2020 MathWorks 中国汽车年会

从认证方和工具商角度解读A-SPICE实例

杨环宇
上海先起
樊朝祥
MathWorks中国区应用工程师

MathWorks®

Introduction

杨环宇 (Thomas Yang)

- 上海先起公司首席过程及软件顾问
- 国内最早的Automotive SPICE® 从业人员（2009年）
- 国内第三方中，中国大陆最早获取Automotive SPICE® Principal Assessor资质
- 国内唯一同时具备ASPICE最高级评估师资质及CMMI主任评估师资质的专家
- 国内较早的汽车功能安全从业人员（2012年）
- 软件工程硕士，22年从业经验（车载E/E项目开发管理、过程咨询评估）
- 丰富的CMMI-Dev, Automotive SPICE®, ISO26262项目经验

资质

- intacs™ Certified Automotive SPICE® Principal Assessor
- CMMI Institute Certified CMMI Leader Appraiser
- Functional Safety Professional
- Project Management Professional (PMP)

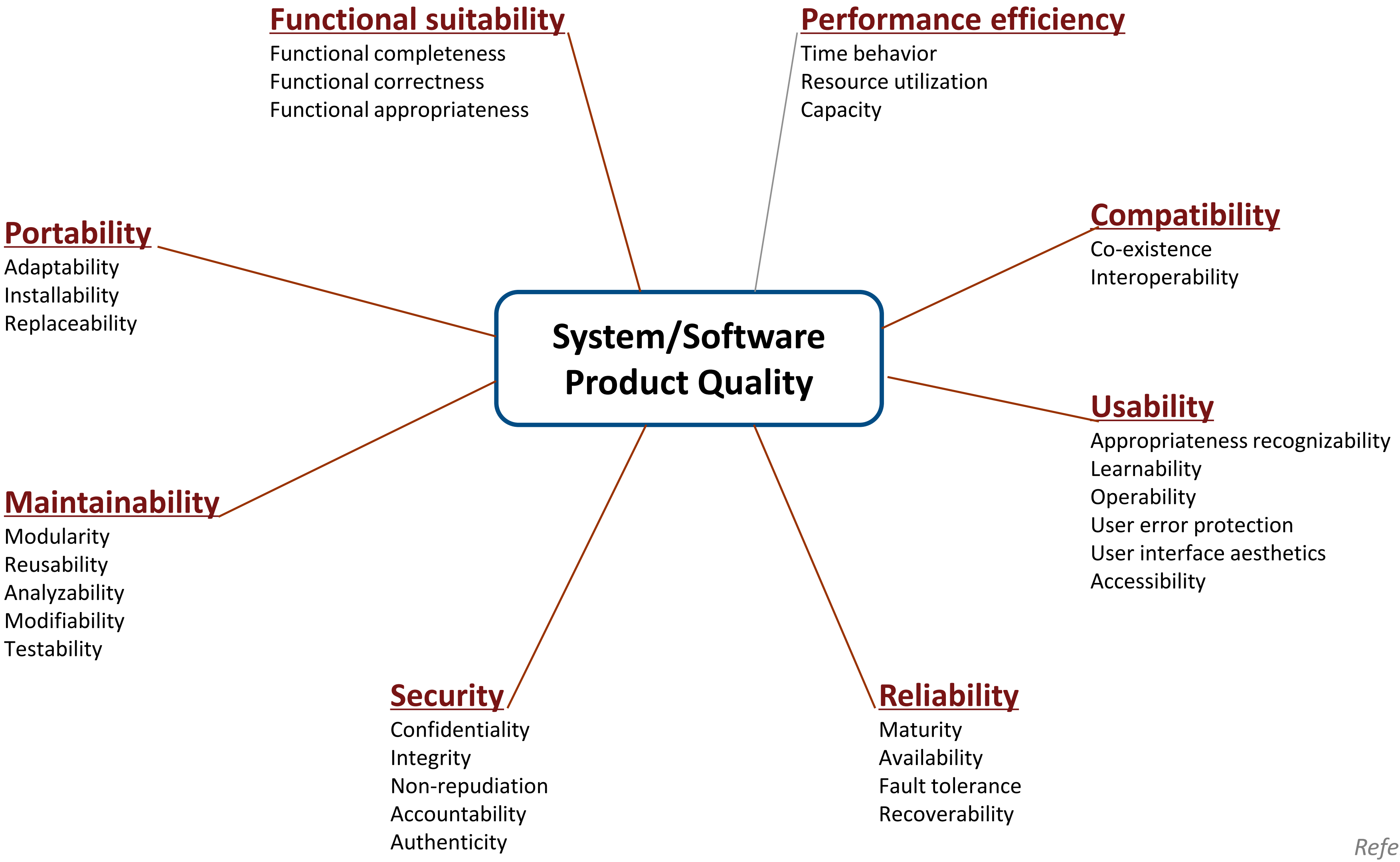
樊朝祥

- MathWorks中国应用工程师
- 10年嵌入式系统软件开发经验
- 主要负责基于模型的设计，测试验证，代码生成相关工作
- 毕业于重庆理工大学，专业方向为软件工程。
- 曾就职于Valeo，从事汽车电子嵌入式系统软件开发工作，在嵌入式系统软件开发，基于模型的设计，软件架构，软件项目管理领域有多年工作经验。

主题

- 背景介绍
- 采用MBD方法，满足ASPICE要求
  - MBD开发概述
  - 详细举例：SWE.3 软件详细设计与单元实现
  - 详细举例：SWE.4 软件单元测试

System/Software Product Quality



System/Software Product Quality

Functional suitability
Functional completeness
Functional correctness
Functional appropriateness

Performance efficiency
Time behavior
Resource utilization
Capacity

Compatibility
Co-existence
Interoperability

Usability
Appropriateness recognizability
Learnability
Operability
User error protection
User interface aesthetics
Accessibility

Reliability
Maturity
Availability
Fault tolerance
Recoverability

Security
Confidentiality
Integrity
Non-repudiation
Accountability
Authenticity

Maintainability
Modularity
Reusability
Analyzability
Modifiability
Testability

Portability
Adaptability
Installability
Replaceability

Refer from ISO/IEC 25010

Error correction costs today

Typical fault correction during:

concept phase	1	kEuro
A sample	3,5	kEuro
B sample	4	kEuro
C sample	6	kEuro
PV series	65	kEuro
0 series	80	kEuro
series	90	kEuro

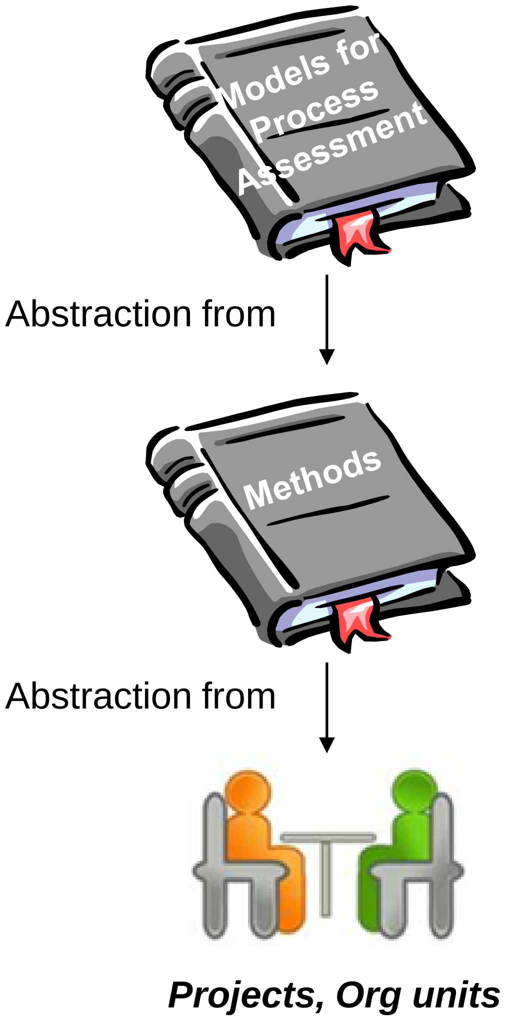
Therefore: resolve defects as early in the process as possible!

Source: HIS (Audi, BMW, Daimler, Porsche and Volkswagen), not considering vehicle modifications like flashing, commissioning etc.

Consensus: the better the processes...

- … the earlier defects are detected
- … the less systematic faults remain in the product
- … the more accurate are the plans & estimates
- … the more predictable is the organization’s performance
- … the more reusable are assets and knowledge/experience
- … the lower is the cost

Levels of abstraction of the term “process”



Projects, Org units

The “**WHAT**“ (the goals):

(What is to be done, and why, and what are the technical dependencies)

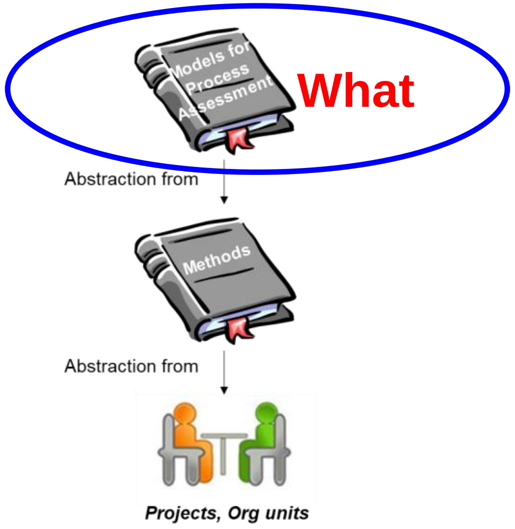
The “**HOW**“ (the way to the goals):

(Lifecycle models, tools, templates, methods, metrics, best practice, guidance, procedures, roles & skills, tailoring guidance, “interweaving“ all this to form workflows)

The “**DOING**“:

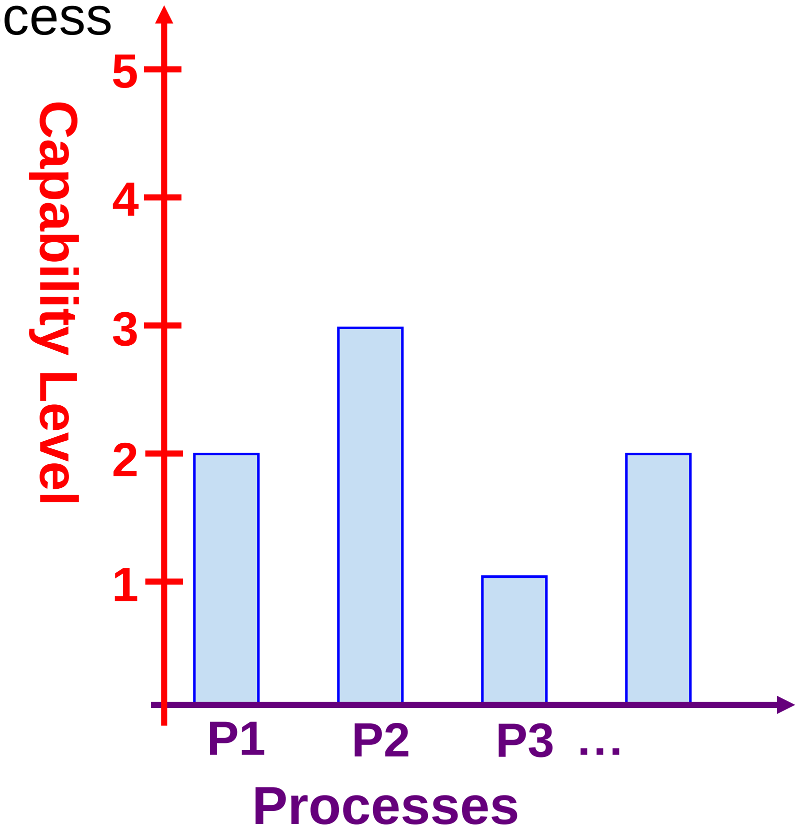
(Tailoring, set-up, and project performance according to the tailored method)

Process in “What” Level - Automotive SPICE®

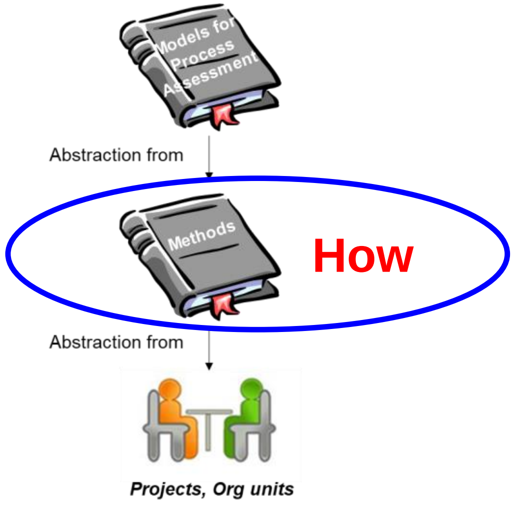


Two dimensional model for Process & Process Capability

- Process dimension
  - □ Process Categories
  - □ Processes (P1, …, Pn)
- Capability dimension
  - □ Capability Levels (CL 1 , …, CL 5)
  - □ Process Attributes

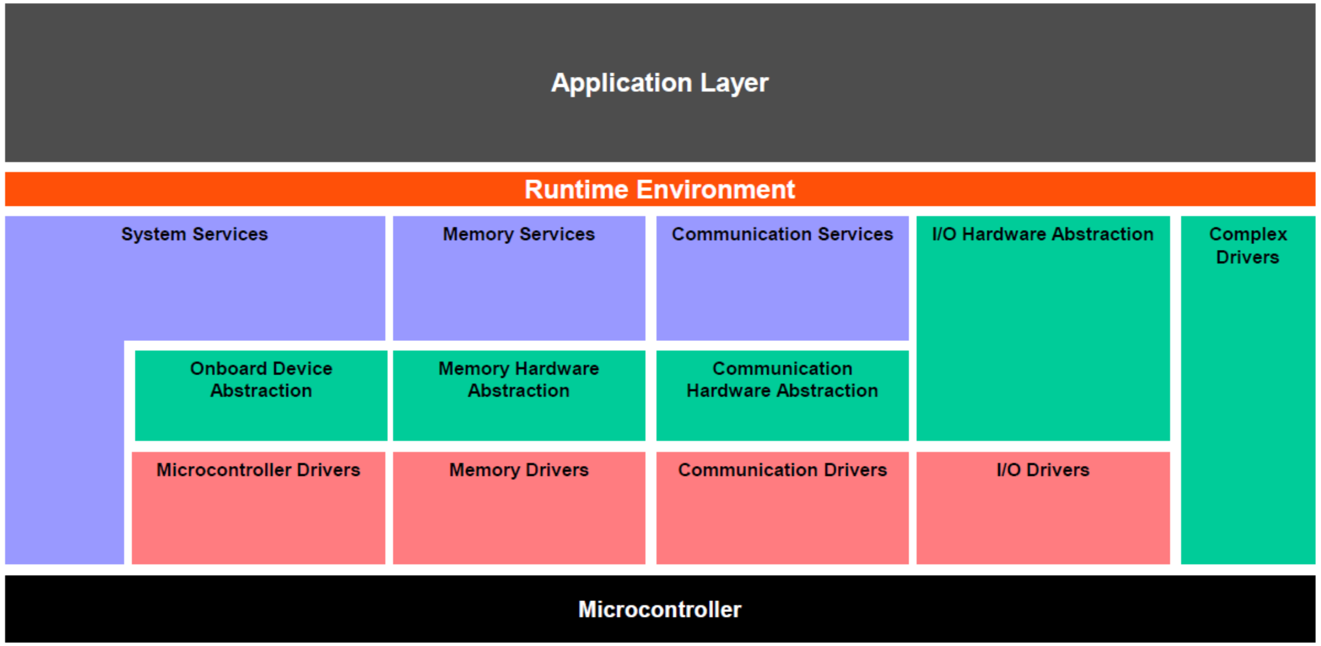


Process in “How” Level - methodology



标准化，专业化，工具化：

- AUTOSAR架构
- 基于模型开发(MBD)



Application Layer

Runtime Environment

System Services

Memory Services

Communication Services

I/O Hardware Abstraction

Complex Drivers

Onboard Device Abstraction

Memory Hardware Abstraction

Communication Hardware Abstraction

Microcontroller Drivers

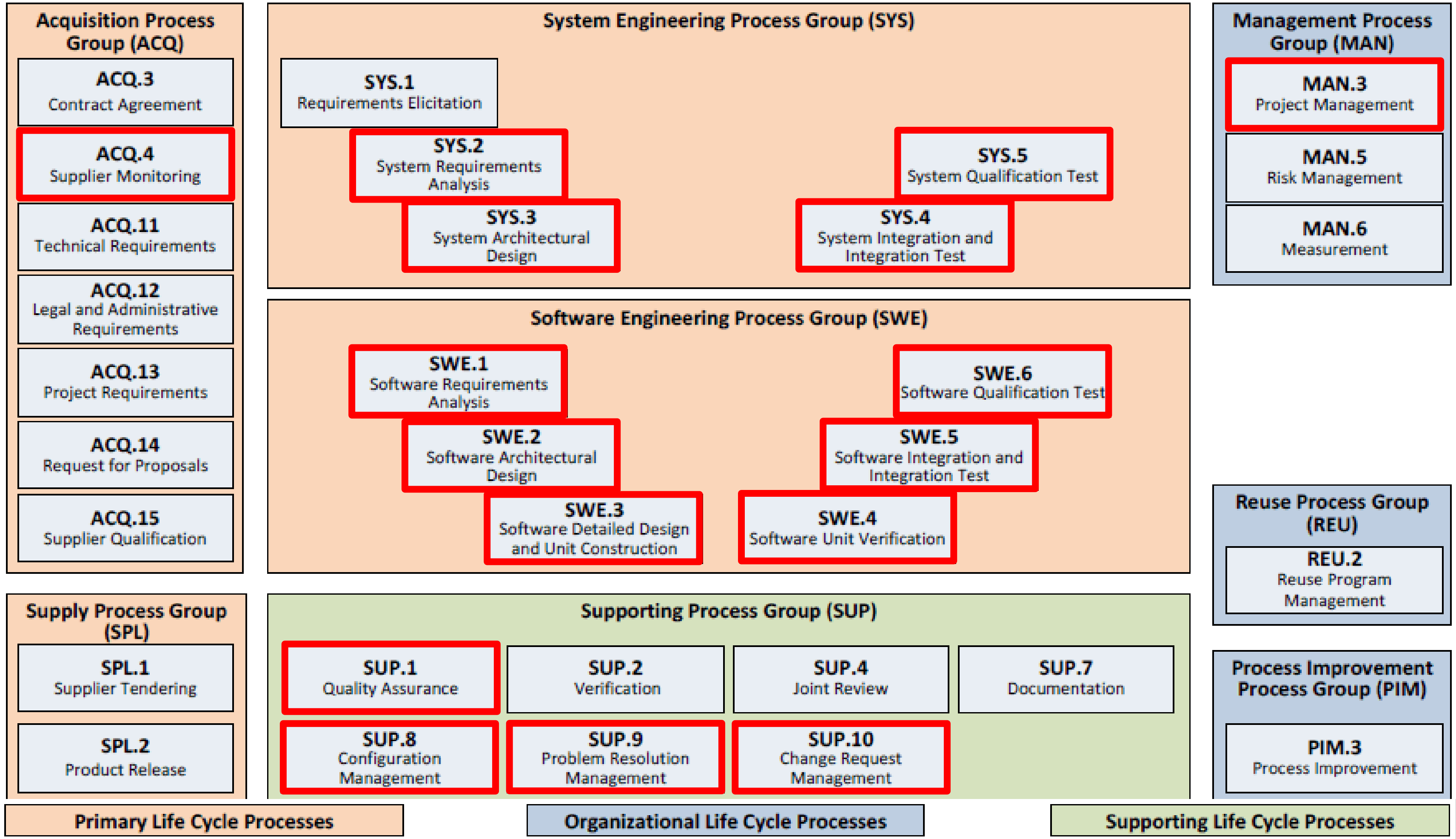
Memory Drivers

Communication Drivers

I/O Drivers

Microcontroller

Automotive SPICE® PAM and ‘VDA scope’



Acquisition Process Group (ACQ)

ACQ.3 Contract Agreement

ACQ.4 Supplier Monitoring

ACQ.11 Technical Requirements

ACQ.12 Legal and Administrative Requirements

ACQ.13 Project Requirements

ACQ.14 Request for Proposals

ACQ.15 Supplier Qualification

System Engineering Process Group (SYS)

SYS.1 Requirements Elicitation

SYS.2 System Requirements Analysis

SYS.3 System Architectural Design

SYS.4 System Integration and Integration Test

SYS.5 System Qualification Test

Management Process Group (MAN)

MAN.3 Project Management

MAN.5 Risk Management

MAN.6 Measurement

Software Engineering Process Group (SWE)

SWE.1 Software Requirements Analysis

SWE.2 Software Architectural Design

SWE.3 Software Detailed Design and Unit Construction

SWE.4 Software Unit Verification

SWE.5 Software Integration and Integration Test

SWE.6 Software Qualification Test

Reuse Process Group (REU)

REU.2 Reuse Program Management

Supply Process Group (SPL)

SPL.1 Supplier Tendering

SPL.2 Product Release

Supporting Process Group (SUP)

SUP.1 Quality Assurance

SUP.2 Verification

SUP.4 Joint Review

SUP.7 Documentation

SUP.8 Configuration Management

SUP.9 Problem Resolution Management

SUP.10 Change Request Management

Process Improvement Process Group (PIM)

PIM.3 Process Improvement

Primary Life Cycle Processes

Organizational Life Cycle Processes

Supporting Life Cycle Processes

Red frame = processes of VDA scope

主题

- 背景介绍
- 采用MBD方法，满足ASPICE要求
  - MBD开发概述
  - 详细举例：SWE.3 软件详细设计与单元实现
  - 详细举例：SWE.4 软件单元测试

MBD可用于满足A-SPICE要求

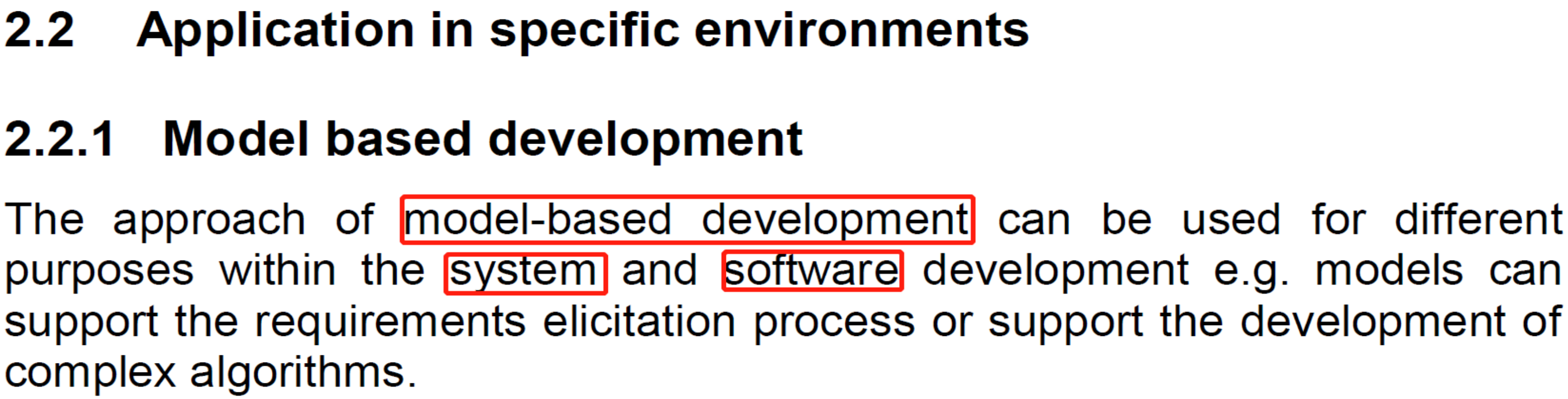
VDA Verband der Automobilindustrie

Joint Quality Management in the Supply Chain

Automotive SPICE®

- Guidelines

Process assessment using Automotive SPICE in the development of software-based systems



2.2 Application in specific environments

2.2.1 Model based development

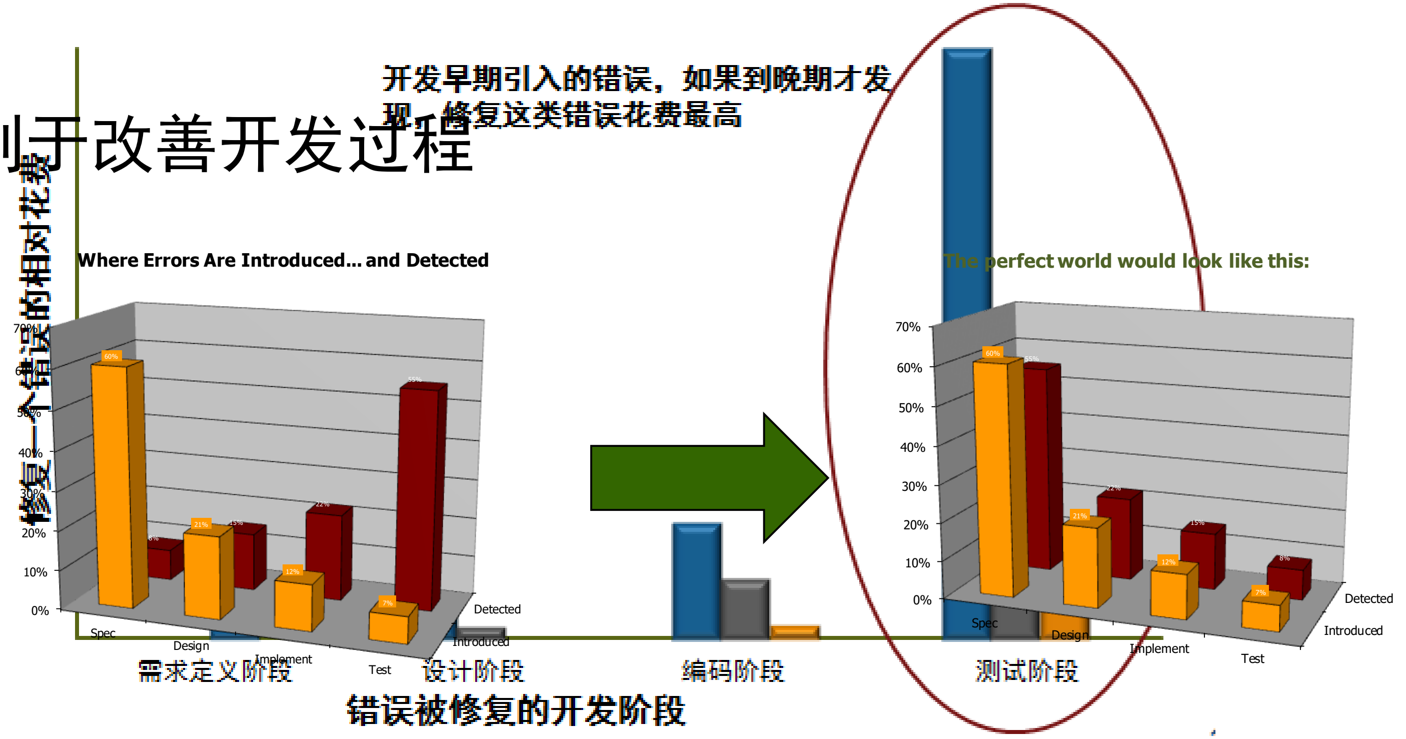
The approach of model-based development can be used for different purposes within the system and software development e.g. models can support the requirements elicitation process or support the development of complex algorithms.

早期验证

- 早期引入的错误晚期发现增加修复成本

软件开发过程中修复错误费用示意

- 早期验证有利于改善开发过程



开发早期引入的错误，如果到晚期才发现，修复这类错误花费最高

基于模型设计的优势

图形化设计

- 简洁、明确
- 便于交流
- 便于维护

早期验证

- 及早纠错
- 改善开发过程

代码自动生成

- 开发效率
- 代码品质

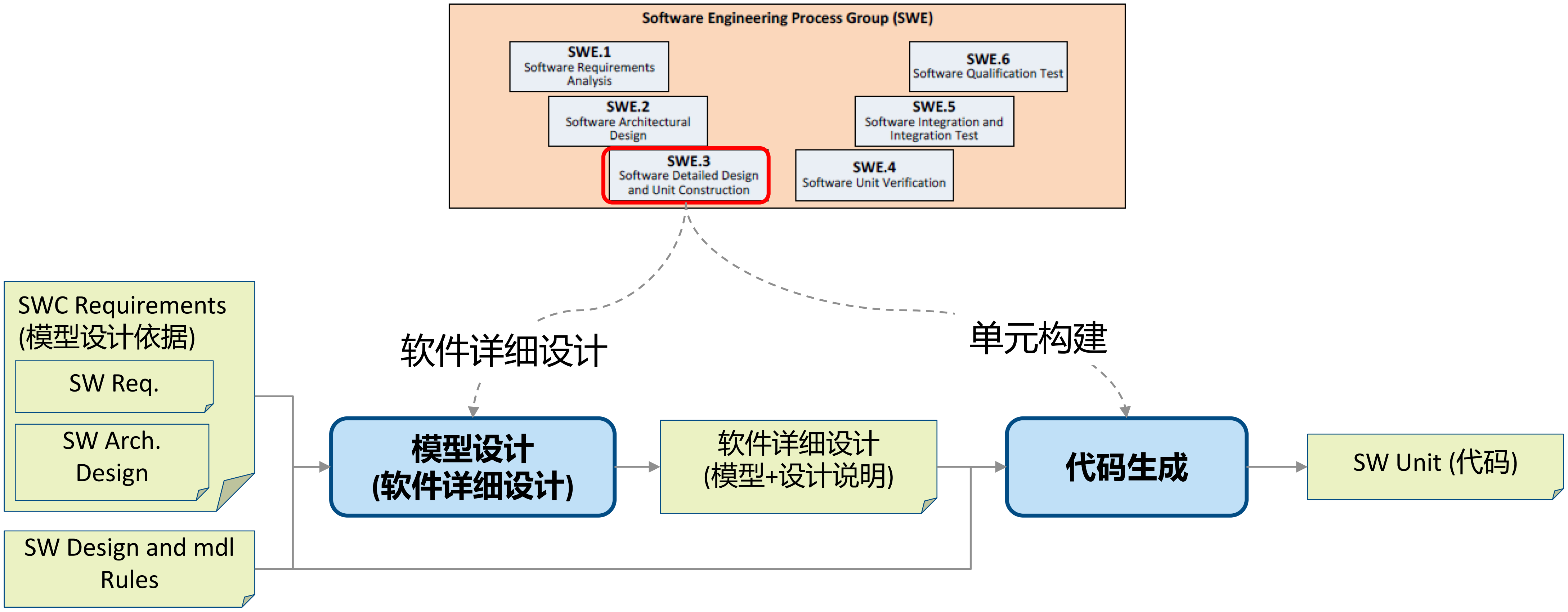
文档自动化

- 提高效率
- 便于交流
- 改善开发过程

主题

- 背景介绍
- 采用MBD方法，满足ASPICE要求
  - MBD开发概述
  - 详细举例：SWE.3 软件详细设计与单元实现
  - 详细举例：SWE.4 软件单元测试

SWE.3 软件详细设计与单元构建概述(1)



Software Engineering Process Group (SWE)

SWE.1 Software Requirements Analysis

SWE.2 Software Architectural Design

SWE.3 Software Detailed Design and Unit Construction

SWE.4 Software Unit Verification

SWE.5 Software Integration and Integration Test

SWE.6 Software Qualification Test

软件详细设计

单元构建

SWC Requirements (模型设计依据)

SW Req.

SW Arch. Design

SW Design and mdl Rules

模型设计 (软件详细设计)

软件详细设计 (模型+设计说明)

代码生成

SW Unit (代码)

SWE.3 软件详细设计与单元构建概述(2)

- 为每个SWC开发详细设计，设计模型
  - 使用Simulink, Stateflow等
  - 考虑该SWC需要满足的功能性需求和非功能性需求(SWC Req., Design Rules)
  - 通过simulation，评价设计/算法的正确性
  - 通过Model-Advisor Checks，确保满足automotive行业相关准则（如：MAAB, MISRA, ISO26262等)

- 记录相关的设计理由
  - 通过Text形式，在模型上记录设计理由(思路)
  - 建立模型block与之相关的SWC Req.(设计依据)之间的追溯性

SWE.3 基本实践与输出

SWE.3 – 基本实践(BP)

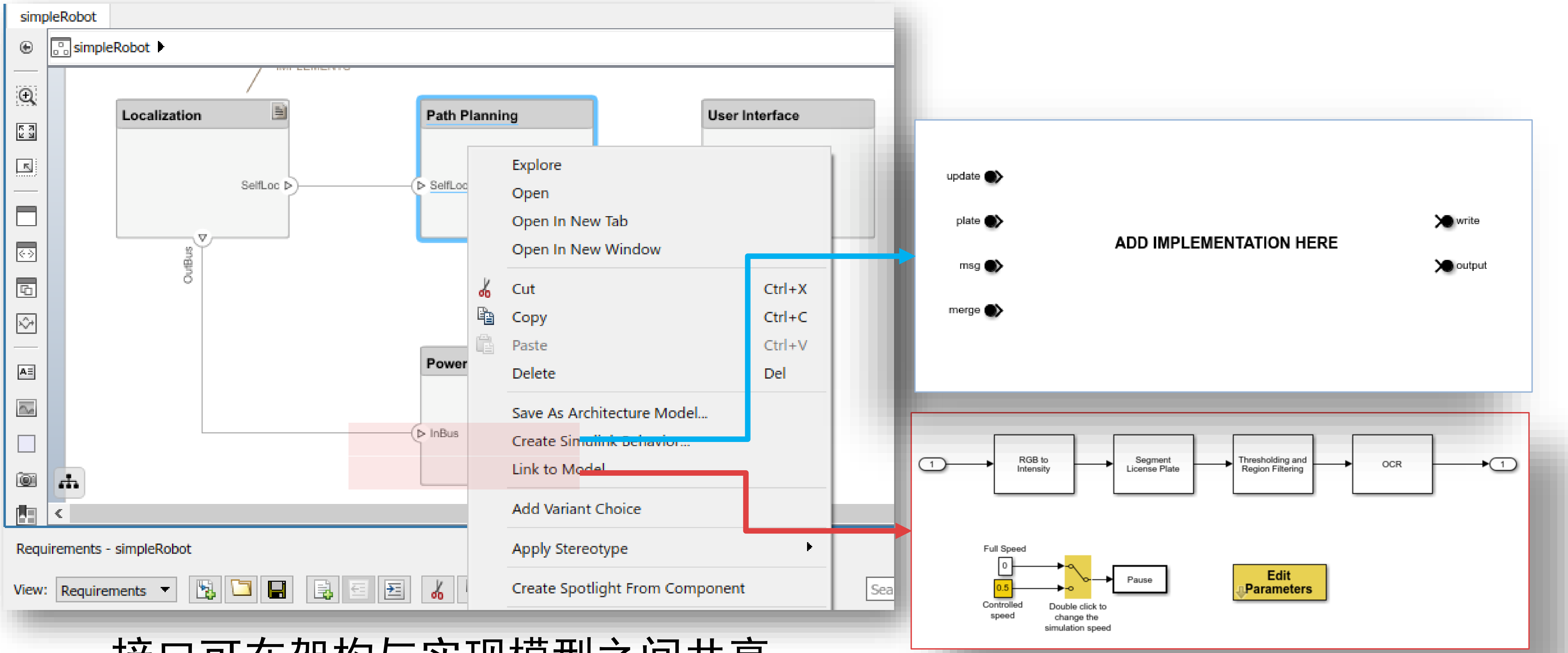
- SWE.3.BP1: 开发软件详细设计
- SWE.3.BP2: 定义软件单元接口
- SWE.3.BP3: 描述动态行为
- SWE.3.BP4: 评估软件详细设计
- SWE.3.BP5: 建立双向追溯性
- SWE.3.BP6: 确保一致性
- SWE.3.BP7: 沟通达成一致的软件详细设计
- SWE.3.BP8: 构建软件单元

实施SWE.3过程的结果如下

- 开发了描述软件单元的详细设计
- 定义了各软件单元的接口
- 定义了软件单元的动态行为
- 建立了双向追溯性和一致性：
  - 软件需求与软件单元之间
  - 软件架构设计与软件详细设计之间
  - 软件详细设计与软件单元之间
- 构建了软件详细设计所定义的软件单元

Model-Based Design and Automotive SPICE

SWE.3.BP1: 开发软件详细设计 – 与架构追溯

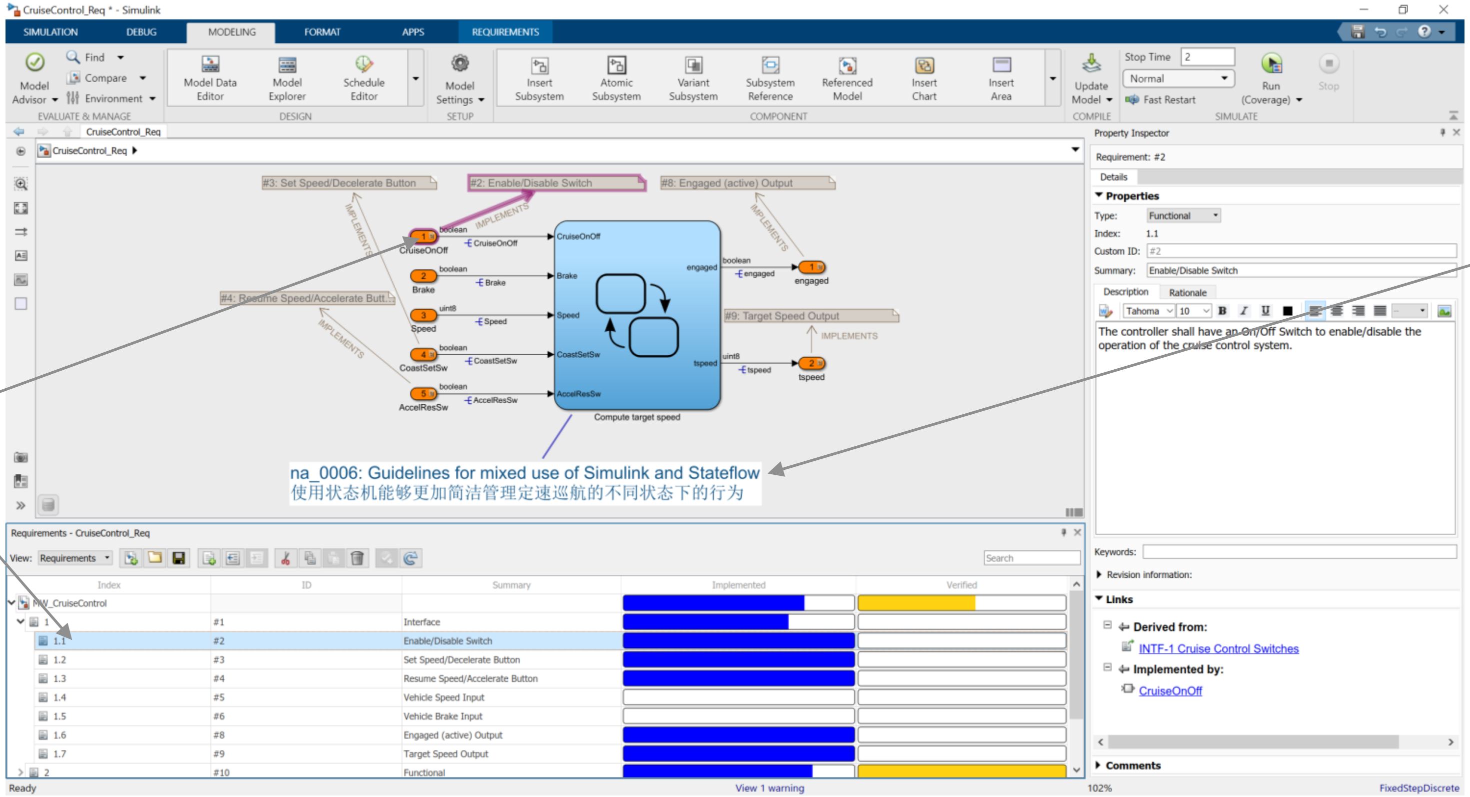


接口可在架构与实现模型之间共享

Model-Based Design and Automotive SPICE

SWE.3.BP1: 开发软件详细设计 – 需求实现与追溯

双向追溯
需求可以从
外部环境
Doors,
Excel,
Word
导入



na_0006: Guidelines for mixed use of Simulink and Stateflow
使用状态机能够更加简洁管理定速巡航的不同状态下的行为

Requirements - CruiseControl_Req

View: Requirements

Index	ID	Summary	Implemented	Verified
MW_CruiseControl			🟦	🟨
1	#1	Interface	🟦	
1.1	#2	Enable/Disable Switch	🟦	
1.2	#3	Set Speed/Decelerate Button	🟦	
1.3	#4	Resume Speed/Accelerate Button	🟦	
1.4	#5	Vehicle Speed Input		
1.5	#6	Vehicle Brake Input		
1.6	#8	Engaged (active) Output	🟦	
1.7	#9	Target Speed Output	🟦	
2	#10	Functional	🟦	🟨

Ready View 1 warning 102% FixedStepDiscrete

Property Inspector

Requirement: #2

Details

Properties

Type: Functional
Index: 1.1
Custom ID: #2
Summary: Enable/Disable Switch

Description | Rationale

The controller shall have an On/Off Switch to enable/disable the operation of the cruise control system.

Keywords:

Revision information:

Links

Derived from:
INTF-1 Cruise Control Switches

Implemented by:
CruiseOnOff

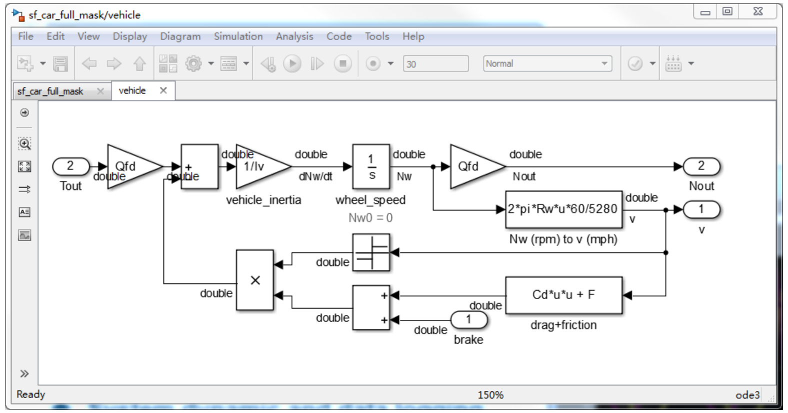
Comments

非功能性需求，
设计选择
可以以备注的形式
添加到模型

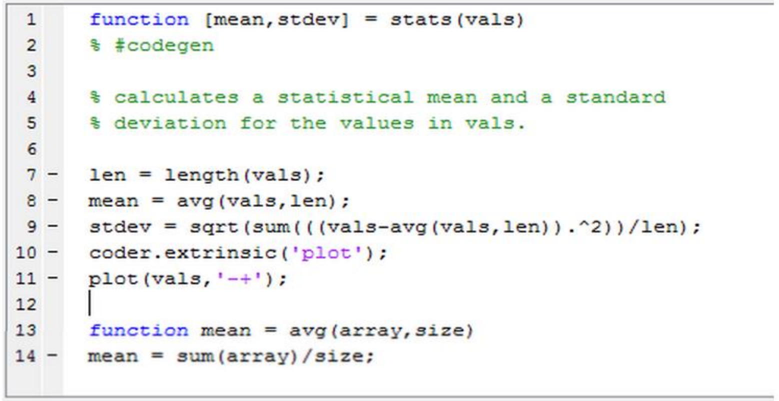
Model-Based Design and Automotive SPICE

SWE.3.BP1: 开发软件详细设计 – 功能分解

Simulink



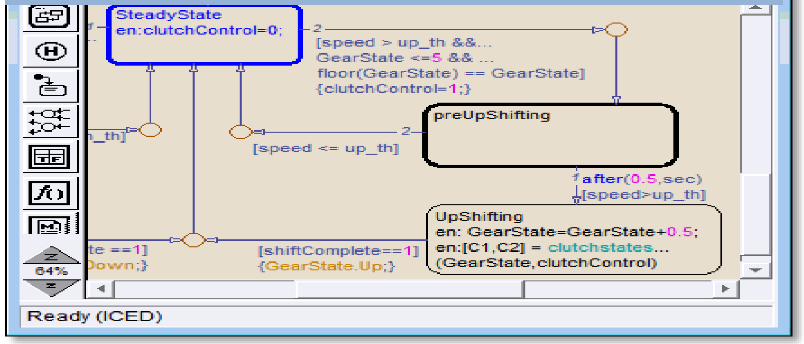
MATLAB



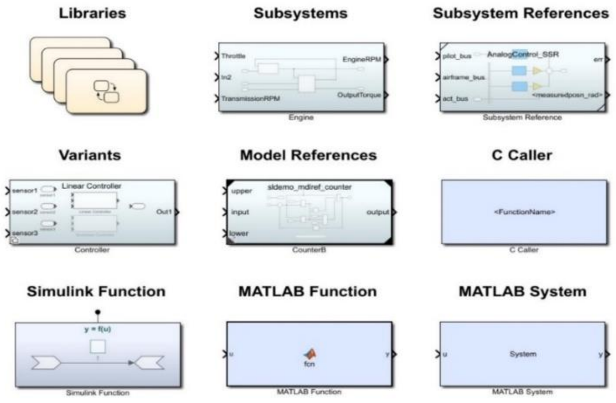
```
function [mean,stdev] = stats(vals)
% #codegen

% calculates a statistical mean and a standard
% deviation for the values in vals.

len = length(vals);
mean = avg(vals,len);
stdev = sqrt(sum(((vals-avg(vals,len)).^2))/len);
coder.extrinsic('plot');
plot(vals,'-+');

function mean = avg(array,size)
mean = sum(array)/size;
```

Stateflow

Stateflow – **instantaneous** changes



功能分解



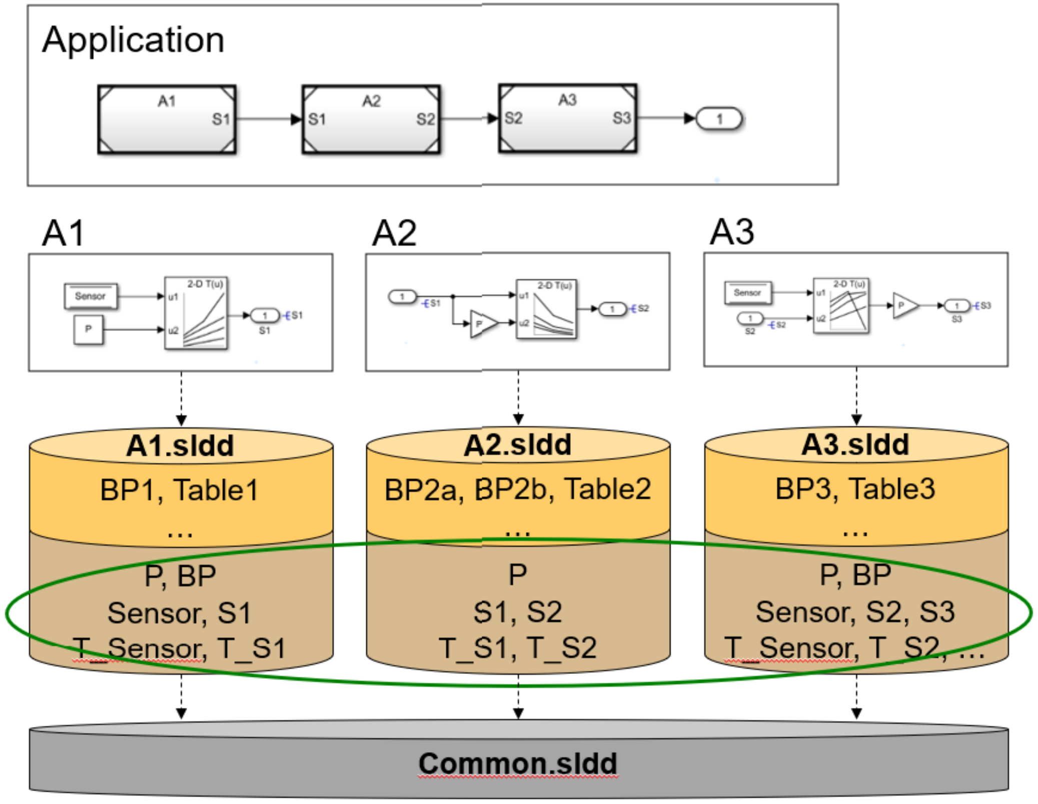
Model-Based Design and Automotive SPICE

SWE.3.BP2: 定义软件单元接口 – 数据字典

- 通过数据字典管理单元接口，标定参数以及观测量

- 数据字典引用：相同接口在多个模型之间维护公用的data dictionary，通过数据字典引用的方式应用到模型，确保接口在不同模型间的一致性
  - R2019a 支持同一接口在多个数据字典重复定义，模型编译期间检查接口的一致性，最终生成代码只有一份定义，解耦数据管理依赖.

- 模型生成的SDD文档包括data dictionary定义的接口信息，方便阅读和确认接口信息。



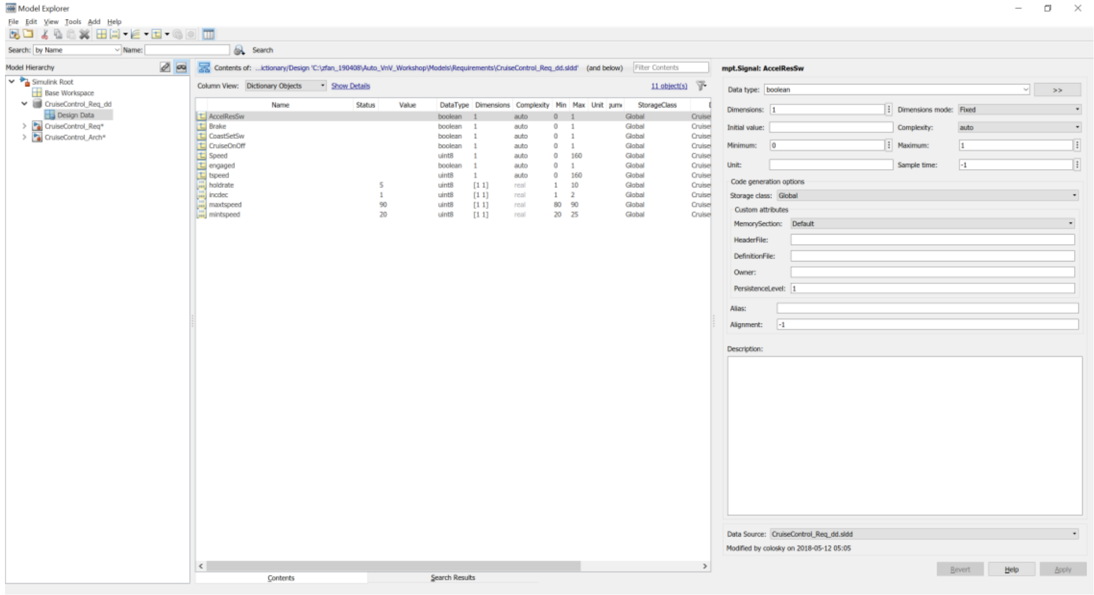
Check consistency for duplicate data across components

Model-Based Design and Automotive SPICE

SWE.3.BP2: 定义软件单元接口 – 接口示例

数据字典

SDD报告接口



Contents of: ...ictionary/Design 'C:\zfan_190408\Auto_VnV_Workshop\Models\Requirements\CruiseControl_Req_dd.sldd' (and below)

Column View: Dictionary Objects Show Details 11 object(s)

Name	Status	Value	DataType	Dimensions	Complexity	Min	Max	Unit	jum	StorageClass	
AccelResSw			boolean	1	auto	0	1			Global	Cruise
Brake			boolean	1	auto	0	1			Global	Cruise
CoastSetSw			boolean	1	auto	0	1			Global	Cruise
CruiseOnOff			boolean	1	auto	0	1			Global	Cruise
Speed			uint8	1	auto	0	160			Global	Cruise
engaged			boolean	1	auto	0	1			Global	Cruise
tspeed			uint8	1	auto	0	160			Global	Cruise
holdrate		5	uint8	[1 1]	real	1	10			Global	Cruise
incdec		1	uint8	[1 1]	real	1	2			Global	Cruise
maxtspeed		90	uint8	[1 1]	real	80	90			Global	Cruise
mintspeed		20	uint8	[1 1]	real	20	25			Global	Cruise

mpt.Signal: AccelResSw

Data type: boolean

Dimensions: 1 Dimensions mode: Fixed

Initial value: Complexity: auto

Minimum: 0 Maximum: 1

Unit: Sample time: -1

Code generation options

Storage class: Global

Custom attributes

MemorySection: Default

HeaderFile:

DefinitionFile:

Owner:

PersistenceLevel: 1

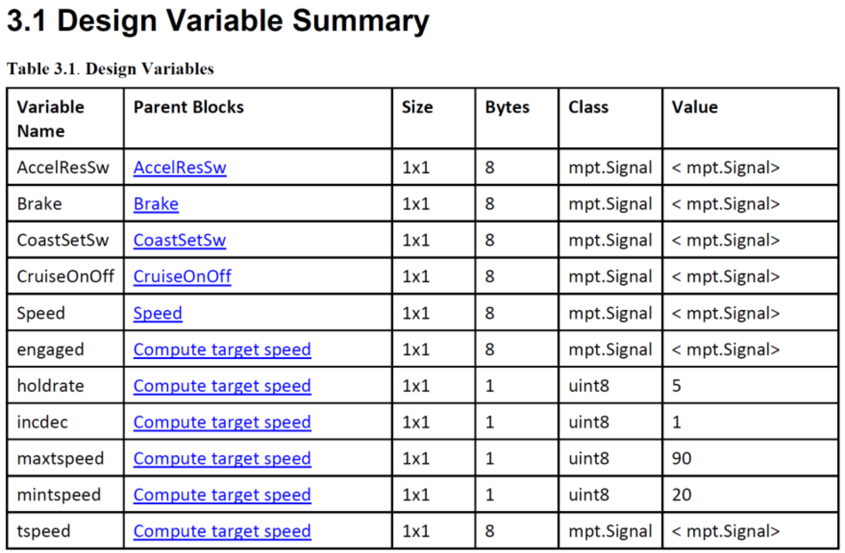
Alias:

Alignment: -1

Description:

Data Source: CruiseControl_Req_dd.sldd

Modified by colosky on 2018-05-12 05:05



3.1 Design Variable Summary

Table 3.1. Design Variables

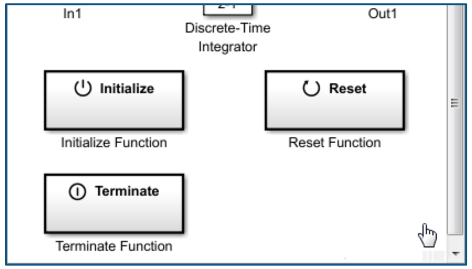
Variable Name	Parent Blocks	Size	Bytes	Class	Value
AccelResSw	AccelResSw	1x1	8	mpt.Signal	< mpt.Signal>
Brake	Brake	1x1	8	mpt.Signal	< mpt.Signal>
CoastSetSw	CoastSetSw	1x1	8	mpt.Signal	< mpt.Signal>
CruiseOnOff	CruiseOnOff	1x1	8	mpt.Signal	< mpt.Signal>
Speed	Speed	1x1	8	mpt.Signal	< mpt.Signal>
engaged	Compute target speed	1x1	8	mpt.Signal	< mpt.Signal>
holdrate	Compute target speed	1x1	1	uint8	5
incdec	Compute target speed	1x1	1	uint8	1
maxtspeed	Compute target speed	1x1	1	uint8	90
mintspeed	Compute target speed	1x1	1	uint8	20
tspeed	Compute target speed	1x1	8	mpt.Signal	< mpt.Signal>

Model-Based Design and Automotive SPICE

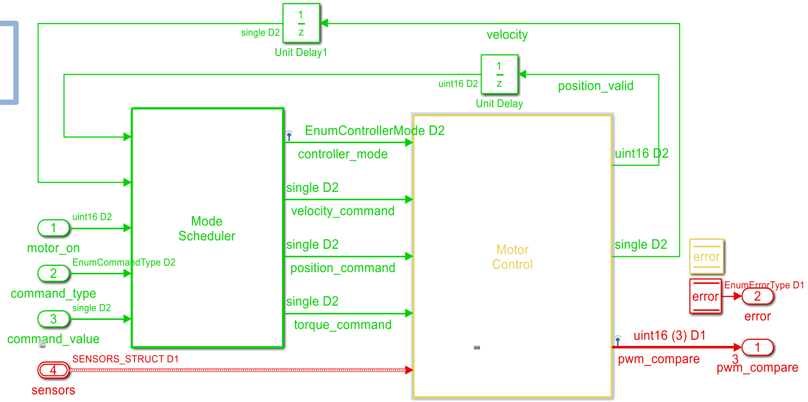
SWE.3.BP3: 描述动态行为

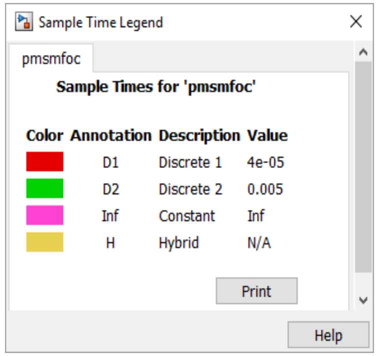
1. 应用不同操作模式函数Initialize, Reset, Terminate
2. 给子系统指定不同的采样周期
3. 通过Stateflow输出显性调度功能模块
4. 使用Schedule Editor 可视化调度

1



2



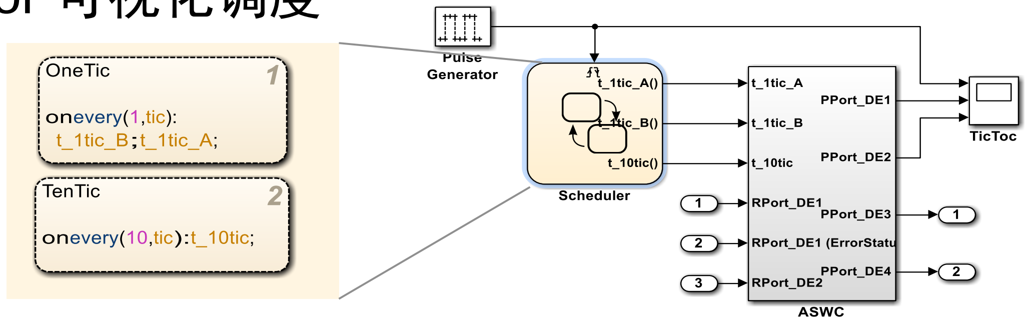

Sample Time Legend

pmsmfoc

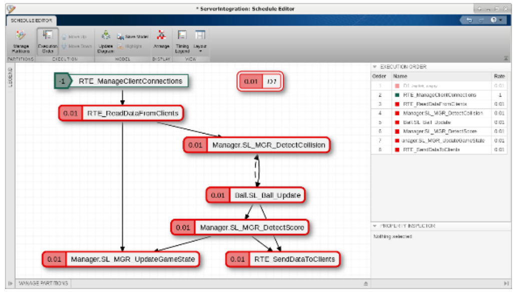
Sample Times for 'pmsmfoc'

Color	Annotation	Description	Value
🟥	D1	Discrete 1	4e-05
🟩	D2	Discrete 2	0.005
🟪	Inf	Constant	Inf
🟨	H	Hybrid	N/A

3



4

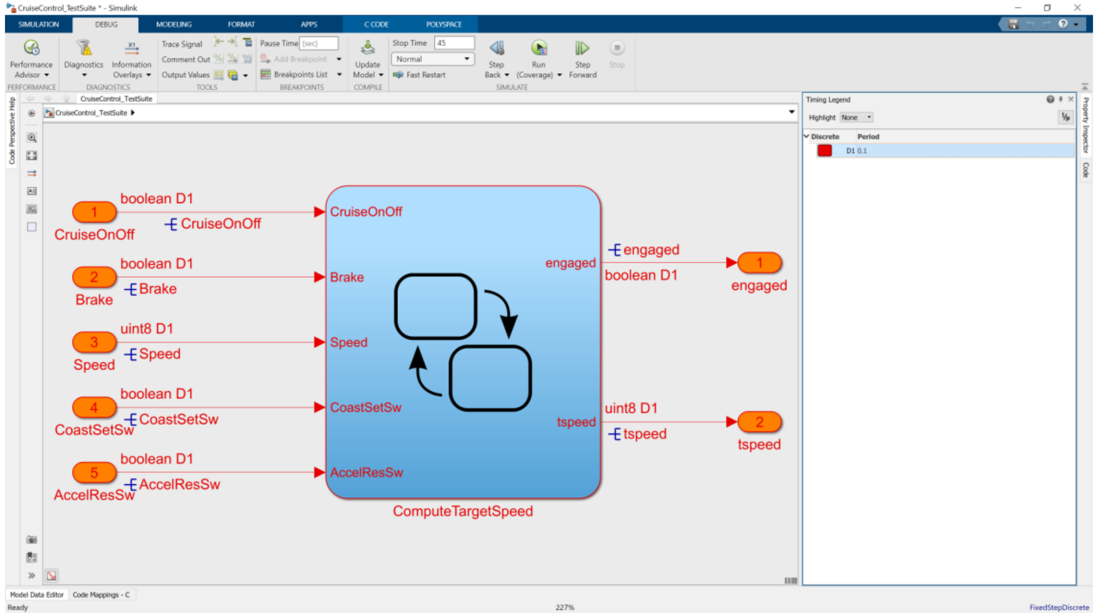


RTE_ManageClientConnections
RTE_ReadDataFromClients
Manager.SL_MGR_DetectCollision
Ball.SL_Ball_Update
Manager.SL_MGR_DetectScore
Manager.SL_MGR_UpdateGameState
RTE_SendDataToClients

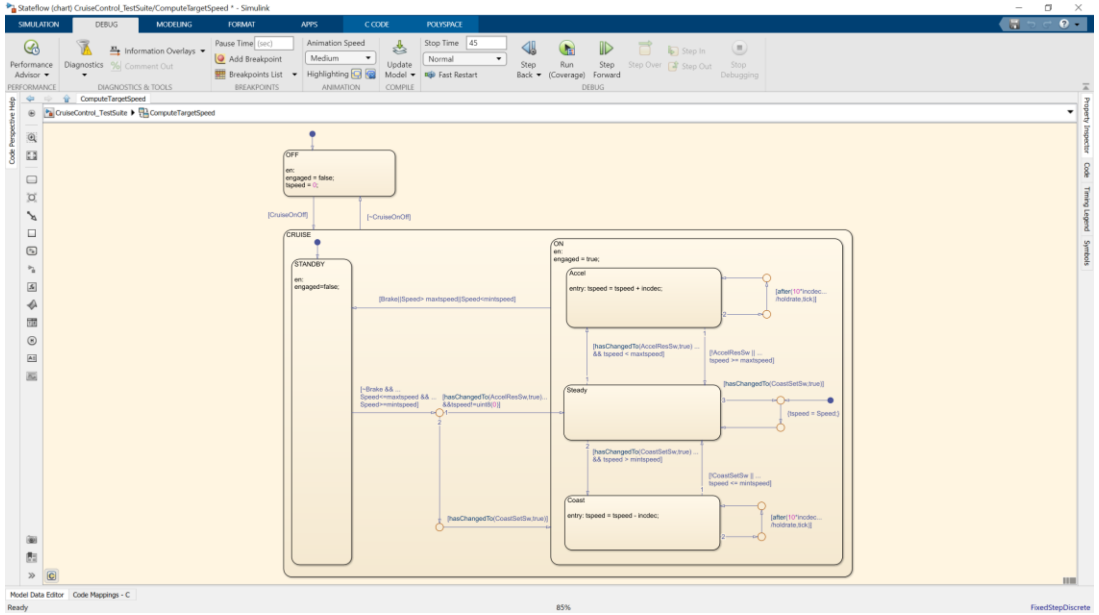
Model-Based Design and Automotive SPICE

SWE.3.BP3: 描述动态行为 - 示例

调度周期



内部交互


Stateflow (chart) CruiseControl_TestSuite/ComputeTargetSpeed * - Simulink
OFF
en:
engaged = false;
tspeed = 0;
[CruiseOnOff]
[~CruiseOnOff]
CRUISE
STANDBY
en:
engaged=false;
ON
en:
engaged = true;
Accel
entry: tspeed = tspeed + incdec;
[after(10*incdec... /holdrate,tick)]
[Brake||Speed> maxtspeed||Speed<mintspeed]
[hasChangedTo(AccelResSw,true) ... && tspeed < maxtspeed]
[!AccelResSw || ... tspeed >= maxtspeed]
[hasChangedTo(CoastSetSw,true)]
Steady
{tspeed = Speed;}
[~Brake && ... Speed<=maxtspeed && ... Speed>=mintspeed]
[hasChangedTo(AccelResSw,true)... &&tspeed!=uint8(0)]
[hasChangedTo(CoastSetSw,true) ... && tspeed > mintspeed]
[!CoastSetSw || ... tspeed <= mintspeed]
Coast
entry: tspeed = tspeed - incdec;
[hasChangedTo(CoastSetSw,true)]
[after(10*incdec... /holdrate,tick)]
85%
FixedStepDiscrete

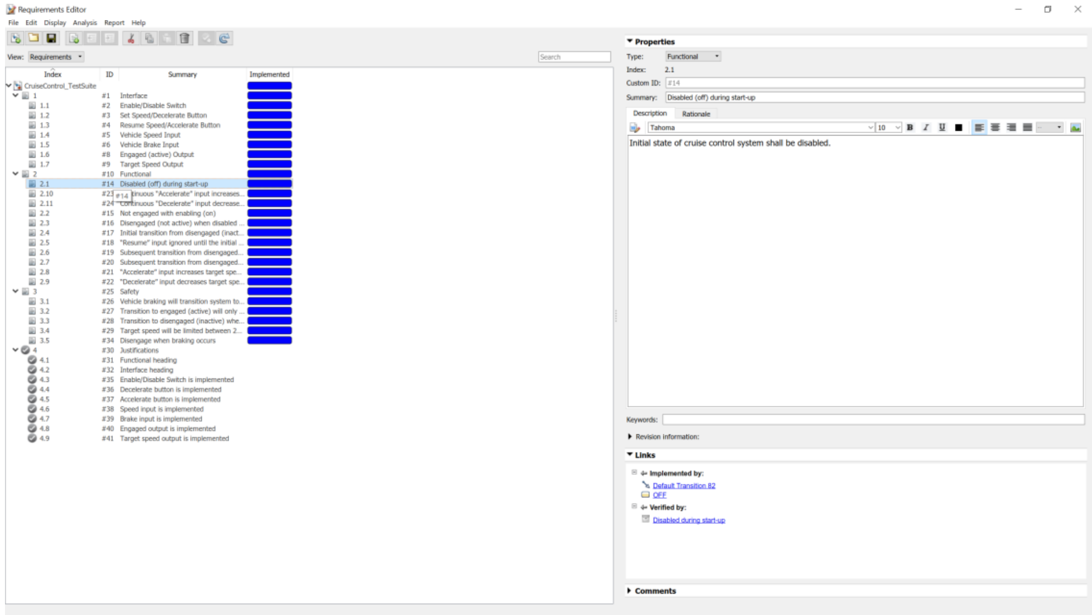
Model-Based Design and Automotive SPICE

SWE.3.BP4: 评估软件详细设计 – 双向追溯

- 评审模型，并确认是否符合与之追溯的SWC Req. (设计依据)

Functional suitability

Functional completeness
Functional correctness
Functional appropriateness



Index	ID	Summary	Implemented
CruiseControl_TestSuite			🟦
1	#1	Interface	🟦
1.1	#2	Enable/Disable Switch	🟦
1.2	#3	Set Speed/Decelerate Button	🟦
1.3	#4	Resume Speed/Accelerate Button	🟦
1.4	#5	Vehicle Speed Input	🟦
1.5	#6	Vehicle Brake Input	🟦
1.6	#8	Engaged (active) Output	🟦
1.7	#9	Target Speed Output	🟦
2	#10	Functional	🟦
2.1	#14	Disabled (off) during start-up	🟦
2.10	#23	#14 tinuous "Accelerate" input increases...	🟦
2.11	#24	Continuous "Decelerate" input decrease...	🟦
2.2	#15	Not engaged with enabling (on)	🟦
2.3	#16	Disengaged (not active) when disabled ...	🟦
2.4	#17	Initial transition from disengaged (inact...	🟦
2.5	#18	"Resume" input ignored until the initial ...	🟦
2.6	#19	Subsequent transition from disengaged...	🟦
2.7	#20	Subsequent transition from disengaged...	🟦
2.8	#21	"Accelerate" input increases target spe...	🟦
2.9	#22	"Decelerate" input decreases target spe...	🟦
3	#25	Safety	🟦
3.1	#26	Vehicle braking will transition system to...	🟦
3.2	#27	Transition to engaged (active) will only ...	🟦
3.3	#28	Transition to disengaged (inactive) whe...	🟦
3.4	#29	Target speed will be limited between 2...	🟦
3.5	#34	Disengage when braking occurs	🟦
4	#30	Justifications	
4.1	#31	Functional heading	
4.2	#32	Interface heading	
4.3	#35	Enable/Disable Switch is implemented	
4.4	#36	Decelerate button is implemented	
4.5	#37	Accelerate button is implemented	
4.6	#38	Speed input is implemented	
4.7	#39	Brake input is implemented	
4.8	#40	Engaged output is implemented	
4.9	#41	Target speed output is implemented	

Properties

Type: Functional
Index: 2.1
Custom ID: #14
Summary: Disabled (off) during start-up

Description | Rationale

Tahoma 10

Initial state of cruise control system shall be disabled.

Keywords:

Revision information:

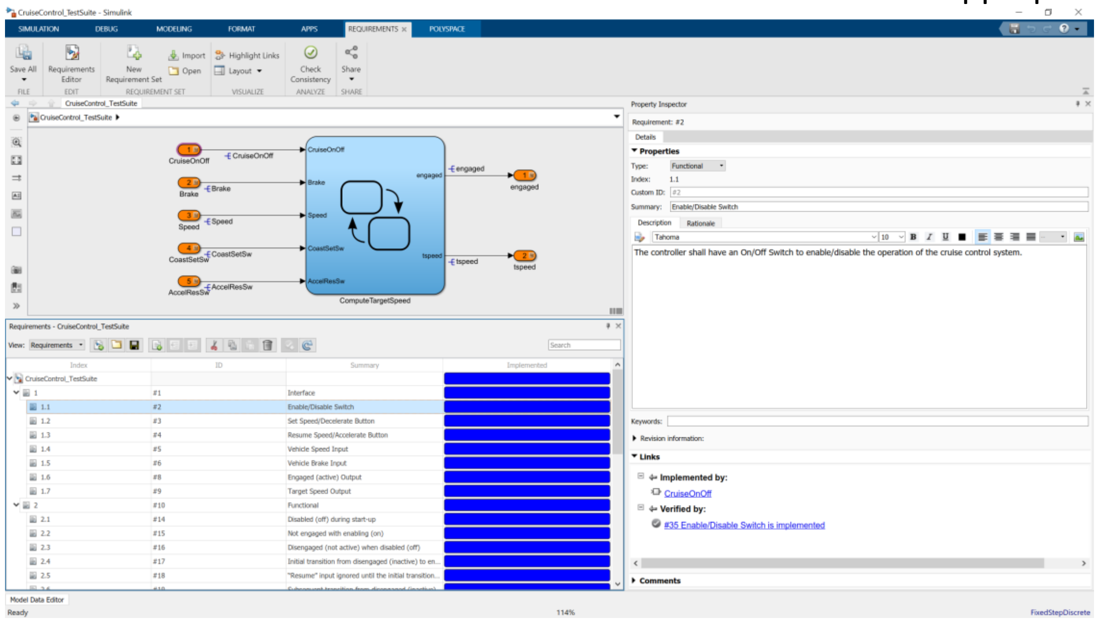
Links

Implemented by:
Default Transition 82
OFF

Verified by:
Disabled during start-up

Comments

需求编辑器视图



Index	ID	Summary	Implemented
CruiseControl_TestSuite			🟦
1	#1	Interface	🟦
1.1	#2	Enable/Disable Switch	🟦
1.2	#3	Set Speed/Decelerate Button	🟦
1.3	#4	Resume Speed/Accelerate Button	🟦
1.4	#5	Vehicle Speed Input	🟦
1.5	#6	Vehicle Brake Input	🟦
1.6	#8	Engaged (active) Output	🟦
1.7	#9	Target Speed Output	🟦
2	#10	Functional	🟦
2.1	#14	Disabled (off) during start-up	🟦
2.2	#15	Not engaged with enabling (on)	🟦
2.3	#16	Disengaged (not active) when disabled (off)	🟦
2.4	#17	Initial transition from disengaged (inactive) to en...	🟦
2.5	#18	"Resume" input ignored until the initial transition...	🟦

Requirement: #2

Details

Properties

Type: Functional
Index: 1.1
Custom ID: #2
Summary: Enable/Disable Switch

Description | Rationale

Tahoma 10

The controller shall have an On/Off Switch to enable/disable the operation of the cruise control system.

Keywords:

Revision information:

Links

Implemented by:
CruiseOnOff

Verified by:
#35 Enable/Disable Switch is implemented

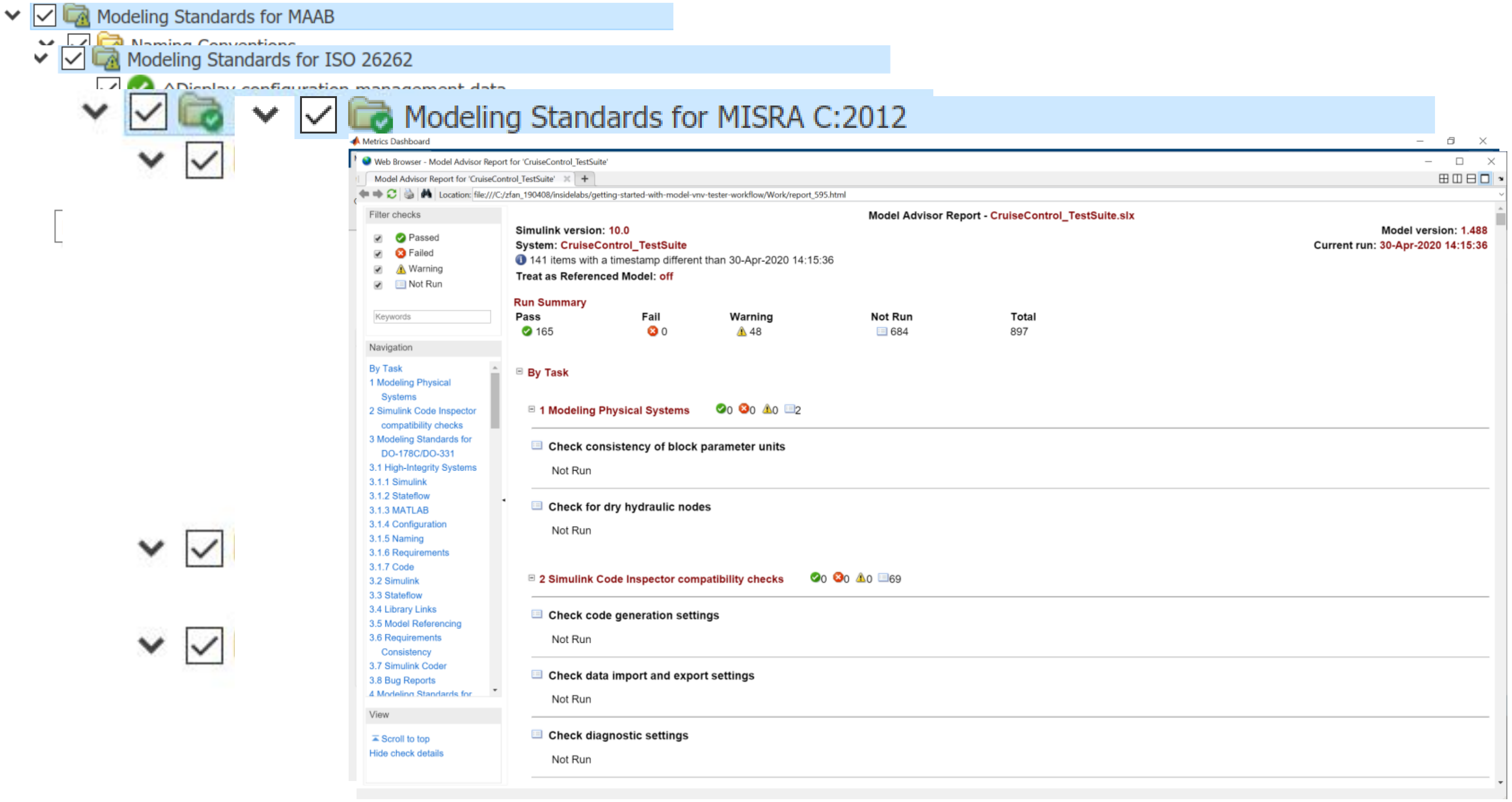
Comments

模型需求透视图

Model-Based Design and Automotive SPICE

SWE.3.BP4: 评估软件详细设计 – 建模规范

- 通过Model-metrics，评价模型的复杂度、规模等
- 评价模型与相关行业标准的符合性（如：ISO26262, MISRA, MAAB等）



☑ Modeling Standards for MAAB

☑ Naming Conventions

☑ Modeling Standards for ISO 26262

☑ ADisplay configuration management data

☑ Modeling Standards for MISRA C:2012

Metrics Dashboard

Web Browser - Model Advisor Report for 'CruiseControl_TestSuite'

Model Advisor Report for 'CruiseControl_TestSuite'

Location: file:///C:/zfan_190408/insidelabs/getting-started-with-model-vnv-tester-workflow/Work/report_595.html

Filter checks

- ☑ Passed
- ☑ Failed
- ☑ Warning
- ☑ Not Run

Keywords

Navigation

- By Task
- 1 Modeling Physical Systems
- 2 Simulink Code Inspector compatibility checks
- 3 Modeling Standards for DO-178C/DO-331
- 3.1 High-Integrity Systems
- 3.1.1 Simulink
- 3.1.2 Stateflow
- 3.1.3 MATLAB
- 3.1.4 Configuration
- 3.1.5 Naming
- 3.1.6 Requirements
- 3.1.7 Code
- 3.2 Simulink
- 3.3 Stateflow
- 3.4 Library Links
- 3.5 Model Referencing
- 3.6 Requirements Consistency
- 3.7 Simulink Coder
- 3.8 Bug Reports
- 4 Modeling Standards for

View

- Scroll to top
- Hide check details

Model Advisor Report - CruiseControl_TestSuite.slx

Simulink version: 10.0

System: CruiseControl_TestSuite

141 items with a timestamp different than 30-Apr-2020 14:15:36

Treat as Referenced Model: off

Model version: 1.488

Current run: 30-Apr-2020 14:15:36

Run Summary

Pass	Fail	Warning	Not Run	Total
✓ 165	✗ 0	⚠ 48	□ 684	897

⊟ **By Task**

⊟ **1 Modeling Physical Systems** ✓0 ✗0 ⚠0 □2

□ **Check consistency of block parameter units**

Not Run

□ **Check for dry hydraulic nodes**

Not Run

⊟ **2 Simulink Code Inspector compatibility checks** ✓0 ✗0 ⚠0 □69

□ **Check code generation settings**

Not Run

□ **Check data import and export settings**

Not Run

□ **Check diagnostic settings**

Not Run

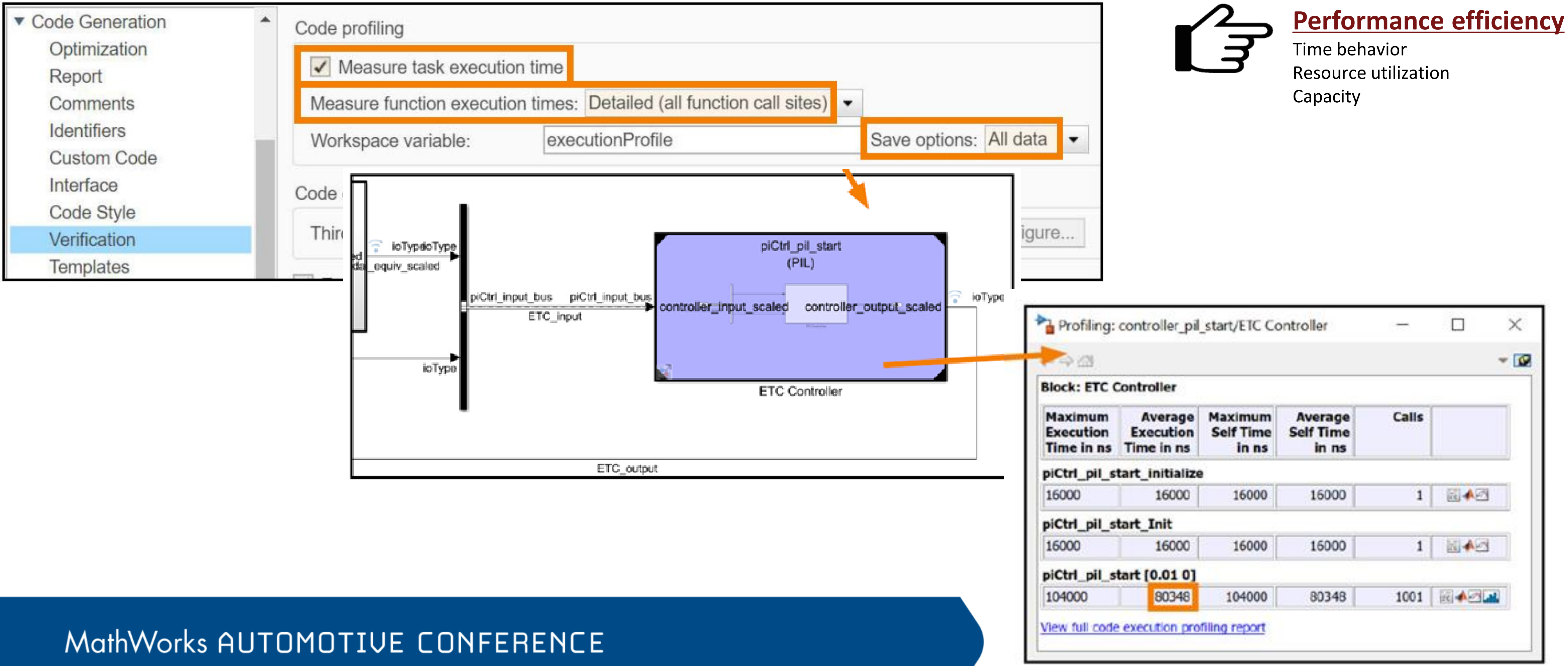
Maintainability

Modularity
Reusability
Analyzability
Modifiability
Testability

Model-Based Design and Automotive SPICE

SWE.3.BP4: 评估软件详细设计 - PIL

- 通过PIL (Processor-In-the-Loop)，确认目标处理器上的资源负载、性能等



Code profiling

☑ Measure task execution time

Measure function execution times: Detailed (all function call sites)

Workspace variable: executionProfile

Save options: All data

Profiling: controller_pil_start/ETC Controller

Block: ETC Controller

Maximum Execution Time in ns	Average Execution Time in ns	Maximum Self Time in ns	Average Self Time in ns	Calls
piCtrl_pil_start_initialize				
16000	16000	16000	16000	1
piCtrl_pil_start_Init				
16000	16000	16000	16000	1
piCtrl_pil_start [0.01 0]				
104000	80348	104000	80348	1001

View full code execution profiling report

Performance efficiency

Time behavior

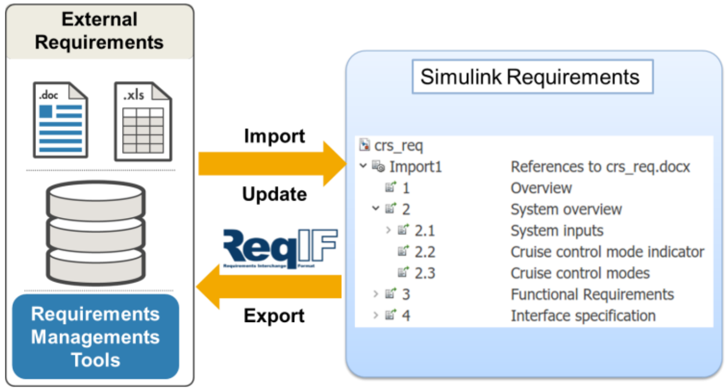
Resource utilization

Capacity

Model-Based Design and Automotive SPICE

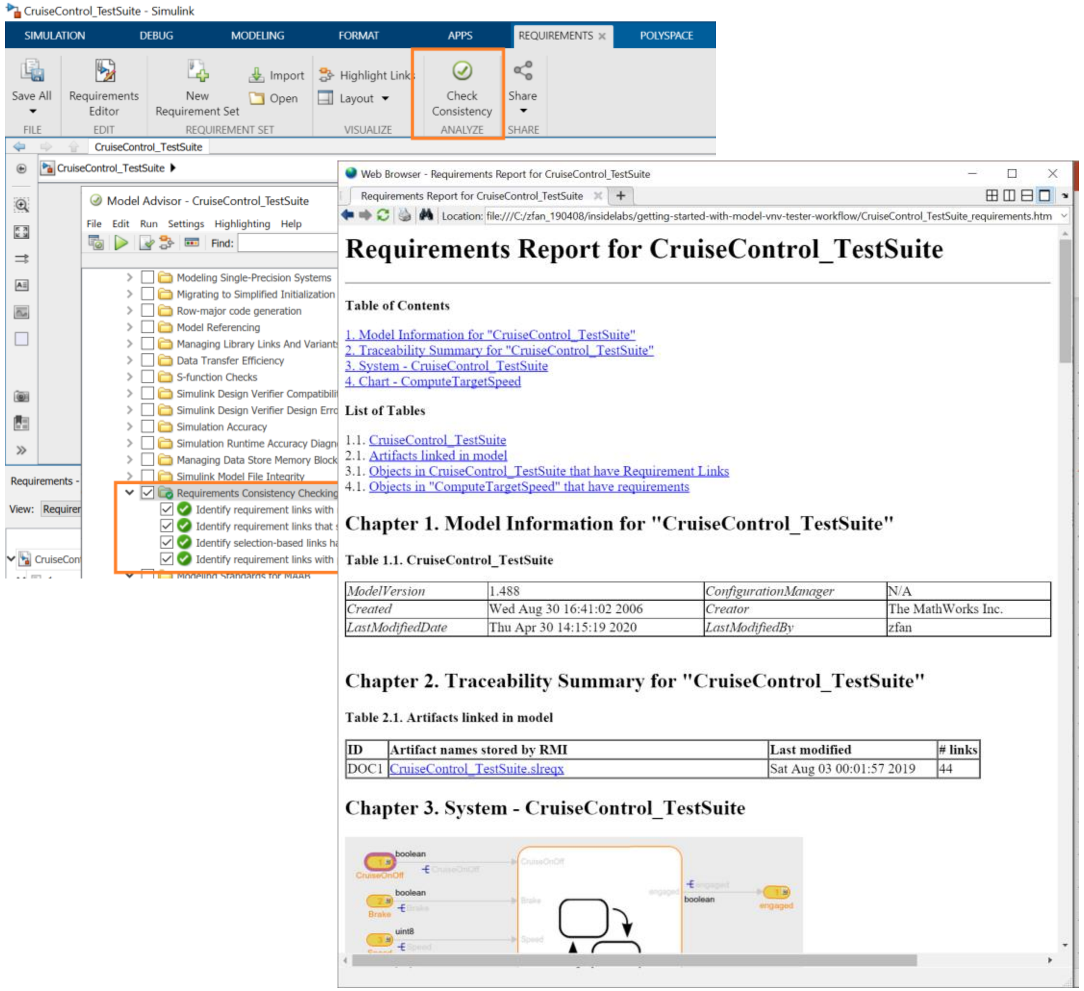
SWE.3.BP5: 建立双向追溯性 & SWE.3.BP6: 确保一致性

- 在模型与其设计依据之间，建立双向追溯性链接
- 设计依据的Format，可以是Word/Excel, DOORs等
- 通过traceability Report确认追溯性的完整性



crs_req	
Import1	References to crs_req.docx
1	Overview
2	System overview
2.1	System inputs
2.2	Cruise control mode indicator
2.3	Cruise control modes
3	Functional Requirements
4	Interface specification

- 导入格式:
  - Word / Excel
  - IBM® Rational® DOORS®
  - ReqIF™ standard
- 同步源端变更到Simulink环境
- 在Simulink环境下对导入需求做修改 R2019a
- 导出标准格式 ReqIF
  - Enables roundtrip with external tools R2019a



- □ Modeling Single-Precision Systems
- □ Migrating to Simplified Initialization
- □ Row-major code generation
- □ Model Referencing
- □ Managing Library Links And Variants
- □ Data Transfer Efficiency
- □ S-function Checks
- □ Simulink Design Verifier Compatibili
- □ Simulink Design Verifier Design Erro
- □ Simulation Accuracy
- □ Simulation Runtime Accuracy Diagn
- □ Managing Data Store Memory Block
- □ Simulink Model File Integrity
- ☑ Requirements Consistency Checking
  - ☑ ✓ Identify requirement links with
  - ☑ ✓ Identify requirement links that
  - ☑ ✓ Identify selection-based links ha
  - ☑ ✓ Identify requirement links with
- □ Modeling Standards for MAAB

file:///C:/zfan_190408/insidelabs/getting-started-with-model-vnv-tester-workflow/CruiseControl_TestSuite_requirements.htm

Requirements Report for CruiseControl_TestSuite

Table of Contents

List of Tables

Chapter 1. Model Information for "CruiseControl_TestSuite"

Table 1.1. CruiseControl_TestSuite

ModelVersion	1.488	*ConfigurationManager*	N/A
Created	Wed Aug 30 16:41:02 2006	*Creator*	The MathWorks Inc.
LastModifiedDate	Thu Apr 30 14:15:19 2020	*LastModifiedBy*	zfan

Chapter 2. Traceability Summary for "CruiseControl_TestSuite"

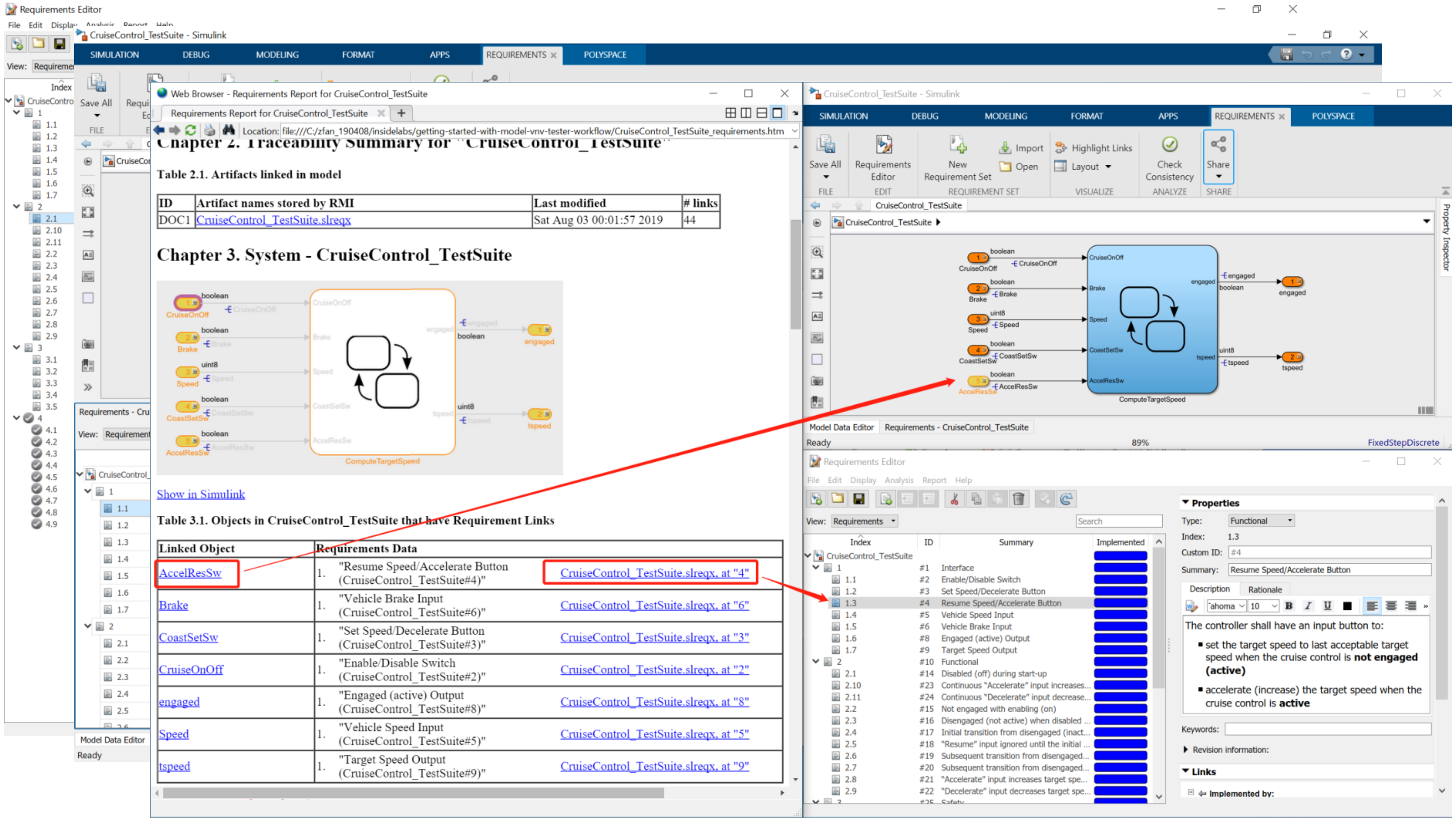
Table 2.1. Artifacts linked in model

ID	Artifact names stored by RMI	Last modified	# links
DOC1	CruiseControl_TestSuite.slreqx	Sat Aug 03 00:01:57 2019	44

Chapter 3. System - CruiseControl_TestSuite

Model-Based Design and Automotive SPICE

SWE.3.BP5: 建立双向追溯性 & SWE.3.BP6: 确保一致性 – 示例



Chapter 2. Traceability Summary for "CruiseControl_TestSuite"

Table 2.1. Artifacts linked in model

ID	Artifact names stored by RMI	Last modified	# links
DOC1	CruiseControl_TestSuite.slreqx	Sat Aug 03 00:01:57 2019	44

Chapter 3. System - CruiseControl_TestSuite

Show in Simulink

Table 3.1. Objects in CruiseControl_TestSuite that have Requirement Links

Linked Object	Requirements Data	
AccelResSw	1. "Resume Speed/Accelerate Button (CruiseControl_TestSuite#4)"	CruiseControl_TestSuite.slreqx, at "4"
Brake	1. "Vehicle Brake Input (CruiseControl_TestSuite#6)"	CruiseControl_TestSuite.slreqx, at "6"
CoastSetSw	1. "Set Speed/Decelerate Button (CruiseControl_TestSuite#3)"	CruiseControl_TestSuite.slreqx, at "3"
CruiseOnOff	1. "Enable/Disable Switch (CruiseControl_TestSuite#2)"	CruiseControl_TestSuite.slreqx, at "2"
engaged	1. "Engaged (active) Output (CruiseControl_TestSuite#8)"	CruiseControl_TestSuite.slreqx, at "8"
Speed	1. "Vehicle Speed Input (CruiseControl_TestSuite#5)"	CruiseControl_TestSuite.slreqx, at "5"
tspeed	1. "Target Speed Output (CruiseControl_TestSuite#9)"	CruiseControl_TestSuite.slreqx, at "9"

View: Requirements

Index	ID	Summary	Implemented
CruiseControl_TestSuite			■
1	#1	Interface	■
1.1	#2	Enable/Disable Switch	■
1.2	#3	Set Speed/Decelerate Button	■
1.3	#4	Resume Speed/Accelerate Button	■
1.4	#5	Vehicle Speed Input	■
1.5	#6	Vehicle Brake Input	■
1.6	#8	Engaged (active) Output	■
1.7	#9	Target Speed Output	■
2	#10	Functional	■
2.1	#14	Disabled (off) during start-up	■
2.10	#23	Continuous "Accelerate" input increases...	■
2.11	#24	Continuous "Decelerate" input decrease...	■
2.2	#15	Not engaged with enabling (on)	■
2.3	#16	Disengaged (not active) when disabled ...	■
2.4	#17	Initial transition from disengaged (inact...	■
2.5	#18	"Resume" input ignored until the initial ...	■
2.6	#19	Subsequent transition from disengaged...	■
2.7	#20	Subsequent transition from disengaged...	■
2.8	#21	"Accelerate" input increases target spe...	■
2.9	#22	"Decelerate" input decreases target spe...	■
3	#25	Safety	■

Properties

Type: Functional

Index: 1.3

Custom ID: #4

Summary: Resume Speed/Accelerate Button

Description | Rationale

The controller shall have an input button to:

- set the target speed to last acceptable target speed when the cruise control is **not engaged (active)**
- accelerate (increase) the target speed when the cruise control is **active**

Keywords:

Revision information:

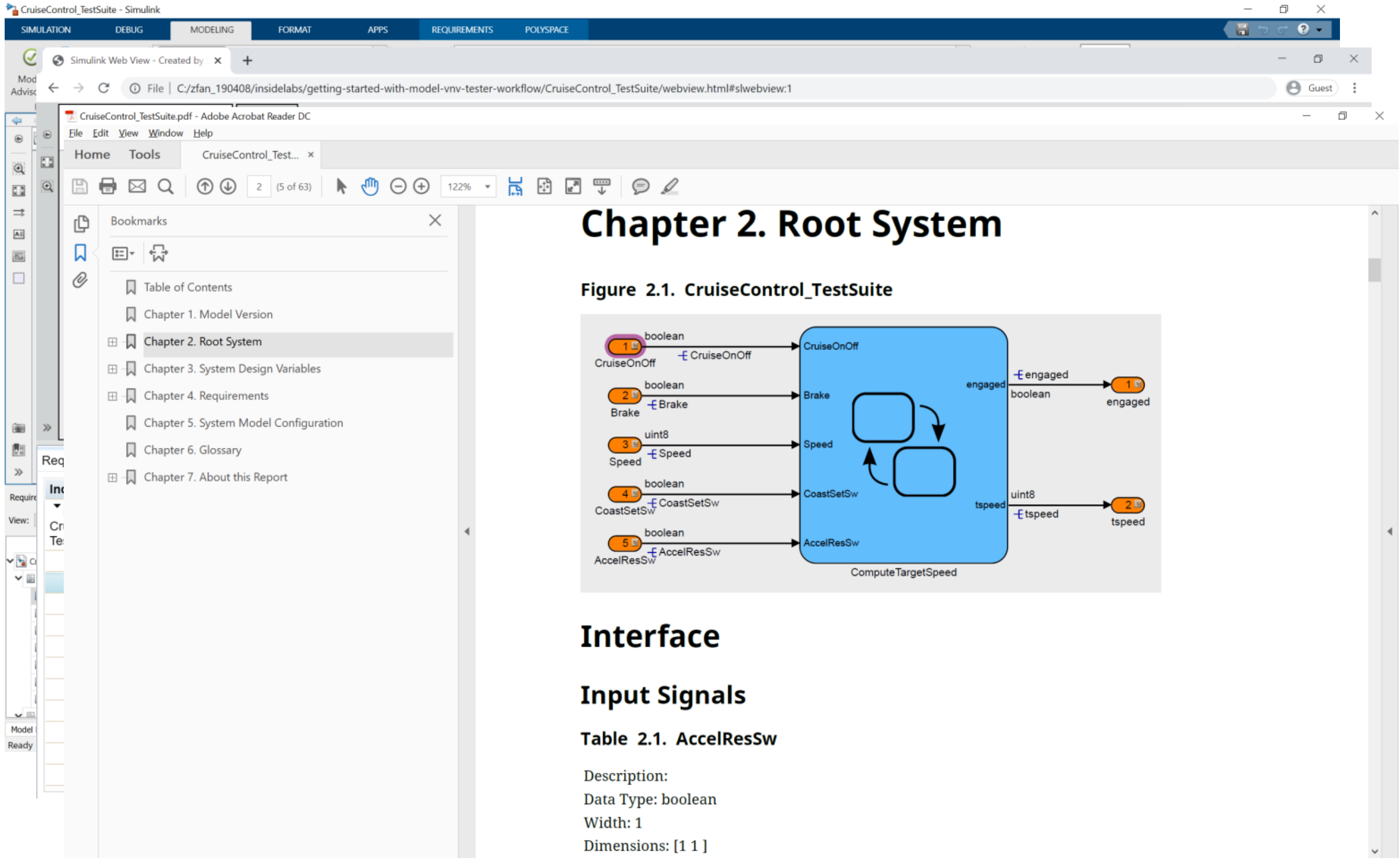
Links

Implemented by:

Model-Based Design and Automotive SPICE

SWE.3.BP7 沟通达成一致的软件详细设计

- 通过多种形式，非常容易的在相关方之间沟通模型设计并达成一致
  - 模型
  - Web View (HTML)
  - Design Report (PDF)


CruiseControl_TestSuite - Simulink
SIMULATION
DEBUG
MODELING
FORMAT
APPS
REQUIREMENTS
POLYSPACE
Simulink Web View - Created by
File | C:/zfan_190408/insidelabs/getting-started-with-model-vnv-tester-workflow/CruiseControl_TestSuite/webview.html#slwebview:1
Guest
CruiseControl_TestSuite.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools CruiseControl_Test...
2 (5 of 63)
122%
Bookmarks

Chapter 2. Root System

Figure 2.1. CruiseControl_TestSuite

Interface

Input Signals

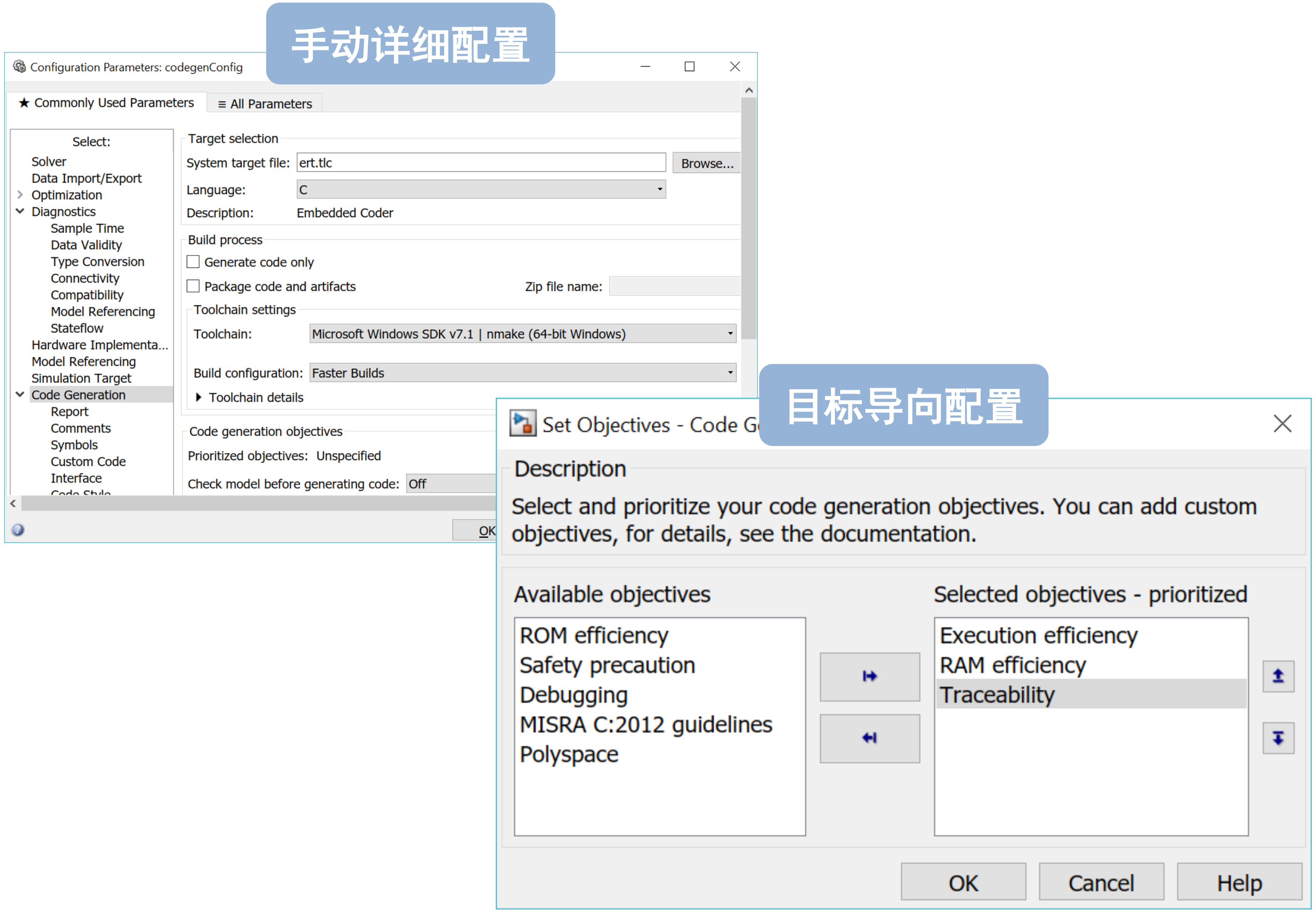
Table 2.1. AccelResSw

Description:
Data Type: boolean
Width: 1
Dimensions: [1 1]

Model-Based Design and Automotive SPICE

SWE.3.BP8: 构建软件单元

- MBD自动代码生成
  - 数据字典做数据管理
  - 代码生成配置
  - 优化选项



手动详细配置

Configuration Parameters: codegenConfig

Target selection

System target file: ert.tlc

Language: C

Description: Embedded Coder

Build process

☐ Generate code only

☐ Package code and artifacts   Zip file name:

Toolchain settings

Toolchain: Microsoft Windows SDK v7.1 | nmake (64-bit Windows)

Build configuration: Faster Builds

▸ Toolchain details

Code generation objectives

Prioritized objectives: Unspecified

Check model before generating code: Off

目标导向配置

Set Objectives - Code G

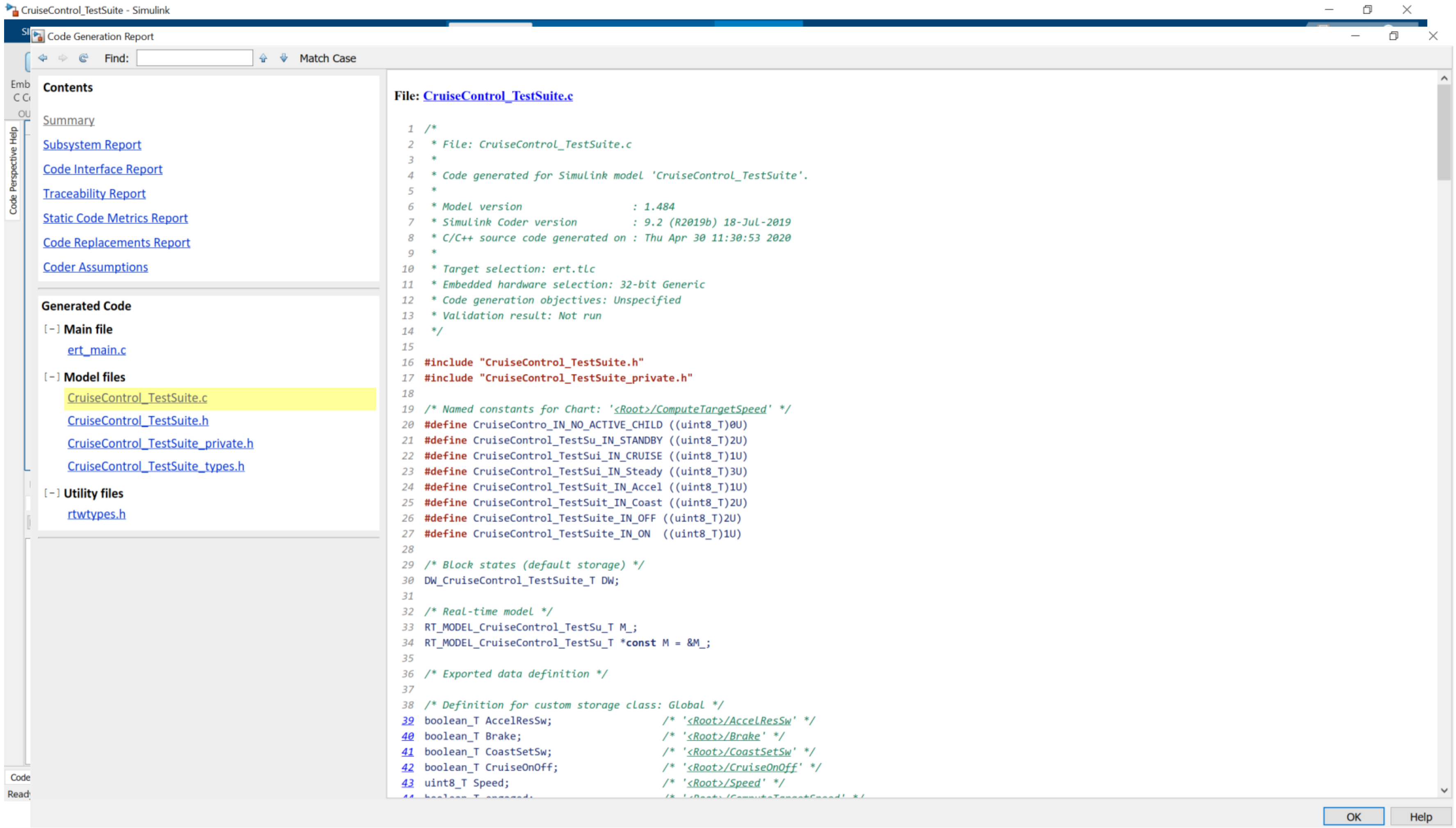
Description

Select and prioritize your code generation objectives. You can add custom objectives, for details, see the documentation.

Available objectives	Selected objectives - prioritized
ROM efficiency	Execution efficiency
Safety precaution	RAM efficiency
Debugging	Traceability
MISRA C:2012 guidelines	
Polyspace	

Model-Based Design and Automotive SPICE

SWE.3.BP8: 构建软件单元



File: CruiseControl_TestSuite.c

```
/*
 * File: CruiseControl_TestSuite.c
 *
 * Code generated for Simulink model 'CruiseControl_TestSuite'.
 *
 * Model version                  : 1.484
 * Simulink Coder version         : 9.2 (R2019b) 18-Jul-2019
 * C/C++ source code generated on : Thu Apr 30 11:30:53 2020
 *
 * Target selection: ert.tlc
 * Embedded hardware selection: 32-bit Generic
 * Code generation objectives: Unspecified
 * Validation result: Not run
 */

#include "CruiseControl_TestSuite.h"
#include "CruiseControl_TestSuite_private.h"

/* Named constants for Chart: '<Root>/ComputeTargetSpeed' */
#define CruiseContro_IN_NO_ACTIVE_CHILD ((uint8_T)0U)
#define CruiseControl_TestSu_IN_STANDBY ((uint8_T)2U)
#define CruiseControl_TestSui_IN_CRUISE ((uint8_T)1U)
#define CruiseControl_TestSui_IN_Steady ((uint8_T)3U)
#define CruiseControl_TestSuit_IN_Accel ((uint8_T)1U)
#define CruiseControl_TestSuit_IN_Coast ((uint8_T)2U)
#define CruiseControl_TestSuite_IN_OFF ((uint8_T)2U)
#define CruiseControl_TestSuite_IN_ON  ((uint8_T)1U)

/* Block states (default storage) */
DW_CruiseControl_TestSuite_T DW;

/* Real-time model */
RT_MODEL_CruiseControl_TestSu_T M_;
RT_MODEL_CruiseControl_TestSu_T *const M = &M_;

/* Exported data definition */

/* Definition for custom storage class: Global */
boolean_T AccelResSw;                  /* '<Root>/AccelResSw' */
boolean_T Brake;                       /* '<Root>/Brake' */
boolean_T CoastSetSw;                  /* '<Root>/CoastSetSw' */
boolean_T CruiseOnOff;                 /* '<Root>/CruiseOnOff' */
uint8_T Speed;                         /* '<Root>/Speed' */
boolean_T engaged;                     /* '<Root>/ComputeTargetSpeed' */
```

主题

- 背景介绍
- 采用MBD方法，满足ASPICE要求
  - MBD开发概述
  - 详细举例：SWE.3 软件详细设计与单元实现
  - 详细举例：SWE.4 软件单元测试

SWE.4 基本实践与输出

SWE.4 – 基本实践(BP)

- SWE.4.BP1: 开发包括回归策略的软件单元验证策略
- SWE.4.BP2: 开发单元验证准则
- SWE.4.BP3: 实施软件单元的静态验证
- SWE.4.BP4: 测试软件单元
- SWE.4.BP5: 建立双向追溯性
- SWE.4.BP6: 确保一致性
- SWE.4.BP7: 总结并沟通结果

实施SWE.4过程的结果如下

- 开发软件单元验证策略
- 开发软件单元验证准则
- 实施软件单元验证，并记录验证结果
- 建立了双向追溯性：
  - 软件单元和静态验证结果之间
  - 软件详细设计和单元测试规范之间
  - 软件单元测试规范和单元测试结果之间之间
- 确保一致性:
  - 软件详细设计和单元测试规范之间
- 总结验证结果，并与所有相关方沟通

Model-Based Design and Automotive SPICE

MBD场景下的测试验证概述

- 在使用模型进行设计，并基于模型自动生成代码，则[SWE.4 软件单元验证]所要求的软件单元层面的验证（静态验证+单元测试）可在模型层面上来实施。

[MBD.RL.8] If software units that are generated from the verified model by using a qualified tool chain (and without any further modification after generation) are not statically verified, the indicator SWE.4.BP3 must not be downrated.
[MBD.RL.9] If software units that are generated from the verified model by using a qualified tool chain (and without any further modification after generation) are not unit tested, the indicator SWE.4.BP4 must not be downrated.
Note: Qualified tool chain for the code generation means that there is evidence that the generated code is correct and consistent with the model.

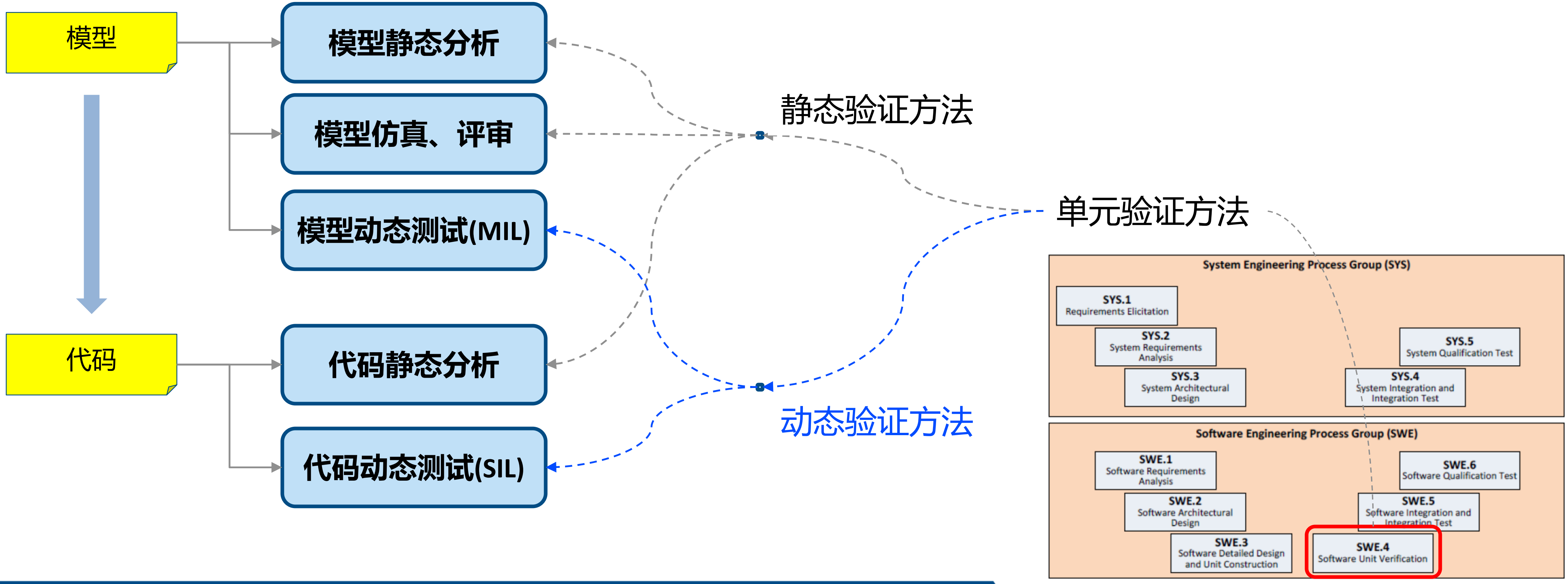
From Automotive SPICE Guideline 1st edition

Part 6 – 9.4.1
NOTE 3 For model-based software development, the corresponding parts of the implementation model also represent objects for the verification planning. Depending on the selected software development process the verification objects can be the code derived from this model, the model itself, or both.

From ISO26262:2018

Model-Based Design and Automotive SPICE

SWE.4.BP1: 制定软件单元验证策略



模型
代码
模型静态分析
模型仿真、评审
模型动态测试(MIL)
代码静态分析
代码动态测试(SIL)
静态验证方法
单元验证方法
动态验证方法
System Engineering Process Group (SYS)
SYS.1 Requirements Elicitation
SYS.2 System Requirements Analysis
SYS.3 System Architectural Design
SYS.4 System Integration and Integration Test
SYS.5 System Qualification Test
Software Engineering Process Group (SWE)
SWE.1 Software Requirements Analysis
SWE.2 Software Architectural Design
SWE.3 Software Detailed Design and Unit Construction
SWE.4 Software Unit Verification
SWE.5 Software Integration and Integration Test
SWE.6 Software Qualification Test

Model-Based Design and Automotive SPICE

SWE.4.BP2: 开发单元验证准则 & SWE.4.BP3: 实施软件单元的静态验证

- 模型静态分析/模型仿真、评审
  - 参见SWE.3.BP4

- 代码静态分析(Polyspace)
  - 相关行业标准的符合性（如：ISO26262, MISRA等）
  - 代码质量相关指标（如：圈复杂度）
  - 形式化方法的语义分析和抽象解释，验证软件进程间、控制流和数据流行为
  - 运行时错误检查（如：溢出、被零除、数组访问越界）

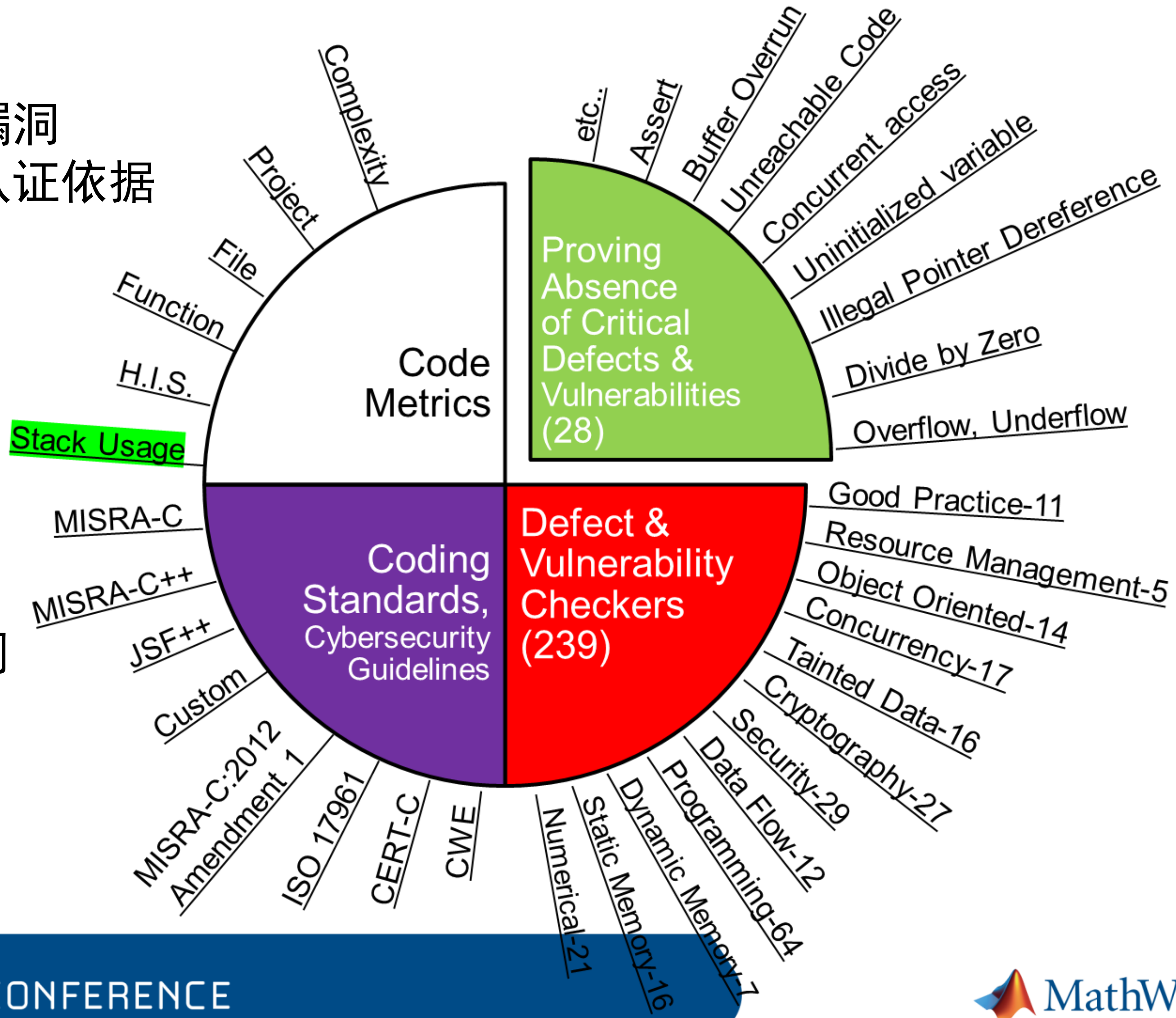
静态测试支持 - Polyspace功能一览

Bug Finder

- 保证可测量性和可维护性
- 排除绝大多数软件缺陷和漏洞
- 提供功能安全和网络安全认证依据

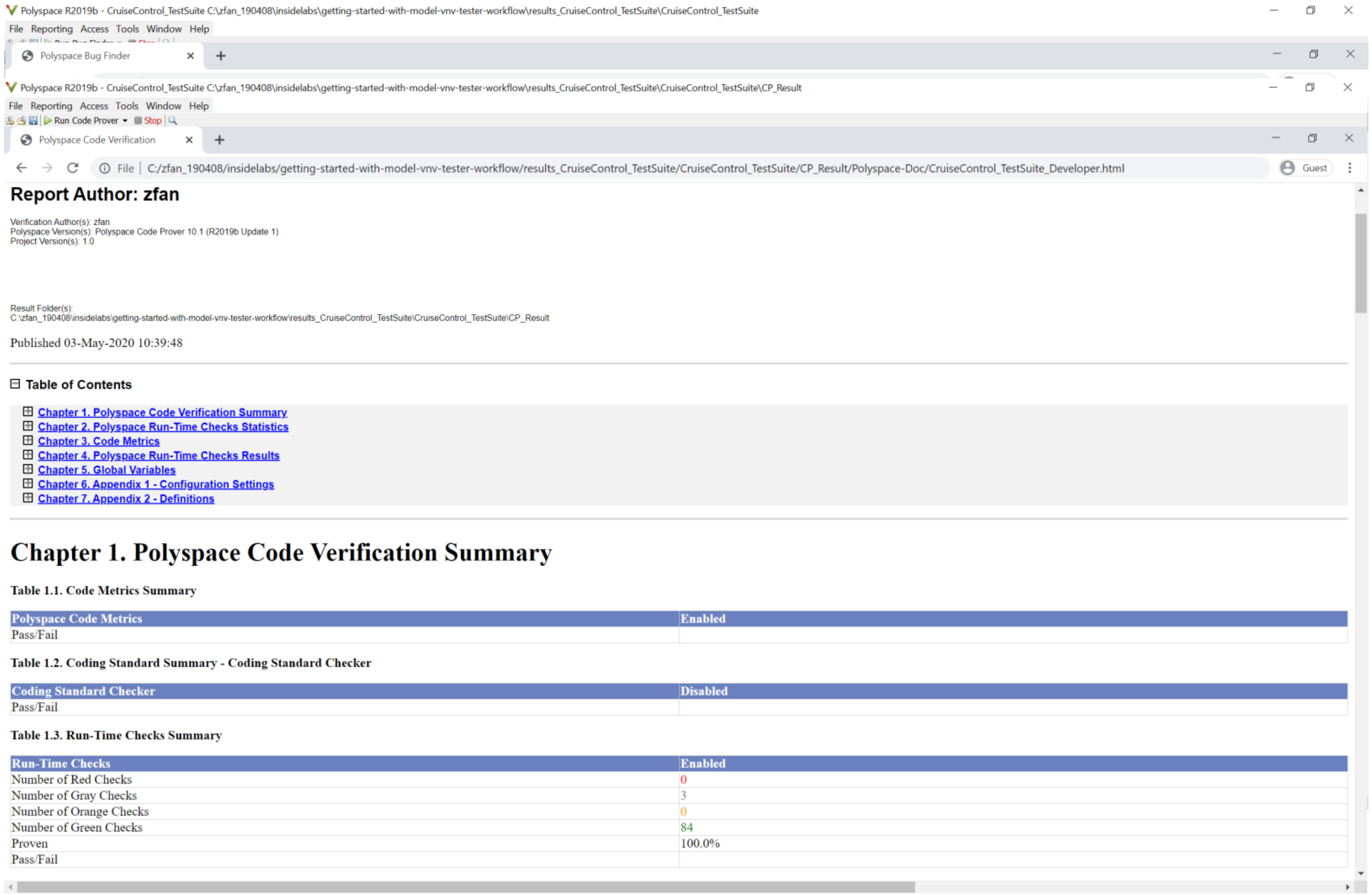
Code Prover

- 确保可靠性和安全性
- 证明无关键运行错误和漏洞
- 提供附加认证审查证据



Model-Based Design and Automotive SPICE

SWE.4.BP2开发单元验证准则 & SWE.4.BP3实施软件单元的静态验证 – 示例


Polyspace R2019b - CruiseControl_TestSuite C:\zfan_190408\insidelabs\getting-started-with-model-vnv-tester-workflow\results_CruiseControl_TestSuite\CruiseControl_TestSuite
File Reporting Access Tools Window Help
Polyspace Bug Finder
Polyspace R2019b - CruiseControl_TestSuite C:\zfan_190408\insidelabs\getting-started-with-model-vnv-tester-workflow\results_CruiseControl_TestSuite\CruiseControl_TestSuite\CP_Result
File Reporting Access Tools Window Help
Run Code Prover
Stop
Polyspace Code Verification
File | C:/zfan_190408/insidelabs/getting-started-with-model-vnv-tester-workflow/results_CruiseControl_TestSuite/CruiseControl_TestSuite/CP_Result/Polyspace-Doc/CruiseControl_TestSuite_Developer.html
Guest

Report Author: zfan

Verification Author(s): zfan
Polyspace Version(s): Polyspace Code Prover 10.1 (R2019b Update 1)
Project Version(s): 1.0

Result Folder(s):
C:\zfan_190408\insidelabs\getting-started-with-model-vnv-tester-workflow\results_CruiseControl_TestSuite\CruiseControl_TestSuite\CP_Result

Published 03-May-2020 10:39:48

⊟ Table of Contents

Chapter 1. Polyspace Code Verification Summary

Table 1.1. Code Metrics Summary

Polyspace Code Metrics	Enabled
Pass/Fail	

Table 1.2. Coding Standard Summary - Coding Standard Checker

Coding Standard Checker	Disabled
Pass/Fail	

Table 1.3. Run-Time Checks Summary

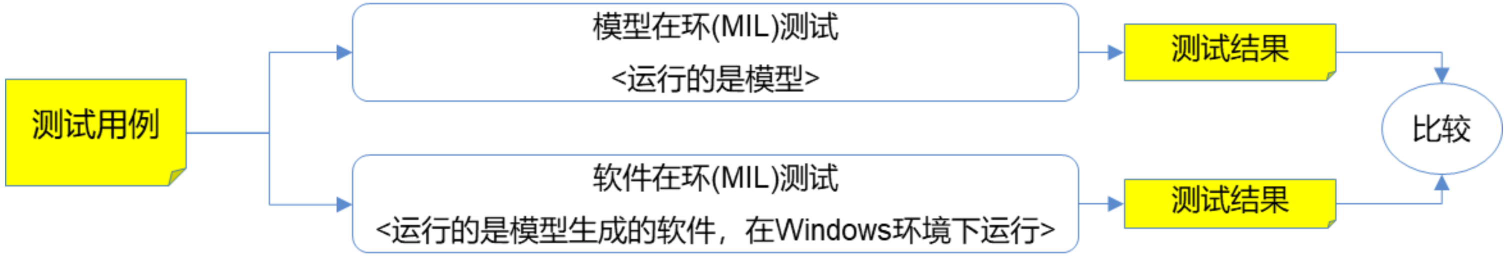
Run-Time Checks	Enabled
Number of Red Checks	0
Number of Gray Checks	3
Number of Orange Checks	0
Number of Green Checks	84
Proven	100.0%
Pass/Fail	

Model-Based Design and Automotive SPICE

SWE.4.BP2: 开发单元验证准则 & SWE.4.BP4: 测试软件单元(动态测试)

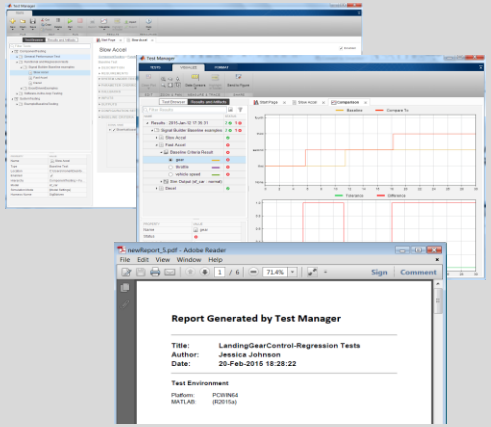
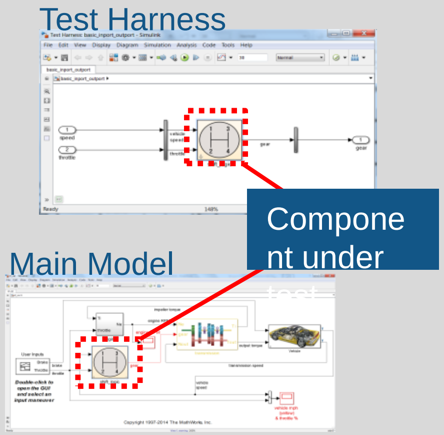
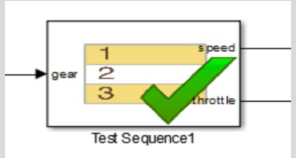
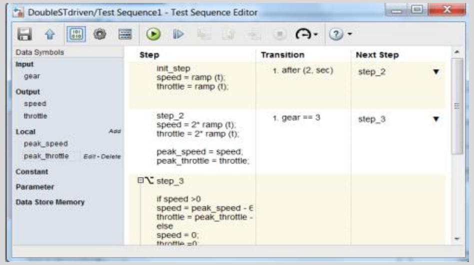
- 模型在环(MIL)测试
  - 验证SWC Req. (设计依据)是否被正确实现
  - 验证模型内部逻辑的正确性，可用结构化覆盖度指标衡量，比如MC/DC等

- 软件在环(SIL)测试
  - 验证代码与模型的等效性



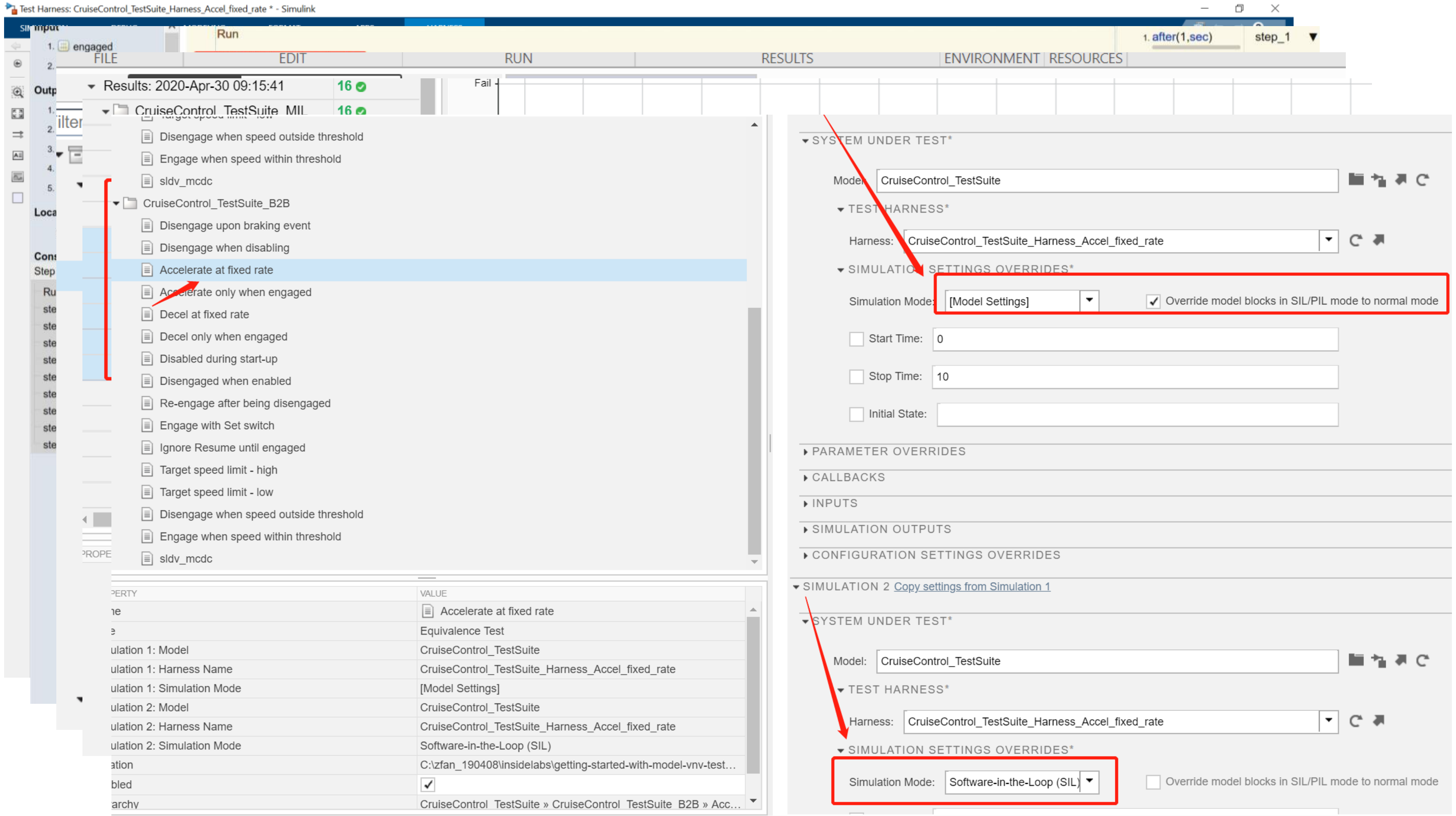
- Simulink Test
  - Test Manager, Test Sequence, Test Harness等协助进行测试管理、测试用例设计、测试执行等

动态测试支持 - Simulink Test

Test Manager	Test Harness	Test Sequence Block
• Author, execute, manage test cases • Review, export, report	• Synchronized, simulation test environment	• Test Inputs and assessments • Based on logical, temporal conditions
 newReport_5.pdf - Adobe Reader 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)	 Test Harness Main Model Compone nt under test	  DoubleSTdriven/Test Sequence1 - Test Sequence Editor Data Symbols Input: gear Output: speed, throttle Local: peak_speed, peak_throttle Constant Parameter Data Store Memory Step: init_step / speed = ramp (t); / throttle = ramp (t); — Transition: 1. after (2, sec) — Next Step: step_2 Step: step_2 / speed = 2* ramp (t); / throttle = 2* ramp (t); / peak_speed = speed; / peak_throttle = throttle; — Transition: 1. gear == 3 — Next Step: step_3 Step: step_3 / if speed >0 / speed = peak_speed - 6 / throttle = peak_throttle - / else / speed = 0; / throttle =0;

Model-Based Design and Automotive SPICE

SWE.4.BP2: 开发单元验证准则 & SWE.4.BP4: 测试软件单元(动态) – 示例



Results: 2020-Apr-30 09:15:41 16 ✓

CruiseControl_TestSuite_MIL 16 ✓

- Disengage when speed outside threshold
- Engage when speed within threshold
- sldv_mcdc
- CruiseControl_TestSuite_B2B
  - Disengage upon braking event
  - Disengage when disabling
  - Accelerate at fixed rate
  - Accelerate only when engaged
  - Decel at fixed rate
  - Decel only when engaged
  - Disabled during start-up
  - Disengaged when enabled
  - Re-engage after being disengaged
  - Engage with Set switch
  - Ignore Resume until engaged
  - Target speed limit - high
  - Target speed limit - low
  - Disengage when speed outside threshold
  - Engage when speed within threshold
  - sldv_mcdc

PERTY	VALUE
ne	Accelerate at fixed rate
e	Equivalence Test
ulation 1: Model	CruiseControl_TestSuite
ulation 1: Harness Name	CruiseControl_TestSuite_Harness_Accel_fixed_rate
ulation 1: Simulation Mode	[Model Settings]
ulation 2: Model	CruiseControl_TestSuite
ulation 2: Harness Name	CruiseControl_TestSuite_Harness_Accel_fixed_rate
ulation 2: Simulation Mode	Software-in-the-Loop (SIL)
ation	C:\zfan_190408\insidelabs\getting-started-with-model-vnv-test…
bled	☑
archy	CruiseControl_TestSuite » CruiseControl_TestSuite_B2B » Acc…

SYSTEM UNDER TEST*

Model: CruiseControl_TestSuite

TEST HARNESS*

Harness: CruiseControl_TestSuite_Harness_Accel_fixed_rate

SIMULATION SETTINGS OVERRIDES*

Simulation Mode: [Model Settings] ☑ Override model blocks in SIL/PIL mode to normal mode

□ Start Time: 0

□ Stop Time: 10

□ Initial State:

PARAMETER OVERRIDES

CALLBACKS

INPUTS

SIMULATION OUTPUTS

CONFIGURATION SETTINGS OVERRIDES

SIMULATION 2 Copy settings from Simulation 1

SYSTEM UNDER TEST*

Model: CruiseControl_TestSuite

TEST HARNESS*

Harness: CruiseControl_TestSuite_Harness_Accel_fixed_rate

SIMULATION SETTINGS OVERRIDES*

Simulation Mode: Software-in-the-Loop (SIL) □ Override model blocks in SIL/PIL mode to normal mode

Model-Based Design and Automotive SPICE

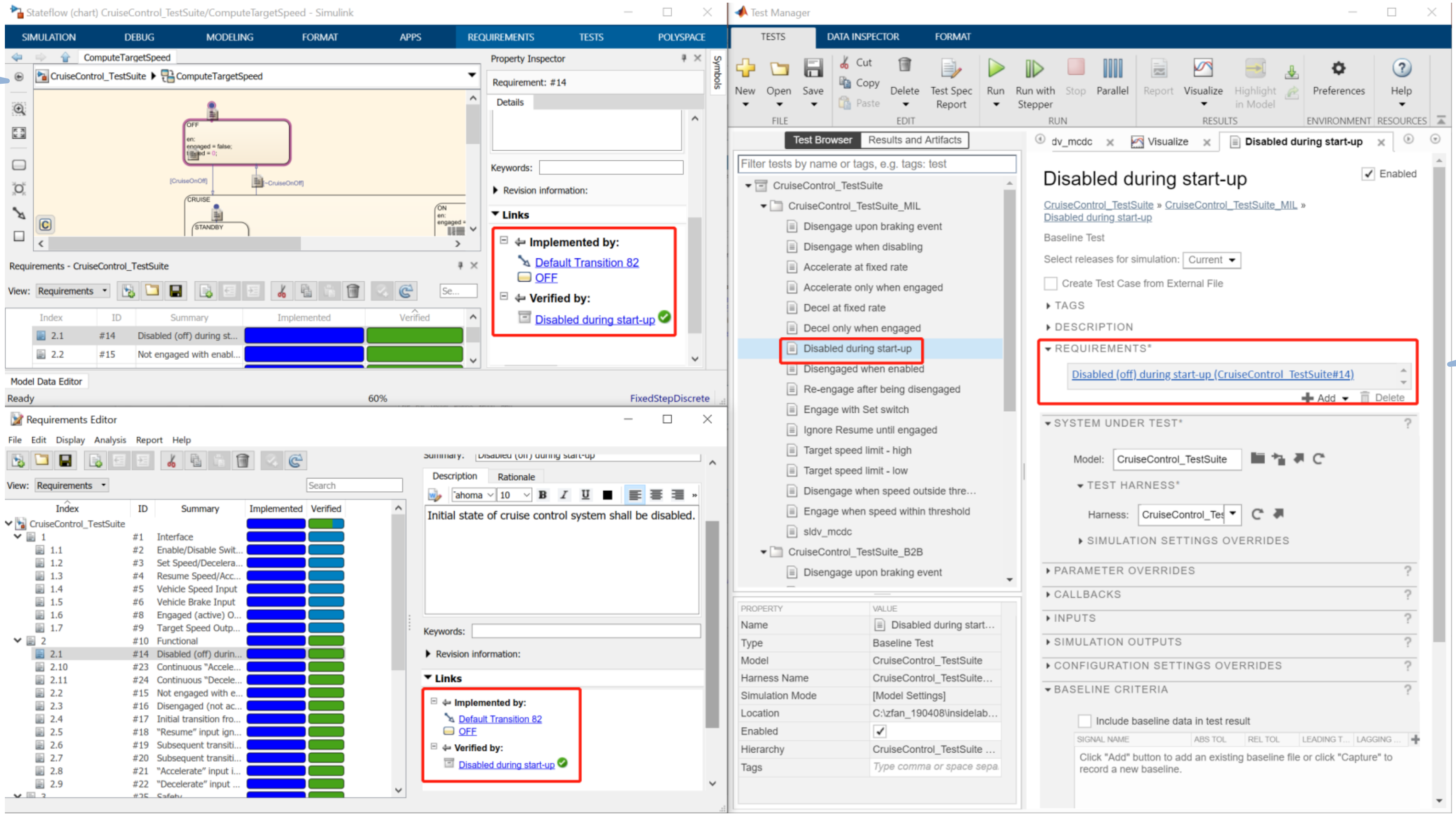
SWE.4.BP5: 建立双向追溯性 & SWE.4.BP6: 确保一致性

- 工具能建立：
  - 测试用例与SWC Req.之间的追溯性
  - 测试用例与测试结果之间的追溯性
  - 静态分析结果与代码之间的关联

- 基于如上的追溯性链接，方便确认追溯项之间的一致性

Model-Based Design and Automotive SPICE

SWE.4.BP5: 建立双向追溯性 & SWE.4.BP6: 确保一致性 (动态测试)



Requirement: #14

Details

Keywords:

▸ Revision information:

▾ Links

⊟ Implemented by:
- Default Transition 82
- OFF

⊟ Verified by:
- Disabled during start-up ✓

View: Requirements

Index	ID	Summary	Implemented	Verified
2.1	#14	Disabled (off) during st...		
2.2	#15	Not engaged with enabl...		

View: Requirements

Index	ID	Summary	Implemented	Verified
CruiseControl_TestSuite				
1	#1	Interface		
1.1	#2	Enable/Disable Swit...		
1.2	#3	Set Speed/Decelera...		
1.3	#4	Resume Speed/Acc...		
1.4	#5	Vehicle Speed Input		
1.5	#6	Vehicle Brake Input		
1.6	#8	Engaged (active) O...		
1.7	#9	Target Speed Outp...		
2	#10	Functional		
2.1	#14	Disabled (off) durin...		
2.10	#23	Continuous "Accele...		
2.11	#24	Continuous "Decele...		
2.2	#15	Not engaged with e...		
2.3	#16	Disengaged (not ac...		
2.4	#17	Initial transition fro...		
2.5	#18	"Resume" input ign...		
2.6	#19	Subsequent transiti...		
2.7	#20	Subsequent transiti...		
2.8	#21	"Accelerate" input i...		
2.9	#22	"Decelerate" input ...		
3	#25	Safety		

Summary: Disabled (off) during start-up

Description | Rationale

Initial state of cruise control system shall be disabled.

Keywords:

▸ Revision information:

▾ Links

⊟ Implemented by:
- Default Transition 82
- OFF

⊟ Verified by:
- Disabled during start-up ✓

Filter tests by name or tags, e.g. tags: test

- CruiseControl_TestSuite
  - CruiseControl_TestSuite_MIL
    - Disengage upon braking event
    - Disengage when disabling
    - Accelerate at fixed rate
    - Accelerate only when engaged
    - Decel at fixed rate
    - Decel only when engaged
    - Disabled during start-up
    - Disengaged when enabled
    - Re-engage after being disengaged
    - Engage with Set switch
    - Ignore Resume until engaged
    - Target speed limit - high
    - Target speed limit - low
    - Disengage when speed outside thre...
    - Engage when speed within threshold
    - sldv_mcdc
  - CruiseControl_TestSuite_B2B
    - Disengage upon braking event

PROPERTY	VALUE
Name	Disabled during start...
Type	Baseline Test
Model	CruiseControl_TestSuite
Harness Name	CruiseControl_TestSuite...
Simulation Mode	[Model Settings]
Location	C:\zfan_190408\insidelab...
Enabled	☑
Hierarchy	CruiseControl_TestSuite ...
Tags	Type comma or space sepa...

Disabled during start-up ☑ Enabled

CruiseControl_TestSuite » CruiseControl_TestSuite_MIL » Disabled during start-up

Baseline Test

Select releases for simulation: Current

□ Create Test Case from External File

▸ TAGS

▸ DESCRIPTION

▾ REQUIREMENTS*

Disabled (off) during start-up (CruiseControl_TestSuite#14)

Add ▾ Delete

▾ SYSTEM UNDER TEST*

Model: CruiseControl_TestSuite

▾ TEST HARNESS*

Harness: CruiseControl_Tes

▸ SIMULATION SETTINGS OVERRIDES

▸ PARAMETER OVERRIDES

▸ CALLBACKS

▸ INPUTS

▸ SIMULATION OUTPUTS

▸ CONFIGURATION SETTINGS OVERRIDES

▾ BASELINE CRITERIA

□ Include baseline data in test result

SIGNAL NAME	ABS TOL	REL TOL	LEADING T...	LAGGING ...

Click "Add" button to add an existing baseline file or click "Capture" to record a new baseline.

需求透视图

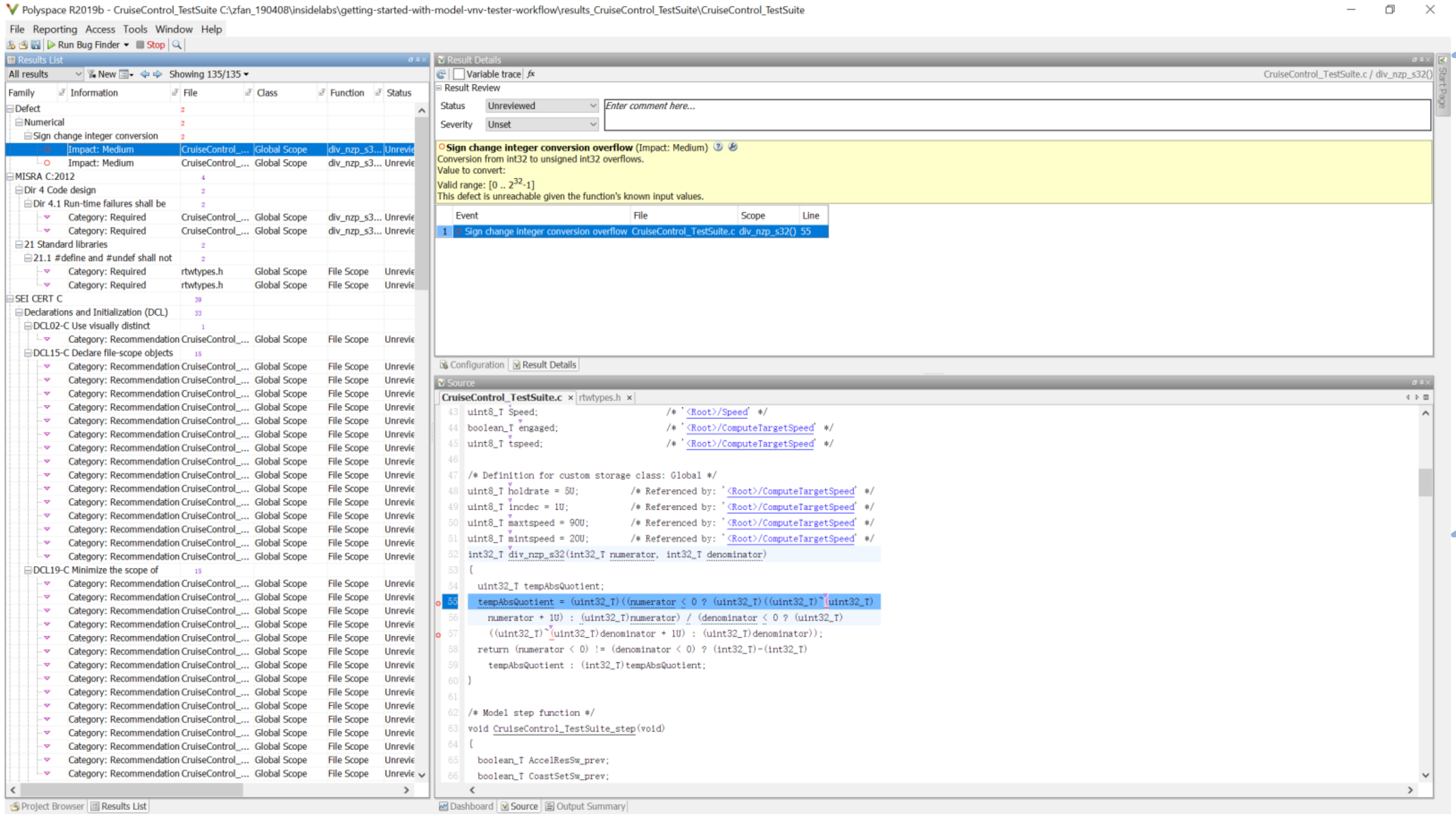
需求编辑视图

测试用例视图

Model-Based Design and Automotive SPICE

SWE.4.BP5: 建立双向追溯性 & SWE.4.BP6: 确保一致性 (静态分析)

Polyspace 结果列表


Polyspace R2019b - CruiseControl_TestSuite C:\zfan_190408\insidelabs\getting-started-with-model-vnv-tester-workflow\results_CruiseControl_TestSuite\CruiseControl_TestSuite
File
Reporting
Access
Tools
Window
Help
Run Bug Finder
Stop
Results List
All results
New
Showing 135/135
Result Details
Variable trace
CruiseControl_TestSuite.c / div_nzp_s32()
Start Page
Configuration
Result Details
Source
CruiseControl_TestSuite.c
rtwtypes.h
Project Browser
Results List
Dashboard
Source
Output Summary

Family	Information	File	Class	Function	Status
Defect		2			
Numerical		2			
Sign change integer conversion		2			
○	Impact: Medium	CruiseControl_...	Global Scope	div_nzp_s3...	Unrevie
○	Impact: Medium	CruiseControl_...	Global Scope	div_nzp_s3...	Unrevie
MISRA C:2012		4			
Dir 4 Code design		2			
Dir 4.1 Run-time failures shall be		2			
▽	Category: Required	CruiseControl_...	Global Scope	div_nzp_s3...	Unrevie
▽	Category: Required	CruiseControl_...	Global Scope	div_nzp_s3...	Unrevie
21 Standard libraries		2			
21.1 #define and #undef shall not		2			
▽	Category: Required	rtwtypes.h	Global Scope	File Scope	Unrevie
▽	Category: Required	rtwtypes.h	Global Scope	File Scope	Unrevie
SEI CERT C		39			
Declarations and Initialization (DCL)		33			
DCL02-C Use visually distinct		1			
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
DCL15-C Declare file-scope objects		15			
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
DCL19-C Minimize the scope of		15			
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie
▽	Category: Recommendation	CruiseControl_...	Global Scope	File Scope	Unrevie

Result Review

Status: Unreviewed

Severity: Unset

Enter comment here...

○ **Sign change integer conversion overflow** (Impact: Medium)
Conversion from int32 to unsigned int32 overflows.
Value to convert:
Valid range: [0 .. 2^{32}-1]
This defect is unreachable given the function's known input values.

	Event	File	Scope	Line
1	○ Sign change integer conversion overflow	CruiseControl_TestSuite.c	div_nzp_s32()	55

```
43  uint8_T Speed;                          /* '<Root>/Speed' */
44  boolean_T engaged;                      /* '<Root>/ComputeTargetSpeed' */
45  uint8_T tspeed;                         /* '<Root>/ComputeTargetSpeed' */
46
47  /* Definition for custom storage class: Global */
48  uint8_T holdrate = 5U;          /* Referenced by: '<Root>/ComputeTargetSpeed' */
49  uint8_T incdec = 1U;            /* Referenced by: '<Root>/ComputeTargetSpeed' */
50  uint8_T maxtspeed = 90U;        /* Referenced by: '<Root>/ComputeTargetSpeed' */
51  uint8_T mintspeed = 20U;        /* Referenced by: '<Root>/ComputeTargetSpeed' */
52  int32_T div_nzp_s32(int32_T numerator, int32_T denominator)
53  {
54    uint32_T tempAbsQuotient;
55    tempAbsQuotient = (uint32_T)((numerator < 0 ? (uint32_T)((uint32_T)~(uint32_T)
56      numerator + 1U) : (uint32_T)numerator) / (denominator < 0 ? (uint32_T)
57      ((uint32_T)~(uint32_T)denominator + 1U) : (uint32_T)denominator));
58    return (numerator < 0) != (denominator < 0) ? (int32_T)-(int32_T)
59      tempAbsQuotient : (int32_T)tempAbsQuotient;
60  }
61
62  /* Model step function */
63  void CruiseControl_TestSuite_step(void)
64  {
65    boolean_T AccelResSw_prev;
66    boolean_T CoastSetSw_prev;
```

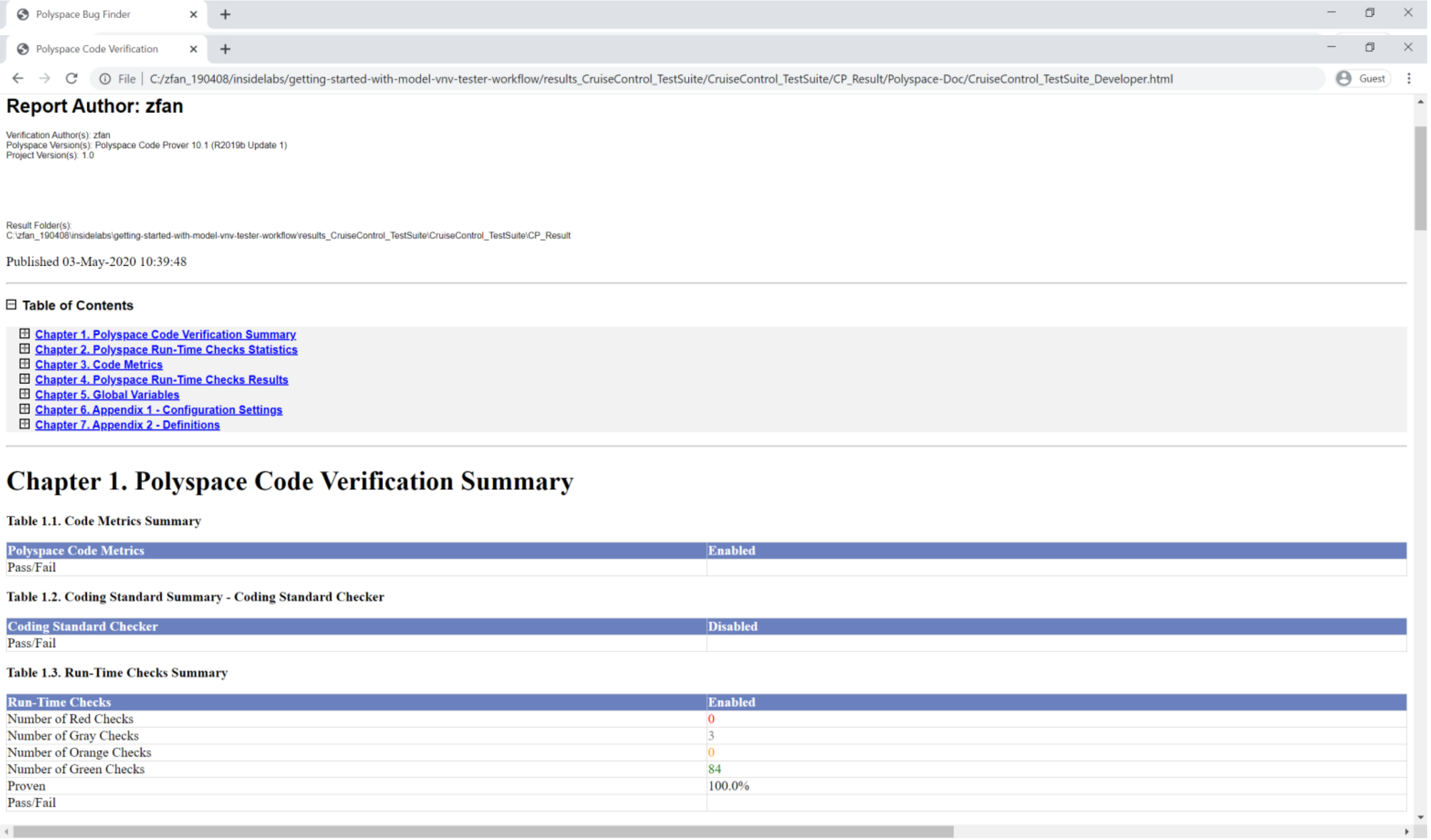
Polyspace 结果说明

Polyspace 代码区域

Model-Based Design and Automotive SPICE

SWE.4.BP7: 总结并沟通结果(静态分析)

- 多种形式的静态分析和动态测试的验证结果，方便在相关方中沟通单元验证结果。



C:/zfan_190408/insidelabs/getting-started-with-model-vnv-tester-workflow/results_CruiseControl_TestSuite/CruiseControl_TestSuite/CP_Result/Polyspace-Doc/CruiseControl_TestSuite_Developer.html

Report Author: zfan

Verification Author(s): zfan
Polyspace Version(s): Polyspace Code Prover 10.1 (R2019b Update 1)
Project Version(s): 1.0

Result Folder(s):
C:\zfan_190408\insidelabs\getting-started-with-model-vnv-tester-workflow\results_CruiseControl_TestSuite\CruiseControl_TestSuite\CP_Result

Published 03-May-2020 10:39:48

Table of Contents

Chapter 1. Polyspace Code Verification Summary

Table 1.1. Code Metrics Summary

Polyspace Code Metrics	Enabled
Pass/Fail	

Table 1.2. Coding Standard Summary - Coding Standard Checker

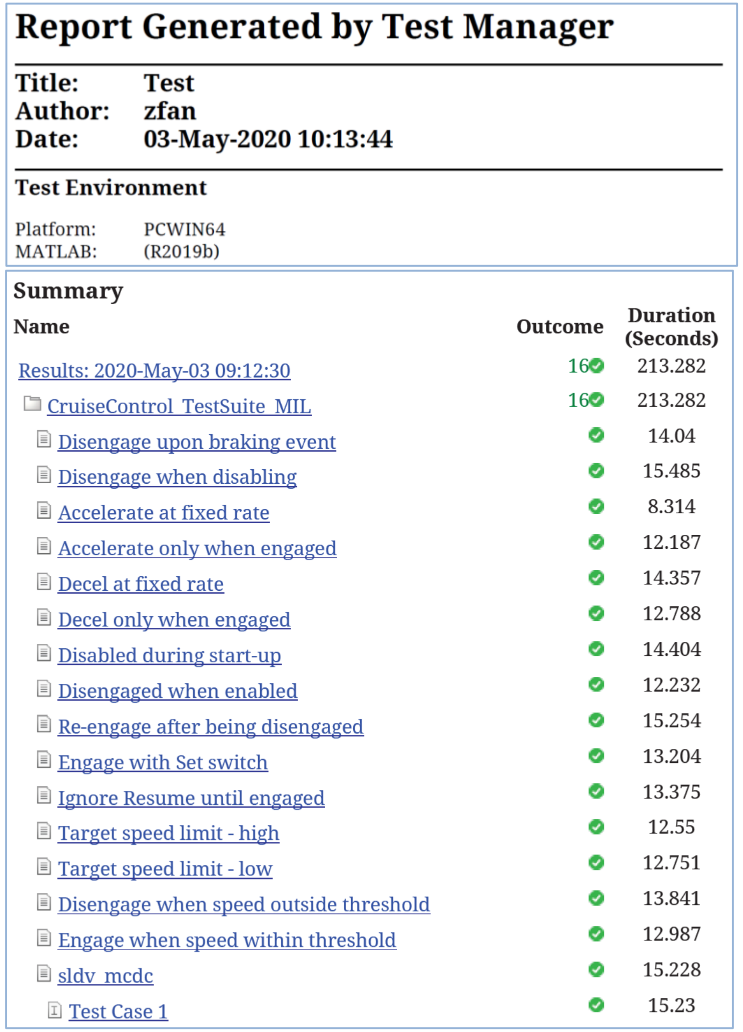
Coding Standard Checker	Disabled
Pass/Fail	

Table 1.3. Run-Time Checks Summary

Run-Time Checks	Enabled
Number of Red Checks	0
Number of Gray Checks	3
Number of Orange Checks	0
Number of Green Checks	84
Proven	100.0%
Pass/Fail	

Model-Based Design and Automotive SPICE

SWE.4.BP7: 总结并沟通结果 (动态测试)



Report Generated by Test Manager

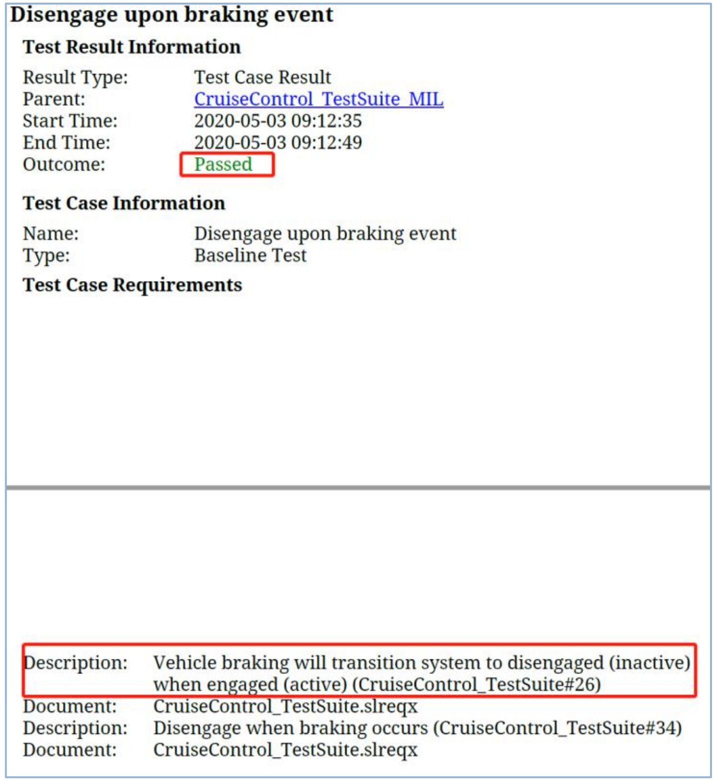
Title: Test
Author: zfan
Date: 03-May-2020 10:13:44

Test Environment

Platform: PCWIN64
MATLAB: (R2019b)

Summary

Name	Outcome	Duration (Seconds)
Results: 2020-May-03 09:12:30	16✓	213.282
CruiseControl_TestSuite_MIL	16✓	213.282
Disengage upon braking event	✓	14.04
Disengage when disabling	✓	15.485
Accelerate at fixed rate	✓	8.314
Accelerate only when engaged	✓	12.187
Decel at fixed rate	✓	14.357
Decel only when engaged	✓	12.788
Disabled during start-up	✓	14.404
Disengaged when enabled	✓	12.232
Re-engage after being disengaged	✓	15.254
Engage with Set switch	✓	13.204
Ignore Resume until engaged	✓	13.375
Target speed limit - high	✓	12.55
Target speed limit - low	✓	12.751
Disengage when speed outside threshold	✓	13.841
Engage when speed within threshold	✓	12.987
sldv_mcdc	✓	15.228
Test Case 1	✓	15.23



Disengage upon braking event

Test Result Information

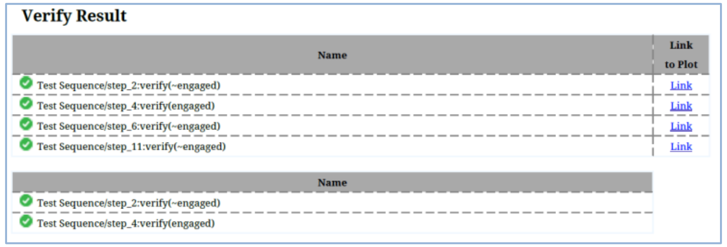
Result Type: Test Case Result
Parent: CruiseControl_TestSuite_MIL
Start Time: 2020-05-03 09:12:35
End Time: 2020-05-03 09:12:49
Outcome: Passed

Test Case Information

Name: Disengage upon braking event
Type: Baseline Test

Test Case Requirements

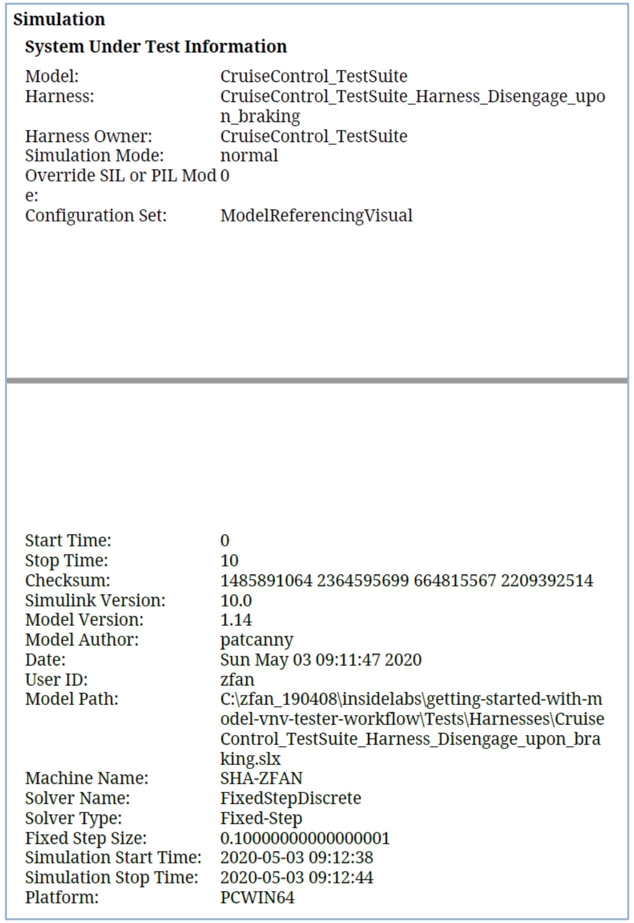
Description: Vehicle braking will transition system to disengaged (inactive) when engaged (active) (CruiseControl_TestSuite#26)
Document: CruiseControl_TestSuite.slreqx
Description: Disengage when braking occurs (CruiseControl_TestSuite#34)
Document: CruiseControl_TestSuite.slreqx



Verify Result

Name	Link to Plot
✓ Test Sequence/step_2:verify(~engaged)	Link
✓ Test Sequence/step_4:verify(engaged)	Link
✓ Test Sequence/step_6:verify(~engaged)	Link
✓ Test Sequence/step_11:verify(~engaged)	Link

Name
✓ Test Sequence/step_2:verify(~engaged)
✓ Test Sequence/step_4:verify(engaged)



Simulation

System Under Test Information

Model:	CruiseControl_TestSuite
Harness:	CruiseControl_TestSuite_Harness_Disengage_upon_braking
Harness Owner:	CruiseControl_TestSuite
Simulation Mode:	normal
Override SIL or PIL Mode:	0
Configuration Set:	ModelReferencingVisual
Start Time:	0
Stop Time:	10
Checksum:	1485891064 2364595699 664815567 2209392514
Simulink Version:	10.0
Model Version:	1.14
Model Author:	patcanny
Date:	Sun May 03 09:11:47 2020
User ID:	zfan
Model Path:	C:\zfan_190408\insidelabs\getting-started-with-model-vnv-tester-workflow\Tests\Harnesses\CruiseControl_TestSuite_Harness_Disengage_upon_braking.slx
Machine Name:	SHA-ZFAN
Solver Name:	FixedStepDiscrete
Solver Type:	Fixed-Step
Fixed Step Size:	0.10000000000000001
Simulation Start Time:	2020-05-03 09:12:38
Simulation Stop Time:	2020-05-03 09:12:44
Platform:	PCWIN64

MathWorks A-SPICE 解决方案概述

Overall mapping A-SPICE to MathWorks solution

Process Group		MathWorks Solution										
		Simulink	StateFlow	Embedded, Simulink Coder	Simulink Requirements	System Composer	Simulink Test	Simulink Check	Simulink Design Verifier	Simulink Coverage	Polyspace Bug Finder	Polyspace Code Prover
System Engineering Process Group	System Requirements Analysis				○							
	System Architectural Design				○	○						
	System Integration/ Integration Test				○		○					
	System Qualification Test				○		○					
Software Engineering Process Group	Software Requirements Analysis				○							
	Software Architectural Design				○	○						
	Software Detailed Design	○	○				○	○	○			
	Unit Construction			○								
	Software Unit Verification						○			○	○	○
	Software Integration and Integration Test				○		○					
	Software Qualification Test				○		○					