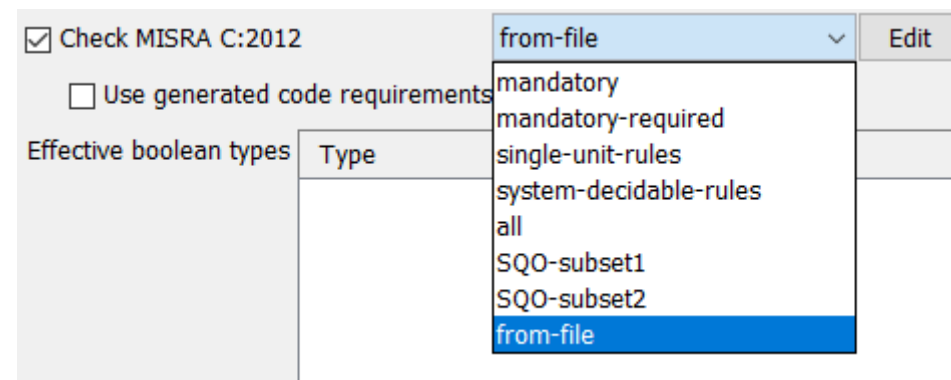
R2020a

- 使用之前版本生成的代码用于创建 SIL/PIL 测试框架
- 修改现有 SIL/PIL 测试框架，保存需编译文件夹信息用于再编译



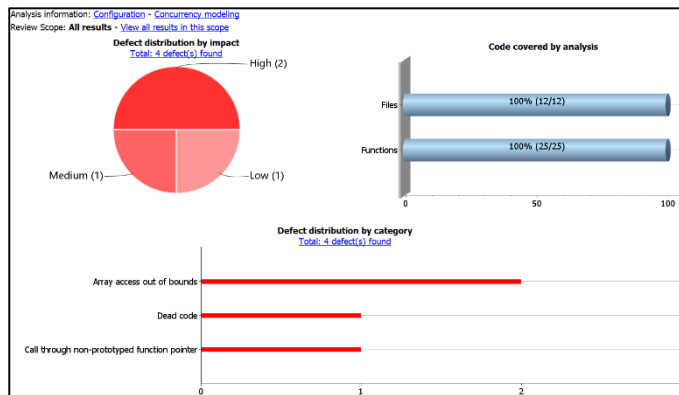
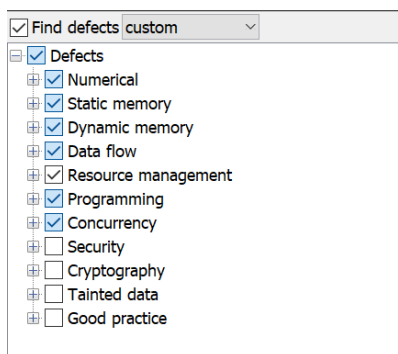
手写代码的编码规范检查

- 支持带代码规范包括
 - MISRA C 2004/2012/AGC
 - MISRA C++ 2008
 - CWE
 - CERT-C
- 内置常见规范集合
- 支持自定义检查范围
- 使用Code Prover进行违规说明



集成测试的代码缺陷检查

Bug Finder Analysis



- 12大类，近300多种缺陷检查
- 不同风险等级的缺陷划分
- 具体的定位和详细的问题原因
- 修复的建议

Array access out of bounds (Impact: High)
Attempt to access to array element 10.
Valid index range: [0 .. 9].

Event	File	Scope
1	analog_io.c	acquire_ai_hw_data() 25

Fix

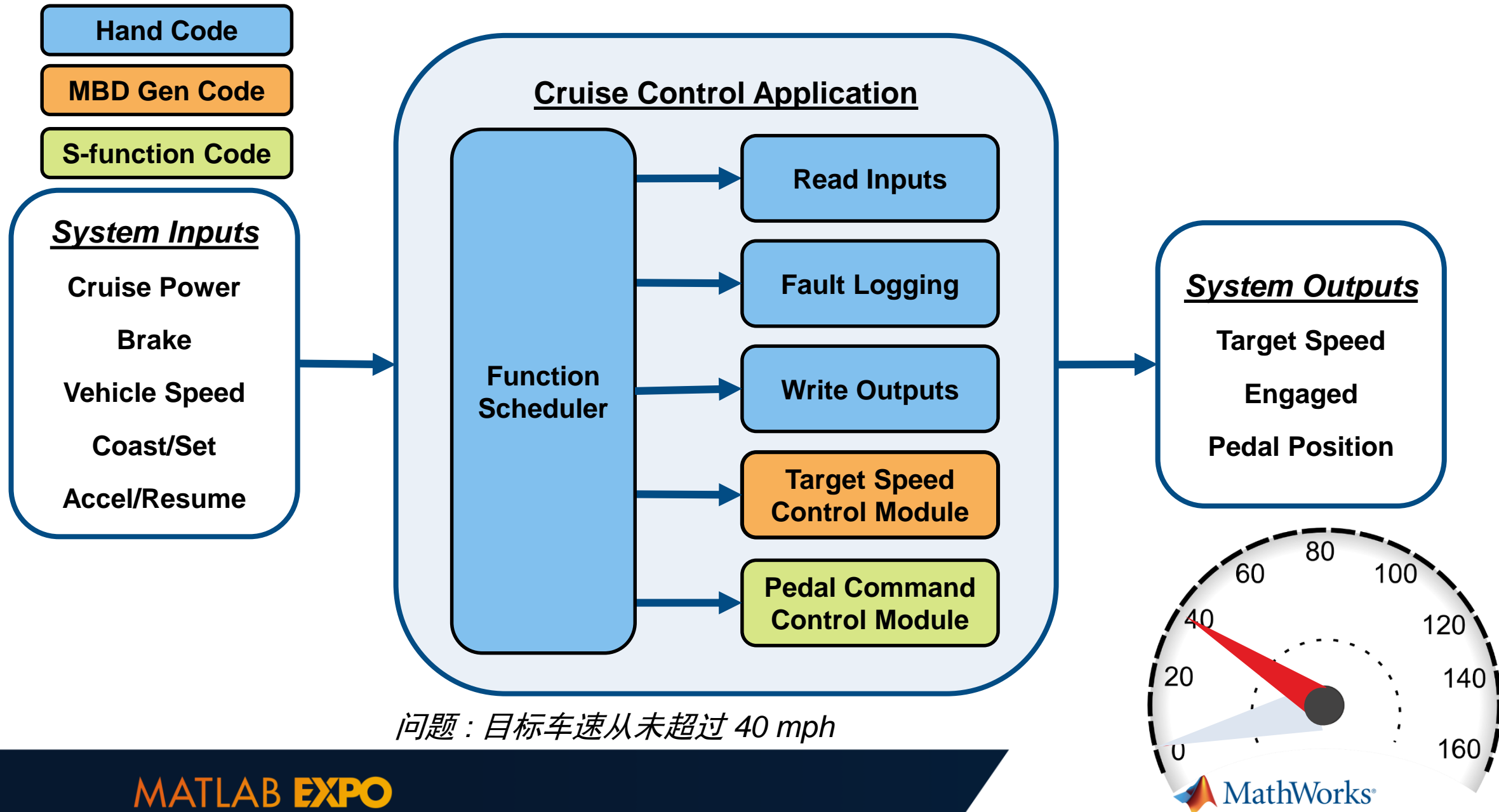
The fix depends on the root cause of the defect. For instance, situations happened:

- The upper bound of the loop is too large.
- You used an array index that is the same as the loop index.

To fix the issue, you have to modify the loop bound or the array.

```
24 {  
25     uint32_t loop_index;  
26  
27     for (loop_index = 0u; loop_index <= MAX_AI_RAW_COUNTS_BUFFER_SIZE; loop_index++)  
28     {  
29         AI_Raw_Counts[loop_index] = HW_A2D_Data_Addr;  
30     }  
31  
32 }
```

应用级分析和证明



集成代码分析

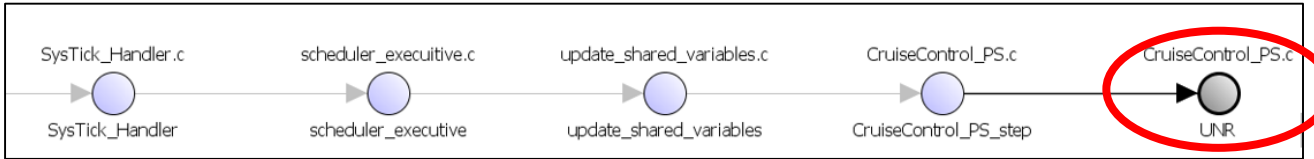
```

104
105  /* Entry 'STANDBY': '<S1>:52
106  engaged = false;
107  } else if (Speed > maxtspeed)
108  /* Transition:
109  /* Exit Intern
110  CruiseControl_
111  CruiseControl_
112
113  /* Entry 'STAN
114  engaged = fals
115  } else if (Speed < mintspeed) {
    
```

Global variable 'maxtspeed' (unsigned int 8): 90
 Conversion from unsigned int 8 to unsigned int 32
 right: 90
 result: 90

Global variable 'Speed' (unsigned int 8): [0 .. 40]
 Conversion from unsigned int 8 to unsigned int 32
 right: [0 .. 40]
 result: [0 .. 40]

Variables	Values	# Reads	# Writes	Written by t...	Read by task
CS_UI					
AI_Raw_Counts	full-range [-128 .. 127]	1	2	ps_main	ps_main
AI_Speed		6	5	ps_main	ps_main
AccelResSw	full-range [0 .. 255]	3	3	ps_main	ps_main
Brake	full-range [0 .. 255]	2	3	ps_main	ps_main
CoastSetSw	full-range [0 .. 255]	3	3	ps_main	ps_main
CruiseOnOff	[0 .. 1]	2	3	ps_main	ps_main
M		3	1		
M_		0	2		
PedalCmdY	0.0 or 0.5 or 1.0 or 1.5...	5	1		ps_main
PedalPos	[-35.5 .. -2.9802E-08] or	0	4	ps_main	
PedalPosRaw	0.0	1	2		ps_main
Speed	[0 .. 40]	7	3	ps_main	ps_main
_init_globals()	0				
CruiseControl_Integ_PS_initialize()	0				
update_shared_variables()	[0 .. 40]				
CruiseControl_PS()	[0 .. 40]				
CruiseControl_PS()	[0 .. 40]				
CruiseControl_PS()	[20 .. 40]				
CruiseControl_PS()	[0 .. 40]				



- 调用关系图
- 全局变量访问树、范围给定

问题原因

模拟量到数字量转换因子没有随不同ECU宽度变化，导致死代码。

```
analog.h
19 /* Conversion factors of speed */
20 #define NEW_ECU
21 #ifndef NEW_ECU
22     #define SPEED_MASK 0xFFF /* New ECU */
23 #else
24     #define SPEED_MASK 0x3FFF /* Original design specification */
25 #endif
26
27 /* Scaling for conversion factor for translating sensor input to miles/hr */
28 #define CONV_FACTOR 0.01 /* FAILS */
29
30 #define MAX_AI_RAW_COUNTS_BUFFER_SIZE 10
31
32     Average = (AI_Speed.SensorRawCounts / CONV_FACTOR);
33
34     /* Convert raw counts to speed */
35     AI_Speed.Speed = ((AI_Speed.Average & SPEED_MASK) * CONV_FACTOR);
36
37     /* Updated analog inputs */
38     MDB_Shared_Data.Speed = AI_Speed.Speed;
39 }
```

MASK – accounts for scaling down for new ADC from 14-bit to 12-bit

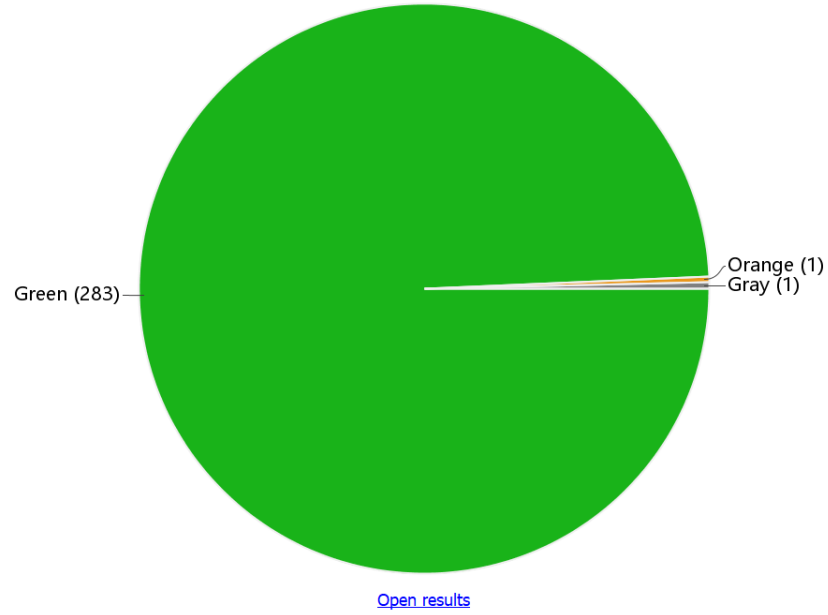
代码更改:

新的 ADC 时的 CONV_FACTOR 值

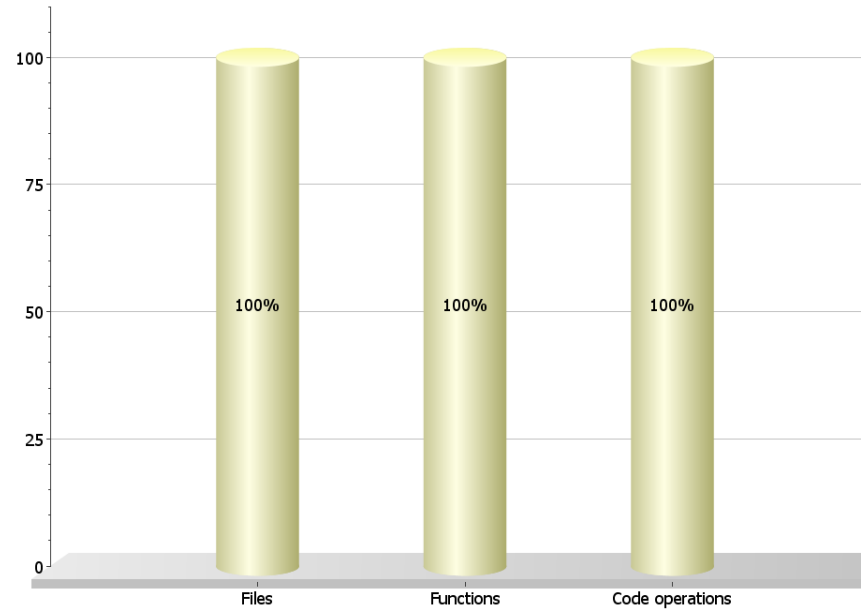
无运行时错误证明

Analysis information: [Configuration](#) - [Analysis assumptions](#)

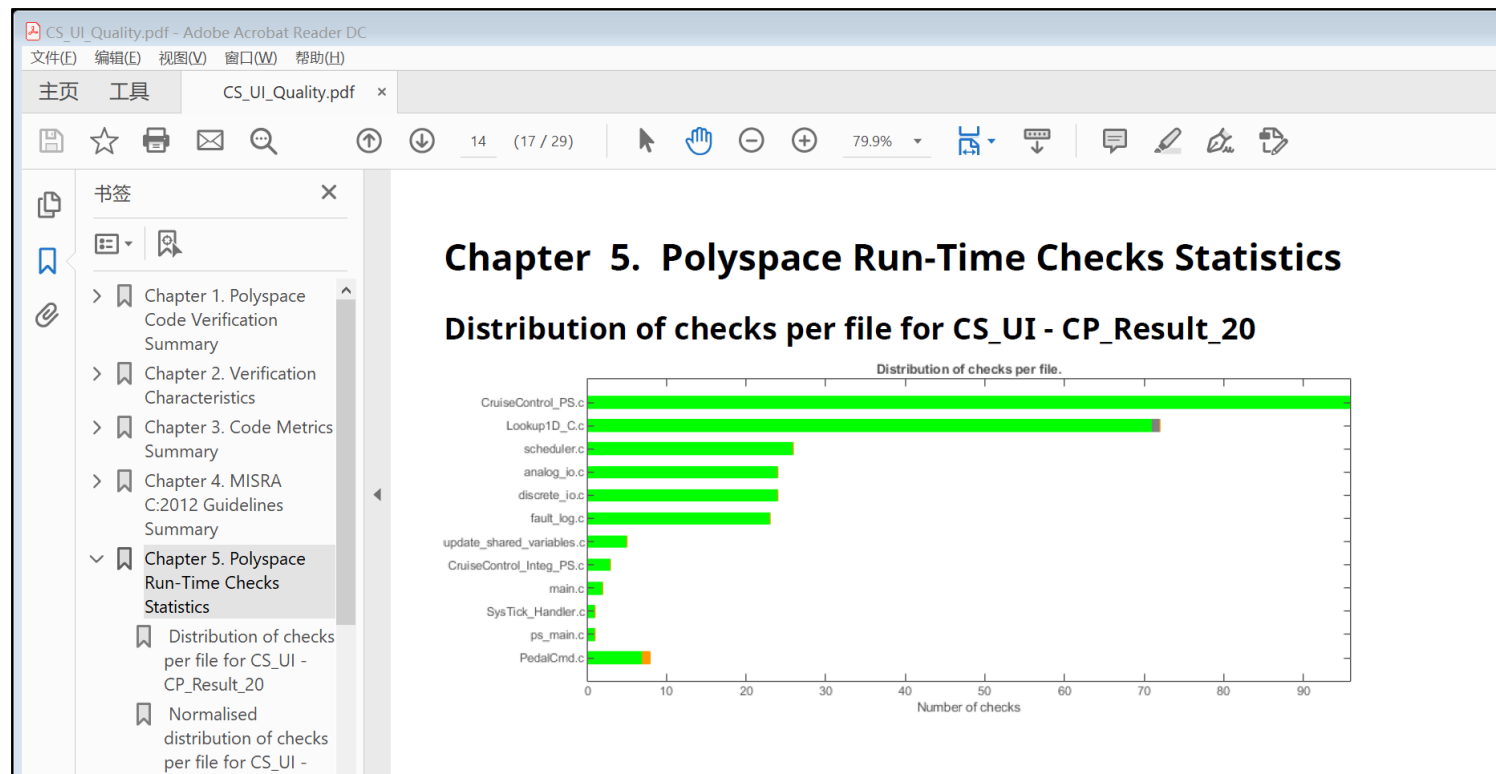
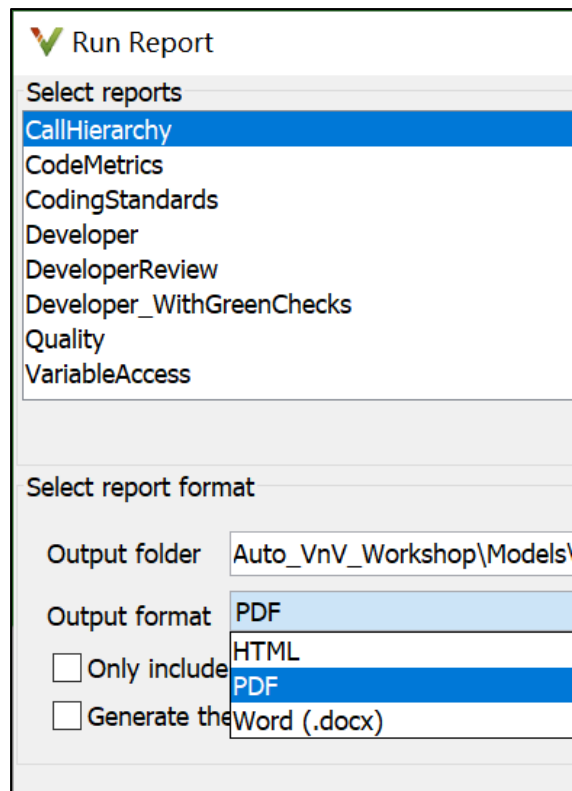
Check distribution
Proven: 99%



Code covered by verification ②



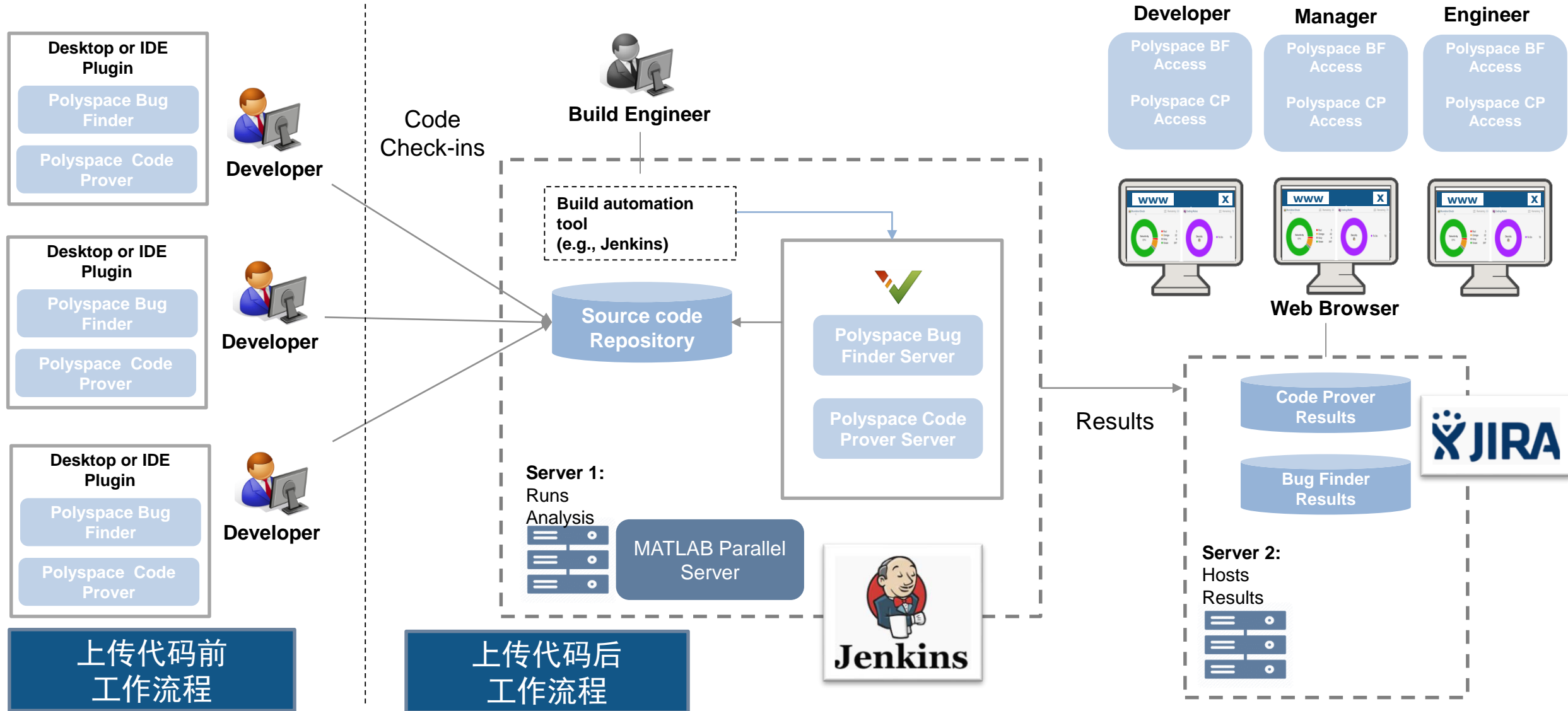
生成取证证物



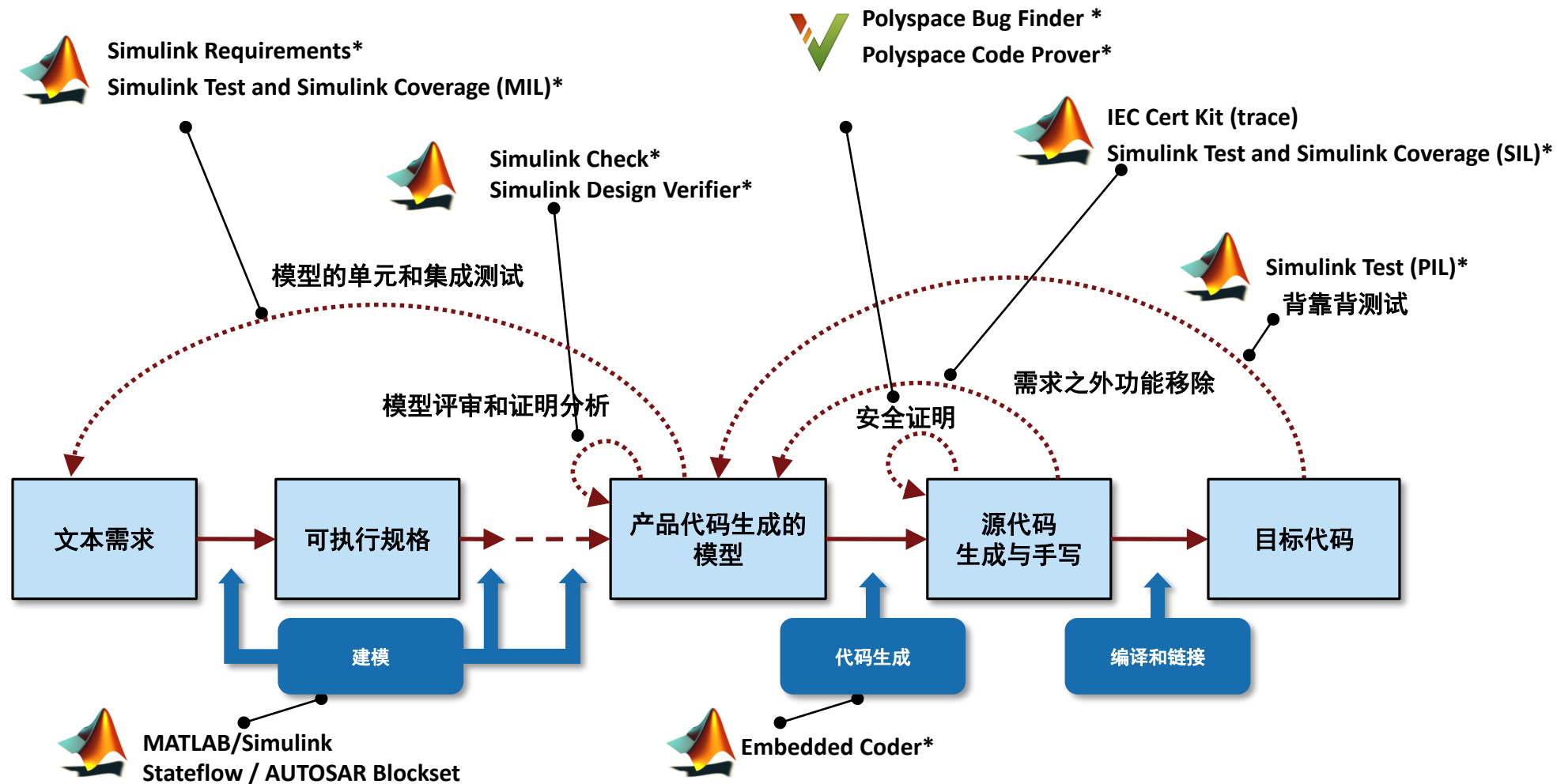
不同类型和格式报告

质量报告

整个团队协作使用 Polyspace



参考流程



*Qualifiable

我们的用户正在使用



空中客车直升机运用基于模型设计加速了DO-178B认证软件的开发
软件测试时间减少三分之二



LS Automotive通过基于模型的设计减少了汽车组件软件的开发时间
在早期发现了需求规格错误

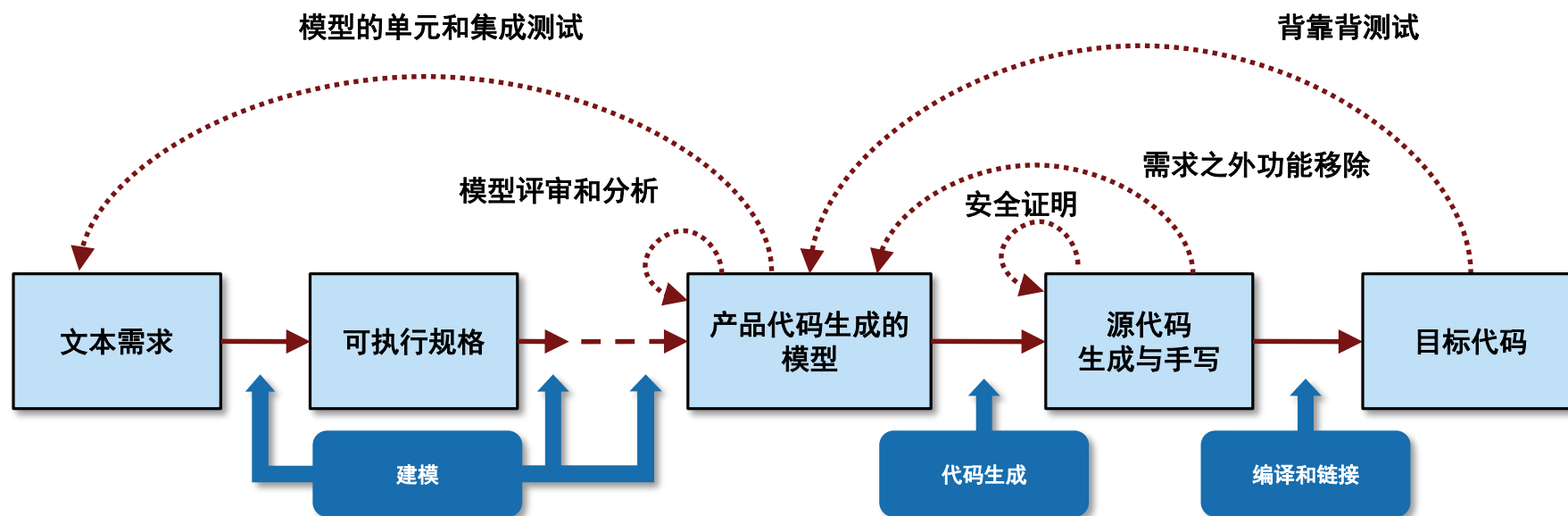


日产公司使用 Polyspace 提高软件的可靠性
发现了供应商代码中难以发现的运行时错误

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

使用参考流程加速标准认证

- 尽早开始验证流程
- 自动化验证任务（背靠背测试、批处理、持续集成）
- 基于需求的测试完成度量



更多关于验证内容

- [基于模型的测试和验证解决方案主页](#)
- [基于需求的测试验证流程示例](#)
- [对高集成度系统进行模型和代码的验证](#)
- [模型的测试和验证入门](#)
- [Polyspace 让关键代码安全无虞](#)

谢谢大家!