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

MathWorks®

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

ISO 26262-6:2018
Simulink 和 Stateflow 适用于软件架构、设计和代码生成

Table 5 — Notations for software unit design

	Notations	ASIL A	ASIL B	ASIL C	ASIL 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®.

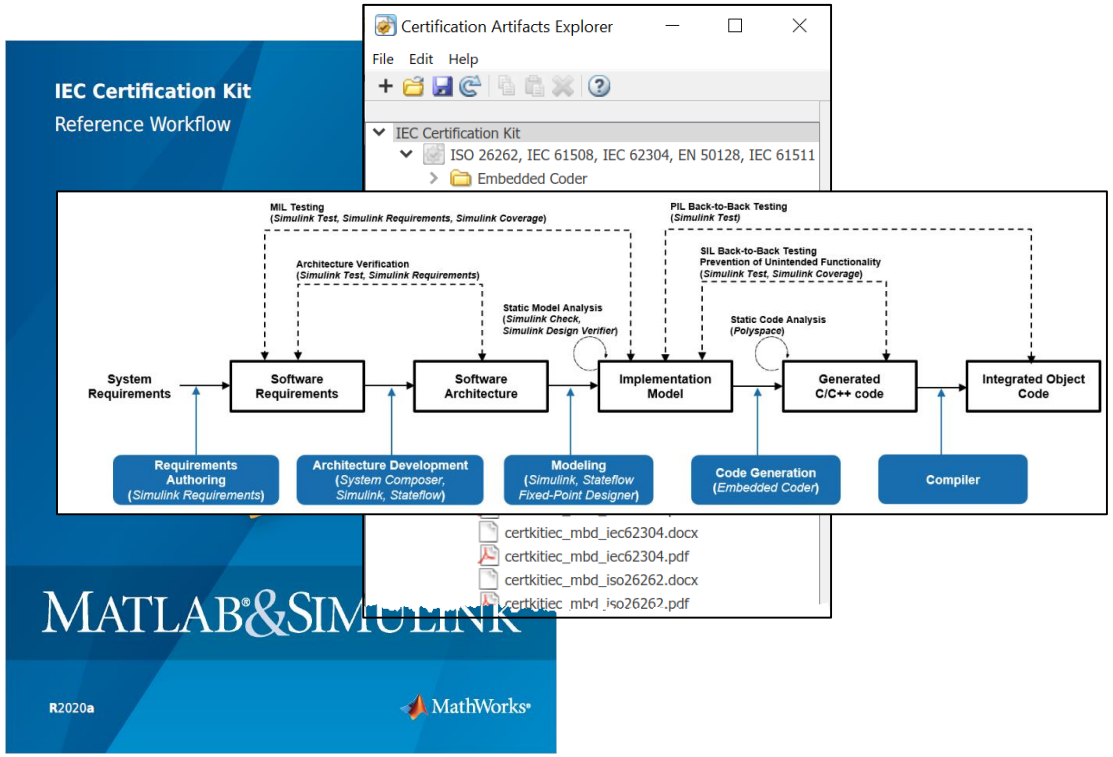
NOTE UML®, SysML®, Simulink® and Stateflow® are examples of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of these products.

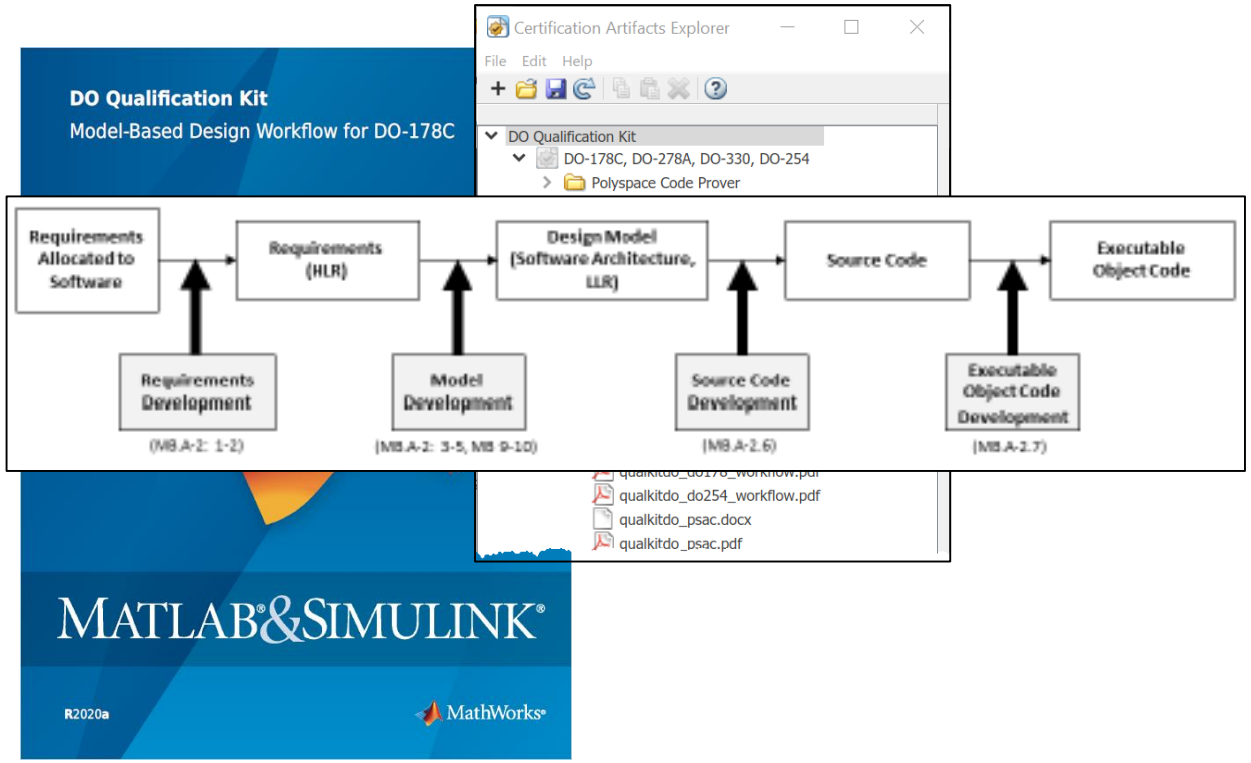
NOTE In the case of model-based development with automatic code generation, the methods for representing the software unit design are applied to the model which serves as the basis for the code generation.

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

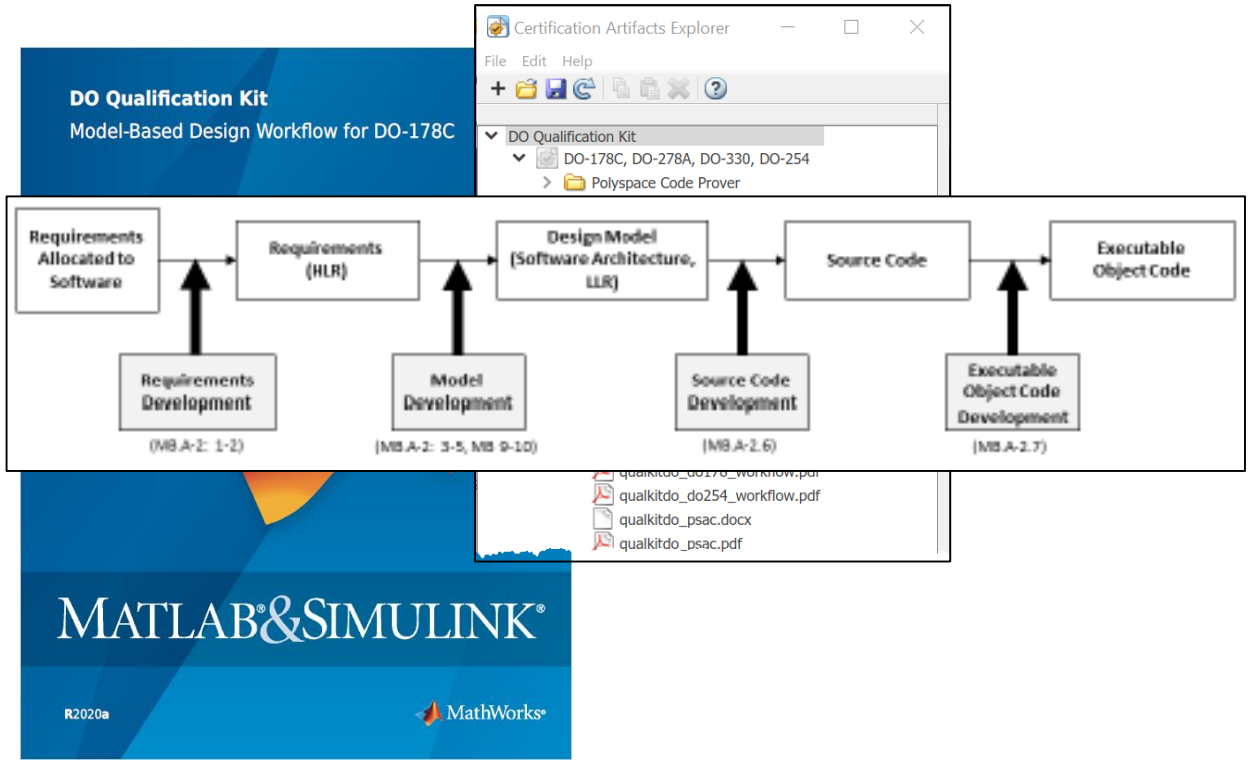
- 能够对代码生成和验证产品工具进行认证
- 包含文档、测试用例和认证流程





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 Desian

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.

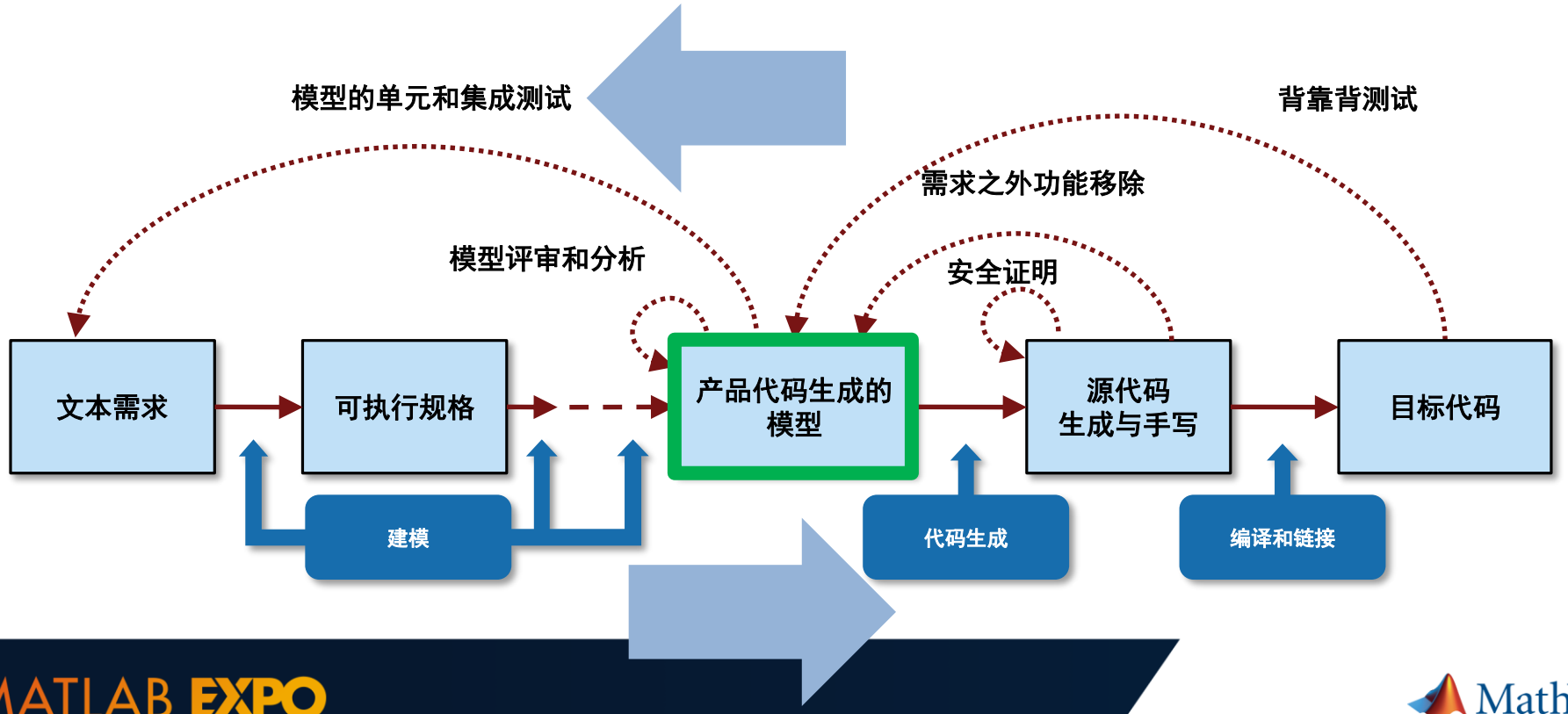
使用参考流程满足认证标准

模型验证

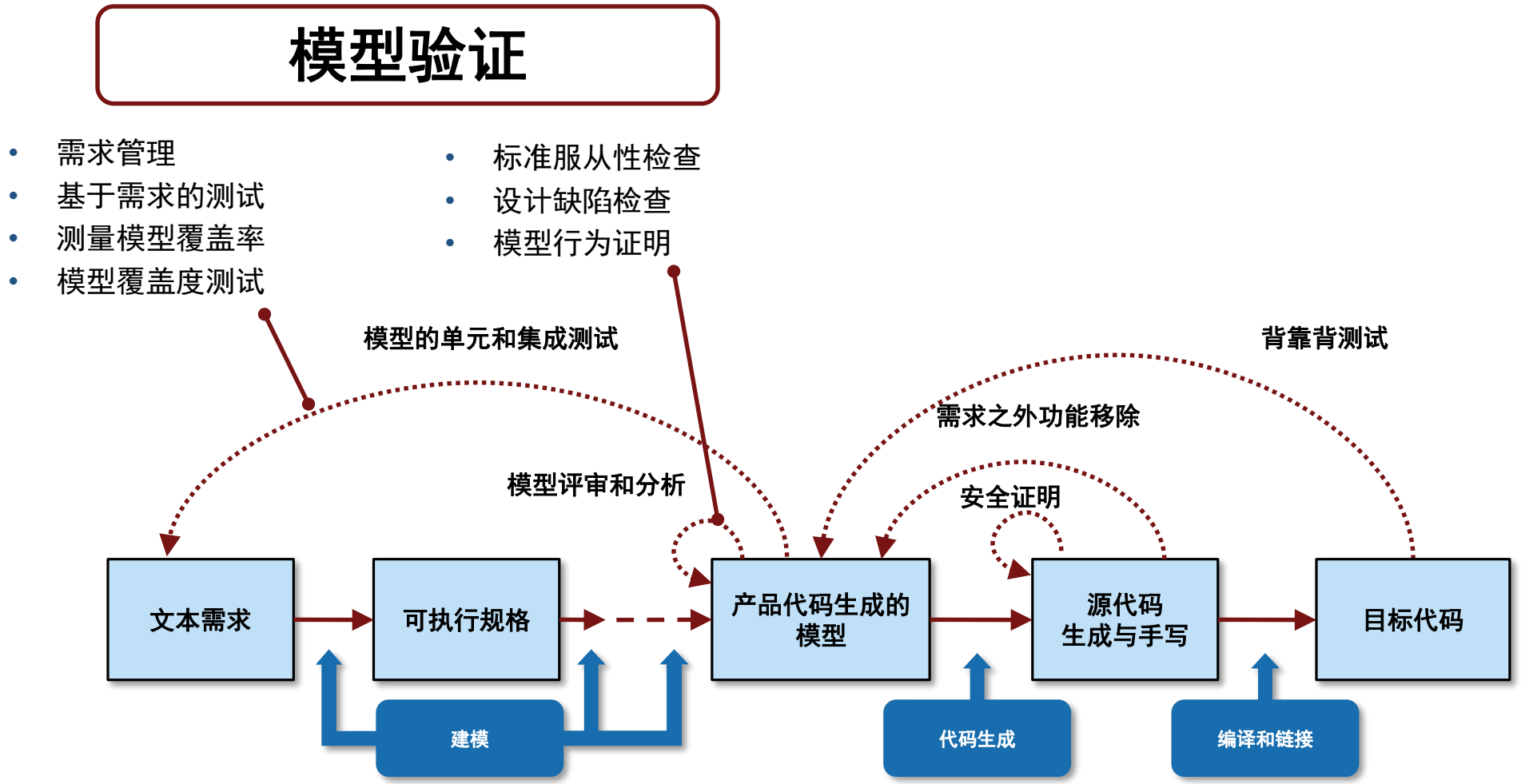
在设计阶段发现设计缺陷

代码验证

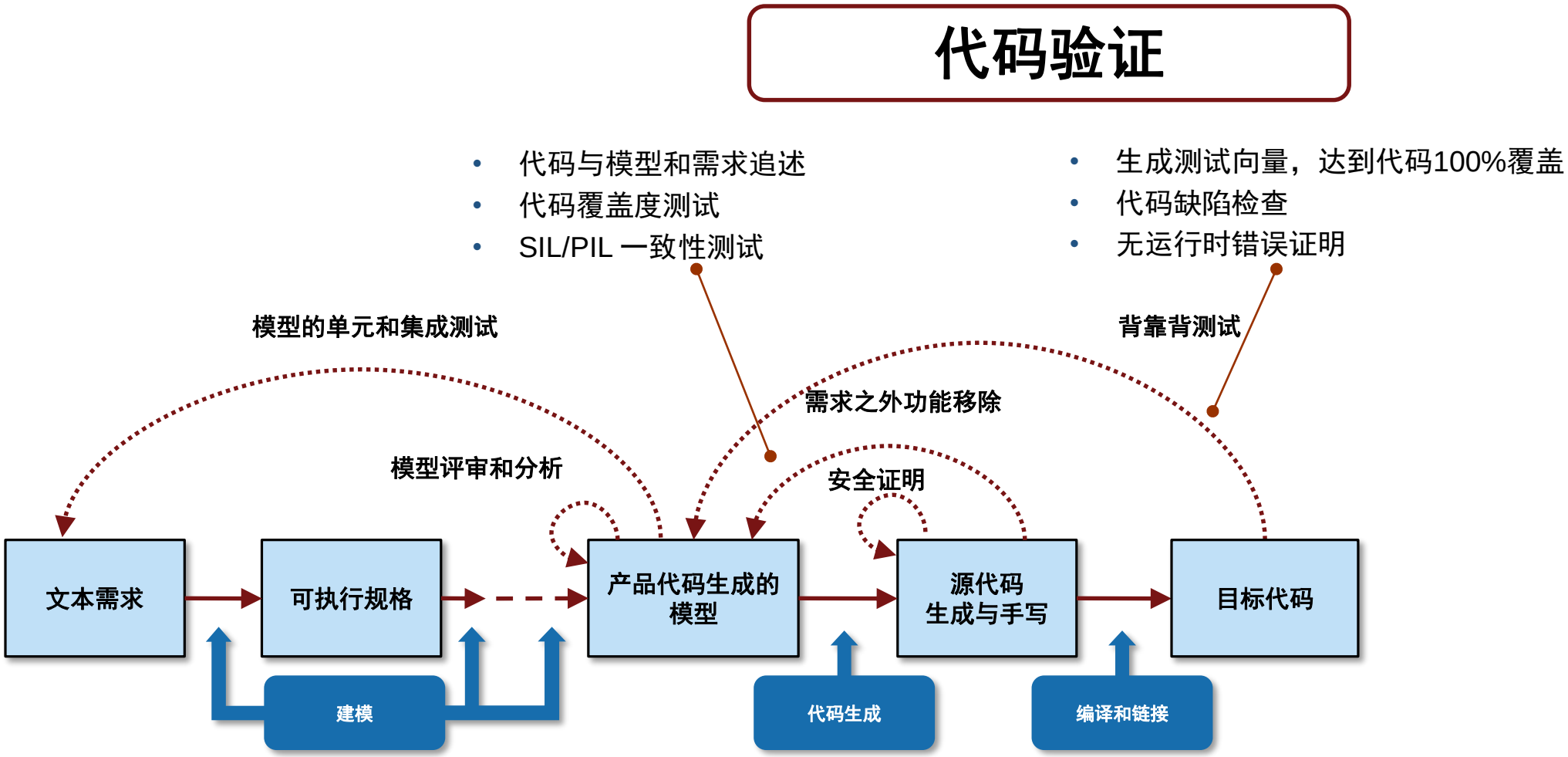
在代码层面提高可靠度



模型验证: 在设计阶段发现设计缺陷



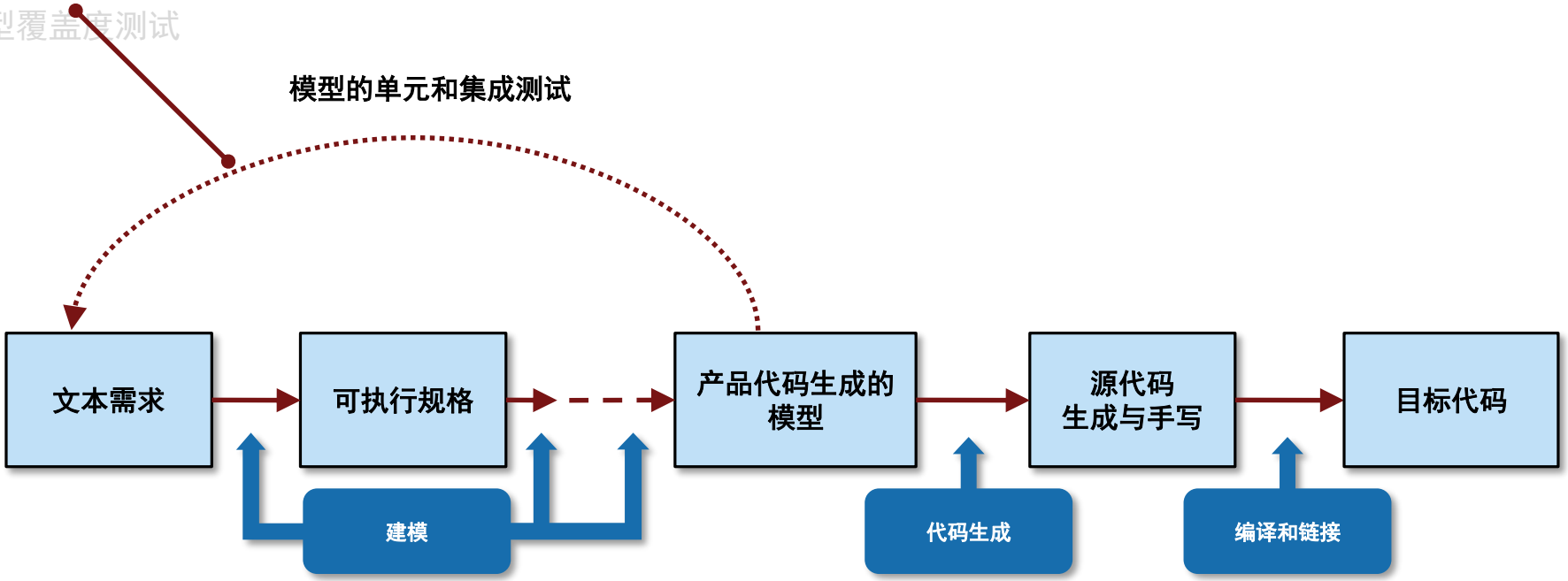
代码验证: 在代码层面提高可靠度



需求管理

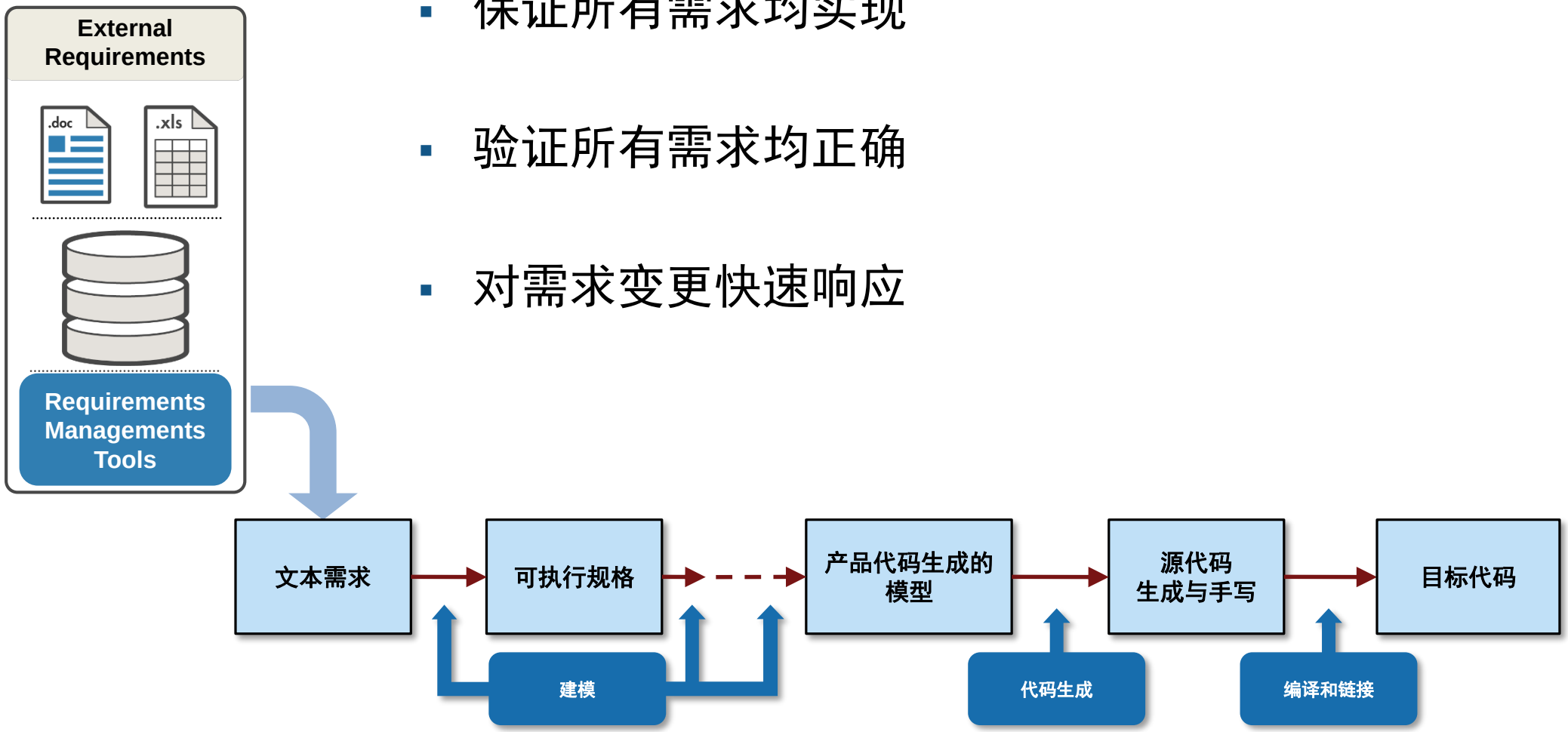
模型验证

- **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

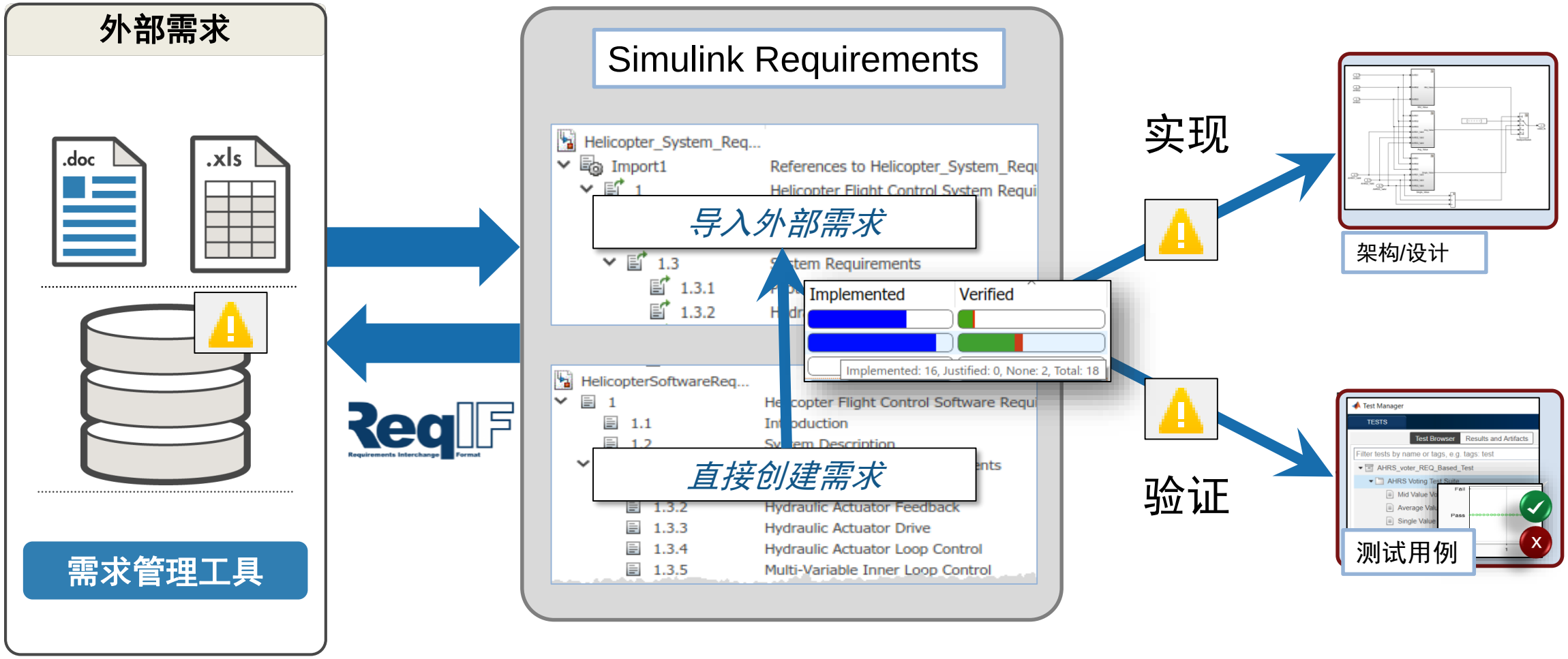


需求管理

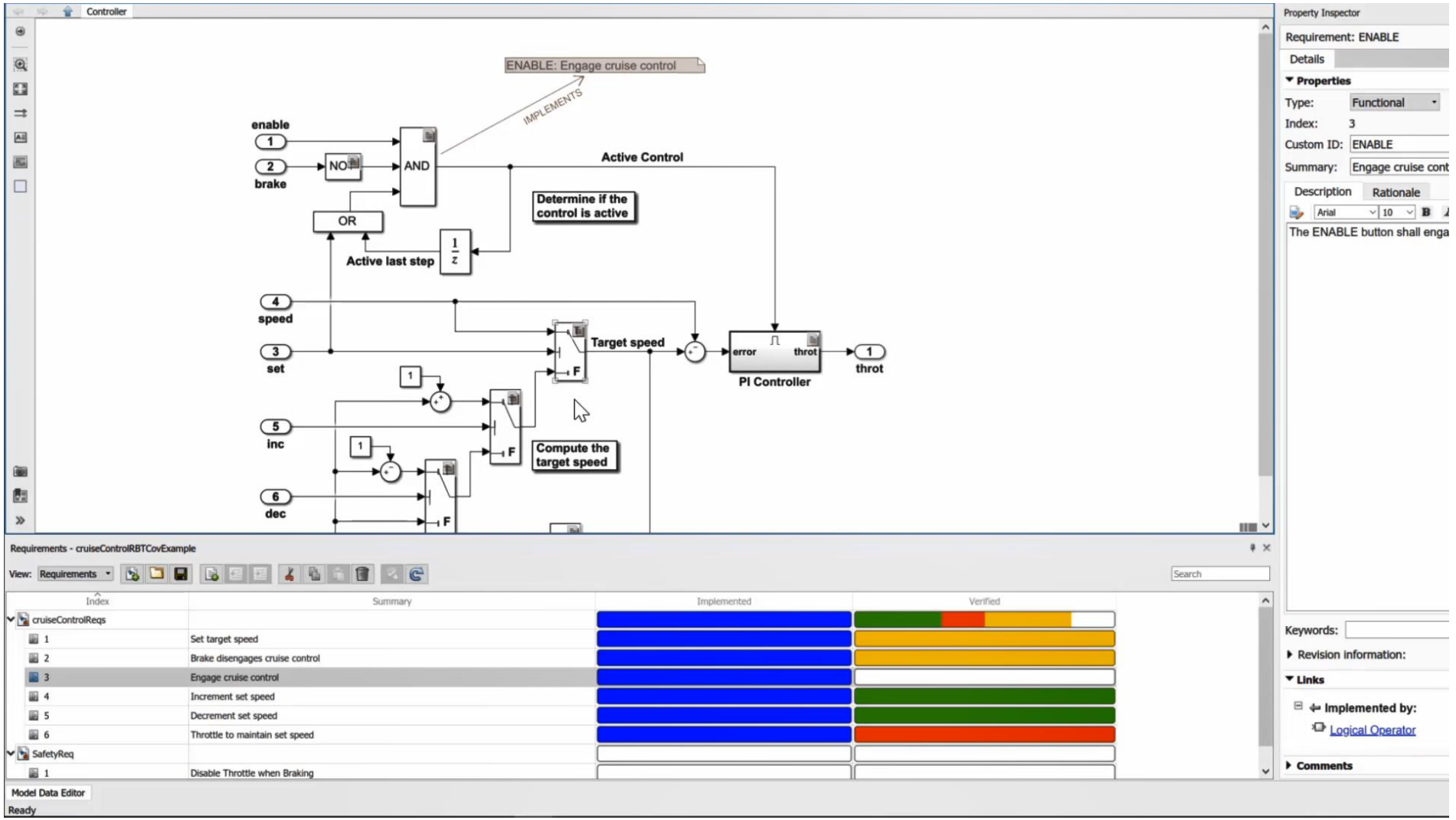
- 保证所有需求均实现
- 验证所有需求均正确
- 对需求变更快速响应



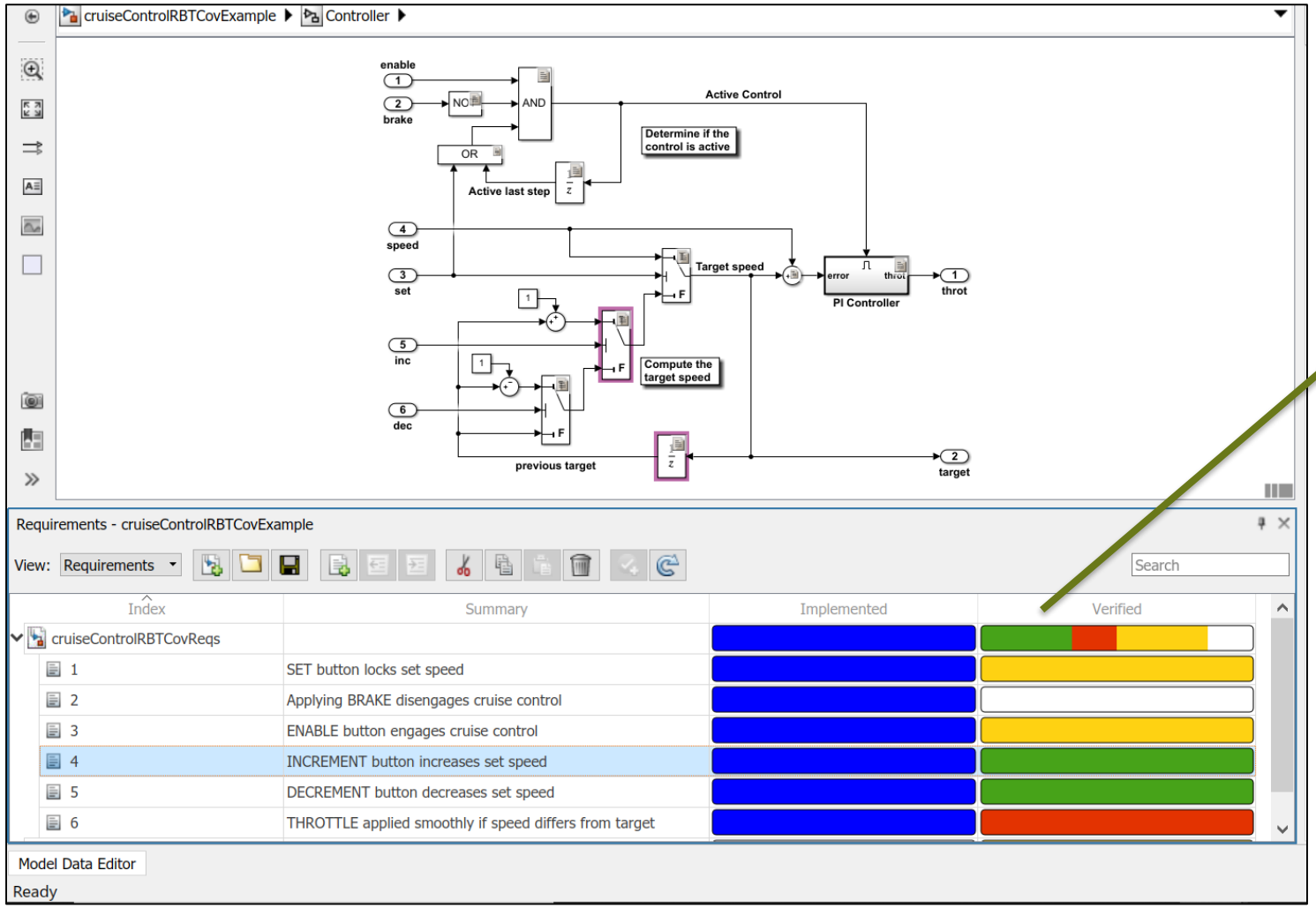
将需求、架构和设计放在一个框架下工作

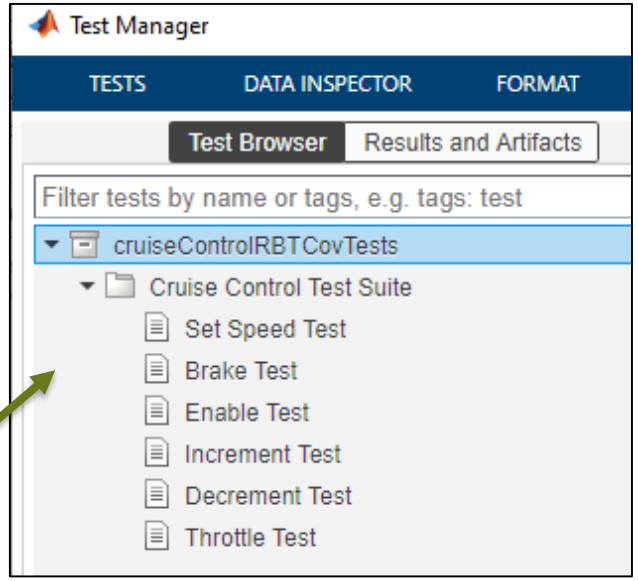


演示: 需求视图


Controller
ENABLE: Engage cruise control
IMPLEMENTS
enable
1
2
brake
NO
AND
Active Control
Determine if the control is active
OR
Active last step
1/z
4
speed
3
set
Target speed
F
error
throt
PI Controller
1
throt
1
5
inc
F
Compute the target speed
1
6
dec
F
Property Inspector
Requirement: ENABLE
Details
Properties
Type: Functional
Index: 3
Custom ID: ENABLE
Summary: Engage cruise cont
Description
Rationale
Arial
10
The ENABLE button shall enga
Requirements - cruiseControlRBTCovExample
View: Requirements
Search
Index
Summary
Implemented
Verified
cruiseControlReqs
1 Set target speed
2 Brake disengages cruise control
3 Engage cruise control
4 Increment set speed
5 Decrement set speed
6 Throttle to maintain set speed
SafetyReq
1 Disable Throttle when Braking
Keywords:
Revision information:
Links
Implemented by:
Logical Operator
Comments
Model Data Editor
Ready

测试和需求的追溯性

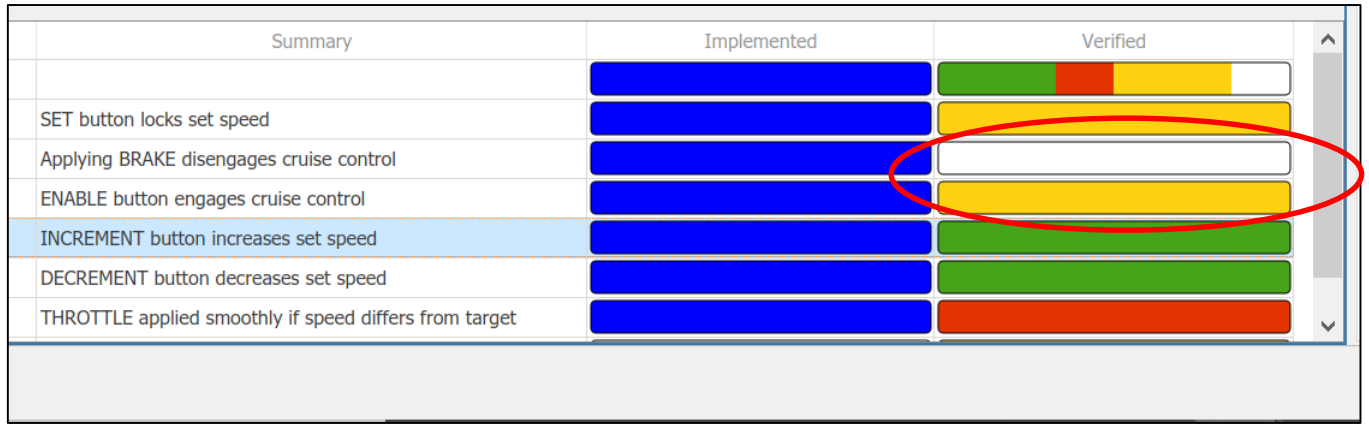




测试验证状态

- 通过
- 不通过
- 未执行
- 无测试用例

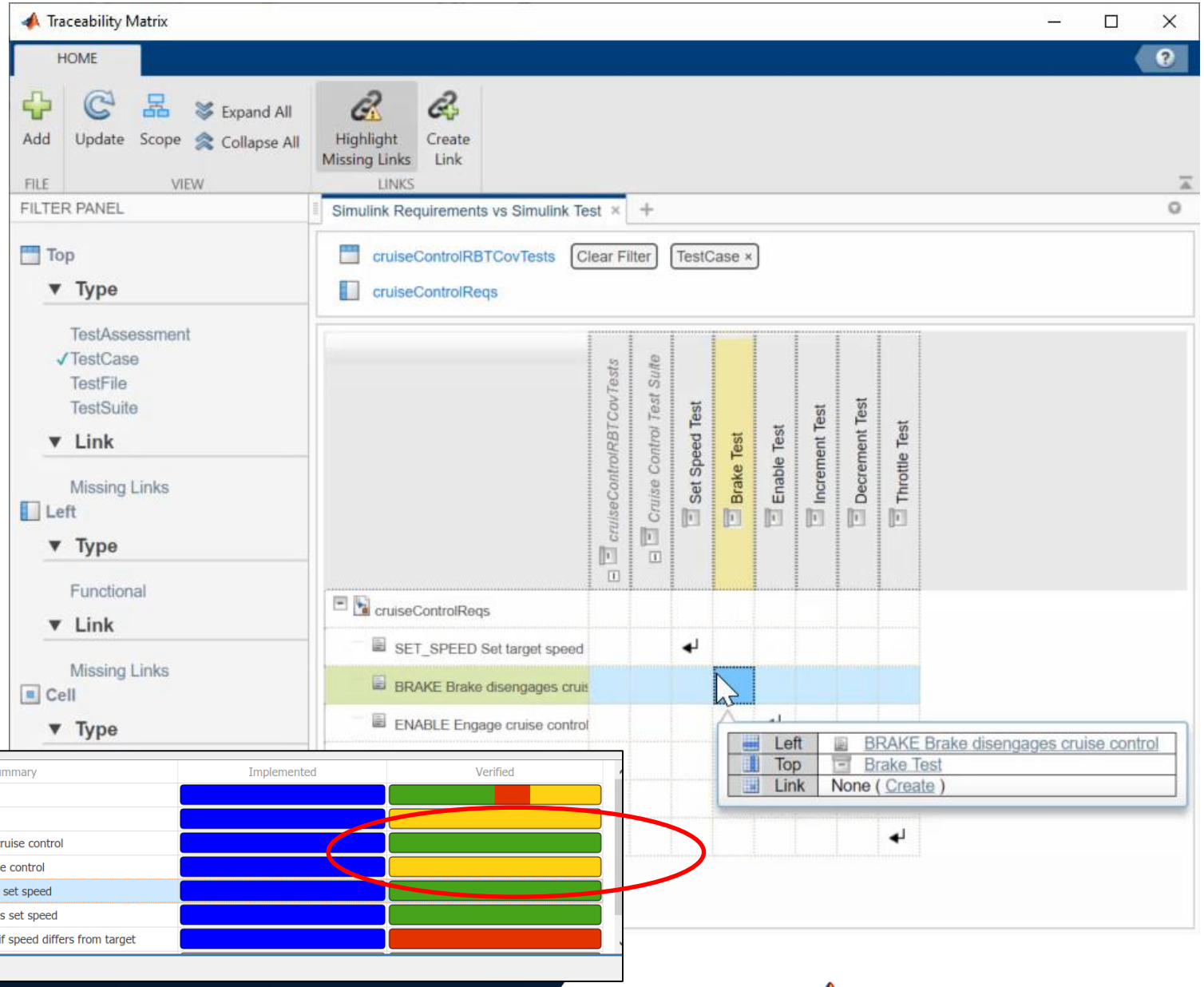
使用追溯性矩阵审查和分析追溯关系



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

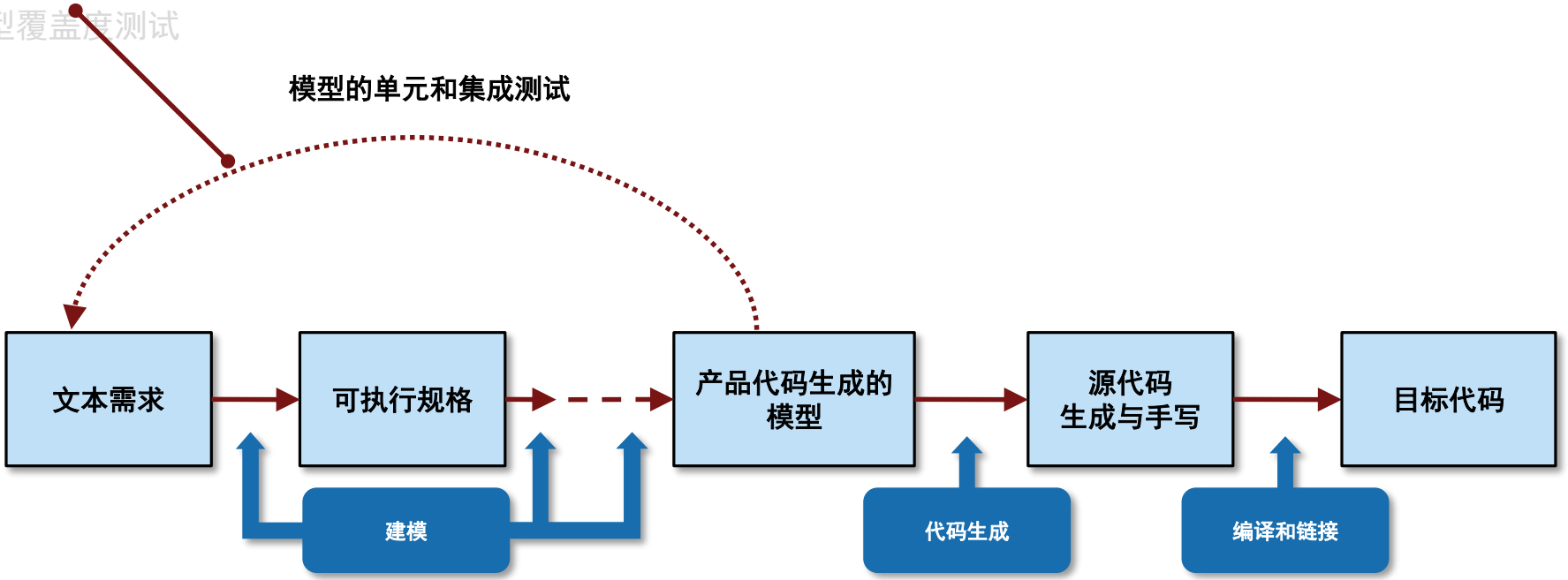
- 需求、模型和测试追溯性审查
- 建立筛选视图
- 高亮缺失的关联
- 创建关联，补充缺失



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

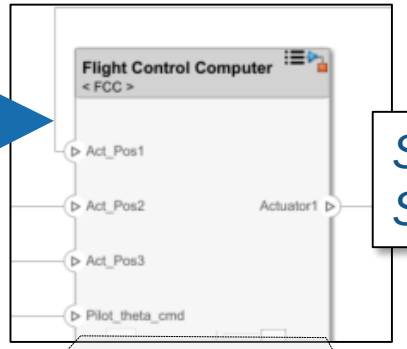


使用 Simulink Test 进行基于需求的验证

功能需求
飞行控制系统应...

被实现

被验证



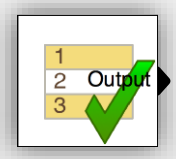
System Composer / Simulink / Stateflow

测试用例

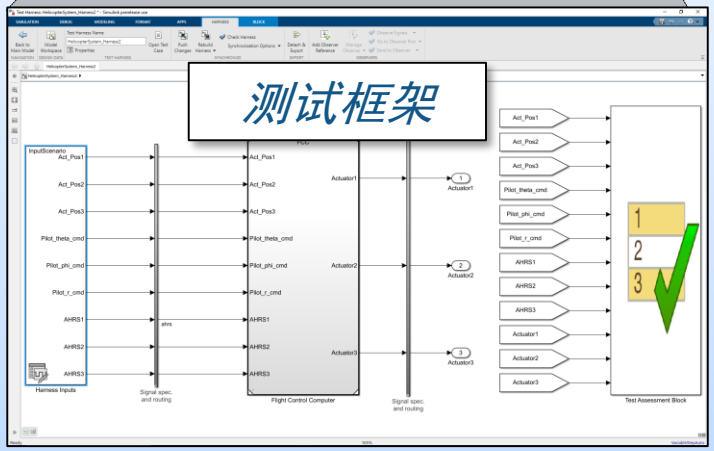
测试输入

MAT / Excel file (input)

Signal Editor



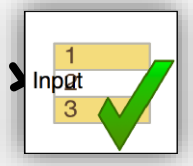
Test Sequence



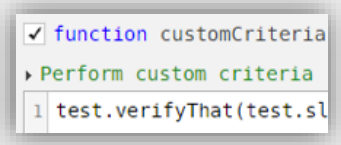
Simulink Test

输出评估

MAT / Excel File (baseline)



Test Assessments

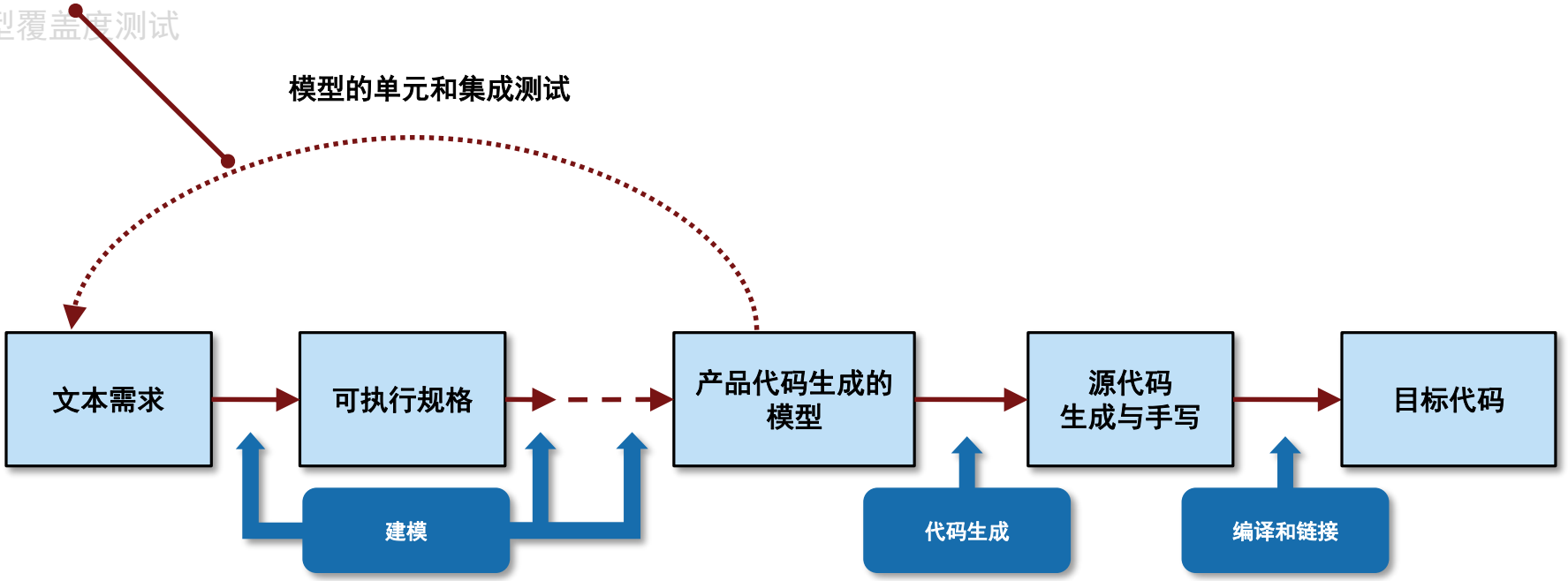


MATLAB Unit Test

测试完整性度量

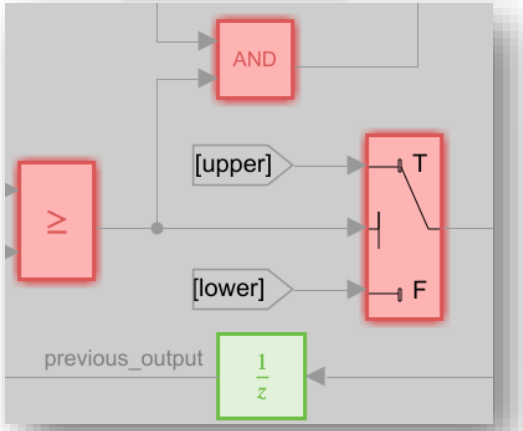
模型验证

- 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

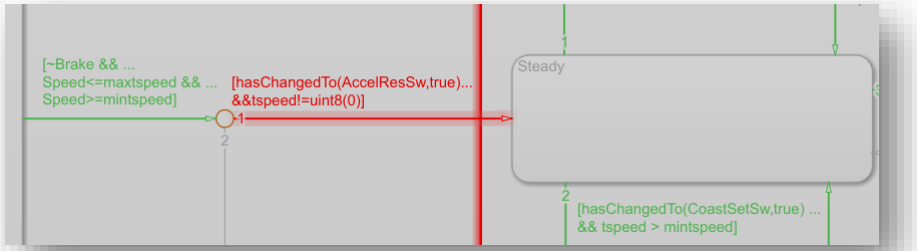


覆盖度分析

Simulink



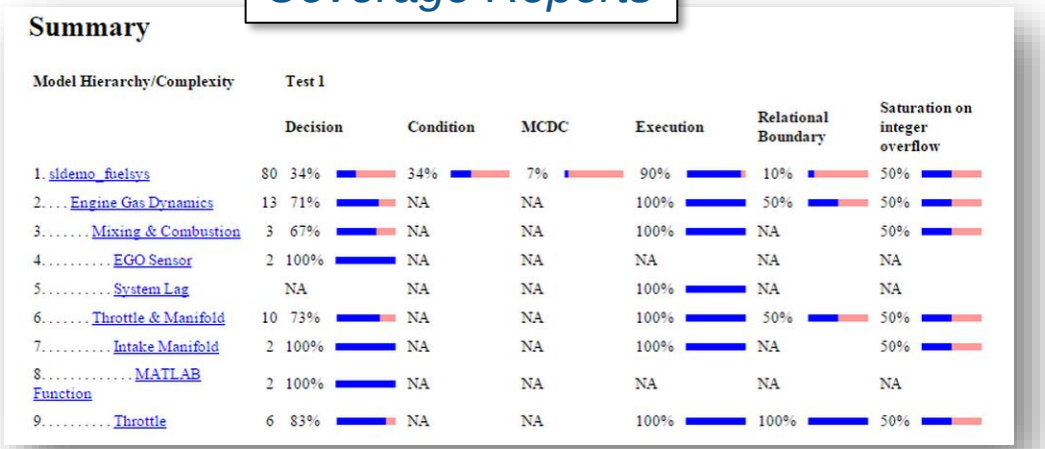
Stateflow



- 识别测试不足
- 需求不全
- 非需要功能
- 设计错误

Code

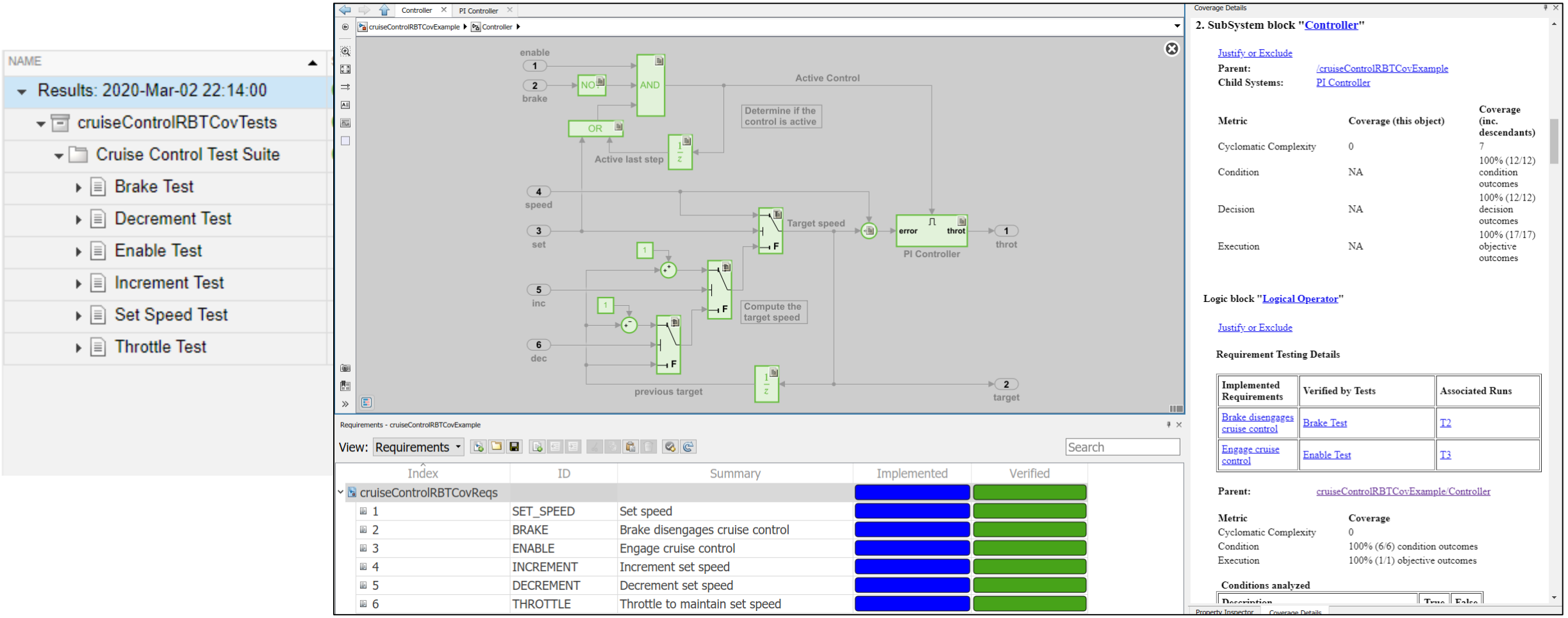
Coverage Reports



Summary

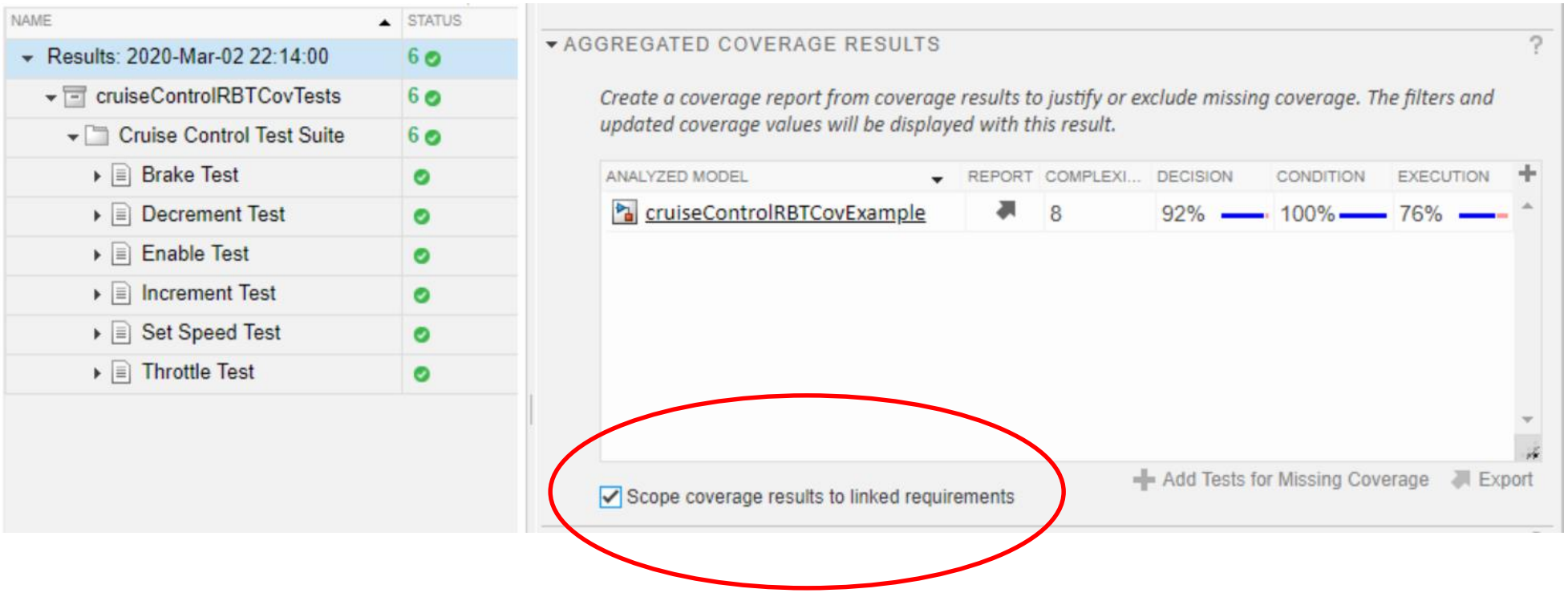
Model Hierarchy/Complexity	Test 1									
		Decision		Condition		MCDC		Execution	Relational Boundary	Saturation on integer overflow
1. sldemo_fuelsys	80	34%		34%		7%		90%	10%	50%
2. Engine Gas Dynamics	13	71%		NA		NA		100%	50%	50%
3. Mixing & Combustion	3	67%		NA		NA		100%	NA	50%
4. EGO Sensor	2	100%		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%

覆盖度结果中测试和需求的追溯关系



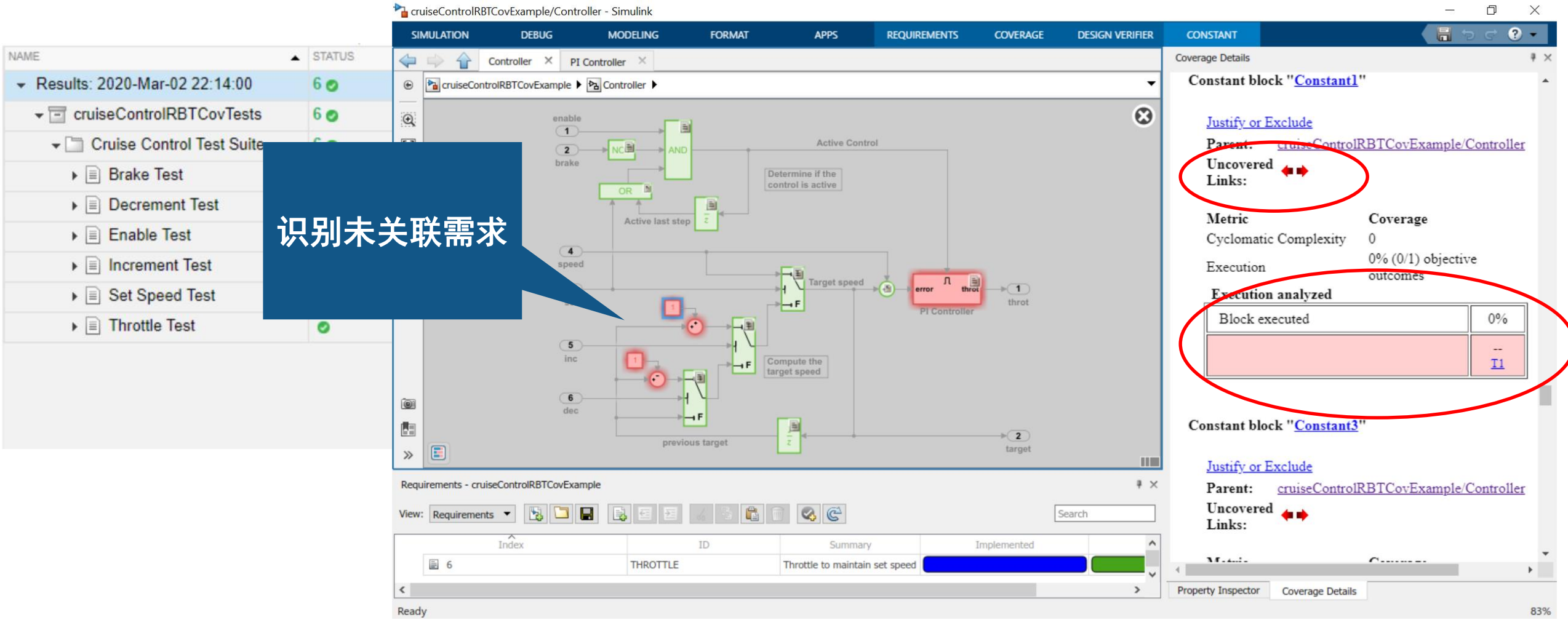
模型覆盖度限定在基于需求测试中

R2020a

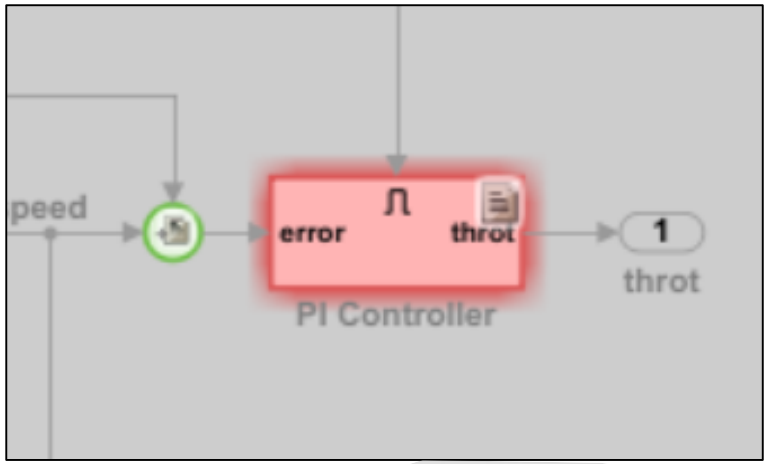


模型覆盖度限定在基于需求测试中

R2020a



覆盖度结果中测试和需求的追溯关系

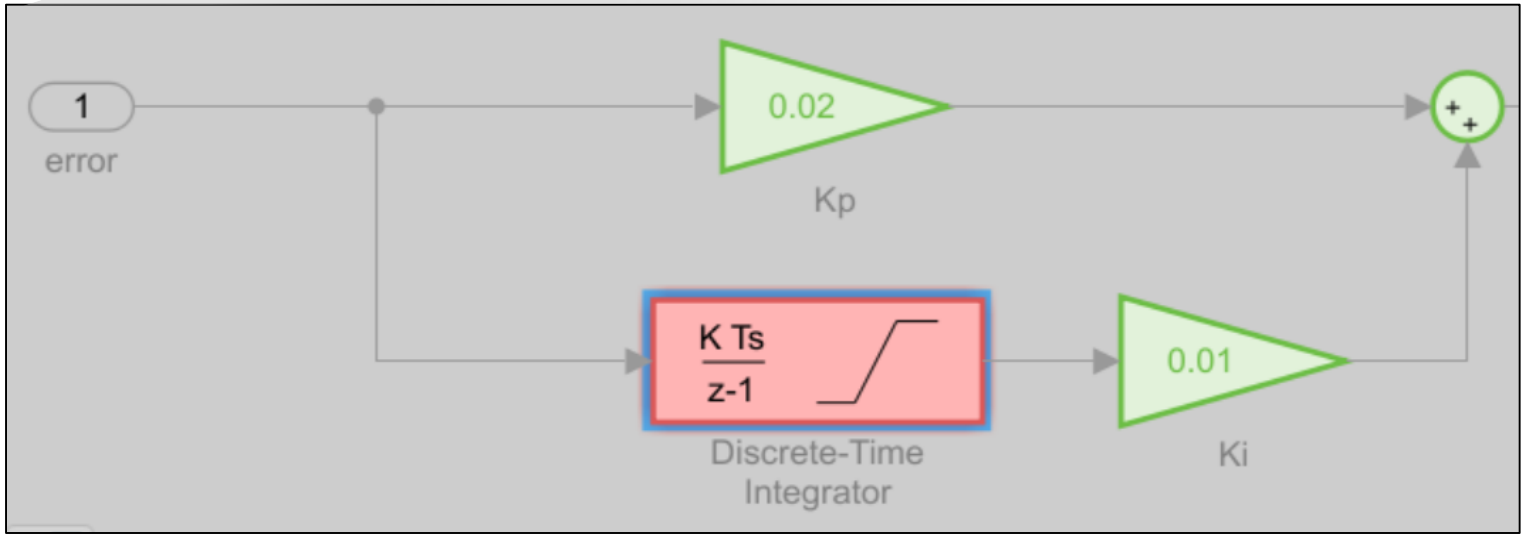


3. SubSystem block "PI Controller"

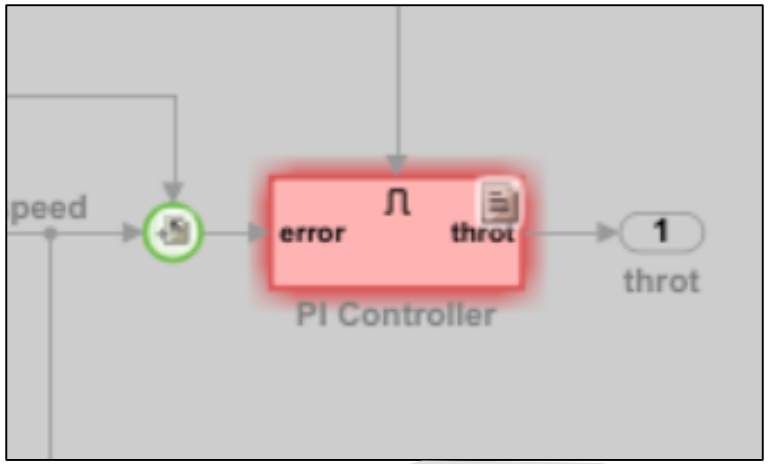
Justify or Exclude

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

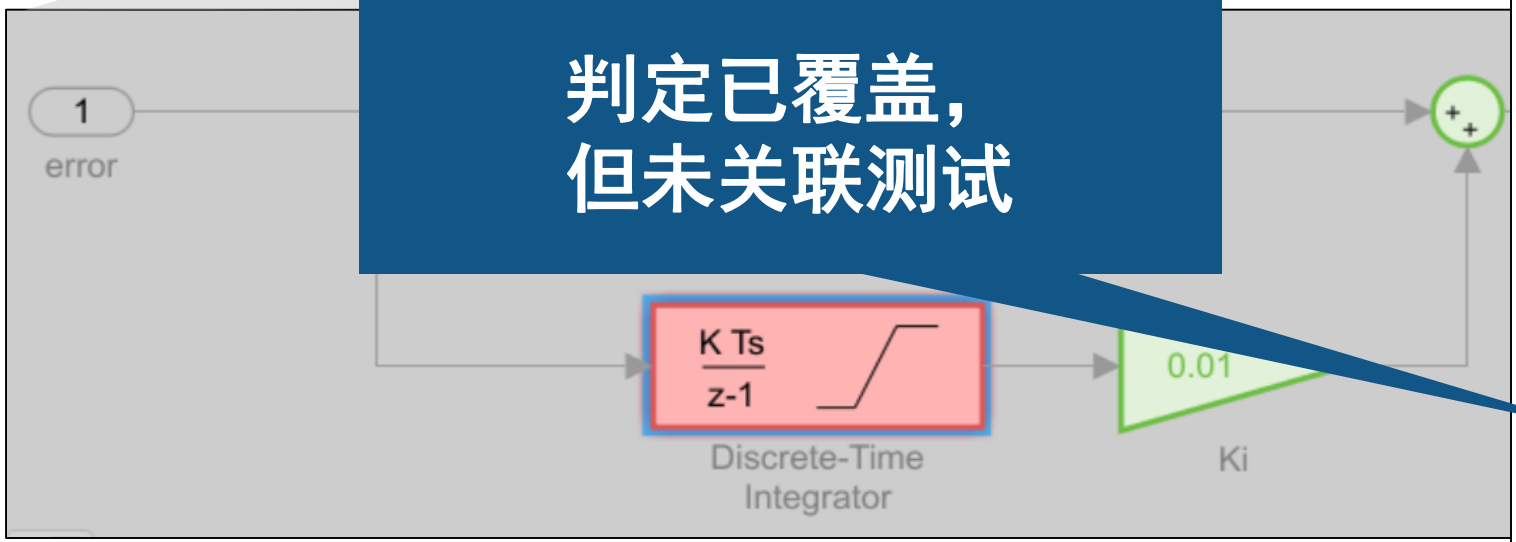
Parent: cruiseControlRBTCovExample/Controller/PI Controller

Uncovered Links:

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

Decisions analyzed

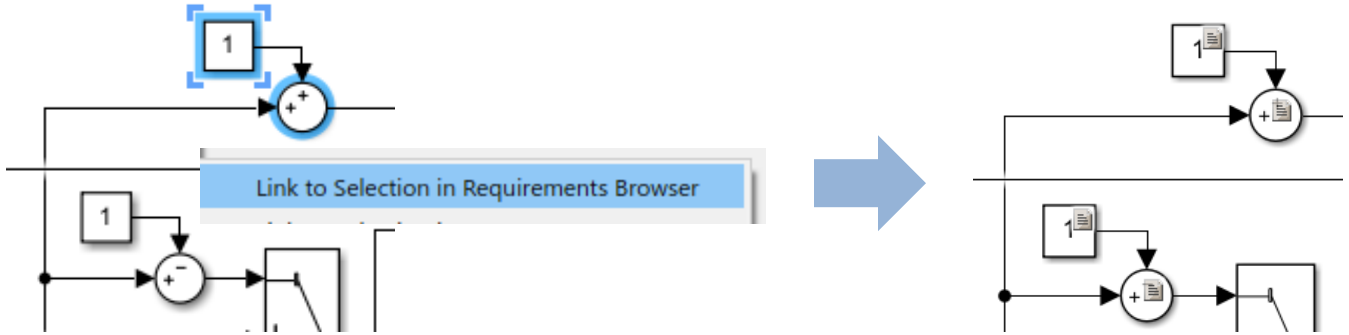
integration result <= lower limit	100%
false	391/801 T6
true	410/801 T6
integration result >= upper limit	50%
false	801/801 T6
true	0/801 T4



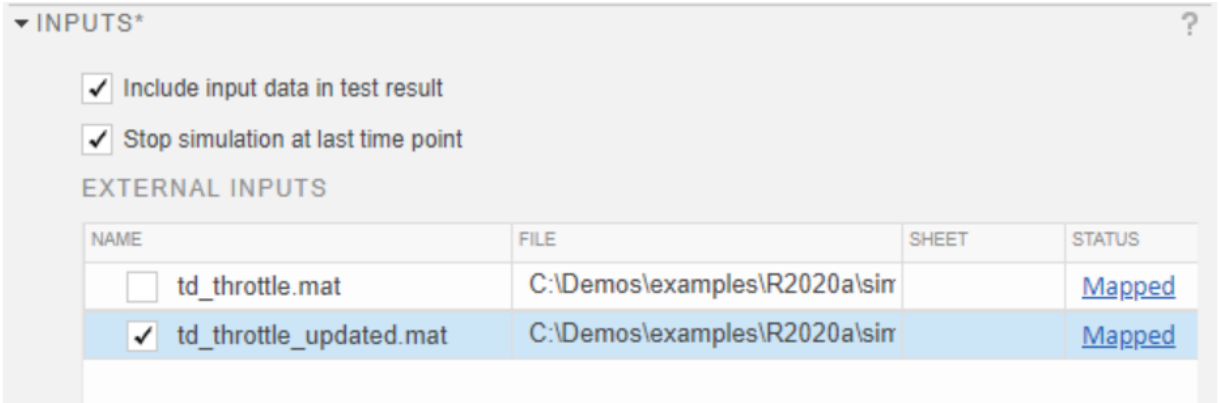
判定已覆盖，但未关联测试

基于需求测试覆盖度不足的处理

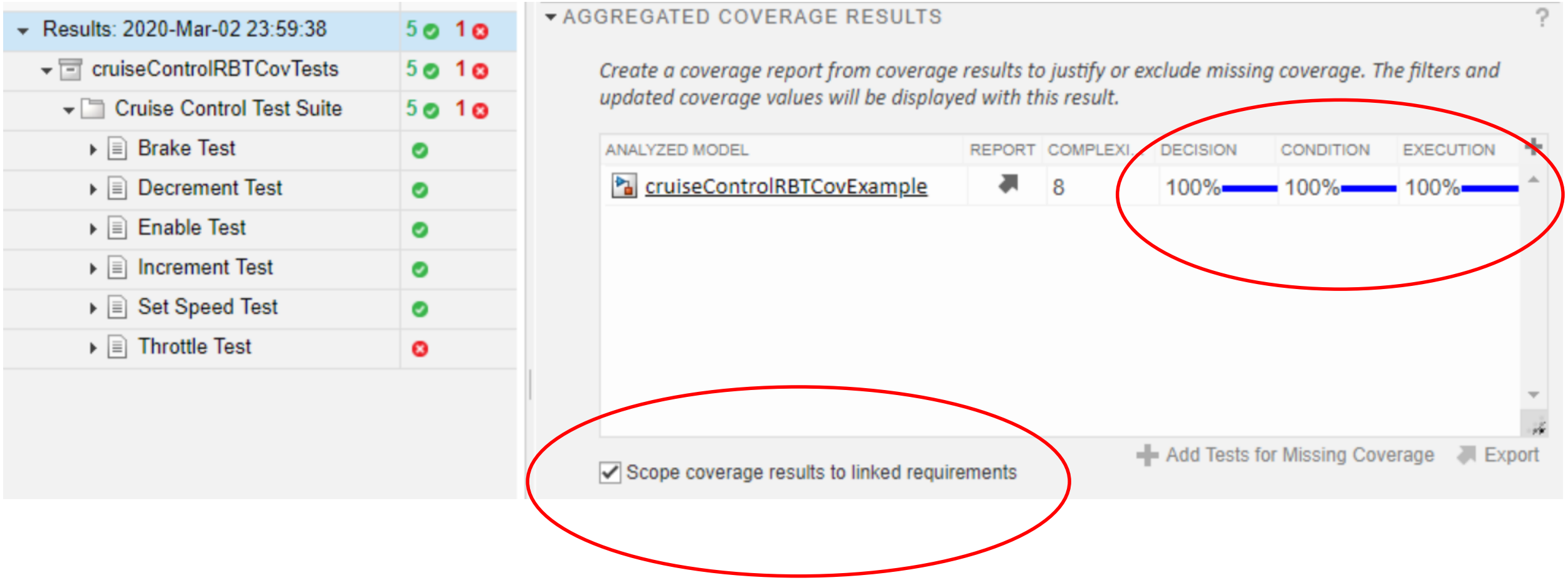
- 添加模型和需求的关联



- 更新测试：提高目标速度



100%覆盖度时，测试不通过

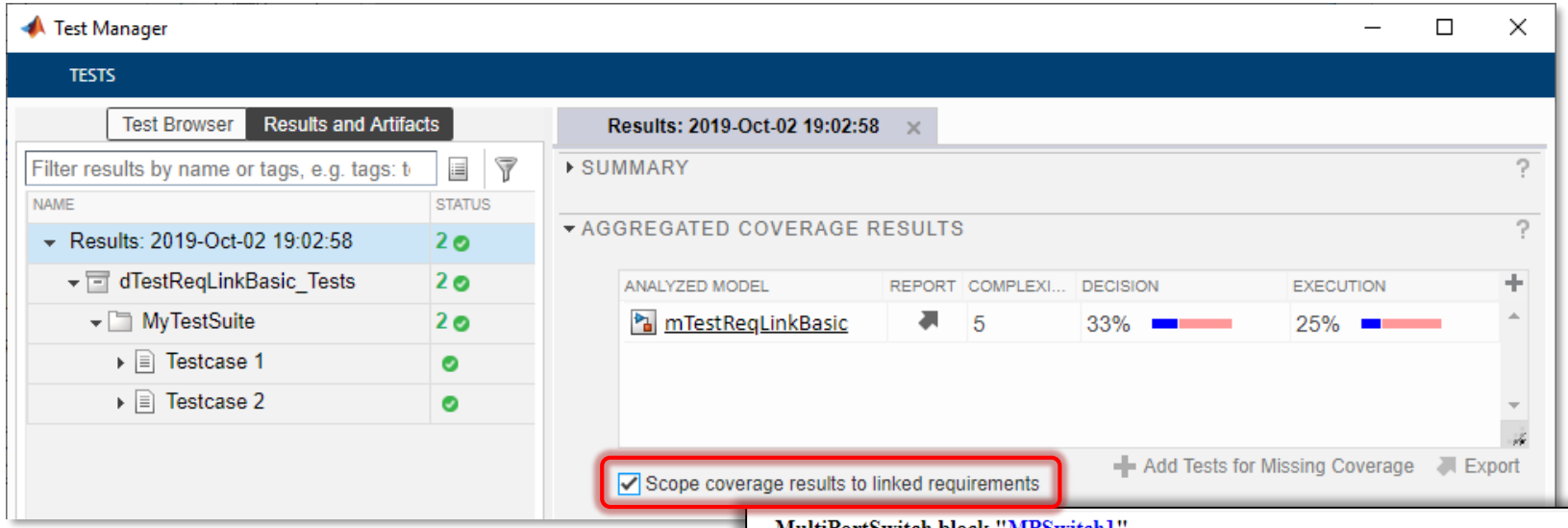


添加测试，发现错误


Results: 2020-Mar-02
cruiseControlRBT
Cruise Control
Brake Test
Decrement
Enable Test
Increment T
Set Speed T
Throttle Tes
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 2.30949999999999.
Upper bound
Lower bound
EXPRESSION TREE
PLOTS
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
Fail
Pass
True
False
Untested
10.50
de missing coverage. The filters and
CISION
CONDITION
EXECUTION
100%
Export

基于需求测试的模型覆盖度

R2020a



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

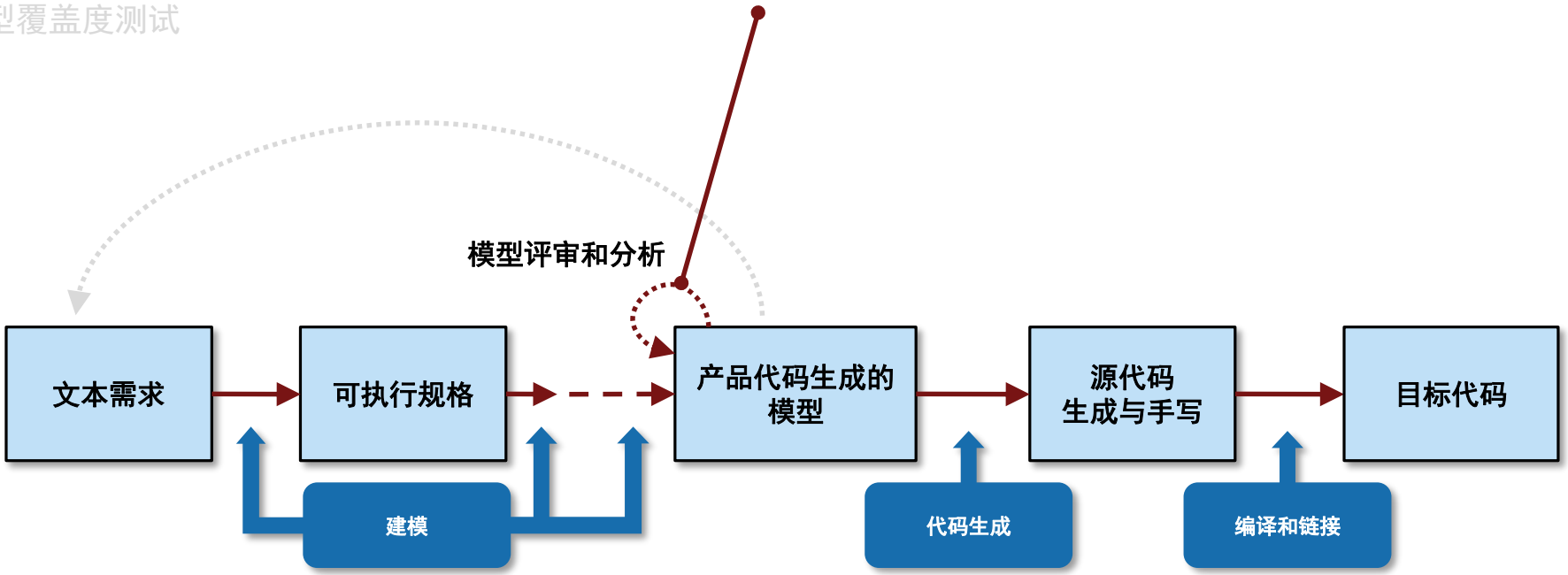
Hit by linked RBT -- **Satisfied**

Hit, but not by linked RBT -- **Unsatisfied**

标准服从性检查

模型验证

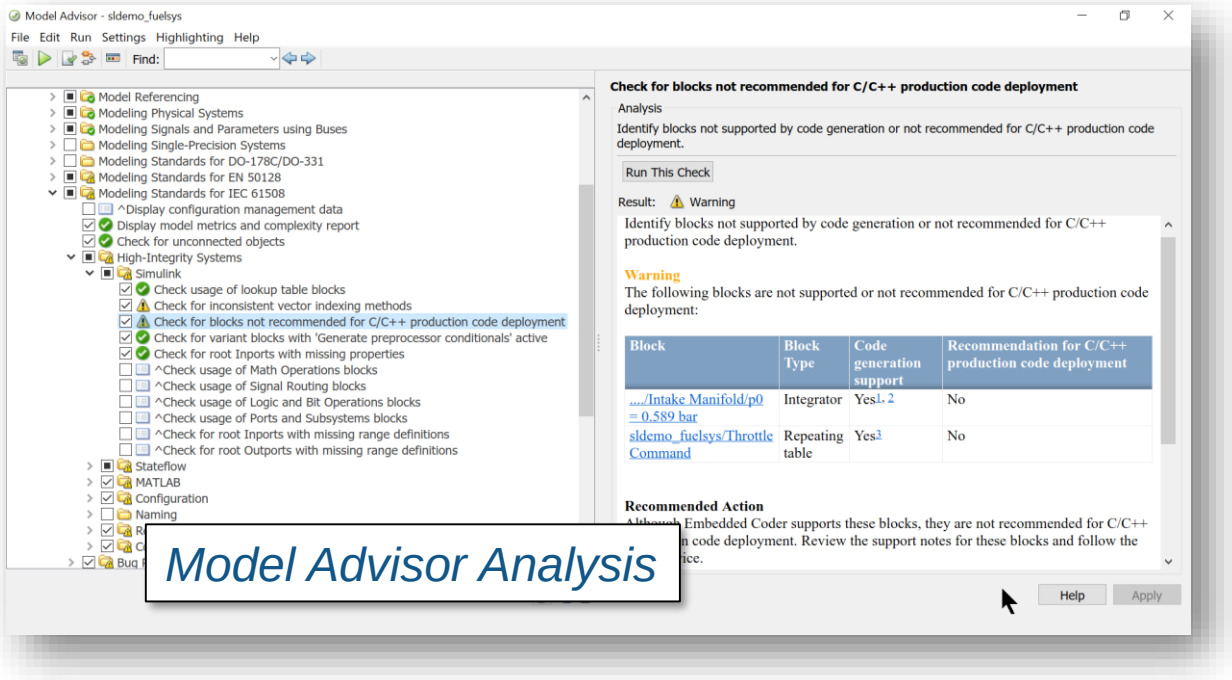
- 需求管理
- 基于需求的测试
- 测量模型覆盖率
- 模型覆盖度测试
- **标准服从性检查**
- 设计缺陷检查
- 模型行为证明

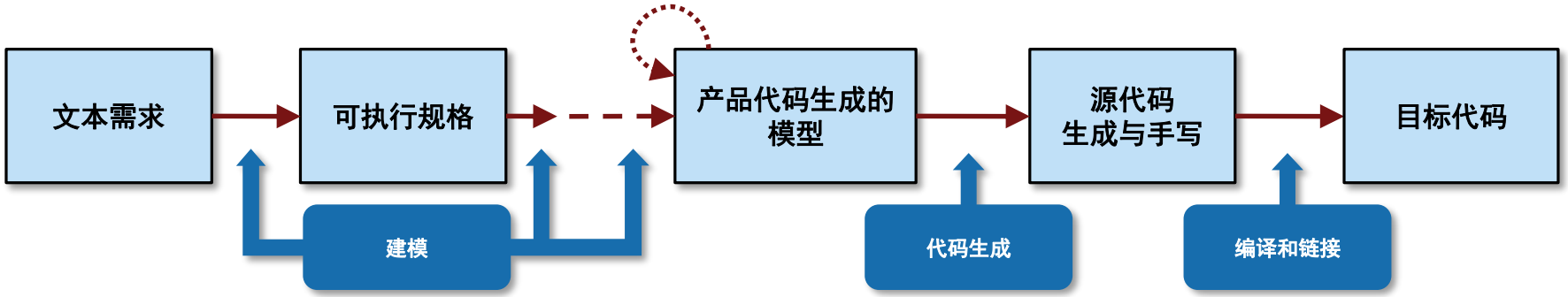


检查设计对设计规范和行业标准的符合性

检查：

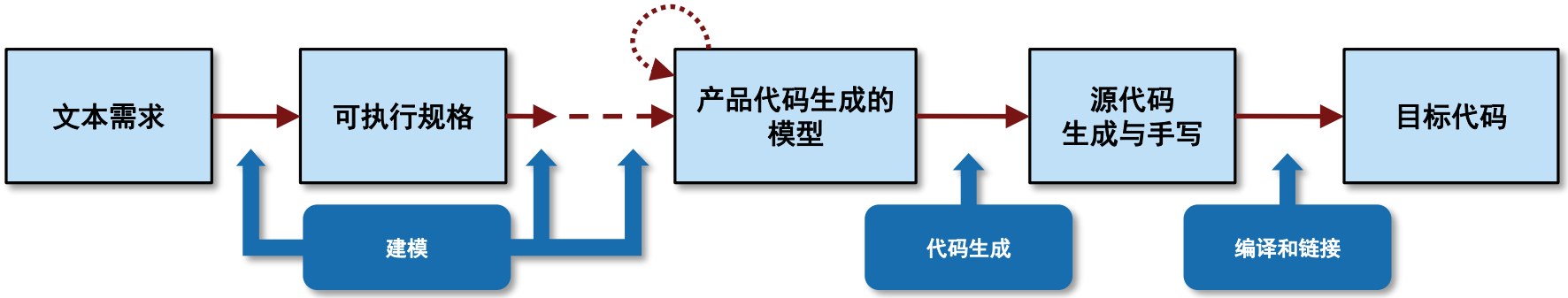
- 可读性与语义
- 性能和效率
- 复制的模块等





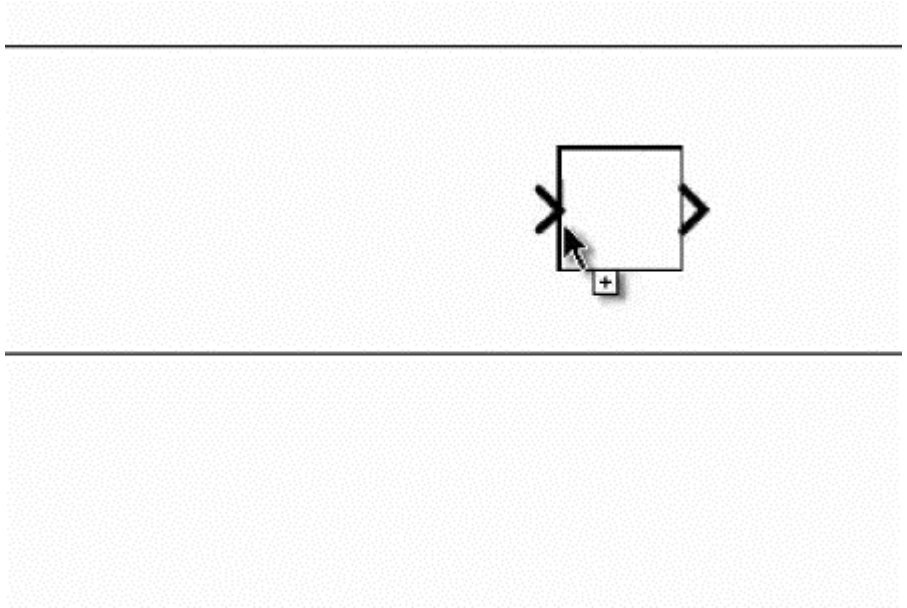
内置工业标准和规范的检查

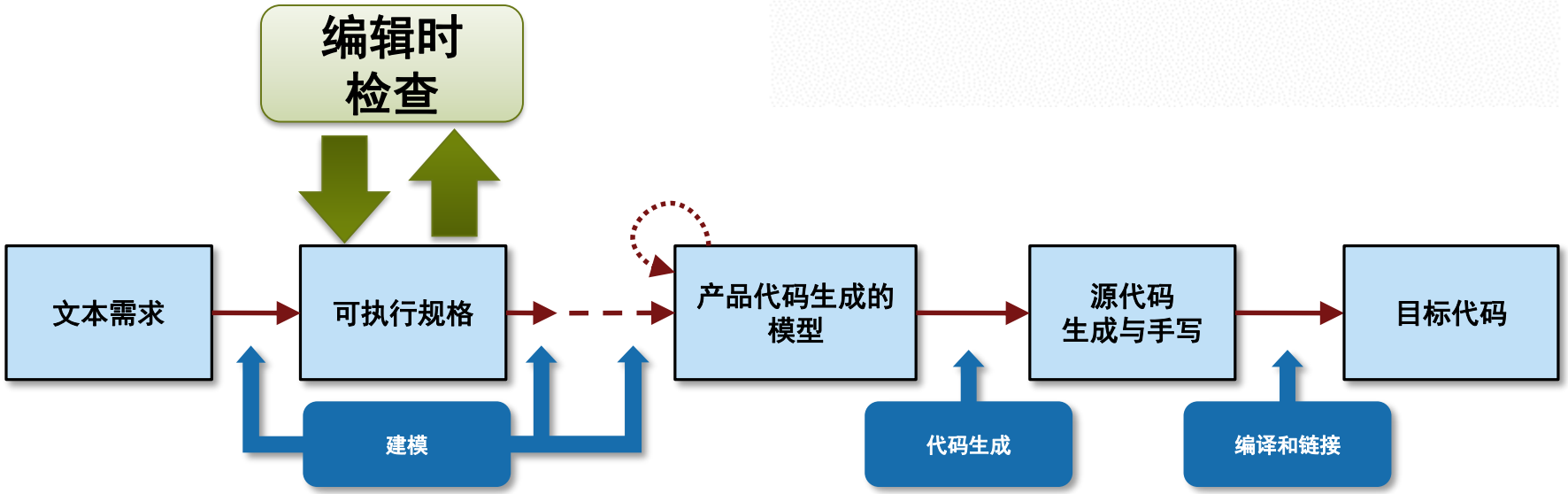
- DO-178/DO-331
- ISO 26262
- IEC 61508
- IEC 62304
- EN 50128
- MISRA C:2012
- CERT C, CWE, ISO/IEC TS 17961
- MAB (MathWorks Advisory Board)
- JMAAB (Japan MATLAB Automotive Advisory Board)



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

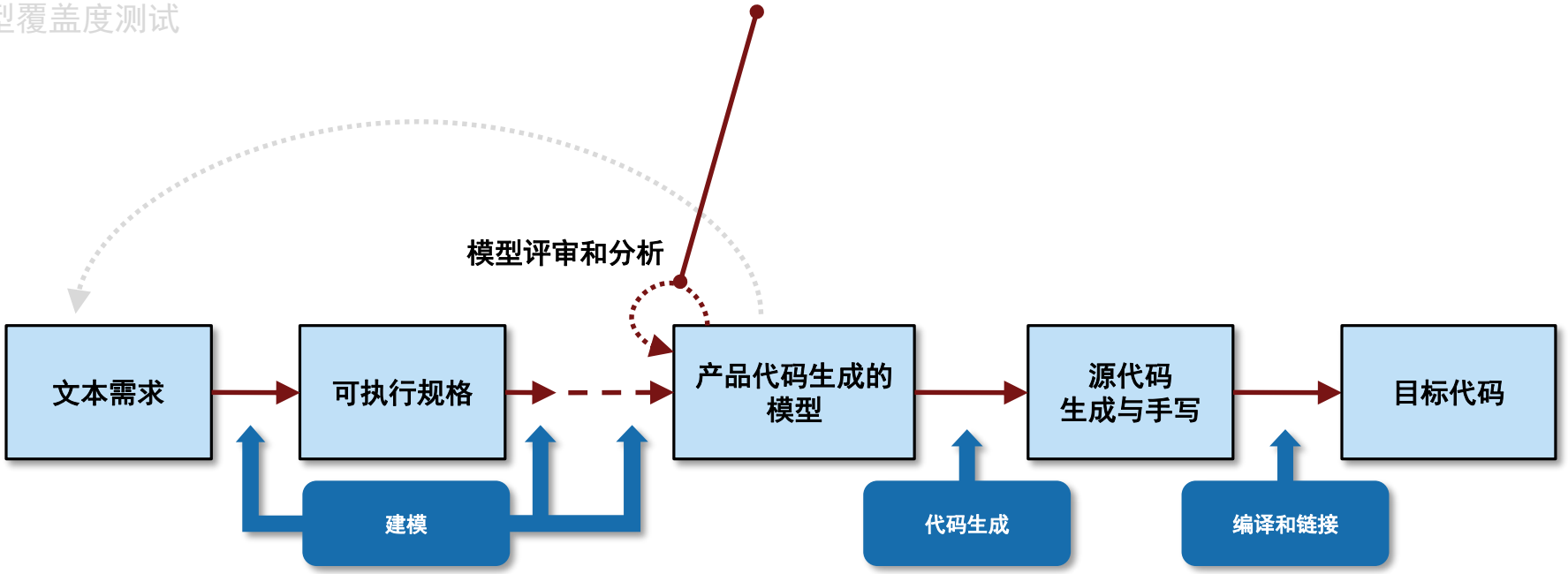




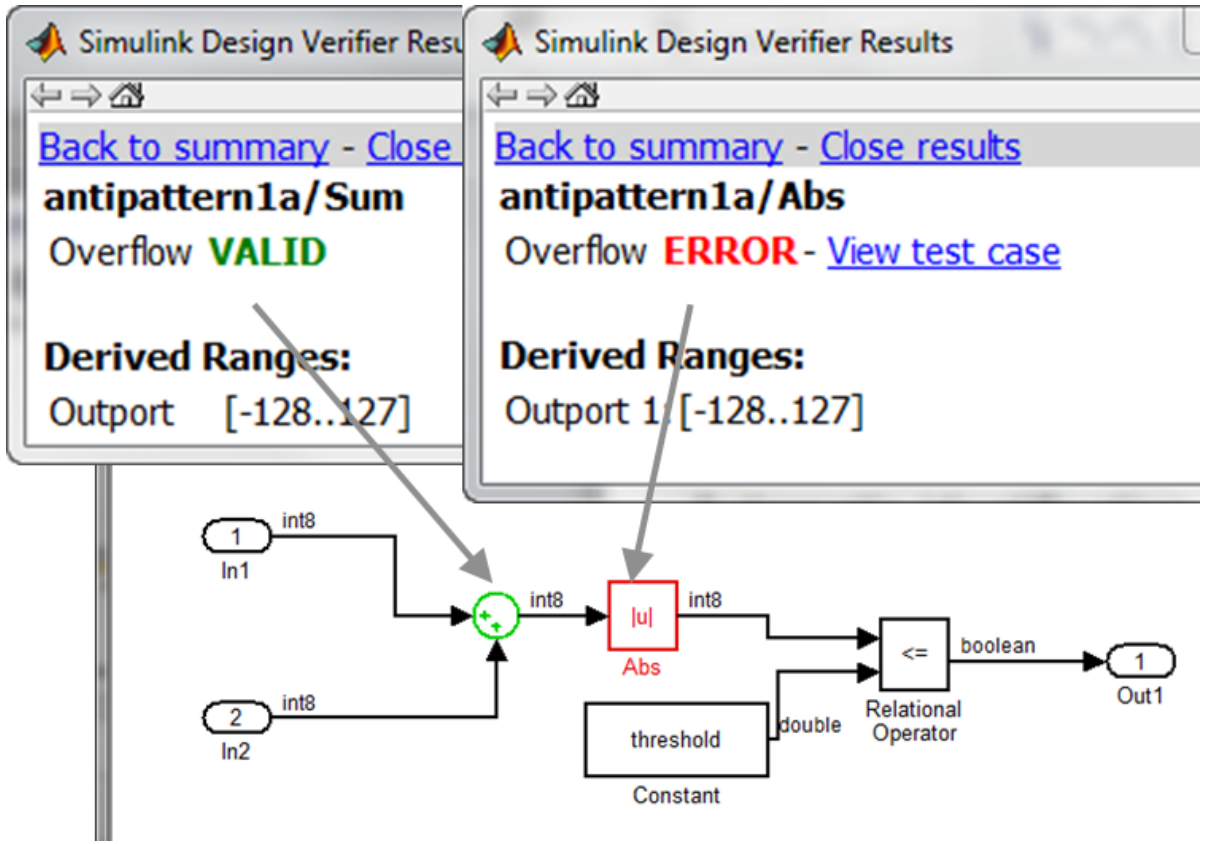
使用形式化方法检查设计错误

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

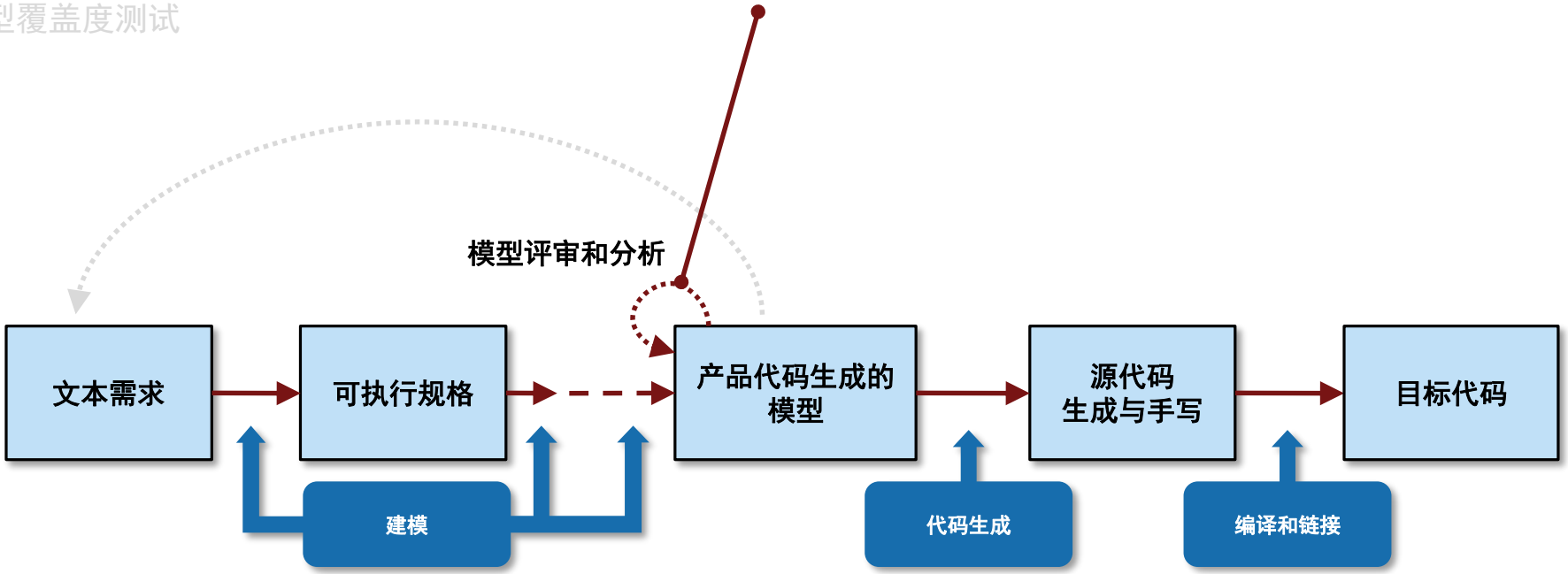


- 检查设计缺陷
  - 整形溢出
  - 死逻辑
  - 除零
  - 数组越界
- 生成反例复现错误

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**

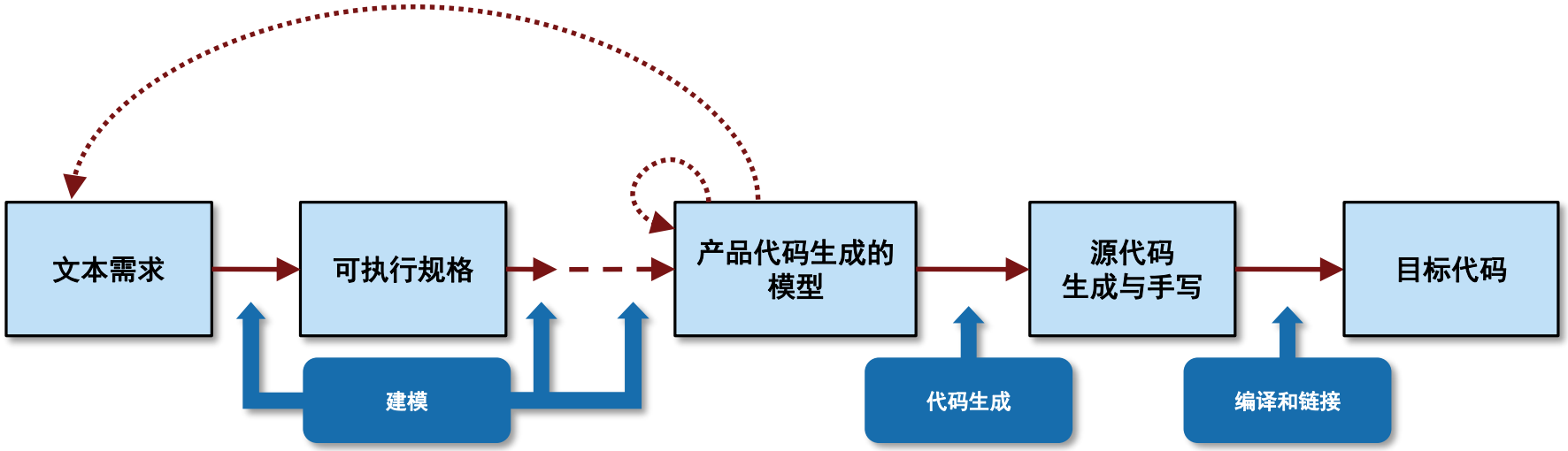


证明模型行为满足需求

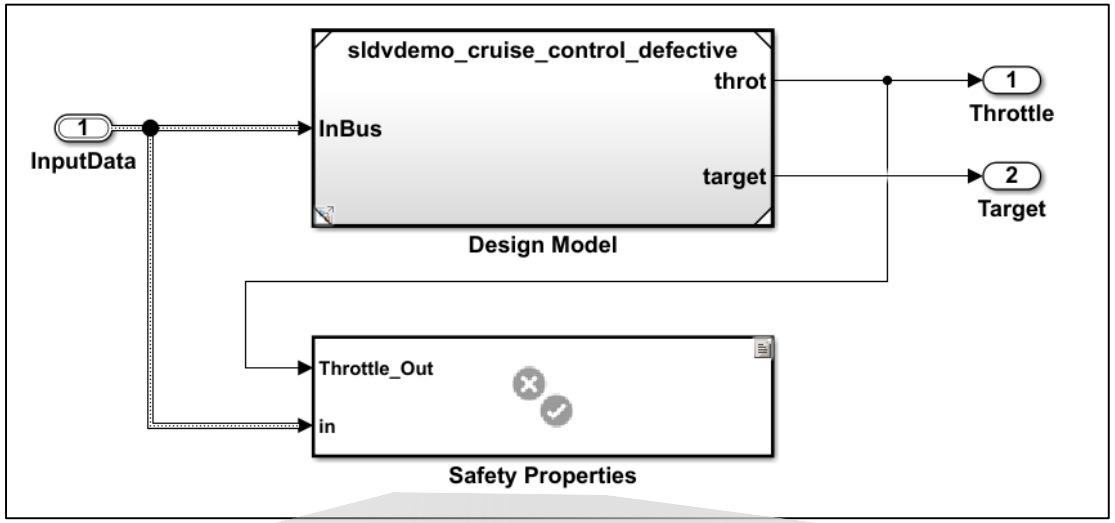
功能安全需求:

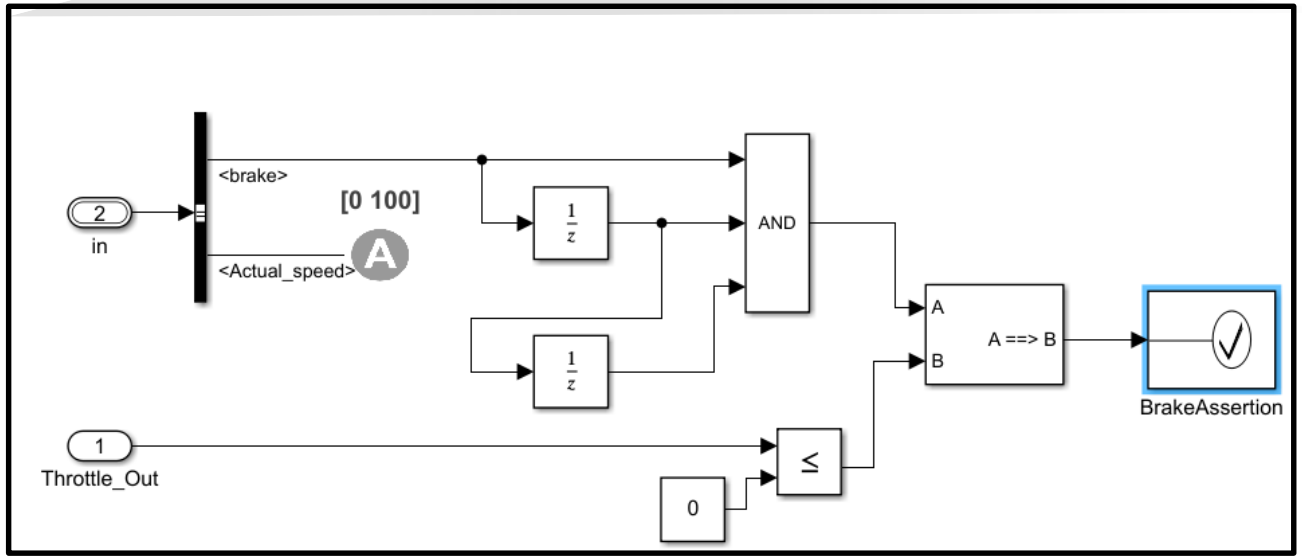
当刹车持续作用3个迭代周期，油门应归零。

- 需要证明：设计完全满足功能需求

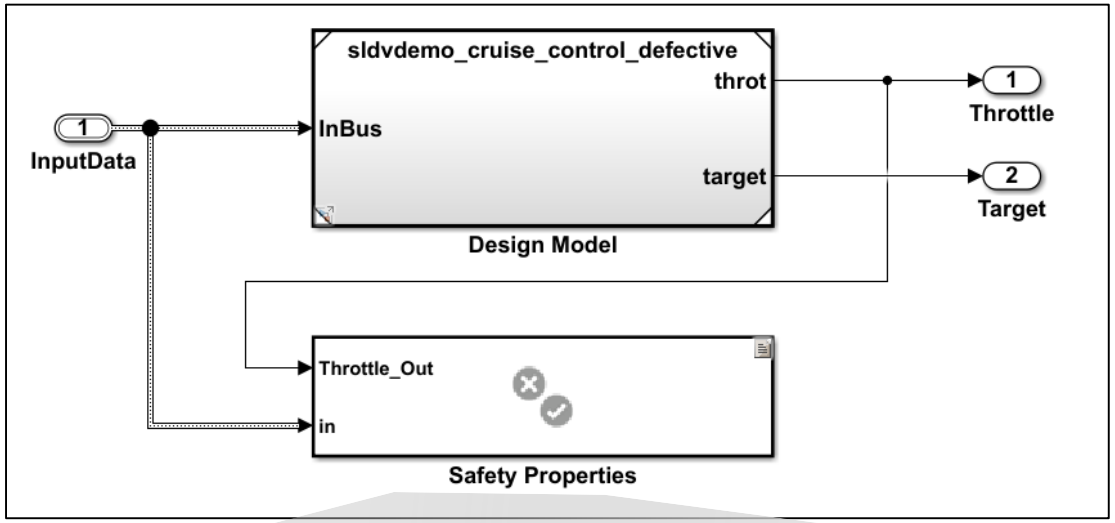


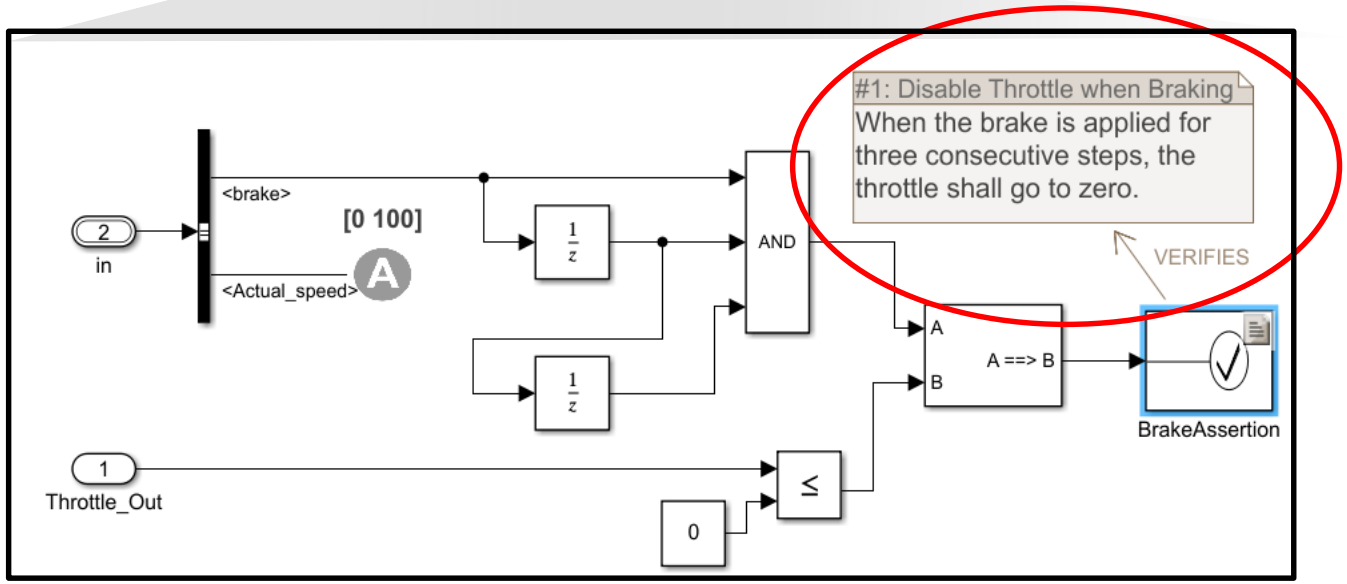
功能需求和安全需求建模





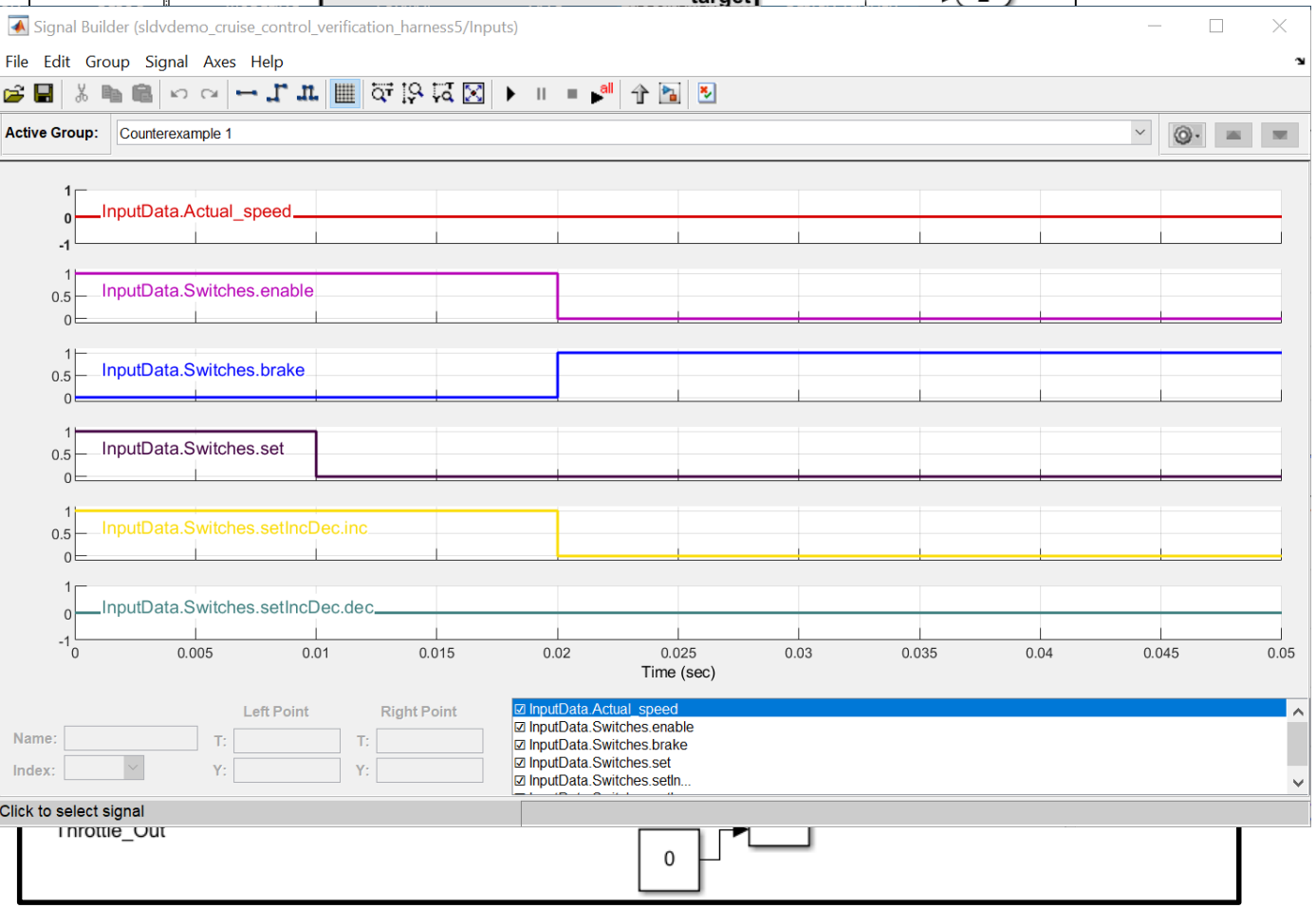
将需求与属性建立关联


sldvdemo_cruise_control_defective
throt
InBus
target
Design Model
1
InputData
1
Throttle
2
Target
Throttle_Out
in
Safety Properties

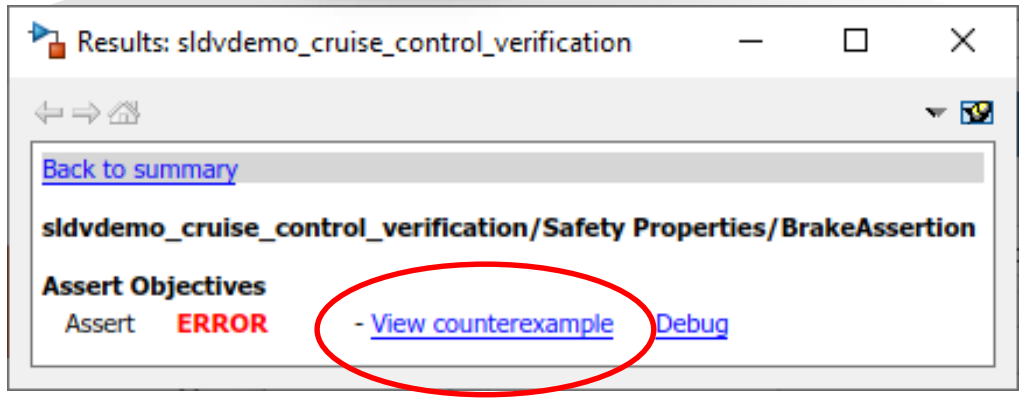

#1: Disable Throttle when Braking
When the brake is applied for three consecutive steps, the throttle shall go to zero.
VERIFIES
2
in
<brake>
[0 100]
<Actual_speed>
A
1/z
1/z
AND
A
B
A ==> B
BrakeAssertion
1
Throttle_Out
0
≤

证明设计满足需求

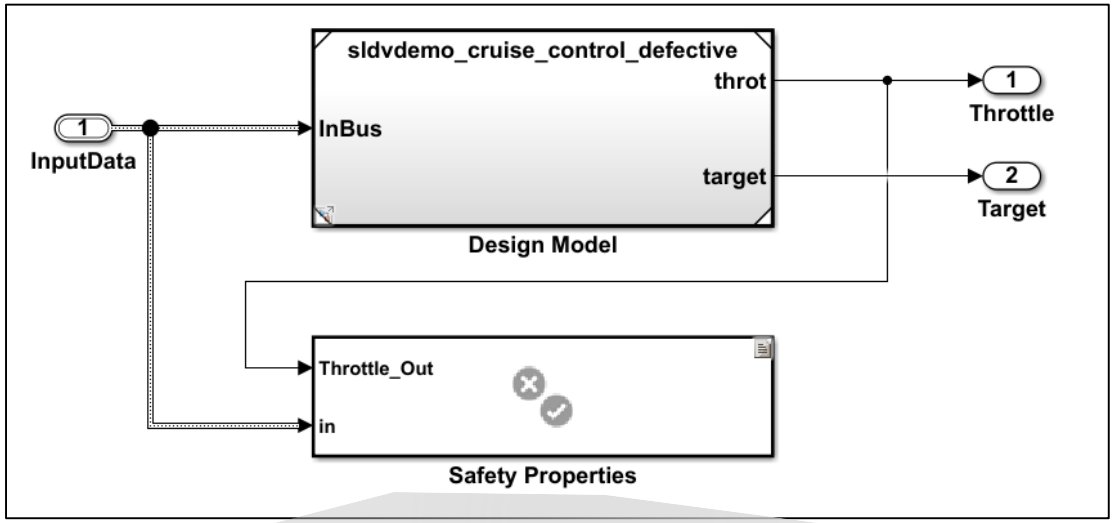

sldvdemo_cruise_control_defective
throt
InBus
target
1
InputData
1
Throttle
2

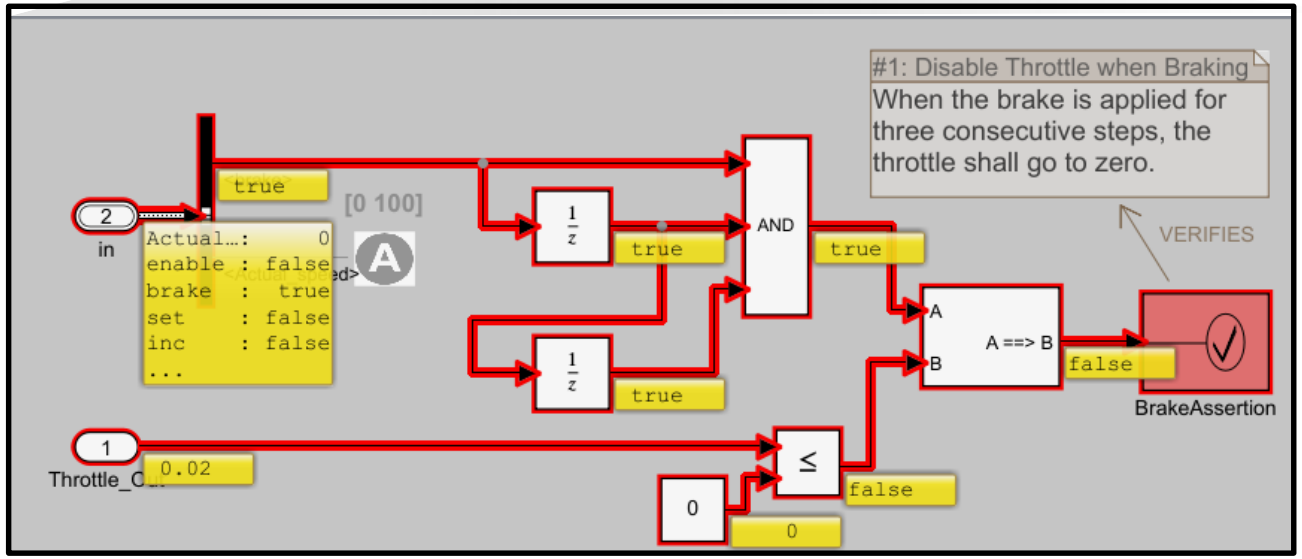

Signal Builder (sldvdemo_cruise_control_verification_harness5/Inputs)
File Edit Group Signal Axes Help
Active Group:
Counterexample 1
InputData.Actual_speed
InputData.Switches.enable
InputData.Switches.brake
InputData.Switches.set
InputData.Switches.setIncDec.inc
InputData.Switches.setIncDec.dec
Time (sec)
Left Point
Right Point
Name:
Index:
InputData.Actual_speed
InputData.Switches.enable
InputData.Switches.brake
InputData.Switches.set
InputData.Switches.setIn...
Click to select signal
Throttle_Out
0

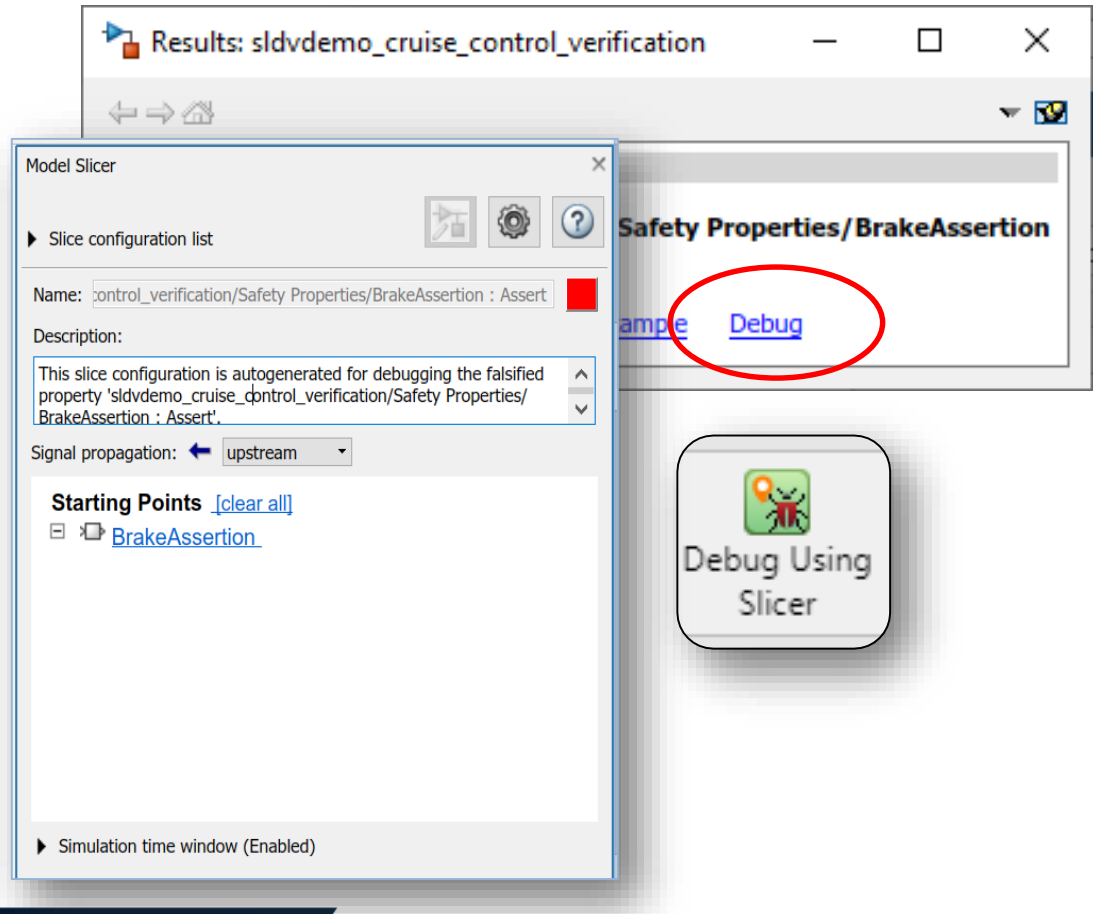

Prove
Properties


Results: sldvdemo_cruise_control_verification
Back to summary
sldvdemo_cruise_control_verification/Safety Properties/BrakeAssertion
Assert Objectives
Assert
ERROR
- View counterexample
Debug

Model Slicer 用于属性证明反例的调试







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

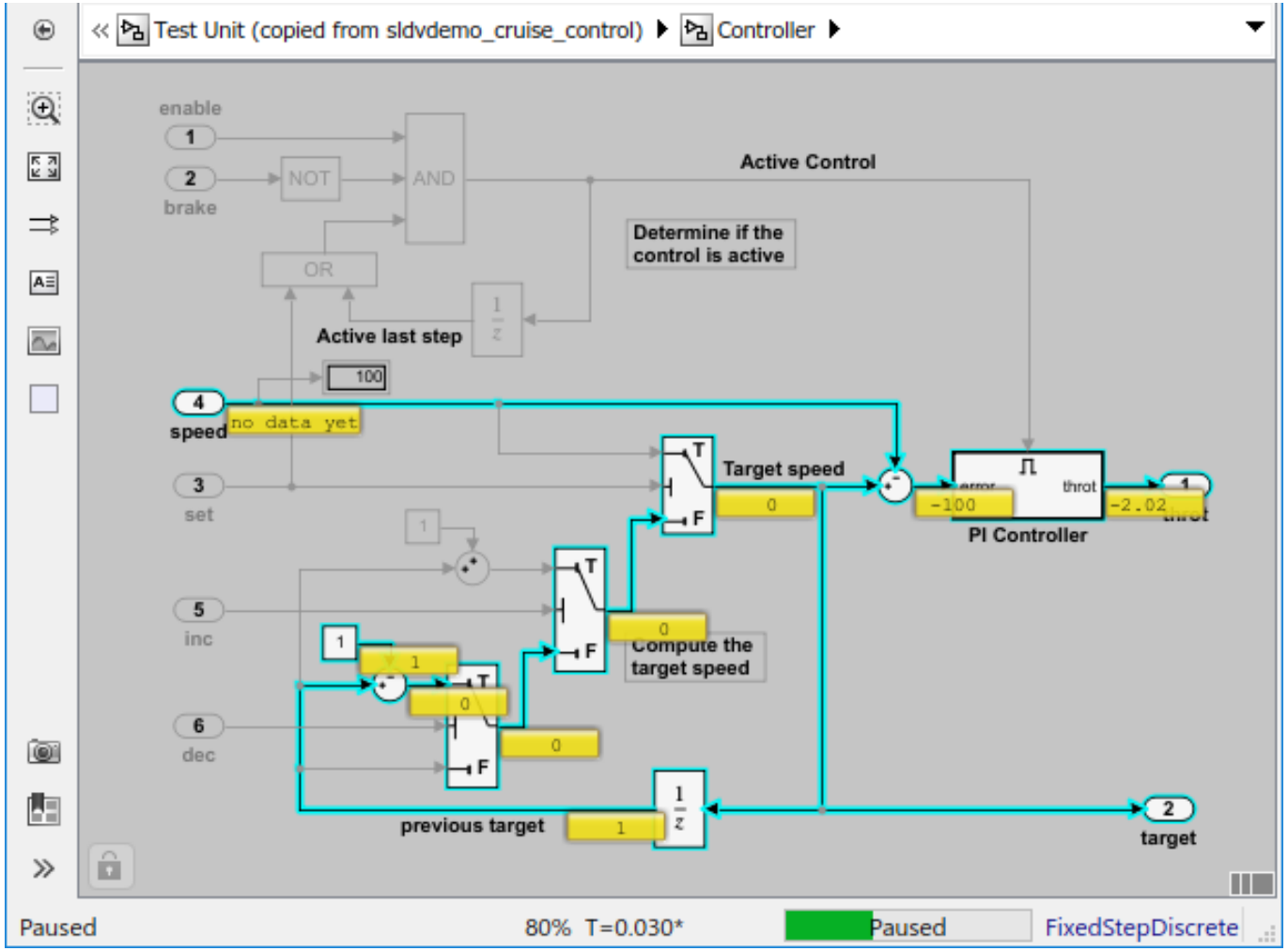
分析依赖性
理解大型、复杂模型中，数据流和控制流的依赖关系

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

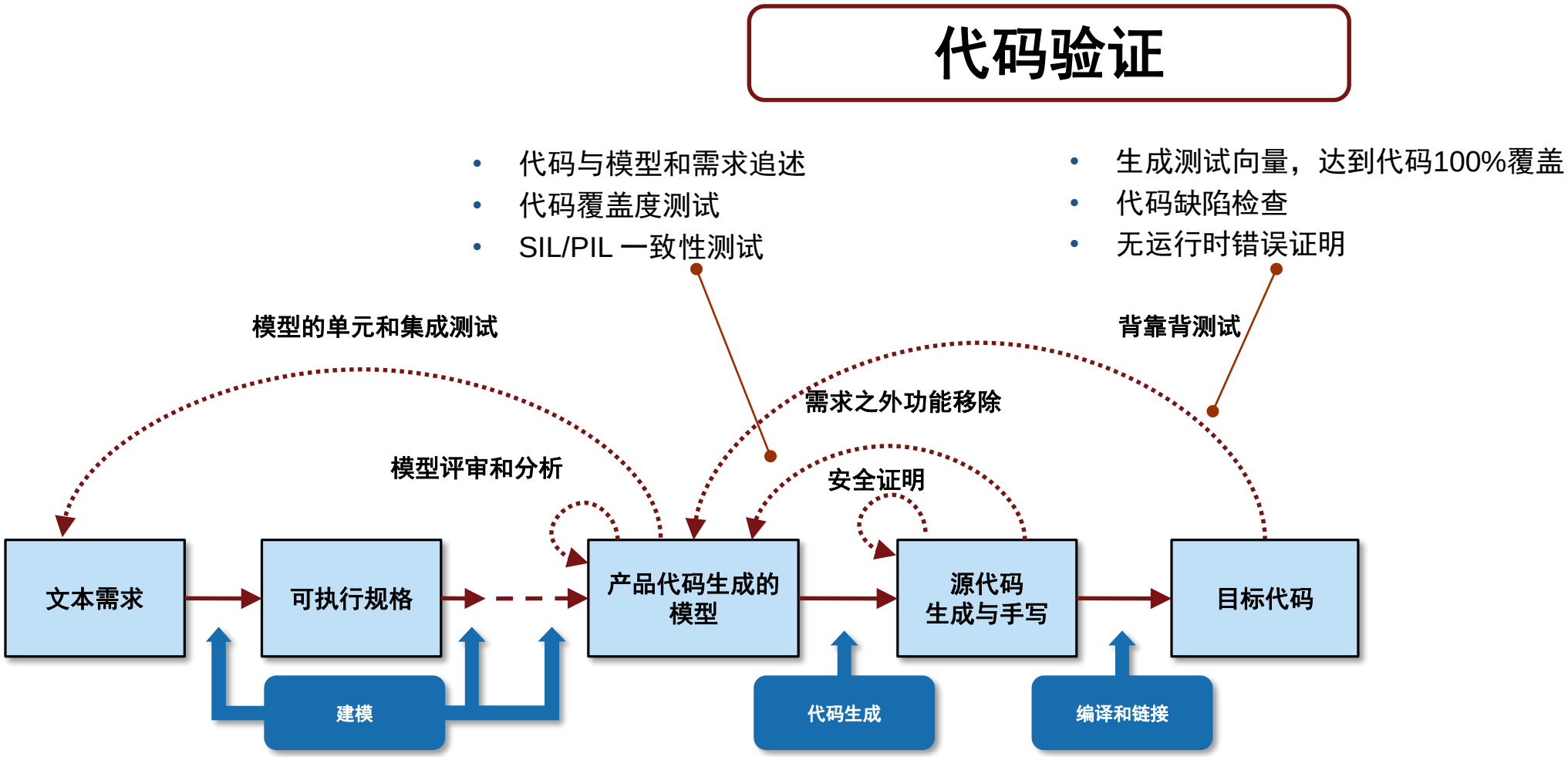
仿真行为调试
对分离的模型单步调试，理解信号、端口值及其传递关系

迭代

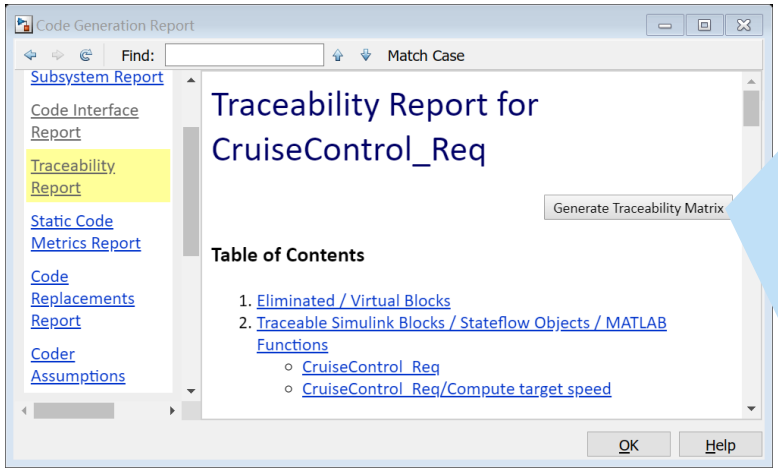
修改后的模型

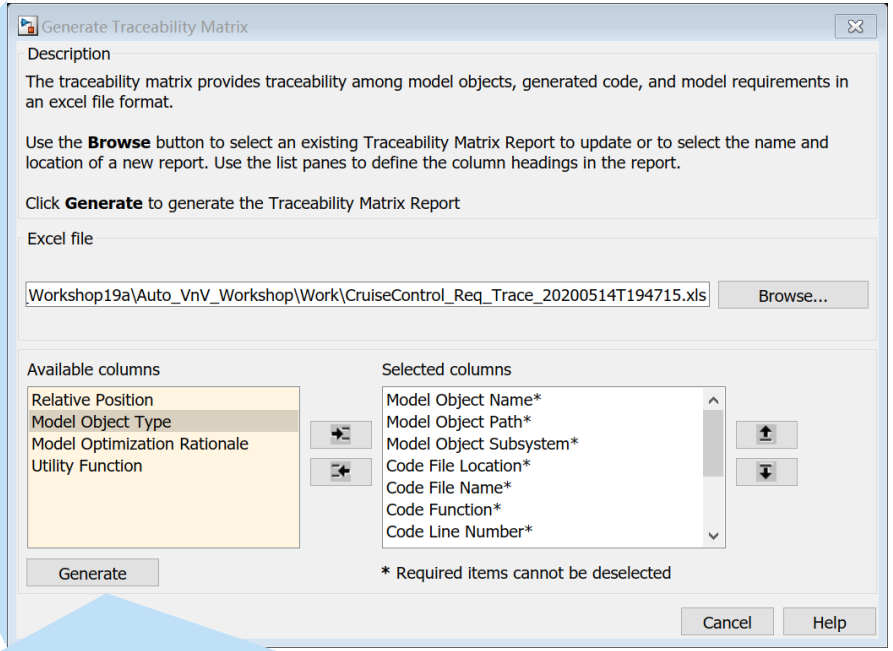


代码验证: 在代码层面提高可靠度



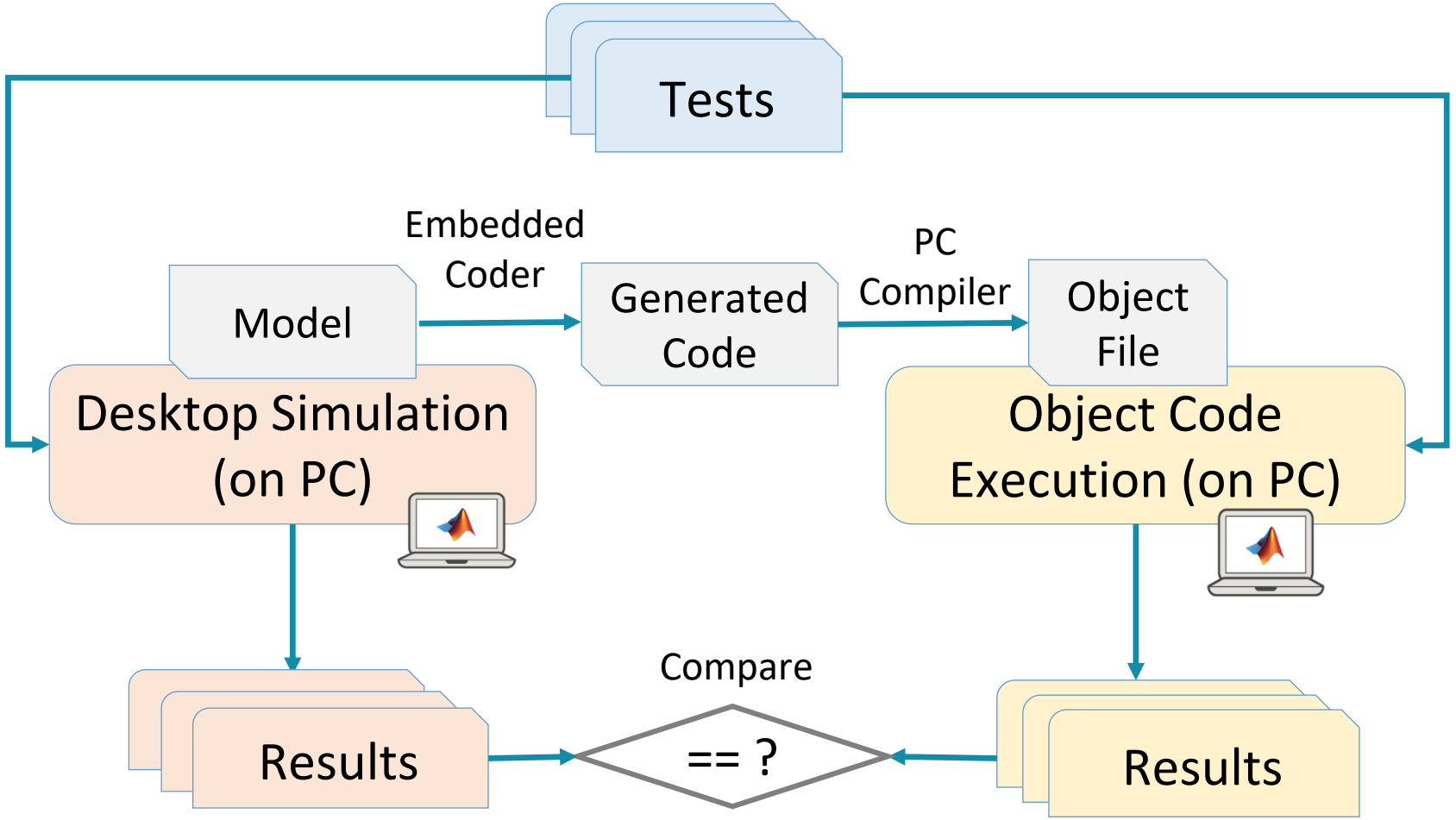
生成追溯性矩阵





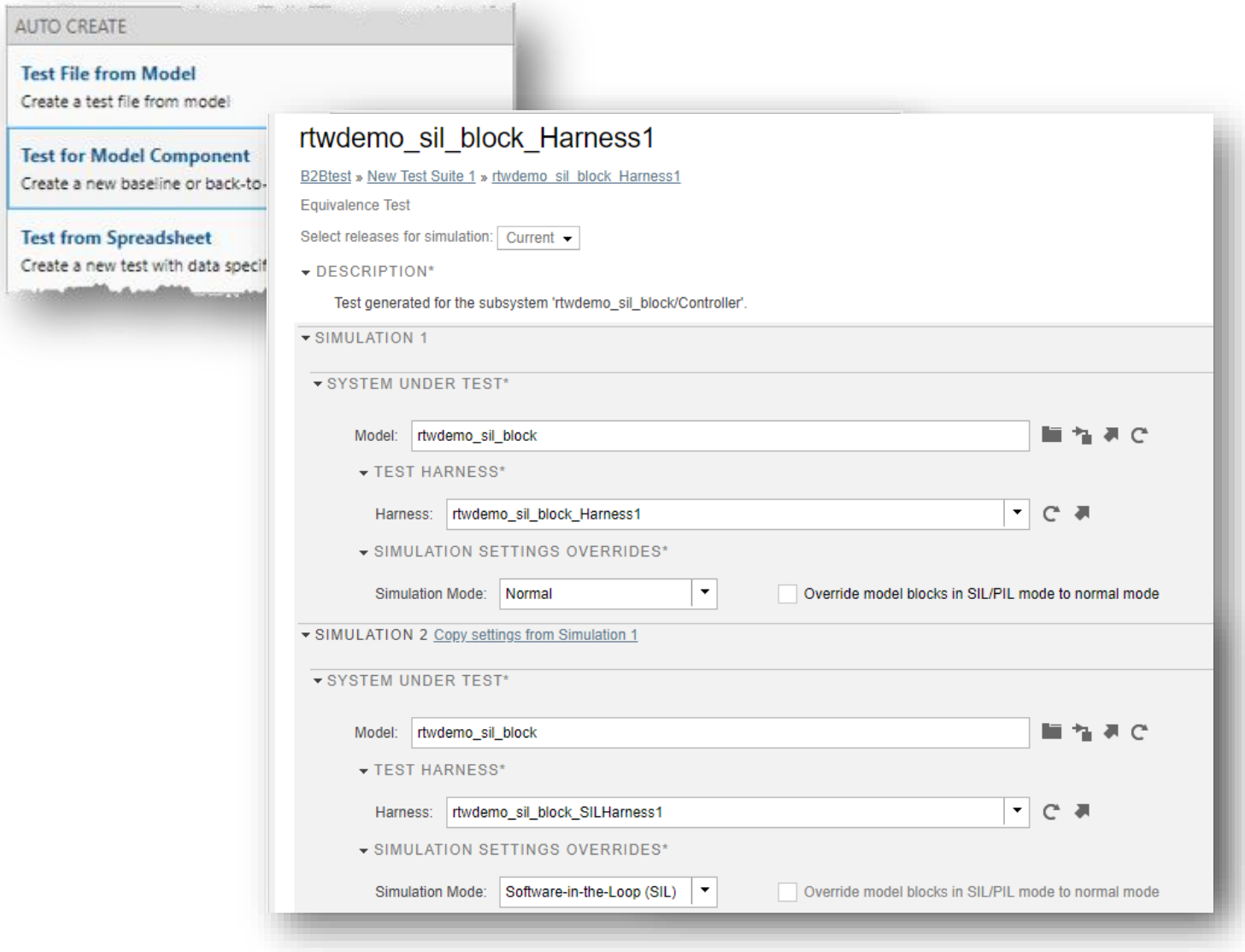
A	B	C	E	F	G	H	K	L
Model Object Name	Model Object Path	Model Object Subsystem	Code File Name	Code Function	e Line Num	Model Object Unique ID	Requirements Source	Requirements Location
CruiseOnOff	CruiseControl_Req	CruiseControl_Req	CruiseControl_Req.c	Global	42	CruiseControl_Req:26	MW_CruiseControl.slreqx	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

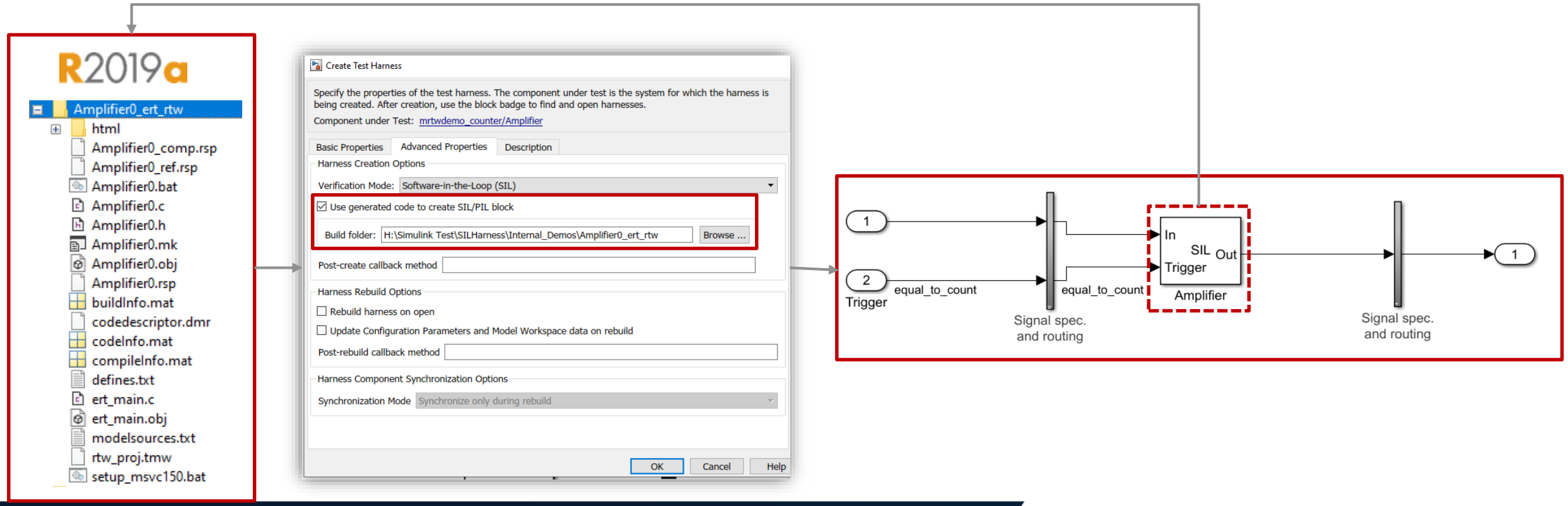


- 向导式步骤定义输入、测试类型和输出格式
- 向导式生成需要的测试框架
- 使用 Simulink Design Verifier 自动生成测试用例

支持跨版本的SIL/PIL 测试框架生成

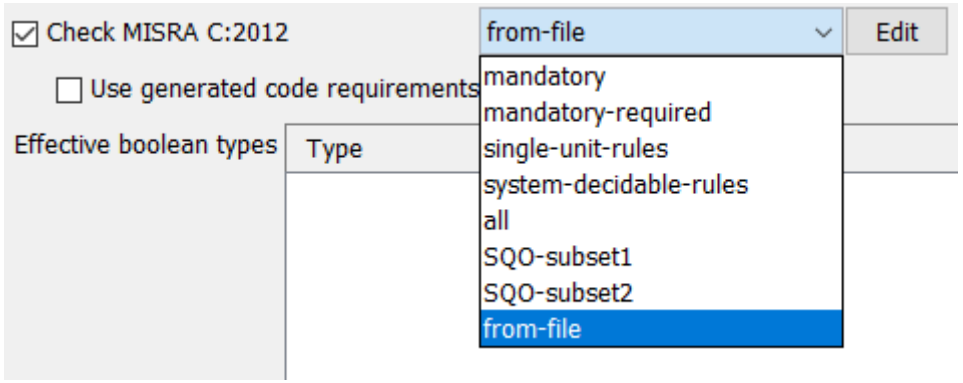
R2020a

- 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

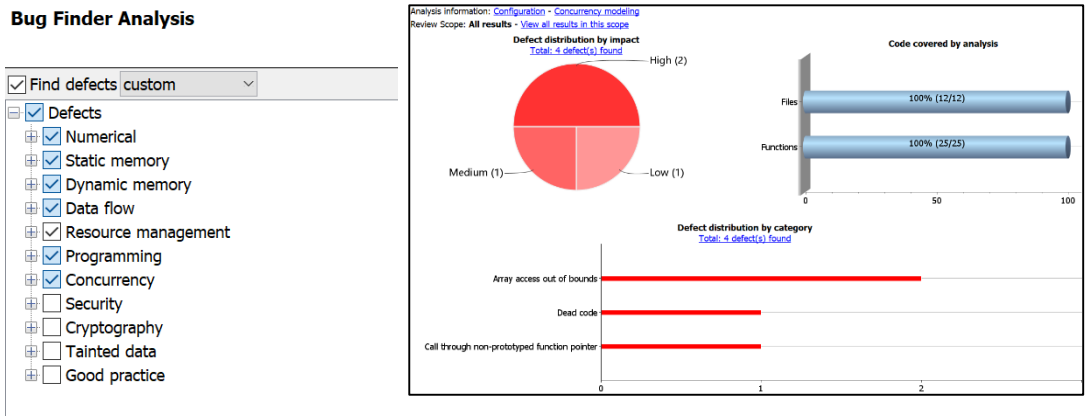


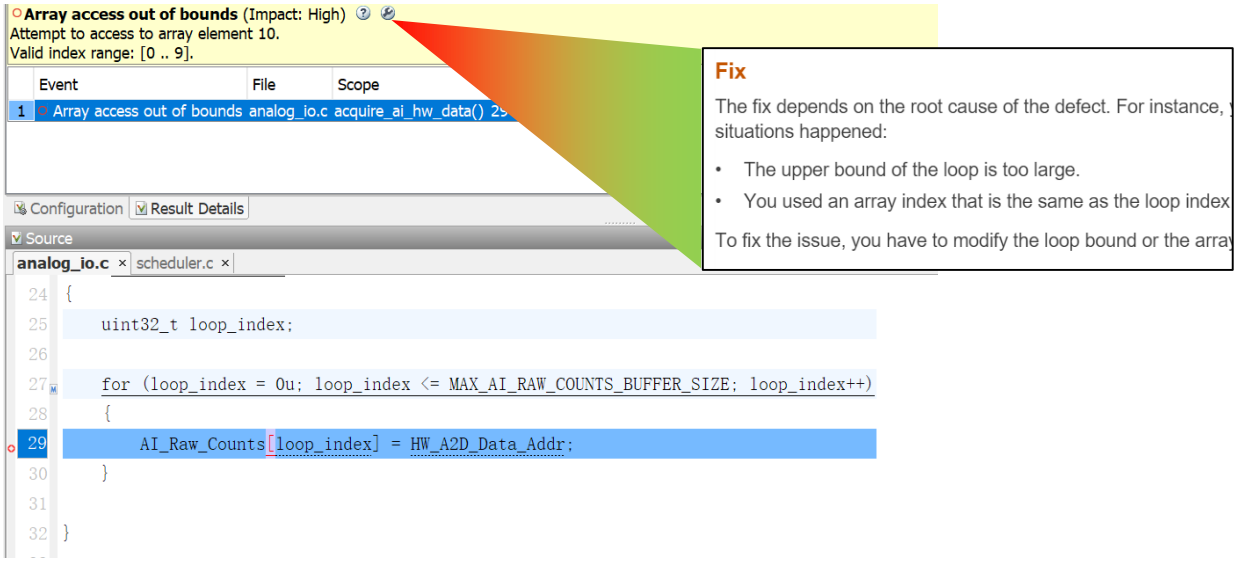
手写代码的编码规范检查

- 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





- 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

应用级分析和证明

Hand Code

MBD Gen Code

S-function Code

System Inputs

Cruise Power

Brake

Vehicle Speed

Coast/Set

Accel/Resume

Cruise Control Application

Function Scheduler

Read Inputs

Fault Logging

Write Outputs

Target Speed Control Module

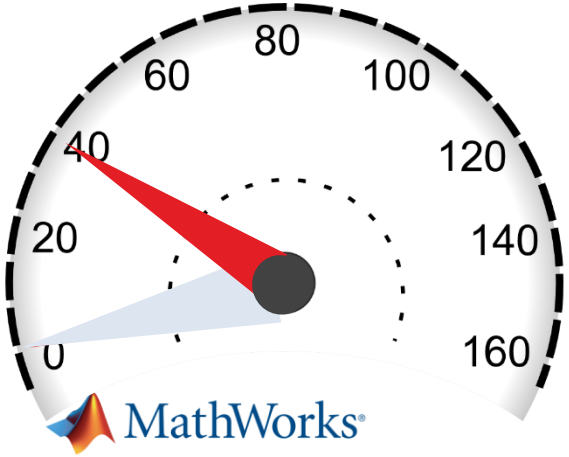
Pedal Command Control Module

System Outputs

Target Speed

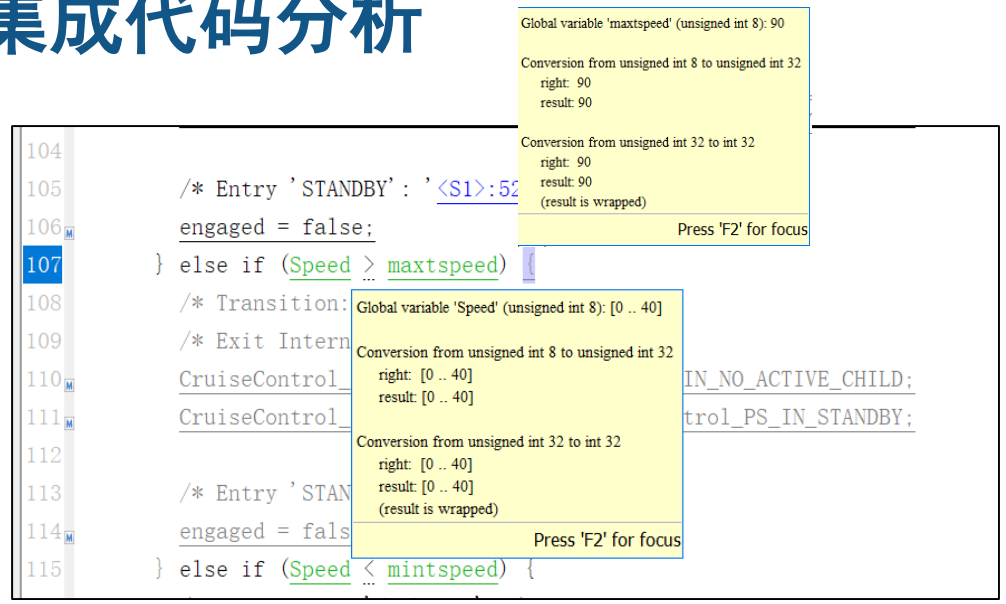
Engaged

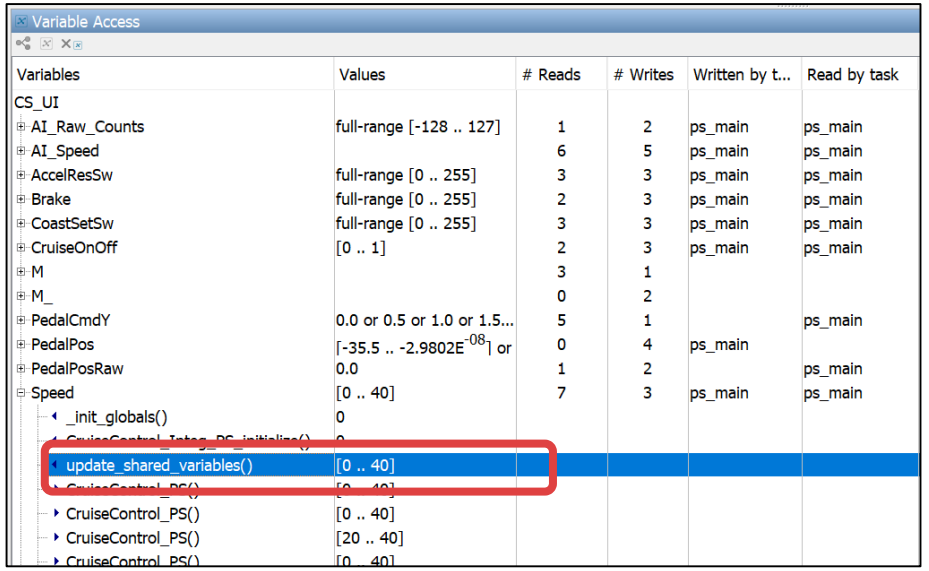
Pedal Position

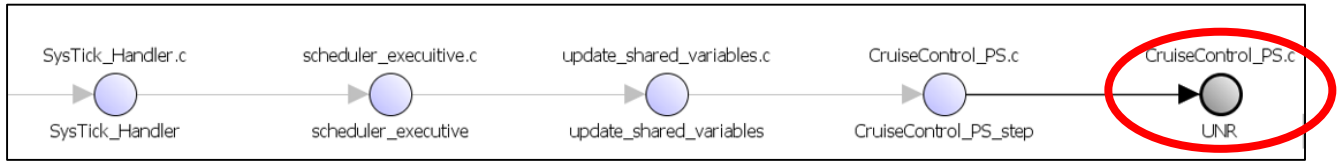


问题：目标车速从未超过 40 mph

集成代码分析







- 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 #ifdef 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
```

```
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 }
```

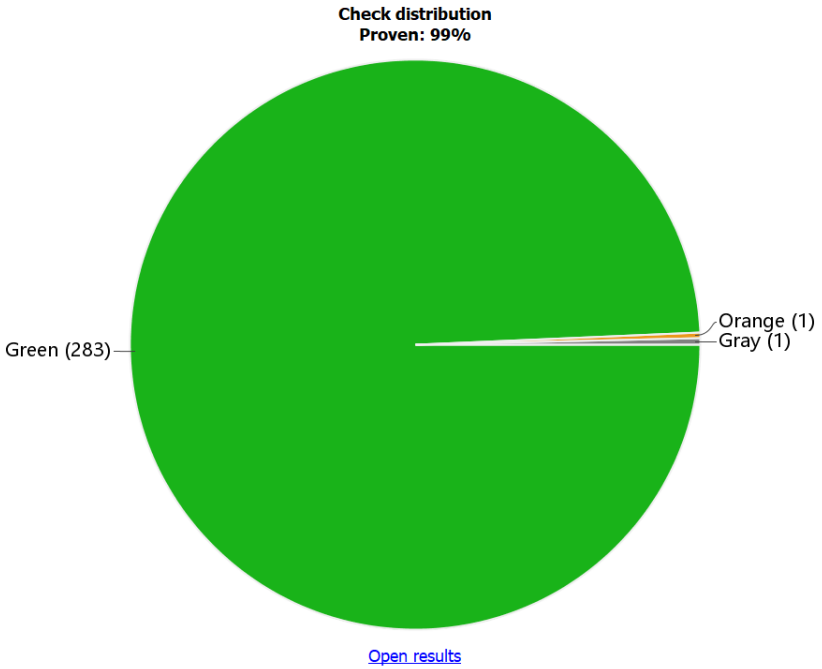
MASK – accounts for scaling down for new ADC from 14-bit to 12-bit

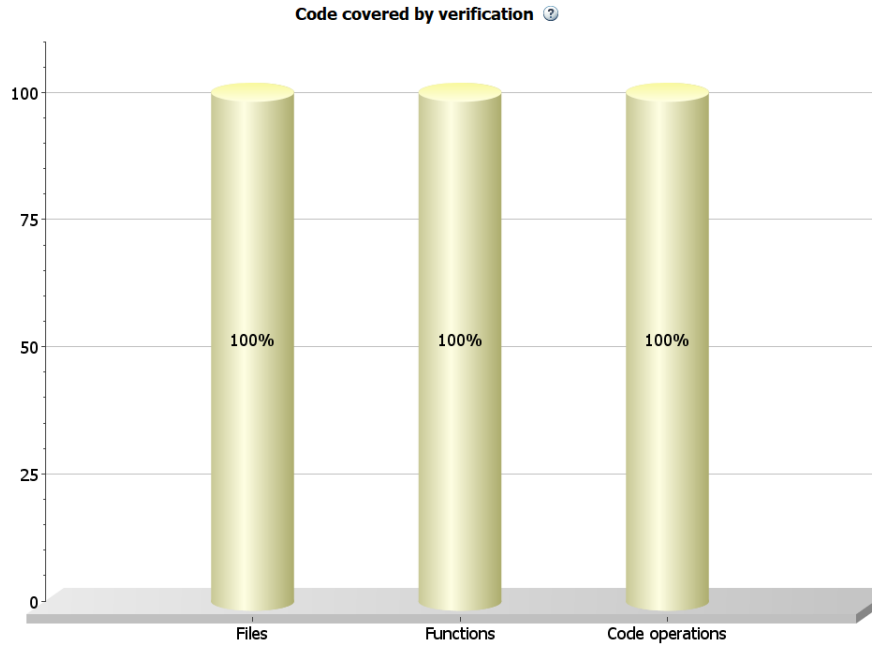
代码更改：

新的 ADC 时的 CONV_FACTOR 值

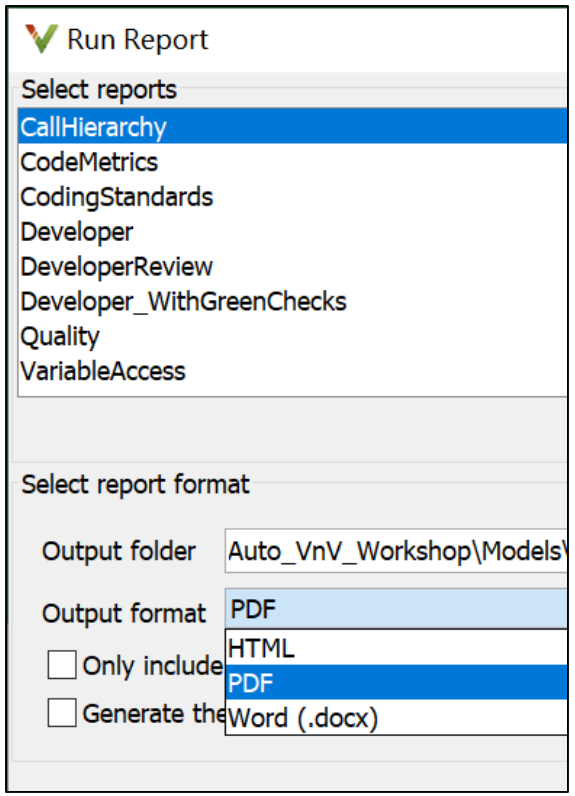
无运行时错误证明

Analysis information: Configuration - Analysis assumptions

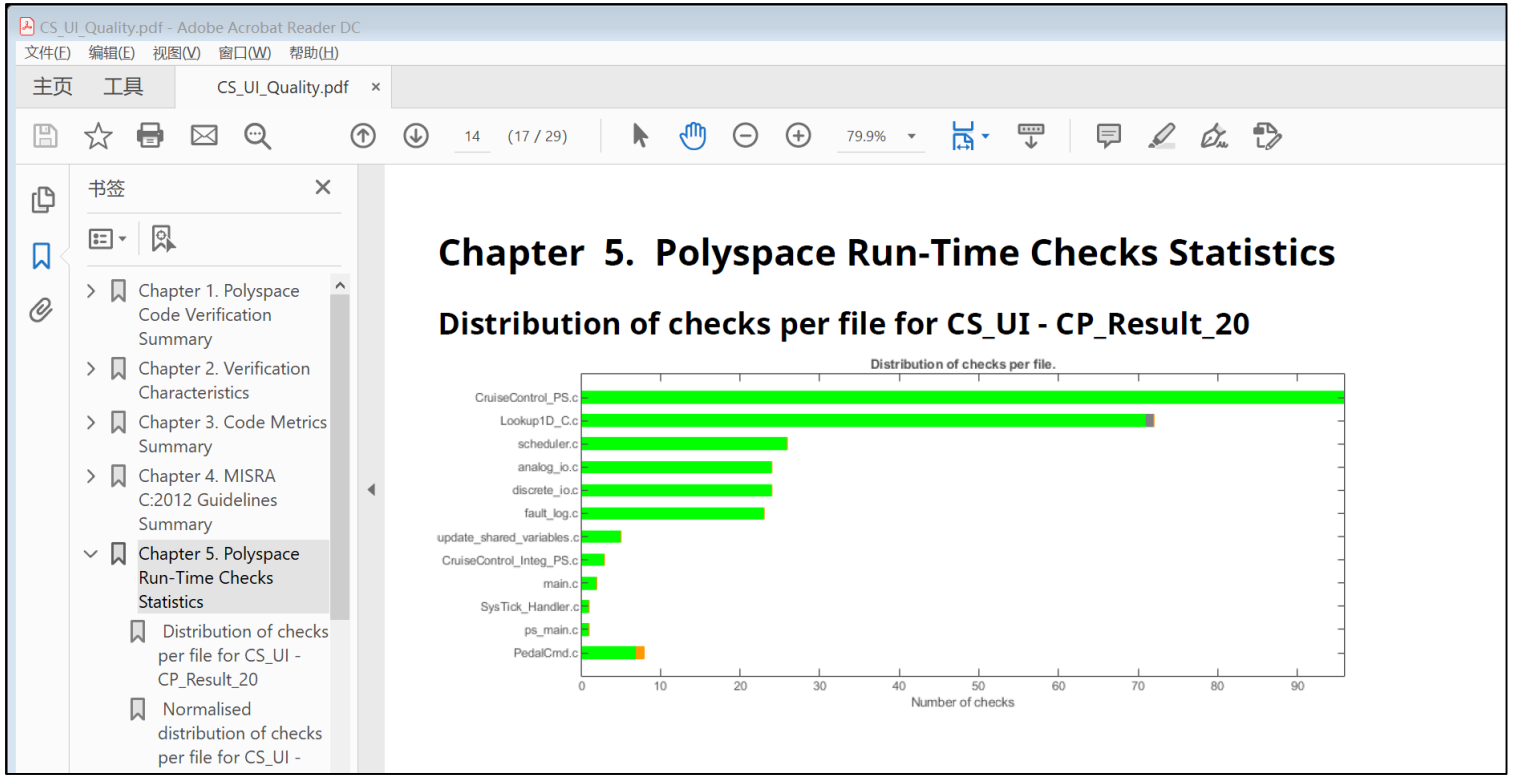




生成取证证物

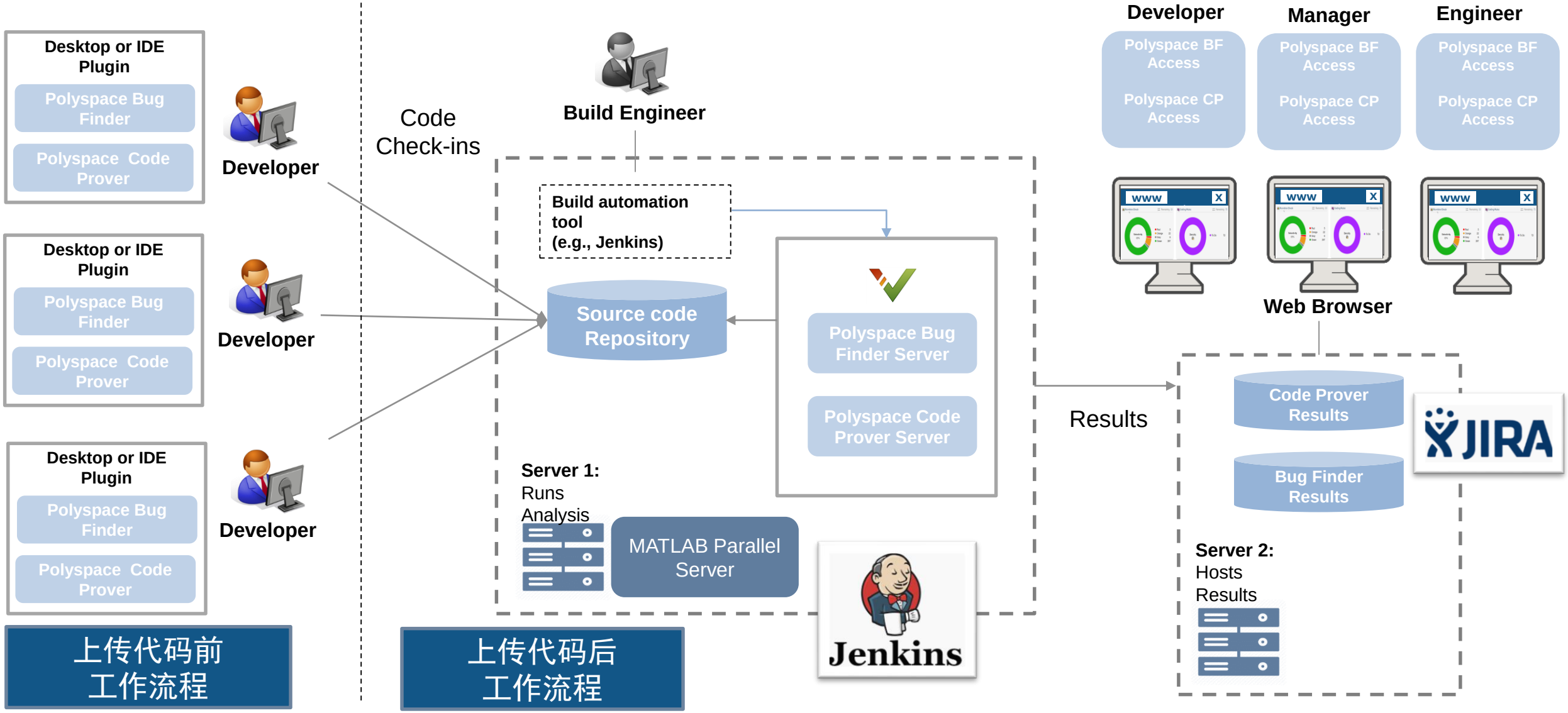


不同类型和格式报告

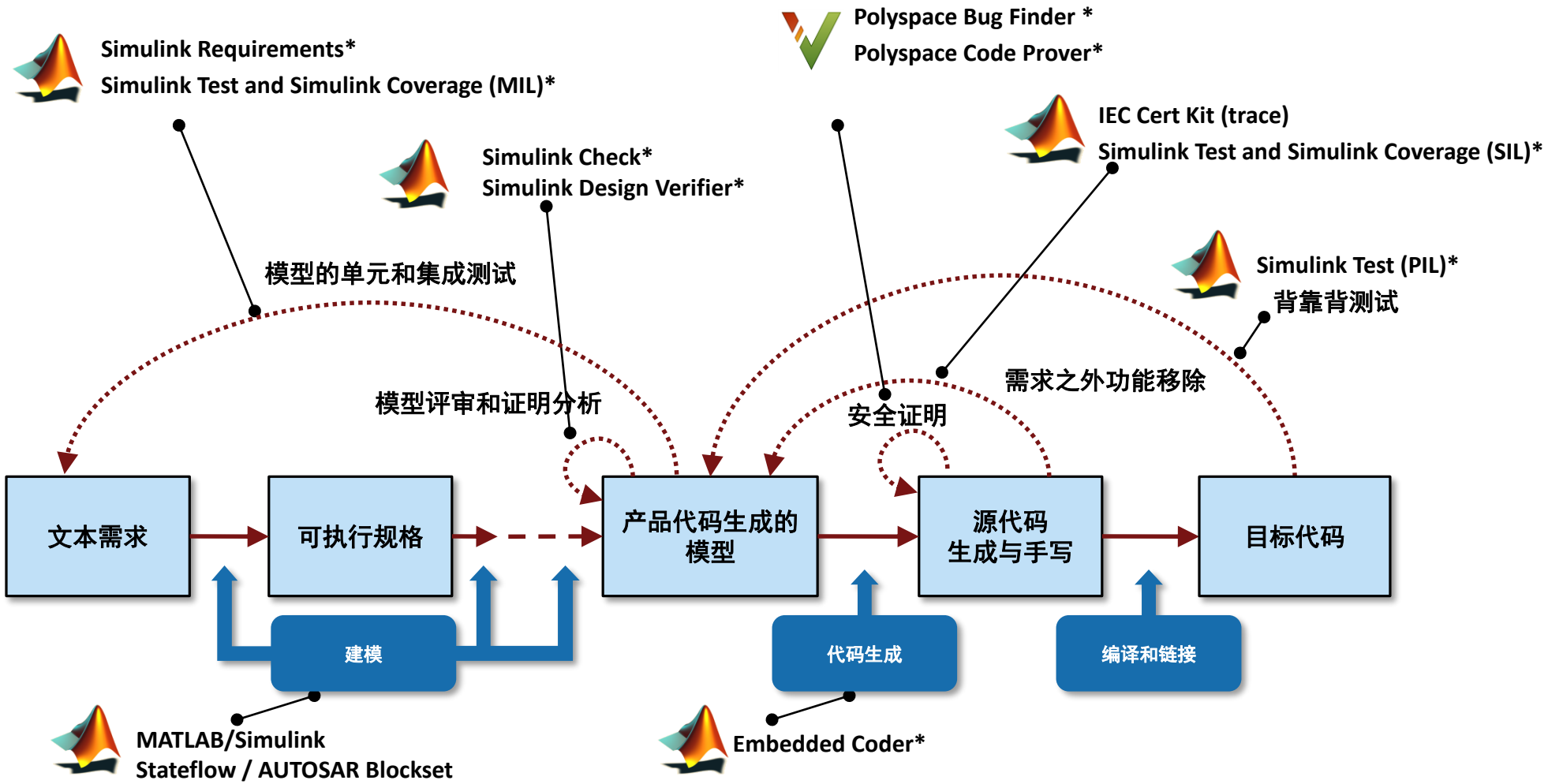


质量报告

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

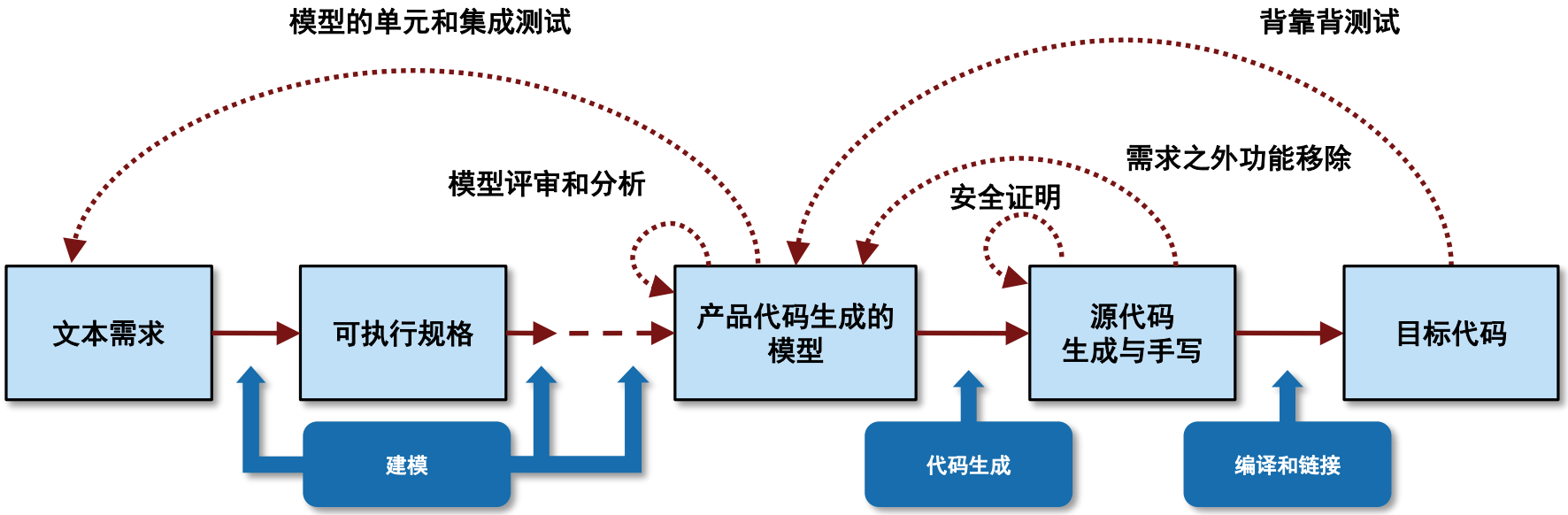
日产公司使用 Polyspace 提高软件的可靠性

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！